APCERT
Asia Pacific Computer Emergency Response Team

TLP:CLEAR

ANNUAL REPORT 2025

Table of Contents

From the Chair

The Asia–Pacific region continues to face a rapidly evolving and increasingly complex cyber threat environment. Our economies, governments and communities are more interconnected than ever, making collaboration not just valuable, but essential. APCERT's strength has always been its ability to unite diverse teams, share expertise openly, and respond collectively to challenges that no single economy can address alone.

It is a privilege for the Australian Cyber Security Centre (ACSC) to serve as Chair of the Steering Committee. We take on this responsibility with great appreciation for the steady, inclusive, and highly effective leadership of KrCERT/CC over the past two years. Their commitment to trust based engagement, revitalising in person cooperation, and broadening participation across APCERT has positioned our community for continued success in the years ahead.

In today's highly interconnected digital environment, we all face cyber threats from ransomware, credential theft and supply chain attacks that are growing in scale and complexity. Emerging technologies such as artificial intelligence and quantum computing present both opportunities and new risks. Meeting these challenges requires a collective effort grounded in transparency, technical excellence and mutual support.

As we look to the year ahead, APCERT will continue to focus on strengthening regional resilience through practical cooperation, expanding sustainable membership, and deepening engagement with strategic, liaison, and corporate partners. APCERT's working groups, annual drill, training programs, and information sharing initiatives remain central to this effort. These community driven activities help uplift capability across the region, promote best practice, and create the trusted relationships that are essential in times of crisis. Enhancing active participation across all teams will be a key priority.

As Chair, ACSC is committed to continuing APCERT's tradition of open collaboration, and constructive engagement. We will support initiatives that deepen technical cooperation, elevate member contributions, and further strengthen the mechanisms that allow us to share information quickly and securely across borders.

Our collective success relies on the dedication of our member teams and partners, whose commitment, expertise and generosity underpin APCERT's work. Together, we will continue to build a safer, more resilient and more reliable cyberspace for the Asia–Pacific region.

Michael Boyd
Chair, APCERT Steering Committee
Australian Cyber Security Centre (ACSC)

About APCERT

Objectives and Scope of Activities

The Asia Pacific Computer Emergency Response Team (APCERT) is a coalition of Computer Emergency Response Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs) within the Asia Pacific. The organization was established in February 2003 with the objective of encouraging and supporting the activities of CERTs/CSIRTs within the region.

The APCERT maintains a trusted network of cyber security experts in the Asia Pacific region to improve the region's awareness of malicious cyber activities and the collective abilities to detect, prevent and mitigate such activities through:

i. Enhancing the Asia Pacific's regional and international cooperation on cyber security;
ii. Jointly developing measures to deal with large-scale or regional network security incidents;
iii. Facilitating information sharing and technology exchange on cyber security among its members;
iv. Promoting collaborative research and development on subjects of interest to its members;
v. Assisting other CERTs and CSIRTs in the region to conduct efficient and effective computer emergency response; and
vi. Providing inputs and/or recommendations to help address legal issues related to cyber security and incident response across regional boundaries.

The APCERT approved its vision statement in March 2011 – "APCERT will work to help create a safe, clean, and reliable cyber space in the Asia Pacific Region through global collaboration." Cooperating with our partner organizations, we continue to work towards its actualization.

The formation of CERTs/CSIRTs at the organizational, national, and regional levels is essential for effective and efficient response against malicious cyber activities, widespread security vulnerabilities and incident coordination throughout the region. One important role of CERTs/CSIRTs is building cyber security capabilities and capacities in the region, including through education and training, to raise awareness and encourage best practices in cyber security. APCERT coordinates activities with other regional and global organisations.

The geographical boundary of the APCERT activities is the same as that of the APNIC. This covers the entire Asia Pacific, comprising 56 economies. The list of those economies is available at:
https://www.apnic.net/about-apnic/organization/apnic-region/

APCERT Members

The APCERT was formed in 2003 with 15 teams from 12 economies across the Asia Pacific region, and the membership has continued to increase since then. For further information on the APCERT membership structure and criteria, please refer to the APCERT Operational Framework:
https://www.apcert.org/documents/pdf/APCERT_Operational_Framework_18Oct2022.pdf
As of December 2025, APCERT consists of 34 Operational Members from 24 economies across the Asia Pacific region, 5 Liaison Partners, 4 Strategic Partners, and 6 Corporate Partners.

Operational Members

Team	Official Team Name	Economy
ACSC	Australian Cyber Security Centre	Australia
AusCERT	Australian Computer Emergency Response Team	Australia
bdCERT	Bangladesh Computer Emergency Response Team	Bangladesh
BGD e-GOV CIRT	Bangladesh e-Government Computer Incident Response Team	Bangladesh
BruCERT	Brunei Computer Emergency Response Team	Brunei Darussalam
BtCIRT	Bhutan Computer Incident Response Team	Bhutan
CCERT	CERNET Computer Emergency Response Team	People's Republic of China
CERT-In	Indian Computer Emergency Response Team	India
CERT-PH	Philippines National Computer Emergency Response Team	Philippines
CERT Tonga	Tonga Computer Emergency Response Team	Tonga
CERT VU	Computer Emergency Response Team Vanuatu	Vanuatu
CNCERT/CC	National Computer network Emergency Response technical Team / Coordination Center of China	People's Republic of China
CyberSecurity Malaysia	CyberSecurity Malaysia	Malaysia
ETDA	Electronic Transactions Development Agency	Thailand
GovCERT.HK	Government Computer Emergency Response Team Hong Kong	Hong Kong, China
HKCERT	Hong Kong Computer Emergency Response Team Coordination Centre	Hong Kong, China
ID-CERT	Indonesia Computer Emergency Response Team	Indonesia

ID-SIRTII/CC	Indonesia Security Incident Response Team of Internet Infrastructure/Coordination Center	Indonesia
JPCERT/CC	Japan Computer Emergency Response Team / Coordination Center	Japan
KN-CERT	Korea National Computer Emergency Response Team	Republic of Korea
KrCERT/CC	Korea Internet Security Center, Korea Internet & Security Agency	Republic of Korea
LaoCERT	Lao Computer Emergency Response Team	Lao People's Democratic Republic
mmCERT/CC	Myanmar Cyber Emergency Response Team	Myanmar
MNCERT/CC	Mongolia Cyber Emergency Response Team / Coordination Center	Mongolia
MOCERT	Macau Computer Emergency Response Team Coordination Centre	Macau, China
National CSIRT of Mongolia	National Computer Security Incident Response Team of Mongolia	Mongolia
NCSC NZ	National Cyber Security Centre New Zealand	New Zealand
Public CSIRT/CC of Mongolia	Public Computer Security Incident Response Team	Mongolia
SingCERT	Singapore Cyber Emergency Response Team	Singapore
Sri Lanka CERT|CC	Sri Lanka Computer Emergency Readiness Team Coordination Centre	Sri Lanka
TechCERT	TechCERT	Sri Lanka
TWCERT/CC	Taiwan Computer Emergency Response Team / Coordination Center	Chinese Taipei
VNCERT/CC	Viet Nam Cybersecurity Emergency Response Teams/Coordination Center	Vietnam

Chair, Deputy Chair, Steering Committee (SC) and Secretariat

At the APCERT AGM 2025, ACSC was elected as the Chair of the APCERT, and KrCERT/CC as the Deputy Chair. The terms of each Steering Committee (SC) member are as follows:

Team	Term	Other positions
ACSC	2024 - 2026	Chair
CNCERT/CC	2024 – 2026	
CyberSecurity Malaysia	2025 – 2027	
JPCERT/CC	2025 – 2027	Secretariat
KrCERT/CC	2024 – 2026	Deputy Chair
Sri Lanka CERT|CC	2025 – 2027	
TWCERT/CC	2024 – 2026	

Working Groups (WGs)

There are 7 Working Groups (**WG**s) in APCERT.

5G Security WG (formed in 2024)

Objectives

- Assess the 5G policy responses by member countries.
- Identify priority risk areas in 5G networks.
- Provide recommendations on addressing the identified risk areas.
- Develop/ improve risk and resilience best practices for securing 5G networks.

Convener (1): Sri Lanka CERT|CC

Members (5): ACSC, CNCERT/CC, CyberSecurity Malaysia, HKCERT, TechCERT

Coordinated Vulnerability Disclosure WG (formed in 2023)

Objectives

- Enhance AP regional and international cooperation.
- Jointly develop capacity to deal with global CVD challenges.

- Facilitate knowledge and experience sharing/exchange within the WG participants and APCERT members as a whole.
- Assist other CERTs in AP region and around the world.
- Find solutions to overcome challenges encountered while carrying out CVD/CVE activities.
- Develop a cooperative framework for CVD activities, including vulnerability reporting mitigation, and disclosure.

Convener (1): JPCERT/CC

Members (8): ACSC, AusCERT, BtCIRT, CERT-In, CyberSecurity Malaysia, KrCERT/CC, MNCERT/CC, TWCERT/CC

Drill WG (formed in 2017)

Objectives

- Serve as an Organizing Committee for the annual cyber drills and assist the Lead Organizing CERT
- Maintain centralized documentation for the drills, their working documents, procedures, handbooks, and feedback
- Provide continuous improvements

Convener (1): KrCERT/CC

Members (11): ACSC, AusCERT, CERT-In, CyberSecurity Malaysia, ETDA, HKCERT, JPCERT/CC, SingCERT, Sri Lanka CERT|CC, TechCERT, TWCERT/CC

Information Sharing WG (formed in 2011)

Objectives

- Improve information and data sharing within APCERT, including improving members' understanding of the value of data sharing and motivating APCERT members to exchange information and data
- Organize members to establish and enhance the necessary mechanisms, protocols and infrastructures to provide a better environment to share information and data
- Organize members to establish and enhance the necessary mechanisms, protocols and infrastructures to provide a better environment to share information and data
- Work as the Point of Contact (PoC) for APCERT to other organizations on information sharing.

Convener (1): CNCERT/CC

Members (19): AusCERT, bdCERT, Bkav Corporation, CERT-In, CyberSecurity Malaysia, ETDA, GovCERT.HK, HKCERT, Huawei PSIRT, ID-CERT, ID-SIRTII/CC, JPCERT/CC, KrCERT/CC, Microsoft, SingCERT, Sri Lanka CERT|CC, TechCERT, TWCERT/CC, VNCERT/CC

Membership WG (formed in 2011)

Objectives

- Promote collaboration and participation by all APCERT members and partners
- Establish the organizational basis to enhance the partnership with cross-regional partners

- Guide activities such as checking and monitoring for sustaining the health of the membership and partnership structure
- Support a fellowship program to promote members' participation in APCERT in-person activities

Convener (1): KrCERT/CC

Members (13): ACSC, AusCERT, BruCERT, CNCERT/CC, CyberSecurity Malaysia, HKCERT, ID-CERT, ID-SIRTII/CC, JPCERT/CC, MOCERT, Sri Lanka CERT|CC, TechCERT, VNCERT/CC

Policy, Procedure and Governance WG (formed in 2013)

Objectives

- Develop, maintain and periodically review the policies, procedures and governance structures that make up the APCERT Operational Framework. The PPGWG will advise the Steering Committee on changes required to keep APCERT fit-for-purpose and underpinned by strong governance.

Convener (1): ACSC

Members (6): AusCERT, CyberSecurity Malaysia, HKCERT, JPCERT/CC, KrCERT/CC, Sri Lanka CERT|CC

Training WG (formed in 2015)

Objectives

- Establish an overall training program to assist members to develop, operate, and improve their incident management capabilities
- Provide a channel for members to share and exchange valuable experiences with other member teams at regular intervals
- Nurture cooperation and collaboration among members, providing training activities such as conducting online or face-to-face technical workshops to enhance fellow members' cyber security capabilities and capacities in mitigating cyber incidents more efficiently and effectively

Convener (1): TWCERT/CC

Members (9): CERT-In, CNCERT/CC, ETDA, HKCERT, ID-SIRTII/CC, JPCERT/CC, KrCERT/CC, NCSC NZ, Sri Lanka CERT|CC

APCERT Website

In its role as the APCERT Secretariat, JPCERT/CC manages and updates the APCERT website: https://www.apcert.org/

APCERT Activity Report

International Activities and Engagements

International Conferences and Events

APCERT has been dedicated to representing and promoting its activities at various international conferences and events. From January to December 2025, APCERT Teams hosted, participated and/or contributed to the following events:

APEC TEL STSG Meeting (5 March – Gyeongju, Korea)

APCERT participated in the APEC TEL STSG Meeting in Gyeongju, Korea and introduced its activities during the session. APCERT has guest status in the APEC TEL community.

37th FIRST Annual Conference (22-27 June – Copenhagen, Denmark)

https://www.first.org/conference/2025/

APCERT Teams attended the Annual FIRST Conference in Copenhagen, Denmark, and shared valuable experience and expertise through various presentations.

National CSIRT Meeting (27-28 June – Copenhagen, Denmark)

APCERT teams attended the Annual Technical Meeting for CSIRTs with National Responsibility (NatCSIRT 2025) and exchanged various activity updates as well as recent projects and research.

APCERT Cyber Drill 2025 (29 July – Virtual)

Press Release (29 July 2025)

The APCERT Cyber Drill 2025 was successfully conducted to test the response capabilities of the participating APCERT Teams. The theme for the year was "When Ransomware Meets Generative AI." 24 CSIRTs from 18 economies of APCERT (Australia, Bangladesh, Brunei Darussalam, Bhutan, People's Republic of China, Chinese Taipei, Hong Kong, India, Japan, Republic of Korea, Lao People's Democratic Republic, Malaysia, Myanmar, Mongolia, Philippines, Singapore, Sri Lanka, and Thailand) participated in the drill. From the external parties, 3 CSIRTs from 2 economies of OIC-CERT and AfricaCERT participated.

ASEAN CERT Incident Drill (ACID) 2025 (21-22 October – Hybrid)

ACID 2025, led and coordinated by SingCERT, entered its 20th iteration with participation including ASEAN CERTs and APCERT Teams. The theme was "Securing Network Devices at the Edge," and the drill was completed successfully, providing an opportunity for teams to improve their knowledge and skills on investigation and response.

APCERT Annual General Meeting (AGM) and Conference 2025 (25-27 November – Sydney, Australia)

The APCERT Annual General Meeting (AGM) and Conference were held in Sydney, Australia. The program overview is as follows:

- 25 November: APCERT Annual General Meeting
- 26 November: APCERT Closed Conference
- 27 November: APCERT Open Conference

Other International Activities and Engagements

DotAsia

The APCERT serves as a member of the Advisory Council of DotAsia to assist in policy development and relevant community projects. HKCERT represented APCERT in attending the meetings of the Advisory Council.

Forum of Incident Response and Security Teams (FIRST)

Many APCERT teams are also members of the FIRST. The APCERT signed a Memorandum of Understanding (MoU) with the FIRST on 6th November 2020 to enhance further collaboration.

STOP. THINK. CONNECT (STC)

The APCERT has collaborated with STOP. THINK. CONNECT (STC) under a MoU since June 2012 to promote cybersecurity awareness and a more secured network environment.

Asia Pacific Network Information Security Centre (APNIC)

The APCERT and the Asia Pacific Network Information Centre (APNIC) signed an MoU in 2015, which was renewed in 2019

Africa Computer Emergency Response Team (AfricaCERT)

The APCERT and AfricaCERT signed an MoU in 2019.

APCERT SC Meeting

From January to December 2025, the SC members held 5 teleconferences and 2 face-to-face meetings to discuss the APCERT operations and activities.

Date	Location
15 January	Teleconference
10 March	Face-to-face meeting (Seoul)
22 May	Teleconference
28 July	Teleconference
9 October	Teleconference
18 November	Teleconference
25 November	Face-to-face meeting (Sydney)

APCERT Training

The APCERT held 6 training calls in 2025 to exchange technical expertise, information, and ideas.

Date	Title	Presenter
24 February	Ransomware Trends and Case Studies	KrCERT/CC
29 April	Centralized Threat Monitoring/Threat Hunting	NRD Cyber Security
24 June	Using AI to Enhance Incident Response in CERTs	CyberSecurity Malaysia
26 August	Introduction to Malware Analysis Methods	Huawei PSIRT
28 October	Cybersecurity Exercises for Taiwan's Government Agencies and Critical Infrastructures	TWCERT/CC
30 December	Impact of AI on Cyber Threat Intelligence	CERT-In

For further information on the APCERT, please visit the APCERT website or contact the APCERT Secretariat as below.

URL: https://www.apcert.org/

Email: apcert-sec@apcert.org

Disclaimer on Publications

The contents of "Activity Reports from Members" and "Activity Reports from APCERT Partners" are written by each APCERT members and partners based on their individual analysis. Responsibility for the information and views expressed in each report lies entirely with the authors.

Activity Reports from Members

ACSC

Australian Cyber Security Centre

1. Highlights of 2025

1.1 Summary of major activities

In FY2024–25, ACSC received over 42,500 calls to the Australian Cyber Security Hotline, a 16% increase from the previous year. ACSC also responded to over 1,200 cyber security incidents, an 11% increase. During FY2024–25, ACSC notified entities more than 1,700 times of potentially malicious cyber activity – an 83% increase from last year – highlighting the ongoing need for vigilance and action to mitigate against persistent threats. ACSC works with federal and state governments, international counterparts, and industry partners to identify and disrupt malicious cyber threats.

1.2 Achievements & milestones

ACSC is the Australian Government's technical authority on cyber security and below are some of our key achievements and milestones during FY2024–25.

What ACSC saw in Financial Year 2024-2025

- Answered over 42,500 calls to the Australian Cyber Security Hotline, up 16% and on average 116 calls per day.
- Received over 84,700 cybercrime reports to ReportCyber, down 3%. On average a report every 6 minutes, consistent with last year.
- Average self-reported cost of cybercrime per report for businesses, up 50% (AUD $80,850).

What ACSC did in Financial Year 2024–25

- Responded to over 1,200 cyber security incidents, an 11% increase from last year.
- Notified entities of potential malicious cyber activity more than 1,700 times, up 83%.
- Australian Protective Domain Name System blocked customer access to 334 million malicious domains, up 307%.
- Cyber Threat Intelligence Sharing (CTIS) partners grew by 13% to over 450 partners. To date, the CTIS platform shared over 2,984,000 indicators of compromise.
- Published or updated 26 PROTECT publications, including guidance publications related to the Essential Eight

Maturity Model and updates to the Information Security Manual.
- ACSC's Cyber Security Partnership Program grew by 11% to over 133,000 partners.
- Led 17 cyber security exercises, involving over 120 organisations, to strengthen Australia's resilience.

2. About ACSC

2.1 Introduction

- ACSC brings together capabilities to improve Australia's national cyber resilience. Its services include:
- providing the Australian Cyber Security Hotline, which is contactable 24 hours a day, 7 days a week, via 1300 CYBER1 (1300 292 371)
- publishing technical advice alerts, advisories and notifications on significant cyber security threats
- monitoring cyber threats and sharing intelligence with partners, including through the Cyber Threat Intelligence Sharing (CTIS) platform
- helping Australian organisations respond to cyber security incidents
- providing exercises and uplift activities designed to enhance the cyber security resilience of Australian organisations
- supporting collaboration between over 133,000 Australian organisations and individuals on cyber security issues through ACSC's Cyber Security Partnership Program.

2.2 Resources

- ACSC brings together capabilities from partner agencies and works closely with partners across Government, including the Department of Home Affairs, Australian Federal Police, Department of Foreign Affairs and Trade, and industry.

2.3 Constituency

ACSC has a whole-of-economy remit to help make Australia the most secure place to connect online, providing cyber security advice and assistance to Australian governments, industry, and individuals.

3. Activities & Operations

3.1 Incident handling reports

ACSC categorises each cyber security incident it responds to on a scale of Category 1 (C1), the most severe, to Category 6 (C6), the least severe. Cyber security incidents are categorised on severity of impact and significance of the organisation's impact to Australia.

	Member(s) of the public	Small organisation(s) Sole traders	Medium-sized organisation(s) Schools Local government	State government Academia/R&D Large organisation(s) Supply chain	Federal government Government shared services Regulated critical infrastructure	National security Systems of National Significance
Sustained disruption of essential systems and associated services	C6	C5	C4	C3	C1	C1
Extensive compromise	C6	C5 7	C4 10	C3 7	C2 2	C1
Isolated compromise	C6	C5 52	C5 79	C3 51	C3 28	C2
Coordinated low-level malicious attack	C6 1	C6	C5 2	C4 2	C3 3	C3 1
Low-level malicious attack	C6 1	C6 128	C5 65	C4 109	C4 94	C3 9
Unsuccessful low-level malicious attack	C6	C6 33	C6 12	C6 183	C6 334	C6 40

Figure 1: Cyber security incidents by severity category for FY2024–25 (total 1,253)

3.2 Statistics

In FY2024–25, ACSC received over 42,500 calls to the Australian Cyber Security Hotline, a 16% increase from the previous year. On average, 116 calls per day, an increase from 100 calls per day from the previous year. ACSC also responded to over 1,200 cyber security incidents, an 11% increase from the previous year.

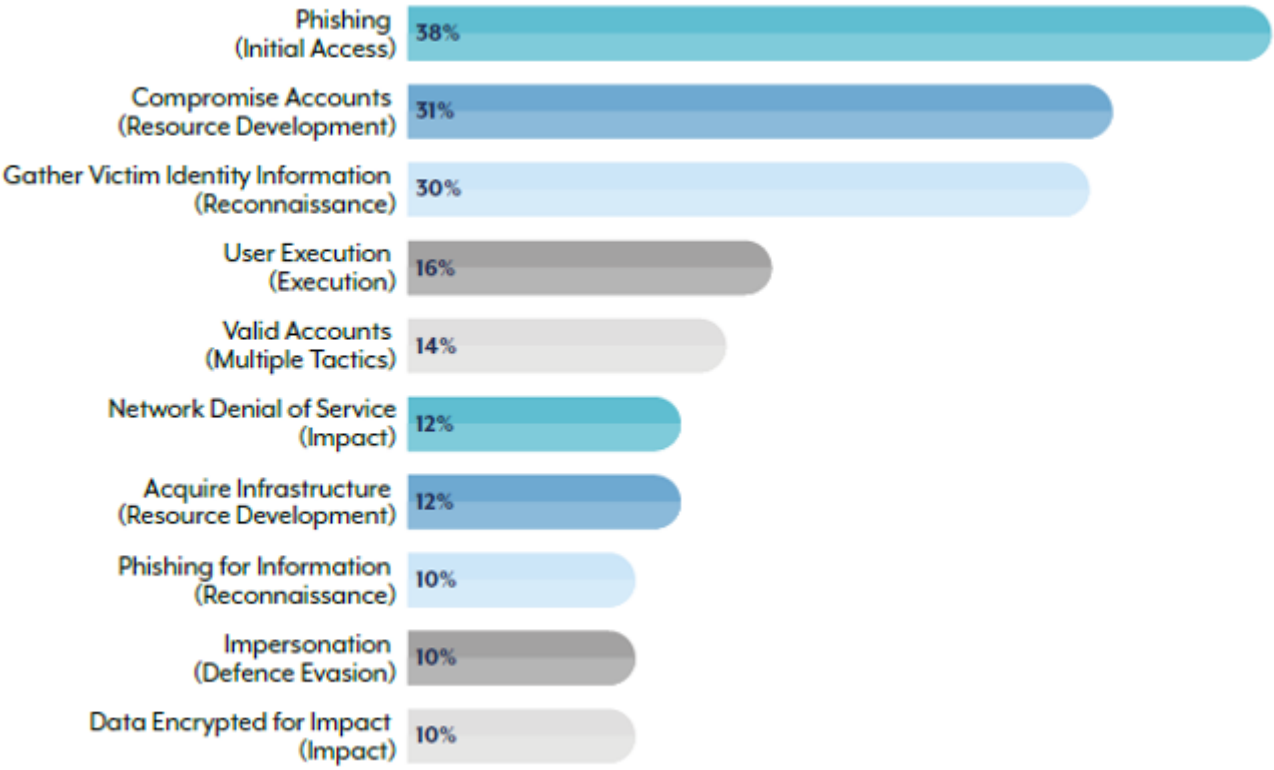
Compared to FY2023–24, there was a notable increase in successful and unsuccessful low-level malicious attacks. While the raw number of high-end attacks is lower this year, ACSC nevertheless continued to see the use of complex and sophisticated tradecraft.

Critical infrastructure is, and will continue to be, an attractive target for state-sponsored cyber actors, cybercriminals,

and hacktivists, primarily due to large sensitive data holdings and the critical services that support Australia's economy. Critical infrastructure made up 13% of all incidents for the reporting period.

Australia's federal, state, and local governments remain the most frequently reporting sectors for incidents. ACSC observed an increase in reporting from financial and insurance services for the reporting period, compared to the previous period.

ACSC analysed incidents using the MITRE ATT&CK framework. The most prevalent techniques are detailed below.



3.3 Publications and advisories

In FY2024–25, ACSC published a combination of 108 alerts, advisories, knowledge articles and publications on both cyber.gov.au and the Partner Portal.

ACSC also published or updated 26 PROTECT publications, including guidance publications related to the Essential Eight Maturity Model.

3.4 New services

To bolster a freer flow of information sharing between industry and ACSC, on 25 November 2024, the Australian Government passed the *Intelligence Services and Other Legislation Amendment (Cyber Security) Act 2024*. The amendment legislates a 'limited use' obligation for ACSC. This means any information that an Australian organisation voluntarily provides to ACSC about a cyber security incident or potential cyber security incident (including vulnerability information) cannot be used for regulatory purposes.

4. Events organized / hosted

4.1 Training

ACSC delivers a **Government Uplift Program**, which assists key government entities to strengthen their cyber defences through a range of targeted activities. It delivers hands-on technical assessments of an entity's environments and systems to determine the effectiveness of both prevention and detection security controls as well as also uplift Essential Eight maturity.

ACSC delivers **Privileged User Training** (PUT) that offers government and critical infrastructure privileged users an overview of the best practices in cyber security. Attendees acquire practical knowledge on tools and techniques, learn to manage cyber security risk within an enterprise setting, and explore approaches to cultivating a positive security culture. Most importantly, the course delves deeply into how privileged users can implement tactics to reduce the occurrence of cyber security incidents in their daily work. At the end of FY2024–25, PUT had been delivered to approximately 7,500 participants across 460 entities.

4.2 Drills & exercises

Overall, ACSC led 17 cyber security exercises, involving over 120 organisations, to strengthen Australia's resilience.

ACSC's National Exercise Program (NEP) helps critical infrastructure and government organisations validate and strengthen Australia's nationwide cyber security arrangements. The program uses exercises and other readiness activities that target strategic decision-making as well as operational and technical capabilities.

In 2024, the NEP delivered the inaugural ACSC Cyber Drill. This provided an opportunity for ACSC Network Partner cyber defence teams to gain valuable hands-on experience detecting and responding to cyber incidents, simulating the TTPs of real-world malicious cyber actors. Technical teams from across key critical infrastructure sectors participated in the

ACSC Cyber Drill, which ran via a cyber range and included:

- 25 teams competing in up to 3 knockout rounds
- teams completing a Live Fire Exercise (LFE) each round
- LFEs covering 52 different MITRE ATT&CK techniques
- teams progressing to the next round based on their LFE scores and completion times.

The ACSC Cyber Drill exercised the technical capabilities of ACSC network partners, enhancing their ability to detect and respond to malicious cyber activity at speed. The team-based approach to the ACSC Cyber Drill promoted collaboration and capability enhancement and enabled cyber security teams to rehearse and improve their responses to cyber incidents while using a virtual environment designed to mirror a corporate network, complete with a range of common industry security tools.

4.3 Conferences and seminars

ACSC hosted the 2025 APCERT Annual General Meeting and Conference on 25–27 November. The theme *Cyber Horizons: Strengthening Regional Resilience – Together* reflected our shared commitment to collaboration in an evolving cyber threat landscape. The event brought together 21 CERTs/CSIRTs from 18 of APCERT's 24 economies, 3 APCERT Partners, plus industry representatives and Australian Government officials. Over 3 days, participants engaged in strategic discussions, technical presentations, and team-building activities designed to strengthen operational trust and resilience across the region.

5. International Collaboration

5.1 International partnerships and agreements

ACSC engages with international partners to increase cyber threat awareness and to uplift cyber security for both the Australian Government and our partners. Engagement with partners also provides opportunities to improve regional cyber security and build strategic relationships. ACSC monitors cyber threats targeting Australian interests, and provides advice and information, including through international networks of Computer Emergency Response Teams such as APCERT.

5.1.1 Capacity building

As Secretariat of the Pacific Cyber Security Operations Network (PaCSON), ACSC also facilitated the sharing of cyber threat information for a network of Pacific working-level cyber security experts.

5.1.2 Drills & exercises

ACSC participated in the annual APCERT drill. The drill provided an opportunity to collaborate with regional cyber security

partners to ensure we are well prepared to respond to a potential cyber security incident.

5.1.3 Seminars & presentations

ACSC delivered presentations to a number of international partners in support of Australian and whole-of-government international engagement objectives.

5.2 Other international activities

Cybercrime is borderless in nature and requires significant international collaboration to be countered effectively. During FY2024–25, global law enforcement disruption efforts have successfully prevented harm against Australian individuals and organisations, including through disruption of a scam centre suspected of stealing money from Australians.

6. Future Plans

6.1 Project REDSPICE

Looking ahead, we are focused on delivering and implementing the REDSPICE (**R**esilience, **E**ffects, **D**efence, **SP**ace, **I**ntelligence, **C**yber, **E**nablers) Project. Under REDSPICE, ACSC capabilities will be enhanced to further protect Australians from cyber adversaries.

7. Conclusion

Through strong partnerships, ACSC works to defend Australians from cyber threats and make our country a harder target for malicious cyber actors. Australia cannot face increasingly sophisticated cyber threats alone. Through networks like APCERT, we continue to partner with organisations to share information and expertise to collectively face shared cyber threats.

AusCERT

Australian Computer Emergency Response Team

1. Highlights of 2025

AUSCERT continues operation and improving services in spite of resources being limited. Being just operational is not enough in this interconnected field of work of being a CERT/CSIRT. Therefore, AUSCERT recognises that the highlights are not just the internal milestones and achievements performed but also the external assistance to the CERT/CSIRT community in a manner that is aligned with the requirements of an APCERT Operational Member.

1.1 Constituency focused highlights

AUSCERT has:

- Improved the flow of creating security bulletins based from PSIRT sources
- Introduced more training courses in type and frequency of delivery
- Install Tabletop exercises as a stable ongoing service to the constituency
- Further automated phishing takedown requests
- Create APIs for the constituency to use

1.2 Community focused highlights

AUSCERT has:

- Assisted a CERT outside the Asia Pacific region in using IntelMQ to process their feeds
- Assisted KrCERT/CC in the tabletop exercise at the APCERT AGM
- Assisted a CERT in the Asia Pacific region in performing a Strategy and Service review

2. About CSIRT

2.1 Introduction

AUSCERT is a leading Cyber Emergency Response Team for Australia and provides information security advice to its members, including the higher education sector. As a not-for-profit security group based at the University of Queensland's (UQ) Information Technology Services (ITS), AUSCERT is the single point of contact for dealing with cyber security incidents affecting or involving member networks. AUSCERT helps members prevent, detect, respond to and mitigate cyber and Internet based attacks.

2.2 Establishment

AUSCERT was officially established on 8 March 1993 through the collaboration of three Brisbane based universities, including the University of Queensland.
Formed in 1993, AUSCERT is one of the oldest CERTs in the world and was the first CERT in Australia to operate as the national CERT, which it did until 2010.
Over time, as the Internet grew and government, business and ordinary users began to use the Internet for daily communications and business, AUSCERT's focus changed from being university centric to include the interests of all sectors.

2.3 Resources

AUSCERT is self-funded and covers its operating costs through a variety of sources including member subscriptions, the annual AUSCERT conference and service contracts. As an active member of the Forum for Incident Response and Security Teams (FIRST) and Asia Pacific Computer Emergency Response Team (APCERT), AUSCERT has access to accurate, timely and reliable information about emerging computer network threats and vulnerabilities on a regional and global basis.

2.4 Constituency

AUSCERT, due to its origins, continues to assist Australian private and public organisations and companies.
This is made possible by providing priority incident handling and additional services to our membership base of which covers all industry definitions under the ANZ Standard Industry Classification.
AUSCERT works closely with Australian government agencies, industry and technology vendors and provides computer security and incident handling advice to a range of subscribers throughout Australia, New Zealand and the Asia-Pacific region. All Australian universities and the majority of New Zealand universities are members of AUSCERT and there is a

strong relationship with the Council of Australian University Directors of Information Technology (CAUDIT). AUSCERT participates in the Australian government's IT Security Experts' Advisory Group (ITSEAG).

3. Activities & Operations

3.1 Scope and definitions

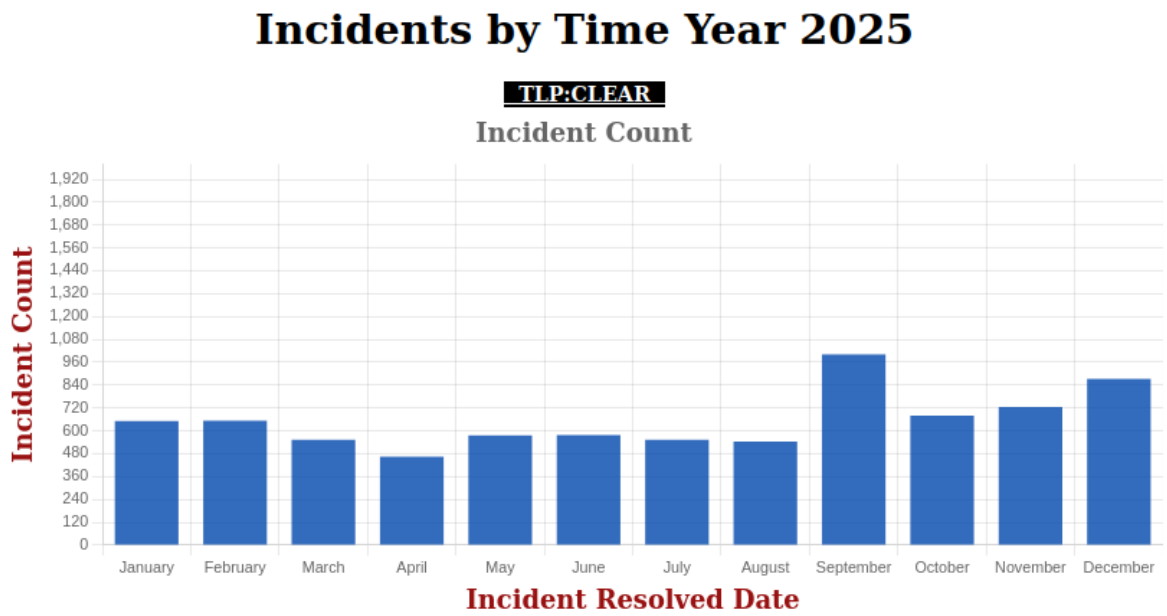
AUSCERT monitors and evaluates global cyber network threats and vulnerabilities and remains on-call for members after hours. AUSCERT publishes the Security Bulletin Service, drawing on material from a variety of sources, with recommended prevention and mitigation strategies.
Services provided are listed as:

- Incident Support [3.2]
  https://auscert.org.au/services/incident-support/
- Early Warning Service
  https://auscert.org.au/services/vulnerability-management/
- Malicious URL Feed
  https://auscert.org.au/services/threat-intelligence/
- Security Bulletin Service [3.3]
  https://auscert.org.au/services/vulnerability-management/
- Member Security Incident Notification's (MSIN) [3.4]
  https://auscert.org.au/services/vulnerability-management/
- Critical Member Security Incident Notification's (Critical MSIN) [3.5]
  https://auscert.org.au/services/vulnerability-management/
- Phishing take-down
  https://auscert.org.au/services/incident-support/
- Sensitive Information Advisories (SIA) [3.6]
  https://auscert.org.au/services/vulnerability-management/
- AUSCERT's member only Slack
- AUSCERT Conference
  https://auscert.org.au/events/auscert2025-evolve-and-thrive/

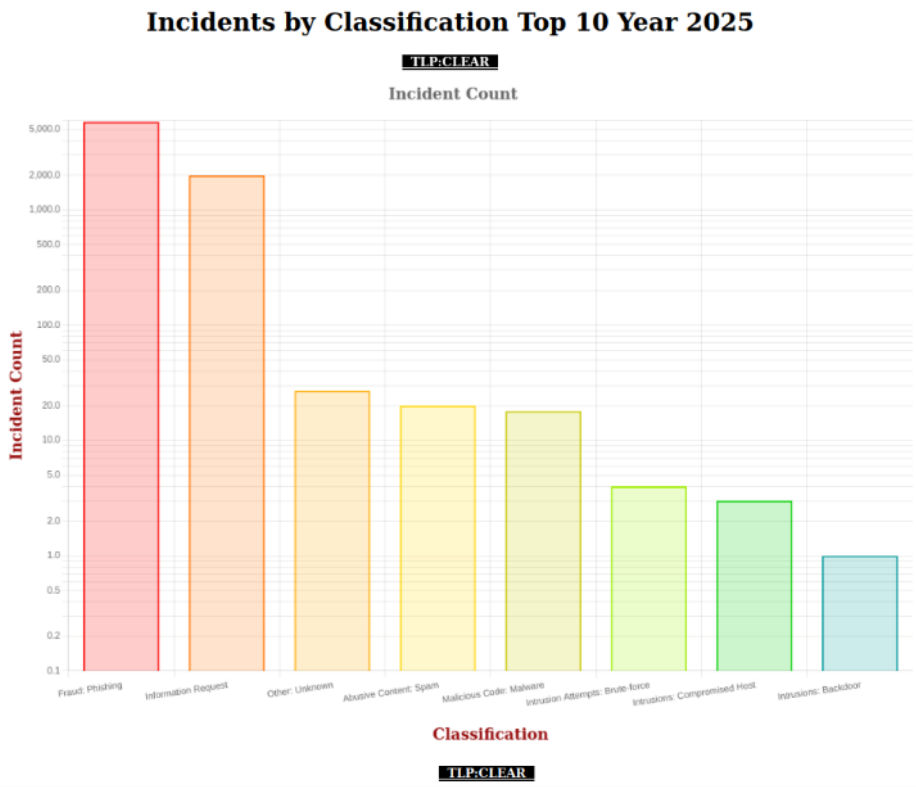
3.2 Incident Support

AUSCERT's Incident Support Service (sometimes referred to as incident response) includes incident coordination and incident handling, both of which are standard inclusions as part of AUSCERT's membership services. As a 24/7

membership benefit, it is perhaps AUSCERT's most focal service offering

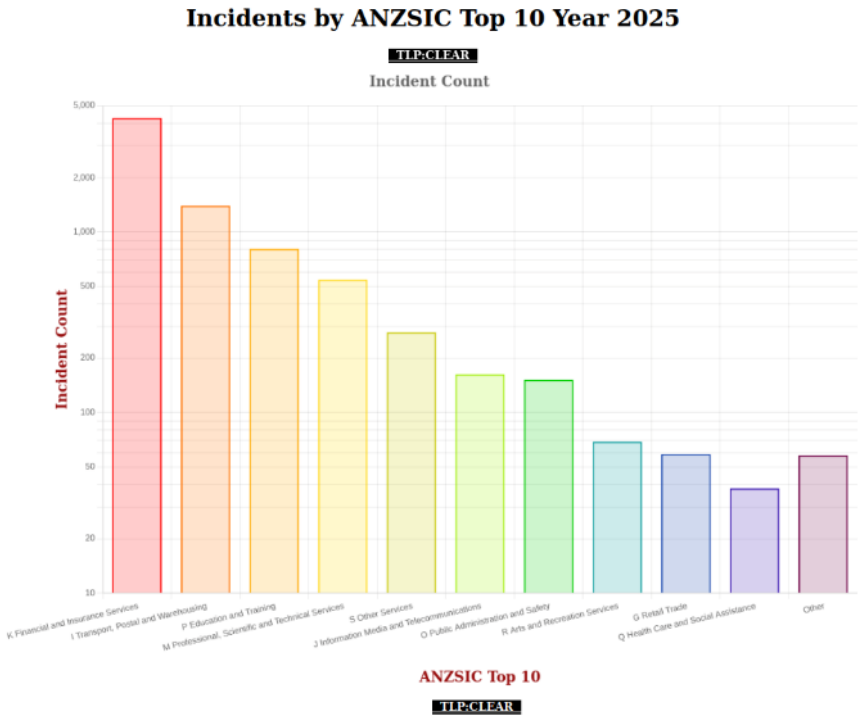


The diagram above shows the statistics of incidents that required handling for the calendar year of 2025. Overall, AUSCERT serviced 7850 tickets which resulted in just over 31 tickets per business day of operation.



Counts	Classification
5794	Fraud: Phishing
1983	Information Request
27	Other: Unknown
20	Abusive Content: Spam
18	Malicious Code: Malware
4	Intrusion Attempts: Brute-force
3	Intrusions: Compromised Host
1	Intrusions: Backdoor

A vast majority of the work continue to be around handling of phishing sites.



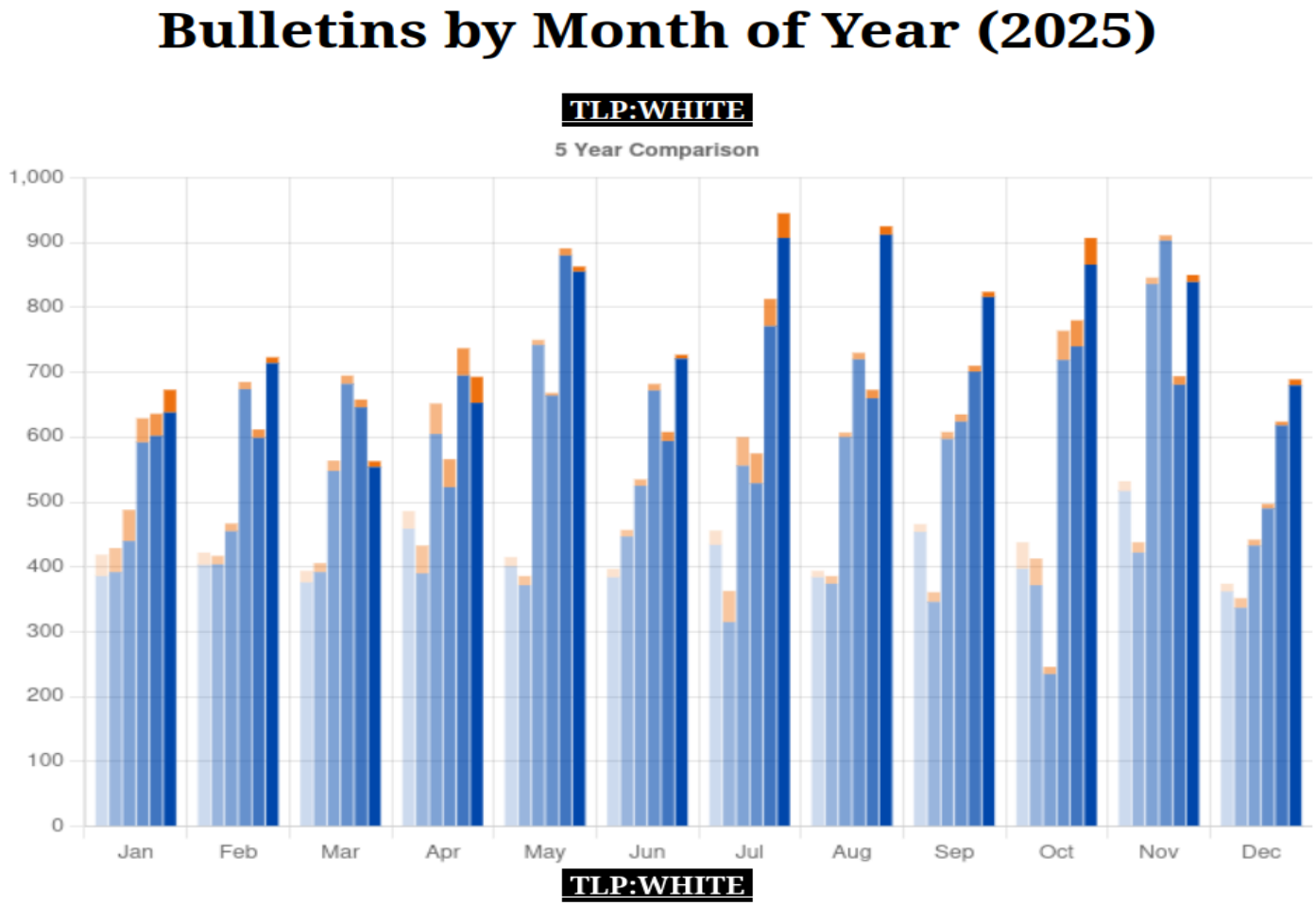
Counts	ANZSIC
4282	K Financial and Insurance Services
1398	I Transport, Postal and Warehousing
808	P Education and Training
545	M Professional, Scientific and Technical Services
278	S Other Services
163	J Information Media and Telecommunications
152	O Public Administration and Safety
69	R Arts and Recreation Services
59	G Retail Trade
3	Other

Incidents have happened across a wide varied range of industry. The following diagram, on a log scale, shows the top 10 industries with respect to the number of incident tickets handled.
The industry definition used is the Australian and New Zealand Standard Industrial Classification (ANZSIC) and further details can be found at:
https://www.abs.gov.au/statistics/classifications/australian-and-new-zealand-standard-industrial-classification-anzsic/latest-release

3.3 Security Bulletins

AUSCERT distributes security advisories and bulletins to its members by email on each items as well as a summary of the day's volume.
Bulletins are published in a standardised format with a consistent approach to highlighting the maximum CVSS score, as well as the maximum EPSS that the patch release is addressing. Also, notes are made about whether a CVE is in the Known Exploited Vulnerability (KEV), a list maintained by the United States of America's Cybersecurity Infrastructure Security Agency (CISA).

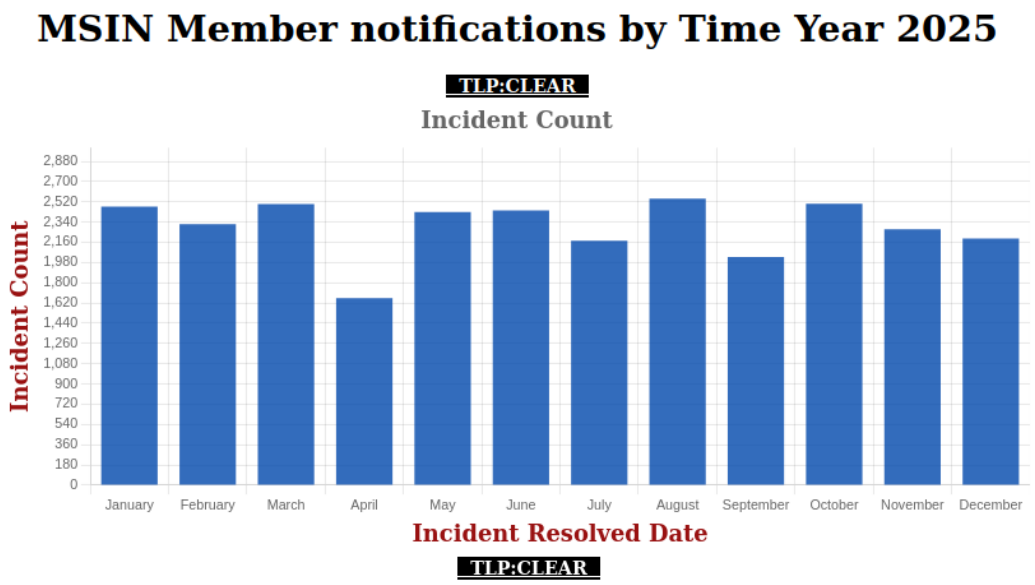
In 2025, 9155 External Security Bulletins (ESBs) and 227 AUSCERT Security Bulletins (ASBs) were published.



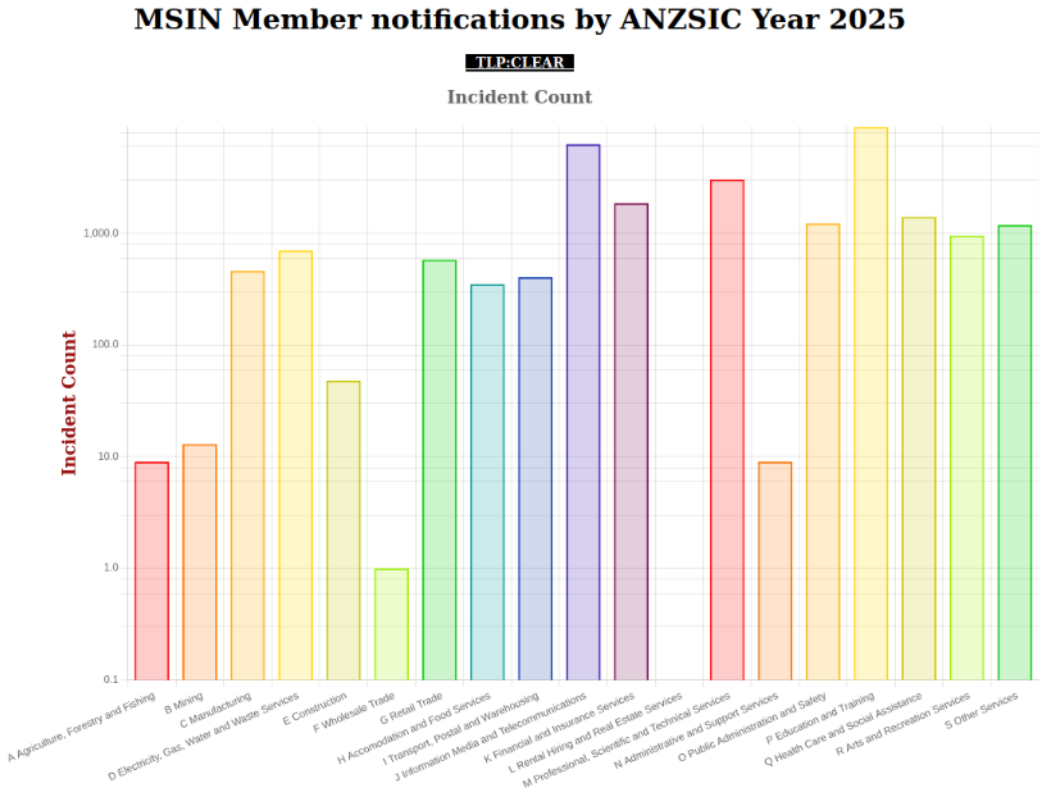
3.4 Member Security Incident Notifications (MSIN)

AUSCERT members benefit from its considerably large overseas and local threat intelligence feeds with respect to incidents that have been detected by other parties but concern the members.

There are several categories of incidents and this service has been running for members for several years. These notifications are a mix of Indicators of Vulnerabilities (IoV) and Indicators of Compromise (IoC).



The following shows the distribution of the year's notifications with respect to the Industry Classification.



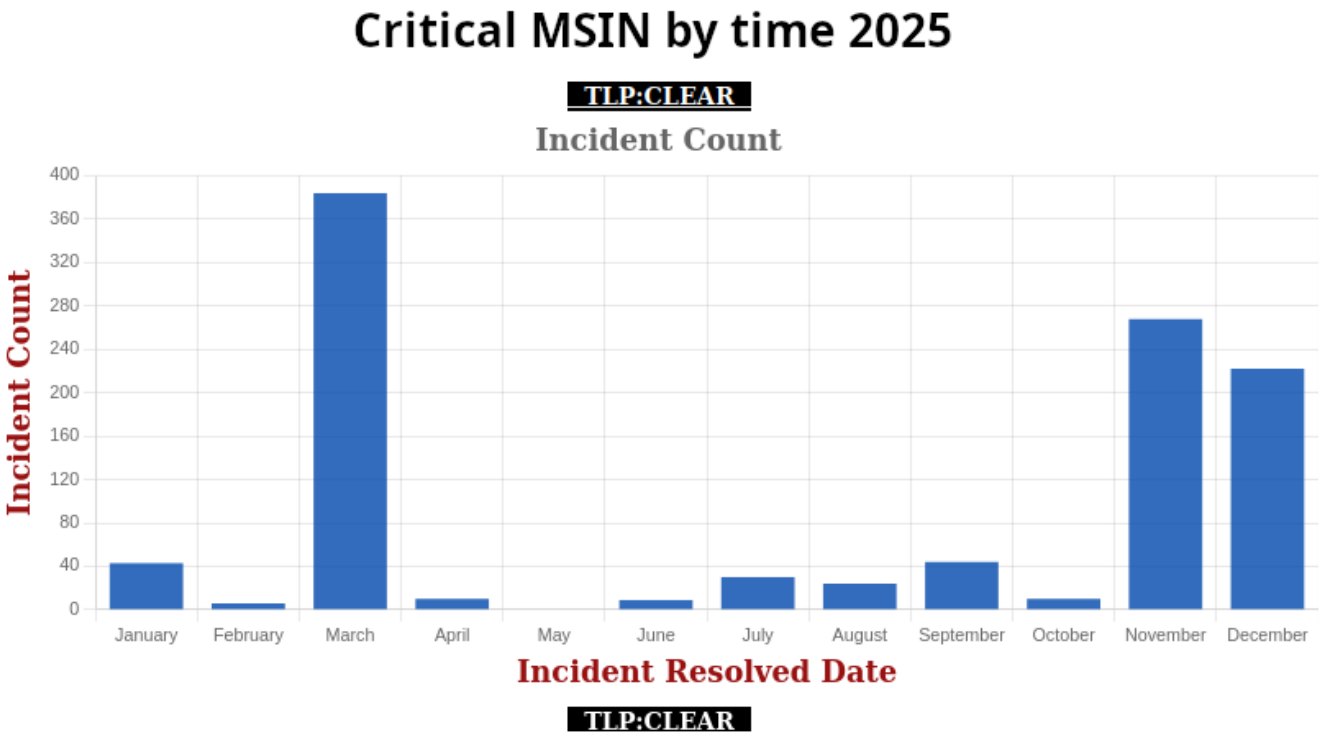
Counts	ANZSIC Top 10 + Other
8977	P Education and Training
6291	J Information Media and Telecommunications
3044	M Professional, Scientific and Technical Services
1872	K Financial and Insurance Services
1406	Q Health Care and Social Assistance
1230	O Public Administration and Safety
1190	S Other Services
957	R Arts and Recreation Services
705	D Electricity, Gas, Water and Waste Services
582	G Retail Trade
1299	Other

3.5 Critical Member Security Notifications (Critical MSIN)

Critical notifications are issued when serious vulnerabilities, such as zero-day threats, are detected. The AUSCERT team researches current and emerging threats to determine potential impact to members based on their nominated IPs and domains.

Critical MSINs are flagged for urgent action and contain details of the threat, references and mitigation strategies for high-priority risks.

The Critical MSIN service notified organisations, one thousand and fifty (1050), times within the period of Year 2025.



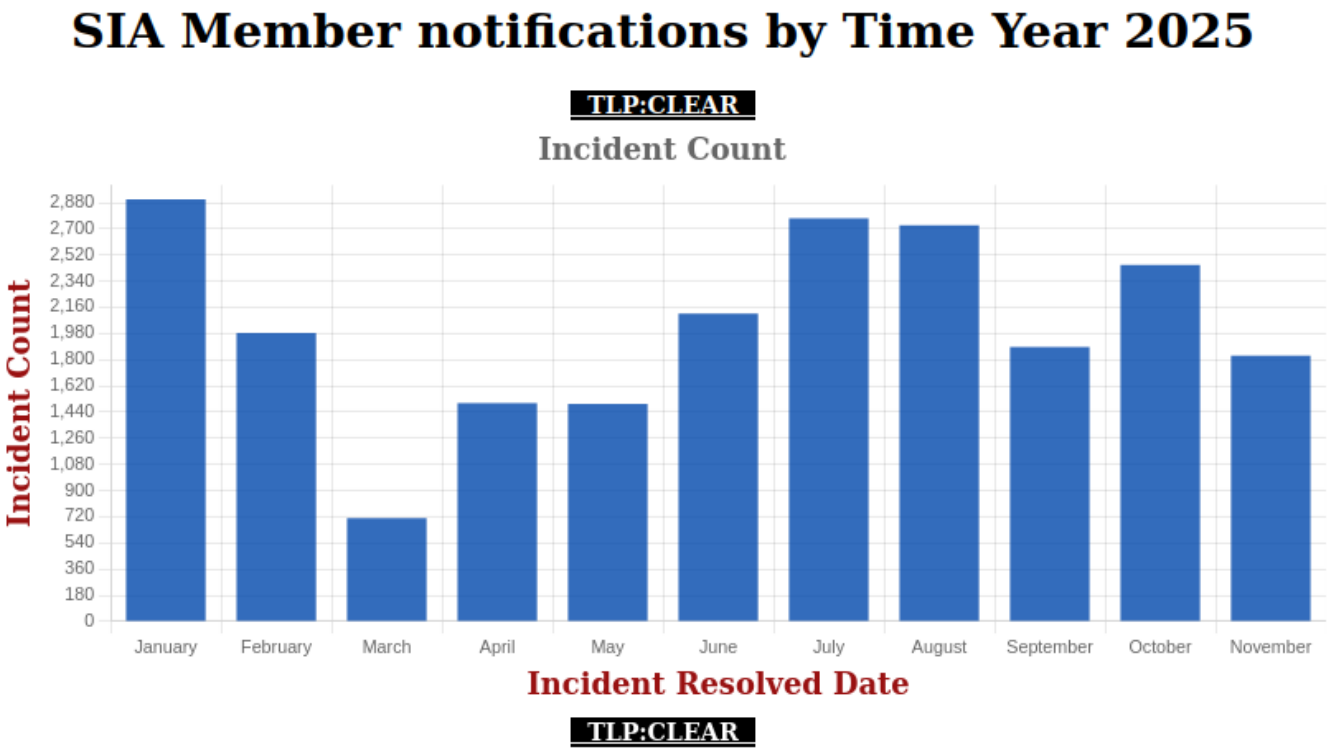
Counts	ANZSIC Top 10 + Other
304	P Education and Training
147	K Financial and Insurance Services
124	J Information Media and Telecommunications
71	M Professional, Scientific and Technical Services
71	O Public Administration and Safety
45	I Transport, Postal and Warehousing
43	Q Health Care and Social Assistance
35	R Arts and Recreation Services
32	G Retail Trade
23	S Other Services
155	Other

3.6 Sensitive Information Alerts (SIA)

When leaked credentials or other sensitive material related to the constituency is identified, they are notified on the day of collection. The AUSCERT team utilises a wide range of sources, including the dark web, ransomware leak sites,

international CERTs, and trusted partners.

The alerts typically involve compromised credentials, such as usernames in the form of email addresses and associated authentication strings (hash or passwords). This sensitive information is provided via an encrypted file for your internal review and action.



The Sensitive Information Alerts (SIA) service sent out, twenty-two thousand, three hundred and seventy-four (22374), alerts within the period of Year 2025.

Counts	ANZSIC Top 10 + Other
10272	P Education and Training
3254	K Financial and Insurance Services
1360	J Information Media and Telecommunications
1051	O Public Administration and Safety
1042	G Retail Trade
983	I Transport, Postal and Warehousing
960	M Professional, Scientific and Technical Services
891	R Arts and Recreation Services

665	Q Health Care and Social Assistance
320	S Other Services
1576	Other

3.7 Publications

3.7.1 ADIR

The AUSCERT Daily Intelligence Review is a publication sent to members and public about the news items that affect cyber security in the Australian context.

3.7.2 Week in Review

Every week the highlights of the week's Incident handling and bulletin publications are listed in the Week-In-Review.

3.7.3 Social Media

Publishing is great but getting the word out of a publication or an event is best done using the current social media platforms. AUSCERT supports heralding news and events through two platforms, Twitter, LinkedIn, and Facebook.

3.7.4 Newsletter

Newsletters are also supported in getting the word out about what AUSCERT is doing. Member newsletters come out every two (2) months to keep members engaged in AUSCERT activities.

3.7.5 Blog Post

Depending upon the gravity of news, articles are published for the public of ongoing issues. This is placed in the AUSCERT website in the Blog sections.

3.7.6 Podcast

Every month there is a podcast that discusses events of the month and an interview of a prominent cyber security figure in the Australian context.

4. Events organized / hosted

4.1 Training

AUSCERT provides nine (9) types of cyber security training courses, suitable for cyber security, IT or risk management professionals, as well as cyber security awareness training that delivers important foundational knowledge in an engaging way that online, self-service training does not. Training courses are available to everyone, membership is not required. These training courses have been delivered throughout the year.

4.2 Tabletop Exercises

AUSCERT's Tabletop Exercises help organisations enhance their cyber incident preparedness through customised, scenario-driven simulations that test decision-making and response strategies. Each includes tailored information gathering, an interactive simulation, a detailed post-exercise report, and a follow-up meeting to ensure continuous improvement in cyber resilience. Table top exercise were delivered throughout 2025 to organisations that have recognised that these activities assist in validating and verifying their approach to cyber security.

4.3 AUSCERT Conference 2025

The AusCERT Conference 2025, took place from 20th May - 23rd May 2025 at the Star, Gold Coast with the theme of "Evolve and Thrive". The conference included more than 50 presenters of ranging topics on cyber security. The conference has two format with the first two days with tutorial and the latter two days with speakers talking about contemporary topics on cyber security.

5. International Collaboration

5.1 International partnerships and agreements

AUSCERT maintains relationships with various like-minded CERTs and CSIRTs around the world and carry these relationships with a mutual understanding on what are areas of collaboration. These relationships are active and are worked beyond written agreements. During 2025 AUSCERT has assisted another CERT outside the Asia Pacific region on using IntelMQ to handle their cyber security information feeds.
AUSCERT also maintains membership with Asia Pacific Computer Emergency Response Team (APCERT) and the Forum of Incident Response and Security Teams (FIRST).

5.2 Capacity building

5.2.1 APCERT Drill 2025

Every year, AUSCERT participates in an exercise that tests its operational readiness to the full. The Asia Pacific Computer Emergency Response Team (APCERT), of which AUSCERT is a member, conducts an annual drill among its constituents. This year, the theme was "When Ransomware meet Generative AI". The drill fosters communication between the CERTs in the region and beyond. In all, 24 APCERT CERT/CSIRT teams from 18 economies participated.

5.2.2 ACID 2025

AUSCERT was also invited in participating the ASEAN Cyber Incident Drill hosted by Singapore Cyber Security Agency. This well composed drill allowed further interaction with the CERT/CSIRT community and validate internal processes and skill sets.

6. Conclusion

AUSCERT continues to assist the constituency of Australia in the face of a changing workforce composition and tooling. AUSCERT, as any other CERT/CSIRT, are in the maintenance industry of keeping the internet safe and resilient. When something breaks or something attacks the resources we set out in our charter to protect, we gather information, find out what went wrong, alert and assist in the process of enabling a fix. In performance of that task the ingesting of information from sources, embellishing that information with correlating data, derive information into knowledge and then republishing it, as a value-added product, is a chain of work tasks we are all familiar with.

The value that is added to this work depends upon the sources garnered, the domain knowledge and skills of the staff deriving actionable intelligence out of the data. The amount of value created depends on the volumes of sources that can be ingested and turned into the final product, be it an advisory or an action such as a too familiar phishing take-down request. This type of work seems ripe for the introduction of Machine Learning along with models that are able to generate sensible phrases and even enabling these models to be agentic.

Apprehension to its introduction comes from the temptation to do drop-in replacement of models into tasks that previously performed by staff. Difficulties from this shift in workflow may not be the capturing of domain knowledge staff into machine learning models, or re-skilling and re-purposing the existing human capital, but it may be in the reception of the final outcome. For the final outcome of what CERT/CSIRT produce is used by a human. Our constituency are people, who at times are under a level of stress. The best service is not to forget that our value is from the message received which can best be served by having that human connection to our constituency. It is by providing assistance to our constituency, how to understand and affect the most use of products we make, under their predicament, that our constituency can make their piece of the internet, a safe and resilient one.

BruCERT

Brunei Computer Emergency Response Team

1. About BruCERT

1.1 Introduction

Cyber Security Brunei (CSB) is the national cybersecurity agency of Negara Brunei Darussalam, responsible for safeguarding the nation's cyberspace and coordinating national efforts to address cybersecurity threats and cybercrime. CSB operates under the Ministry of Transport and Infocommunications (MTIC), with the Minister of MTIC serving as the Minister-in-Charge of Cybersecurity.

CSB plays a key role in strengthening the country's cybersecurity posture by providing services and initiatives that support government agencies, private sector organisations, and the general public. These efforts focus on protecting Critical Information Infrastructure (CII), enhancing national cyber incident response capabilities, supporting cybercrime investigations through the National Digital Forensics Laboratory (NDFL), and promoting cybersecurity awareness across the nation.

BruCERT (Brunei Computer Emergency Response Team) was established in May 2004 as Brunei Darussalam's national incident response team. Originally formed in collaboration with the Authority for Info-communications Technology Industry of Brunei Darussalam (AITI) and the then Ministry of Communications, BruCERT serves as the country's trusted focal point for handling computer-related and internet-related security incidents. Today, BruCERT operates under Cyber Security Brunei and provides incident response coordination, cybersecurity advisory, and threat analysis services.

Supporting these operations is the Cyber Watch Centre (CWC), which functions as the national cybersecurity monitoring and situational awareness center. CWC conducts continuous monitoring of cyber threats affecting government systems and Critical Information Infrastructure (CII) through advanced security monitoring technologies, intelligent sensors, and threat intelligence capabilities. The center plays a crucial role in detecting potential cyber threats, analysing malicious activities, and providing early warning alerts to strengthen national cyber defence.

BruCERT actively collaborates with regional and international cybersecurity communities to enhance information sharing, technical cooperation, and coordinated incident response. The team is a member of several global cybersecurity organisations, including:

- Asia Pacific Computer Emergency Response Team (APCERT) – joined in 2005
- Organisation of Islamic Cooperation Computer Emergency Response Team (OIC-CERT) – joined in 2009
- Forum of Incident Response and Security Teams (FIRST) – joined in 2014

Through these collaborations, CSB, BruCERT, and the Cyber Watch Centre continue to strengthen Brunei Darussalam's national cyber resilience, incident response capabilities, and international cybersecurity cooperation.

1.1.1 BruCERT Services

- 24X7 Security Related Incidents and Emergency Response from BruCERT.
- 24X7 Security Related Incidents and Emergency Response onsite (Deployment response is within 2hrs after an incident is received). This service only applies to BruCERT Constituents.
- Broadcast alerts (Early Warning) of new vulnerabilities, advisories, viruses and Security Guidelines from BruCERT Website. BruCERT Constituents will receive alerts through email and telephone as well as defense strategies in tackling IT Security related issues.
- Promote Security Awareness program to educate and increase public awareness and understanding of information security and technical know-how through education, workshop, seminar, and training.
- Coordinating with other CERT, Network Service Providers, Security Vendors, Government Agencies as well as other related organizations to facilitate the detection, analysis, and prevention of security incidents on the internet.

1.2 BruCERT Establishment

BruCERT coordinates with local and international Computer Security Incident Response Team (CSIRTs), Network Service Providers, Security Vendors, Law Enforcement Agencies as well as other related organizations to facilitate the detection, analysis, and prevention of security incidents on the Internet.

1.3 BruCERT Workforce

BruCERT currently comprises a workforce of 66 personnel, all of whom are local professionals, reflecting the organisation's commitment to nurturing and strengthening national cybersecurity talent in Brunei Darussalam. The majority of the team consists of highly skilled information technology and cybersecurity specialists, supported by personnel responsible for administrative and technical operations.

To ensure operational excellence and readiness in addressing the evolving cyber threat landscape, BruCERT continuously invests in the professional development and technical capacity building of its workforce. Staff members have undergone

extensive training across a broad spectrum of information technology and cybersecurity disciplines, supported by internationally recognised professional certifications.

These include industry certifications such as CompTIA A+, Network+, Linux+, Server+, and Security+, as well as advanced cybersecurity certifications including SCNP, SCNA, CIW, CEH, CCNA, CISSP, and ISO/IEC 27001 Implementer.
In addition, BruCERT personnel have participated in specialized training programmes offered by the SANS Institute, including GREM (Reverse Engineering Malware), GCIA (Intrusion Analysis), GCIH (Incident Handling), GCFA (Forensic Analysis), and GPEN (Penetration Testing). Many members of the team have successfully obtained these certifications, further strengthening BruCERT's capabilities in incident response, malware analysis, digital forensics, threat intelligence, and cybersecurity operations.

Through continuous professional development and skills enhancement, BruCERT remains committed to building a highly capable and resilient cybersecurity workforce, enabling the organisation to effectively safeguard the digital ecosystem and support the national cybersecurity mission of Brunei Darussalam.

1.4 BruCERT Constituents

BruCERT has close relationships with Government agencies, 1 major ISPs and various numbers of vendors.

Government Ministries and Departments
BruCERT provide Security incident response, Managed Security Services via Cyber Watch Centre (CWC) and Consultancy services to the government agencies. Security Trainings such as forensic and awareness trainings were provided by BruCERT in collaboration with some Government Agencies.

E-Government National Centre (EGNC)
E-Government National Centre provides IT Services to all Government Departments and Ministries in Brunei Darussalam. Services such as IT Central procurement, Network Central Procurement, Co-location, ONEPASS (a PKI initiative), Co-hosting are provided by EGNC. BruCERT works closely with EGNC in providing Incident Response and Security Monitoring since most of the government equipment resided at EGNC.

AITI
Authority for Info-communications Technology Industry of Brunei Darussalam (AITI) is an independent statutory body to regulate, license and develop the local ICT industry and manage the national radio frequency spectrum.
AITI has appointed ITPSS (Information Technology Protective Security Services), an IT local security company to become the national CERT in dealing with incident response in Brunei.

Royal Brunei Police Force (RBPF) and other Law-Enforcement Agencies (LEAs)
BruCERT has been collaborating with RBPF and other LEAs to resolve computer-related incidents through our Digital

and Mobile Forensic services.

Unified National Network – UNN

UNN, the main Internet service provider. BruCERT have been working together to engage information sharing of internet-related statistics and the current situation of IT environment in Brunei.

Brunei Cyber Security Association – BCSA

Brunei Cyber Security Association (BCSA) aims to. Bring together professionals, experts, and enthusiasts in the field of cybersecurity to collaborate, share knowledge and collectively address the evolving challenges posed by cyber threats.

1.5 BruCERT Contact

The Brunei Computer Emergency Response Team Coordination Centre (BruCERT) welcome reports on computer security related incident. Any computer related security incident can be reported to us by:

- Telephone: (673) 2458001
- Facsimile: (673) 2456211
- Whatsapp: (673) 7170766
- Email: cert@brucert.org.bn
- Reporting: reporting@brucert.org.bn

2. BruCERT Operation in 2025

2.1 Incidents response

For the year 2025, Cyber Security Brunei (CSB), through BruCERT and the Cyber Watch Centre (CWC), identified multiple instances of suspicious and malicious activities through its secure monitoring infrastructure and intelligent sensors deployed across constituent systems.

Based on the collected monitoring data, Malware-related incidents accounted for the majority of detected cases, with a total of 1,955 incidents, making it the most prominent cybersecurity concern observed during the year. Malware infections typically indicate attempts by threat actors to compromise systems, establish persistence, or deploy malicious payloads within targeted networks.

Meanwhile, Denial of Service (DoS) incidents recorded only 2 cases, suggesting that large-scale service disruption attempts were relatively minimal compared to other forms of cyber threats observed during the year. The distribution of these detected activities is illustrated in Figure 1.

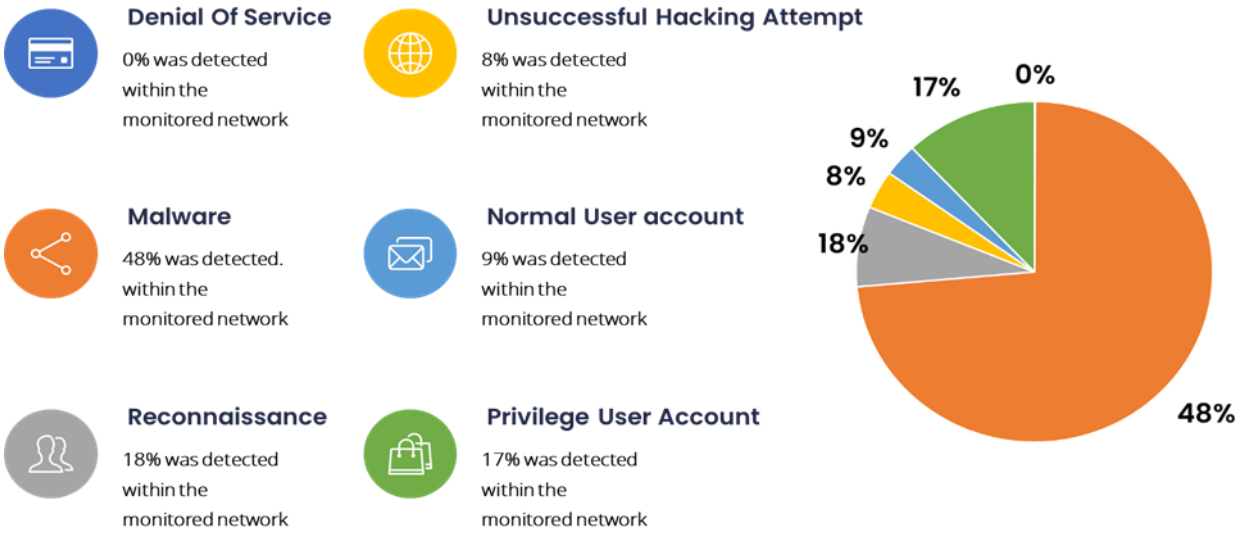


Figure 1

This was followed by Unsuccessful Hacking Attempts (320 cases), which reflect repeated attempts by attackers to gain unauthorized access to systems through methods such as credential brute-force attacks, exploitation of vulnerabilities, or unauthorized login attempts. In addition, Reconnaissance activities (202 cases) were also detected, indicating that attackers were actively probing and scanning systems to gather information about potential vulnerabilities and system configurations before launching further attacks.

The monitoring system also identified several security events related to user account activities, including Normal User Account incidents (97 cases) and Privilege User Account incidents (83 cases). These events highlight potential risks associated with user access management and may indicate suspicious login behavior, privilege misuse, or attempts to escalate system privileges.

Overall, the data highlights that malware infections and unauthorized access attempts remain the dominant cybersecurity threats, emphasizing the importance of continuous monitoring, strong access control policies, and proactive threat detection to safeguard critical systems and digital infrastructure in Brunei Darussalam.

Types of Attacks	Count
Denial of Services	1
Malicious Software	504
Reconnaissance	192
Unsuccessful Hacking Attempt	81
Normal User Account	95
Privilege User Account	182

Table 1

2.2 BruCERT Honey Pot

Cyber Security Brunei (CSB) through BruCERT has deployed honeypot systems, which are intentionally exposed decoy servers designed to attract and record malicious activities from cyber attackers. These systems allow BruCERT to observe attacker behaviours, identify commonly targeted services, and analyse emerging cyber threats.

Based on the analysis of logs collected from the honeypot in 2025, it was observed that port 445, commonly associated with Server Message Block (SMB) services, was the most abused port, recording approximately 2,868,603 attack attempts. This indicates a significant number of exploitation attempts targeting SMB-related vulnerabilities, which are commonly used for unauthorised remote access, lateral movement, or malware propagation within networks.

The second most targeted port was port 1433, which is associated with Microsoft SQL Server (MS-SQL) services, with 1,757,603 attempts detected. This suggests that attackers were actively attempting to exploit database services through brute-force login attempts or vulnerability exploitation.

This was followed by port 22 (Secure Shell – SSH) with 989,166 attempts, indicating persistent attempts by attackers to gain remote access to systems through credential brute-forcing or unauthorized login attempts. Other frequently targeted ports included port 23 (Telnet), port 135 (RPC), port 5060 (SIP), port 8728 (MikroTik RouterOS), port 443 (HTTPS), and port 1900 (UPnP), reflecting a broad range of automated scanning and exploitation activities targeting various network services.

Overall, the data demonstrates that attackers continue to focus on commonly exposed services such as SMB, database servers, and remote access protocols, highlighting the importance of proper network hardening, secure configuration, and continuous monitoring to mitigate potential exploitation attempts.
The distribution of the top 10 most abused ports observed by the BruCERT honeypot in 2025 is illustrated in Figure 2.

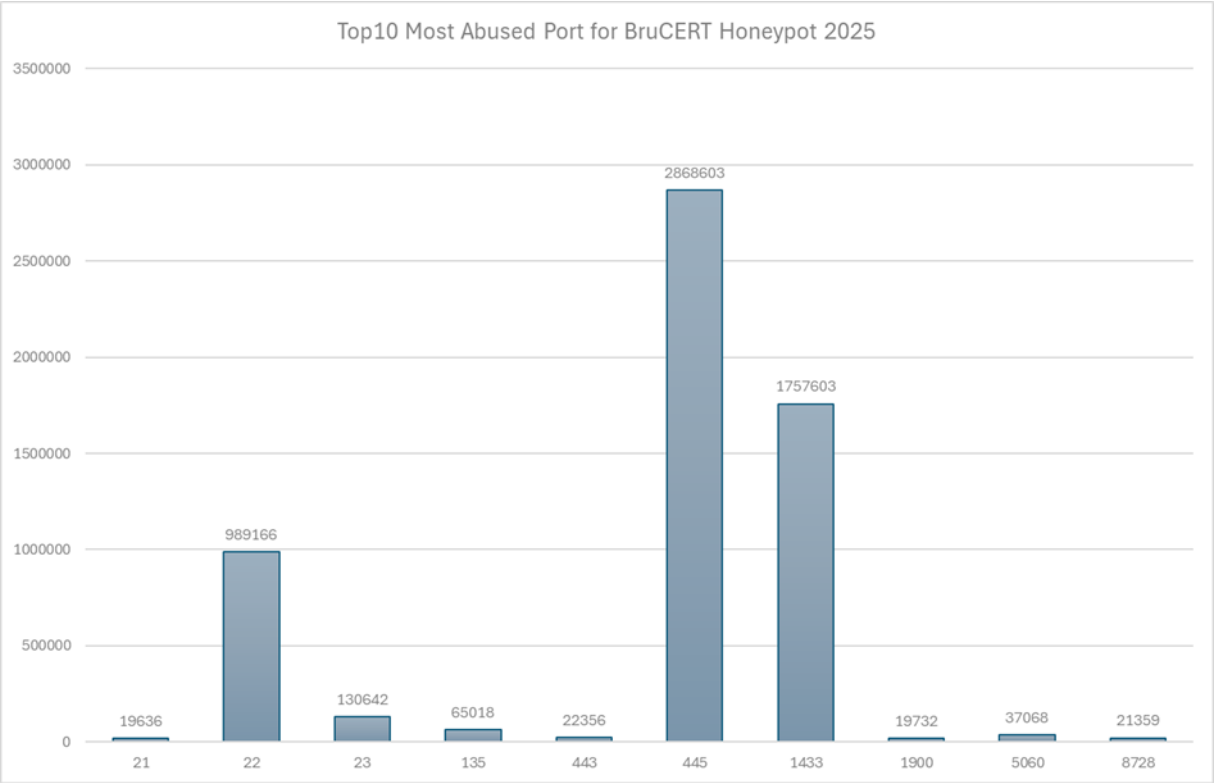


Figure 2

Port No	Count
21	19636
22	989166
23	130642
135	65018
443	22356
445	2868603
1433	1757603
1900	19732
5060	37068
8728	21359

Table 2

Similarly, port 22, which supports Secure Shell (SSH) remote access, recorded 989,166 attempts, highlighting continued efforts by attackers to gain unauthorized administrative access through brute-force login attempts or compromised

credentials. The notable activity on port 23 (Telnet), with 130,642 attempts, reflects ongoing exploitation of legacy remote access services that are often poorly secured or misconfigured.

Other ports also demonstrated consistent malicious activity. Port 135 (RPC) recorded 65,018 attempts, suggesting reconnaissance and exploitation targeting Windows remote procedure call services. Port 5060, commonly associated with Session Initiation Protocol (SIP) used in Voice over IP (VoIP) systems, recorded 37,068 attempts, which may indicate attempts to exploit telecommunication infrastructure.

In addition, port 8728, used by MikroTik RouterOS management services, recorded 21,359 attempts, indicating automated scanning targeting network infrastructure devices. Smaller but notable activity was also observed on port 1900 (UPnP) with 19,732 attempts, which could potentially be leveraged for reflection-based DDoS attacks, and port 21 (FTP) with 19,636 attempts, suggesting continued attempts to exploit unsecured file transfer services. Meanwhile, port 443 (HTTPS) recorded 22,356 attempts, which may reflect scanning activities targeting web services and encrypted communication channels.

Overall, the findings highlight that attackers continue to focus on widely deployed and commonly exposed services such as SMB, SSH, and database servers, while also probing legacy services and network infrastructure devices for potential weaknesses. These observations emphasize the importance of secure configuration, regular patching, network segmentation, and continuous monitoring to reduce the risk of exploitation and strengthen the cybersecurity posture of organisations in Brunei Darussalam.

Based on observations from the BruCERT honeypot deployment, several variants of malware were detected attempting to compromise exposed systems. Analysis of the captured samples indicates that Generic Trojan malware constituted the largest proportion of detected threats, accounting for approximately 53% of the total captured malware. This suggests that attackers frequently deploy Trojan-based payloads to gain unauthorized access, establish persistence, or deliver additional malicious components into targeted systems.

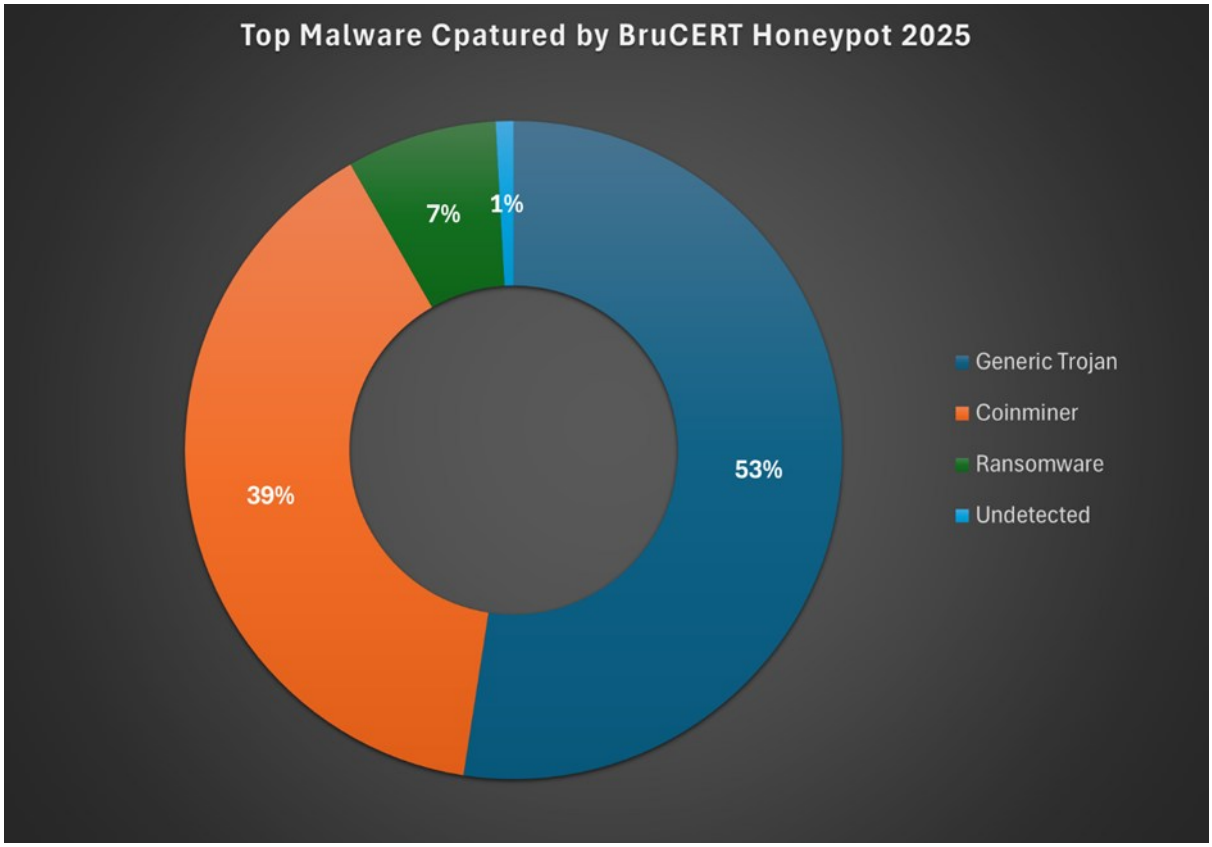


Figure 3

The second most prevalent threat observed was Coinminer malware, representing 39% of the captured samples. Coinminer infections typically aim to exploit compromised systems by utilizing their computational resources for unauthorized cryptocurrency mining, which can significantly degrade system performance and operational stability.

Malware Type	Total
COINMINER	2767
GENERIC TROJAN	3693
RANSOMWARE	520
UNKNOWN	62
Grand Total	7042

Table 3

In addition, Ransomware accounted for around 7% of the detected malware, indicating continued attempts by threat actors to deploy ransomware payloads that could potentially encrypt organizational data and disrupt critical services. A small proportion, approximately 1%, remained undetected or unidentified, reflecting malware samples that could not be immediately classified during the analysis process.

The distribution of malware captured by the honeypot is illustrated in Figure 3, which highlights the dominance of Trojan and cryptocurrency-mining malware in the observed threat landscape. These findings demonstrate the importance of maintaining continuous monitoring mechanisms, such as honeypots, to detect emerging threats and enhance situational awareness of cyberattack patterns targeting networks in Brunei Darussalam.

In 2025, BruCERT recorded a total of 609 reported cybersecurity incidents submitted by the public, government agencies, and private sector organisations in Brunei Darussalam. Analysis of these reports indicates that Phishing incidents constituted the highest number of cases, with 111 reports, followed by Scam-related incidents (91 cases) and Cyberbullying (89 cases).

Other notable incident categories included general cyber-related cases classified as Others (80 cases) and Account Takeover incidents (65 cases), where attackers gained unauthorized access to online accounts. In addition, Impersonation (44 cases), Smishing (37 cases), and Phishing-related variants (35 cases) were also reported, highlighting the continued use of social engineering techniques by cybercriminals.

A smaller number of incidents were recorded under Unethical Communication (18 cases), Sextortion (16 cases), Blackmail or Extortion (16 cases), and Compromised Devices (6 cases). These cases reflect emerging threats that target individuals through harassment, coercion, or unauthorized device access.

Overall, the data demonstrates that social engineering and online fraud remain the dominant cybersecurity threats affecting users in Brunei Darussalam, with phishing and scam-related activities continuing to be the primary methods used by threat actors to exploit victims.

The distribution of reported incidents is illustrated in Figure 4.

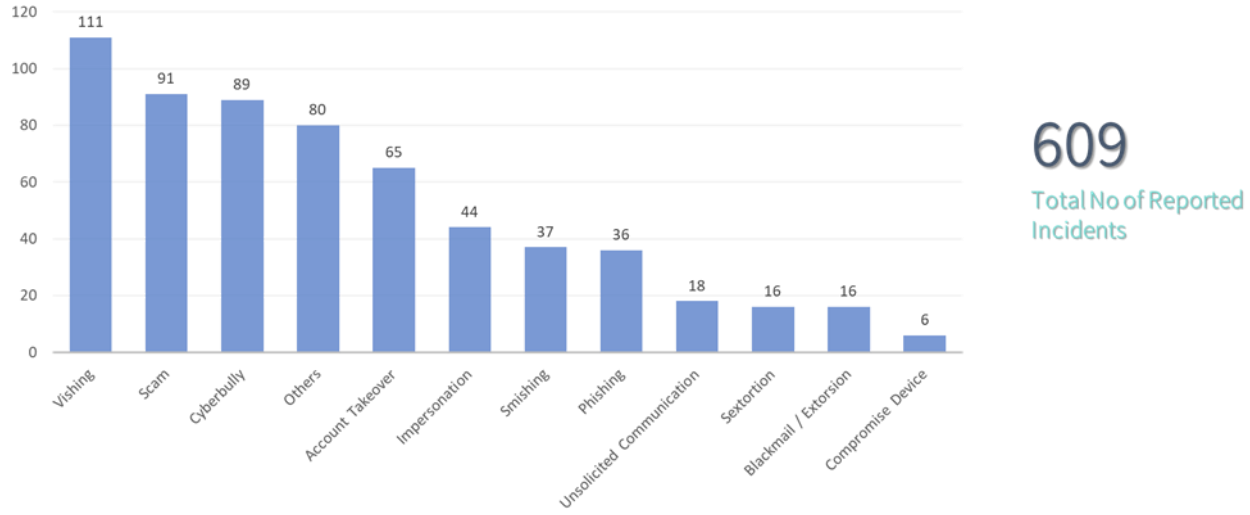


Figure 4

3. BruCERT Activities in 2025

3.1 Seminars/Conferences/Meetings/Visits

In 2025, BruCERT continued to actively participate in various international cybersecurity meetings, conferences, and capacity-building programmes to strengthen collaboration with global Computer Emergency Response Teams (CERTs) and cybersecurity communities. These engagements provided valuable opportunities for information sharing, incident coordination, and discussions on emerging cybersecurity threats and best practices. Several meetings were conducted both physically and through virtual platforms.

- From 25th November 2025 until 27th November 2025 – BruCERT delegates attended the 23rd Annual General Meeting (AGM) and Annual Conference of the Asia Pacific Computer Emergency Response Team (APCERT) hosted by the Australian Cyber Security Centre in Sydney, Australia. The meeting gathered APCERT member teams from across the Asia-Pacific region to discuss regional threat trends, incident response coordination, and strategies to strengthen cybersecurity cooperation among member economies.
- From 15th September 2025 until 16th September 2025 – BruCERT delegates attended the 17th Annual Conference of the Organisation of Islamic Cooperation Computer Emergency Response Team (OIC-CERT). The conference brought together cybersecurity professionals and CERT representatives from OIC member states to discuss regional cyber threats, policy coordination, and collaborative initiatives aimed at enhancing cybersecurity resilience across member countries.
- From April 2025 – BruCERT participated in the APCERT Cyber Drill 2025, a regional cybersecurity exercise organised by APCERT to strengthen incident response capabilities among member teams. The exercise simulated various cyberattack scenarios and allowed participating CERTs to practice information sharing, incident analysis, and coordinated response mechanisms.
- In 2025 – BruCERT participated in the ITU Regional Cyber Drill hosted in Mongolia, organised by the International Telecommunication Union (ITU). Notably, BruCERT contributed its expertise in developing cyber incident scenarios for the exercise, supporting the design of realistic attack simulations used during the drill. The exercise included scenarios such as phishing campaigns, malware infections, and distributed denial-of-service (DDoS) attacks, enabling participating teams to practice coordinated incident response, technical investigation, and cross-border threat intelligence sharing among international CERT communities.

3.2 Awareness Activities

Throughout 2025, Cyber Security Brunei (CSB), through BruCERT, continued to strengthen national cybersecurity awareness through a series of public outreach and education initiatives targeting government agencies, organisations, and the public.

A total of 132 awareness sessions were conducted during the year, reaching 15,337 participants across schools, government institutions, and community groups. These programmes were delivered by seven certified trainers, focusing on key topics such as cyber hygiene, online safety, scam awareness, and emerging cyber threats.

BruCERT's digital awareness platform, www.secureverifyconnect.info, served as a central resource hub for cybersecurity information and recorded an average of 773 visits per month. In addition, BruCERT expanded its outreach through media and digital engagement, including participation in the "Rampai Pagi" radio segment and the production of 111 awareness episodes, with an average of six educational videos played monthly.

Complementing these efforts, 12 structured awareness sessions and targeted engagement programmes were conducted, while 146 users successfully completed the online awareness modules, demonstrating growing public participation in cybersecurity education.

Figure 5

These initiatives reflect BruCERT's continued commitment to enhancing cybersecurity awareness and fostering a safer digital environment across Brunei Darussalam.

In 2025, BruCERT conducted a total of 132 cybersecurity awareness sessions across various sectors in Brunei Darussalam. Most of these sessions were delivered to schools (77 sessions), reflecting a strong focus on educating students and youth on safe digital practices. This was followed by government agencies (38 sessions), community groups (17 sessions), and corporate organisations (7 sessions). These initiatives demonstrate BruCERT's continued efforts to promote cybersecurity awareness and strengthen cyber resilience across multiple segments of society.


Students
11,803
Audience
15,337
Workers
2,217
Public/ Community
1,317
Schools
77
Awareness Session
132
Organizations
38
Community
17
Cyber Security Awareness Trainer
7

Figure 6

BtCIRT

Bhutan Computer Incident Response Team

1. Highlights of 2025

1.1 Summary of Major Activities

- October 2025 saw the successful conclusion of the 5th Cybersecurity Month, an initiative dedicated to building awareness and technical expertise. The month featured a high-impact full-day conference, technical sessions on forensics and network analysis, and practical cyber hygiene programs.
- In collaboration with leading technical colleges, a National Capture the Flag (CTF) challenge was hosted to sharpen national cybersecurity talent. The competition drew a diverse field of participants, including students from three technical colleges alongside seasoned professionals from both the public and private sectors.
- A 2-day Cybersecurity Capacity Building was organized specifically for high-level executives from critical sectors. The primary objective of the session was to strengthen cybersecurity awareness and leadership engagement at the executive level.

2. About BtCIRT

2.1 Introduction

The Bhutan Computer Incident Response Team (BtCIRT) is part of the GovTech Agency. The overall mission of BtCIRT is to enhance cyber security in the country by implementing relevant cybersecurity plans and programs, including coordinating cybersecurity information and establishing computer security incident handling capabilities in the country. It is also mandated to proactively monitor government systems for cyber threats.

2.2 Establishment

BtCIRT was formally established on 20th May 2016 as the national focal point for coordinating and implementing

cybersecurity activities and initiatives for Bhutan.

2.3 Resources

BtCIRT operates with fifteen working team members as of December 2025.

2.4 Constituency

BtCIRT constituents are all government institutions under the Royal Government of Bhutan (RGOB) utilizing government network infrastructure to host their IT resources and services. The services like awareness and reactive services are extended to all users within the country.

3. Activities & Operations

3.1 Scope and definitions

As the apex body for cybersecurity in the country, BtCIRT is responsible for identifying and carrying out relevant cybersecurity plans and programs that contribute towards achieving the vision of safe and secure Bhutan.

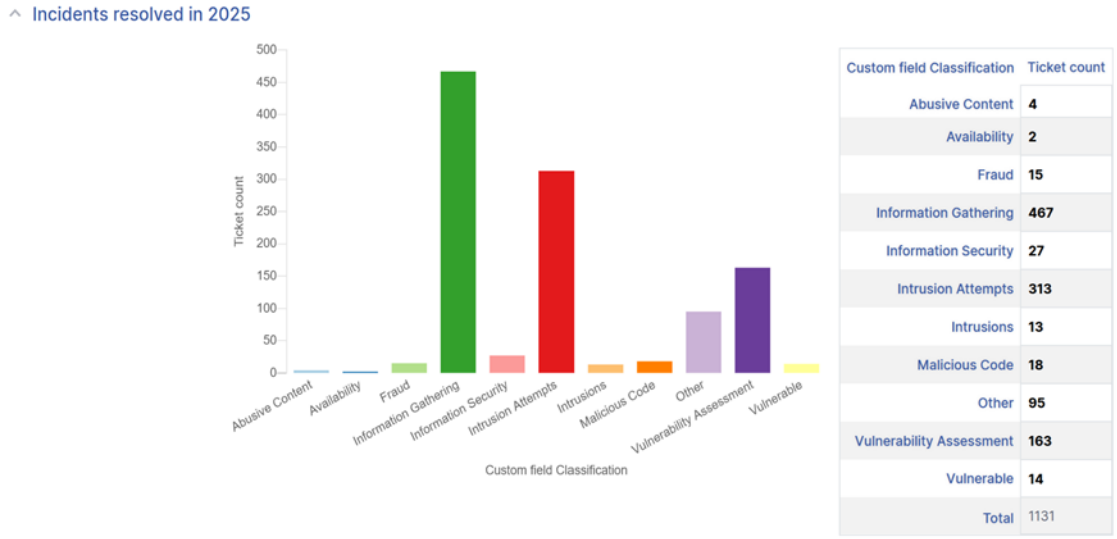
The specific mandates of BtCIRT are as follows:

- Operate as a national contact in relation to coordinating and implementing all cyber security issues, plans and programs.
- Conduct end-user awareness at national level and disseminate information on threats and vulnerabilities, and conduct security workshops related to various cyber security domains.
- Actively monitor systems hosted in the Government Data Centre (GDC) for attacks and vulnerabilities and provide timely reports to the GDC operating team and the system administrators.
- Conduct periodic security assessment of government systems and provide services to non-government organizations on request.
- Represent Bhutan in international forums.
- Develop relevant strategies, policies, standards, guidelines and baseline documents.

3.2 Incident Handling Report

The incident trends in figure 1 show that Information Gathering (467) is the most frequently recorded category followed by Intrusion Attempts (313). The Vulnerability Assessment (163) figures highlight a strong focus on proactively

identifying and addressing security weaknesses. The least recorded is Availability (2) related. Other categories of incidents handled are as depicted in the following graph:



Custom field Classification	Ticket count
Abusive Content	4
Availability	2
Fraud	15
Information Gathering	467
Information Security	27
Intrusion Attempts	313
Intrusions	13
Malicious Code	18
Other	95
Vulnerability Assessment	163
Vulnerable	14
Total	1131

Figure 1: Incident handled by Incident Classification type in 2025

4. Events organized / hosted

4.1 Workshops/ Training

Capacity development is another important mandate of BtCIRT to ensure that all the stakeholders in the cybersecurity ecosystem are prepared to meet the challenge of the ever-changing cybersecurity threat landscape. In that note, several capacity development activities have been carried out to strengthen the capabilities of all stakeholders. The key workshops are highlighted as follows:

4.1.1 Cybersecurity Capacity Building by ITU-JICA

The International Telecommunication Union (ITU) and the Japan International Cooperation Agency (JICA) Bhutan Office, the ITU-in collaboration with the Government Technology (GovTech) Agency and the Royal Government of Bhutan—conducted Cybersecurity Capacity Building training from May 20-21, 2025, in Thimphu, Bhutan. The training included participants from 21 government and regulatory agencies. A cyber crisis simulation and scenario focused on Critical Information Infrastructure was also conducted as a part of the training.

Figure 2: Group photo of the Participants

4.1.2 Cyber Threat Management and monitoring Workshop

A four-day Cyber Threat Management and Monitoring workshop was conducted with over 50 participants from government agencies, financial institutions, telecom providers, regulatory bodies, the Royal Bhutan Army, and academic institutions. The training focused on cyber threat identification, vulnerability assessment, risk management, and global cybersecurity frameworks and best practices, along with hands-on training using open-source security tools for threat detection, monitoring, and incident response.

Figure 3: Participants of the workshop

4.1.3 Technical workshop on digital forensics and network analysis

In collaboration with the National Cybersecurity Agency of the Czech Republic (NUKIB) and National Counterterrorism, Extremism, and Cybercrime Agency (NCTEKK), a three-day workshop on "Digital forensics and Network analysis" was conducted from 14 - 16 October 2025 with participation from 35 officials from different agencies.

Figure 4: Participants at the workshop

4.1.4 Cyber conference

The Bhutan Cybersecurity Conference 2025, held as a hybrid event on 24th October in Thimphu, brought together local and international cybersecurity experts to promote awareness, share insights, and foster partnerships in Bhutan. Featuring 13 speakers, including 5 international experts, the conference attracted over 60 participants from both public and private sectors, facilitating knowledge exchange, networking, and further strengthening Bhutan's cybersecurity community.

Figure 5: Participants at the Cybersecurity Conference

4.2 Drills/Exercises

The following drills were conducted:

4.2.1 Cybersecurity Capture The Flag Challenge (24-25 October)

The Cybersecurity Capture The Flag (CTF) challenge was held from 24–25 October 2025 in collaboration with at Gyalpozhing College of Information Technology (GCIT) and Jigme Namgyel Engineering College (JNEC). The event engaged participants from three technical colleges: College of Science and Technology (CST), JNEC, and GCIT, as well as professionals from government and private sectors. A one-day workshop covering essential cybersecurity concepts, practical tools, exploitation demonstrations, and a CTF orientation was followed by a CTF competition.

Figure 6: Teams competing at the Capture the Flag challenge

5. International Collaboration

5.1 International partnerships and agreements

BtCIRT has been a member of FIRST and APCERT since 2017 and with CAMP and GFCE since 2023.

5.2 Capacity building

BtCIRT members participated in various skill development programs, including training sessions, workshops, and conferences. These engagements have served as a foundation for enhancing the knowledge and expertise of our team while facilitating networking with national and international cybersecurity and CIRT communities. BtCIRT extends its gratitude to the organizers and sponsors for providing these valuable capacity-building opportunities.

5.2.1 Trainings

BtCIRT members participated in the following trainings, meetings and seminars:

- APT Training Course on Cyber Security Technologies by KDDI Foundation from 15-24 January 2025 in Japan
- CAMP Annual Meeting by Korea Internet & Security Agency (KISA) from 3-5 July 2025 in South Korea

- APISC Training by KrCERT/CC Korea Internet Security Agency (KISA) in 23 August to 1 September 2025 in South Korea
- Integrated Cybersecurity for safer digital world by Singapore Cooperation Programme (SCP) from 13-17 October in Singapore

5.2.2 Drills and Exercises

- BtCIRT Participated in APCERT Cyber Drill in July 2025
- BtCIRT Participated in ITU Regional Asia-Pacific CyberDrill from 2-5 September 2025 in Mongolia

5.2.3 Contribution to Seminars, Conference & Presentations

- BtCIRT participated in the South Asian Network Operator Groups (SANOG) Conference on August 22-23 August 2025, delivering a presentation titled **"Updates on BtCIRT."** an annual event organized by volunteers comprising network, system, and ICT professionals, serves as a platform for knowledge sharing and collaboration.

6. Future Plans

BtCIRT is committed to enhancing its incident handling capabilities and further working on areas to improve the overall cybersecurity maturity of Bhutan. BtCIRT's future goals include:

Strengthening National Resilience: Continuous collaboration with critical sectors to protect Critical Information Infrastructure (CII) through national risk assessments, the development of regulations and standards, and the enhancement of institutional and technical capabilities.

Enhancing Incident Response and Monitoring Services: Building team capacity to proactively monitor security events by enhancing our Security Operations Center (SOC) and incident response capabilities. This includes the proactive assessment of applications, systems, and networks.

Strengthening National and International Collaborations: BtCIRT remains committed to improving national collaboration to ensure an efficient and effective coordinated response to incidents. Furthermore, we will continue to explore new partnerships with security organizations both within the region and beyond.

These goals are key components of the National Cybersecurity Strategy's action plans and programs.

7. Conclusion

In 2025, in addition to handling cybersecurity incidents, BtCIRT delivered a range of cybersecurity programs including capacity development and awareness initiatives for diverse target groups. Looking ahead, key priorities for the year will be strengthening national cybersecurity resilience, enhancing incident response and monitoring services, and strengthening national and international collaboration.

CERT-In

Indian Computer Emergency Response Team

1. Highlights of 2025

1.1 Summary of major activities

- In the year 2025, Indian Computer Emergency Response Team (CERT-In) handled **29,44,248** incidents. The type of incidents handled were Website Intrusion & Malware Propagation, Malicious Code, Phishing, Distributed Denial of Service attacks, Website Defacements, Unauthorized Network Scanning/Probing activities, Ransomware attacks, Data Breach and Vulnerable Services. Remedial measures for handling incidents were suggested and implemented in coordination with relevant stakeholders.
- CERT-In tracks latest cyber threats and vulnerabilities. A total of **1530** security alerts, **65** advisories and **390** Vulnerability Notes were issued during the year 2025.
- CERT-In conducted **32** cyber security training and awareness programs for Government, Public, Private sector organisations across all sectors to provide insights on latest cyber-attack trends, threat landscape and countermeasures, incident response and remediation, network and infrastructure security, application security, Internet of Things (IoT) security, Governance, Risk and Compliance and various latest topics in the area of Cyber Security.
- CERT-In conducted **18** domestic cyber crisis exercises in 2025 for various organizations across Sectors and State Government Departments.
- CERT-In has conducted 05 international exercise, contributed to planning & scenario development in 1 exercise and participated as a player in 4 International cyber security drills in 2025.

1.2 Achievements & milestones

- CERT-In's initiative to strengthen cybersecurity resilience in Indian cooperative banks has been featured in the Global Cybersecurity Outlook 2025 report by the World Economic Forum (WEF). The report featured a case study lauding the Indian Computer Emergency Response Team (CERT-In) for its groundbreaking initiative to enhance cybersecurity resilience.

- World Economic Forum's Global Communications Group released a video on Cyber Swachhta Kendra (CSK) of CERT-In on January 18, 2025, before the Annual Meeting in Davos which was held on January 20, 2025. CSK is a free service from CERT-In for citizens to clean their digital devices from bots and malware as well as help organisations identify understand their vulnerable systems.
- In April 2025, CERT-In was able to contribute to the "Cyber Resilience Compass" paper published by the World Economic Forum and the University of Oxford. The report outlines 7 critical domains for strengthening resilience drawn from the front-line practices of leading organizations globally.
- The Indian Computer Emergency Response Team (CERT-In) is one of the international partners to co-sign the joint high-level risk analysis report on Artificial Intelligence (AI) entitled "Building trust in AI through a cyber-risk-based approach," published by the National Cybersecurity Agency for France (ANSSI) in February 2025. The report advocates for a risk-based approach to support trusted AI systems and secure AI value chains and calls for discussions on AI-related cyber risks and how to mitigate them to foster trusted AI development.
- A white paper published by the World Economic Forum and the Institute for Security and Technology in December 2025 highlighted that during the course of 2024, CERT-In leveraged AI and situational awareness systems to analyse over 9,800 billion DNS queries, identifying 128 million phishing domains from 2.2 billion malicious queries in addition to sharing DNS-based threat intelligence with global partners to strengthen international cooperation and secure the digital ecosystem.

2. About CERT-In

2.1 Introduction

i. CERT-In under Ministry of Electronics and Information Technology (MeitY), Government of India is established with the objective of securing Indian cyber space. CERT-In provides Incident Prevention and Response services as well as Security Quality Management Services.

ii. Under Section 70B of the Information Technology Act, 2000, CERT-In has been designated to serve as national agency for incident response and for performing various other functions in the area of cyber security. CERT-In operates 24x7 incident response Help Desk for providing timely response to reported cyber security incidents. CERT-In provides incident prevention and response services as well as security quality management services.

CERT-In performs the following functions in the area of cyber security:

- Collection, analysis and dissemination of information on cyber incidents
- Forecast and alerts of cyber security incidents
- Emergency measures for handling cyber security incidents
- Coordination of cyber incident response activities
- Issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents

- Such other functions relating to cyber security as may be prescribed.

iii. CERT-In creates awareness on cyber security issues through dissemination of information on its websites (https://www.cert-in.org.in and https://www.csk.gov.in).

2.2 Establishment

CERT-In has been operational since January, 2004.

2.3 Constituency

The constituency of CERT-In is the Indian cyber community and Indian cyberspace. CERT-In provides services to the government, public and private sector organizations across all sectors. In addition, CERT-In provides services to the individuals and home users also.

3. Activities & Operations

3.1 Scope and definitions

CERT-In provides:

- Proactive services such as advisories, security alerts, vulnerability notes, sharing of technical information such as Indicators of Compromises (IoCs), situational awareness of existing & potential cyber security threats and security guidelines for helping organizations to secure their systems and networks.
- Reactive services when security incidents occur so as to minimize damage.
- Security quality management services in the form of cyber security audits, promotion of best practices and cyber security exercises/drills.

3.2 Incident handling reports

The summary of activities carried out by CERT-In during the year 2025 is given in the following table:

Activities	Incidents in 2025
Security Incidents handled	2944248
Vulnerability Notes Published	390
Advisories Published	65

Security Alerts issued	1530
Security Drills	23
Trainings Organized	32

Table 1: CERT-In Activities during year 2025

3.3 Abuse statistics

In the year 2025, CERT-In handled 29,44,248 incidents. The types of incidents handled were website intrusion & malware propagation, malicious code, phishing, distributed denial of service attacks, website defacements, unauthorized network scanning/probing activities, ransomware attacks, data breaches/leaks and vulnerable services.
The summary of various types of incidents handled is given below:

Security Incidents	2025
Phishing	806
Unauthorized Network Scanning/Probing	24,36,320
Vulnerable Services	3,41,646
Virus/ Malicious Code	1,48,223
Website Defacements	8,386
Website Intrusion & Malware Propagation	1,118
Others	7,749
Total	29,44,248

Table 2: Breakup of Security Incidents handled

3.4 Botnet Cleaning Initiatives

- Botnet Cleaning and Malware Analysis Centre (Cyber Swachhta Kendra – CSK) has been established by CERT-In for detection of compromised devices in India and to notify, enable cleaning and securing systems of end users to prevent further malware infections. The Centre is working in close coordination and collaboration with Internet Service Providers (ISPs), Antivirus companies, Academia and Industry.
- Currently, CSK is covering ~98% of the subscriber base for notifications about botnet/malware infection. CSK also provides services for organizations from various sectors including Communications (Internet Service Providers), Finance, Healthcare, Transport, IT & ITeS, Government, Academia, 'Industries & Manufacturing', Energy and Smart Cities are collaborating and being benefited by using CSK services.

- CSK celebrated awareness campaign 'Cyber Swacchhta Pakhwada' from 1-15 February 2025 and 'National Cyber Security Awareness Month' in October 2025, in coordination with Internet Service Providers (ISP) and Antivirus Companies for spreading awareness and information regarding cyber security threats, challenges and safeguarding citizens against them.
- CSK provides three Free Bot Removal Tools (FBRTs) developed in collaboration with "QuickHeal", "K7" and "eScan" with a cumulative of 89.55 lakh downloads recorded till December 2025. These FBRTs are available for Microsoft Windows and Google Android platforms. CSK also provide Mobile Security Application for Android platform to users via web portal.

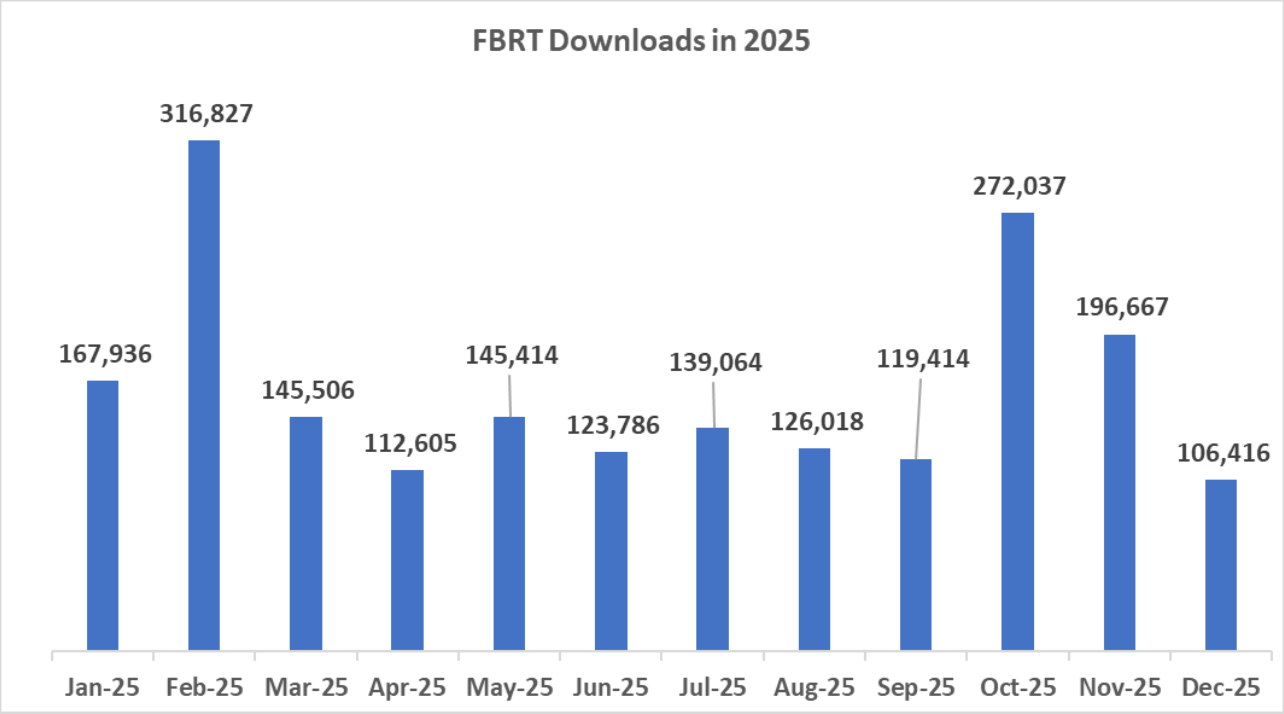


Figure 3: CSK Free botnet removal tools download statistics 2025

3.5 Security Profiling, Assurance framework and Audit Services

- Under Security Assurance Framework, Indian Computer Emergency Response Team (CERT-In) has created a panel of 'IT security auditing organizations' for carrying out information security auditing, including vulnerability assessment and penetration testing of computer systems, networks & applications of various organizations of the Government, critical infrastructure organizations and those in other sectors of Indian economy.
- CERT-In has empanelled **237** Information Security Auditing organizations, on the basis of stringent qualifying criteria, to carry out information security audit, including the vulnerability assessment and penetration testing of the networked infrastructure of government and critical sector organizations. This list of CERT-In empanelled information security auditing organizations is being consulted frequently by the entities in Government and critical sectors for their information security auditing requirements.
- CERT-In has implemented data science platform for conducting periodic data analysis on audit findings from across

country. The project enabled identification of areas for policy interventions. CERT-In has published Guidelines for Secure Application Design, Development, Implementation & Operations.

- Government and critical sector organizations are implementing the security best practices in accordance with ISO 27001 standard and as per the advice issued by CERT-In. Implementation enabling workshops/interactions are conducted periodically. Services of CERT-In empanelled technical IT security auditors are being used for technical as well as compliance audits. CERT-In has also carried out episodic security audits of key organizations for enhancing their security posture.

3.6 Cyber Threat Intelligence Sharing

- A core part of CERT-In's mission as the first responder with respect to Incident Response and Security Teams is to provide a trusted community platform for sharing cyber threat intelligence and situational awareness. CERT-In releases Indicators of Compromises (IoC's) covering operational, tactical and strategic, alerts, advisories & vulnerability notes to update the Government and critical sector organizations about the existing and potential threats and suitable necessary actions to counter those threats.
- CERT-In has operationalised its own Threat Intelligence eXchange platform based on STIX and TAXII standards. This automated platform facilitates bidirectional sharing of operational, strategic, enriched tactical threat intelligence to various counterparts and stakeholders in near real time in automatic fashion, thus helping to build a cyber-resilient ecosystem in the Indian cyber space.
- The platform collects, correlates, enriches, contextualizes, analyses, integrates and pushes to the partners in near real time with Traffic Light Protocol (TLP) tags. The shared data can be consumed by the recipients into their automated workflows. This will help to streamline their threat detection, management, analysis and defensive process.
- During the year 2025, CERT-In via its email mechanism and with its automatic threat Intel sharing platform- shared threat intelligence alerts with the constituency. Chief Information Security Officers (CISOs) of various organizations are getting benefitted by the curated operational and tactical threat intelligence digest shared through an automated platform as well as email covering latest cyber threats targeting Indian Cyber space and enabling proactive mitigation actions.

3.7 National Cyber Coordination Centre (NCCC)

Continuously evolving cyber threat landscape and its impact on well-being of information technology, national economy, and cyber security necessitates the need for near-real time situational awareness and rapid response to cyber security incidents. Government has set up the National Cyber Coordination Centre (NCCC) to generate macroscopic views of the cyber security threats in the country. The centre scans the cyberspace in the country at meta-data level and generates near real time situational awareness. The centre is facilitating various organizations and entities in the country to mitigate cyber-attacks and cyber incidents on a near real time basis.

3.8 Cyber Forensics

Cyber Forensics Lab (CFL) of CERT-In is equipped with the equipment and tools to carry out data retrieval, processing and analysis of the raw data extracted from the digital data storage and mobile devices using sound digital forensic techniques. The primary task of the Lab is to assist the Incident Response (IR) team of CERT-In on occurrence of a cyber-incident and extend digital forensic support to carry out further investigation. In addition, cyber forensics lab is being utilized in investigation of the cases of cyber security incidents and cyber-crimes, submitted by central and state government ministries / departments, public sector organisations, law enforcement agencies, etc. The Cyber Forensics Lab of CERT-In has been notified as Examiner of Electronic Evidence in exercise of the powers conferred by section 79A of the information Technology Act, 2000.

3.9 CVE Numbering Authority (CNA)

CVE is an international, community-based effort and relies on the community to discover vulnerabilities. The vulnerabilities are discovered then assigned and published to the CVE List. Information technology and cybersecurity professionals use CVE Records to ensure they are discussing the same issue, and to coordinate their efforts to prioritize and address the vulnerabilities. The vulnerabilities are discovered then assigned and published by organizations from around the world that have partnered with the CVE Program. Partners publish CVE Records to communicate consistent descriptions of vulnerabilities.

CNAs are organizations responsible for the regular assignment of CVE IDs to vulnerabilities, and for creating and publishing information about the Vulnerability in the associated CVE Record. The CVE List is built by CVE Numbering Authorities (CNAs). Every CVE Record added to the list is assigned by a CNA. The CVE Records published in the catalog enable program stakeholders to rapidly discover and correlate vulnerability information used to protect systems against attacks.

CERT-In has been undertaking responsible vulnerability disclosure and coordination for vulnerabilities reported to CERT-In since its inception. To move a step further in the direction to strengthen trust in "Make in India" as well as to nurture responsible vulnerability research in the country, CERT-In has now partnered with the CVE Program, MITRE Corporation, USA. In this regard, Indian Computer Emergency Response Team (CERT-In) has been authorized by the CVE Program, as a CVE Numbering Authority (CNA) for vulnerabilities impacting all products designed, developed and manufactured in India.

3.10 Publications

CERT-In published the following key guidelines and whitepapers in 2025.

i. Cyber Security Guidelines for Smart City Infrastructure

ii. Technical Guidelines on Software Bill of Material, Quantum Bill of Material, Cryptography Bill of Material, AI Bill Of Material & Hardware Bill of Material.
iii. 15 Elemental Cyber Defense Controls for Micro, Small, and Medium Enterprises (MSMEs).
iv. Comprehensive Cyber Security Audit Policy Guidelines.
v. Digital Threat report for BFSI Sector
vi. India Ransomware Report 2024
vii. Whitepaper on "Transitioning to Quantum Cyber Readiness"
viii. Whitepaper on "Good Practices for protecting Unmanned Aircraft Systems (UAS) against Cyber Security Threats"
ix. Advisory on "Cybersecurity Threats and Best Practices for Satellite Communications"
x. Advisory on "Essential Measures for Industry for Safeguarding Business Operations against Cyber Security Threats".
xi. Advisory on "Essential Measures for MSMEs for Safeguarding Business Operations against Cyber Security Threats"
xii. Advisory on "Best Practices against vulnerabilities while using Generative AI solutions"

CERT-In published several cyber security awareness booklets in 2025.

i. "Cyber Smart Kids: Suraksha Guide" for children to protect from cyber threats.
ii. "Cyber Security Best Practices for Senior Citizens" to educate senior citizens on cyber security best practices for a safe online experience.
iii. "Cyber Security Handbook for Mahila Suraksha" on the occasion of International Women's Day 2025.
iv. "Digital Safety compass Handbook" on the occasion of Safer Internet Day on 11 February 2025.
v. CERT-In created its own awareness content in various forms such as one liner quick safety tips, detailed posters with best practices, infographics in 9 Indian languages, visual meme posters, AI videos, awareness booklets for dissemination on official websites and social media handles. A total of 351 such posters/videos have been made and published for spreading awareness among digital nagriks and enterprises during NCSAM October 2025

Research Publications

i. "A robust and implementable approach for AI vulnerability risk scoring", in International Journal of Cybernetics and Cyber-Physical Systems.
ii. "Cyber Security and High-Performance Computing—the Intertwined Future" in 40th Indian Engineering Congress, 19-21 December 2025, Durgapur.
iii. "Bridging Intelligence and Security: Cyber Defense Strategies for Human– Computer Interfaces" in 40th Indian Engineering Congress, 19-21 December 2025, Durgapur.

4. Events organized / hosted

4.1 Training

- CERT-In regularly conducts cyber security training/workshop programs for development of cyber security capacities, skill building within Government, Public and Private Sector organizations across all sectors on various contemporary and focused topics of Cyber Security. In 2025, CERT-In has conducted **32** such training/workshop programs on various specialized topics of cyber security. A total of **20,799** participants have been trained covering system/network administrators, database administrators, application developers, IT managers, Chief Information Security Officers (CISOs)/ Chief information officers (CIOs), and IT/Security professionals.
- CERT-In regularly carry out various activities for creation of cyber security awareness within organisations as well as for upgrading the technical knowhow of various stakeholders, and citizen sensitization campaigns with respect to cyber-attacks and incidents. CERT-In observed the National Cyber Security Awareness Month (NCSAM) during October 2025 by organizing various events and activities for citizens as well as the technical cyber community in India with a theme of " Cyber Jagrit Bharat". The total outreach of National Cyber Security Awareness Month (NCSAM) October 2025 is 35,85,81,238. CERT-In also observes "Safer Internet Day" on 2nd Tuesday of February Month every year, Swachhta Pakhwada from 1 to 15 February of every year and Cyber Jagrookta Diwas (CJD) on 1st Wednesday of every month for sensitizing internet users on cyber-attacks & incidents and safety measures. In 2025, CERT-In conducted 78 such awareness sessions for different sectors including programs in collaboration with partners. A total of 91,265 participants were covered in these programs.
- CERT-In is regularly sharing safety & security tips and awareness posters, infographics and videos through its official websites and social media handles such as Facebook, X (Twitter), Instagram, YouTube and LinkedIn for sensitising internet users on cyber-attacks, incidents, cybersecurity best practices. CERT-In also shares information about cyber security alerts, advisories, vulnerability notes and current events on regular basis through its official social media handles.

4.2 Drills & exercises

- Cyber security exercises are being conducted by CERT-In to help the organizations to assess their preparedness to withstand cyber-attacks. These exercises have helped tremendously in improving the cyber security posture of the information infrastructure and training of manpower to handle cyber incidents, besides increasing the cyber security awareness among the key sector organizations. CERT-In has conducted 18 such cyber security exercises in 2025.
- Till 2025, CERT-In has conducted 126 Cyber security exercises of different complexities, including table top exercises, with participation from around 1651 organizations covering various sectors of Indian economy from Government/Public/Private including Defense, Paramilitary forces, Space, Energy, Telecommunications (ISPs), Finance, Health, Oil & Natural Gas, Transportation (Railways & Civil Aviation), IT/ ITeS/ BPO sectors and State Data

Centers.

4.3 Conferences and seminars

- CERT-In in collaboration with NeGD conducted a 2-day Cyber Security Workshop & Table Top eXercise (TTX). 100+ participants from 27 states, 38 ministries attended the event which focused on State CSIRT establishment, CERT-In guidelines, Security operation Centre, Cyber Crisis Management Plan, TTX and Cyber laws & Quantum Risks.
- To promote the importance of post quantum cyber readiness, CERT-In organized a one-day training programme at CERT-In during October 2025. More than 80 participants from different Government organizations across the country participated in the event.

5. International Collaboration

5.1 International partnerships and agreements

- Strengthening International cooperation to effectively deal with cyber security issues has been one of the main focus areas of the government. As such, this aspect is being dealt with by way of security cooperation arrangements in the form of Memorandum of Understandings (MoUs) between Indian Computer Emergency Response Team and its overseas counterpart agencies that are willing to work together and share information in a timely manner for preventing cyber incidents and cyber-attacks as well as collaborating for providing swift response to such incidents.
- CERT-In is regularly coordinating with leading service providers and product vendors within and outside the country to obtain advance information on latest cyber threats and attack trends and devise appropriate proactive and preventive measures.
- CERT-In is a member of various working groups under APCERT such as Information sharing working group, Drill working group, Malware Mitigation working group, Tsubame working group and Training Working Group.
- CERT-In is a member of global Forum of Incident Response and Security Teams (FIRST). The membership in FIRST enables incident response teams to more effectively respond to security incidents in a reactive as well as proactive manner.
- CERT-In is also an Accredited Member of Task Force for Computer Security Incident Response Teams / Trusted Introducer (TF-CSIRT/TI).

5.2 Capacity building

5.2.1 Training

- CERT-In delivered the technical training session on "Impact of AI on Cyber Threat Intelligence (CTI)" for APCERT members on 30 December 2025.

- CERT-In participated in the APISC security training course hosted by KrCERT/CC, KISA during Aug 25-29 at Seoul, South Korea.
- CERT-In participated in the APCERT online training on "Centralized threat monitoring/threat hunting" on 29th April 2025.
- CERT-In participated in the APCERT online training on "Ransomware Trends and Case Studies" on 24th February 2025.
- CERT-In officials also participated in the 301L ICS Cybersecurity Training provided by CISA in Idaho falls USA in 2025.

5.2.2 Drills & exercises

- CERT-In has conducted 5, contributed in 1 international exercise planning & scenario development and participated as player in 4 International cyber security drills in 2025.
- CERT-In participated in the Global Inter-governmental POC Directory Simulation Exercise for the Asia-Pacific region on 17 March 2025. The simulation enabled POC from 20 countries to practice operational and diplomatic coordination workflows while strengthening their understanding the use of technical and diplomatic Point of Contact directory and their roles in Cybersecurity cooperation.
- CERT-In contributed and participated in the APCERT Drill 2025 held on 29th July 2025. The theme of the drill was

"When Ransomware Meets Generative AI". The exercise witnessed participation from 22 CERTs across 18 APCERT economies and 7 CSIRTs from OIC-CERT and AfricaCERT, fostering international collaboration and preparedness against AI-driven ransomware threats.

- CERT-In participated in the ACID Drill 2025 conducted during 21–22 October 2025, focusing on "Securing Network Devices at the Edge" along with a parallel TTX on "Cross-Border Threats to Critical Information Infrastructure." The exercise strengthened international readiness by testing response approaches to evolve multi-jurisdictional cyber threats.
- CERT-In participated in the 2nd BRICS Cyber Drill held during 29 – 30 October 2025, focusing on the theme "Central Bank Digital Currency (CBDC) Node Compromise – Systematic Implications". The two-day drill enhanced cross-nation coordination and preparedness for financial-sector cyber incidents with systemic impact.
- CERT-In participated in the global Quantum Dawn VIII international cybersecurity exercise held during 04–06 November 2025, organized by the Securities Industry and Financial Markets Association (SIFMA). The three-day simulation engaged over 900 participants from more than 100 CSIRTs and institutions worldwide, including financial firms, central banks, regulators, and law enforcement. The exercise tested the resilience of core financial operations through multi-faceted crisis scenarios and strengthened global crisis management, recovery planning, and cross-sector information-sharing mechanisms. Participants collaboratively assessed impacts and response strategies, enhancing coordinated decision-making and regulatory preparedness for large-scale cyber events.

5.2.3 Seminars & presentations

- CERT-In participated in the APCERT AGM and presented in the Conference held in Sydney Australia during 25- 27 November 2025.

- CERT-In participated in the FIRST Conference during 22-27 June 2025 in Copenhagen, Denmark.
- CERT-In participated in DEF CON 33, held during 7-10 August 2025 in Nevada USA.
- CERT-In participated in Blue Team Conference held during 9-12 September 2025 in Fairmont Chicago.
- CERT-In participated in Underground Economy held during 01-04 September 2025 in Strasbourg, France.
- CERT-In participated in the 75th Task Force for Computer Security Incident Response Teams (TF-CSIRT) Meeting at Reykjavik, Iceland held during 29 September to 01 October 2025.
- CERT-In participated in CyberCon-2025 held during 15-17 October in Australia.
- CERT-In participated in AUSCERT conference at Star Gold coast, Australia during 20-23 May 2025.

- CERT-In participated in 16th Annual Billington Cybersecurity Summit, held during 9-12 September in Washington DC USA.

5.3 Other international activities

- CERT-In participated in the Eleventh substantive session of the Open-ended Working Group on security of and in the use of information and communications technologies held during 07-11, July 2025.
- CERT-In, MeitY along with MEA conducted a familiarization visit and interactive session for Journalists from EU countries chaired by Dr. Sanjay Bahl, Director General, CERT-In in New Delhi, India on roles and responsibilities of Indian Computer Emergency Response Team (CERT-In), Research and Development as well as Startups in building a secure and resilient cyberspace, countering cyber threats and enforcing security policies etc. followed by a Q&A session on 29 October 2025 at Ministry of Electronics and Information Technology (MeitY).
- The Indian Computer Emergency Response Team (CERT-In), Ministry of Electronics and Information Technology (MeitY), in collaboration with the Ministry of External Affairs (MEA), conducted a cybersecurity familiarization visit and interactive session for visiting journalists from Europe, America and Central Asian countries on 12 December 2025. The session was chaired by Dr. Sanjay Bahl, Director General, CERT-In in New Delhi, India. Shri Krishan Kumar Singh, Joint Secretary, MeitY, offered welcome remarks to the delegation and highlighted various initiative of the ministry, including the India AI Impact Summit

6. Conclusion

CERT-In is the national agency for incident response and various other functions in the area of cyber security for the Indian cyber community. CERT-In is working to improve the security of Indian Cyber space. CERT-In committed to continue its efforts and contributions to the APCERT community to make the Asia Pacific region cyberspace safe and secure.

Contact Information

Postal Address 1:
Indian Computer Emergency Response Team (CERT-In)
Ministry of Electronics & Information Technology (MeitY)
Government of India
Electronic Niketan
6, CGO Complex, Lodhi Road
New Delhi – 110003, India

Postal Address 2:

CERT-In Office, Block – 1

Delhi IT Park, Shastri Park

Delhi – 110053, India

Phone: +91-11-22902703, 22902704

Incident Response Help Desk:

Phone: +91-11-22902657, +91-11-24368572, +91-1800-11-4949 (Toll Free)

Fax: +91-11-24368546, +91-1800-11-6969 (Toll Free)

Incident report to Incident Response Help Desk at:

Email: incident@cert-in.org.in

- User ID: incident@cert-in.org.in
- Key ID: 0xB620D0B4
- Key Type: RSA
- Expires: 2026-12-31
- Key Size: 4096/4096
- Fingerprint: A768 083E 4475 5725 B81A A379 2156 C0C0 B620 D0B4
- Phone: +91-11-22902657
- Toll Free Phone: +91-1800-11-4949
- Toll Free Fax: +91-1800-11-6969

Vulnerability report, security alerts, or any other technical questions/feedback related to cyber security, contact CERT-In Information Desk at:

Email: info@cert-in.org.in

PGP Key Details:

- User ID: info@cert-in.org.in, advisory@cert-in.org.in, subscribe@cert-in.org.in
- Key ID: 0x275CCACF
- Key Type: RSA
- Expires: 2026-12-31
- Key Size: 4096/4096
- Fingerprint: EABE 086A 6FC4 CB47 3F29 A90B DE30 A071 275C CACF
- Phone: +91-11-22902657
- Toll Free Phone: +91-1800-11-4949
- Toll Free Fax: +91-1800-11-6969

Email: csk@cert-in.org.in

PGP Key Details:

- User ID: csk@cert-in.org.in
- Key ID: 0x4EE11788
- Key Type: RSA
- Expires: 2030-05-31
- Key Size: 4096/4096
- Fingerprint: E204 D43D 0296 40FB 8DB9 0290 706D EF4D 4EE1 1788

For International Liaison activities

Email: international@cert-in.org.in

Official social media handles of @IndianCERT

- Facebook: https://www.facebook.com/IndianCERT/
- X (formerly Twitter): https://twitter.com/IndianCERT
- Instagram: https://www.instagram.com/cert_india/
- LinkedIn: https://www.linkedin.com/company/indiancert-cert-in/
- YouTube: https://youtube.com/@indiancert

CERT PH

Philippines National Computer Emergency Response Team

1. Introduction

The Philippine National Computer Emergency Response Team (CERT-PH) Division under the Cybersecurity Bureau, Department of Information and Communications Technology (DICT) is responsible for receiving, reviewing, and responding to computer security incident reports and activities.

CERT-PH also monitors the implementation of the information security incident response plan to ensure that detected and reported cybersecurity incidents and events are given appropriate and immediate response.

The CERT-PH is the highest body for cybersecurity related activities. All CERTs, Government CERTS, Sectoral (or Private) CERTs, as well as organizational CERTs shall coordinate and report incidents to the National CERT.

1.1 NCERT Core Functions

1.1.1 Incident Response

- Responds to Cybersecurity incidents reported to the Bureau (internal and external to the Department); Monitors the implementation of the Information
- Security Incident Response Plan to ensure that detected, and reported incidents are given appropriate immediate action
- Develops well-structured processes for handling and managing information security events and enabling tools, methodologies, and practices.

1.1.2 Vulnerability and Penetration Testing

- Conducts Vulnerability Assessment and penetration testing to Government Agencies and Instrumentalities.
- Examines and evaluates websites/ web applications, mobile applications, network assets, and source code to identify existing vulnerabilities that can be exploited by adversaries.

1.1.3 National Security Operations Center

- Provides technical details and analysis of discovered vulnerabilities and criticality to system owners.
- Ensures the continuous operation of the National SOC, its 24/7 monitoring and response, secure end-point access, protection against DNS-base attacks, and the reputation of connected agencies.
- serves as the centralized facility for detection, monitoring, and rapid response to security incidents in the connected agencies.
- Monitors the system for possible information security threats and injects countermeasures and remedies.

1.1.4 Cyber Threat Monitoring

- Collects and analyzes data from publicly available sources and feeds regarding cyber threats
- Collaborates with international and local communities and organizations on existing and new threats in cyberspace
- Develops an effective implementation approach to monitoring and information sharing of cyber security incidents.

2. Operations and Delivery of Frontline Services

2.1 Incident Response and Handling

From January 1 to December 31, 2025, NCERT managed a total of 2,042 cybersecurity incidents across various critical infrastructure sectors in the Philippines. During this reporting period, the CIR team managed a high volume of security incidents with perfect adherence to service level agreements.

Notably, the team achieved a 100% SLA response rate, ensuring that every threat was acknowledged and addressed within the mandated timeframes. Our resolution speed remains consistent across all severity levels, indicating a robust and scalable response framework.

Figure 1. Incident Handling Overview

2.1.1 Key Performance Indicators (KPIs)

Metric	Achievement	Note
Total Incidents Responded	2,042	Total volume of security events handled.
SLA Compliance Rate	100%	All incidents acknowledged/ responded within target.
Avg. Resolution (High/Critical)	8.94 Days	Time from detection to final remediation.
Avg. Resolution (Med/Low)	8.63 Days	Time from detection to final remediation.

2.1.2 Monthly Breakdown

Throughout the year, the team successfully responded to incidents on a monthly basis, demonstrating sustained operational capability and adaptability to fluctuating demand. Incident response activities remained steady during the first quarter, increased gradually in the second quarter, and peaked significantly in July, when the highest number of incidents were addressed.

Despite the surge, the team effectively managed elevated workloads through August and September, maintaining consistent response efforts during this high-demand period. Incident volumes then declined toward the final quarter, concluding with the lowest number of cases in December.

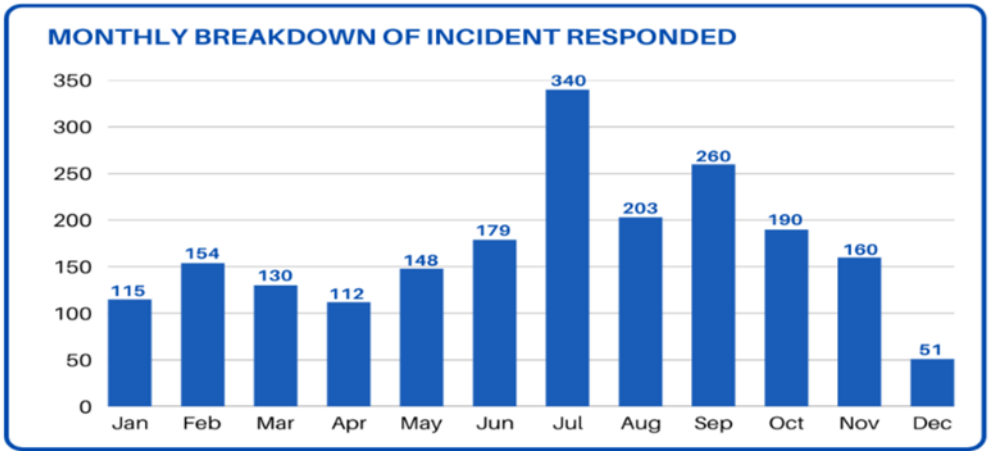


Figure 2. Incidents Handled per Month

2.1.3 Breakdown of Incidents based the Sectors Affected

This accomplishment reflects the wide reach and impact of incident response efforts across both government and non-government sectors. National Government Agencies (NGAs) accounted for the highest number of assisted incidents at 760, highlighting the priority given to protecting core government operations and critical national systems. The private sector followed with 424 incidents, underscoring strong engagement in supporting businesses that are vital to economic continuity.

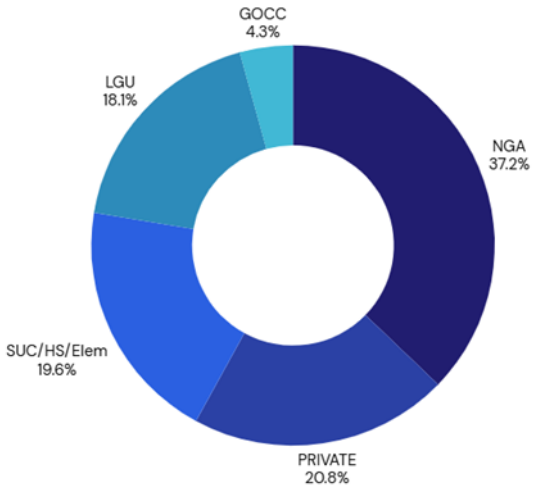


Figure 3. Incidents Handled vs. Sectors Affected

Educational institutions, including state universities and colleges, high schools, and elementary schools (SUC/HS/Elem), recorded 401 incidents, showing a sustained focus on safeguarding learning environments and academic systems. Local Government Units (LGUs) were assisted in 370 incidents, reflecting support extended to frontline public service providers at the local level.

Lastly, Government-Owned and Controlled Corporations (GOCCs) logged 87 incidents, indicating targeted assistance to specialized government enterprises. Overall, the breakdown demonstrates a comprehensive and inclusive approach to incident handling across critical sectors.

2.1.4 Breakdown of Incidents based on Incident Category

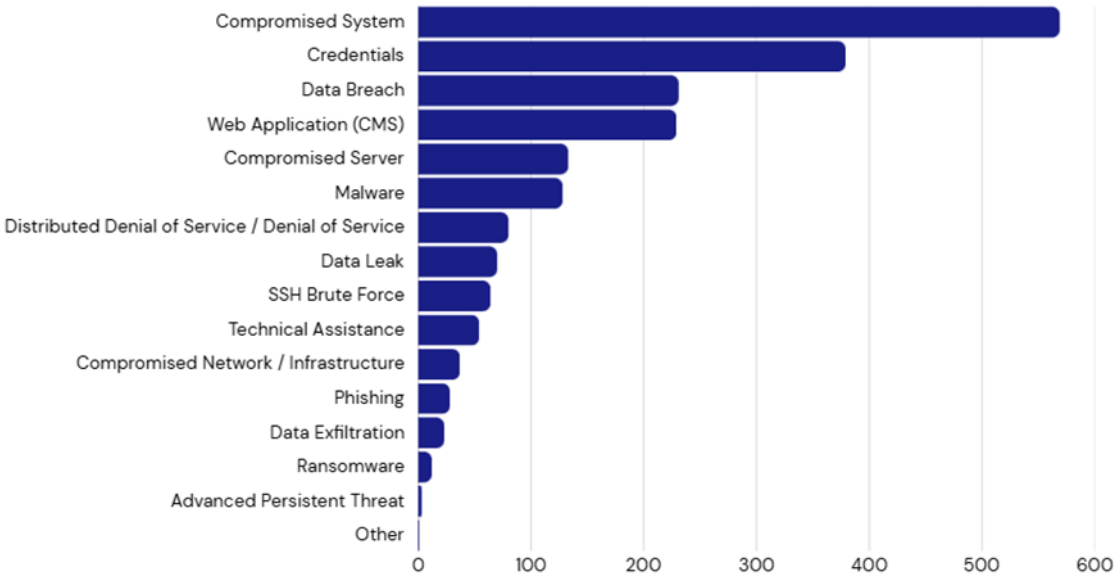


Figure 4. Incidents Handled vs. Incident Type

This breakdown reflects the full range of cyber incidents handled, led by compromised systems, followed by credential-related incidents, data breaches, and web application (CMS) compromises, with additional cases involving servers, malware, and service disruptions. All recorded incidents across all categories were responded to within the prescribed Service Level Agreement (SLA), achieving a 100% SLA compliance rate. This means every incident handled—regardless of severity or type—received timely action within the required response timeframe, demonstrating consistent operational readiness, effective incident management processes, and strong coordination in responding to cyber threats.

2.1.5 Breakdown of Incidents based on Severity Level

This severity-level breakdown shows that the majority of incidents handled were classified as **Moderate (1,499 cases)**, indicating a high volume of routine but operationally significant cyber issues requiring prompt action. This is followed by **Low-severity incidents (278 cases)** and **High-severity incidents (188 cases)**, reflecting a mix of minor events and serious threats with potential operational impact. **Elevated incidents (63 cases)** and a smaller number of **Critical incidents (14 cases)** represent the most sensitive cases that required immediate and heightened response.

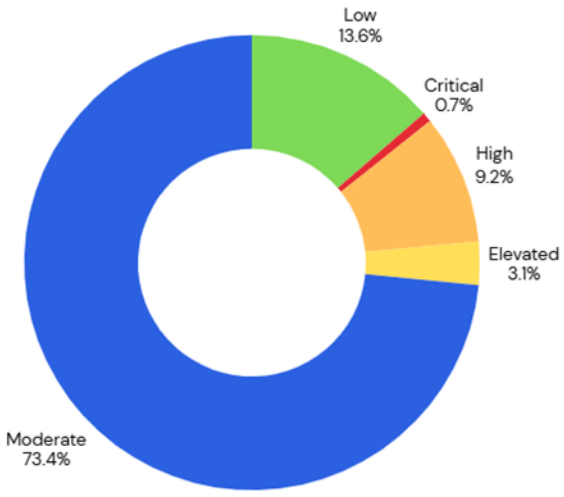


Figure 5. Incidents Handled vs. Severity Level

2.2 Vulnerability Assessment and Penetration Testing

2.2.1 Number of Accomodated Requests for VAPT

From January to December 2025, CERT-PH received and responded to a total of 214 requests from various government agencies and instrumentalities with an average of 18 requests each month.

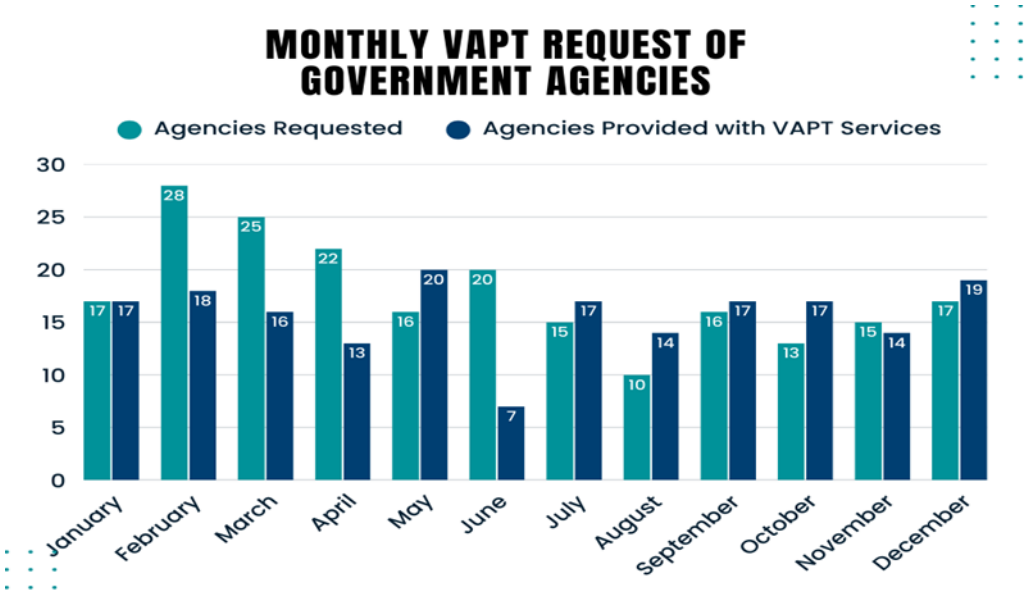


Figure 6. Monthly VAPT request and agencies undergone VAPT

Of these requests, 189 agencies were provided with VAPT services. Most requests originate from National Government Agencies (NGAs), followed by Local Government Units (LGUs), State Universities and Colleges (SUCs), and Government-Owned and Controlled Corporations (GOCCs).

In line with these requests, Vulnerability Assessment and Penetration Testing (VAPT) services were conducted, both remotely and on-site, on a total of 3,251 assets including web applications, networks, and source codes.

These activities aimed to identify potential attack vectors that could be exploited by adversaries to compromise the security, privacy, and operational integrity of government agencies and other stakeholders of DICT. The engagements also involved proactive collaboration with various stakeholders to strengthen their overall cybersecurity posture.

Moreover, from the total assessed and tested assets, a cumulative 2,844 vulnerabilities were identified, of which 628 were successfully remediated. The remaining vulnerabilities were either classified as false positive or could not be verified as resolved due to the non-submission of the Post-Assessment Form (PAF).

Further, some government agencies risk-accept identified vulnerabilities when they fall within their defined risk appetite, meaning potential impacts align with acceptable business disruption levels. Also, dependencies delayed fixes of the agencies, such as third-party vendor involvement, unavailable patches or updates, and lack of skilled manpower to remediate the vulnerabilities. Another reason why agencies risk-accept vulnerabilities is to meet the given remediation timeline by CERT-PH, as they need additional timeline especially when numerous and highly complex vulnerabilities were identified during the assessment.

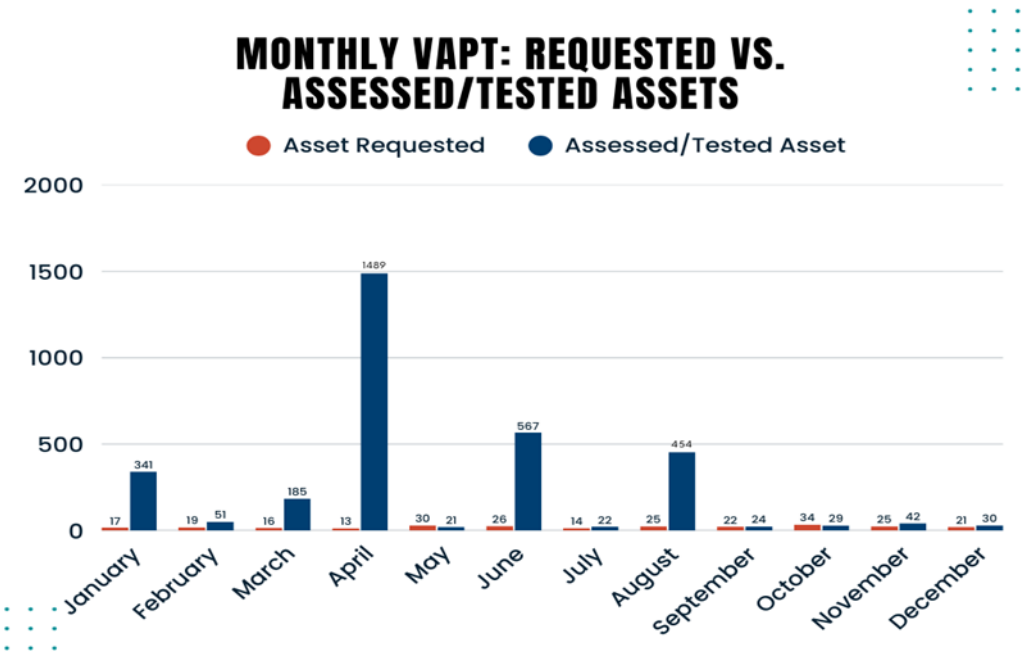


Figure 7. Systems requested for VAPT and systems undergone VAPT monthly

2.2.2 Project Secure Online Network Assessment and Response System (SONAR)

In the exigency of service and to ensure data privacy and security of the information assets of the various government agencies, the CERT-PH is conducting Monthly Vulnerability Scanning of publicly accessible assets under the GOV.PH and EDU.PH domains through the PROJECT SONAR. The Project encompasses the Automated Vulnerability Scanning and Detection and Domain Name System (DNS).

The conduct of vulnerability scanning and detection across various government agencies and instrumentalities adopts a comprehensive and proactive strategy to monitor and mitigate risks associated with identified flaws and misconfigurations of publicly accessible digital assets of government agencies and instrumentalities. These assets include websites, web applications, portals, web servers, name servers, among others. Although this proactive approach is different from the frontline service provided by the CERT-PH through its Vulnerability Assessment and Penetration Testing (VAPT), this endeavor is in line with National Cybersecurity Plan (NCSP) and the Department's commitment and unwavering resolve mitigate vulnerabilities and reducing cyber risk of Philippine government publicly accessible digital assets.

In 2025, CERT-PH has conducted automated vulnerability assessment to approaching 3000 website/web applications of 1,224 government agencies and instrumentalities, identifying almost 370,000 vulnerabilities, of which 13,851 were remediated.

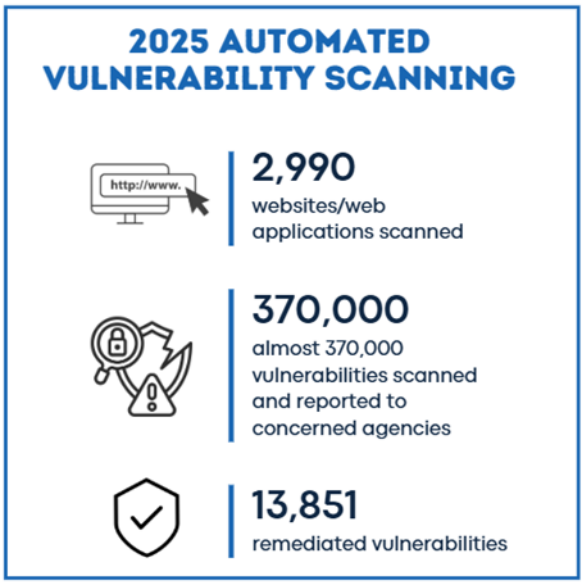


Figure 8. 2025 scanned websites, reported vulnerabilities, and remediated vulnerabilities

2.3 National Security Operations Center

2.3.1 Deployment Overview

NSOC successfully achieved its target of establishing connections with thirty (30) national government agencies in 2025, marking a significant milestone in strengthening inter-agency cybersecurity coordination and incident monitoring capabilities. This accomplishment reflects the continued commitment to enhancing the government's overall cyber defense posture through improved collaboration, information sharing, and centralized security operations.

Building on this achievement, NCERT aims to significantly expand its coverage to ninety (90) national government agencies in 2026. This expansion is intended to further reinforce the government's resilience against the ever-evolving cyber threat landscape by enabling broader visibility, faster incident response, and more proactive threat detection across critical government systems and networks.

2.3.2 Security Metrics

Among the thirty (30) connected agencies, twenty-eight (28) are fully operational within the NSOC framework, demonstrating effective coordination and integration across multiple government sectors.

Significant progress has also been made in strengthening the cybersecurity posture of these agencies through the implementation of standardized security measures to protect data and ensure operational continuity.

- 97% Endpoint protection has been implemented in 29 out of 30 agencies.
- 93% Endpoint policies have been configured in 28 out of 30 agencies.
- 97% Server policies have been put in place in 29 out of 30 agencies.

These efforts are central to NSOC's mission to protect and secure the nation's most critical assets, ensuring that the agencies can operate effectively in a complex cybersecurity environment.

2.3.3 Ticket Status

In 2025, NSOC handled a total of **36,509 tickets**, highlighting the system's comprehensive nature and the increasing volume of incidents managed.

The significant increase in the number of tickets, from **4,101** in **2024**, can be attributed to enhanced visibility resulting from the expanded NSOC coverage through deployment to more government agencies and institutions.

With **26,754 tickets closed**, NSOC demonstrated efficiency in monitoring and mitigating the incident. The **60 tickets closed with no response** represent cases that were closely monitored and had reached the maximum follow-up threshold, highlighting the section's commitment to addressing and resolving detected incidents.

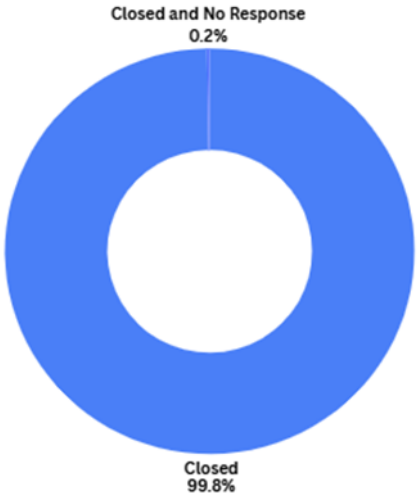


Figure 9. Percentage of Closed Tickets with No Response and Closed Tickets

2.3.4 Incident Case Severity

As for the severity classification of resolved incidents, NSOC handled a total of **15,400 low-risk** cases, followed by **10,708 medium-risk**, **9,624 high-risk**, and **637 critical-risk** cases.

This distribution of incidents across severity levels reflects the dynamic nature of threats encountered throughout the year by the connected agencies and the continuous efforts to address them. Effectively managing low- and medium-risk cases helps prevent potential escalation, while high- and critical-risk cases require meticulous scrutiny and swift mitigation to protect government systems and infrastructure.

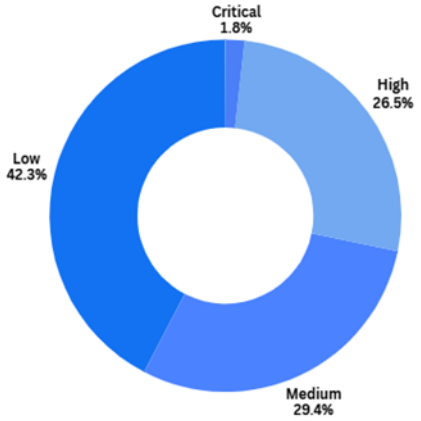


Figure 10. Severity Classification of Resolved Incidents

To enhance incident management, the section refined its ticketing system and reporting processes, ensuring better tracking, follow-up, and documentation of each case. These improvements contributed to a more structured and efficient approach.

As cyber threats continue to evolve, NSOC remains committed to strengthening its capabilities, improving operational workflows, and fostering collaboration with agencies to enhance national cybersecurity resilience.

2.3.5 Protective Domain Name System (Pdns)

To intensify the DICT's capability to protect personal and sensitive data processed and stored within government assets, the PDNS is crucial in preventing further attacks and ensuring the integrity and stability of the domain name system.

This system further bolsters DICT's cybersecurity framework by preventing malicious activities at the DNS level, helping to mitigate a range of cyber threats.

In 2025, PDNS processed an average of 1.06 billion DNS queries per month and **blocked an average of 14.68 million malicious queries**, resulting into the following:

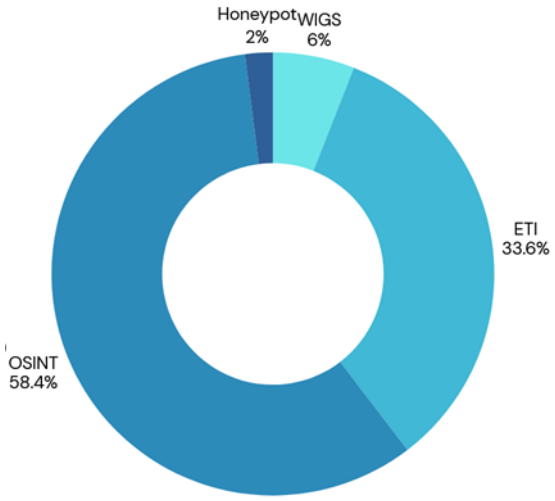
- **12.77B DNS** queries processed for the year
- **176.13M** Malicious queries blocked for the year

This capability not only enhances the security of online interactions but also mitigates the risk of malware infections, phishing attempts, and other cyber threats in connected government entities.

By addressing potential risks before they can escalate, PDNS exemplifies DICT's proactive approach to cybersecurity. This approach complements other layers of security, ensuring a comprehensive defense against emerging threats and reinforcing the overall security posture of government networks.

2.4 Cyber Threat Monitoring and Information Sharing

Throughout the period spanning January to December 2025, a comprehensive tally of 1,828 monitored threats were meticulously documented. The vigilant efforts of CERT-PH were channeled through multiple platforms, showcasing the organization's robust approach to threat intelligence.



2.4.1 Monitoring Sources

- Web Information Gathering System (WIGS): 109 Threats
- External Threat Intelligence System (ETI): 615 Threats
- Open Sources: 1,067 Threats
- Honeypot and other Sources: 37

2.4.2 Type Of Threats Monitored

- Credential Leakage
- Website Redirection
- Website Defacement
- Data Breach

100% of reported or escalated threats are promptly addressed by the Incident Response Section.

Government and Emergency Services (NGAs, LGUs, GOCCs and instrumentalities) account for **58.8% of Total Monitored Threats**.

2.4.3 Threats Feeds and Advisories

Cyber threat feeds and advisories are issued on a regular basis. Reports and information about the latest cyber threat news, topics, and articles from the web that may impact the Philippine government and cyberspace are gathered and analyzed to provide timely, actionable advice to our stakeholders so they can protect themselves online.

2.4.4 Summary Of Achievements

- Assisted the CII for immediate resolution of Monitored Vulnerabilities
- Provided 1,828 monitoring reports for various CII sector
- Delivered 282 Cyber Threat and Intel Advisories and Feeds to CII
- 3,562 agency assets were monitored

3. Cybersecurity Capability Building, Awareness Activities, and Information Campaign

3.1 HackforGov Capture the Flag Competition 2025

The program was successfully launched in October 2025, bringing together 15 teams from state universities and colleges (SUCs) Region across Region IV-A. Building on this momentum, regional qualifying rounds were conducted across 16 regions from October to December 2025, demonstrating strong coordination and participation. The program achieved significant engagement, with a total of 855 participants representing 158 SUCs nationwide.

On December 9, 2025, the nation's brightest students showcased their cybersecurity talents in the much-anticipated HackforGov: Cyber Challenge Competition. The event took place at the Sequoia Hotel Manila Bay in Parañaque, where a total of 20 elite teams from various regions across the Philippines competed for the prestigious title of National Champion.

This year's participants improved their problem-solving and technical skills compared to last year as reflected in their higher scores. Team Akira: Requiem of the Asia Pacific College emerged as the national champion setting a record high of 3,755 points.

Following closely behind is the team from Central Visayas Sly Kint Bacalso won 1st runner-up with 3,680, while Team 0x0FBYON3 of Wildcard Teams placed 2nd runner-up with 3,510 points.

This year's theme, "Cyber Guardians: Empowering Today's Defenders, Securing Tomorrow's Digital Nation," aimed to inspire young minds to step into the role of digital defenders. As cyber threats grew in complexity and scale, the need for skilled, ethical, and innovative cybersecurity talent became increasingly critical.

Through this theme, HackForGov 2025 envisioned a future where youth were not just passive users of technology, but active protectors of digital infrastructures. By equipping students with the skills, mindset, and mission of a cyber guardian, the event empowered them to play a vital role in safeguarding national digital sovereignty and resilience. Participants tackled real-world challenges, simulated defense scenarios, and collaborated to build a safer cyberspace for all.

Throughout the event, students demonstrated their cybersecurity skills on the Capture-the-Flag (CTF) platform, a competitive environment simulating real-world cybersecurity scenarios. Participants tackled a series of challenges designed to test their technical abilities, critical thinking, and problem-solving skills across various domains of cybersecurity.

3.2 Conduct of Cybersecurity Drills and Simulation Exercises

Philippine CERT Conference (CERTCON) 2025

Successfully conducted the 3rd Annual Philippine CERT/CSIRT Conference (CERTCON) 2025. CERTCON 2025 aimed to address pressing cybersecurity challenges and foster collaboration nationwide. This year's conference introduced a more technically focused format, departing from previous years by placing greater emphasis on both foundational knowledge and practical skills development in the field of cybersecurity. Speakers and participants came together to exchange insights and experiences under the theme, "From Innovation to Protection: Innovating Security, Empowering Progress".

The conference featured a series of workshops, presentations, and interactive sessions led by industry experts. Participants engaged in discussions on critical topics such as threat intelligence, digital forensics, and security policy development, fostering a comprehensive understanding of contemporary cybersecurity issues.

As cybersecurity threats continue to evolve, CERTCON 2025 served as a vital platform for knowledge sharing, skills enhancement, and the development of a unified response to cyber incidents.

The program began with expert-led discussions and technical briefings designed to provide participants with a solid understanding of current cyber threats, defense mechanisms, and emerging technologies. These sessions established the necessary theoretical foundation to effectively support the practical activities that followed.

Following the discussions, participants engaged in a series of guided, hands-on exercises that replicated real-world

cybersecurity scenarios. These exercises were facilitated by technical experts who provided structured walkthroughs to ensure that all participants, regardless of technical background, could actively engage with the material and gain meaningful insights. The hands-on activities covered key areas such as threat identification, incident response, vulnerability management, and the application of cybersecurity tools.

This event brought together a diverse group of participants from various government agencies and the cybersecurity community, to address pressing cybersecurity challenges and foster collaboration across the nation.
WATCH CERTCON AVP HERE: https://www.facebook.com/share/v/18JMKmaWsP/

3.3 Cyber Range Exercise

In a proactive effort to enhance cybersecurity readiness and collaboration among various government agencies, a series of Cyber Range exercises were conducted over the course of the year. These exercises, totaling 20 sessions, brought together a diverse group of 792 individuals from different government agencies.

The participants engaged in hands-on Cyber Range simulations, simulating real-world cyber threats and incidents in a controlled environment. The exercises provided a unique opportunity for cybersecurity professionals to test their skills, improve incident response capabilities, and strengthen their ability to work together effectively in the face of evolving cyber threats.

The collaborative nature of the exercises fostered knowledge sharing and cross-agency cooperation, ensuring that each participant gained valuable insights into the latest cybersecurity challenges. As a result of these Cyber Range exercises,

the participants not only honed their technical skills but also established a network of contacts across government agencies, laying the groundwork for improved coordination in the event of a real-world cyber incident. The commitment to regular training and collaboration demonstrated a collective dedication to maintaining a robust and resilient cybersecurity posture across the government sector.

3.4 NCERT's Collaborative Activities and Information Sharing with different CERTs

3.4.1 APCERT (Asia Pacific Computer Emergency Response Team):

NCERT is a recipient of APCERT's daily issuance of cyber threat feeds, ensuring the timely receipt of relevant threat intelligence to enhance cybersecurity measures. NCERT also actively participates in various APCERT-organized activities, including webinars, trainings, and cyber drills, which contribute to capacity building and regional cooperation in cybersecurity.

3.4.2 TWNCERT (Taiwan Computer Emergency Response Team):

NCERT engages in continuous information sharing with TWNCERT, particularly concerning suspicious cyber activities. This ongoing exchange of data strengthens the cybersecurity response capabilities of both teams and helps address potential cyber threats effectively.

3.4.3 CAMP (Cybersecurity Alliance for Mutual Progress)

NCERT regularly receives updates for inclusion in the CAMP Newsletter, ensuring that relevant cybersecurity information reaches the broader community. NCERT also participates in various CAMP-led activities, such as webinars and trainings, further enhancing the knowledge and skills required for robust cybersecurity defense.

3.4.4 SingCERT (Singapore Computer Emergency Response Team):

NCERT collaborates with SingCERT through the sharing of information on the evolving threat landscape. NCERT also participates in SingCERT's activities, including webinars and training, and cyber Drill contributing to mutual efforts aimed

at addressing emerging cyber threats and improving cybersecurity resilience.

3.4.5 AJCCBC (ASEAN-Japan Cybersecurity Capacity Building Centre):

NCERT collaborates closely with AJCCBC in various capacity-building initiatives focused on enhancing cybersecurity skills and knowledge. These activities include specialized training, joint exercises, and participation in programs aimed at developing cybersecurity professionals within ASEAN. NCERT also engages in information sharing with AJCCBC on current and emerging cyber threats, contributing to a broader regional effort to strengthen cybersecurity resilience across the ASEAN region.

These partnerships between different CERT's enhance the exchange of threat intelligence, foster regional cooperation, and support the development of advanced cybersecurity capabilities through shared knowledge and participation.

CERT Tonga

Tonga Computer Emergency Response Team

1. Highlights of 2025

1.1 Summary of major activities

In 2025, CERT Tonga reached two significant milestones in its cybersecurity landscape: a major defensive response to a national crisis and the enactment of landmark legislation.

1.1.1 The National Health Information System (NHIS) Ransomware Attack

In June 2025, Tonga's Ministry of Health was targeted by a major ransomware attack that crippled the National Health Information System (NHIS).

- The Incident: Discovered on June 15, 2025, the attack encrypted vital patient records, prescriptions, and medical histories across the country's four hospitals.
- The Response: Hackers encrypted the NHIS Oracle database API (VAMED application not the actual data files) and sent ransom note threatening that they are aware of cases where recovery companies tell MoH that the ransom price is $5M dollars, but in fact they secretly negotiate with them for $1M. If MoH approached them directly without intermediaries MoH would pay several times less. The Tongan Government refused to pay nor negotiate with the perpetrators. However, Tonga (MoH) requested to the Australian Government for the emergency Cyber Disaster Relief provided by the Cyber RAPID Team (Deloitte).
- Recovery: A specialist cyber team from Australia was deployed to assist CERT Tonga and the MoH. By July 18, 2025, the system was reported as fully restored using backups and enhanced security protocols, though the event underscored the urgent need for digital resilience.

1.1.2 The Cybersecurity Act 2025

Following the health sector crisis, the Kingdom formally strengthened its legal framework with the Cybersecurity Act 2025, which received Royal Assent on August 28, 2025.

1.2 Achievements & milestones

In 2025, CERT Tonga significantly advanced the Kingdom's digital resilience through international collaboration, specialized capacity building, and intensive national outreach. Key achievements include:

- International Strategic Alignment: The signing of a landmark Cybersecurity MoU with Australia established a framework for threat intelligence sharing and coordinated incident response, serving as a pillar of the 2025 Australia–Tonga Development Partnership Plan.
- Advanced Institutional Capability: Internal technical expertise was substantially elevated by the return of a senior staff member following the completion of a Master of Cybersecurity Analysis in Australia. This specialised skill set enhances the department's daily operation.
- National Resilience & Outreach: The department successfully delivered 10 comprehensive awareness sessions across the Kingdom. These targeted initiatives improved the security posture of Government Ministries and NGOs ensuring that critical infrastructure and civil society remain protected against evolving digital threats

2. About CSIRT

2.1 Introduction

Tonga Computer Emergency Response Team (CERT Tonga) is a national body that serves to be the main point of coordination for cyber security issues with one of the aims to serve as the Kingdom of Tonga's national point of contact for cyber security issues. CERT Tonga is one of the departments of the Ministry of MEIDECC and is still the only CERT in Tonga. CERT Tonga mainly engages with domestic (both public and private sectors), regional and international stakeholders within its statutory scope to gather information, knowledge, and expertise to raise awareness, mitigate threats, while allowing safe developments and usage of digital technologies within Tonga cyberspace.

2.2 Establishment

CERT Tonga was established and effective from July 15th, 2016, with a Term of Reference (TOR) as approved by His Majesty's Cabinet Decision (HM CD, Tonga) on July 15th, 2016. The CERT Tonga Board was established concurrently to provide oversight and strategic direction in accordance with the TOR.

Vision: A safe and secure digital environment for the Kingdom of Tonga and its citizens.

Mission: To coordinate and collaborate amongst stakeholders to prevent through public awareness, detect and manage cyber threats in the Kingdom of Tonga.

2.3 Resources

CERT Tonga serves as the Kingdom of Tonga's National Computer Emergency Response Team. It acts as the central point of contact for national cybersecurity matters, including incident response, digital forensics, awareness programs, professional training, and the dissemination of security bulletins and advisories.

The department operates under the **Ministry of Meteorology, Energy, Information, Disaster Management, Environment, Communications, and Climate Change (MEIDECC)**.

Organizational Structure and Divisions

To better align with international standards and national needs, CERT Tonga recently restructured from two divisions (Engagement and Technical) into three specialized divisions:

i. Governance, Risk Management, and Compliance (GRC)
ii. Communication, Awareness, and Engagement (CAE)
iii. Digital Forensics and Incident Response (DFIR)

Workforce and Development

The department's current workforce is a blend of permanent establishment staff and contracted specialists.

- Permanent Staff: Director for CERT Tonga, Senior Engagement Officer, Assistant Engagement Officer, and Security Analyst.
- Cybersecurity Workforce Development Program (CWDP): Funded by CERT NZ since November 2021, this program supplements the team with an IT System Operator (Apprentice) and a Security/Forensic Analyst. The CWDP completed in August 2025.
- Future Growth: For the 2025–2026 fiscal year, a proposal has been submitted to establish several new leadership and technical roles, including:
  - Deputy Director / Communication, Awareness and Engagement (CAE) Team Leader
  - Deputy Director / Digital Forensics and Incident Response (DFIR) Team Leader
  - Chief Information Security Officer (CISO)
  - Senior Information Security Analyst
  - Digital Forensic Analyst
  - IT System Operator

2.4 Constituency

CERT Tonga provides cybersecurity services and support to a broad range of stakeholders across the Kingdom, including:

- Government Ministries, Departments, and Agencies.
- Private Sector Businesses
- Public Enterprises

- Non-Governmental Organizations (NGOs)

3. Activities & Operations

3.1 Scope and definitions

As mandated in the Term of Reference (ToR) of HM CD 15th July 2016, CERT Tonga aims to:

- Serve as the Kingdom of Tonga's main point of contact for cybersecurity issues.
- Collaborate with the regional and international CERTs.
- Issuance of security warnings and alerts
- Provide security awareness campaigns.
- Conduct an annual cyber security threat survey.
- Identify capacity-building programs for staff.
- Digital evidence handling.
- Provide forensic services.

CERT Tonga's current services within the Ministry of MEIDECC are:

- **Engagement** – Engaging with Domestic, Regional, and international organizations and committees are managed and fit for purpose to assist CERT Tonga in carrying out its function.
- **Proactive Services** – Maintaining proactive services (awareness raising, trainings, security bulletin and advisories) to ensure cyber threats are mitigated and cyber incidents prevented.
- **Reactive Services** – Be prepared with reactive services (incident response SOPs and best practices) to ensure that the impact of cyber incidents is contained, investigated, mitigated, and restored back to normal services.
- **Digital Forensic Services** – From time to time, providing digital forensic analysis services to the Tonga Police when requested to assist them. To enable their obtaining of digital evidence for investigation and battling cybercrime.
- **Administration and Management** - Relevant administrative and support services are provided to ensure that the department can deliver its intended output, and with its collaboration with other departments of the Ministry of MEIDECC.

3.2 Incident handling reports

Throughout 2025, several reports were received regarding malicious IP address activities originating from third parties attempting to scan and probe publicly exposed services. Phishing and fraud incidents were also detected and investigated during the year. In addition, multiple requests for digital forensic assistance were provided to law enforcement agencies, particularly the Tonga Police, to support ongoing cybercrime investigations.

Notably, a ransomware incident significantly impacted the Ministry of Health Tonga, temporarily crippling critical systems and disrupting some health services. This incident highlighted the growing threat of ransomware attacks and

underscored the need for strengthened cybersecurity measures, improved incident response capabilities, and greater collaboration between government agencies and national cybersecurity stakeholders.

3.3 Publications

- Advisories and Security Bulletins can be seen through our CERT Tonga Website (https://cert.gov.to/)

4. Events organized / hosted

4.1 Training

Threat Hunting Practical Training – The CERT Tonga team and the Digital Transformation Department had the opportunity to partake in the threat hunting training lead by the Cyber Rapid Team of the Australia's Department of Foreign Affairs and Trade.


Above: Threat Hunting with Rapid Team at the Ministry of MEIDECC Conference Room [March 2025].

Hands-on session exploring tools for security monitoring, incident response, and investigation. with APNIC whereas CERT Team with APNIC hands-on session exploring tools for security monitoring, incident response, and investigation.

Above: CERT Team at the main office during the training session with Adli Wahid in [July 2025]

CERT Tonga's Cybersecurity Awareness to the following stakeholders:

Throughout 2025, CERT Tonga executed a series of targeted awareness initiatives involving key stakeholders, including various Government Ministries, departments, and our strategic partner, Tonga Women in ICT (TWICT). These sessions were designed to provide a comprehensive overview of CERT Tonga's operational mandate and an in-depth analysis of the 2025 cyber threat landscape. By fostering these partnerships, CERT Tonga continues to strengthen the nation's collective defence against evolving digital risks.

Community - Free Wesleyan Church of (Halafo'ou) Pahu

Tonga Women in ICT (TWICT) ICT Expo, 2nd of May 2025

Non-government organisation, Government Ministry & Departments

Below: Tonga Women in ICT staff & Intern

Below: Department of Meteorology operates under the Ministry of MEIDECC

Below: Department of Communication operates under the Ministry of MEIDECC

4.2 Drills & exercises

CERT Tonga was also invited to join with The Women in ICT (TWICT) hosting a Capture the Flag exercise for the schools with our Security Trainer from APNIC, Adli Wahid in [July 2025]

5. International Collaboration

5.1 International partnerships and agreements

In September 2025, CERT Tonga significantly elevated its strategic partnership with Australia to address the rising frequency of regional cyber threats. This cooperation was formalised through a new Memorandum of Understanding (MoU) and the elevation of bilateral ties via the "Kaume'a Ofi" (Close Friends) Partnership Agreement. These initiatives focus on intelligence sharing, capacity building, and coordinated incident response.

5.2 Capacity building

CERT Tonga became a co-convener with NCSC NZ for the Capacity Building Working Group (CBWG) and the first formal meeting took place in Wellington, NZ June 2025. However, a key part of PaCSON is the Capacity Building Working Group. Over the years, we have seen the implementation of various initiatives and the capacity growth of members that have contributed to their respective national efforts. To help shape future efforts in the Pacific and noting the increase of partners wanting to engage on Capacity Building, members have agreed to the establishment of the Capacity Building Working Group Three-Year Action Plan to signal the areas of need at a Pacific regional level.

The five pillars will channel our focus to help build capacity in areas that matter most to our PaCSON members and chart a way forward that will be tangible and measurable.

5.2.1 Training

CERT Tonga with representative from Tonga Women in ICT and Digital Transformation Department joined the Cybersecurity Training & Exercise for Pacific Island facilitated by MIC Japan and JICA in Fiji [September 2025]

Senior Internet Security Specialist Adli Wahid and Dr. Etuate Cocker led a regional cybersecurity workshop in Port Vila. Collaborating with ITU and APNIC, the program—which included a CERT Tonga staff member—built capacity for ten Pacific nations. The session focused on strengthening digital pathways and fostering regional cooperation [December 2025]

Two participants from CERT Tonga attended the APISC training course in Korea [August 2025] hosted by KISA

CERT Tonga also participated in the APT Training Course on AI and Cybersecurity in Shanghai CHINA [September 2025]

5.2.2 Drills & exercises

CERT Tonga also attended the GISEC- GLOBAL Cyber Drill 2025 that was hosted by ITU and UAE Cybersecurity in Dubai, May 2025. significant events in the cybersecurity domain, it took place from May 6 to 8, 2025, in Dubai. Organized by the International Telecommunication Union (ITU) and hosted by the UAE Cyber Security Council, this drill aims to enhance international cyber resilience and strengthen cybersecurity capacity through regional cooperation. It involved over 130 national cybersecurity authorities and global CERTs/CIRTs/CSIRTs, fostering cross-border collaboration and response strategies against evolving cyber threats. cybersecurity tactics and procedures.

The 2025 ITU Regional Asia-Pacific CyberDrill took place from September 2 to 5, 2025, in Ulaanbaatar, Mongolia. This event aim was to unite the cybersecurity community across the region and foster international cooperation. It will feature four thematic sessions: Reflect, Share, Learn, and Practice, focusing on building cyber resilience and safeguarding critical information infrastructure. The event will include high-level regional conferences, hands-on training sessions, and simulated cyber incident response exercises.

Below: CERT Tonga and a few from the Pacific Region attended the Asia Pacific Cyber Drill in Mongolia, September 2025.

5.2.3 Seminars & presentations

FIRST Conference 2025 in Copenhagen, DENMARK

Below: CERT Tonga and participants from PaCSON Community, attended the FIRST Conference in Copenhagen June 2025

Below: CERT Tonga with APCERT Members joined the FIRST Conference in Copenhagen 2025

Below: CERT Tonga was fortunate to attend the Cybersecurity Workshop for ASEAN Member States and Pacific Island Forum Member States (SG Cyber Leadership Programme) in [December 2025]

The RSA Conference International Cybersecurity Forum 2025 from May 28th to 01st June in San Francisco, USA

Telecommunication Study Tour to Australia's Regulators and Commission Authorities from 5 – 9 May 2025, Melbourne and Canberra, AUSTRALIA


Global Forum on Cyber Expertise (GFCE) Annual Working Group Meeting and Global Conference on Cyber Capacity Building (GC3B), 13 – 15 May 2025 in Geneva, SWITZERLAND.


The first Pacific Cyber Week, with 2nd Pacific Cyber Capacity Building and Coordination Conference (P4C) from August 11th to 14th 2025 in Nadi, FIJI

Internet Corporations for Assigned Names and Number 84 (ICANN84) 2025 AGM, 25 – 30 October 2025 in Dublin, Republic of IRELAND.

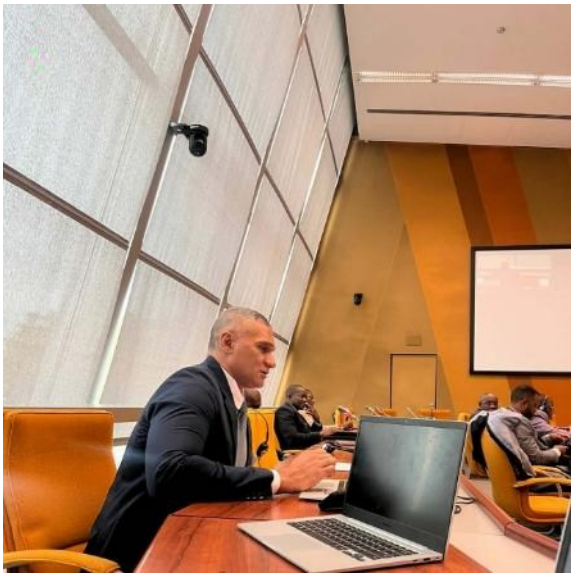
Asia Pacific Internet Governance Academy (APIGA) 2025 from 18 – 22 August 2025 in Busan, ROK

5.3 Other international activities

Under the engagement between CERT Tonga and the Council of Europe, here are the following activities that CERT Tonga attended in 2025.

The TCY 32, Octopus Conference and the Glacy-e Steering Committee

Representative from the Pacific to the events



Director of CERT Tonga – Mr. 'Esau L.M Tupou

Attending the **Underground Economy Conference 2025**, co-hosted by the Cybercrime Programme Office of the Council of Europe (C-PROC) in cooperation with Team Cymru, on 1 – 4 September 2025, at the Headquarters of the Council of Europe in Strasbourg, France.

CERT Tonga is currently a member of the PaCSON Community joining in with 17 Pacific Island countries in this community. In 2025, the PaCSON AGM was held in Christmas Island, Kiribati in [October 2025], Director for CERT Tonga and Security Analyst attended this AGM.

CERT Tonga also attended the APCERT AGM and Conference that was held in Sydney Australia in [November 2025]

6. Future Plans

6.1 Future projects

CERT Tonga has started the Foundation of Security Operation Center (SOC) for small CERT/CSIRT team in July 2025. This will be developed to become an operational and real-time SOC for small organizations in Tonga to monitor and collect firsthand data for analysis and reporting.

CERT Tonga is in the process of discussion and collaboration with key stakeholders to develop the Tonga National Cyber Security Strategy for 2026 – 2030.

Discussion of developing the Armed Forces (His Majesty's Armed Forces) Cyber Command Component (Cyber Defence) capability is also another ambition for CERT Tonga soon.

6.2 Future Operation

CERT Tonga continues to work closely (as the alternative Government Advisory Committee (GAC) representative for Tonga) with the Internet Corporations for Assigned Names and Numbers (ICANN) mainly for the governance of the ".to" ccTLD and to become more active and engaging the APAC Space with the Asia-Pacific partners. This will include collaboration for ICANN Capacity building opportunities of trainings and awareness for Tonga's Tertiary Institutions (Christ's University in the Pacific, Tonga National University, and Tupou Tertiary Institutions), ISPs, Law enforcement and

policy makers for awareness of the digital architecture of the Internet, namely the Domain Name System (DNS). DNS abuse is one of the issues CERT Tonga is facing when it comes to the ".to" ccTLD. Also encourage opportunities for the next generations of Tonga to enroll (nextGen program) and anyone to apply to the ICANN Fellowship program, which offers a lot of online trainings and awareness about the Internet and preserving it to be "One World, One Internet".

7. Conclusion

As a member of APCERT, CERT Tonga endeavor to maintain the international coordination, collaboration, capacity building and sharing of information with other members of APCERT.

CERT VU

Computer Emergency Response Team Vanuatu

1. Highlights of 2025

1.1 Summary of major activities

- In 2025, CERTVU successfully responded to over 1,000 cybersecurity incidents, demonstrating sustained operational readiness and growing national demand for incident response support.
- CERTVU continued to strengthen its regional engagement, particularly through active participation in PaCSON initiatives.
- Implemented the CERTVU capacity-building program for rural communities, expanding cybersecurity outreach beyond urban centers.
- CERTVU consistently delivered National Cybersecurity Awareness through multiple initiatives, including:
- Active engagement via CERTVU social media platforms.
- Weekly radio talk shows every Friday morning with the Vanuatu National Radio Broadcaster.
- Delivered Cyber Capacity Building through the Famili i Redi Program, in collaboration with World Vision Vanuatu, providing cybersecurity training for seasonal workers traveling to Australia and New Zealand.
- Continued to provide cybersecurity awareness programs for schools nationwide.
- Extended cybersecurity awareness and education to rural communities to improve digital resilience at the grassroots level.

1.2 Achievements & milestones

- Senior High School Cybersecurity Bootcamp – CERTVU conducted a successful two-day cybersecurity bootcamp for senior secondary students, aimed at guiding youth toward cybersecurity academic and career pathways at university level.
- Cyber Smart Vanuatu – CERTVU continued delivering Cyber Smart Pacific initiatives across Vanuatu, with key activities aligned to Cybersecurity Awareness Month in October.
- A Successful Digital Week Event – A full week dedicated to collaboration with key stakeholders, delivering

cybersecurity awareness, handling public concerns, and responding to reported incidents.

- Famili i Redi Program – In collaboration with the Department of Labor and World Vision Vanuatu, CERTVU delivered targeted cybersecurity awareness and training to families and citizens participating in the national labor mobility program.

2. About CERTVU

2.1 Introduction

CERTVU, the Vanuatu National Computer Emergency Response Team, serves as the central authority for national cybersecurity. It collaborates closely with government agencies, private sector entities, and civil society organizations to address cybersecurity incidents. CERTVU provides trusted advisory services and remains committed to strengthening Vanuatu's cybersecurity posture through awareness initiatives and capacity-building programs.

2.2 Establishment

CERTVU was established in 2018 within the Department of Communications and Digital Transformation, under the Ministry for the Prime Minister, as the Minister responsible for Information and Telecommunication.

2.3 Resources

CERTVU operates within the Department of Communications and Digital Transformation, supported by three dedicated staff members responsible for national cybersecurity operations, including awareness raising, capacity building, and incident response activities.

2.4 Constituency

CERTVU is the national CERT for Vanuatu and serves the entire country, including government institutions, private sector organizations, NGOs, civil society, and visitors who live in or visit Vanuatu.

3. Activities & Operations

3.1 Scope and definitions

CERTVU is mandated to provide

- Incident response services to Vanuatu's constituents, including government entities, private businesses, and citizens.
- Promotion and delivery of cybersecurity awareness across all sectors.
- Collaboration with regional and international CERT communities.
- Identification of system vulnerabilities.
- Issuance of cybersecurity advisories and alerts.
- Coordination of cyber incident reporting and response handling.
- Continued support for the national cybersecurity collaboration framework.
- Identification and implementation of national capacity-building programs.
- Provision of forensic services to the Vanuatu Police Force.

3.2 Incident handling reports

CERTVU's top five reported cybersecurity incidents highlight persistent threats to Vanuatu's digital landscape:

i. Phishing & Credential Harvesting
ii. Ransomware Attacks
iii. Malware Infections
iv. Email Compromise
v. DDoS Attacks

3.3 Publications

- Publication of a national press release on Vanuatu's signing of the **Budapest Convention on Cybercrime**.
- Publication of press coverage on the **Luganville Cybersecurity Bootcamp**.

3.4 New Initiative

Famili i Redi Initiative

Through our Famili i Redi initiative, we are partnering with the Department of Labor, World Vision Vanuatu, and other key local stakeholders to deliver targeted training for citizens (and their families) participating in labor mobility programs with Australia and New Zealand. Our primary focus is equipping these families to become cyber-savvy across all fronts—

from identifying threats to proactive prevention measures for staying safe online—while emphasizing trusted, accessible tools and platforms for secure communication and more.

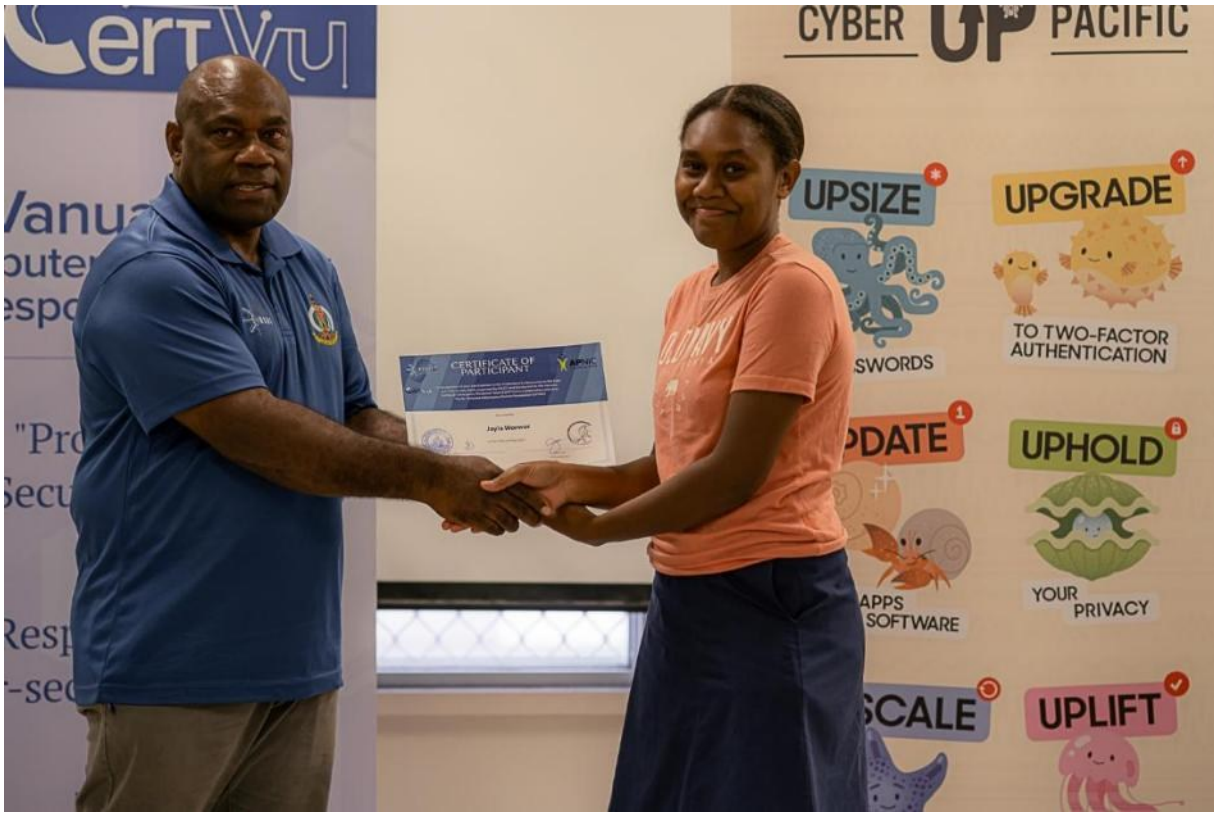
4. Events organized/hosted

4.1 Training

Cyber Security Bootcamp for Senior High Schools

The first cybersecurity bootcamp held in Lusganville successfully brought together over 50 students for an intensive two-day program. Designed to equip participants with essential skills and inspire cybersecurity careers, the event sparked strong interest among local youth.

Lectures session during the cybersecurity bootcamp



Awarding of certificate of participation to those who complete the cybersecurity bootcamp

Train the Trainers

We continued our Train the Trainers initiative by equipping rural community leaders in Emua Village with foundational knowledge to identify various cyber-attacks. On the prevention front, all participating leaders received a cybersecurity pack containing practical guides and instructions on essential steps to help community members stay protected while using the internet.

4.2 Digital Week event

CERTVU joined Santo Island's Digital Week this year alongside key stakeholders to celebrate a series of digital events. Our focus included delivering educational cybersecurity awareness sessions, hosting engaging cybersecurity games with prizes for participants, and offering real-time incident response services to the public throughout the week.

4.3 Youth Partnership Seminar

CERTVU was invited by the National Council of Youth to participate in International Youth Day, delivering a presentation on empowering youth in the cyber and digital space.

4.4 Cybersecurity Awareness Initiatives for Schools

CERTVU has extended its outreach to schools across two provinces of Vanuatu, delivering educational cybersecurity awareness programs under its #CyberUP and #Cybersmart initiatives.

5. International Collaboration

5.1 International partnerships and agreements

- Our continuous collaborations through the PaCSON community Platform continue to provide support to the Pacific community in terms of cybersecurity.
- CERTVU attended the 37th FIRST Annual Conference in the beautiful city of Copenhagen, Denmark.
- CERTVU continues to proactively participate in the Pacific Cyber Week (P4C) initiatives in Nadi from 11th – 14th August 2025.
- CERTVU joins the Pacific SOC, providing Cybersecurity incident response and monitoring during the 54th Pacific Island Forum Leaders Meeting in Honiara, Solomon Islands.

6. Future projects

The CERTVU is committed to continuing to implement the Vanuatu National Cybersecurity Strategy, including the following critical action items:

- The development of the Cyber Security Legislation.
- The development and establishment of the National Cyber Security Agency.
- Cyber Security Capacity Building Roadmap.
- Cyber Defense and Intelligence Framework.

7. Conclusion

CERT Vanuatu, operating under the Government of Vanuatu, conducts essential operations to maintain a secure cyberspace and internet environment for its citizens. This enables safe living, information exchange, business activities, and economic growth. Cybersecurity and CERT functions are vital to Vanuatu's implementation of its National Cyber Security Strategy (NCSS) 2030. Guided by NCSS priorities and its Implementation Matrix, Vanuatu addresses incidents, refines the Cybercrime Act No. 22 of 2021, and collaborates through a Cybersecurity MOU with the Vanuatu Police Force (VPF), Telecommunications & Radiocommunications Regulator (TRBR), Vanuatu Internet Governance Forum (VanIGF), and Vanuatu Bureau of Standards (VBS). In conclusion, Vanuatu prioritizes cyber resilience to protect its cyberspace and sovereignty. Strengthening its cybersecurity stance requires robust frameworks, improved technical capabilities, governance, and legislation—including the Data Protection and Privacy Policy (Act No. 13 of 2024) and the Harmful Digital Communications Policy (Act No. 14 of 2024).

CNCERT/CC

National Computer network Emergency Response technical Team / Coordination Center of China

1. Highlights of 2025

1.1 Summary of major activities

Looking back on 2025, the field of cybersecurity stands as a testament to resilience and innovation in an era of unprecedented digital transformation. Each challenge encountered has illuminated a path for growth, fostering an environment where vigilance and exploration merge to navigate the complexities of an ever-evolving threat landscape.

Amid emergence of new AI models and other new cyber trends, we continue to play our role in APCERT and the wider community underpinned by a host of events. The National Computer Network Emergency Response Technical Team/Coordination Center of China (known as CNCERT/CC) successfully hosted several international and domestic conferences, such as the Cybersecurity Forum for Technology Development and International Cooperation in 2025 World Internet Conference Wuzhen Summit, the 22nd CNCERT Annual Conference and the Cyber Security Collaborative Governance Sub-Forum of China Cybersecurity Week, China-ASEAN Network Security Emergency Response Capacity Building Seminar and China-Cambodia Online Cybersecurity Training. These conferences are increasingly well-received and supported by the international community. We also make active presence in cybersecurity drills, such as APCERT Drill 2025 and ASEAN CERT Incident Drill 2025. Our engagement in international and regional stage facilitated collaboration in information sharing, cross-border incident handling, technical training, capacity building and other vital areas. Overall, it was a year of concrete outcomes and sustained endeavor.

1.2 Achievements & milestones

The 2025 AI Large Model Product Vulnerability Crowd-sourcing Testing

On 8th July, 2025, the 2025 Vulnerability Crowd-sourcing Testing for Artificial Intelligence Large Model Products organized by CNCERT/CC was officially launched. The testing targeted at the mainstream foundational large model products and large model-related applications currently available on the market. A total of 559 white-hat security hackers were mobilized for the crowd-sourcing testing, during which vulnerability assessments were conducted on 15 large

models and applications from 10 domestic AI vendors. The testing identified 281 security vulnerabilities, including 177 unique vulnerabilities specific to large models and 104 traditional vulnerabilities. The testing has mapped out the current vulnerability landscape of mainstream domestic AI systems and effectively enhanced the cybersecurity for AI large model products. The results of the crowd-sourcing testing were released at the 22nd CNCERT Annual Conference and the Cyber Security Collaborative Governance Sub-Forum of China Cybersecurity Week. The release drew considerable interest from the industry and the media.

2. About CNCERT/CC

2.1 Introduction

CNCERT/CC is a non-government, non-profit cybersecurity technical center and the key coordination team for China's cybersecurity emergency response community.

2.2 Establishment

CNCERT/CC was founded in August 2001. It is a full member of FIRST and one of the founders of APCERT. As of 2025, CNCERT/CC has established "CNCERT/CC International Cooperation Partnership" with 294 teams in 87 countries and regions.

2.3 Constituency

As a national CERT, CNCERT/CC strives to secure the nation's public cybersecurity and safeguard the security of critical information infrastructure. CNCERT/CC leads efforts to prevent, detect, alert, coordinate and handle cybersecurity threats and incidents, in accordance with the guiding principle of "proactive prevention, timely detection, prompt response and maximized recovery".

3. Activities & Operations

3.1 Services

CNCERT/CC works to build China's cybersecurity emergency response ecosystem by coordinating with key network operators, domain name registrars, cybersecurity vendors, academia, civil society, research institutes and other CERTs to jointly handle major cybersecurity incidents. To further strengthen sector-wide synergy, CNCERT/CC initiated and established of Anti Network-Virus Alliance of China (ANVA) and China Cyber Threat Governance Alliance (CCTGA).

CNCERT/CC also operates the China National Vulnerability Database (CNVD).

CNCERT/CC actively carries out international cooperation in cybersecurity and is committed to establishing the mechanism of prompt response to and coordinative handling of cross-border cybersecurity incidents. CNCERT/CC is a full member of the Forum of Incident Response and Security Teams (FIRST) and one of the founders of the Asia Pacific Computer Emergency Response Team (APCERT). CNCERT/CC has also actively engaged in activities of APEC, ITU, SCO, ASEAN, BRICS and other international and regional organizations.

3.2 Incident handling reports

Persistent US Cyber Espionage Against China's Defense Sector

CNCERT/CC has observed and identified that in recent years, US intelligence agencies have targeted entities within China's high-tech and military-industrial sectors including universities, research institutes and enterprises—as prime objectives for cyber attacks and espionage. They targeted sensitive information—from military research data to core production secrets—at every stage, from design and development to manufacturing. Their operations are now more precisely targeted and their tactics more covert, posing a severe threat both to the research and production in China's defense and industrial security, and to the national security at large. Since the 2022 exposure of the US National Security Agency's (NSA) cyber attack on Northwestern Poly Technical University, US intelligence agencies have repeatedly and brazenly targeted China's defense and industrial sectors with cyber espionage.

A detailed report on this has been published by CNCERT/CC on 1st August, 2025.

3.3 Publications

In 2025, CNCERT/CC' s weekly reports and related advisories gained significant recognition, being widely cited by authoritative media and academic papers both in China and abroad.

Table 1: Lists of CNCERT/CC' s publications throughout 2025

Title	No. of Issues	Description
CNCERT Weekly Reports (Chinese)	52	Emailed to relevant organizations and individuals and published on CNCERT/CC's Chinese website (https://www.cert.org.cn/)
CNCERT Weekly Reports (English)	52	Emailed to relevant organizations and individuals and published on CNCERT/CC's English website (https://www.cert.org.cn/publish/english/115/index.html)
CNVD Vulnerability Weekly Reports (Chinese)	51	Published on CNCERT/CC's Chinese website (https://www.cert.org.cn/)

4. Events organized / hosted

4.1 The 2025 World Internet Conference Wuzhen Summit: Cybersecurity Forum for Technology Development and International Cooperation

Hosted by CNCERT/CC, the Cybersecurity Forum for Technology Development and International Cooperation of the 2025 World Internet Conference Wuzhen Summit was held in Wuzhen Zhejiang on 8th November. With the theme of "Strengthening Threat Information Sharing and Fostering Collaborative Incident Response", the Forum conducted in-depth discussions on the latest global trends in the field of cybersecurity, exchanged insights on recent threat information sharing, and jointly explored ways to enhance cybersecurity in the digital age.

CNCERT/CC also shared its insights on cybersecurity emergency response and global collaboration based on its practical experience and the latest outcomes released in international conferences. It introduced four recently released outcomes in detail: the Artificial Intelligence Security Governance Framework 2.0, the test results of 2025 AI-enabled cybersecurity application scenarios, the 2025 Vulnerability Crowd-sourcing Testing for AI Large Model Products, and the 12387 Cybersecurity Incident Reporting Platform. It also proposed to enhance international cooperation to jointly address the challenges as cyber landscape evolves, improve mechanisms for sharing cybersecurity information, strengthen global synergy in emergency response, and work to build a community with a shared future in cyberspace.
The forum was organized by CNCERT/CC and the Zhongguancun Laboratory (ZGC LAB). Over 100 representatives from governments, international organizations, research institutions, industry associations, and enterprises attended it.

4.2 The 22nd CNCERT Annual Conference and the Cyber Security Collaborative Defense Sub-Forum of China Cybersecurity Week in Kunming

On 16th September, the 22nd CNCERT Annual Conference and the Cyber Security Collaborative Governance Sub-Forum of as part of the National Cybersecurity Week were successfully held in Kunming, China. With the theme of "Collaborative Emergency Response, Jointly Defending Against Risks and Challenges", the Conference was hosted by CNCERT/CC. Since its launch in 2004, the Conference has been successfully held for 21 consecutive years, serving as a key platform for dialogue and collaboration among national and local authorities, critical information infrastructure operators, the cybersecurity industry, and the academia. It has consistently contributed to strengthening China's cybersecurity

resilience and bolstering the national cyber defense capabilities.

4.3 China-ASEAN Network Security Emergency Response Capacity Building Seminar

On 15th April, 2025, the China-ASEAN Network Security Incident Response Capability Building Seminar, hosted by CNCERT/CC, was successfully held in Hong Kong, China. Representatives from over 10 domestic and international organizations attended the seminar. Officials from CNCERT/CC also participated in the event and delivered a speech.

The Cybersecurity Bureau of Indonesia's Ministry of Communication and Digital Affairs and Malaysia's National Cyber Security's Agency, representing ASEAN, delivering remarks on their national strategic policies, governance frameworks, and integrated applications, centered on artificial intelligence and cybersecurity. Following this, representatives engaged in in-depth discussions on topics such as cybersecurity AI-powered cybersecurity capabilities, information sharing regarding website security of critical sectors and data breaches, and collaborative analysis and management of cross-border incidents.

4.4 China-Cambodia Online Cybersecurity Training

From 13rd to 14th October 2025, CNCERT/CC successfully conducted an online cybersecurity training with the Cambodia Computer Emergency Response Team (CamCERT). The training was carried out under the "Proposal on China-ASEAN Cybersecurity Onsite Training" and serves as a concrete measure to advance the development of the China-ASWAN Information Port. Nearly 100 local partner members invited by CamCERT participated in the training. The training focused on cybersecurity frameworks and emergency mechanisms, with technical discussions covering threat information sharing, incident response and remediation, and AI's role in cybersecurity. This program aims to strengthen mutual understanding and build trust between China and Cambodia, supporting deeper collaboration in regional cyber resilience efforts.

5. International Collaboration

5.1 International partnerships and agreements

5.1.1 APCERT Cyber Drill 2025

On 29th July, 2025, CNCERT/CC participated in the 2025 Asia-Pacific Cybersecurity Incident Drill initiated and organized by APCERT and successfully completed all drill tasks. The theme of this year's APCERT Drill is "When Ransomware Meets Generative AI." This exercise reflects emerging real-world cybersecurity threats posed by the malicious use of Generative

AI, an evolving technology that is increasingly being misused by cyber threat actors. Participating teams reviewed and tested their incident response procedures through simulated scenarios involving malicious code unintentionally generated by Generative AI, exploitation of open-source vulnerabilities, and so on. 24 CSIRTs from 18 economies of APCERT participated in the drill. From the external parties, 3 CSIRTs from 2 economies of OIC-CERT and AfricaCERT participated.

5.1.2 ASEAN CERT Incident Drill (ACID) 2025

On 21st and 22nd October, 2025, CNCERT/CC, as the Dialogue Partner, participated in the ASEAN CERT Incident Drill (ACID) 2025. Themed "Securing Network Devices at the Edge", this year's ACID focused on cyber incidents affecting network edge devices, such as VPN appliances and secure remote access gateways, which often act as a first line of defense. As organizations increasingly relied on network edge devices, the drill enabled participants to learn practical techniques to secure these devices. The participants conducted investigations, analysis, and reporting of cyber incidents, and formulated corresponding remediation and mitigation measures. By testing incident response protocols, ACID reinforced cybersecurity preparedness and cooperation among CERTs in ASEAN member states and dialogue partners.

6. Future Plans

i. Identify the new needs of members of the Information Sharing Working Group, organize teleconferences to facilitate communication among members, encourage them to share information within APCERT, and enrich the sources and content of APCERT data sharing
ii. Plan to host Cybersecurity Forum for Technology Development and International Cooperation in 2026 World Internet Conference Wuzhen Summit
iii. Plan to host China-ASEAN Network Security Emergency Response Capacity Building Seminar

7. Conclusion

As 2025 comes to a close, a review of CNCERT/CC's work highlights its active efforts to enhance cybersecurity resilience and expand cooperation domestically and internationally. While significant progress has been made, the evolving cyber threat landscape demands greater adaptability and innovation. Guided by the shared vision of the APCERT community, we are committed to working with global partners to build a safer, cleaner, and more reliable cyberspace across the Asia Pacific region.

Looking ahead, CNCERT/CC will build on its role within the APCERT community—both as a Steering Committee member and as the convener of the Information Sharing Working Group, to address emerging challenges. We remain dedicated to working alongside all APCERT partners to advance our shared goal: a more secure and resilient cyberspace.

CyberSecurity Malaysia

CyberSecurity Malaysia

1. Highlights of 2025

1.1 Summary of major activities

20 - 24 Jan 2025	Co-organised with UK High Commission and BAE UK on IPCP Training: i. UK – CyberSecurity Malaysia Cyber Cooperation - Review and Further Develop Knowledge and Skills Development (20-22 Jan 2025, 22 participants) ii. Digital Trust Managers (23 & 24 January 2025, 21 participants)
5 Mar 2025	Organised the Webinar through the OIC-CERT Platform "Quantum Computing Threats to the Digital World"
10 Mar 2025	Participated in the APCERT Steering Committee Face to Face meeting, Seoul, South Korea
28 – 30 Apr 2025	Participated in the OIC-CERT Face to Face meeting and the "Future of Digital Countries (FDC) Summit 2025", Cairo, Egypt
8 May 2025	Co-organised sectoral-level Cyber Drill Exercise for Malaysia Capital Markets, participated by 119 organisations, in close partnership with Malaysia Securities Commission (SC) and National Cyber Security Agency of Malaysia (NACSA)
20 – 23 May 2025	Participated in Cyber Games Kuala Lumpur 2025 and scored 4th place (individual) by CyberSEE, CyberEast+, CyberSouth+, GLACY-e and Octopus Projects, in close partnership with INTERPOL and National Cyber Security Agency of Malaysia (NACSA)
26 May 2025	Participated in International Cybersecurity Championship 2025 by Solar RU Group In Cooperation With The Ministry of Digital Development, Communications And Mass Media of The Russian Federation
18 Jun 2025	Organised the ASEAN Webinar "Building Trust in Southeast Asia's Digital Future" in cooperation with Cyber Security Brunei, National Cyber and Crypto Polytechnic Indonesia and Cyber Security Agency of Singapore (online)
18 – 20 June 2025	Two teams participated in Standoff Cyberbattle for SPIEF 2025 by Positive Technologies – First team defending Aviation and Logistics Sector scored 4th place from 12 teams (12

	countries), and another team defending Oil & Gas Sector scored 6th place from 13 teams (12 countries)
27 Jul – 10 Aug	Participated in Positive Hack Camp by Positive Technologies, and scored 1st in the final leaderboard and awarded with CyberED Certified Offensive Security Explorer and White Hacker certifications
29 Jul 2025	Exercise Controller (EXCON) for the APCERT Cyber Drill "When Ransomware Meets Generative AI" (online)
19 – 27 Aug 2025	Organised capacity building training under the Malaysian Technical Cooperation Program (MTCP), attended by selected APCERT members, titled "Digital Security & Lifelong Learning Programme" (**DLSP**)
15 – 19 Sep 2025	Participated in the OIC-CERT Board Meeting and 17th OIC-CERT Annual Conference in conjunction with the Arab Regional Cybersecurity Summit and FIRST & ITU-ARCC Regional Symposium 2025, Rabat, Morocco
30 Sep – 2 Oct 2025	Organised the Cyber Digital Services, Defence and Security Asia (**CyberDSA**) 2025
1 Oct 2025	Co-Organised ASEAN Programme during CyberDSA "Quantum Safe Migration: Securing ASEAN's Digital Future."
6 – 8 Oct 2025	Participated in Standoff 16 Cyberbattle as Red Team by Positive Technologies
13 – 16 Oct 2025	Co-organised with UK High Commission and BAE UK on IPCP Training - Threat Hunting Training
27 – 31 Oct 2025	Co-organised with UK High Commission and TAG International Team on IPCP Training - Cyber Security Standards and Governance, Risk & Compliance
6 Nov 2025	Participated in AfricaCERT Drill
25 - 27 Nov 2025	Participated in the APCERT Annual General Meeting and Conference 2025, Sydney, Australia Co organised as Exercise Controller (**EXCON**) for APCERT Tabletop Exercise (TTX) themed "Responding to Ransomware Using Generative AI"
28 Nov – 1 Dec 2025	Trainer for Artefacts Development Essential for Red Team Operators at Malaysia Cybersecurity Camp 2025

Table 1. Summary of major activities

2. About CSIRT

2.1 Introduction

CyberSecurity Malaysia is the national cybersecurity specialist agency under the purview of the Ministry of Digital Malaysia, having the vision of being a globally recognised National Cyber Security and Specialist Centre. The services provided can be categorised as follows

i. Cybersecurity Responsive Services
- Digital Forensics
- Security Operation Centre (SOC)
- Security Incident Handling

ii. Cybersecurity Pre-emptive Services
- Digital Trust
- AI
- Cyber Risk Intelligence
- Red Team
- Digital Information Analysis

iii. Cybersecurity Proactive Services
- Security Assurance
- Information Security Certification Body

iv. Capacity Building and Outreach
- Info Security Professional Development
- Outreach

v. Strategic Studies and Engagement
- Government and International Engagement
- Strategic Research

vi. Industry and Research Development

2.2 Establishment

CyberSecurity Malaysia started with the formation of the Malaysian Computer Emergency Response Team (**MyCERT**) on 13 Jan 1997 under the Ministry of Science, Technology, and Innovation Malaysia. In 2023, with the restructuring of the government administration, CyberSecurity Malaysia was put under the purview of the Ministry of Digital Malaysia. CyberSecurity Malaysia is committed to providing a broad range of cybersecurity innovation-led services, programmes, and initiatives to help reduce the vulnerability of digital systems and, at the same time, strengthen Malaysia's self-reliance in cyberspace.

2.3 Resources

2.3.1 Cyber Security Incident Response

CyberSecurity Malaysia responds to and handles cyber security incidents through Malaysia Computer Emergency Response Team (**MyCERT**), Digital Forensics (**DF**), and Cyber999 Cyber Incident Response Centre (**Cyber999**). MyCERT and DF departments are the technical reference point for Malaysian organisations facing cybersecurity incidents through on-site services. Cyber999 is a technical reference point for Malaysian Internet users facing cybersecurity incidents

through online services. MyCERT, DF, and Cyber999 facilitate the handling and mitigation of cybersecurity incidents for organisations and Malaysian digital users and organisations.

The types of incidents received and responded to are intrusion, fraud, malicious codes, vulnerability reports, intrusion attempts, spam, denial of service (**DOS**) and data breaches. CyberSecurity Malaysia receives incident reports from various parties in the constituency, such as the general public, the private sector, and SMEs. Additionally, we receive information about incidents involving Malaysian IPs or domains from trusted security teams from abroad (foreign CERTs) and Special Interest Groups such as Shadowserver Foundation and through CyberSecurity Malaysia proactive monitoring. Works closely with ISPs, CERTs, Special Interest Groups (**SIGs**) and Law Enforcement Agencies (**LEAs**), from local and international, to remediate and mitigate computer security incidents affecting Malaysia's organisations and the public.

CyberSecurity Malaysia allows Internet users, organisations, and SMEs in Malaysia to report cybersecurity incidents that threaten Internet users' or organisations' security, safety, and privacy. A list of channels for reporting cybersecurity incidents to Cyber999 Cyber Incident Response Centre and for getting technical assistance is available at: https://www.mycert.org.my/portal/

CyberSecurity Malaysia responded to 7,616 incidents in 2025, with most reported incidents being fraud, data breach, malicious code, and intrusion.

2.4 Constituency

MyCERT and DF constituencies are Malaysian organisations and government agencies that may voluntarily request service related to cybersecurity incidents.

Cyber999 constituencies are non-NCII sectors that include SMEs, businesses and Malaysian Internet users. Cyber security incidents reported to the Cyber999 Cyber Incident Response Centre will be handled and resolved according to the Standard Operating Procedure and Service Level Agreement, together with technical assistance and guidance.

3. Activities & Operations

3.1 Scope and Definitions

3.1.1 Monthly Cyber Incidents Statistics

Cyber999 proactively produced 200 advisories and 3 alerts in 2025 to inform and warn the constituency about recent cyber threats. The security advisories, alerts, and summary reports produced by Cyber999 Cyber Incident Response Centre can be viewed at https://www.mycert.org.my/portal/advisories2025

Figure 1 shows the reported incidents handled by Cyber999 Cyber Incident Response Centre of CyberSecurity Malaysia.

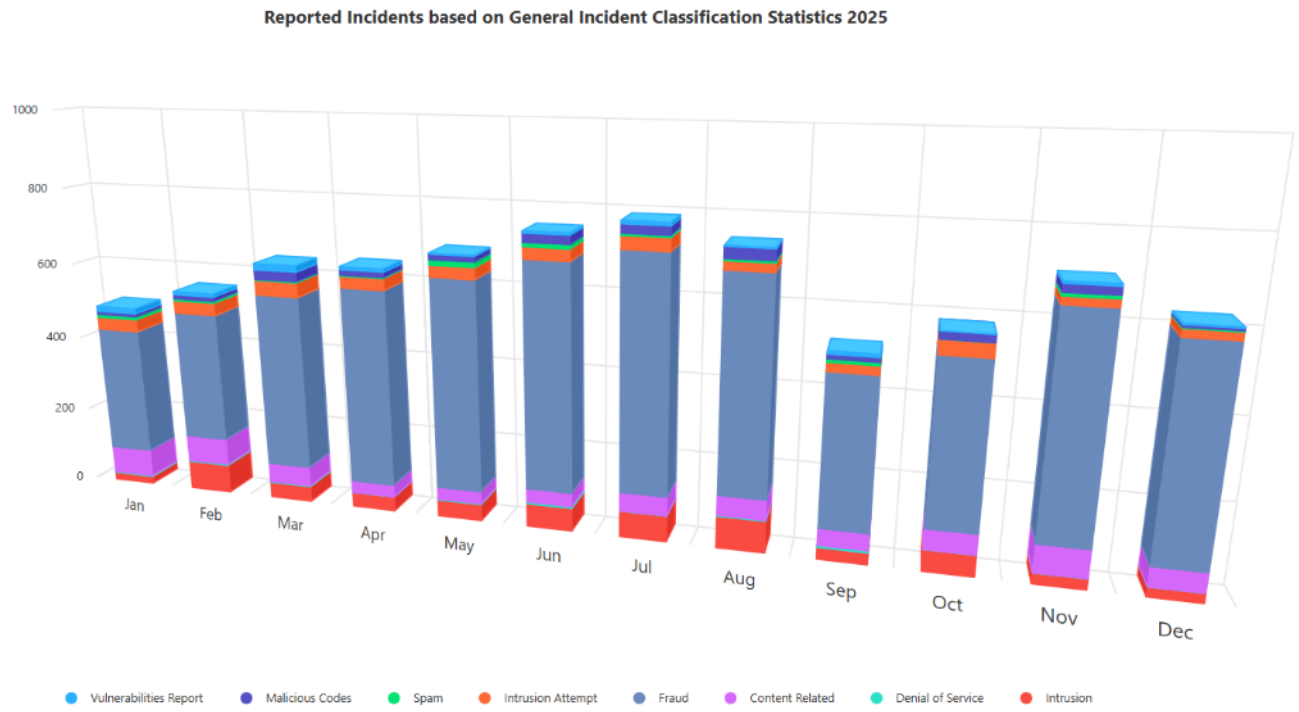


Figure 1: Incidents Reported to Cyber999 of CyberSecurity Malaysia in 2025

The monthly cyber incident statistics can be viewed at: https://www.mycert.org.my/portal/

3.1.2 Security Alert and Advisory

In addition to assisting in technical support for incident handling, Cyber999 also produces security alerts and advisories on the latest cyber threats targeting Malaysia, with reference to patches for software vulnerabilities.

Alerts are urgent notifications about active security threats, vulnerabilities, or ongoing cyberattacks that typically are issued when immediate action is required to mitigate a threat. Cyber999 will provide specific details about the threat issues, affected systems and recommended actions for users to mitigate the threat. While in advisories, Cyber999 will provide information about potential security risks, vulnerabilities, or best practices. Advisories are less urgent than alerts but are still important for long-term security planning for mitigation strategies, patches, and general security recommendations.

A list of Security Alert and Advisory published can be referred to here: https://www.mycert.org.my/portal/advisories

3.1.3 Cyber Incident Quarterly Summary

The Cyber Incident Quarterly Summary Report 2025 provides an overview of computer security incidents handled by the Cyber999 Incident Response Centre of CyberSecurity Malaysia quarterly. Cyber Incident Report also highlights statistics of incidents dealt with by the Cyber999 Incident Response Centre in each quarter of 2025 according to their categories,

security alerts and advisories released, and current security threats and trends. It should be noted that the statistics provided in this report reflect only the total number of incidents reported and handled by the Cyber999 Incident Response Centre, excluding elements such as monetary value or aftermaths of the incidents. Computer security incidents dealt with by the Cyber999 Incident Response Centre involved IP addresses and domains from Malaysia.

3.2 CyberSOC (Security Operation Centre)

CyberSOC, managed by the MyCERT, is a centralised facility that integrates various cybersecurity functions and capabilities to enhance an organisation's ability to protect, detect, analyse, and respond to cyber threats more proactively and effectively. It helps to strengthen cybersecurity infrastructure, promote resilience, and protect against both internal and external cyber threats.

This facility managed 3 core services as follows:

- Manage, Detect and Respond (**MDR**)
- Compromised Network Assessment (**CMERP**)
- Compromised Endpoint Assessment (**EDR/XDR**)

3.3 The LebahNET Project

LebahNET, managed by MyCERT is a Honeypot Distributed System where a collection of honeypots is used to study the exploits that function as well as to collect malware binaries. Honeypots are computer software mechanisms set up to mimic a legitimate site to ensnare malicious software into believing that it is a legitimate site which is in a weak position for attacks. Honeypot allows researchers to detect, monitor, and counter malicious activities by understanding the activities done during the intrusion phase and attacks' payload. It can be viewed at https://dashboard.honeynet.org.my/

3.4 Mobile Assessment Security Scanning Application (MASSA)

MASSA or Mobile Assessment Security Scanning Application is a security tool developed and managed by MyCERT that provides partially automated security scanning for analysts and end-users. This application provides comprehensive information according to the scanning result, enabling analysts to detect any risk or misconfigured security control in an Android smartphone. It identifies any possible entry point for malicious activity, indicator of compromise or possible malicious applications installed on the device. Figure 2 below shows the total devices and applications scanned using MASSA in 2025.

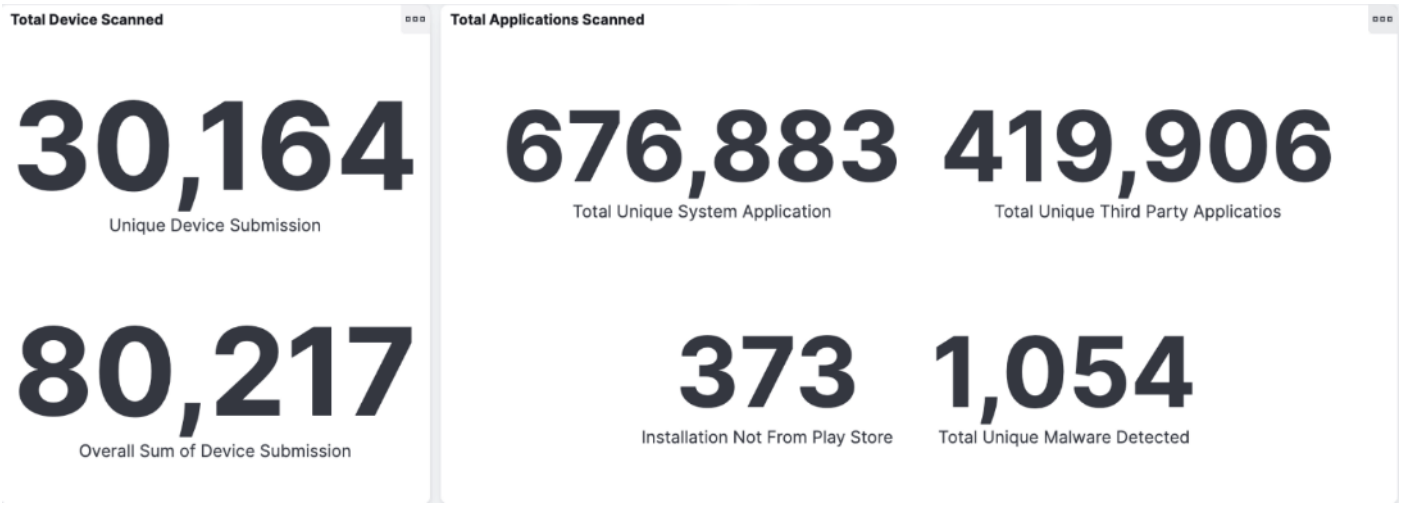


Figure 2: Total Scanned Using MASSA in 2025

3.5 Compromise Assessment

MyCERT provides compromise assessment services to help organizations determine whether their systems or networks have been breached. This process involves examining hosts, network traffic, and security logs to identify indicators of compromise, malicious artifacts, and unauthorized activities. By leveraging threat intelligence and forensic analysis techniques, the team can detect potential intrusions and determine their scope and impact, enabling organizations to take timely containment and remediation actions.

3.6 Root Cause Analysis

Following a confirmed security incident, Cyber999, MyCERT and DF conduct root cause analysis to identify how the compromise occurred and which vulnerabilities or weaknesses were exploited. By reconstructing the attack timeline and analyzing relevant evidence, the team determines the underlying causes of the incident. The findings support organizations in addressing security gaps, strengthening their defenses, and reducing the risk of similar incidents in the future.

3.7 Red Teaming Exercises

CyberSecurity Malaysia also manages and conducts comprehensive red teaming exercises to assess and strengthen security posture of companies and organizations. Through structured adversarial simulations, the team emulates real-world threat actors to identify vulnerabilities across people, processes, and technology. These exercises encompass planning, reconnaissance, exploitation, lateral movement, and reporting, ensuring a realistic evaluation of detection and response capabilities. By delivering detailed findings and actionable recommendations, CyberSecurity Malaysia enables continuous improvement, enhance resilience against evolving cyber threats, and support informed risk management at

both operational and strategic levels.

3.8 CyberSecurity Malaysia – National AI Office (NAIO) Working Group

CyberSecurity Malaysia actively participates in the National AI Office (NAIO) working group, which aims to develop and implement national action plans to advance the responsible and strategic adoption of artificial intelligence. Through this collaboration, CyberSecurity Malaysia contributes expertise across several key areas, including AI security, AI advisory, AI sovereignty, AI regulation and policy, AI talent development, AI governance and ethics, and AI safety. CyberSecurity Malaysia involvement supports the development of a secure, trustworthy, and sustainable AI ecosystem while ensuring that cybersecurity considerations are integrated into national AI initiatives.

4. Events organized/hosted

4.1 Training

4.1.1 Malaysian Technical Cooperation Programme (MTCP)

Hands-on training program, titled the Digital Security Lifelong Learning Program (DSLP) under the Malaysian Technical Cooperation Programme (MTCP), was conducted by CyberSecurity Malaysia from 19 – 27 Aug 2025. A total of 13 participants form Commonwealth countries attended the program, representing Bangladesh, Eswatini, Fiji, Gambia, Ghana, Kenya, Lesotho, Malawi, Maldives, Mauritius, Nigeria, Sierra Leone and Sri Lanka.

4.1.2 Indo-Pacific Cyber Programme

CyberSecurity Malaysia together with the British High Commission in Kuala Lumpur and a consortium led by BAE Digital Intelligence (DI) on behalf of the UK Foreign Commonwealth and Development Office (FDCO) had co-organised several capacity-building initiatives under the Indo-Pacific Cyber Programme (IPCP).

These training programmes included:

- UK–CyberSecurity Malaysia Cyber Cooperation training on reviewing and enhancing knowledge and skills development, held from 20 – 22 January 2025 with 22 participants,
- Digital Trust Managers Programme on 23 – 24 January 2025 involving 21 participants.
- Threat Hunting Training from 13 – 16 October 2025 with 11 participants
- Cyber Security Standards and Governance, Risk & Compliance training delivered from 27 – 31 October 2025 with 23 participants.

4.2 Drills & exercises

Organised the Capital Market Cyber Simulation (**CMCS**), a cyber-attack and defence simulation project under the Securities Commission and Cyber Security Malaysia through MyCERT department. CMCS started in 2018 with only 38 participants and has grown rapidly over the years; today, it has 120 participants. For CMCS 2025, the project focuses on simulating real incident scenarios that cover technical assessments and policy adherence through cyber drill platform. This approach ensures seamless accessibility for all participants and enhances their readiness to handle real-world cyber-attack simulations. Additionally, organised cyber drills and Tabletop Exercises (**TTX**) for the financial sector, supporting the planning, coordination, and execution of cyber incident response simulations to strengthen organisational preparedness and resilience. Also served as Exercise Control (**EXCON**) for the APCERT Cyber Drill and APCERT Tabletop Exercise (**TTX**) 2025, contributing to the coordination and execution of regional cyber incident response exercises aimed at enhancing collaboration, information sharing, and collective cyber resilience among APCERT member teams.

4.3 Conferences and seminars

Cyber Digital Services, Defence and Security Asia (**CyberDSA**) is a prestigious annual cybersecurity event held in Kuala Lumpur, Malaysia. The 2025 edition took place from 30 Sep – 2 Oct 2025 at the Malaysian International Trade and Exhibition Centre (**MITEC**), under the theme "Pioneering the Future: Building a Resilient and Trusted Digital Nation." Organised by CyberSecurity Malaysia, the event is supported by a diverse range of partners from both the public and private sectors, including government agencies, industry leaders, and cybersecurity professionals.

In conjunction with Malaysia's ASEAN Chairmanship in 2025, CyberSecurity Malaysia also identified several ASEAN-related initiatives and events to be implemented throughout the year, further strengthening regional cooperation in cybersecurity and digital resilience.

5. International Collaboration

5.1 International partnerships and agreements

The Malaysia Cybersecurity Strategy 2025 identified international cooperation as one of the areas in enhancing cybersecurity. In line with this, CyberSecurity Malaysia is actively establishing collaborative relationships with foreign parties.

5.1.1 Working Visits

CyberSecurity Malaysia conducted working visits to relevant organisations overseas to further enhance the country's cybersecurity posture. The objective of the visits is to seek potential collaborations in cybersecurity. This agency also received working visits from foreign organisations that have similar objectives. Among them are:

i. National Communications Authority (**NCA**) of Somalia
ii. Brunei Cybersecurity Association (**BCSA**)
iii. The Russian Trade Mission
iv. Blackfire, Philippines
v. Representatives of the Third Country Training Programme (**TCTP**) 2025
vi. The Government of Bangladesh (Cabinet Division & Finance Division) and Universiti Putra Malaysia
vii. Cyber Security Brunei
viii. Universiti Teknologi Mara & Standing Committee on Scientific and Technological Cooperation (**COMSTECH**)
ix. SUE "Cybersecurity centre" ("**UZCERT**"), Uzbekistan

5.1.2 International Roles

Amongst the international roles and contributions by CyberSecurity Malaysia

i. Asia Pacific Computer Emergency Response Team (**APCERT**) Steering Committee Member
ii. Member of APCERT Coordinated Vulnerability Disclosure Working Group (**CVD WG**)
iii. Member of APCERT Policy, Procedures and Governance Working Group (**PPGWG**)
iv. Member of the Forum of Incident Response and Security Teams (**FIRST**)
v. Member of the National CSIRT Committee
vi. The Permanent Secretariat of the Organisation of Islamic Cooperation – Computer Emergency Response Team (**OIC-CERT**), where a major role is to undertake daily operations and facilitate cooperation and interaction among the member countries
vii. The lead for the Capacity Building Initiatives in the OIC-CERT
viii. Certificate authorising a member of the Common Criteria Recognition Arrangement (**CCRA**)
ix. Member of the ShadowServer Foundation
x. Member of the ASEAN Forensic Science Network
xi. Member of the Digital Forensics Working Group

xii. Member of the Traffic Accident Reconstruction Working Group
xiii. Member of the INTERPOL Regional Expert Group for Cryptocurrency Investigation (**REG-CI**)
xiv. Member of the United Nations Office on Drugs and Crime (**UNODC**) Women in Cyber
xv. Member of the Cybersecurity Alliance for Mutual Progress (**CAMP**)
xvi. Member of the Women of FIRST SIG
xvii. Member of OWASP Foundation

5.2 Capacity building

5.2.1 Cyber Drills & Exercises

CyberSecurity Malaysia participated in three (3) international cyber drills in 2025, namely the APCERT Cyber Drill, the OIC-CERT Cyber Drill, and the AfricaCERT Drill.

5.2.2 Seminars & presentations

CyberSecurity Malaysia's representatives had been invited to give presentations and talks at international conferences and seminars as follows:

i. 26 Nov 2025 – Speaker entitled "Helping Analysts Overcome Alert Fatigue Using AI Agent" at the APCERT Annual General Meeting and Conference 2025, Sydney, Australia
ii. 28 – 29 Oct 2025 - As a speaker at the conference entitled "AI for Next-Gen Cyber Threat Detection" at the 46th Edition of The World AI Show
iii. 8 – 9 Oct 2025 - As a speaker at the conference entitled "Securing the Cyber Supply Chain in an Increasingly Connected World" at Cyber Security World Asia (in conjunction with Tech Week Singapore)
iv. 1 Oct 2025 – Speaker entitled "PC Gaming Ubuntu" at Ubuntu Malaysia MiniCon 2025 at CyberDSA, MITEC, Kuala Lumpur
v. 30 Sept 2025 – Speaker and demonstration entitled "Mobile Adversary and Safety Awareness" at CyberDSA, MITEC, Kuala Lumpur
vi. 23 – 24 Sept 2025 - As a speaker at the conference entitled "Challenges of Cybersecurity in Malaysia" at Digital Nation Summit, Kuala Lumpur, ASEAN Edition
vii. 16 -17 September 2025 - As a speaker at the conference entitled "Validating a Set of Candidate Criteria for Evaluating Software Tools and Data Sources for National CSIRTs' Cyber Incident Responses" at the 14th International Conference on IT Security Incident Management and IT Forensics
viii. 21 Aug 2025 – Speaker for Malaysian Ministry of Digital: Digital Talk Series 5: Cybersecurity Trends: May The Resilience Be With You
ix. 21 Aug 2025 – Speaker for ISC2 Malaysia Chapter "Navigating Cybersecurity Certifications For Career Growth"
x. 20 – 21 Aug 2025 - As a speaker at the conference entitled "Digital landscape: Preparing for the next frontier in cybersecurity" at Cybersecurity, IT Assurance, and Governance (**CIAG**) Conference 2025
xi. 12 – 13 Aug 2025 - As a speaker at the conference entitled "AI-Powered CyberSecurity: Defending Organisations in the Age of Intelligent Threats" at ASEAN AI Summit 2025

xii. 5 – 6 Aug 2025 - As a speaker at the conference entitled "Digital Transformation & Cyber Resilience" at IERP® Global Conference 2025

xiii. 6 Aug 2025 - As a speaker at the conference entitled "Cloud, AI, and Cybersecurity Convergence – Building Resilient Digital Infrastructure" at CloudTech & DataCentre Conference 2.0

xiv. 24 Jul 2025 - As a speaker at the conference entitled "Emerging Threats in the Cyber Landscape: What Malaysian Organisations Need to Know" at Cybersecurity Summit 2025

xv. 21 – 22 Jul 2025 - As a speaker at the conference entitled "Cybersecurity's Role in Crisis Management: Supporting Resilience and Sustainability During Digital Disruptions" at DRI ASEAN 2025 Conference & Award of Excellence 2025

xvi. 15 – 17 Jul 2025 - As a speaker at the conference entitled "Cybersecurity Begins At Home" at ASEAN 5G & OT Security Summit

xvii. 9 – 10 Jul 2025 - As a speaker at the conference entitled "Securing Malaysia's Digital Future: Unifying Efforts in the Age of AI and Emerging Threats" at the 49th Edition of AIBP Conference & Exhibition 2025

xviii. 1 Jul 2025 - As a speaker at the conference entitled "Cyber security in Aviation: Strengthening Airspace Resilience Through Experience and Collaboration" at Cyber Defence & Security Exhibition and Conference (**CYDES**)

xix. 1 Jul 2025 - As a speaker at the conference entitled "Migration to Quantum-Safe Cryptography: Challenges and Roadmap for Malaysia" at Cyber Defence & Security Exhibition and Conference (**CYDES**)

xx. 14 -15 May 2025 - As a speaker at the conference entitled "Securing Malaysia's Critical Information Infrastructure: Safeguarding Against Cyberattacks and Data Breaches" at Datacentre & Cloud Infrastructure Summit (**DCCI**) 2025

xxi. 14 – 16 Jan 2025 – As a speaker at the conference entitled "Threat Analysis on Emerging Data Breach in Malaysia with Causes, Challenges, Preventions, and Moving Forward: at TF-CSIRT Meeting & FIRST Regional Symposium for Europe, Monte Carlo, Monaco

5.3 Other international activities

5.3.1 Research Papers

CyberSecurity Malaysia actively contribute research papers to journals and conference proceedings. The following are some of the papers published.

i. A Novel DNA Technique to Strengthen Cryptographic Permutation Tables in Encryption Algorithm - IEEE Access Research Article

ii. Validating a Set of Candidate Criteria for Evaluating Software Tools and Data Sources for National CSIRTs' Cyber Incident Responses - Association for Computing Machinery (ACM)

iii. Conceptual-based Procedure on Data Privacy for Dark Web Data with Standard and Ethical Perspectives – Springer

iv. Enhancement of Privacy Preserving Algorithm Based on K-Anonymization and Homomorphic Encryption on Dark Web Data – Springer

v. A Case Study on Data Privacy Implementation in Higher Education Application Systems in Malaysia - OIC-CERT

vi. A Systematic Literature Review on Continuous Authentication in Zero Trust Architecture for Business - IADITI - International Association for Digital Transformation and Technological Innovation
vii. Investigation And Prosecution Challenges in Financial Crime Investigation: Insights from a Malaysian Survey - OIC-CERT
viii. Study of Cyber Threat Landscape in Malaysia for the Year 2024 - OIC-CERT
ix. Assessment of Third-Party Accessory for Autonomous Driving System in Malaysia - Laboratory of Accident Mechanisms Analysis (**LMA**) at Gustave Eiffel University, in collaboration with the Society of Automotive Engineers of Japan (**JSAE**)
x. Toward Quantum-Resilient PKI: A Systematic Literature Review of Post-Quantum Certificates Model - USIM Press
xi. RENTAKA: Detecting Ransomware at Pre-Attack Stage Using Machine Learning Approach – IEEE

5.3.2 Social Media

In 2025, CyberSecurity Malaysia received continuous invitations to speak at cybersecurity events at the local radio and television stations. CyberSecurity Malaysia also actively disseminates cybersecurity concerns through social media such as Facebook, Instagram, Threads and X, which as of now the Facebook Page has about 65,000 followers, the CyberSecurity Malaysia X has 8,104 followers, CyberSecurity Instagram has 10,000 followers, and CyberSecurity Malaysia Threads has 1,849 followers.

6. Future Plans

6.1 Future Operation

To encourage a safer cyber environment, CyberSecurity Malaysia realises the need to work together with the local and international cybersecurity organisations through the establishment of formal relationship arrangements, such as through Memorandum of Understanding (**MoU**) and agreements.

CyberSecurity Malaysia and Aerosea Exhibitions Sdn. Bhd will be organising an international event known as the Cyber Digital Services, Defence and Security Asia (CyberDSA'26). This event is scheduled to take place from 5 to 7 October 2026, at the MITEC, Kuala Lumpur. CyberDSA aspires to be a leading content-driven event, serving key stakeholders protecting national, public and business interests in cyberspace. It aims to connect decision makers in governments and the private sector to accelerate the digital drive with security on a regional scale. This event aims to impart the latest knowledge and insights while showcasing cutting-edge technologies that would safeguard digital economies and foster global competitiveness. At the international arena, CyberSecurity Malaysia, as the Permanent Secretariat of the OIC-CERT, continues to spearhead collaborations and organise international events such as the OIC-CERT Annual Conferences and Trainings. With such understanding, CyberSecurity Malaysia supports newly established local and international CSIRTs by providing consultation and assistance, especially in becoming members of the international security communities such as the APCERT, FIRST, and OIC-CERT.

CyberSecurity Malaysia aims to develop GSOC and GCSIRT capabilities while strengthening local development of

cybersecurity technologies, such as SOAR, EDR, and NDR. In addition to conducting cyber drills at the sectoral level, CyberSecurity Malaysia also plans to expand these exercises to the organizational level to further enhance incident preparedness. These initiatives will support the long-term vision of integrating all cybersecurity domains into a unified Digital Fusion Center to enable more coordinated monitoring, analysis, and response capabilities.

CyberSecurity Malaysia strives to improve its service capabilities and encourages local Internet users to report cybersecurity incidents to the Cyber999 Cyber Incident Reference Centre. The development of new and better reporting channels and further promotion of services through the mass media are aspects that will be intensified.

7. Conclusion

CyberSecurity Malaysia will continuously work with international allies to generate useful cooperation in safeguarding the cyber environment. The agency will work together to meet APCERT's vision to create a safe, clean, and reliable cyberspace in the Asia Pacific region.

In line with the CyberSecurity Malaysia Strategy to emphasise capacity and capability building, mitigation of cyber threats, and international collaboration, CyberSecurity Malaysia will continue to enhance existing and develop new cybersecurity processes, capabilities, and technologies. CyberSecurity Malaysia will also continue with the commitment to seek new edges in cybersecurity and to be a catalyst in developing the industry.

International cooperation and collaboration are essential facets in mitigating cybersecurity challenges. Since cyberspace transcends physical national boundaries, strong international relations will remain a critical initiative. With the rapid development of the internet, economies increasingly depend on public network applications such as online banking, online stock trading, e-business, and e-governments, making the protection of national information infrastructures a global priority.

Looking ahead, artificial intelligence (AI) will play a pivotal role in strengthening cybersecurity. AI-driven tools can enhance threat detection, automate responses, and predict emerging risks, but they also introduce new vulnerabilities that require coordinated oversight. Therefore, collaboration must extend beyond traditional frameworks to include shared AI governance, ethical standards, and joint innovation in AI-powered defense systems.

CyberSecurity Malaysia will continue to establish and support cross-border collaboration through bilateral and multilateral platforms, while also pursuing new partnerships with cybersecurity and AI agencies regionally and globally. By combining human expertise with AI capabilities, we aim to make cyberspace a safer, more resilient environment for all.

ETDA

Electronic Transactions Development Agency – Thailand

1. About CSIRT

1.1 Introduction

ETDA was founded to provide responses to changes in economic and social structures due to the transition from an analog society to a digital society where everyone has access to news and information at their fingertips.

Conversations have moved beyond face-to-face meetings to online chats or video calls. A person from one part of the world can communicate with another person from the other side of the world within a second. Work communications and documents no longer need to be printed and submitted to offices. Documents can now be sent via systems with various forms of authentication and sender identifications. Meetings can now be held as e-meetings without needing space for large numbers of people. Commerce has transitioned from walking into a store to buy things to buying things on a screen. Payments can now also be made online.
Changes in the structure of peoples' lives have created a need for agencies or organizations designed to support and govern services in the aforementioned topics in the digital world with reliable, secure and safe standards or "digital governance", in other words. This can help the economy and societies grow in step with the world's rapid changes.

This is why the ETDA was founded. The Agency was founded in 2011 to play a major role in promoting, supporting and developing electronic transactions (e-transactions) or online transactions under the Electronic Transactions Act of B.E. 2544 (A.D. 2001) (Revised Edition) and the Electronic Transactions Development Agency Act of B.E. 2562 (A.D. 2019).

The ETDA prioritizes 3 main sectors: government, private and public. All three sectors engage in the following types of transactions:

- G2X, or Government-to-Government transactions, Government-to-Business transactions and Government-to-Citizen transactions.
- B2X, or Business-to-Business transactions, Business-to-Government transactions and Business-to-Citizen transactions.

- C2C, or Citizen-to-Citizen transactions such as transactions via social media platforms.

Some of these transactions are conducted through online services. Therefore, the ETDA has the responsibility to oversee the transactions, covering government- citizen dimensions such as e-services or platforms that are major components of electronic transactions.

Because online transactions may be vulnerable to fraud, data leaks, cyber-bullying, etc., digital governance must be promoted in the digital world.

To build the system-wide digital governance, the ETDA's roles of promotion and regulation through its working mechanisms for digital governance consist of licensing, registration, notifications, standard-setting, legislation and sandbox-testing.

- Licensing – Licenses are granted to platforms or providers of vital services. Vital services need special oversight due to the potential for widespread damage. This mechanism is necessary for vital service providers, meaning that service providers are required to apply for a license before providing vital services.
- Registration – Because service risks are different, low-risk service providers may be required only to register.
- Notifications – Extremely low-risk service providers may give be required only to give notifications. Minimal-risk services may be provided without notifications, registration or licenses.
- Standard-setting – The ETDA continually works on standards. Electronic transactions must be based on the same standards of security and safety. Service user data must be maintained and have interoperability. Services provided by one provider must have interoperability with other providers and must be interchangeable.
- Legislation – Legislation includes major laws such as acts concerned with electronic transactions including digital ID, and lower-level regulation such as royal decrees in order to clarify practical implementation in compliance with laws.
- Sandbox-testing – Sandboxes are test sites for services unregulated by law. All parties have to create an understanding about services in sandboxes to control risk and conduct limited initial experimentation of services. Once oversight and governance of services is understood, services may leave the sandbox.

In addition to licensing, registrations, notifications, legislation and sandbox-testing , the ETDA's basic work is as follows:

- Data Analysis – If laws are to be enacted with a view toward the future, data is needed to see what will happen in order to prevent laws from becoming obsolete in new technological environments.
- Personnel Development – The ETDA develops personnel to be fully effective and useful in the electronic transactions ecosystem.
- Consultation – The ETDA provides consultation for government agencies, private organizations or citizens in order to understand what is legal, illegal, appropriate, reliable or inadvisable when conducting electronic transactions.
- Fraud Prevention – The ETDA emphasizes connections with platforms to provide education on self-defense and consultation or accept complaints in order to coordinate with the agencies responsible and provide support for

affected individuals.

- Innovation Promotion – Because electronic transactions and digital services come with new technologies, the ETDA's status as a governing agency over services may prevent newly fledged services from surviving. Therefore, the ETDA sees the significance of promoting innovation and sandboxes.

Soon after ETDA was established, the Thai Cabinet decided to move the National CERT role to ETDA as well. ETDA performed this role until 2023, when it was moved to the National Cyber Security Agency (NCSA).

1.2 Establishment

ETDA was founded in 2011.

1.3 Resources

ETDA is supported by a skilled team focused on driving Thailand's digital transformation. The agency's resource strength is divided into key strategic pillars:

- Expertise: Professional teams in Information Security, Legal Affairs, and International Cooperation.
- Specialized Centers: Management of national-level resources such as the Foresight Center, the Online Fraud and Complaint Center (1212 ETDA), and the AIGC (AI Governance Center).
- Standards & Infrastructure: Technical resources dedicated to developing and certifying digital ID frameworks, e-Tax invoices, and e-Signature standards.

This multidisciplinary resource pool ensures that ETDA remains the primary driver for secure and reliable electronic transactions in Thailand.

1.4 Constituency

The constituency of ETDA is all Digital Platform Service Providers (locally or abroad) who provide services in Thailand, as per the Digital Platform Royal Decree of 2023.

2. Activities & Operations

2.1 Incident handling reports

2024 marked the year when the role of the National CERT was officially transferred from ETDA to the National Cyber Security Agency (NCSA). ETDA's role has since been limited to initial coordination between incident reporters and the NCSA, who handled all cases.

3. Events organized / hosted

3.1 Conferences and seminars

- Thailand PKI D-Day Conference 2025, Aug 2025

4. International Collaboration

4.1 Capacity building

4.1.1 Training

- 2025 APISC Security Training Course, Aug 2025

4.1.2 Drills & exercises

- APCERT Annual Drill 2025, Jun 2025

4.1.3 Seminars & presentations

- Cybersec Asia x Thailand International Cyber Week 2025, Jan 2025
- DEFCON Bangkok Community (DC2325), Jan 2025
- 2025 Taiwan Cybersecurity Day, Aug 2025
- TB-CERT Cybersecurity Annual Conference 2025, Aug 2025

GovCERT.HK

Government Computer Emergency Response Team Hong Kong – Hong Kong, China

1. Highlights of 2025

1.1 Summary of Major Activities

The Government Computer Emergency Response Team Hong Kong (GovCERT.HK) persistently collaborated with relevant stakeholders to deliver a wide range of initiatives to strengthen cybersecurity resilience, enhance defensive capabilities and promote cybersecurity awareness amid an increasingly complex threat landscape. In view of several major events in 2025, including the 15th National Games and the eighth Legislative Council General Election, we reinforced safeguards for digital infrastructure and government information systems, enhanced monitoring and threat intelligence, and strengthened operational readiness through regular drills and collaboration to ensure safe and stable operation of Hong Kong's digital infrastructure and government information systems.

1.2 Achievements and Milestones

Cyber Security Assurance and Resilience

To strengthen government-wide cyber resilience, we organised attack-and-defence training and tournament activities in collaboration with the Cyber Security and Technology Crime Bureau (CSTCB) of the Hong Kong Police Force (HKPF) and the Hong Kong Internet Registration Corporation Limited (HKIRC) to enhance the professional skills and incident response capabilities of cybersecurity personnel. We also partnered closely with the CSTCB of HKPF, HKIRC and the Hong Kong Institute of Information Technology (HKIIT) to continuously enhance operational readiness through inter-departmental cybersecurity drill exercises and the Hong Kong Cybersecurity Attack and Defence Drill, enabling participants to validate incident response procedures, sharpen technical skills and improve coordination under simulated scenarios. Furthermore, we also conducted a comprehensive review of government information security policies and guidelines, carried out regular compliance audits for bureaux and departments (B/Ds) to assess adherence to relevant security requirements, and enhanced monitoring and intelligence-gathering mechanisms to improve detection and response, thereby strengthening resilience against evolving threats and challenges.

Awareness and Capability Building

To enhance public awareness of information security and strengthen the cybersecurity capabilities of IT practitioners, we collaborated with industry stakeholders to deliver the Cybersecurity Awareness Campaign 2025 under the theme "Let's Secure as we Digitalise", comprising contests, a prize campaign, seminars and forums that promoted practical cyber hygiene and secure digital practices. The Cybersecurity Symposium 2025 was a key highlight, convening industry leaders and experts to exchange views on emerging threats and effective defence strategies. In parallel, we organised thematic seminars, technical workshops and certificate training on information security and cybersecurity incident response to uplift professional competencies and operational readiness and worked with the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) and HKIRC to launch the "Cybersecurity Service Providers Connect Programme" and "Cybersec One" programme respectively, to strengthen organisational resilience.

Liaison and Collaboration

We maintained close liaison and collaboration with local partners such as HKIRC and HKCERT, relevant stakeholder groups, and Greater Bay Area counterparts, while also actively participating in international CERT community activities, exchanges, training and drill exercises in Asia Pacific Computer Emergency Response Team (APCERT) and the Forum of Incident Response and Security Teams (FIRST), with the aim of strengthening coordination, intelligence exchange and collective preparedness.

2. About GovCERT.HK

2.1 Introduction

GovCERT.HK is a governmental CERT responsible for coordinating incident responses for over 80 departmental Information Security Incident Response Teams (ISIRTs) of the Government of the Hong Kong Special Administrative Region of the People's Republic of China ("the Government").

GovCERT.HK works closely with HKCERT and HKIRC, local industries and critical Internet infrastructure stakeholders on cyber threat intelligence sharing, capability development, public education and continuous promotion on cyber security. GovCERT.HK also actively collaborates with other governmental and regional CERTs, and international organisations in sharing cyber threat intelligence and incident information; participating in training events, workshops, forums and drills; and organising activities for public awareness promotion and capability development, with a view to enhancing information and cybersecurity in the region.

2.2 Establishment

GovCERT.HK was established on 1 April 2015 through the consolidation of internal IT security teams within the Digital Policy Office (DPO) (formerly Office of the Government Chief Information Officer (OGCIO)) of the Government.

2.3 Resources

GovCERT.HK is an establishment under DPO (formerly OGCIO) and funded by the Government.

2.4 Mission and Constituency

Being the governmental CERT, GovCERT.HK centrally manages incident responses within the Government and develops CERT-related services to assist government departments in understanding the associated risks of information and cyber security, implementing appropriate security measures, monitoring potential threats and responding to security events with a view to ensuring robust protection of government's information infrastructure.

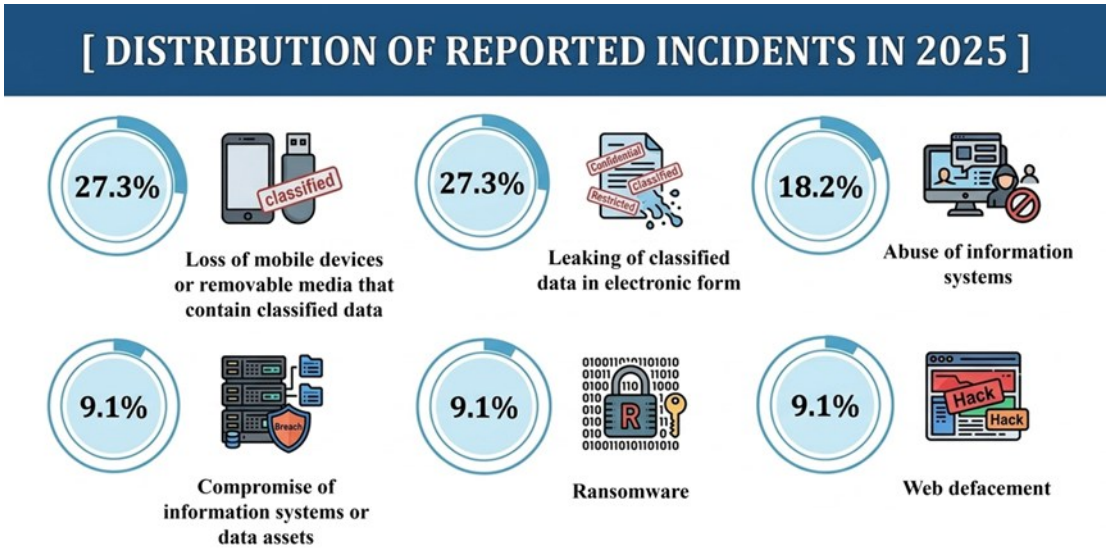
3. Activities and Operations

3.1 Alerts and Advisories

In 2025, GovCERT.HK issued 263 security alerts on known vulnerabilities in common products. We proactively requested government departments to implement prompt and appropriate preventive measures for all reported vulnerabilities, with particular emphasis on those assessed at higher severity levels to mitigate potential information security risks.

3.2 Incident Handling Reports

GovCERT.HK handled 11 reported incidents related to government installations, with the incident types shown below:



Relevant statistics on information security incidents in the Government are also available on the Government's Public Sector Information Portal for public access.
(http://www.data.gov.hk/en-data/dataset/hk-dpo-pgc_div_01-information-security-incident)

3.3 Abuse Statistics

GovCERT.HK assisted government departments to take effective and prompt measures to prevent and reduce the risks and impacts of cyberattacks on their information systems, with the types of security issues shown below:

3.4 Publications and Mass Media

To proactively reach out to the public, we continued to share tips and best practices against cyber threats through multiple channels.

- We partnered with Radio Television Hong Kong (RTHK) to broadcast radio episodes "e-World Smart Tips", covering a wide range of topics such as tips for safe online sharing, secure online shopping, Wi-Fi security, mobile payments, netiquette, data loss prevention, digital identity protection, password hygiene, and the safe use of instant messaging and AI, in a lively and interesting way.
  (www.cybersecurity.hk/en/media.php#Radio)
- We published practical leaflets and infographics on themes such as digital signage security, online shopping security tips, phishing awareness and guidance on identifying and responding to deepfakes, to raise public awareness and encourage protective measures against cyber threats.
  (www.cybersecurity.hk/en/resources.php)

- We organised the "Let's Secure as we Digitalise" Instant Messaging Apps Stickers Design Contest, which attracted many creative and impactful submissions. The designs effectively raised public awareness of cybersecurity through artistic expression and were well received. They also served as timely reminders for the public to stay vigilant against online scams, strengthening city-wide cyber resilience and collective defence against cyberattacks.

- We provided timely updates and practical tips on the latest cybersecurity news and events on the DPO Facebook page, including guidance on the safe use of cloud services and AI to enhance public awareness. (http://www.facebook.com/digitalpolicyhk)

3.5 Government-wide Health Check

GovCERT.HK has implemented a centralised cyber security health check platform since December 2024 to perform regular and continuous health checks on government public-facing information systems and websites. This initiative aims to enhance the detection of potential security vulnerabilities, thereby strengthening the prevention of information and cyber security incidents. For government information systems and websites with relatively higher risk, GovCERT.HK adopts a risk-based approach, selecting government information systems for manual penetration testing to identify application-level security vulnerabilities.

4. Events Organised/Hosted

4.1 Training

Seminars/Webinars

In 2025, we organised a range of seminars, webinars, and training sessions covering the latest IT security technologies and solutions, emerging cybersecurity threats, and response strategies. More than 6 900 government staff participated in these events, which addressed topics including phishing prevention, AI and social media security, safe browsing practices, network security, and credential-based threats.

In collaboration with the Civil Service College, we delivered an Innovation and Technology (I&T) leadership series of thematic seminars to strengthen government senior management's understanding and capabilities in information systems management, cybersecurity, and data security.

Certificate in Cybersecurity for the Public Sector

To enhance government staff's information security competencies, we commissioned the Hong Kong Institute of Information Technology (HKIIT) to design and deliver the Certificate in Cybersecurity for the Public Sector, an accredited programme recognised under the Hong Kong Qualifications Framework (HKQF). The programme comprises three levels: Foundation, Intermediate, and Advanced to comprehensively enhance the information security skills of government staff.

4.2 Audit, Drills and Exercises

Government-wide information security compliance audit

A new round of government-wide information security compliance audits was launched in late 2024, and audits covering all B/Ds were completed in 2025. In addition, nine major government IT systems were identified under a risk-based approach for in-depth compliance audits, to ensure B/Ds' adherence to government information security requirements.

Inter-departmental Cyber Security Drill

GovCERT.HK partnered with the CSTCB of HKPF to organise the annual Inter-departmental Cyber Security Drill, with a view to strengthening the preparedness and overall defensive capabilities of B/Ds against cyberattacks since 2017. In 2025, the exercise reached new milestones in both scale and participation, over 280 government officers from 71 B/Ds, together with industry experts from six professional and academic institutions, participated in this drill and an online training workshop to share the latest strategies and techniques for handling cyber incidents.

Hong Kong Cybersecurity Attack and Defence Drill

Following the success of the first Hong Kong Cybersecurity Attack and Defence Drill (the Drill) organised last year, we spearheaded to organise the Drill again in collaboration with the CSTCB of HKPF, HKIRC, Cyberport, and HKIIT in 2025, to enhance the technical skills, strategy, experience, and overall defence capabilities of participants in identifying and responding to cyberattacks. The scale of this year's drill has been expanded to include the participation of 25 government departments and 9 public organisations forming the defensive teams, and 15 red teams formed by cyber security enterprises and post-secondary colleges, thereby enhancing the drill effectiveness. Experienced teams from the Mainland were also invited to participate in the red teams this year to promote technical exchanges between the two places. Moreover, over 250 representatives from more than 60 government departments and organisations took part in the drill on-site as observers to monitor the operation and progress of the exercise and learn more about the latest trends in cybersecurity threats from the Drill.

Government-wide Phishing Drill Campaign

A new round of the Government-wide Phishing Drill Campaign was completed in 2025. The campaign leveraged new technologies, including AI, to simulate realistic phishing emails, thereby strengthening government staff's awareness and ability to identify and report phishing attempts.

4.3 Conferences and Seminars

Build a Secure Cyberspace Promotional Campaign

A series of promotional activities under the theme "Let's Secure as we Digitalise" were organised for organisations, schools and the public to raise their cyber security awareness and strengthen their cyber security postures. The prize campaign integrates the creative outcomes from the earlier Instant Messaging Apps Stickers Design Contest with social media activities, enabling the public to learn proper cybersecurity knowledge in a fun and relaxed atmosphere, and apply it to daily life. Webinars and seminars were also organised under the campaign to further deepen cybersecurity knowledge of the participants.

School visits and security talks for non-governmental organisations (NGOs)

To promote cyber security awareness and cyber etiquette, we organised a total of 35visits to primary and secondary schools, tertiary institutions, and NGOs to deliver information security talks to students, teachers, parents, service recipients and staff of NGOs.

InfoSec Tours with RTHK Radio 2

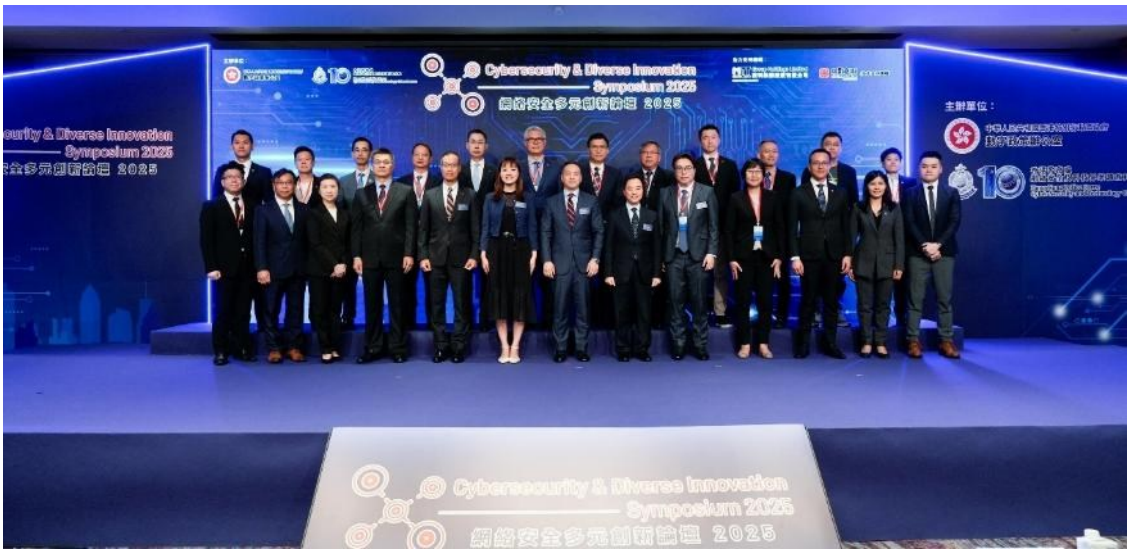
We continued to partner with the RTHK to conduct three InfoSec Tours with topics of "Essential Cybersecurity Awareness and Digital Literacy in the Age of AI", "Safe Internet Surfing with Netiquette" and "The Pitfalls in Cyberspace", which delivered information security messages in a relaxing way while promoting the importance of online safety and security.

Cybersec Infohub engagement activities

To encourage the engagement and effective discussion among public and private organisations on cybersecurity, various activities such as sector-specific meeting and networking, technical professional workshops, webinars and seminars were arranged under the Cybersec Infohub partnership programme with affirmative feedback.

Cybersecurity & Diverse Innovation Symposium

We co-organised the "Cybersecurity & Diverse Innovation Symposium 2025" with the CSTCB of HKPF. The Symposium examined a range of topics, including emerging cybersecurity challenges, cross-sector collaboration, and innovation-led defence strategies. It attracted over 600 experts from Hong Kong and the Mainland, representing multiple sectors.



China Cybersecurity Week Hong Kong Sub-forum

We, along with the CSTCB of HKPF, the HKIRC and the Hong Kong Cybersecurity Professional Association (HKCSPA), jointly organised the "China Cybersecurity Week Hong Kong Sub-forum 2025". It brought together over 400 experts and business leaders from the Guangdong-Hong Kong-Macao Greater Bay Area (GBA), who exchanged views on various topics such as emerging threats in cybersecurity and the latest cybersecurity defence technologies, jointly exploring Hong Kong's cybersecurity trends.

Cybersecurity Symposium

We organised the Cybersecurity Symposium in collaboration with the CSTCB of HKPF, the HKIRC and the HKCSPA, aiming at fostering collaboration between public and private organisations and supporting Hong Kong's development as a leading digital economy, thereby strengthening Hong Kong's overall cybersecurity defence and resilience capabilities. Several insightful keynote speeches and panel discussion sessions were held during the symposium. More than 30 experts from the Government, academia, technology, telecommunications, finance, and insurance sectors were invited as speakers and over 1 000 cybersecurity professionals and industry leaders from various sectors attended.

5. Local and International Collaboration

5.1 Local Collaboration

Promoting Cyber Security Information Sharing and Collaboration

We continued to promote and operate the Cybersec Infohub with HKIRC to establish closer connections among local information security stakeholders. The programme attracted over 3 130 organisations and more than 4 470 representatives from various local sectors as of the end of 2025.

In response to the increasing frequency of cybersecurity threats affecting public and private organisations in Hong Kong and to prepare for the major events held in Hong Kong, we convened special meetings in July, October and November with the Internet Infrastructure Liaison Group and representatives of the cybersecurity industry to discuss enhancements to technical protection measures and risk management strategies.

Nurturing Cyber Security Talents

We continued to support our working partners to organise various programmes and campaigns to groom cybersecurity talents with the latest cybersecurity skills and knowledge, thereby attracting and retaining talents in the cybersecurity industry in a long run, including the following events:

- "Capture the Flag Challenge 2025" by HKCERT
- "Cyber Attack and Defence Elite Training cum Tournament" by HKIRC
- "Cyber Youth Programme 2025" including training courses, competition and a game-aided learning platform by HKIRC

Enhancing Overall Cyber Security Resilience

We also supported our working partners to organise various programmes and campaigns to provide free services and resources for promoting cybersecurity awareness and enhancing defence capabilities among SMEs and public to address emerging threats. GovCERT.HK supported the following initiatives:

- "Cybersecurity Service Providers Connect Programme" co-organised with HKCERT

- "Cyber Security Summit Hong Kong 2025" by HKCERT
- "Cybersec One Programme" by HKIRC
- "Healthy Web" with free web screening service by HKIRC
- "Cybersec Training Hub" with free training resources online by HKIRC
- "Cyber Security Staff Awareness Recognition Scheme 2025" by HKIRC

5.2 Chinese Mainland and International Collaboration

To foster closer collaboration with international security experts for sharing experience in information security and for strengthening the knowledge base of emerging cyber threats, vulnerabilities and mitigation solutions, GovCERT.HK strived to learn from the CERT community on the global cyber security trends from different facets, including international standards development, global information security and data privacy policies and technological researches.

GovCERT.HK participated in the following events in 2025:

- 2025 China Cybersecurity Week
- 2025 China Cybersecurity Week Macau Sub-forum
- APCERT Annual General Meeting and Conference
- APCERT Drill with the theme of "When Ransomware Meets Generative AI"
- APCERT on-line training sessions
- NatCSIRT Meeting 2025 and 37th FIRST Annual Conference
- 2025 World Internet Conference Asia-Pacific Summit
- 2025 World Internet Conference Wuzhen Summit

To promote cybersecurity exchange and collaboration in the Guangdong–Hong Kong–Macao Greater Bay Area (GBA), we signed a memorandum of understanding (MoU) last year. We have held regular experience-sharing meetings with the Cyberspace Administration of Guangdong Province and the Cybersecurity Incident Alert and Response Centre of Macao to exchange updates on the latest cybersecurity developments and initiatives, and to discuss priority areas for cybersecurity cooperation among Guangdong, Hong Kong, and Macao.

6. Future Plans

GovCERT.HK will continue to enhance cybersecurity awareness, preparedness and resilience among government, industry and public through various initiatives:

- Enhance technical skills, strategies and defensive readiness across government and the public sector via training and attack-and-defence drills to effectively address emerging threats;
- Strengthen collaboration with local, regional, and international cybersecurity partners to support cross-boundary incident coordination and regular information exchange;

- Deepen engagement with stakeholders to deliver programmes supporting the education sector, public organisations, and SMEs in strengthening cybersecurity readiness and resilience, nurturing talent, and promoting cybersecurity awareness across different sectors; and
- Promote the responsible and secure use of AI at work, fostering a sustainable culture of AI safety and cybersecurity readiness across the community.

7. Conclusion

To maintain a secure and resilient cyber environment that supports the Government's digital services and Hong Kong's continued development, GovCERT.HK will continue to strengthen cybersecurity governance, operational preparedness, technical defence capabilities, and community awareness. We will also deepen collaboration with local, regional, and international partners to enhance information sharing, coordination, and collective readiness in response to an evolving cyber threat landscape.

HKCERT

Hong Kong Computer Emergency Response Team Coordination Centre

1. Highlights of 2025

1.1 Summary of major activities

- Organised the "Build a Secure Cyberspace 2025 - Let's Secure as we Digitalise" campaign with the Digital Policy Office and Hong Kong Police Force.
- Launched Cybersecurity Service Providers Connect Programme
- Organised the "HKCERT Capture the Flag 2025"
- Presented at different international conferences and local press briefing.
  - "Year Ender" in local media briefing to call on public to raise awareness of cybersecurity
  - Media interviews in local media, radio and TV programme to raise general public awareness on cyber security risks
- Published timely security guidelines and advisories in response to the emerging technology

1.2 Achievements & milestones

- Organised the "Build a Secure Cyberspace 2025 - Let's Secure as we Digitalise" campaign with the Digital Policy Office and Hong Kong Police Force. The campaign featured one webinar, one public seminar, an instant messaging Apps stickers design contest, and an award presentation ceremony. The contest attracted over 2,000 participants while more than 600 participants attended the webinar and seminar.
- Launched Cybersecurity Service Providers Connect Programme. The programme is a long-term initiative designed to connect service providers with enterprises and build a trusted ecosystem. To date, more than 20 service providers have met the requirements and are now listed on the platform.
- Organised "HKCERT Capture the Flag 2025". The HKCERT Capture the Flag 2025 event featured 3 workshops, a 48-hour online qualifying contest, and a 1 day in-person competition for the finals with an award ceremony. This year was the first time the competition incorporated both attack and defence elements, making the format much closer to real-world scenarios. The event drew a record-breaking 1,900 participants from worldwide.

- Published security advisories on latest risks of emerging technology and emerging cyber threats
- Continued the Healthcare Cyber Security Programme and Critical Infrastructure Cyber Security Programme.

2. About HKCERT

2.1 Establishment

Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) was established in 2001 with funding from the Hong Kong Special Administrative Region (HKSAR) Government. The Hong Kong Productivity Council (HKPC), a government subvented organisation in Hong Kong, has operated the centre since then.

2.2 Organisation and Workforce Power

The senior management of HKPC oversees the overall direction and operation of the centre. The daily operations are taken care of by the Centre Manager, two Consultants and six Security Analysts and one Assistant Project Manager.

2.3 Mission and Constituency

HKCERT is the centre of coordination of computer security incident response for the constituency (local enterprises and Internet users) in Hong Kong.
The mission of HKCERT is to be the cyber threats response and defence coordinator in Hong Kong to protect the Internet environment and the economic and social interests of Hong Kong.
The objectives of HKCERT are to serve as a focal point in Hong Kong for information security incident reporting and responses; to provide a focal point in Hong Kong for cooperation and coordination with other Computer Emergency Response Teams (CERTs), and relevant bodies outside Hong Kong; to promote awareness of the community on computer security issues and the latest international best practices and standards; and to provide assistance to the community in the protection against computer security threats and the prevention of security attacks and in recovery actions for computer security incidents

3. Activities & Operations

3.1 Incident Handling

During the period from January to December of 2025, HKCERT handled 15,877 security incidents which was 27% increase of the previous year (see Figure 1).

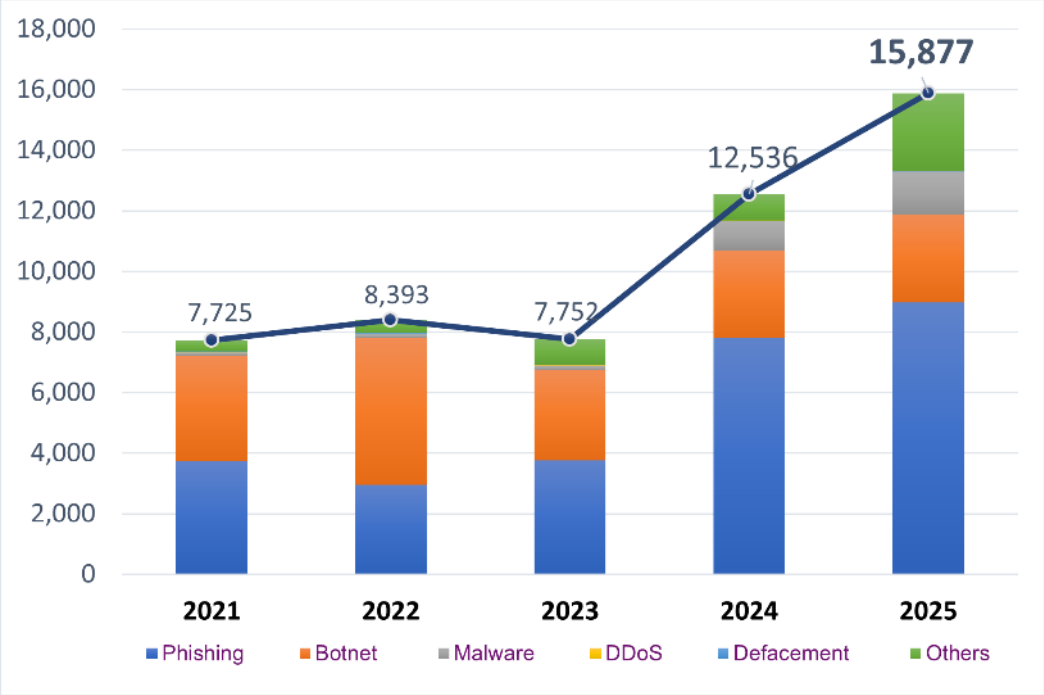


Figure 1. HKCERT Security Incident Reports

While the number of overall security incidents handled by HKCERT broke the record in 2025. It was the first time to hit over 15,000 cases. Phishing (8,973 cases or 57% of total cases) went up 15% and total phishing URLs was increased by 29%. Phishing primarily targeted the social media, instant messaging sectors, followed by crypto, banking, tech enterprises and e-commerce, respectively. Malware incidents also rose significantly in 2025, increasing 3.6-fold year-over-year, with most cases involving trojans targeting smart devices disguised as legitimate applications.

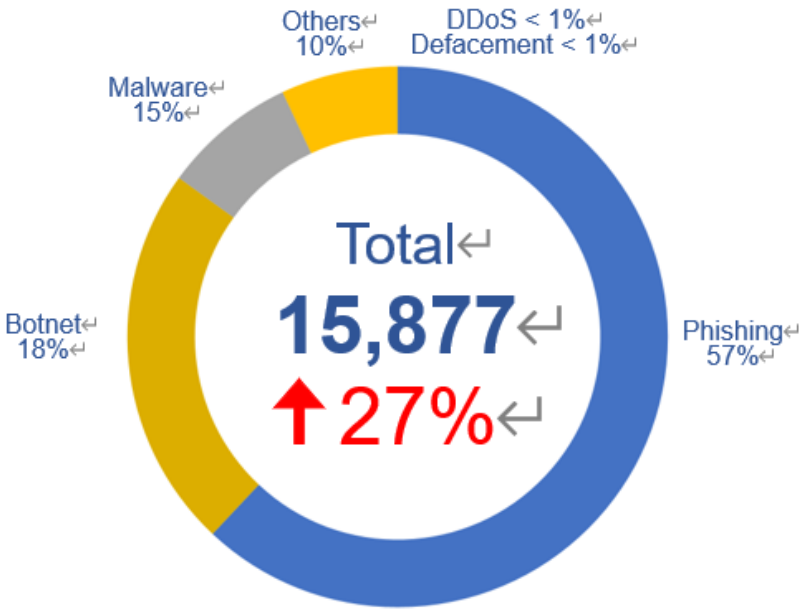


Figure 2. Distribution of Incident Reports

3.2 Watch and Warning

During the period from January to December of 2025, HKCERT published 415 security bulletins for the vulnerabilities of major software (see Figure 3) on the website. In addition, HKCERT have also published 22 security advisories, topics such as risks from third-party and weaponisation of AI.

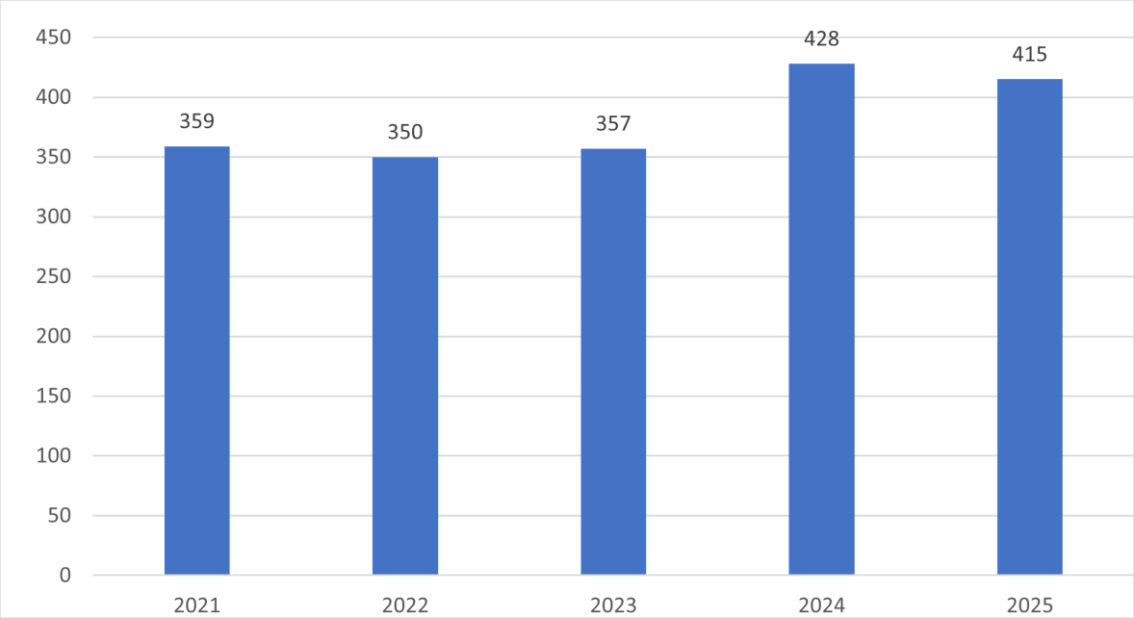


Figure 3. HKCERT Published Security Bulletins

HKCERT used the centre's website (https://www.hkcert.org), RSS, Hong Kong Government Notification mobile app, social media platforms such as Facebook and LinkedIn to publish security bulletins, blogs and news. HKCERT also used email and SMS to publish selected security bulletins to subscribers. The subscriptions are free of charge.

3.2.1 Embrace Global Cyber Threat Intelligence

HKCERT used the Information Feed Analysis System (IFAS) to collect intelligence of compromised machines in Hong Kong from global security researchers. The system provided a better picture of security status of Hong Kong and a way to verify the effectiveness of the security incident response. For example, figure 4 showed the number of bot-related in Hong Kong network detected in IFAS.

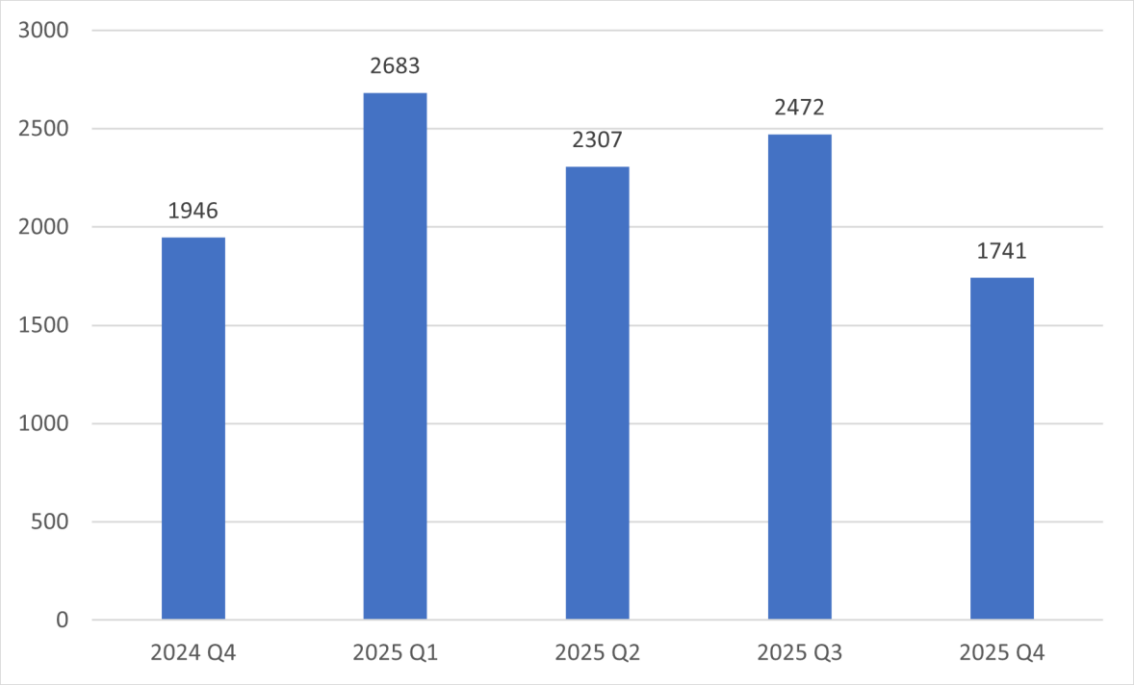


Figure 4. Trend of Bot related security events in the past year
(Source: data feeds from overseas security researchers, not from incident reports)

3.3 Publications

- HKCERT had published 4 quarterly issues of Hong Kong Security Watch Report showing the status of compromised computers in Hong Kong from the data collected from overseas security researchers (see https://www.hkcert.org/watch-report).

- HKCERT had published 12 issues of monthly e-Newsletter in the period (see https://www.hkcert.org/newsletters).
- HKCERT had published the statistics of incident reports every month (see https://www.hkcert.org/statistics).

4. Events organised and co-organised

4.1 Build a Secure Cyberspace 2025 – Let's Secure as we Digitalise

HKCERT jointly organised the "Build a Secure Cyberspace 2025" campaign with the Digital Policy Office and Hong Kong Police Force. The campaign involved 1 webinar, 1 public seminar and an instant messaging Apps stickers design contest. An award presentation ceremony was organised in Sep 2025.

For the instant messaging Apps stickers design contest, HKCERT received about more than 2,000 applications from Open Group, Secondary School and Primary School Group. A professional judge panel selected winners with most creative and meaningful.
Winning entries: https://www.cybersecurity.hk/en/contest-2025.php)

4.2 Cybersecurity Service Providers Connect Programme

- The "Cybersecurity Service Providers Connect Programme (CSPCP)," launched by the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT), is designed to link local cybersecurity service providers with enterprises and institutions via a dedicated platform. This initiative streamlines the search for cybersecurity solutions and promotes the growth of the local cybersecurity ecosystem.
- On 23 October 2025, the programme was officially launched, and more than 20 service providers participated in

the programme until now. On 22 January 2026, CSPCP organised a seminar featuring exhibition booths and panel discussions, attracting over 100 participants who visited the service provider booths. HKCERT will continue to engage more service providers to build up a trusted ecosystem.

- (Programme Website: https://spconnect.hkcert.org/)

4.3 HKCERT Capture the Flag 2025

- The "HKCERT Capture the Flag 2025" partnered associations in information and education sectors. It was open to all participants who were enthusiastic about Capture the Flag. This year, it was the first time for HKCERT CTF to introduce attack and defence elements. It was a success with more than 600 teams and 1,900 participants from universities, secondary schools, open categories and international. Following the final round, a public seminar with award ceremony was held in February 2026.
- (Winners: https://www.hkcert.org/event/hkcert-capture-the-flag-challenge-2025)

5. Collaboration

5.1 International Collaboration

HKCERT participated in a number of international coordination and collaboration events in year 2025:

- Collaboration Meeting with CNCERT
- Participated in the AusCERT Conference 2025
- Participated in the FIRST Conference 2025
- Participated in the NatCSIRT Conference 2025
- Participated in 2025 APCERT Cyber Security Drill Exercise
- Participated in HITCON 2025
- Participated in CNCERT Annual Conference
- Participated in APCERT AGM and Conference
- Collaboration Meeting with MNCERT/CC

HKCERT collaborated with APNIC closely in taking down bad reputation ASNs whose owners were suspicious and may not provide proper contact information.

5.2 Local Collaboration

HKCERT worked with a number of local organisations in different areas. Some examples:

- HKCERT continued to work closely with the government (GovCERT.HK) and law enforcement agency and held

meetings to exchange information and to organise joint events regularly.

- HKCERT continued to actively participate in the Cyber Security Information Sharing platform 'Cybersec Infohub" which comprised of over 2,000 companies, critical infrastructure organisations, banks and other enterprises in Hong Kong.
- HKCERT continued to work with police, ISPs and domain registries on closing down bulletproof hosting, phishing sites and botnet command and control centres in Hong Kong.
- HKCERT collaborated with Microsoft in the Healthcare Cyber Security Watch Programme to promote cyber security situational awareness in healthcare sector. The objective of this programme is to make use of global cyber threat intelligence to inform Hong Kong Healthcare sector of attacks targeting their IT infrastructure so that they can better mitigate security risks. The Programme was officially launched in December 2020 with 14 organisations including the Hospital Authority and most of the private hospitals in Hong Kong joining.
- HKCERT collaborated with Microsoft in the Critical Infrastructure Cyber Security Watch Programme to promote cyber security situational awareness in critical infrastructure sector. The objective of this programme is to make use of global cyber threat intelligence to inform Hong Kong critical infrastructure sector of attacks targeting their IT infrastructure so that they can better mitigate security risks. The Programme was officially launched in December 2021 with 7 organisations that provide essential public services to the citizens in Hong Kong joining.
- HKCERT collaborated with local regulators to deliver talks to related regulated organisations and members.
- HKCERT collaborated with local universities to conduct research on IoT and OT security.

6. Achievements & Milestones

6.1 Advisory Group Meeting

HKCERT held two Advisory Group Meetings in October 2025. The meetings solicited input from the advisors and invited guests from SME associations on the development strategy of HKCERT.

6.2 Three Year Strategic Plan

HKCERT had prepared its rolling Three Year Strategic Plan based on inputs from Advisory Group, the Strategy and Service Review Report and discussion with the government. The plan is updated annually. HKCERT is based on this plan to prepare the annual work plan and budget to solicit funding support from the government.

6.3 Embrace Global Intelligence and Build Security Health Metrics

HKCERT had implemented the IFAS to collect intelligence of compromised machines in Hong Kong. The system provided a better picture of security status of Hong Kong and help clean up the botnets and C&C servers in Hong Kong. HKCERT publicised the information to the public quarterly and used the information in decision making.

6.4 Open Data

HKCERT had a plan to provide open data for the count of monthly security incidents on website for public access (see https://www.hkcert.org/open-data) starting January 2020.

6.5 Year Ender Press Briefing

HKCERT organised a year ender press briefing to media in January 2026 to review cybersecurity landscape of 2025 and provided a cybersecurity forecast for 2026 to warn the public for better awareness and preparedness. It received very good press coverage.

7. Future Plans

7.1 Strategy

"Proactivity", "Share to Win" and "Security is not an Island" are the strategic directions of HKCERT which would work closer with other CERTs and security organisations to build a more secure Hong Kong and Internet.

7.2 Funding

HKCERT had secured Government funding to provide the basic CERT services in 2026/2027. We shall work closely with the Government to plan for the future services of HKCERT and seek their support.

7.3 Enhancement Areas

HKCERT will enhance the "Cybersecurity Service Providers Connect Programme" by introducing additional features, enabling organisations to more easily identify reputable service providers.

HKCERT will continue to strengthen public cybersecurity awareness, with new promotional campaigns planned for the coming year.

In addition, HKCERT will continue organising Capture the Flag (CTF) competitions. In 2026, HKCERT will partner with various associations to host another CTF for university students, secondary school students, and open-category participants.

8. Conclusion

In 2025, the number of overall security incidents reported to HKCERT increased by 27% and broke the record. The phishing cases and phishing URLs recorded a rise, increased by 15% and 29%, respectively. It became the first major security incident in Hong Kong. Malware cases also recorded a rise, increased by 3.6-fold due to adding new sources of threat intelligence.

In 2026, HKCERT will continue to actively study the trends of cyber attacks and security technologies, and assist the community in meeting the ever-changing security challenges through various channels, such as issuing early warnings of cyber attacks, security recommendations, etc. HKCERT will also organise major international seminars and competitions such as Capture the Flag competition, to raise local cyber security awareness and nurture the next generation of cyber security talents.

There are five major information security risks that must be addressed in 2026:

i. **AI-Driven Attacks and Agentic AI Risks**: With rapid advancements in AI technology, cyber attackers are increasingly leveraging AI to launch more sophisticated attacks. Particularly agentic AI systems—which possess autonomous learning and execution capabilities—can make judgments and act on their own without human intervention. Once hacked, they will carry out potentially malicious commands automatically. These traits make such attacks harder to predict and defend against.

ii. **Weak AI Governance of Enterprises Increases Data Leakage Risks**: Some enterprises lack clear internal guidelines regarding the use of AI. As a result, sensitive information—such as customer data and contract details—may be leaked if employees misuse public AI platforms. In certain cases, employees have used unauthorised AI tools or lacked understanding of the AI platform's privacy statement, thereby misjudging data security, entering sensitive data and unintentionally causing information leaks.

iii. **Supply Chain Vulnerabilities and Third-Party Security Gaps**: Companies are increasingly relying on outsourced services and third-party platforms to handle their business processes during operations. However, when these partners fall victim to cyberattacks or suffer from security flaws, the impact can cascade against client organisations. Even companies with strong internal cybersecurity measures may be compromised indirectly due to weaknesses in their supply chain.

iv. **Over-Reliance on Cloud Infrastructure Creates Single Points of Failure**: Cloud platforms have become essential to enterprise operations, supporting data storage, application deployment, communications, and backups.

However, over-dependence on a single cloud provider without adequate redundancy or contingency planning can be dangerous. In the event of a platform outage or service disruption, businesses may face complete operational paralysis.

v. **Emerging Threats from AI-Enabled Devices**: As AI-enabled devices (e.g., voice assistants, office robots, and customer service bots) are more integrated into business operations, they are revealing new security vulnerabilities. These devices usually employ Large Language Models (LLMs) to understand and parse human commands. With LLMs being embedded in physical systems, security vulnerabilities that originally existed in the digital environment may extend into the real world. Without strict authentication mechanisms in place, they are susceptible to voice spoofing or erroneous instructions, potentially triggering harmful actions.

IDSIRTII/CC

Indonesia Security Incident Response Team On Internet Infrastructure / Coordination Center

1. Highlights of 2025

1.1 Summary of major activities

ransomware, and phishing activities. Indonesia Security Incident Response Team on Internet Infrastructure / Coordination Center (Id-SIRTII/CC) issued 2,821 incident notifications, identified 254 data breach indications, detected 44,772,291 exposed data findings affecting 461 stakeholders, and recorded 4,433 web defacement incidents, including attacks targeting government websites. Through cybersecurity operations and services, Id-SIRTII/CC also handled 1,965 cyber complaints, published 144 security advisories, and identified 1,689 vulnerabilities across 368 applications through IT Security Assessment activities.

1.2 Achievements & milestones

1.2.1 Cyber Battle: Capture the Flag (CTF) 2025 – Brunei Darussalam

The Cyber Battle: Capture the Flag (CTF) 2025, organized by ITPSS Sdn Bhd alongside the Cyber Security Conference (CySec) 2025, was held on 15–16 September 2025 at The Rizqun International Hotel, Brunei Darussalam, in collaboration with Cyber Security Brunei (CSB) and the Brunei Cybersecurity Association (BCSA). The Indonesian delegation represented by Team Id-SIRTII/CC secured 1st place, achieving the highest score among 16 teams invited from ASEAN national cyber authorities, including national CIRT, CERT, and cybersecurity agencies.

1.2.2 BeAI Hackathon 2025

Id-SIRTII/CC team participated in the BeAI Hackathon, an internal innovation program aimed at developing artificial intelligence–based solutions to enhance productivity across BSSN work units. The event was held from 15 September to 9 October 2025 in both online and offline formats within the BSSN environment. Team Leaklens, consisting of three personnel from the Directorate of Cyber Security Operations, achieved 2nd place with the development of an AI-based all-in-one threat intelligence lifecycle tool designed to detect compromised servers, exposed credentials, and sensitive data leaks, demonstrating the directorate's capacity to innovate and strengthen cybersecurity capabilities through

emerging technologies.

1.2.3 Cyber SEA Games 2025 – Thailand

The Cyber SEA Games 2025, organized by the ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC), was held in Bangkok, Thailand on 16–17 October 2025, with support from NCSA Thailand and the Japan International Cooperation Agency (JICA). In this competition involving participants from ten ASEAN member states, the Indonesian delegation represented by Team Id-SIRTII/CC secured 3rd place, and three Indonesian team members were selected to represent ASEAN at the International Cybersecurity Challenge (ICC) 2025.

1.2.4 3rd ASEAN Cyber Shield (ACS) Hacking Contest 2025

Team Id-SIRTII/CC participated in the 3rd ASEAN Cyber Shield (ACS) Hacking Contest 2025, organized by the ASEAN Korea Cooperation Fund (AKCF) in collaboration with the Korea Internet & Security Agency (KISA), with participation from teams representing ten ASEAN member states. In this competition, which featured CTF Jeopardy and Attack–Defense challenges covering domains such as reverse engineering, binary exploitation, forensics, cryptography, blockchain, OSINT, network, and web exploitation, Team Id-SIRTII/CC secured 2nd place, while the 1st and 3rd places were won by teams from Vietnam.

2. About CSIRT

2.1 Introduction

Indonesia Security Incident Response Team on Internet Infrastructure / Coordination Center (Id-SIRTII/CC) is the national Computer Security Incident Response Team (CSIRT) responsible for monitoring, detecting, analyzing, and responding to cybersecurity incidents related to internet infrastructure in Indonesia. Id-SIRTII/CC plays a strategic role in strengthening national cybersecurity resilience by coordinating incident handling, providing early warning and threat intelligence, and supporting the protection of national critical information infrastructure. In addition, Id-SIRTII/CC actively collaborates with government agencies, private sector organizations, international cybersecurity communities, and other CSIRTs to enhance information sharing, capacity building, and coordinated response to cyber threats.

2.2 Establishment

Id-SIRTII/CC was established in 2007 under the Ministry of Communication and Information Technology (KOMINFO) as Indonesia's national focal point for incident response and cybersecurity coordination related to internet infrastructure. Its establishment was driven by the increasing reliance on internet-based systems and the growing number of cyber threats targeting national networks and critical sectors. In 2018, following the establishment of the National Cyber and Crypto Agency (Badan Siber dan Sandi Negara / BSSN), the operational management of Id-SIRTII/CC was placed under BSSN to strengthen the national cybersecurity governance framework. Since then, Id-SIRTII/CC has continued to evolve

its capabilities in cyber monitoring, incident response coordination, threat intelligence, vulnerability assessment, and cybersecurity capacity building at the national and regional levels.

2.3 Resources

Id-SIRTII/CC is a semi-governmental organization. Which means, it is fully funded by The Government of Republic of Indonesia and non-binding sources of funds in accordance with applicable laws and regulations.

2.4 Constituency

Id-SIRTII/CC constituencies include local CSIRTs across Indonesia, ministries and institutions within Critical Information Infrastructure (CII) sectors, and other agencies associated with these sectors. As the National CSIRT of Indonesia, Id-SIRTII/CC is also mandated to support organizations or constituencies that are not yet served by any other CSIRT, providing assistance upon request. In addition to incident response and coordination roles, Id-SIRTII/CC also delivers proactive awareness and educational initiatives for its constituencies, including small and medium enterprises (SMEs) and the public.

3. Activities & Operations

3.1 Scope and definitions

Id-SIRTII/CC (Indonesia Security Incident Response Team on Internet Infrastructure/Coordination Center) plays a strategic role in securing Indonesia's internet infrastructure by conducting threat monitoring, managing cyber incidents, and coordinating national response efforts. The organization also collaborates with law enforcement and various stakeholders to support regulatory compliance and promote cybersecurity awareness and capacity building. Through its annual publications, Id-SIRTII/CC presents an overview of Indonesia's cybersecurity landscape, including incident patterns, threat developments, policy updates, and major initiatives undertaken during the year. Furthermore, Id-SIRTII/CC contributes to strengthening national digital resilience by developing monitoring platforms, analytical resources, and fostering cooperation among government agencies, industry partners, and academic institutions.

3.2 Incident handling reports

Id-SIRTII/CC has carried out 35 cyber incident response assistance activities involving 34 stakeholders. The implementation falls into the following three categories:

- Handled by Id-SIRTII/CC

There were 12 incidents in which the cyber incident handling assistance process was carried out entirely by Id-SIRTII/CC.

- Collaboration handling by Id-SIRTII/CC and Organizational CSIRT
  There were 10 incidents in which the cyber incident handling assistance process was carried out entirely by Id-SIRTII/CC and Organizational CSIRT.
- Handled by Organizational CSIRT
  There were 13 incidents in which the cyber incident handling assistance process was carried out entirely by Organizational CSIRT.

The following is the classification of incidents handled by the Cyber Incident Response Assistance Service:

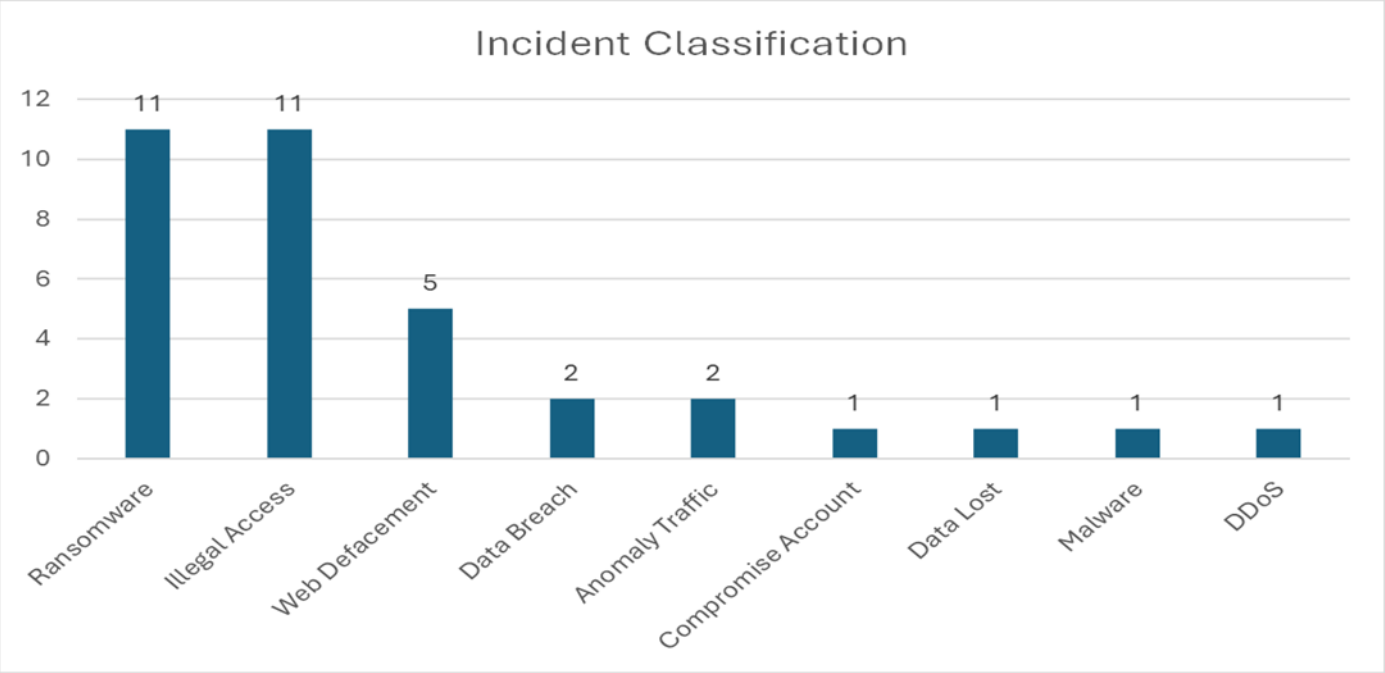


Figure 1. classification of incidents handled by Id-SIRTII/CC.

Among the 35 incidents handled in 2025, the most common cases included ransomware, illegal access, and web defacement, along with several other types of cyber incidents. One of the most significant threats identified was ransomware, a type of malware that encrypts critical data on infected systems and demands payment—often in digital currency—in exchange for restoring access. Such attacks can lead to financial losses, operational disruption, and reputational damage for affected organizations.

Lessons learned from ransomware incidents highlight the importance of strengthening initial access controls, monitoring endpoint activities, implementing network segmentation to prevent lateral movement, enforcing strict privilege management, and maintaining secure and regularly tested data backups. In addition, effective incident response requires clear procedures, continuous monitoring, and strong management support to ensure timely detection and coordinated

mitigation of cyber threats.

3.3 Abuse statistics

3.3.1 Anomaly Traffic Trend

The figure shows the monthly distribution of anomalous traffic detected in Indonesia throughout 2025. During the first quarter, the number of incidents fluctuated moderately before increasing significantly in April and reaching a peak in May with 755,639,091 incidents, the highest level recorded during the year, likely influenced by the global surge of Mirai Botnet activities. Following this peak, anomalous traffic gradually declined from June to September, with a slight increase observed in October before continuing to decrease toward the end of the year. The lowest level occurred in December, with 213,041,476 incidents, marking a substantial drop compared to the peak in May. Overall, Indonesia recorded 5,462,352,220 anomalous traffic incidents in 2025, indicating the continued presence of cyber threats targeting the country's internet infrastructure.

Such anomalous traffic can have several potential impacts, including network performance degradation, unauthorized access to sensitive information, operational disruption, and reputational damage to affected organizations. Therefore, continuous monitoring, threat intelligence sharing, and proactive mitigation measures remain essential to reduce the risks posed by large-scale cyber activities.

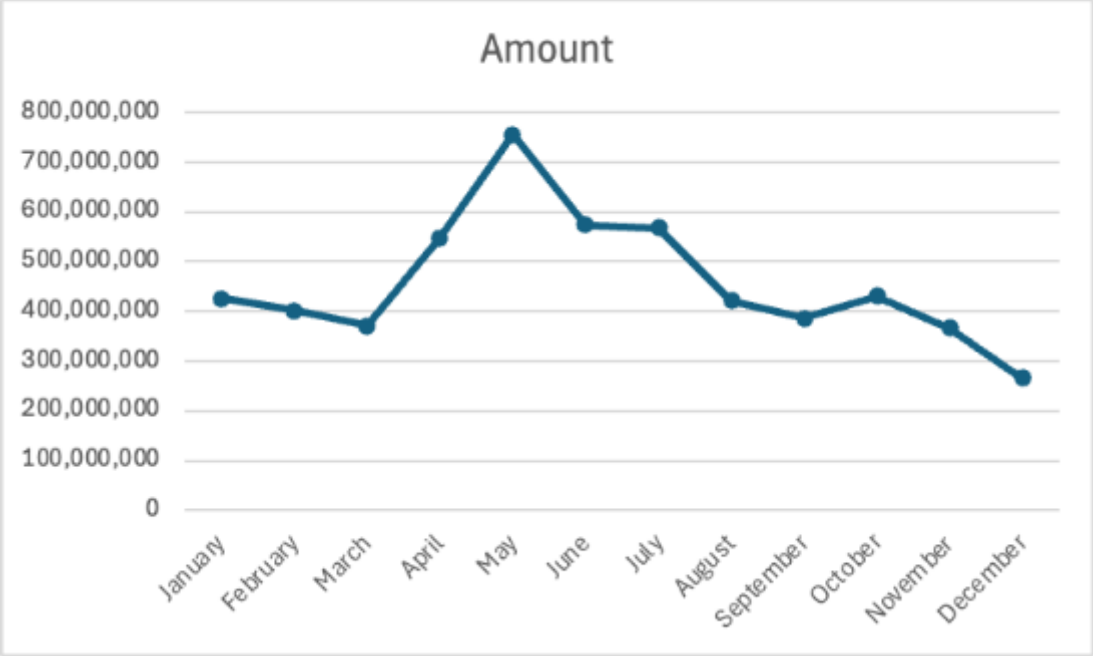


Figure 2. The number of traffic anomalies in Indonesia in a year.

3.3.2 Top 10 Anomaly Traffic

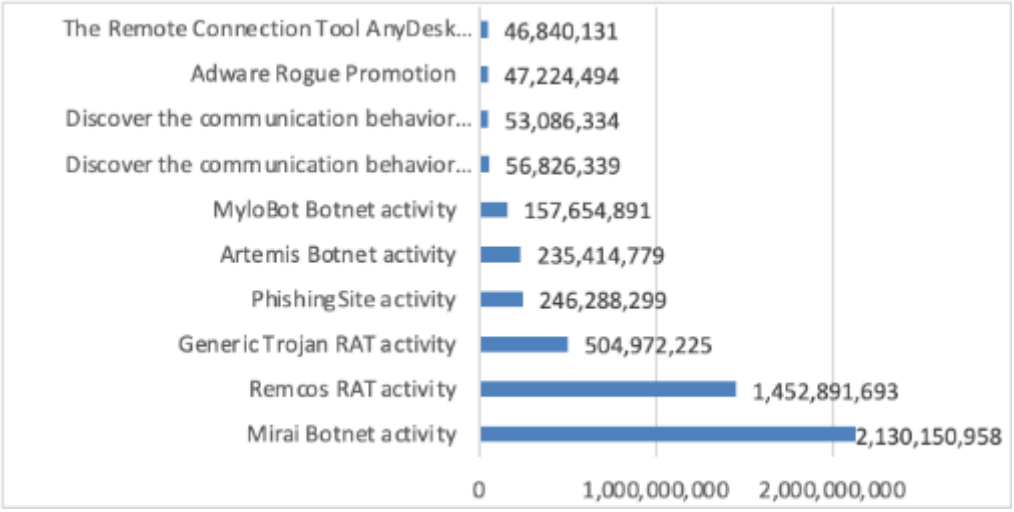


Figure 3. Top 10 traffic anomalies.

Cybersecurity monitoring during 2025 revealed several major threats affecting Indonesia's networks and information systems, particularly those linked to botnet and malware infections. The most prominent threats included Mirai Botnet, Artemis Botnet, and MyloBot Botnet, which exploit vulnerable devices and allow attackers to remotely control infected systems. These botnets are frequently leveraged to carry out Distributed Denial of Service (DDoS) attacks, distribute spam campaigns, exfiltrate sensitive information, and deliver additional malicious payloads. As a result, infected devices may experience performance degradation, increased exposure to data breaches, and involvement in large-scale cyber operations without the knowledge of their owners. Strengthening device configurations, applying regular software and firmware updates, using reliable security tools, and maintaining continuous network monitoring are essential to reduce these risks.

In addition, the monitoring activities identified credential-stealing and remote-access malware, such as Remcos RAT, Generic Trojan RAT, and phishing-related malware, which typically spread through deceptive emails, malicious files, or fraudulent websites. Once a device is compromised, attackers may obtain unauthorized system access, extract confidential data, record user activity, or alter system settings, potentially causing identity theft, financial loss, and operational disruption. Network observations also revealed the presence of tools and anomalies related to OpenVPN, WireGuard, AnyDesk, and adware campaigns, which, although sometimes legitimate, may be misused to disguise malicious communication channels or establish unauthorized remote connections. To minimize these threats, organizations are advised to adopt secure email handling practices, strict privilege management, routine security assessments, robust firewall policies, and network segmentation across their infrastructure.

3.3.3 Ransomware Activity

During the 2025 reporting period, monitoring activities detected approximately 13,915,440 ransomware-related incidents targeting Indonesian cyberspace. Ransomware is a type of malware that encrypts files or systems, preventing users from accessing their data until a ransom payment is made, typically in digital currency. These attacks can affect

individual users, private organizations, and government institutions, and may lead to data loss, financial damage, operational disruption, and reputational impact. As a result, ransomware continues to represent one of the most serious cyber threats to digital infrastructure and information systems.

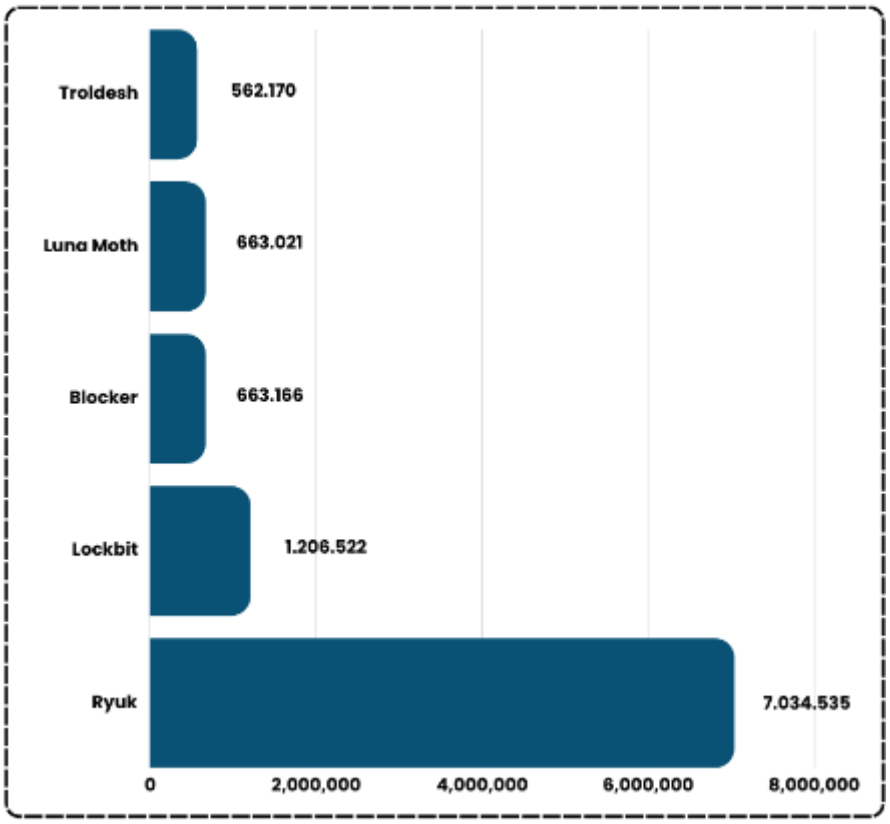


Figure 4. Top 5 most frequently detected Ransomware.

Analysis of the most frequently observed ransomware families shows that Ryuk was the dominant variant, with 7,034,535 detected incidents, accounting for about 50.5% of the total ransomware activity. Other ransomware families were identified at considerably lower levels, including LockBit (1,206,522 incidents), Blocker (663,166 incidents), Luna Moth (663,021 incidents), and Trolldesh (562,170 incidents). The large gap between Ryuk and the other variants suggests that Ryuk operators may have conducted more extensive campaigns or utilized more effective distribution methods compared to other ransomware groups detected during the year.

3.3.4 Phishing Activity

Phishing continues to be one of the most widespread cyberattack methods, relying on social engineering techniques to impersonate legitimate entities and deceive victims. These attacks are commonly delivered through emails, text messages, or fraudulent websites that contain malicious links or attachments. During 2025, monitoring activities identified approximately 246,288,299 phishing attempts targeting Indonesian cyberspace. Such attacks are particularly dangerous because they often function as an initial access vector, enabling attackers to install malware or obtain unauthorized access to systems and sensitive information.

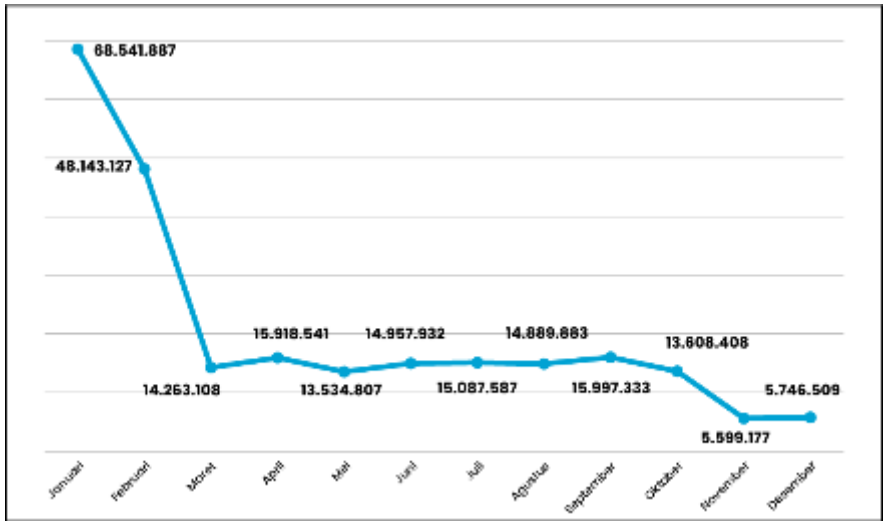


Figure 5. Monthly Report Phishing Distribution.

The monthly pattern of phishing activity shows significant variation throughout the year. The highest number of incidents occurred in January, reaching 68,541,887 cases, followed by February with 48,143,127 incidents, indicating a substantial surge in phishing activity at the beginning of the year. After February, the number of incidents dropped sharply in March to 14,263,108 and then remained relatively stable between 13–16 million cases per month until October. The lowest level was recorded in November, with 5,599,177 incidents, before experiencing a slight increase in December to 5,746,509 incidents.

3.4 Publications

Id-SIRTII/CC regularly produces and publishes a range of cybersecurity information products that serve as references for stakeholders across Indonesia. These publications include Cyber Blitz (cybersecurity news updates), monthly reports, annual reports, and security advisories, all of which provide important insights and guidance related to emerging threats, incident developments, and cybersecurity awareness.

3.4.1 Cyber Blitz

Cyber Blitz is a publication produced by Id-SIRTII/CC that delivers updates on global cybersecurity developments based on current and credible sources. The publication highlights topics such as international cyberattacks, major cyber incidents, emerging technologies, and newly discovered vulnerabilities, helping Indonesian stakeholders stay informed about trends in the global cybersecurity environment.

3.4.2 Monthly Reports

The monthly reports provide a summary of cyber incidents and attack activities detected in Indonesia. They also include information on regional and international engagements involving Id-SIRTII/CC personnel, as well as an overview of services and support provided to stakeholders during the reporting period.

3.4.3 Annual Reports

The annual reports present a comprehensive overview of cybersecurity conditions and developments in Indonesia over the course of the year, including key trends, activities, and strategic initiatives related to national cybersecurity.

3.4.4 Security Advisories

Security advisories are official alerts issued to notify stakeholders about newly discovered vulnerabilities, emerging threats, and other cybersecurity risks. These advisories typically outline the nature of the threat, affected systems, potential impacts, and recommended mitigation measures, enabling organizations and users to take prompt actions to strengthen their security posture and minimize cyber risks.

4. Events organized / hosted

4.1 Conferences and seminars

Id-SIRTII/CC actively organizes various cybersecurity events and knowledge-sharing activities to support capacity building and strengthen collaboration among stakeholders. In 2025, the following activities were organized:

- Implementation of the Sectoral Coordination Forum (2025)
- Financial Sector Cyber Incident Response Workshop (2025)
- Cybersecurity Information Sharing Analysis Forum (2025)
- Health Sector Cyber Security Drill (2025)
- Discussion Forum on CSIRT (4DESSERT) in 2025 (5 February 2025, 30 June 2025, 17 September 2025 and 13 November 2025)
- ITSHARE Level Up (18 June 2025)
- Uncovering Data Breaches: A Forensic Approach to Tracing the Attack (29 July 2025)
- Offensive Mobile Security: Advanced Penetration Testing for Mobile Applications (26 August 2025)
- Securing Digital Identities: The Role of Identity Brokers in Modern Cybersecurity (24 September 2025)
- Cyber Incident Handling Simulation Workshop for the Financial Sector Cyber Incident Response Teams (23 October 2025)
- Cyber Incident Exchange Forum (CIEF) (28 October 2025)
- Cyber Incident Preparedness Workshop for the Cyber Incident Response Team (28 – 29 October 2025)
- National Cybersecurity Connect 2025 (29 – 30 October 2025)
- OSINT/Dark Web Investigation: Cyber Threat Intelligence: Using OSINT & Dark Web Data for Security Operations (OIC-CERT) (30 October 2025)

5. International Collaboration

5.1 International partnerships and agreements

Id-SIRTII/CC promotes collaboration and trusted information exchange by establishing Memoranda of Understanding (MoUs) with cybersecurity partner organizations. In addition, Id-SIRTII/CC actively participates in international cybersecurity communities, including APCERT, FIRST, and OIC-CERT. Within OIC-CERT, Id-SIRTII/CC serves as the Deputy Chair and is responsible for leading the Cybersecurity Talent Development program.

5.2 Capacity building

5.2.1 Training

As part of its commitment to strengthening cybersecurity capacity and expertise, Id-SIRTII/CC actively participated in various international training and professional development programs. In 2025, Id-SIRTII/CC took part in the following activities:

- UNODC Validation Workshop for Cybercrime Legal Study (28 – 30 January 2025)
- AJCCBC Ensuring Cyber Resilience through Pre-Incident Response and Audit Activities Online 2025 (18 – 21 March 2025)
- AJCCBC Cybersecurity Technical Training - Network Forensics (19 – 23 May 2025)
- Covert Engagement Course Jakarta Centre Law Enforcement Cooperation (JCLEC) Online Training (16 – 20 June 2025)
- UNODC-IASC Digital Forensic and Evidence Training (12 –14 August 2025)
- AJCCBC Cybersecurity Technical Training Cyber Defense Exercise with Recurrence (CYDER) (17 – 23 August 2025)
- 2025 APISC Security Training Course (24 – 30 August 2025)
- Cybersecurity Expert Training Course (25 August – 3 September 2025)
- JP-US-EU Industrial Control Systems Cybersecurity Week (18 – 21 November 2025)
- AJCCBC Cybersecurity Technical Training Cyber Defense Exercise with Recurrence (CYDER) (23 – 29 November 2025)

5.2.2 Drills & exercises

To strengthen operational readiness and enhance international coordination in cyber incident response, Id-SIRTII/CC actively participated in various international cyber exercises and incident response drills. These activities provide opportunities to test response capabilities, improve cross-border coordination, and strengthen collaboration with global cybersecurity stakeholders. In 2025, Id-SIRTII/CC participated in several international cyber drills, including the following:

- International Telecommunication Union (ITU) Global Cyber Drill (6 – 8 May 2025)
- ASEAN Cyber Emergency Response Team Incident Drill (ACID) (21 – 22 October 2025)

5.2.3 Seminars & presentations

In order to strengthen international engagement and facilitate knowledge exchange on emerging cybersecurity issues, Id-SIRTII/CC participated in various regional and global conferences. These platforms provide opportunities to discuss evolving cyber threats and enhance collaboration with international stakeholders. In 2025, Id-SIRTII/CC participated in the following events:

- The Conference on Ransomware and Crypto Investigations in Southeast Asia and Cyber Games 2025 (19 – 23 May 2025)
- China–ASEAN Cybersecurity Seminar (17 – 30 June 2025)

6. Future Plans

National CSIRTs play a vital role in strengthening a country's cybersecurity posture by coordinating the prevention, detection, and response to cyber incidents at the national level. As cyber threats continue to grow in complexity and scale, a National CSIRT is expected not only to handle technical incidents but also to lead strategic initiatives that enhance national cyber resilience. These initiatives typically involve collaboration with government agencies, critical infrastructure operators, private sector organizations, and international partners. Through structured programs and coordinated activities, a National CSIRT can improve threat awareness, strengthen incident response capabilities, and support the overall security of national digital infrastructure. The programs include:

- Focusing on the early detection of national cyber threats.
- Strengthening CSIRTs across critical sectors.
- Building national cyber situational awareness.
- Improving national preparedness for large-scale cyberattacks through national cyber drills.
- Enhancing cybersecurity workforce capacity through online seminars and training.
- Reducing cyber risks affecting communities and organizations.
- Strengthening international cybersecurity cooperation.

7. Conclusion

Overall, the various cybersecurity activities conducted and participated in by Id-SIRTII/CC throughout 2025 demonstrate its strong commitment to strengthening cybersecurity capacity, enhancing operational readiness, and fostering international collaboration. Through participation in global cyber exercises, training programs, conferences, and self-organized initiatives, Id-SIRTII/CC continues to expand technical expertise, promote knowledge sharing, and strengthen partnerships with regional and international stakeholders. These efforts contribute to improving collective preparedness and supporting broader initiatives to enhance cybersecurity resilience at both the national and global levels.

JPCERT/CC

Japan Computer Emergency Response Team / Coordination Center

1. Highlights of 2025

1.1 Summary of major activities

JPCERT/CC continues contributions to global CSIRT communities

JPCERT/CC has been an active member in various global CSIRT communities. Among many communities of different scales and regions, APCERT and FIRST remain JPCERT/CC's top priority for collaboration with counterparts. In APCERT, JPCERT/CC has contributed to its activities in its role as Secretariat, for example supporting the conference host teams, assisting with the Working Group logistics and maintaining APCERT infrastructures such as websites and mailing lists. In 2025, JPCERT/CC was reelected as a Steering Committee member and reappointed as Secretariat.

With regards to FIRST, JPCERT/CC has also actively participated in various activities over the years including serving as conference speakers and participating in SIG discussions. Currently, a JPCERT/CC staff serves on the FIRST board and was reelected in 2025. JPCERT/CC has also actively assisted CSIRTs in Japan to become FIRST members.

JPCERT/CC considers that continuous participation in these international communities is pivotal in enhancing the collaboration among CSIRTs and will continue to further develop and deepen the global outreach.

1.2 Achievements & milestones

JPCERT/CC actively engages in CVD-related communities

JPCERT/CC has been working to streamline the global distribution of vulnerability information in its role as a Common Vulnerability and Exposure (CVE) Numbering Authority (CNA). While strengthening its collaboration with overseas counterparts, JPCERT/CC has also supported the stable operation of the CVE Program as a Root through initiatives such as encouraging product developers in Japan to become CNAs. In addition, JPCERT/CC has participated in the ISO/IEC JTC 1/SC 27 in international standardization efforts related to vulnerability handling and disclosure processes.

JPCERT/CC continues to work to further enhance vulnerability information distribution channels through activities to promote the CVE Program, including leading the CVD Working Group in APCERT.

2. About CSIRT

2.1 Introduction

JPCERT/CC is the first CSIRT (Computer Security Incident Response Team) established in Japan. It is an independent, non-profit organisation, serving as a national point of contact in the technical layer for CSIRTs in Japan and worldwide. After its inception in 1992, JPCERT/CC was officially established in 1996, and since then, the team has been conducting a variety of activities such as incident handling, vulnerability handling, malware and threat analysis, control system security, security alerts and advisories for the wide public, organizing forums and seminars for awareness raising, and supporting the establishment and operations of CSIRTs in both Japan and overseas.

2.2 Constituency

JPCERT/CC's constituencies cover overall Internet users in Japan with a focus on technical staffs of enterprises. JPCERT/CC also coordinates with network service providers, security vendors, government agencies, and industry associations in Japan.

3. Activities & Operations

3.1 Incident handling reports

In 2025, JPCERT/CC received 68,853 computer security incident reports from Japan and overseas.

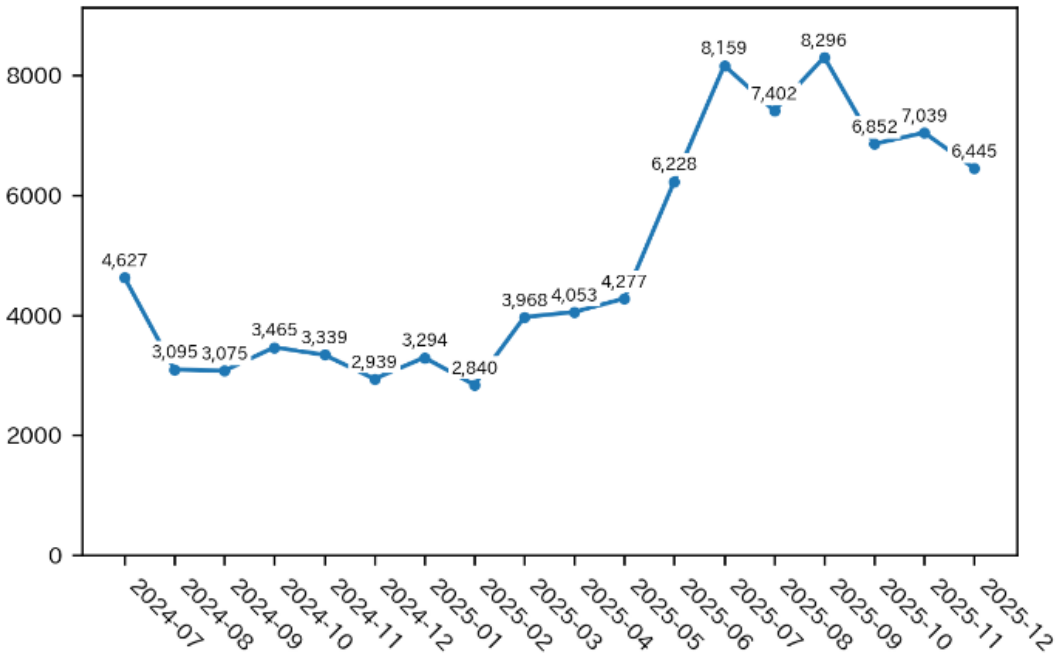


Figure 1. Number of Incident Reports per month

Source: JPCERT/CC Quarterly Report October 1, 2025 to December 31, 2025

(https://www.jpcert.or.jp/qr/2026/QR_FY2025-Q3.pdf)

3.2 Abuse statistics

Incidents reported to JPCERT/CC during the last quarter of 2025 were categorized in Figure 3. More than 90% of the reports were on phishing sites, followed by scan.

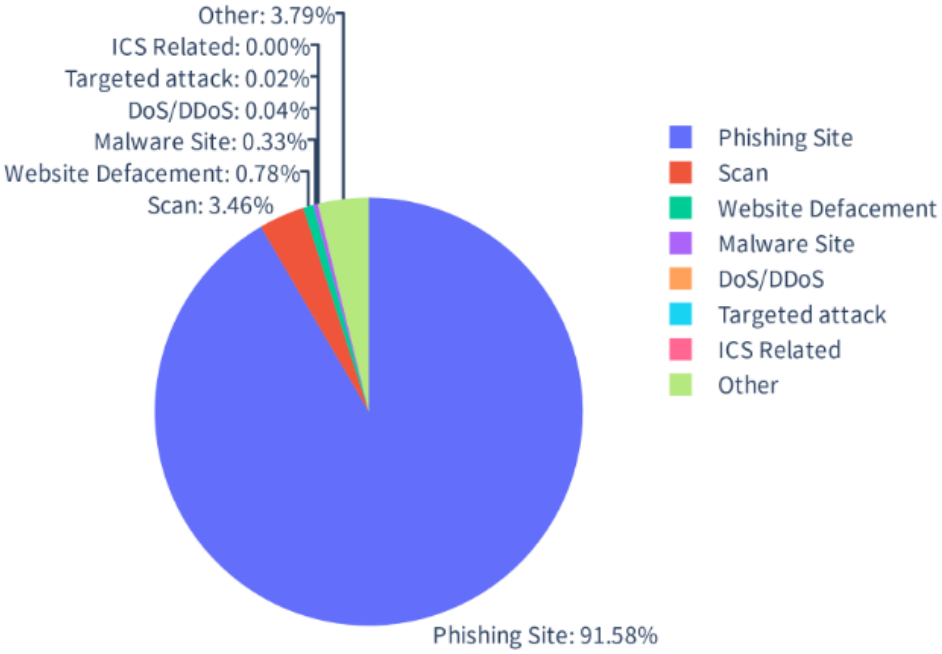


Figure 2. Abuse Statistics of Oct-Dec 2025

Source: JPCERT/CC Quarterly Report October 1, 2025 to December 31, 2025 (https://www.jpcert.or.jp/qr/2026/QR_FY2025-Q3.pdf)

3.3 Security Alerts, Advisories and Publications

Security Alerts

https://www.jpcert.or.jp/english/at/ (English)

JPCERT/CC publishes security alerts on widespread, emerging information security threats and their solutions. In 2025, 27 security alerts were published in Japanese, followed by 17 alerts in English.

Early Warning Information

JPCERT/CC publishes early warning information to many local organisations including the government and critical infrastructure operators through a dedicated portal site called "CISTA (Collective Intelligence Station for Trusted Advocates)." Early warning information contains reports on threats, threat analysis and countermeasures.

Japan Vulnerability Notes (JVN)

https://jvn.jp/en/ (English)

JVN is a portal site that provides vulnerability information and countermeasures for software products. JVN is jointly operated by JPCERT/CC and the Information-technology Promotion Agency (IPA) to provide descriptions, solutions, and developers' statements on vulnerabilities (including information on affected products, workarounds and solutions, such as updates, patches).

JPCERT/CC also directly receives vulnerability reports from overseas researchers and coordinates with the researchers

and developers with vulnerable products. Once solutions become publicly available, JPCERT/CC publishes advisories for the reported issues on JVN.

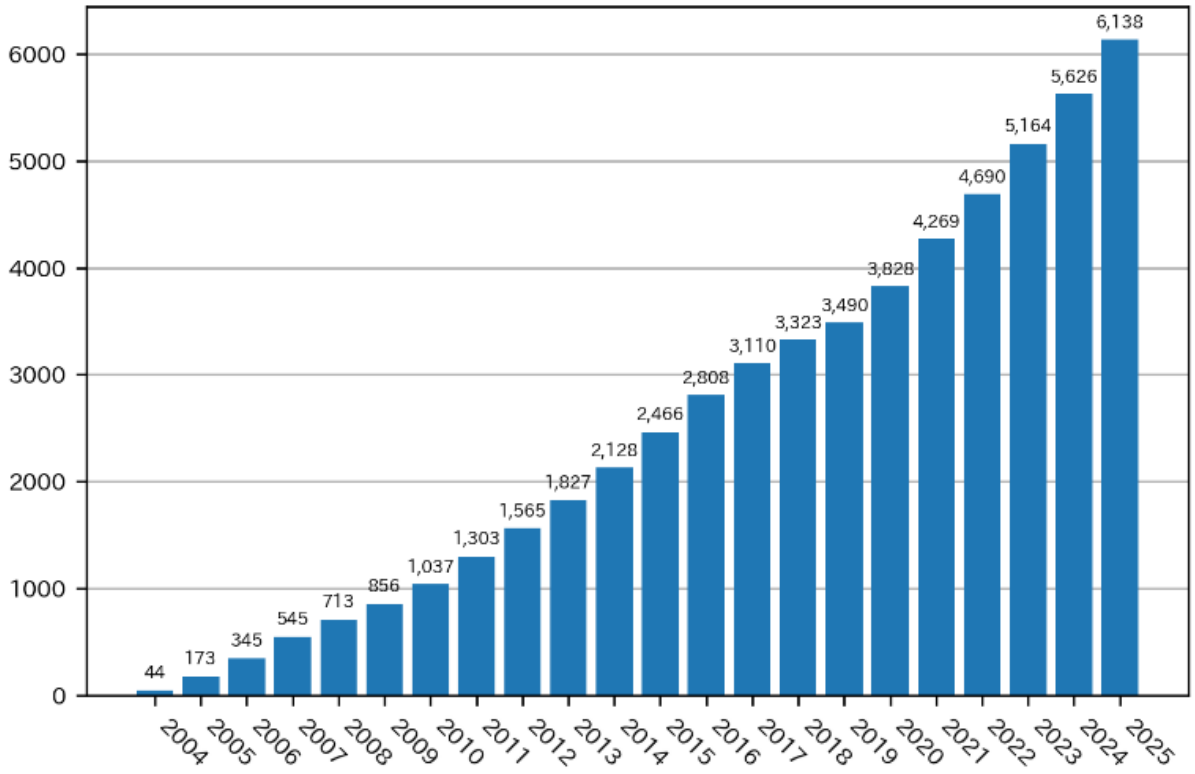


Figure 3. Cumulative Number of JVN Publications

Source: JPCERT/CC Quarterly Report October 1, 2025 to December 31, 2025

(https://www.jpcert.or.jp/qr/2026/QR_FY2025-Q3.pdf)

In June 2010, JPCERT/CC became a CVE Numbering Authority (CNA).

JPCERT/CC's Vulnerability Handling and Disclosure Policy is available here (English):

https://www.jpcert.or.jp/english/vh/2018/20180330-vulpolicy.pdf

Weekly Report

JPCERT/CC publishes weekly reports on selected security information of the preceding week, including a useful tip which is relevant to current issues. (Japanese only)

JPCERT/CC Eyes (Official Blog)

https://blogs.jpcert.or.jp/en/

Since September 2010, JPCERT/CC has been releasing blog posts to provide security news and technical observations related to Japan, as well as updates of international activities that JPCERT/CC engages in.

Quarterly Activity Reports

https://www.jpcert.or.jp/english/menu_documents.html

JPCERT/CC publishes quarterly activity reports and study/research reports both in Japanese and English.

X (Twitter)

https://x.com/jpcert_en

Since January 2009, JPCERT/CC has been providing Security Alerts, Blog updates, etc. via X (Twitter).

GitHub

https://github.com/JPCERTCC

JPCERT/CC's analysis tools and other resources are available on GitHub.

YouTube

https://www.youtube.com/@jpcert_cc

Some recorded presentations from our events as well as tool demonstrations are available on the YouTube channel.

3.4 Associations and Communities

Nippon CSIRT Association (NCA)

https://www.nca.gr.jp/en/index.html (English)

The Association is a community for CSIRTs in Japan. JPCERT/CC supports NCA as part of the founding members.

Council of Anti-Phishing Japan

https://www.antiphishing.jp (Japanese)

JPCERT/CC serves as the Secretariat for the Council of Anti-Phishing Japan.

4. Events organized / hosted

4.1 Training, Seminars and Workshops

JPCERT/CC offers trainings, seminars and workshops for technical staff, system administrators, network managers, etc. JPCERT/CC hosts two annual security conferences; the JSAC in January (since 2018) and the Control System Security Conference in February (since 2009). JSAC is open to the international cyber security community.

JSAC event website: https://jsac.jpcert.or.jp/

5. International Collaboration

5.1 International partnerships and agreements

MoU

To further strengthen the cooperation, JPCERT/CC exchanges a Memorandum of Understanding (MoU) with various security organisations.

FIRST (Forum of Incident Response and Security Teams)

https://www.first.org

JPCERT/CC contributes to the international CSIRT community FIRST, supporting CSIRTs who wish to become a member. JPCERT/CC has been supporting multiple organizations' membership application process.

APCERT (Asia Pacific Computer Response Team)

https://www.apcert.org/

Since its establishment, JPCERT/CC has been serving as a Steering Committee member and Secretariat, and the team is also the convener of the CVD Working Group.

5.2 Capacity building

5.2.1 Drills & Exercises

JPCERT/CC participated in the following drills in 2025 to review our incident response capability:

- Locked Shields 2025 (6-9 May)
- APCERT Drill 2025 (29 July)
- ASEAN CERTs Incident Drill (ACID) 2025 (21-22 October)

5.2.2 Seminars & presentations

In 2025, JPCERT/CC delivered presentations at international cyber security events including:

- CVE/FIRST VulnCon 2025 & Annual CNA Summit (April, Raleigh)
- FIRST Annual Conference (June, Copenhagen)
- Blackhat USA (August, Las Vegas)
- 2025 FIRST & AfricaCERT Symposium: Africa and Arab Regions (December, Mauritius)

5.2.3 Other international activities

In 2025, JPCERT/CC attended international cyber security events including;

- RightsCon
- APAC DNS Forum

- BotConf
- NatCSIRT Meeting
- RECON
- DEFCON
- HITCON
- OrangeCon
- VirusBulletin
- Singapore International Cyber Week
- M3AAWG

6. Future Plans

6.1 Future projects/Operation

Research on recent CVD-related topics aligned with the global trends

JPCERT/CC has been actively contributing to the global CVD community. In advancing these activities, JPCERT/CC plans to initiate several research projects on CVD-related topics. These will include new technical challenges, such as CVD processes for AI-related services, and global policy developments. JPCERT/CC aims to further strengthen its global outreach and collaboration with relevant stakeholders through these research activities and will remain committed to the CVD communities through continued discussions and active participation.

7. JPCERT/CC Contact Information

- URL: https://www.jpcert.or.jp/english/
- E-mail: global-cc@jpcert.or.jp
- Phone: +81-3-6271-8901
- Fax: +81-3-6271-8908

KrCERT/CC

Korea Internet Security Center, Korea Internet & Security Agency

1. Highlights of 2025

1.1 Summary of major activities

Incidents Involving Telecom Operators and a Large Retail Company and Response

In 2025, major cybersecurity incidents occurred involving mobile telecom operators and a large retail company in Korea. The public-private joint investigation team was formed and the team performed a central role throughout the response process. Within the investigation team, KrCERT/CC led practical investigative tasks including technical analysis, assessment of the scale of damage, and inspection of account management practices, thereby contributing to identifying the core nature of the incidents.

KrCERT/CC confirmed that the scale of data leakage was larger than initially reported by the companies and provided important grounds for clarifying victim protection and corporate responsibility. These investigation results led, together with the Ministry of Science and ICT(MSIT), to institutional improvements such as strengthening administrative fines for repeated incidents and imposing penalties for delayed reporting. KrCERT/CC also played a key role in preparing follow-up policy measures. Collaboration with external experts expanded investigative capacity and strengthened the information-sharing system between the government and the private sector.

At the APCERT Annual Meeting

Since being elected as Chair at the 2023 APCERT Annual General Meeting, KrCERT/CC has led the Steering Committee and contributed to activating the organization by hosting the APCERT Annual Cyber Drill and launching the APCERT Membership Awards.

Through the annual cyber drill, KrCERT/CC has taken the lead in strengthening member countries' response capabilities to cyber threats. At the 2025 AGM, as a follow-up activity to the annual cyber drill, a Table Top Exercise was conducted, providing an opportunity for member countries to understand each other's response systems and exchange experience. These activities were positively evaluated within APCERT and served as an opportunity to further solidify the foundation for international cooperation. In recognition of its leadership and contributions, KrCERT/CC received the Contribution

Award at the APCERT Membership Awards. This reflects the key role KrCERT/CC has played in APCERT operations over the past several years.

1.2 Achievements & milestones

Continuation of the "Phishing Zero" Project to Eradicate Phishing Incident

Centered on the Digital User Damage Response Division established within KrCERT/CC in 2024, the "Phishing Zero" project to eradicate phishing incidents has continued.

In 2025, in cooperation with specialized institutions in the financial and gambling sectors (Financial Supervisory Service and Korea Racing Authority), KrCERT/CC analyzed types of financial fraud and illegal gambling messages, extracted blocking keywords, collected gambling-related phone numbers and URLs, and strengthened blocking measures by filtering at the sending stage or suspending phone numbers to prevent the spread of malicious messages.

In addition, in cooperation with Samsung Electronics, AI training data collected and analyzed by KrCERT/CC was shared. Based on this data, Samsung developed and deployed a malicious message filtering service on Samsung devices beginning in March 2025.

To fundamentally prevent SMS phishing (Smishing), KrCERT/CC established the "Smishing Pre-Blocking System X-ray Service." This service automatically detects and blocks messages containing suspected smishing phrases at the sending stage so that only normal messages are delivered.

Previously, blocking occurred only after the recipient reported or verified the message. With the introduction of X-ray, blocking is possible before the sending stage, significantly improving prevention effectiveness. Since April 2025, pilot operation has been conducted for message-sending companies wishing to adopt the system, and MSIT and KrCERT/CC are promoting expansion of the service.

Strengthening Security Management in Areas Closely Related to Daily Life – Development of "Security Vulnerability Cleaning"

KrCERT/CC is operating a pilot "Security Vulnerability Cleaning Service," which detects vulnerable software on user PCs in connection with antivirus software and guides users to update to the latest version in which vulnerabilities have been removed.

Previously, even if software manufacturers distributed security patches, users had to manually confirm and apply them, resulting in low patch application rates and exposure to hacking threats. The Security Vulnerability Cleaning Service supports removal of vulnerable software or application of the latest security patches without requiring installation of additional programs. The service is provided in cooperation with four Korean antivirus companies and is being promoted with the goal of official launch in the first quarter of 2026.

Telecom Incident Response and Full-Scale Operation of the Public-Private Joint Investigation Team

In response to a cybersecurity incident at a major mobile telecom operator in 2025, KrCERT/CC identified the cause and scale of damage through technical analysis including malware analysis, digital forensics, system vulnerability assessment, and traffic pattern analysis.

In Company A's case, a comprehensive and detailed inspection of approximately 42,000 servers confirmed that 28 servers were infected with malware. During this process, 33 types of malware including BPFDoor were discovered. Some of the infected servers were part of the core subscriber authentication system, and approximately 26.96 million USIM data records were confirmed to have been leaked externally.

Following this incident, security inspections were conducted for major domestic platform companies. Malware secured during the investigation was shared with public and private sectors. In addition, a BPFDoor inspection guide was published to allow companies to independently check for impact.

Subsequently, Company B also experienced a cybersecurity incident. An event initially mistaken for simple smishing was confirmed to involve illegally installed large-scale base stations (femtocells) that captured users' IMSI information and induced small-amount payment fraud. Traffic pattern analysis revealed abnormal traffic concentrated in specific regions, different from normal payment flows, confirming that the incident was not a simple device infection but a compromise of network infrastructure. Victims and financial damages were confirmed, and the telecom operator was required to submit recurrence prevention measures and an implementation plan, and reinforcement of identified vulnerabilities was demanded.

Use of AI Technology

To overcome limitations in defensive resources against large-scale and AI-based attacks, KrCERT/CC is building a trustworthy AI-based incident response system. AI continuously analyzes phishing websites, identifies impersonation attempts at the source, and cross-verifies detection results with domestic and international threat intelligence in real time.

After transitioning to an AI-based malicious domain detection system, phishing infrastructure used by specific hacking groups for account theft was detected, and related information was provided to law enforcement authorities. Compared to 2024, malicious domain detection and response increased by 43% in 2025.

AI technology has reduced routine workload for incident analysts and improved operational efficiency. The analysis process was divided into four stages—collection, analysis, tracking, and removal—and AI was applied to extract attack features, analyze malware types and functions, analyze correlations between threat intelligence, automatically update attacker group information, and draft threat analysis reports. This reduced repetitive work and allowed analysts to focus more on detailed analysis of high-risk incidents.

2. About CSIRT

2.1 Introduction

The Korea Computer Emergency Response Team/Coordination Center (KrCERT/CC) is the national CSIRT of Korea, which is responsible for the private sector. Formed under the Korea Internet & Security Agency (KISA), KrCERT/CC is composed of three divisions with eleven teams. KrCERT/CC carries out various responsive and preventive programs designed to minimize cybersecurity damage by enabling prompt response to incidents and to increase awareness in order to prevent incidents.

2.2 Establishment

KrCERT/CC was established in 1996 as a small team responsible for hacking incidents under the Korea Information Security Agency (a former KISA). Since its foundation, it has responded to and handled numerous security issues and tasks. The first major incident was the Internet Crisis caused by so-called 'slammer worm' in 2003. At that time, KrCERT/CC had difficulties in communicating efficiently with a telecommunication carrier, which marked the turning point for the Korean Government to recognize the importance of cooperation with security incident response teams and businesses such as ISP. As a result, the Security Incident Response Team was established under the former KISA in December 2003 and has evolved into its current form by responding to major national security incidents that occurred in 2007, 2009 and 2013. Domestically it is usually called KISC, or the Korea Internet Security Center.

2.3 Constituency

KrCERT/CC serves as the focal point to coordinate security incidents in the Korean cyberspace. According to the national cyber security framework and related legislation, KrCERT/CC is responsible for handling incidents and ensuring the security of information systems and networks in the private sector, such as the telecommunication sector and home users. At the international level, KrCERT/CC cooperates with many leading and national CERTs/CSIRTs, international organizations, and security vendors.

3. Activities & Operations

3.1 Scope and definitions

KrCERT/CC works for safe, reliable cyber space by preventing cyberattacks and enhancing countermeasures. Its mission is to guarantee rapid response to major nationwide Internet incidents to prevent and minimize damages and to cooperate closely with domestic (ISPs, antivirus companies) and foreign partners (FIRST, APCERT, TF-CSIRT, etc.) in 24/7 Monitoring, Early Detection/Response with regard to cyberattacks in the private sector.

3.2 Abuse statistics

According to Article 48-3 of the Information and Communications Network Act, KrCERT/CC receives incident reports from private-sector information service providers.
Reported incidents increased from 1,887('24) to 2,383('25), a 26.3% increase.

Type	2023Y	2024Y	2025Y
DDoS	213	285	588
Malware Infection (Ransomware)	300 (258)	229 (195)	354 (274)
Server Hacking	583	1,057	1,053
Others	181	316	388
Total	1,277	1,887	2,383

3.3 Publications

In 2025, KrCERT/CC published:

- 2 Cyber Threat Trend Reports
- 5 Technical Reports
- 8 Security Guidelines

All publications are available at www.boho.or.kr

4. Events organized / hosted

4.1 Drills & exercises

Private-sector Cyber Crisis Response Drills (twice annually)

4.2 Other activities

Bug Bounty Awards Ceremony
CISO Best Practice Awards

5. International Collaboration

5.1 Capacity building

5.1.1 Training
APISC training for APCERT member economies

5.1.2 Drills & exercises
APCERT Table Top Exercise

5.1.3 Seminars & presentations
Ransomware case presentation for APCERT members
Presentation at APCERT Closed Conference on safe AI service operation

6. Future Plans

To address delays in incident reporting and evidence collection during major incidents, KrCERT/CC is promoting the introduction of special judicial police authority to address the issue of delayed reporting by companies during major incidents, which leads to expansion of damage and delay in securing evidence. In consultation with MSIT and the Ministry of Justice, procedures are underway to complete institutional introduction in the first half of 2026, and the President and relevant ministries recognize its necessity. Based on this authority, KrCERT/CC plans to enable compulsory evidence collection and rapid investigation at the initial stage of incidents, establish an advanced forensic laboratory, and expand personnel to strengthen investigative capability.

7. Conclusion

Although 2025 was a challenging year due to overlapping and consecutive large-scale incidents, KrCERT/CC achieved improvements in related systems and rapid application of AI technologies. By serving as a central axis of technical investigation and policy linkage within public-private joint investigation teams, KrCERT/CC went beyond simple incident response and contributed to strengthening the security management system of national core communication infrastructure and driving institutional change.

In addition, the contributions and efforts of KrCERT/CC in strengthening regional cybersecurity through APCERT were recognized through the APCERT Membership Awards, making the year even more meaningful.

KrCERT/CC will continue to make its best efforts for its constituency.

LaoCERT

Lao Computer Emergency Response Team

1. Highlights of 2025

1.1 Summary of major activities

- Co-host The 2025 1st ASEAN-Japan Cybersecurity Working Group Meeting on 18 to 19 February 2025 in Vientiane, Lao PDR, cooperate with National center of Incident readiness and Strategy for Cybersecurity (NISC) of Japan and participate from ASEAN Member States and Japan to discuss and sharing to develop on the cybersecurity matters and working together to strengthen public-private partnerships
- Co-Organized Ransomware Workshop: Using the NIST CSF Profile & Leading Practices with MITRE Cooperation and United State Embassy on 10-12 September 2025, Vientiane Capital, Lao PDR, which participate from all related public and private sector
- Co-Chair The 18th ASEAN Japan Cybersecurity Policy Meeting and Table Top Exercise on 7-9 October 2025 in Tokyo, Japan, Host by National Cybersecurity Office of Japan

1.2 Achievements & milestones

- Completed The Cyber Security Law issued by 2025
- Disseminated the use of social media security in Vientiane Capital and provincial
- Completed the National Cybersecurity Strategy

2. About CSIRT

2.1 Introduction

Lao Computer Emergency Response Team (LaoCERT) is the national CERT of Lao PDR, under, Ministry of Technology and Communications and it develop on capacity building for its staffs in the field of cyber security with other CERTs

organizations in the region to against with cyber-attack. LaoCERT has been promoted to public and has been known among IT social, government agencies, private organizations in Laos PDR as well as international CERTs and LaoCERT was a member of APCERT in 2014. This annual report will describe activities and operation of LaoCERT in 2025.

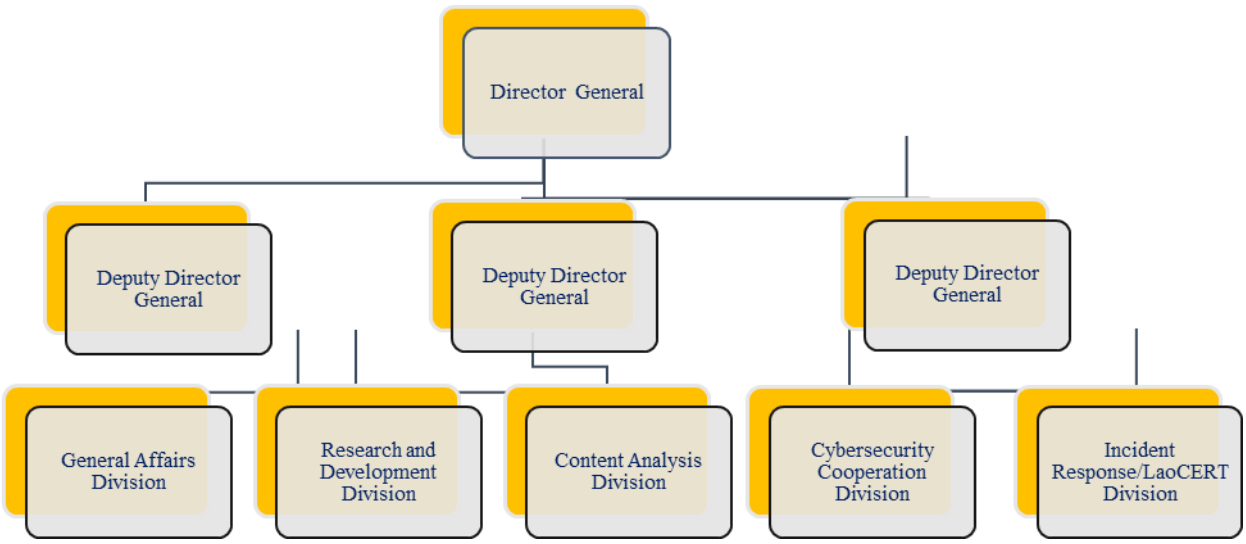
2.2 Establishment

LaoCERT was established in February 2012 by degree 220/MPT as a LaoCERT division under the Lao National Internet Center, Ministry of Post and Telecommunications (MPT), Government of Lao PDR. It was established by following up as ITU-IMPACT recommendations and it has been announced to become the national CERT equivalent department in 2016, directly under the Ministry of Post and Telecommunications.

Currently, the Ministry of Post and Telecommunications has been renamed the Ministry of Technology and Communications and also LaoCERT has been promoted to become the Department of Cyber Security under the Ministry of Technology and Communications (MTC).

2.3 Resources

Department of Cyber Security/LaoCERT currently consist of 5 divisions which control by 1 director general and 3 deputy director generals with the total number of staffs: 28 people, 07 are women.



Department/LaoCERT Organization Charts

2.4 Constituency

Department of Cyber Security/LaoCERT is a coordination center of cyber security within Laos and also cooperation with international CERT organizations in the field of cyber security. Department/LaoCERT is responsible for incident handling,

cyber security protection, disseminating information security and awareness raising for ensuring the cyber safety to all citizens, government agency and private organizations include education institute, banks, internet service providers, etc. in Lao PDR.

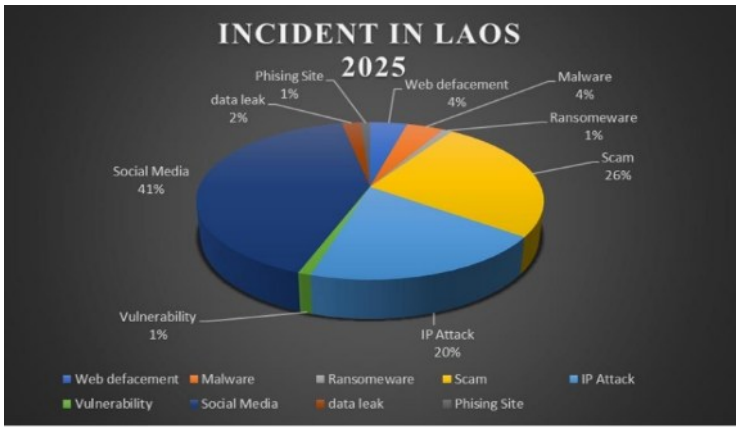
3. Activities & Operations

3.1 Scope and definitions

Department of Cyber Security/LaoCERT aim to raise awareness on cyber security and solving issue on cyber security incident response as well as to collaboration with other CERT organizations to against with cyber-attack.

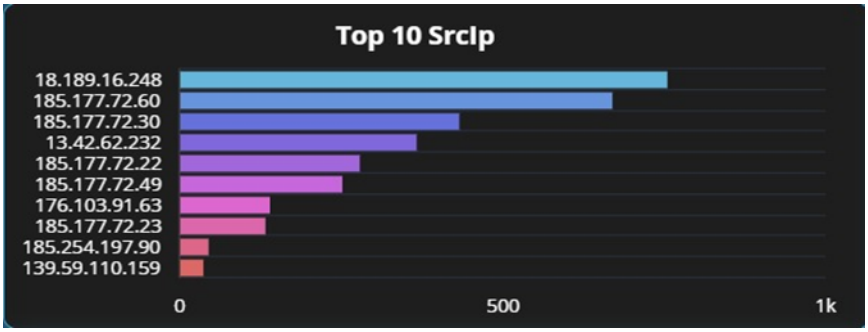
3.2 Incident handling reports

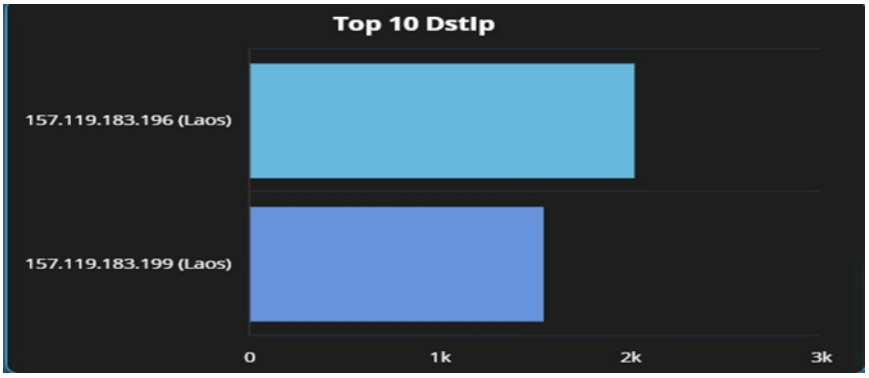
The following graph shows the statistic of incidents that happened in 2025.



3.3 Abuse statistics

The following graph shows Abuse Statistics in 2025:





3.4 Publications

- Website: www.laocert.gov.la
- E-mail: admin@laocert.gov.la
- Tel: +85621 254508 (08:00-16:00) Working hour
- Incident report: report@laocert.gov.la

3.5 New services

- Website vulnerability scanning
- Advisory on the use of Social Media Security
- Awareness raising on Cyber security to society
- Provide training related cyber security
- Monitoring Government Network

4. Events organized / hosted

4.1 Training

- Organized Workshop on cyber security prevention on 23-29 February 2025 in provincial, Lao PDR
- Co-Organized Training with CyberCX Company (Australia) on Cyber Security Incident Response on 23-26 June 2025 in Vientiane Capital, Lao PDR
- Co-Organized Training with Cyberus Company on Lao Cybersecurity Conference on 31 October 2025 in Vientiane Capital, Lao PDR

4.2 Drills & exercises

- Organized Lao Cyber Security Hacking Challenge with Cyberus Company in Vientiane, Lao PDR

4.3 Conferences and seminars

- Co-host The 2025 1st ASEAN-Japan Cybersecurity Working Group Meeting on 18 to 19 February 2025 in Vientiane, Lao PDR, cooperate with National center of Incident readiness and Strategy for Cybersecurity (NISC) of Japan and participate from ASEAN Member States and Japan to discuss and sharing to develop on the cybersecurity matters and working together to strengthen public-private partnerships
- Co-Organized Ransomware Workshop: Using the NIST CSF Profile & Leading Practices with MITRE Cooperation and United State Embassy on 10-12 September 2025, Vientiane Capital, Lao PDR, which participate from all related public and private sector
- Co-Chair The 18th ASEAN Japan Cybersecurity Policy Meeting and Table Top Exercise on 7-9 October 2025 in Tokyo, Japan, Host by National Cybersecurity Office of Japan

5. International Collaboration

5.1 Capacity building

5.1.1 Training

The following has shown the statistic for attended the training in 2025:

- The 34th AJCCBC Technical Cybersecurity Training-J11" (CYDER and Malware Analysis) from 13-17 January 2025 in Bangkok, Thailand

- The 35th AJCCBC Technical Cybersecurity Training-J12" (Penetration Test) from 17-21 February 2025 in Bangkok, Thailand
- The 36th AJCCBC Technical Cybersecurity Training-J13" on Expert Training in Network Forensics from 19-23 May 2025 in Bangkok, Thailand
- The Executive Course on the Application of International Law in Cyberspace for ASEAN Member State from 30 June to 3 July 2025 in Singapore
- The 36th AJCCBC Technical Cybersecurity Training-J13" on Operational Technology (OT) and Security Training from 21-25 July 2025 in Bangkok, Thailand
- The 2025 Singapore-Industrial Control Systems Cybersecurity 301 (SG-ICS301) course from 28July-1 August 2025 in Singapore
- The 38th AJCCBC Technical Cybersecurity Training- J15 (CYDER on New scenario & Malware Analysis) from 17-21 August 2025 in Bangkok, Thailand
- The 2025 APISC Security Training Course from 25 29 August 2025, in Seoul, Korea
- The 10th Singapore International Cyber Week (SICW) and the 10th ASEAN Ministerial Conference on Cybersecurity (AMCC) from 20-23 October 2025 in Singapore
- The 39th AJCCBC Technical Cybersecurity Training- J16 (Advanced Malware Analysis) from 24-28 November 2025 in Bangkok, Thailand
- SIN-AUS Joint Training Programme on Cyber Incident Preparedness and Response from 10 to 14 November 2025 in Singapore
- The Global Cyber Policy Dialogues: Southeast Asia from 19-21 November 2025 in Singapore

5.1.2 Drills & exercises

The following has shown the statistic for participated Drills and Exercises in 2025:

- APCERT Cyber Drill 2025
- ASEAN CERT Incident Drill (ACID) 2025
- The 3rd ASEAN Cyber Shield (ACS) Hacking Contest from 18-21 November 2025 in South Korea
- Capture the Flag (CTF) 2025 an annual cybersecurity competition on 15 September 2025 in Brunei
- Cyber SEA Game on 16-17 October 2025 in Bangkok, Thailand
- The 2025 Regional CyberDrill for Asia and the Pacific Region, from 2 to 5 September 2025, in Ulaanbaatar, Mongolia

5.1.3 Seminars & presentations

The following has shown the statistic for participated the Seminar, Workshop and Meeting in 2025:

- The Workshop for the 15th ASEAN-Japan Information Security Workshop for ISPs on 5-6 March 2025 in Tokyo, Japan
- The 2nd ASEAN-Japan Cybersecurity Working Group Meeting on 27-28 May 2024 in Philippine
- The ASCCE-MS Cybersecurity Roundtable on AI for ASEAN Member States on 19-20 June 2025 in Singapore
- The Mekong–Korea Cooperation Forum on 14 May in Hanoi, Viet Nam
- The Asia-Pacific Digital Transformation Forum 2025 from 24-28 June 2025 in Philippine

- The 3rd ASEAN-Japan Cybersecurity Working Group Meeting and CIIP Workshop on 5-7 August 2025 in Jakarta, Indonesia
- The 18th ASEAN-Japan Cybersecurity Policy Meeting on 7-9 October 2025 in Tokyo, Japan
- The ASEAN-Australia Workshop on Implementing Norms, Rules and Principles of Responsible State Behaviors in Cyberspace on 26-27 February 2025 in Malaysia
- The Conference on Ransomware and Crypto Investigation in Southeast Asia and Cyber Games 2025 from 19-23 May 2025 in Malaysia
- The World Internet Conference Asia-Pacific Summit and China-ASEAN Network Security Emergency Response Capacity Building Seminar on 14-15 April 2025 in Hongkong
- The 16th meeting of the ASEAN Network Security Action Council (ANSAC) on 9 June 2025 in Siem Reap, Cambodia
- The ASEAN-Australia Cyber Policy Dialogue on 2 July 2025 in Malaysia
- The ASEAN 5G & OT Security Summit from 15-17 July 2025 in Kuala Lumpur, Malaysia
- The 2nd ASEAN Regional Computer Emergency Response Team (CERT) Taskforce (ARCTF) Meeting on 26 August 2025 in Singapore
- The 5th Russia-ASEAN Dialogue in ICT Security-Related Issues from 23-24 October 2025 in Sochi, Russian Federation
- The Mekong-Lancang Cybersecurity Forum and Cyber-Drill on 12–13 November 2025 in Siem Reap, Cambodia
- The JP-US-EU Industrial Control Systems Cybersecurity Week for the Indo-Pacific Region from 18-21 November 2025 in Tokyo, Japan
- The 2025 APCERT Annual General Meeting and Conference 25-27 November 2025 in Sydney, Australia

6. Future Plans

- Continue to provide training and seminar on Cybersecurity to province both public and private sector throughout the country
- Continue to collaboration to exchange the lessons and experiences on the development of legislation, laws and information on developing an online social media management system among National CERT, international organization and related sectors in the field of cybersecurity
- Drafting the legislations under the Cybersecurity Law that was issued in 2025
- Revised Cyber Crime Law and data protection Law
- Establish a Cyber Security Operations Center (SOC)
- Planning for Establishing Government Threats Monitoring (GTM)
- Planning to set up the Network Monitoring System

7. Conclusion

The Department of Cyber Security/Lao Computer Emergency Response Team (LaoCERT) continues to develop its team by enhancing both the quality and quantity of its technical capabilities. The focus remains on incident handling, network security, cybersecurity legislation development, and strengthening cooperation with domestic and international cybersecurity organizations. These efforts aim to promote and organize cybersecurity initiatives, including workshops, seminars, and training programs. Additionally, The Department of Cyber Security/LaoCERT seeks to strengthen cooperation and work closely with regional and international organizations to further enhance the technical capabilities of its staff through knowledge exchange, training programs, and capacity-building initiatives. In addition, the Department is committed to raising public awareness of cybersecurity laws, regulations, and policies, as well as promoting best practices for the secure use of social media platforms and computer networks. Through these efforts, the Department seeks to foster a safer and more resilient digital environment, reduce cybersecurity risks, and effectively prevent and respond to potential cyberattacks.

mmCERT

Myanmar Cyber Emergency Response Team

1. Highlights of 2025

1.1 Summary of major activities

During 2025, a series of cybersecurity training programmes and technical webinars were attended to strengthen professional knowledge and operational capabilities in cyber security. These activities covered key areas such as cyber threat intelligence, incident response using artificial intelligence, vulnerability management, and malware analysis techniques. Participation in regional capacity-building initiatives organized by international and regional organizations, including ITU, APCERT, SingCERT, contributed to enhanced technical competencies and awareness of emerging cyber threats. The trainings also provided opportunities to gain practical insights into regional cyber threat landscapes and best practices in cybersecurity management, particularly within the ASEAN context. Overall, these engagements supported continuous professional development and improved readiness to address evolving cybersecurity challenges.

1.2 Achievements & milestones

- Cyber Security Law was enacted on 1st January 2025 and came into force on 30th July 2025.
- Myanmar Cyber Security Challenge 2025 (Open Level) was successfully conducted on 29th August 2025.
- Cyber Security Awareness Video Competition (University Level) was successfully conducted in June and July 2025.

2. About CSIRT

2.1 Introduction

Myanmar Cyber Emergency Response Team (mmCERT) is the national cyber emergency response team of Myanmar responsible for handling cyber security incidents in the country. It became an operational member of APCERT in 2011.

2.2 Establishment

The Myanmar Cyber Emergency Response Team (mmCERT) was initially established as the e-National Task Force on July 23, 2004. Subsequently, on December 15, 2010, mmCERT was formally established under the Ministry of Communications and Information Technology.

On April 1, 2015, it was reorganized as a division named the Myanmar Computer Emergency Response Team under the Information Technology and Cyber Security Department within the Ministry of Communications and Information Technology.

Following an organizational restructuring on July 28, 2025, it was reestablished as the Myanmar Cyber Emergency Response Team division under the Information Technology and Cyber Security Department.

2.3 Resources

All of mmCERT members are recruited by Ministry of Transport and Communications (MOTC). The operation of mmCERT was directly managed by the Director of mmCERT under Information Technology and Cyber Security Department (ITCSD). As the human resources of mmCERT are limited to handling cyber issues at present, it is under process to recruit more professionals.

2.4 Constituency

Since its establishment, mmCERT has been responsible for handling cyber security incidents, disseminating security information and advisories, as well as providing technical assistance to government agencies, telecom operators, internet service providers (ISPs), universities, and individual users in Myanmar. We also have plans to expand the constituency to include Critical Information Infrastructure (CII) sectors in the country.

3. Activities & Operations

3.1 Scope and definitions

- Incident Handling and Response: Identifying, managing, and resolving cyber security incidents in order to minimize damage, restore normal operations, and prevent future incidents.
- Cyber Security Awareness: Conducting awareness raising activities to ensure that individuals have knowledge to understand about emerging cyber threats, online scams and safe online practices, helping them recognize, avoid, and respond to security risks.
- Capacity Building: Developing skills, resources, policies, and infrastructure to improve the CERT's ability to prevent,

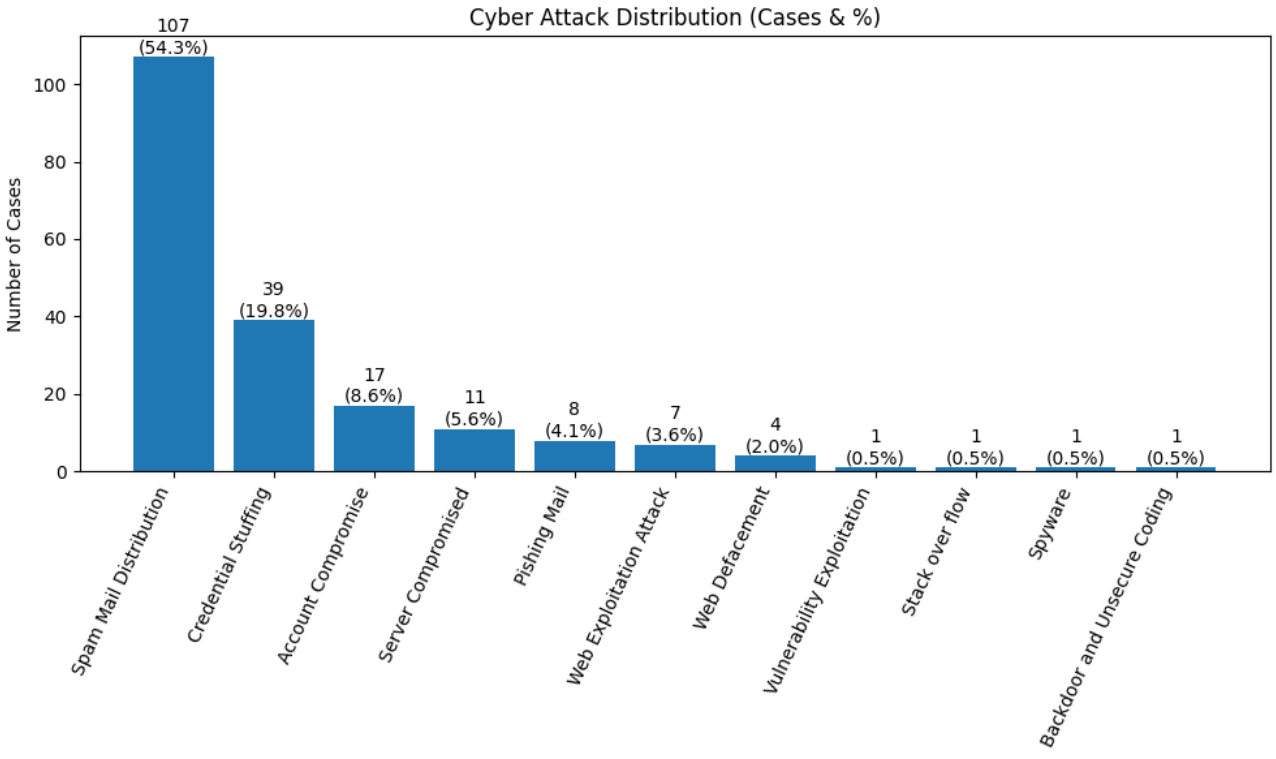
detect, and respond to cyber threats.

- International Relation: Participating in the regional and international cybersecurity cooperation activities to improve cybersecurity resilience and maintain a safe, secure, and stable cyberspace.
- Technical Assistance and Advisory Services: Provides technical support, guidance, and professional assistance to organizations and stakeholders in addressing cybersecurity incidents.

3.2 Incident handling reports

There has been a noticeable shift in cyber incident trends compared with the previous year. While DDoS attacks and Account Compromise incidents were the most dominant threats previously, the current year shows a significant rise in Spam Mail Distribution and Credential Stuffing incidents, indicating a growing use of large-scale and automated attack techniques. Other incidents such as Web Exploitation, Phishing, and Server Compromise continue to be reported at moderate levels, reflecting the persistence of traditional cyber threats. These trends highlight the need for strengthened preventive measures, enhanced user awareness, and closer coordination among organizations to effectively mitigate the evolving cybersecurity risks.

The following graph shows the incidents handled by mmCERT in 2025:

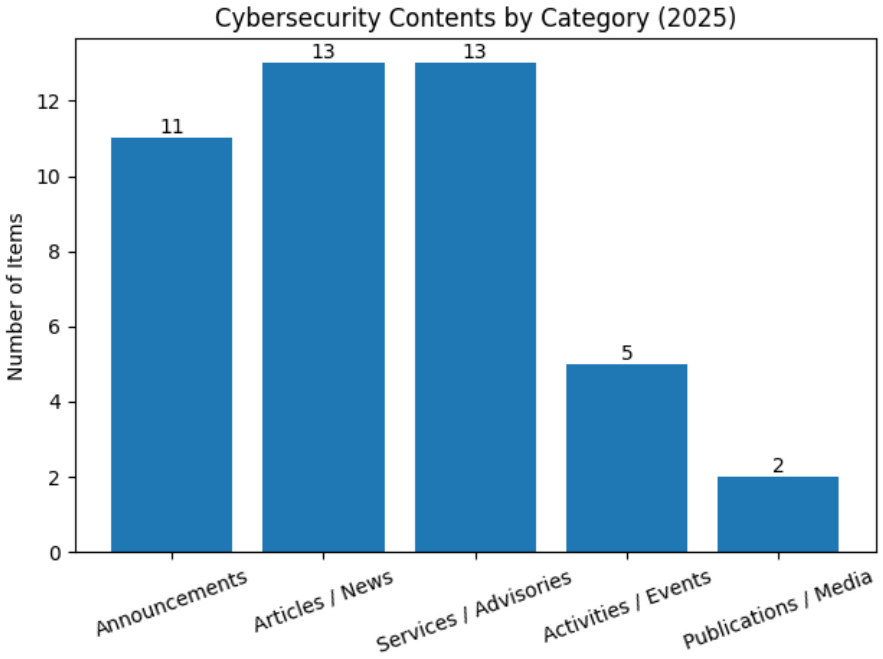


3.3 Publications

In 2025, mmCERT carried out a range of publication activities to improve cybersecurity awareness and share important information with the public and relevant organizations. Throughout the year, mmCERT regularly published news articles and information updates to highlight current cyber threats, major cyber incidents, and global cybersecurity developments. These publications helped readers better understand the changing of cyber threat environment.

mmCERT also issued several technical advisories and awareness materials to inform users about cybersecurity best practices, newly identified system vulnerabilities, and recommended preventive measures. These efforts supported individuals and organizations in strengthening their security readiness and protecting their digital systems.

In addition, selected awareness publications and media content were released to encourage safe and responsible use of digital technologies. Overall, mmCERT's publication activities in 2025 contributed to increasing cybersecurity knowledge, promoting preventive actions, and supporting national efforts to improve cybersecurity awareness. Further details of the publications are provided in the graph and table below.



No	Date	Title (English Translation)
1	1/3/2025	Announcement on application for "The 3rd ASEAN Cyber Shield Online Education Program"
2	1/28/2025	What are Cybersecurity Best Practices?
3	1/28/2025	Announcement to Check whether Passwords Have Been Compromised
4	1/28/2025	Second Meeting of BIMSTEC Expert Group on Cyber Security Cooperation, India
5	1/28/2025	Seminar on "Cybersecurity in the Digital Age", Ministry of Transport and Communications

6	1/30/2025	Capacity Building Training (1/2025), Department of Information and Public Relations
7	2/13/2025	DeepSeek Exposed a Database Containing Over 1 Million Chat Records
8	2/17/2025	Large-scale Brute Force attacks targeting VPN devices using 2.8 million IP addresses
9	2/19/2025	Announcement on application for "The ASEAN Cyber Shield MSc Cyber Security Scholarship 2025/2026"
10	2/19/2025	Meta removed over 2 million accounts involved in scam activities
11	2/22/2025	Lazarus Group identified behind the USD 1.4 billion Bybit hack
12	2/27/2025	"Have I Been Pwned" added 284 million compromised accounts stolen by infostealer malware
13	2/27/2025	Risks of Artificial Intelligence and the need for responsible use
14	3/10/2025	Police arrested suspects involved in an AI-based CSAM distribution network
15	3/17/2025	4th ASEAN-Russia Dialogue on ICT Security-Related Issues
16	3/20/2025	Big Data – Concepts, capabilities and future prospects
17	3/20/2025	Introduction to Cloud Computing Technology
18	6/13/2025	Announcement on application for "The 4th ASEAN Cyber Shield Online Education Program"
19	6/23/2025	Announcement on opening of Capture-the-Flag (CTF) Virtual Training
20	6/24/2025	Invitation to participate in Capture-the-Flag (CTF) for Female Youth competition
21	6/25/2025	The largest data breach exposed 16 billion passwords affecting major online services
22	7/3/2025	Invitation to participate in Capture-the-Flag (CTF) Open Competition
23	7/3/2025	Invitation for teams to participate in Myanmar Cyber Security Challenge 2025 (Open Level)
24	7/7/2025	Security advisory on Roundcube Webmail vulnerability (CVE-2025-49113)
25	7/7/2025	Security advisory on Google Chrome Zero-Day vulnerability (CVE-2025-6554)
26	7/16/2025	Recommendation to mitigate critical vulnerabilities affecting various printer models
27	7/22/2025	Announcement on conducting Cybersecurity Awareness Video Contest 2025 (University Level)
28	7/30/2025	Security advisory on VMware product vulnerabilities (multiple CVEs)
29	8/9/2025	Announcement of teams qualified for Myanmar Cyber Security Challenge 2025
30	8/13/2025	Myanmar participated in APCERT Cyber Drill 2025
31	8/16/2025	Guidance on actions to take when receiving suspicious emails
32	8/19/2025	Video coverage of Myanmar Cyber Security Challenge competition
33	8/30/2025	Award ceremony for Myanmar Cyber Security Challenge 2025 and Cybersecurity Awareness Video Contest 2025
34	9/4/2025	Security advisory on critical Zoom vulnerability affecting Windows systems
35	9/27/2025	Google released security update for Chrome Zero-Day vulnerability

36	10/2/2025	Invitation to participate in The Cyber Security Student Contest Vietnam 2025
37	10/3/2025	Security advisory on Cisco product vulnerabilities (multiple CVEs)
38	10/30/2025	Myanmar representative team participated in Cyber SEA Game 2025
39	10/31/2025	Infostealer malware distributed through TikTok videos using ClickFix attacks
40	11/27/2025	Hackers exploiting Post SMTP plugin to hijack WordPress admin accounts
41	12/15/2025	Warning on Malware Distribution via Viber affecting Windows systems

4. Events organized / hosted

4.1 Training

- "Collection and Preservation of Evidence in Cybercrime." sessions were held at the detective training of Ministry of Home Affairs in January and November 2025. Each training sessions included 120 detectives respectively.
- Provision of Cybersecurity Awareness Training for Internship Students from Technological Universities in May and October 2025.
- Cybersecurity awareness and knowledge sharing sessions were conducted for around 700 participants from various ministries in 2025

4.2 Other Activities

- mmCERT organized the Myanmar Cyber Security Challenge 2025 (Open Level) in 2025 with the aim of promoting cybersecurity awareness and strengthening the technical competencies of participants in cybersecurity. The competition was open to participants from various sectors, encouraging them to demonstrate their skills in solving cybersecurity challenges.
- mmCERT conducted Cyber Security Awareness Video Competition (University Level) in August 2025 for selecting and submitting the representative video of Myanmar to join the ASEAN-JAPAN Cyber Security Awareness Video Competition-2025. There were 55 videos from the university students under 30.

Opening Ceremony of Myanmar Cyber Security Challenge 2025 (Open Level)

5. International Collaboration

5.1 International partnerships and agreements

mmCERT has been participating in the international cyber security activities as follows:

- ASEAN Network Security Action Council (ANSAC)
- ASEAN Cybersecurity Coordinating Committee (ASEAN Cyber CC)
- ASEAN Working Group on Anti-online Scam (WG-AS)
- ASEAN-Japan Cybersecurity Working Group Meetings
- Cyber Policy Dialogues with ASEAN Dialogue Partners

5.2 Capacity building

5.2.1 Training

- Attended the SingCERT virtual training session on "Cybersecurity Labelling Scheme and Local Cyber Threat Landscape for ASEAN Regional CERTs" on 4th June 2025. The session provided insights into regional threat trends and cybersecurity certification frameworks.
- Took part in the APCERT technical training webinar titled "Using AI to Enhance Incident Response in CERTs" on 24th

June 2025. The training explored the application of artificial intelligence technologies in cyber incident detection, analysis, and response operations.

- Attended the AJCCBC cybersecurity training webinar on "Leveraging Cyber Threat Intelligence for Proactive Defense" on 25th June 2025. The programme highlighted methods for utilizing threat intelligence to strengthen preventive cybersecurity measures.
- Participated in the APCERT virtual technical training webinar entitled "Vulnerability Management Automation Using Open-Source Tools" on 20th August 202. The training focused on automated vulnerability assessment and management techniques.
- Completed the APCERT online cybersecurity training course on "Introduction to Malware Analysis Techniques" on 26th August 2025. The course covered fundamental malware analysis methodologies and practical approaches for identifying malicious software behaviour.
- Participated in the APCERT online training course entitled "Impact of Artificial Intelligence on Cyber Threat Intelligence (CTI)" on 30th December 2025. The training examined emerging AI-driven cyber threats and the evolving role of AI in intelligence-led cybersecurity operations.

5.2.2 Drills & exercises

- Participated in the APCERT Cyber Drill 2025.
- Took part in the Cyber Battle: Capture-the-Flag (CTF) Competition 2025 held in Brunei Darussalam.
- Participated in the 20th ASEAN CERT Incident Drill (ACID) convened in Singapore.
- Attended and took part in the Mekong-Lancang Cybersecurity Forum and Cyber Drill 2025 held in Siem Reap, Cambodia.
- Participated in the 3rd ASEAN Cyber Shield (ACS) Hacking Contest held in Busan, Republic of Korea.

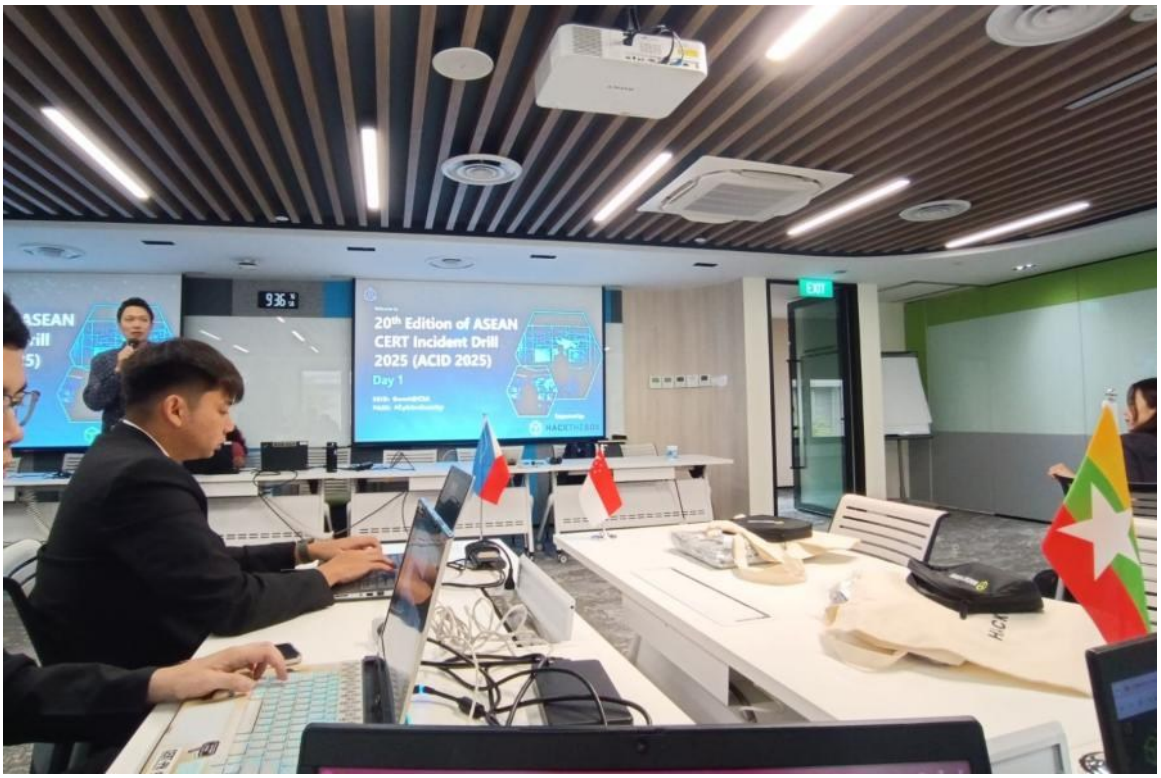
5.2.3 Seminars & presentations

- Attended the 14th ARF Open-Ended Study Group on ICT Security Confidence-Building Measures (Preparatory Meeting) virtually on 12 February 2025.
- Attended the APCERT Webinar on Using Artificial Intelligence to Enhance Incident Response in CERTs virtually on 24 June 2025.
- Attended the AJCCBC Webinar on Leveraging Cyber Threat Intelligence for Proactive Defense virtually on 25 June 2025.
- Attended the Virtual Consultative Workshop on the ASEAN Guide on Anti-Scam Policies and Best Practices, hosted by Singapore, on 16 July 2025, and delivered a presentation on "Anti-Scam Measures in Myanmar."
- Attended the ASEAN Workshop on Public-Private Partnership to Combat Online Scams, organized by the Ministry of Digital Economy and Society of Thailand, virtually on 20 August 2025.
- Attended the 6th ASEAN Cybersecurity Coordinating Committee Meeting and the Workshop on Artificial Intelligence and Post-Quantum Cryptography, hosted by Thailand, virtually from 25 to 26 November 2025.
- Attended the Workshop on Data Protection, Privacy and Governance of Emerging Technologies in support of the ASEAN Digital Economy Framework Agreement (DEFA), held in Bangkok, Thailand, from 4 to 5 December 2025, and

participated as a panellist representing Myanmar.

5.3 Other international activities

- Participated in the 2nd ASEAN-Japan Cybersecurity Working Group Meeting, held in the Republic of the Philippines in 2025.



- Took part in the ASEAN CERT Incident Drill 2025 (ACID 2025), a regional cybersecurity incident response exercise.

- Joined other participants in a commemorative group photograph at the ASEAN CERT Incident Drill 2025 (ACID 2025)

- Took part in the 2025 ASEAN Cyber Shield (ACS) Hacking Contest held in the Republic of Korea.

- Myanmar Representative Team participated at the ASEAN Cyber SEA Games 2025 held in the Kingdom of Thailand.

6. Future Plans

- Cyber Security Awareness Raising Workshops and trainings will be conducted for Chief Information Officers (CIOs) and Assistant Chief Information Officers (ACIOs) from government agencies.
- A Cyber Security Awareness Raising Plan will be developed by mmCERT and implemented among government organizations to promote secure use of digital systems and strengthen endpoint security.
- Myanmar Cyber Security Challenge 2026 will be conducted in August 2025.
- The Cyber Security Awareness Video Competition 2026 will be organized with the objective of improving cyber security knowledge and awareness among youth.
- As an emerging and developing team, mmCERT will continue to enhance its operational maturity through effective incident handling, cyber security research activities, timely dissemination of technical advisories, and organizing the capacity-building programmes such as training courses, seminars, and workshops.
- Coordination with relevant government ministries and agencies will be pursued with a view to establishing Computer Security Incident Response Teams (CSIRTs) in the future.
- Public awareness raising activities, including workshops, seminars, and discussion forums, will be organized to improve cyber knowledge and promote understanding of the importance of cyber security.
- Furthermore, mmCERT will continue to actively participate in international and regional cooperation initiatives related to CERT operations.

7. Conclusion

Throughout 2025, mmCERT continued to strengthen national cybersecurity resilience through expanded engagement with students, young professionals, and key stakeholders. Strategic initiatives were implemented to enhance coordination among government institutions, industry, and academia. Cooperation with international and regional cybersecurity organizations and CERT communities was further reinforced to facilitate the exchange of best practices and threat intelligence. Public awareness programmes were also carried out to encourage responsible digital behaviour and the protection of personal information. These efforts contributed to improving institutional preparedness and supporting proactive cybersecurity risk management across the national landscape. Overall, mmCERT remains committed to advancing cybersecurity capabilities and contributing to a secure and resilient digital environment.

MNCERT/CC

Mongolia Cyber Emergency Response Team/Coordination Center

1. Highlights of 2025

1.1 Summary of major activities

In 2025, MNCERT/CC continued its efforts to strengthen cybersecurity resilience in Mongolia through incident response support, threat intelligence sharing, publications, training, and community engagement. During the year, MNCERT/CC handled 58 cybersecurity incidents and issued 9 publications to support its constituencies and raise awareness of emerging threats and vulnerabilities.

MNCERT/CC also organized and supported practical capacity-building activities, including a malware analysis training, a workshop, and a member cyber drill focused on ransomware response. In addition, MNCERT/CC collaborated with the U.S. Embassy to deliver Cyber Threat Intelligence and Risk Management training for critical information infrastructure organizations and member entities, with more than 100 participants attending.

At the national and international levels, MNCERT/CC continued cooperation with APCERT, FIRST, Team Cymru, NCFTA, APWG, Arctic Security, Microsoft, and other partners, while also supporting key community initiatives such as MNSEC, Haruulzangi, and Haruulzangi U18.

2. About CSIRT

2.1 Introduction

The Mongolian Cyber Emergency Response Team / Coordination Center (MNCERT/CC) is a non-governmental organization established in 2014. MNCERT/CC is responsible for cyber incident response and monitoring, cybersecurity awareness and education, and the development of preventive methodologies to reduce cyber risk. The organization provides cybersecurity intelligence, training, and coordination support to its constituencies and serves as an important platform for national cybersecurity cooperation.

2.2 Establishment

The establishment of MNCERT/CC was driven by the Mongolian National Security Concept and the National Cybersecurity Program. In 2010, the State Great Khural (Parliament of Mongolia) approved Resolution No. 48, which laid the groundwork for the country's cybersecurity development. The resolution outlined key objectives, including:

- Objective 2.2: Establish a cyber incident response system, develop a national CERT, and expand cooperation with international organizations such as APCERT, FIRST, and CERT/CC.
- Objective 4.1: Strengthen the capacity of the organization responsible for securing the state's data and information infrastructure.

These foundational objectives provided the strategic direction for the establishment and operation of MNCERT/CC, ensuring that Mongolia aligns with international best practices in cybersecurity incident response, information sharing, and threat mitigation.

Through its continued efforts, MNCERT/CC remains committed to enhancing Mongolia's cybersecurity resilience, fostering international collaboration, and advancing national cyber defense strategies.

2.3 Resources

In accordance with the Non-Governmental Organizations Code of Mongolia, the founders of MNCERT/CC established a Steering Committee comprising nine members and an Advisory Team with three members. These teams consist of highly qualified professionals and researchers specializing in cybersecurity and information technology, along with a legal advisor.

The Executive Team, operating under the Steering Committee, is responsible for the center's day-to-day operations. This team includes a Chief Executive Officer (CEO), an Operational Manager, a Project Manager, an Incident Handlers, and a Cybersecurity Analysts. Together, they ensure the effective execution of MNCERT/CC's mission, focusing on cyber incident response, cybersecurity research, policy guidance, and legal compliance.

2.4 Constituency

MNCERT/CC serves a diverse range of constituencies, including:

- Internet Service Providers (ISPs)
- Banking and Financial Institutions
- Mobile Network Operators
- Mining companies
- Universities and Academic Institutions
- Other CERT Organizations
- The General Public

3. Activities & Operations

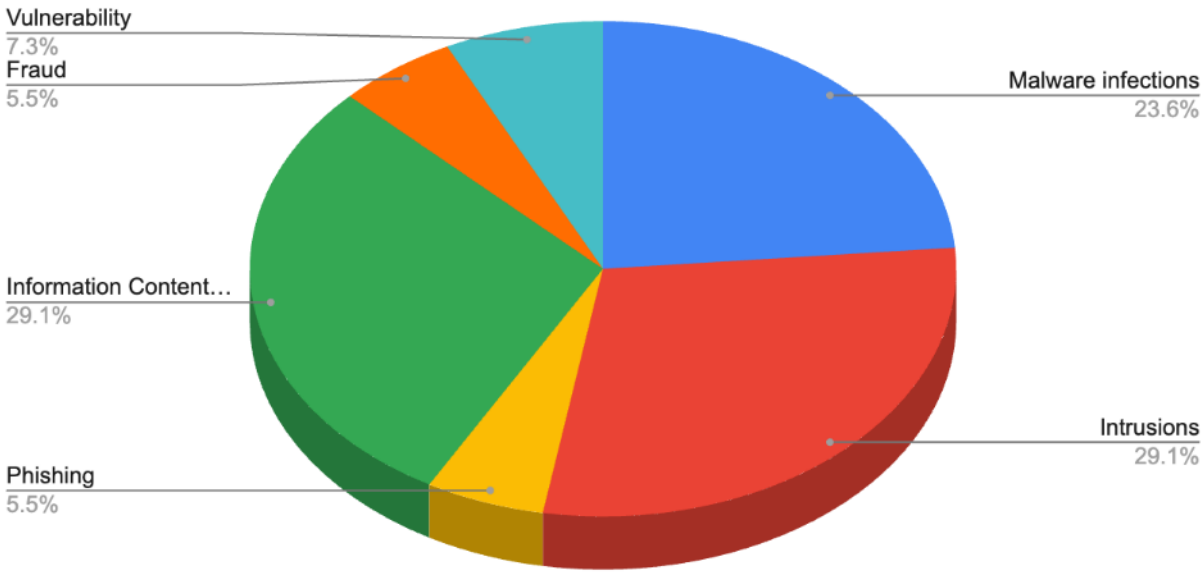
3.1 Scope and definitions

MNCERT/CC serves a diverse constituency, encompassing business enterprises, private sector organizations, financial institutions, universities, non-governmental organizations, and the general public. It delivers a wide range of cybersecurity services, including expert discussions, specialized training, security information and threat intelligence feeds, cybersecurity recommendations, consulting, and comprehensive research and analysis reports. Additionally, MNCERT/CC facilitates collaboration with both local and international CSIRTs to enhance the cybersecurity posture of its member organizations.

3.2 Incident handling reports

In 2025, MNCERT/CC handled a total of **58 cybersecurity incidents**. These cases involved incident response support, advisory services, technical assessment, and coordination with affected entities where appropriate.

The incidents handled during the year continued to demonstrate the importance of timely communication, practical technical support, and trusted coordination. Through its case handling activities, MNCERT/CC supported organizations in addressing cybersecurity issues and reducing the potential impact of incidents on operations and services.



Distribution of cybersecurity incidents

3.3 Abuse statistics

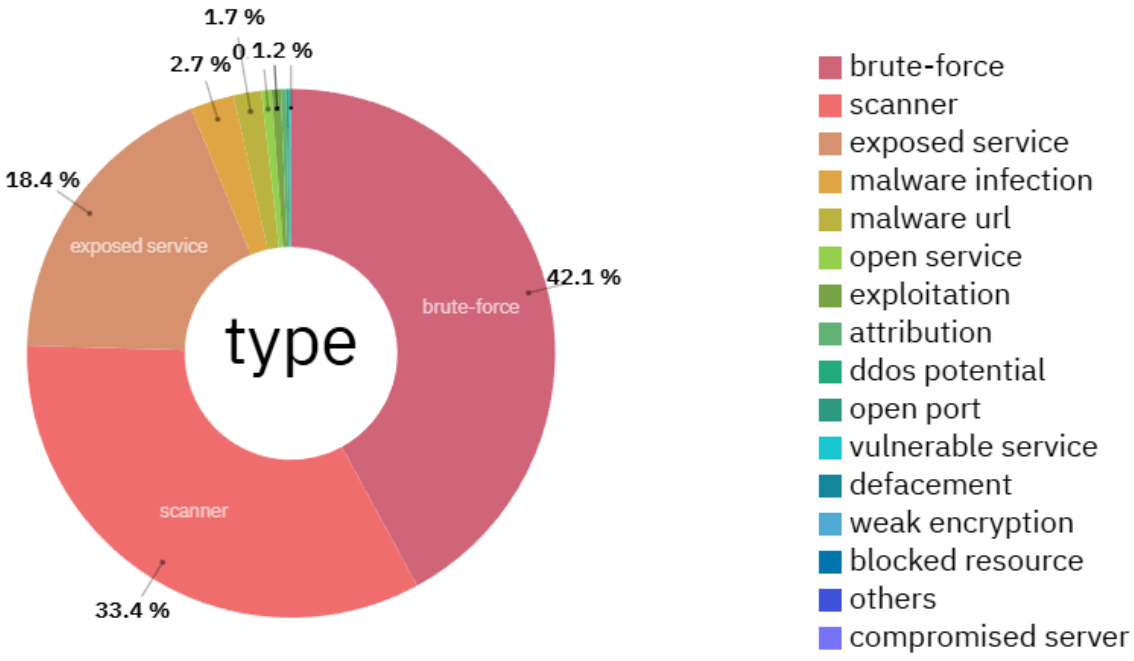
In 2025, a total of 221,674,392 cybersecurity suspicious events to Mongolian cyber environment were recorded, classified into various types of threats and vulnerabilities. The distribution of these events highlights key attack vectors, emphasizing the need for robust cybersecurity measures.

Among the recorded events, the most prevalent type was scanner attacks, accounting for 32.8% of the total incidents. These scanning activities indicate extensive reconnaissance attempts by threat actors to identify exploitable systems.

Brute-force attacks constituted 25.5% of the total, demonstrating a persistent effort by attackers to gain unauthorized access through credential-stuffing and password-guessing techniques. Following this, exposed services were responsible for 15.0% of incidents, further underscoring the risks associated with misconfigured or publicly accessible systems.

Additionally, open services represented 11.4% of the total cases, highlighting potential entry points for unauthorized access. Malware-related incidents, including malware URLs and infections, contributed to 8.1%, posing risks of system compromise and data exfiltration.

The remaining 7.2% of incidents were distributed across various categories, including DDoS potential (3.1%), exploitation attempts (1.2%), open ports (1.2%), vulnerable services (1.0%), and other security threats such as weak encryption, compromised servers, and backdoor access. Following pie chart visualizes the distribution of cybersecurity events towards Mongolia in 2025.



Distribution of cybersecurity events towards Mongolia in 2025

3.4 Publications

A total of nine advisories and warnings were developed and published on mncert.org website and social media platforms to inform organizations and the public about critical and potentially widespread cybersecurity incidents and vulnerabilities. These advisories aimed to enhance awareness and preparedness by providing timely guidance on emerging threats. The detailed information is presented in the following table.

Publications list

No.	Title	Date	Link
1	Монгол Улсыг идэвхтэй чиглэж буй RedDelta APT халдлагын талаар	2025-01-13	https://mncert.org/#/publications/53
2	Төв Азийн орнуудыг онилж буй UAC-0063 халдлагын үйл ажиллагааны талаар	2025-01-21	https://mncert.org/#/publications/54
3	Анхааруулга: FortiOS болон FortiProxy системүүд дээрх эмзэг байдлууд	2025-02-13	https://mncert.org/#/publications/55
4	VMware системүүд дэх өндөр болон ноцтой түвшний эмзэг байдлууд	2025-03-06	https://mncert.org/#/publications/56
5	Roundcube систем дэх CVE-2025-49113 дугаар бүхий ноцтой эмзэг байдал	2025-06-12	https://mncert.org/#/publications/59
6	Notepad++ программд илэрсэн ноцтой кибер зөрчлийн талаар	2026-02-04	https://mncert.org/#/publications/65
7	React, Next.js системүүд дэх ноцтой түвшний эмзэг байдлууд	2025-12-04	http://mncert.org/#/publications/64
8	npm багцууд supply chain халдлагад өртжээ	2025-09-09	https://mncert.org/#/publications/63
9	Jaik бүлийн хортой программд хийсэн шинжилгээ, хариу арга хэмжээний зөвлөмж	2025-07-04	https://mncert.org/#/publications/60

4. Events organized / hosted

4.1 Training

4.1.1 Members meeting and training

MNCERT/CC has been fostering a professional cybersecurity community, providing a platform where security experts from member organizations can discuss challenges, exchange knowledge and experiences, and engage in open

discussions. The member meetings serve as an opportunity for professionals to share research findings, security measures implemented within their organizations, and best practices. Additionally, members can initiate discussions on topics of interest and learn from the experiences of other organizations.

In 2025, MNCERT/CC organized several member meetings and training covering a range of cybersecurity topics, as outlined in the following:

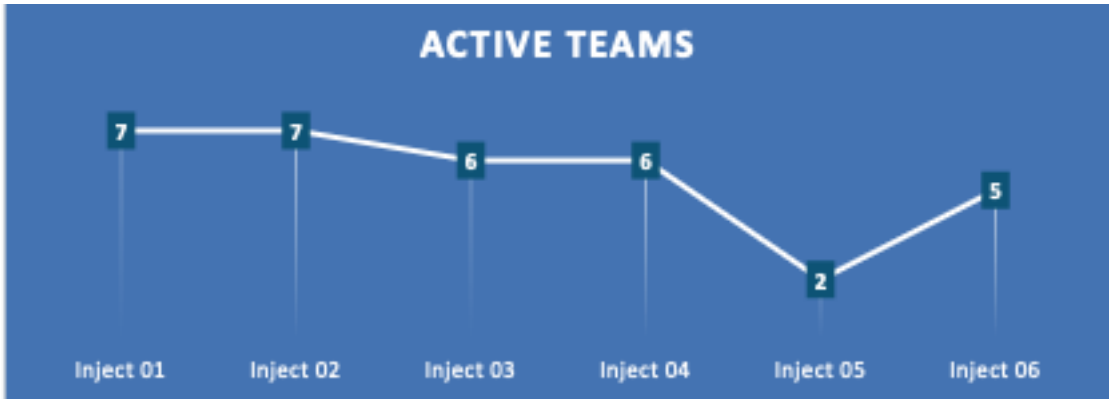
No.	Topic	Date	Venue
1	Overview of the cyber threat landscape in Mongolia; introduction to security feeds and cybersecurity newsletter	2025.01.30	UBH Center
2	Cyber Threat Intelligence practices and information sharing	2025.02.21	UBH Center
3	Security dashboards, cybersecurity posture visualization, and Database Activity Monitoring (DAM)	2025.03.20	Central Tower, Meeting Room 1
4	PCI-DSS 4.0 and client-side protection	2025.04.24	Blue Sky Tower
5	Professional development and international cybersecurity experience sharing	2025.08.21	UBH Center
6	Cyber Threat Intelligence and Risk Management	2025.09.24	American Corner
7	Cybersecurity in AI/ML and introduction to MISP	2025.10.30	American Corner
8	Red teaming practices and offensive security approaches	2025.11.25	Online
9	Community engagement activity	2025.12.17	Irish Pub

4.2 Drills & exercises

4.2.1 Cyber drill

In 2025, MNCERT/CC conducted a cyber drill for member organizations focused on responding to ransomware-type attacks. The exercise was designed to improve both technical and organizational readiness.

Participants were tasked with identifying traces of malicious activity, determining the characteristics of ransomware malware, and performing recovery-related actions such as file decryption and restoration. This practical scenario allowed participating teams to strengthen their incident response procedures and better understand the challenges of handling ransomware incidents in a realistic environment.



4.2.2 Red Team 2025

In collaboration with the Mongolian Banking Association, MNCERT/CC organized the "Red Team 2025 Bug Bounty Program" from March 28 to April 6, 2025, aiming to enhance banking sector security expertise and vulnerability assessment practices. This initiative provided a platform for cybersecurity professionals to exchange knowledge and experience, engage in discussions, and participate in a Capture the Flag (CTF) competition, which was structured around practical cybersecurity challenges.

4.3 Conferences and seminars

4.3.1 MNSEC 2025 Event

MNCERT/CC has been organizing the MNSEC Cybersecurity Conference annually since 2014. The MNSEC 2025 event took place over on September 25th, 2025.

The growing number of participants and their engagement demonstrates that MNSEC has established itself as a highly anticipated industry event for cybersecurity professionals. This year's event featured:

- 14 expert presentations
- Engaging networking activities
- Competitions and interactive challenges
- A total of 500 participants

Participants had the opportunity to attend specialized workshops, including web system penetration testing, hardware hacking and Cyber Threat Intelligence (CTI). Additionally, a hardware security village was set up, where attendees explored the security of automated machines such as massage chairs and vending machines, gaining insights into attack vectors and vulnerabilities.

The conference also featured insightful presentations covering a wide range of cybersecurity topics, including operating system security, artificial intelligence vulnerabilities and platform security risks. Participants had the opportunity to engage directly with speakers, ask questions on topics of interest, and gain valuable knowledge applicable to their roles and interests.

MNSEC 2025 successfully provided a dynamic and informative experience for cybersecurity professionals, IT specialists, and enthusiasts alike, offering valuable insights and networking opportunities within the field of information and

cybersecurity.

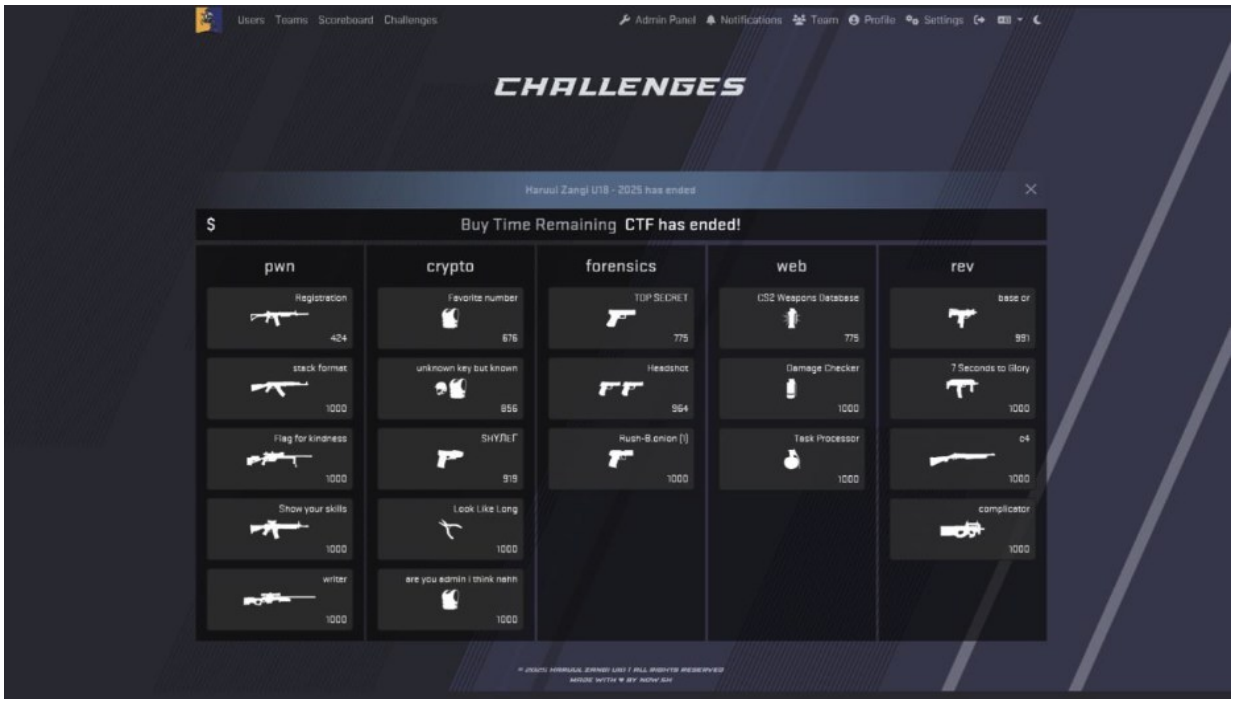
4.3.2 “Haruul zangi” 2025 cybersecurity competition

"Haruulzangi" Cybersecurity Competition has been held annually since 2013, providing an opportunity for all citizens of Mongolia to participate. The competition attracts numerous young professionals from the IT and Security sector, allowing them to test and showcase their cybersecurity skills. The 2025 Haruulzangi Competition was structured into three stages:

First Stage (Online Round) – Conducted in an online format on September 13, 2025.

Second Stage (Onsite Round) – Held on September 22, 2025, at Nest High School, where the top 32 teams from the first stage competed.

Final Stage – The grand finale took place on September 25, 2025, at the Shangri-La Ulaanbaatar Hotel, where the champion of the ethical hacking competition was crowned.



4.3.3 “HaruulZangi U18 2025” Cyber Security Competition

The "HaruulZangi U18" Cybersecurity Competition has been held annually since 2016 for high school students, providing a platform to enhance cybersecurity awareness and knowledge among young learners. The competition aims to:

- Raise awareness of information security and potential cyber threats among students.
- Improve understanding of online risks and cyberattacks in the digital space.
- Encourage students interested in information technology and cybersecurity to pursue further studies in the field.
- Challenge and inspire young talents, fostering early engagement in cybersecurity and IT disciplines.

In 2025, the 7th edition of the competition took place from May 18 to May 26, following a two-stage format. A total of 68 teams participated in the event, demonstrating their skills, problem-solving abilities, and knowledge of cybersecurity concepts.

5. International Collaboration

5.1 International partnerships and agreements

MNCERT/CC partners and collaborates with a broad spectrum of domestic and international organizations to strengthen cybersecurity capability and foster a unified approach to mitigating cyber threats.

Internationally, MNCERT/CC is an active member of FIRST and APCERT. In addition, MNCERT/CC maintains collaborative and contractual relationships with global cybersecurity organizations such as Team Cymru, NCFTA, APWG, Arctic Security, Microsoft, and others. These collaborations provide access to near real-time threat intelligence, vulnerability feeds, and

international cybersecurity expertise.

By contextualizing this information for the local environment, MNCERT/CC helps ensure that its constituencies and other entities in Mongolia are better informed and better prepared to address evolving cybersecurity threats.

5.2 Capacity building

5.2.1 Training

In 2025, MNCERT/CC team members attended the following international training and professional development activities:

- International Visitor Leadership Program (IVLP)
- 2025 APISC Security Training Course, conducted by KISA, Republic of Korea
- AGM 2026

These activities contributed to the continuous strengthening of MNCERT/CC's international exposure, technical knowledge, and professional network.

6. Future Plans

6.1 Future projects

MNCERT/CC plans to continue expanding its contribution to Mongolia's cybersecurity ecosystem through the following priorities:

- Expanding membership and collaboration by engaging more public and private sector organizations and strengthening cross-sector cooperation
- Expanding consultancy services by providing more specialized support to domestic entities and helping shape practical cybersecurity strategies
- Research and studies focused on emerging threats, cybersecurity trends, and best practices, including collaboration with academic institutions and industry experts
- AGM 2027 hosting, or preparation toward hosting, depending on final confirmation

7. Conclusion

In 2025, MNCERT/CC continued to strengthen its role as a national coordination point for cybersecurity support, awareness, training, and collaboration. FIRST publicly lists MNCERT/CC as Mongolia's CERT/CC team, and APCERT continues to provide an important regional framework for cooperation and capacity building.

During the year, MNCERT/CC handled **58 incidents**, issued **9 publications**, delivered technical training activities, conducted a ransomware-focused member drill, collaborated with the U.S. Embassy on cyber threat intelligence and risk

management training for over 100 participants, and continued supporting community initiatives such as MNSEC, Haruulzangi, and Haruulzangi U18. These efforts reflect MNCERT/CC's continued commitment to strengthening cyber resilience, supporting practical capability development, and fostering trusted collaboration across Mongolia's cybersecurity community.

National CSIRT of Mongolia

National Computer Security Incident Response Team of Mongolia

1. Highlights of 2025

In 2025, the National Computer Security Incident Response Team of Mongolia (National CSIRT) Mongolia strengthened its cyber threat intelligence and operational capabilities through the development and deployment of the Malware Information Sharing Platform (MISP). The platform was integrated with more than 100 external threat intelligence sources, enabling the automated collection and sharing of cyber threat information and enhancing analytical capabilities. In parallel, efforts were undertaken to automate the National CSIRT's internal operational processes, improving operational efficiency, streamlining incident handling workflows, and strengthening coordination among cybersecurity monitoring and response teams. Through the Early Warning System, the National CSIRT supported proactive cybersecurity management by delivering vulnerability and incident alerts to stakeholders for timely preventative action. Additionally, the National CSIRT organized and conducted its own national "ITACTIC" Cyber Drill to enhance cyber incident response preparedness. The exercise involved relevant stakeholders and simulated cyber attack scenarios to improve inter-organizational coordination and strengthen readiness for responding to large-scale cybersecurity incidents.

2. About CSIRT

2.1 Introduction

The National CSIRT is dedicated to enhancing national capabilities in responding to cyber threats, establishing a robust cybersecurity system through both domestic and international cooperation. The center is responsible for safeguarding government and critical information infrastructure, detecting and preventing potential cyberattacks, responding to incidents, and ensuring recovery efforts.

2.2 Establishment

In accordance with Mongolia's "Vision-2050" Long-term development policy (Objective 7.5), the National Cybersecurity

Strategy (Clause 3.5.1), and the Cybersecurity Law (Article 21), the National CSIRT was established in December 2022 under the Information Security Department. By September 2023, the legal framework, structure, staffing, and operational regulations of the National CSIRT were officially approved by a government decree.

2.3 Resources

The center consists of the following units:

- Security Operations Center
- Incident Response Unit
- Cyber Threat Intelligence Unit
- International Cooperation Unit

2.4 Constituency

Critical information infrastructure and government organizations connected to the State Information Consolidated Network.

3. Activities & Operations

3.1 Scope and definitions

The National CSIRT collects and analyzes cyber incidents, monitors internet traffic for organizations connected to the state information consolidated network and detects and verifies cyber threats. Relevant authorities are notified of detected threats, and appropriate mitigation measures are implemented. Additionally, expert guidance and recommendations are provided.

3.2 Incident handling reports & Abuse statistics

The National CSIRT carried out response activities throughout 2025, including incident response, mitigation, containment, recovery, and the provision of technical and methodological assistance for cyber incidents that occurred during the year. The types of cyber incidents detected within organizations under the National CSIRT's scope are illustrated in the figure below. (Figure 1).

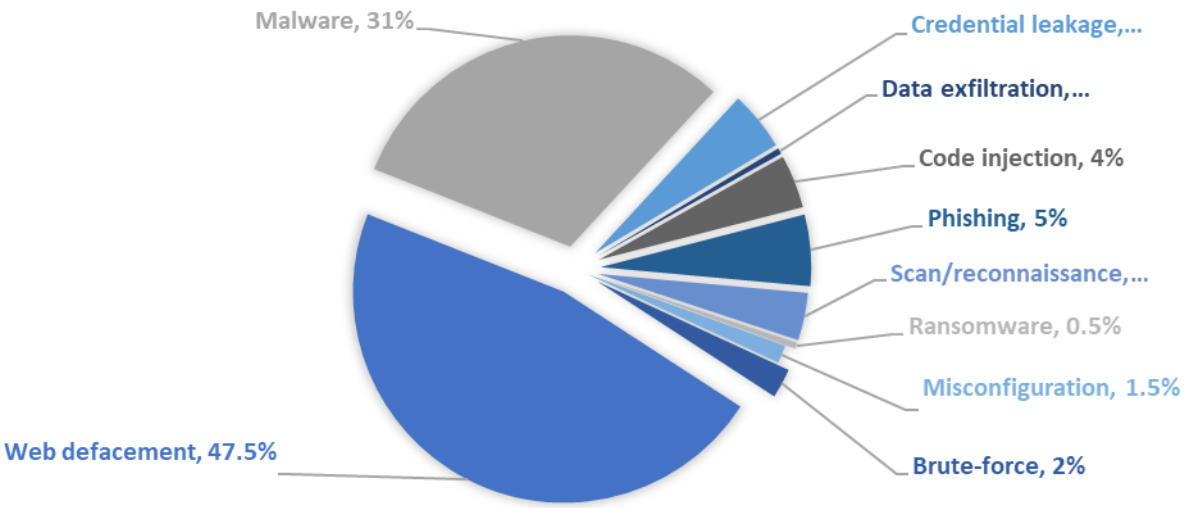


Figure 1. Types of Cyber Incidents Handled

Monitoring activities conducted on the internet networks of organizations connected to the State Information Consolidated Network showed that in 2025 the number of suspicious and potentially malicious connection attempts decreased by 4% compared to the previous year.

Among the detected activities, the most frequent critical-level threat was **Cryptominer Command-and-Control (C&C) traffic**. At the high severity level, SMB brute-force attacks were most observed. At the medium severity level, DNS ANY queries brute-force and SMBv1 scanning were frequently detected.

As part of efforts to automate internal operations, the National CSIRT utilizes multiple data sources from the information systems of organizations within its scope to detect cyber incidents and suspicious activities.

Through this system, the National CSIRT identifies various types of security issues, including open server ports, system vulnerabilities, phishing activities, network scanning attempts, participation in botnets used for DDoS attacks, malware infections, server compromises, and IP addresses being listed on blacklists. When such incidents are detected, automated notifications are sent to the respective organizations to enable timely mitigation and response.

Using this system, security incidents were identified in approximately 50% of the organizations under the National CSIRT's scope. Through the Early Warning System, vulnerability and incident information was promptly communicated to the responsible Information security officers, enabling them to take preventive action before issues could escalate or develop into more serious incidents. Within this framework, over 16,000 alerts and notifications were delivered. The most detected types of incidents are illustrated in the figure below. (Figure 2).

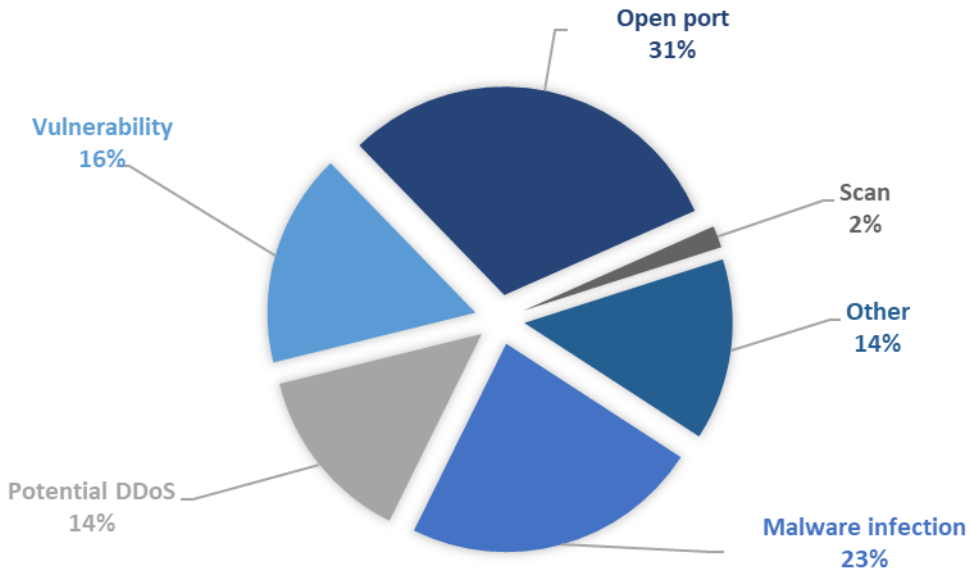


Figure 2. Types of Security Incidents Detected in the Information Systems of Organizations under the National CSIRT's Scope

3.3 Publications

- The National CSIRT disseminates cybersecurity news, alerts, and advisories through its official website ncsirt.gov.mn to inform both the public and government organizations about emerging cyber threats and security best practices.
- A cybersecurity guide and practical recommendations for government officials were developed and distributed to relevant institutions to improve cybersecurity awareness and strengthen organizational security practices.
- As part of efforts to standardize operations, the National CSIRT developed and implemented dedicated procedures for cyber incident detection and response. In addition, standardized documentation templates for incident detection and response activities were created and integrated into operational processes to ensure consistent and well-documented response actions.
- The National CSIRT contributed to the cybersecurity journal published by the Information Security Department, providing information on current cyber threats, security trends, and best practices.

4. International Collaboration

4.1 International partnerships and agreements

- On May 15, 2024, the National CSIRT became an official member of FIRST.
- On August 30, 2024, the National CSIRT joined the regional APCERT community.

- The National CSIRT also serves as the designated Technical Point of Contact for the Organization for Security and Co-operation in Europe's (OSCE) "Cyber/ICT security Confidence building measures" initiative.
- On November 20, 2025, the National CSIRT was registered as a "Listed" member of the TF-CSIRT professional community.

4.2 Capacity building

4.2.1 Training

- APCERT training: "Malware Analysis Methods"
- APCERT training: "Using AI to Enhance Incident Response"
- OSCE training: "Information and Communication Technologies, Cybersecurity and Gender"
- OSCE workshop: "International Cyber Diplomacy"
- Technical and management-level training conducted under the "Asia-Pacific Cyber Drill 2025" organized by the International Telecommunication Union
- Training on "National-Level Cyber Incident Response" organized by the Embassy of the United Kingdom in Mongolia and the Cyber Security Council of Mongolia
- Training on "Artificial Intelligence and Transnational Organized Crime" organized by the United Nations Institute for Training and Research
- JICA training: "Capacity Building in International Law and Policy Formation for Cybersecurity"
- Training on "Cyber Threats and Risk Management" organized by the Embassy of the United States in Mongolia in cooperation with MNCERT/CC
- JICA training: "Comprehensive Exercises for SOC" and "Malware Analysis"

4.2.2 Drills & exercises

- "ITACTIC" Cyber Drill
- APCERT Cyber Drill organized by APCERT
- Asia-Pacific Cyber Drill 2025 organized by the International Telecommunication Union
- "CyberChess" organized by CERT.LV

4.2.3 Seminars & presentations

- OSCE Cyber/ICT Security CBM8 Points of Contact Annual Meeting
- 37th Annual FIRST Conference organized by Forum of Incident Response and Security Teams
- Interregional Conference on Cyber/ICT Security Confidence-Building Measures, organized by the OSCE in cooperation with Information Security Department.
- Conference on AI Security and Ethics and Cyber Stability Conference organized by the United Nations Institute for Disarmament Research
- Asia-Pacific Cyber Drill 2025 Conference organized by the International Telecommunication Union
- CII Summit 2025

- "Dell Technologies" forum
- MNSEC 2025
- "Cyber Risk & Resilience" forum 2025
- "Cyber Sovereignty" forum 2025

4.3 Other international activities

Participation in the "National Big Data and Artificial Intelligence Strategy 2025" event, jointly organized by the Ministry of Digital Development, Innovation and Communications of Mongolia and the United Nations Development Programme Country Office in Mongolia, with recommendations submitted in relation to the development of the national strategy.
Participation in the "AI Readiness Assessment" event, organized jointly by the Ministry of Digital Development, Innovation and Communications of Mongolia and the Global Cyber Security Capacity Centre at the University of Oxford.

5. Future Plans

5.1 Future projects

In the coming years, the National CSIRT will continue to strengthen national cybersecurity resilience through enhanced threat intelligence sharing, and increased cooperation with national and international partners.
Future initiatives will focus on improving cyber incident detection and response capabilities, expanding threat intelligence integration, strengthening automation of operational processes, and enhancing capacity building and cybersecurity awareness among organizations under the National CSIRT's scope.
The National CSIRT also plans to further develop cybersecurity monitoring systems in cooperation with the Ministry of Digital Development, Innovation and Communications of Mongolia (MDDIC).

5.2 Future Operation

The National CSIRT will focus on improving automation of operational processes to enable faster detection, analysis, and response to cybersecurity incidents. Efforts will be directed toward streamlining workflows, integrating security systems, and enhancing monitoring capabilities to ensure more efficient operations.
Aligned with Mongolia's Vision-2050 development policy, the National CSIRT also plans to integrate artificial intelligence into cybersecurity operations to strengthen the protection of critical information infrastructure.

6. Conclusion

In 2025, the National CSIRT continued to strengthen its role in protecting national cyberspace by improving cyber threat intelligence capabilities, enhancing incident detection and response mechanisms, and expanding cooperation with national and international partners.

Through the development of technical systems, automation of operational processes, and active participation in international cybersecurity initiatives, the National CSIRT contributed to improving the overall resilience of Mongolia's digital infrastructure.

NCSC-NZ

National Cyber Security Centre New Zealand

1. Highlights of 2025

1.1 Summary of major activities

Incidents

In the 2024/25 financial year, the NCSC-NZ recorded 5995 reported incidents. The NCSC receives incident reports from individuals through to critical infrastructure organisations. Individuals made 4,343 reports and organisations were responsible for 1,321 reports. Of the 5995 incidents reported, 331 were triaged for specialist technical support.

Figure 1: Total incidents reported to NCSC in 2024/2025

Financial harm

- The direct financial loss reported in 2024/2025 totalled $26.9 million, increasing from $21.6 million in 2023/2024
- It was estimated that NCSC prevented $47.9 million of harm to New Zealand through their detection and disruption capabilities

1.2 Achievements & milestones

NCSC-NZ launched new website and incident reporting function

The NCSC and CERT NZ websites have been consolidated to create a single site for IT specialists, large organisations, government and operators of critical infrastructure to go to for authoritative cyber security advice and insights. This will improve the experience for all New Zealanders reporting cyber security incidents, making it easier for people to know where to go for help. With a refreshed website and a streamlined incident reporting function, cyber security incidents are now being reported in one place, whether the victim is an individual or critical infrastructure operator. This single platform for reporting incidents also enables the NCSC to have a better understanding of the cyber threat landscape across the New Zealand economy. The CERT NZ brand was disestablished while Own Your Online, which targets individuals and small to medium-sized businesses remains.

www.ownyouronline.govt.nz

2. About NCSC-NZ

The National Cyber Security Centre (NCSC) was established in 2011, a part of the Government Communications Security Bureau (GCSB), is Aotearoa New Zealand's lead operational cyber security agency. In July 2024, New Zealand's Computer Emergency Response Team (CERT NZ), formerly a part of the Ministry of Business, Innovation and Employment (MBIE), was integrated into the NCSC's organisational structure to form the New Zealand Government's lead operational cyber security agency.

https://www.ncsc.govt.nz/

3. Activities & Operations

3.1 Scope and definitions

The NCSC provides cyber security services to all New Zealanders - from individuals to small and medium businesses and organisations, large enterprises, government, and nationally significant organisations. We work to improve New Zealand's resilience to cyber security threats. The services we deliver include:

- providing cyber security information and educational resources; receiving reports of - and responding to - cyber security incidents; collating information about the cyber threat landscape to share with partners
- disrupting cyber security attacks; hosting the Government Chief Information Security Officer (GCISO) function and providing system stewardship of public service information security
- delivering cyber security uplift to Pacific Islands nations and supporting government agencies and nationally significant organisations with tailored services and advice.

The NCSC makes use of its domestic and international networks to facilitate information exchanges within sectors, share information with trusted partners, and to support our cyber security work in New Zealand.

3.2 Incident handling reports

The NCSC handles incident reports through two distinct triage processes. Most incident reports are managed through the NCSC's general triage process. A small number of incidents are triaged for specialist technical support due to the nature of the victim or the seriousness of the incident. These incidents could cause high impact at the national level and are referred to as incidents of potential national significance.

In the 2024/25 year, the most severe incidents were categorised as C3. These incidents included several DDoS incidents that were likely linked to ideologically motivated malicious cyber activity, and ransomware incidents that had links to criminal or financially motivated actors. There was also a significant incident involving the network compromise of a New Zealand organisation, which had links to state-sponsored actors.

Figure 2: Incidents reported to NCSC categorised by severity

Scams and fraud continues to be the most commonly reported cyber security incident, followed by phishing and credential harvesting and unauthorised access.

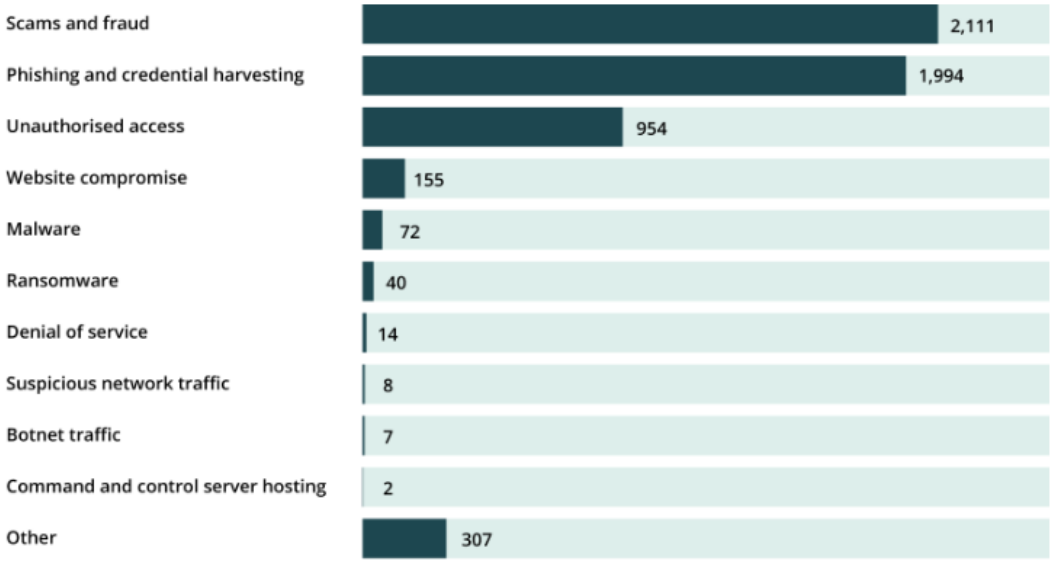


Figure 3: Sub-categories of incidents reported to the NCSC

3.3 Publications

NCSC continued to publish their quarterly reporting with the publication of the Cyber Security Insights Report.

In 2025, the NCSC published research tracking the cyber security behaviour of individuals and small to medium businesses in New Zealand. Highlights of the two research reports were:

- Online threats cost New Zealanders an estimated $1.6 billion
- 94% of New Zealanders believe it's important to protect themselves online
- More than half of New Zealand's small to medium businesses experienced an online threat
- 28% of New Zealand organisations took new cyber security actions in the past six months

In 2025, the NCSC alerted thousands of New Zealanders to let them know their device had been infected with malware known as Lumma Stealer and published guidance on signs your device may have the malware and how to keep safe after a data breach.

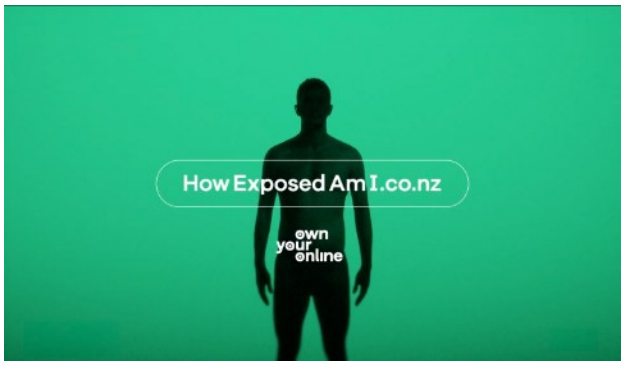
NCSC NZ continued to join several international partners in a number of joint publications. These pieces of cyber security advice and guidance ranged from engaging with artificial intelligence, to cyber security for operational technology and are an effective channel to get advice out to constituents.

NCSC NZ also uses their social media channels to draw attention and raise awareness of these publications and general cyber security advice. Own Your Online social media accounts are tailored for individuals and small to medium businesses while NCSC-NZ accounts target IT professionals and large organisations.

4. Events organized / hosted

NCSC continued to run the annual cyber security awareness campaign, with Cyber Smart week running from 6 to 12 October. The campaign for 2025 was 'How Exposed Am I' which was designed to show New Zealanders what information scammers might already know about them and to show that we are all vulnerable with our ever-growing digital lives.

It exposes that over 4.3 million New Zealand account details are exposed to scammers and an estimated $1.6 billion lost every year. The campaign included a website that analyses live data from public global breaches to provide the user with an exposure score to indicate how exposed their information is online. Following the exposure score, the site then shares ways the user can protect their information through some basic cyber security actions such as implementing two-factor authentication and long, strong and unique passwords.



https://www.ownyouronline.govt.nz/how-exposed-am-i/

5. International Collaboration

5.1 International partnerships and agreements

NCSC NZ maintains relationships with many like-minded cyber security incident response teams around the world. These relationships are highly valued and enable mutually beneficial collaboration to improve the cyber security resilience of our nations.

Key international engagements

- APCERT annual conference
- PaCSON AGM
- FIRST Annual conference
- NatCSIRT annual meeting

5.2 Capacity building

An integral part of our international programme, Pacific Partnerships work closely with Pacific cyber agencies to support capacity building, workforce development, awareness raising and cyber resilience efforts in the Pacific region. The NCSC is a member of the Pacific Cyber Security Operational Network.

Through the cyber capacity building pillar, the NCSC focuses on collaborating with Pacific Island nations to develop national cyber security functions. The NCSC is also co-convenor of the Pacific Cyber Security Operational Network (PaCSON) Capacity Building Working Group alongside CERT-Tonga. This group of operational cyber security organisations is a leading voice on cyber capacity building in the region.

https://pacson.org/

PaCSON Capacity Building Action Plan 2025-2028

Led by NCSC and CERT Tonga, in October 2025 the PaCSON Capacity Building Action Plan 2025-2028 was launched. Designed by the Pacific, the action plan is the key framework for partnering on cyber capacity building initiatives in the region.

6. Future Plans

The NCSC will continue to work towards a New Zealand where good cyber security happens everywhere, all the time, by everyone. We will continue to place value in international collaboration and partnership and welcome continued opportunities for this. We will continue to be present in networks such as APCERT to share information and tackle shared malicious cyber activity collectively.

Public CSIRT/CC

Public Computer Security Incident Response Team of Mongolia

1. Highlights of 2025

1.1 Summary of major activities

In 2025, the Public CSIRT/CC of Mongolia strengthened national cybersecurity capabilities through expanded operational activities, proactive initiatives, and enhanced collaboration. A key development was the establishment of a proactive cybersecurity assessment working group, enabling on-site evaluations to identify vulnerabilities and mitigate risks before incidents occur. This marked a transition from reactive incident response to preventive risk management.

The Public CSIRT also enhanced national coordination by organizing the CII Summit 2025 and conducting sector-specific engagements, fostering closer collaboration among government institutions, critical infrastructure operators, and private sector stakeholders.

Operationally, the Public CSIRT continued national-level threat monitoring and incident response across multiple sectors, while expanding efforts to identify exposed vulnerabilities. Training and awareness initiatives reached more than 3,000 participants, contributing to improved cybersecurity knowledge among organizations and the public. International engagement was further strengthened through active participation in regional and global initiatives and cooperation with international partners.

In addition, the Public CSIRT achieved an important milestone by becoming an official member of the Asia Pacific Computer Emergency Response Team (APCERT), further strengthening Mongolia’s participation in regional cybersecurity cooperation and information sharing.

2. About CSIRT

2.1 Introduction

Public CSIRT/CC of Mongolia operates under the Ministry of Digital Development, Innovation and Communications. It is responsible for the prevention, detection, and response to cybersecurity incidents affecting citizens, legal entities, and private-sector operators of Critical Information Infrastructure (CII).

Public CSIRT/CC provides professional and methodological support for incident response and system recovery, develops cybersecurity recommendations and risk mitigation measures, and conducts threat monitoring, analysis, and information sharing. The center also implements public awareness and capacity building initiatives.

Through these functions, the Public CSIRT/CC plays a central role in strengthening Mongolia's national cybersecurity resilience and coordinating cross-sectoral incident response efforts.

2.2 Establishment

Public CSIRT/CC was established on 30 August 2023 pursuant to Government of Mongolia Decree No. 319. The establishment of the center reflects Mongolia's strategic commitment to strengthening national cybersecurity governance and enhancing institutional capacity for coordinated cyber incident response.

Operating as a state-owned enterprise under the Ministry of Digital Development, Innovation and Communications, the Public CSIRT/CC serves as a national coordination mechanism for incident response, cybersecurity capability development, and stakeholder collaboration across public and private sectors.

2.3 Resources

Public CSIRT/CC is continuously strengthening its human, technical, and organizational capacities to effectively fulfil its national mandate in cyber incident response and cybersecurity coordination.

The center currently operates with an approved staffing capacity of 47 personnel, comprising cybersecurity analysts, engineers, and technical specialists. At the same time, it is progressively enhancing its technological infrastructure to support incident detection and response, threat monitoring and analysis, and secure data collection and management.

In addition, Public CSIRT/CC is developing and maintaining national cyber incident databases to improve threat visibility,

situational awareness, and evidence-based reporting at the national level.

To further expand its operational capabilities, the center actively cooperates with domestic stakeholders and international partners in adopting advanced technologies, strengthening technical expertise, and aligning with global cybersecurity best practices.

2.4 Constituency

Public CSIRT/CC serves a broad national constituency, including citizens, legal entities, and private-sector operators of Critical Information Infrastructure (CII).

In accordance with the Law on Cybersecurity of Mongolia, Critical Information Infrastructure encompasses organizations operating across 17 strategic sectors essential to national security, economic stability, and public safety. These sectors include:

- Energy generation, transmission, distribution, and control systems
- Water supply, wastewater, and centralized heating infrastructure
- Secondary and tertiary healthcare institutions
- Laboratories for highly infectious human and animal diseases
- Producers of pharmaceuticals and hazardous chemical substances
- Banking and financial institutions operating integrated electronic payment and transaction systems
- Telecommunications and information technology service providers with dominant or monopoly status
- Transport management and control systems across air, rail, maritime, and road sectors
- Fuel and petroleum importers, producers, and distributors
- Strategic food production, storage, and distribution entities
- National emergency and operational command centers
- National public broadcasting services
- Custodians of core national information systems and foundational databases
- Data centers, including primary, branch, and backup facilities
- Border control management systems
- Operators of strategically significant mineral resource extraction activities
- Integrated systems for registration and control of cross-border passengers and vehicles

3. Activities & Operations

3.1 Scope and definitions

Public CSIRT/CC of Mongolia is mandated to monitor, detect, analyze, and respond to cyber threats and incidents affecting national information systems and networks, including private-sector operators of Critical Information Infrastructure (CII), legal entities, and the general public.
Its core functions include incident handling and coordination, threat intelligence collection and analysis, vulnerability monitoring, information sharing and reporting, as well as the provision of cybersecurity awareness initiatives and advisory services.

3.2 Incident handling reports

In 2025, the Public CSIRT/CC of Mongolia handled over 40 cybersecurity cases across multiple sectors, including finance, telecommunications, media, healthcare, software development, and other critical service domains.

Case Classification
The cases addressed by the Public CSIRT/CC were broadly categorized into proactively identified vulnerabilities and reported cybersecurity incidents.

Proactively Identified Vulnerabilities
A significant portion of cases (approximately 20+ cases) were identified proactively by the Public CSIRT/CC.

Reported Incidents
The remaining cases were reported by organizations or received through coordination with national and international partners. These included malware infections, website defacement incidents, phishing campaigns, credential compromise cases, and security issues arising from misconfigurations or fraudulent digital content. These incidents required structured response actions, including technical analysis, containment, and recovery coordination.

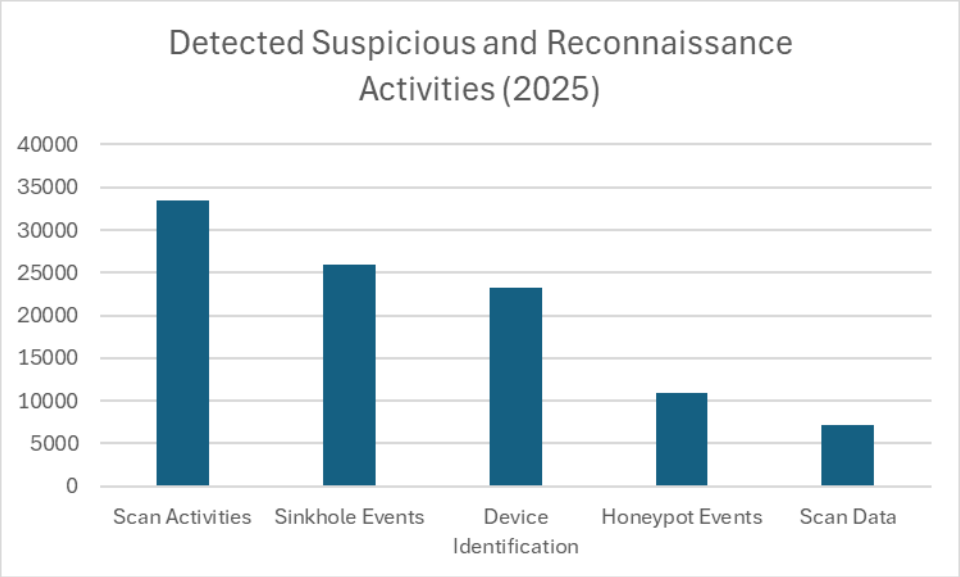
3.3 Abuse statistics

In 2025, Public CSIRT/CC of Mongolia monitored a broad spectrum of cybersecurity indicators reflecting malicious activities, system exposure, and emerging risks across national networks and digital services.

Indicators of Potentially Compromised or Targeted Systems
Monitoring activities revealed significant levels of reconnaissance and suspicious cyber activity. Key indicators included:

- Scan Activities: 33,476

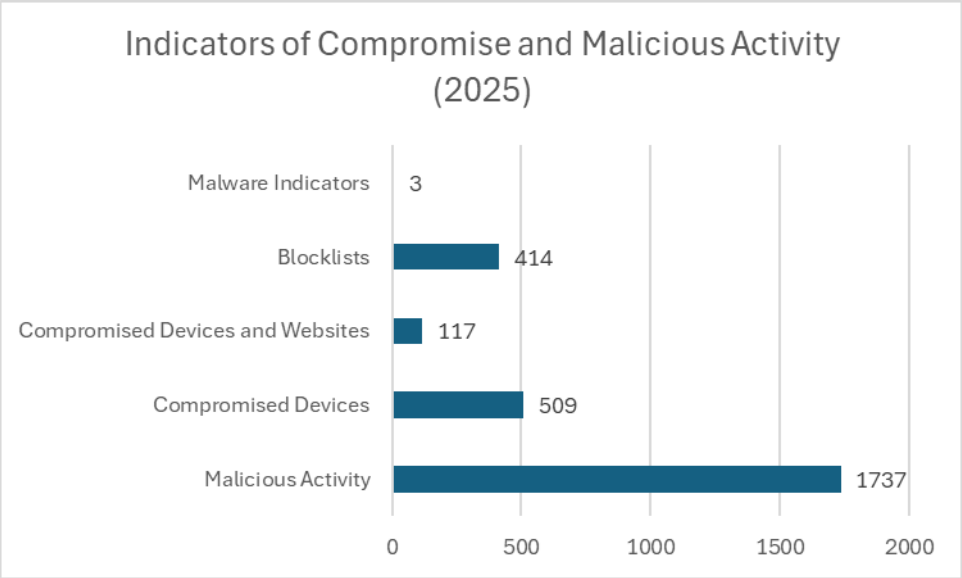
- Device Identification Events: 23,305
- Sinkhole Events: 25,920
- Honeypot Events: 10,909
- Scan Data Events: 7,167



The Public CSIRT/CC operates dedicated honeypot systems to proactively detect, monitor, and analyze malicious activities targeting national networks and digital services. Data collected through these systems provides critical insights into attacker behavior, reconnaissance patterns, and emerging threat trends.

Analysis of honeypot and threat intelligence data identified multiple indicators of compromise and malicious activity, including:

- Compromised Devices: 509 cases
- Malicious Activity: 1,737 cases
- Compromised Devices and Websites: 117 cases
- Blocklisted Entities: 414
- Malware Indicators: 3



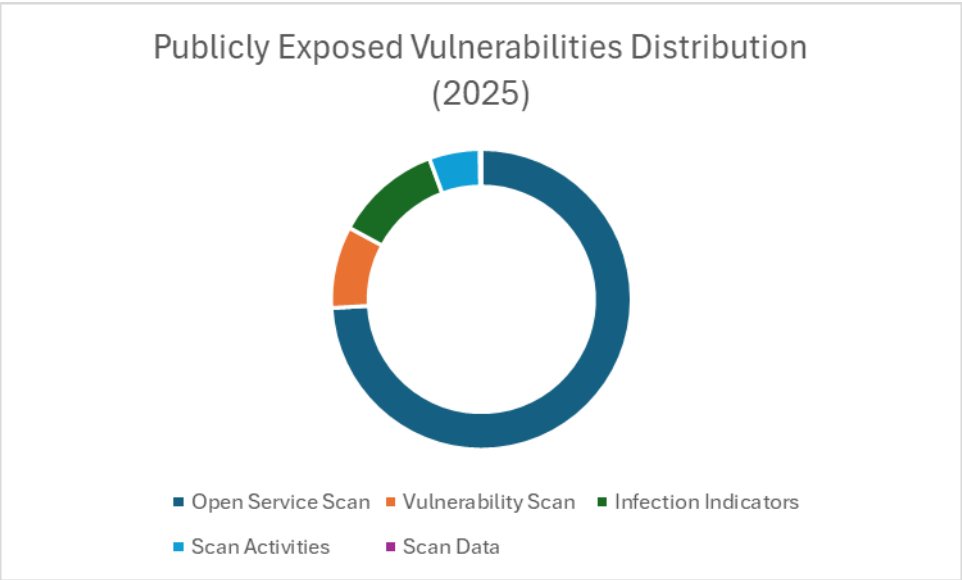
Exposure and Risk Indicators

- Open Service Scan (Potential Risk Exposure): 5,228

Publicly Exposed Vulnerabilities

The following data highlights vulnerabilities identified in publicly accessible systems:

- Open Service Exposure: 16,893
- Vulnerability Scan Events: 2,009
- Infection Indicators: 2,615
- Scan Activities: 1,249
- Scan Data: 36



3.4 Publications

Threat Intelligence and Reporting

The Public CSIRT/CC produced and distributed regular cybersecurity intelligence outputs to support situational awareness and coordinated risk management. These included weekly situational reports submitted to the Asia Pacific Computer Emergency Response Team (APCERT), as well as internal threat monitoring summaries. The reports provided timely insights into emerging cyber threats, evolving vulnerability trends, and indicators of compromise affecting national digital infrastructure.

Policy research

During the reporting period, the Public CSIRT published a policy-oriented analytical publication to support strategic awareness in the field of cyber diplomacy and international digital cooperation, in collaboration with the National Institute for Security Studies under a Memorandum of Understanding (MoU).

Public Advisories and Alerts

Cybersecurity information was actively disseminated through official communication channels, including public announcements and social media platforms. During the reporting period, the Public CSIRT/CC issued 15 public advisories, addressing ongoing cyber threat campaigns, newly identified system vulnerabilities, and emerging cybercrime and online fraud trends targeting citizens. The advisories also included recommended mitigation measures and preventive guidance, enabling timely risk communication to both technical stakeholders and the general public.

Cybersecurity Magazine – CyberRead

In 2025, the Public CSIRT/CC launched a new cybersecurity magazine titled CyberRead, aimed at enhancing public awareness and providing in-depth analysis of national cybersecurity developments. The publication features assessments of the national cyber threat landscape, coverage of major cybersecurity events such as the CII Summit 2025, and analytical articles on digital transformation initiatives, including developments in the judicial sector. It also offers practical guidance on cyber risk prevention and technical insights, such as analyses of botnet activities, including Andromeda.

3.5 New services

Proactive Cybersecurity Assessment Working Group

In 2025, the Public CSIRT/CC of Mongolia introduced a proactive cybersecurity assessment program aimed at strengthening organizational resilience through early identification and remediation of security weaknesses.

As part of this initiative, the Public CSIRT/CC conducted on-site technical assessments at organizations where vulnerabilities or risk exposures had been identified, combined with targeted cybersecurity training and awareness sessions for technical and managerial staff. This integrated approach enabled both immediate remediation of security

gaps and the enhancement of internal cybersecurity capacity.

Between 15 November and 10 December 2025, on-site engagements were carried out for a total of 10 organizations. These activities included vulnerability identification, evaluation of security configurations and exposure levels, delivery of practical training, and provision of tailored recommendations for risk mitigation and system hardening.

4. Events organized / hosted

4.1 Training

In 2025, Public CSIRT/CC of Mongolia delivered cybersecurity training programs upon request, free of charge, as part of its mandate to strengthen national cybersecurity capacity and awareness.

The training programs were tailored to address the specific needs of different target groups, including general employees, cybersecurity and IT professionals, and management-level decision-makers. These initiatives aimed to enhance practical security awareness, promote safe digital behavior, and support institutional resilience against cyber threats.

Training Participation

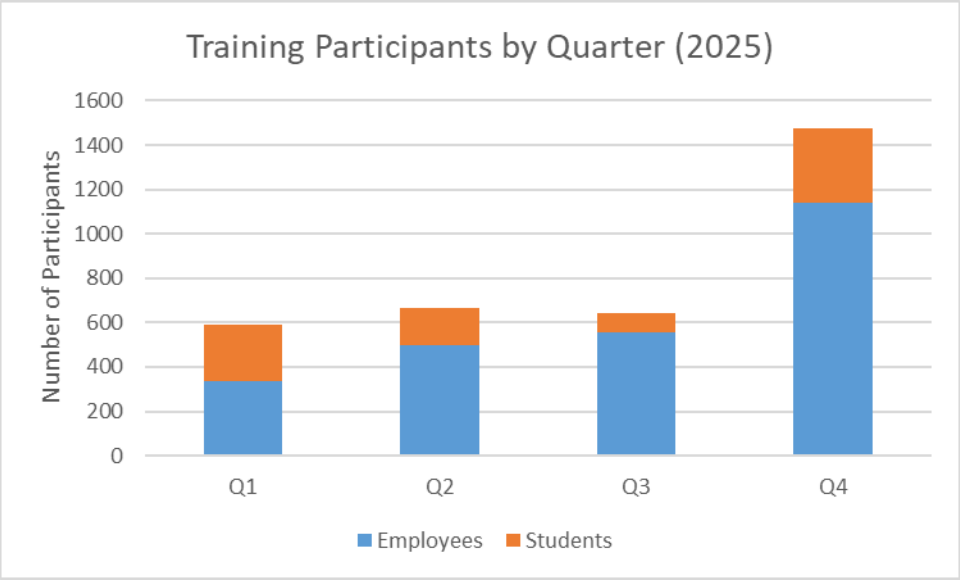
Throughout 2025, training activities were implemented across all four quarters, reaching more than 3,000 participants nationwide. The audience included government officials, organizational staff, as well as students and trainees.

Quarterly breakdown:

- Q1
  - Employees: 334
  - Students: 259
  - Phishing simulation participants: 354
  - Phishing report rate: 23.73%
- Q2
  - Employees: 495
  - Students: 172
  - Phishing simulation participants: 26
  - Phishing report rate: 11.54%
- Q3
  - Employees: 553
  - Students: 90
- Q4

- Employees: 1,137
- Students: 339

These training efforts contributed to strengthening organizational preparedness and improving user-level cyber hygiene across public and private sectors.



As part of the training program, phishing simulation exercises were conducted to assess user awareness and response to cyber threats. During the first half of 2025, a simulated phishing campaign was implemented in Ulaanbaatar involving 380 participants, of whom 87 interacted with the phishing messages, resulting in a click rate of 22.9%.

The exercise revealed persistent gaps in users' ability to identify and appropriately respond to suspicious emails. The findings provided practical insights into user behavior and supported the development of more targeted awareness and capacity-building measures, contributing to improved organizational cybersecurity preparedness.

4.2 Drills & exercises

ITACTIC-2025 Cyber Drill

The Public CSIRT of Mongolia participated in the "ITACTIC-2025" strategic cybersecurity event, held on 13–14 May 2025. This exercise was conducted for the third consecutive year and brought together 22 organizations with over 80 participants. The drill focused on strengthening cyber incident response coordination, enhancing technical and tactical response capabilities, and improving cyber crisis management at the national level. Through active participation, the Public CSIRT team demonstrated strong operational readiness and effective coordination in simulated incident scenarios.

Asia-Pacific Cyber Drill 2025 (ITU)

The Public CSIRT of Mongolia participated in the Asia-Pacific Cyber Drill 2025, organized by the International Telecommunication Union (ITU) in collaboration with the Ministry of Digital Development, Innovation, and Communications. The exercise was held in Ulaanbaatar from 2 to 5 September 2025 and brought together more than 200 participants from 26 countries, including 23 national teams engaged in hands-on cyber incident response scenarios.

The Mongolian team successfully completed all assigned tasks ahead of schedule and secured first place, demonstrating strong technical expertise and effective coordination in incident response operations. This achievement reflects the continued advancement of Mongolia's national cybersecurity capabilities and underscores its active contribution to regional cybersecurity cooperation and capacity building efforts.

Advanced Cybersecurity Simulation Training (Fulbright Program)

The Public CSIRT of Mongolia co-organized and participated in an advanced simulation-based cybersecurity training program conducted from 11 to 15 August 2025 under the U.S. Department of State's Fulbright Program. The training brought together cybersecurity professionals from key national institutions, including the Ministry of Digital Development, Innovation, and Communications, national and public CSIRT teams, the Armed Forces Cyber Command, the National Police Agency's Cybercrime Division, and MNCERT/CC. Delivered by an international cybersecurity expert, the program covered a broad range of technical areas such as cyber incident investigation, network forensics and validation, vulnerability management, web application security, as well as monitoring and detection methodologies. The training emphasized hands-on exercises, simulation-based scenarios, and real-world case studies, while promoting the adoption of international best practices.

4.3 Conferences and seminars

Cyber Sovereignty Forum 2025

The Public CSIRT of Mongolia co-organized the Cyber Sovereignty Forum 2025, a national-level event focused on cybersecurity policy, governance, and strategic coordination. The forum served as a platform for discussing national priorities in cybersecurity and strengthening collaboration among key stakeholders involved in protecting Mongolia's digital environment.

CII Summit - 2025

The Public CSIRT of Mongolia organized the "CII Summit – 2025" conference on 1 May 2025. The event brought together representatives from government agencies, critical information infrastructure (CII) entities, and private sector organizations to discuss key cybersecurity challenges.

Discussions covered national cyber risks, the implementation of cybersecurity legislation, sector-specific vulnerabilities, and practical measures to improve resilience. The summit also emphasized the importance of stronger public–private cooperation in strengthening national cybersecurity.

The event concluded a series of sector-focused consultations conducted in early 2025 and helped improve coordination and information sharing among key stakeholders.

Sectoral Cybersecurity Coordination Meetings (CII Engagements)

To strengthen the protection of Critical Information Infrastructure (CII), the Public CSIRT of Mongolia organized a series of sector-specific coordination meetings across key industries. These engagements involved stakeholders from all CII sectors, including banking and financial services, energy and fuel, healthcare and pharmaceuticals, food and agriculture, telecommunications and Internet Service Providers, as well as relevant government institutions.

CyberSafe Girls Awareness Campaign

The Public CSIRT implemented the "CyberSafe Girls" awareness campaign to prevent cybercrime targeting teenage girls and to strengthen digital safety awareness at the community level. As part of the campaign, a targeted outreach and training activity was conducted for members of the Joint Community Team of Bayanzurkh District, in cooperation with the Bayanzurkh District Citizens' Representative Khural, the Sub-Council for Crime Prevention, and the Women's Council.

The initiative aimed to enhance knowledge and practical skills for preventing cyber-enabled crimes, improve understanding of emerging cyber risks, and promote community-based approaches to protecting vulnerable groups. Discussions also covered international practices, technological solutions, and the role of citizens and local stakeholders in strengthening online safety.

5. International Collaboration

5.1 International partnerships and agreements

APCERT Membership

In 2025, the Public CSIRT of Mongolia became an official member of the Asia Pacific Computer Emergency Response Team (APCERT), marking an important milestone in its international engagement. Following its admission, the Public CSIRT began actively participating in APCERT information sharing activities, including receiving regional cyber threat intelligence and submitting regular weekly situational reports.

MoU with CERT-In (India)

On 9 September 2025, the Public CSIRT of Mongolia signed a Memorandum of Understanding (MoU) with CERT-In (India) to strengthen bilateral cooperation in cybersecurity.

The MoU provides a framework for cyber threat information sharing, capacity building, and joint activities such as

training, seminars, and cyber exercises. The agreement entered into force upon signing and is valid for three years, with the possibility of extension by mutual consent.

FIRST Membership

The Public CSIRT of Mongolia continued its active engagement as a member of the Forum of Incident Response and Security Teams (FIRST). Through this membership, the organization benefits from access to global threat intelligence, coordinated incident response collaboration, and international best practices, further strengthening its operational capacity and international cooperation.

5.2 Capacity building

5.2.1 Cyber Drills & Exercises

Asia-Pacific Cyber Drill 2025 (ITU)

The Public CSIRT of Mongolia participated in the Asia-Pacific Cyber Drill 2025, organised by the International Telecommunication Union (ITU) and held in Ulaanbaatar from 2 to 5 September 2025. The exercise brought together more than 200 participants from 26 countries and featured practical, scenario-based cyber incident response simulations.

The Mongolian team achieved first place, demonstrating strong technical capability, effective coordination, and operational readiness in incident response. In addition to its participation, the Public CSIRT supported national-level preparation and coordination of the event, reinforcing its role in regional cybersecurity cooperation and capacity-building initiatives.

Global CyberDrill 2025

The "Global CyberDrill 2025" international cybersecurity competition was jointly organized by the International Telecommunication Union (ITU), the United Nations Office of Counter-Terrorism (UNCCT), INTERPOL, and the Forum of Incident Response and Security Teams (FIRST). The event was held in the United Arab Emirates in December 2025. Among teams representing 150 countries worldwide, a representative of the Public CSIRT/CC achieved 22nd place in the competition.

5.2.2 Seminars & Presentations

Oxford University Cybersecurity Capacity Assessment (CMM)

The Public CSIRT of Mongolia collaborated with the University of Oxford's Global Cyber Security Capacity Centre (GCSCC) in conducting a national cybersecurity capacity assessment based on the Cybersecurity Capacity Maturity Model (CMM). The assessment findings were presented on 19 February 2025.

The evaluation identified strengths in national cybersecurity policy and governance, while highlighting areas for improvement in technology, standards, and operational practices. The process involved more than 150 experts from over 100 organizations, providing a comprehensive overview of Mongolia's cybersecurity maturity and informing

recommendations for future capacity development.

5.3 Other international activities

Global Digital Forum 2025 (Russia)

Representatives of the Public CSIRT of Mongolia participated in the Global Digital Forum 2025, held in Nizhny Novgorod, Russia, on 5–6 June 2025. The forum focused on strengthening international cooperation and provided a platform to exchange experiences and best practices in cybersecurity.

Tallinn Cyber Diplomacy Summer School 2025

A representative of the Public CSIRT of Mongolia participated in the Tallinn Cyber Diplomacy Summer School 2025, an EU-funded international capacity-building program focused on cyber diplomacy and global cybersecurity governance. The program provided a platform to strengthen knowledge on international cyber norms, digital cooperation, and emerging cyber policy challenges, while facilitating engagement with global experts, diplomats, and policymakers.

CPX 2025 (Thailand)

Representatives of the Public CSIRT of Mongolia also participated in CPX 2025, held in Bangkok, Thailand, from 17 to 22 February 2025. The event covered advanced cybersecurity technologies, threat detection, and incident response strategies, contributing to the enhancement of technical knowledge and operational capabilities.

6. Future Plans

The Public CSIRT/CC of Mongolia will continue its efforts to strengthen the detection, response, and prevention of cybersecurity incidents at the national level. Building on the progress achieved in 2025, the organization aims to further enhance its operational capabilities, expand proactive cybersecurity initiatives, and improve coordination with national and international partners.

One of the main priorities will be progressing towards an advanced level of maturity under the SIM3 CERT maturity model, with a focus on strengthening processes, technical capabilities, and overall organizational effectiveness.

7. Conclusion

In 2025, the Public CSIRT/CC of Mongolia made significant progress in strengthening national cybersecurity capabilities through expanded operational activities, proactive risk management initiatives, and enhanced coordination at both national and international levels. Key achievements included the establishment of a proactive cybersecurity assessment approach, strengthened protection of critical information infrastructure through targeted engagements, and the expansion of capacity building efforts that improved technical competencies and operational readiness.

International cooperation played a central role in advancing Mongolia's cybersecurity development. Active participation in regional and global initiatives, including cyber drills, capacity assessments, and information-sharing mechanisms, contributed to improved situational awareness and institutional capability. Partnerships with international organizations and development partners, including support from initiatives such as JICA, have been instrumental in reinforcing Mongolia's cybersecurity governance framework and promoting sustainable capacity development.

SingCERT

Singapore Cyber Emergency Response Team

1. Highlights of 2025

The Singapore Cyber Emergency Response Team (SingCERT) is part of the Cyber Security Agency of Singapore (CSA). SingCERT serves as a trusted point of contact for cyber incident reporting for the members of the public, private businesses, and international CERTs around the world.

CSA launched three initiatives aimed at promoting cybersecurity awareness and fostering a more secure cyberspace in 2025:

i. Unveiling of the Safe App Portal Pilot
   A online tool that aims to provide clear and actionable safety and security insights on mobile apps.
ii. Quantum-Safe Handbook & Quantum Readiness Index
   Provides a comprehensive resource in preparing for the quantum-safe transition.
iii. 9th Edition of the Singapore Cyber Landscape
   Highlights facts and figures on significant cyber threats and incidents in Singapore for 2024.

2. About SingCERT

2.1 Introduction

The Singapore Cyber Emergency Response Team (SingCERT) is Singapore's national CERT, serving as a trusted point of contact for cyber incident reporting to the members of the public, private businesses, and international CERTs around the world.

It was set up to facilitate the detection, resolution, and prevention of cyber security related incidents on the internet. Besides providing technical assistance and identifying trends in hacking activities, SingCERT also works closely with other security agencies and Internet Service Providers (ISPs) to resolve cybersecurity incidents.

SingCERT's Contact Information:

- Website: https://www.csa.gov.sg/resources/singcert
- Email: singcert@csa.gov.sg

2.2 Establishment

SingCERT was first set up in October 1997 by the then-Infocomm Development Authority of Singapore (IDA), in collaboration with the Centre for Internet Research, National University of Singapore (NUS). SingCERT transited to the Cyber Security Agency of Singapore (CSA) when it was established on 1 April 2015.

CSA is the national body overseeing cybersecurity strategy, operation, education and outreach, technology, and industry development for Singapore's critical information infrastructure. It is managed by the Ministry of Communications and Information and reports to the Prime Minister's Office.

In 2023, SingCERT rebranded from the 'Singapore Computer Emergency Response Team' to the 'Singapore Cyber Emergency Response Team'. The rationale was to modernise SingCERT's branding, as cyber has become a widely recognised and understood term in the context of security and technology, and in many cases, the term computer security has been phased out in favour of cybersecurity. It also better captured the modern interconnected digital landscape and is associated with a more comprehensive and strategic representation of the digital environment.

2.3 Resources

SingCERT publishes specific threat alerts and advisories on cyber threats and trends that affects its constituency on the SingCERT webpage (https://www.csa.gov.sg/resources/singcert). These are broadcasted through the SingCERT subscribers' mailing list, as well as via CSA's Facebook and Twitter platforms. SingCERT also maintains an incident reporting channel, supported by Cyber Aid (https://www.csa.gov.sg/resources/singcert/cyber-aid). Cyber Aid is a tool that helps users with their cybersecurity incidents, as users can get clarity on the cybersecurity issues that they are facing, and advice on how to resolve them.

2.4 Constituency

SingCERT primarily serves the local constituency comprising members of the public and private businesses in Singapore.

3. Activities & Operations

3.1 Scope and definitions

SingCERT provides technical assistance, facilitates communications in response to cybersecurity related incidents, and collaborates with foreign CERT partners in handling cross border cyber threats.
SingCERT also monitors and evaluates global cyber threats and vulnerabilities. It publishes alerts and technical advisories with recommended preventive measures.

3.2 Incident handling reports

SingCERT receives incident reports via our incident reporting channels. Upon receipt of report, SingCERT will assess the incident and advise the victim and any other relevant entity on appropriate steps to take.

In 2025, SingCERT received reports of 5,589 incidents. This resulted in an average of 15.31 incidents per day. The table and graph below show the number of incidents that SingCERT handled over the course of the year.

	Jan – Mar	Apr – Jun	Jul – Sep	Oct – Dec	Total
Number of Incident Reports	1,538	1,208	1,500	1,343	5,589

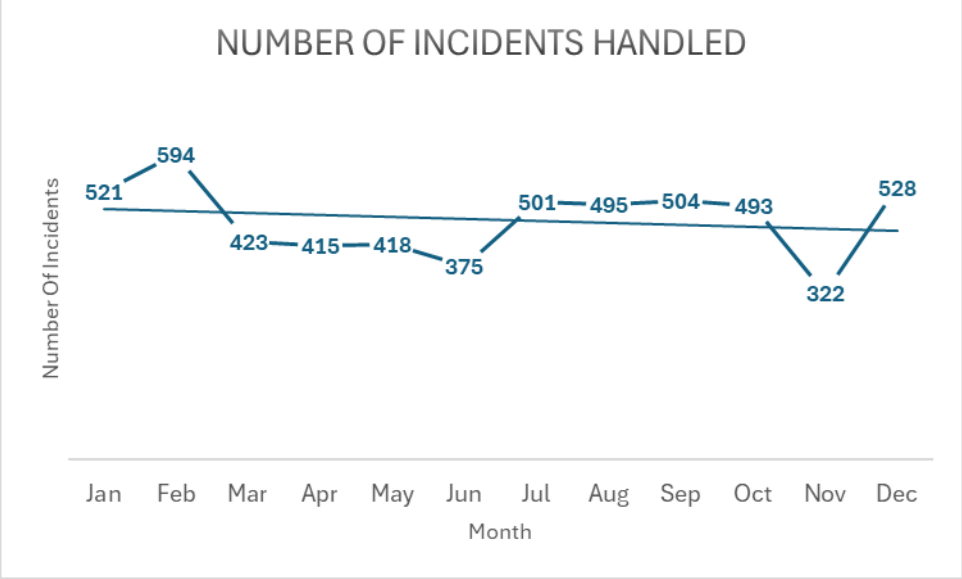


Figure 1: Number of Incidents Reported to SingCERT (2025)

3.3 Abuse statistics

SingCERT receives numerous incident reports on different types of cyber-attacks. As with the previous years, the most common types of cyber incidents handled by SingCERT are phishing, intrusion attempts / attacks, and malware infections.

In 2025, SingCERT handled a total of 5,589 cyber incidents. Phishing was, once again, the most prevalent cyber threat that was reported to SingCERT in Singapore, comprising over 60% of the incidents handled over the course of the year. This has been a trend that SingCERT has observed over the past few years. The phishing threats have also evolved to be more convincing in both the contents and the use of closely similar domain names to legitimate organisations operating in the country.

Cyber Incident Category	# Handled in 2024	# Handled in 2025
Phishing	5443	3567
Intrusion Attempt/Attack	891	988
Malware	475	451
Others	333	275
Vulnerability	351	308

Table 1: Breakup of Cyber Incidents handled (2024 vs 2025)

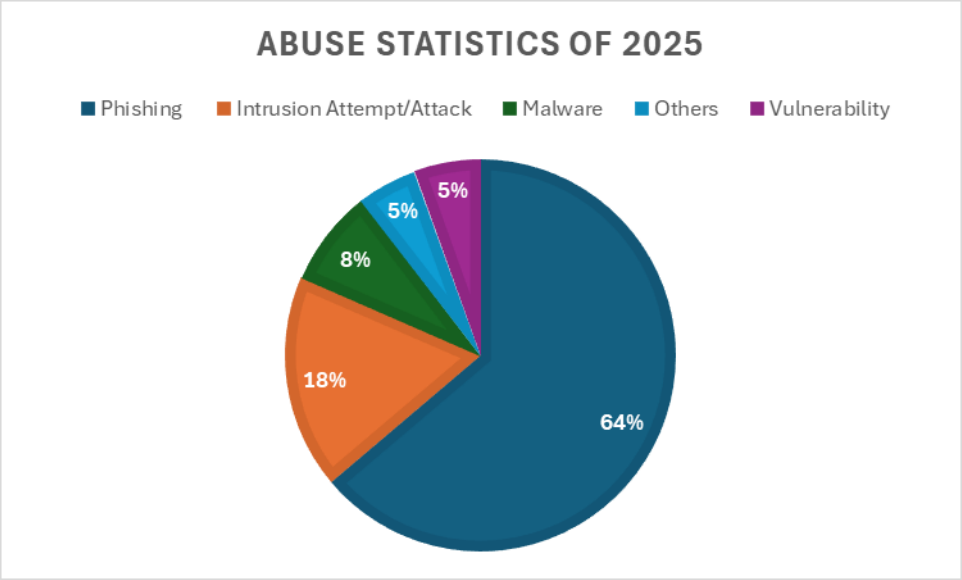


Figure 2: Abuse Statistics (2025)

3.4 Publications and Initiatives

3.4.1 Alerts and Advisories

SingCERT publishes alerts and advisories to raise the awareness and knowledge of our constituents to the current threats and trends, as well as to provide information on emerging threats and vulnerabilities and the recommended mitigation measures to adopt. SingCERT also publishes a weekly Security Bulletin on Wednesdays, which provides a summary of new vulnerabilities, their impacts and affected systems.

In 2025, SingCERT published a total of 148 alerts and advisories, in addition to 52 Security Bulletins, on SingCERT's website. This represented a 12% decrease from the 168 alerts and advisories published in 2024. The chart below shows the month-by-month comparison between 2024 and 2025.

	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Total
2024	14	14	10	14	22	14	19	18	19	8	9	7	168
2025	9	16	11	18	14	14	14	13	9	7	9	14	148

Table 2: Month-by-month comparison of Alerts and Advisories Published (2024 to 2025)

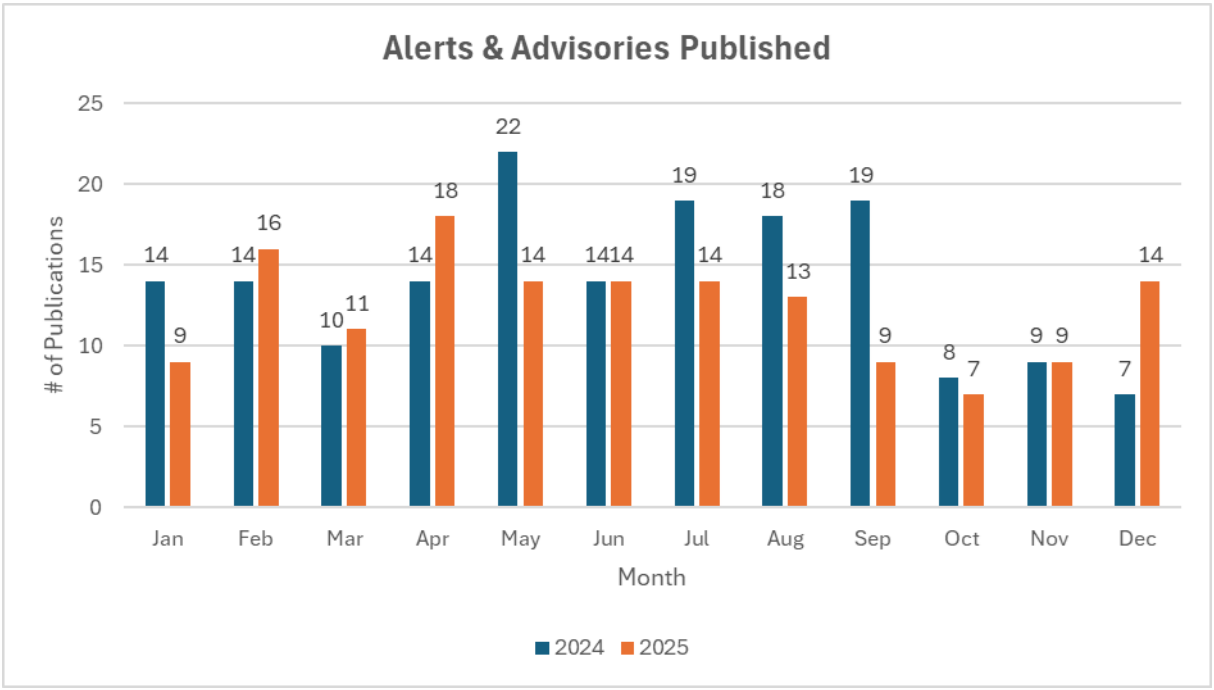


Figure 3: Comparing the Number of Alerts and Advisories Published (2024 to 2025)

Of the 148 alerts and advisories, 114 of them were published to address critical vulnerabilities discovered by software vendors, and the notification of patches released to fix the vulnerabilities. The list of alerts and advisories that were published by SingCERT in 2025 are tabulated below:

Date	Title
10 Jan	Ongoing Mirai Botnet Campaign Targeting Industrial Routers
10 Jan	Active Exploitation of Critical Zero-Day Vulnerability in Ivanti Connect Secure
15 Jan	January 2025 Monthly Patch
16 Jan	Critical Vulnerability in FortiOS and FortiProxy
21 Jan	Vulnerabilities in 7-Zip
21 Jan	Advisory on Phishing Texts Targeting Apple iMessage Users
21 Jan	Advisory on Technical Support Scams
23 Jan	Ongoing Campaign Targeting Amazon Web Services S3 Buckets
28 Jan	Actively Exploited Vulnerability in Apple Products
4 Feb	Critical Vulnerability in Apple Products
4 Feb	Defending Against RedLine Stealer Malware
5 Feb	Multiple Vulnerabilities in Android Products
5 Feb	Joint Advisory on Safeguarding Against Compromise of Cryptocurrency Assets
6 Feb	Critical Vulnerability in Veeam Updater
6 Feb	Critical Vulnerability in Rockwell Automation FactoryTalk View Machine Edition
10 Feb	Multiple Vulnerabilities in Cisco Identity Services Engine (ISE)
11 Feb	Active Exploitation of a Zero-Day Vulnerability in Apple Products
11 Feb	High-Severity Vulnerability in GFI KerioControl Firewalls
12 Feb	High-Severity Vulnerability in Fortinet Products
12 Feb	February 2025 Monthly Patch
19 Feb	Active Exploitation of Cisco Internetworking Operating System eXtended Edition
20 Feb	Critical Vulnerability in Juniper Networks' Products
25 Feb	Critical Vulnerability in SonicWall SonicOS
27 Feb	Critical Vulnerability in Palo Alto Networks PAN-OS
28 Feb	Ongoing Astaroth Phishing Campaign Targeting Gmail, Microsoft and Third-Party Authentication Services
7 Mar	Critical Vulnerability in Elastic Kibana

12 Mar	Active Exploitation of Critical Vulnerabilities in Ivanti Endpoint Manager
12 Mar	March 2025 Monthly Patch
12 Mar	Joint Advisory on Scams Involving Digital Manipulation
24 Mar	Critical Vulnerability in Veeam Software
24 Mar	Critical Vulnerability in Next.js
24 Mar	Critical Vulnerability in Apache Tomcat Software
25 Mar	Active Exploitation of Vulnerabilities in Cisco Smart Licensing Utility
26 Mar	Multiple Vulnerabilities in VMware Products
27 Mar	Zero-day Vulnerability in Google Chrome
28 Mar	Effective IT Change Management: A Guide for Organisations
3 Apr	Critical Vulnerability in Kubernetes Ingress-nginx
7 Apr	Ongoing Campaign Targeting Ivanti Products
8 Apr	Protect Your Systems and Data from Ransomware Attacks
9 Apr	Zero-Day Vulnerability in Microsoft Windows Common Log File System (CLFS) Driver
9 Apr	April 2025 Monthly Patch
11 Apr	Critical Vulnerability in Fortinet's FortiSwitch Web-based Graphical User Interface
15 Apr	Joint Technical Advisory on Akira
15 Apr	Advisory on Cybersecurity for General Election 2025 for Voters
16 Apr	Critical Vulnerability in Apache Roller
17 Apr	Advisory on Cybersecurity for General Election 2025 for Political Parties and Candidates
19 Apr	ADVISORY TO ELECTION CANDIDATES ABOUT FOREIGN INTERFERENCE AND CYBERSECURITY RISKS
21 Apr	Critical Vulnerability in Erlang/OTP SSH Servers
21 Apr	High-Severity Vulnerability in Cisco Webex App
21 Apr	Active Exploitation of Vulnerabilities in Apple Products
25 Apr	Critical Vulnerability in Commvault Command Center
29 Apr	Multiple Critical Vulnerabilities in Planet Technology Industrial Networking Products
30 Apr	Multiple Vulnerabilities in Apache Tomcat Software
30 Apr	Multiple Vulnerabilities in Apple AirPlay Protocol and Software Development Kit
2 May	Joint Technical Advisory on LockBit 3.0 and LockBit 4.0
2 May	Joint Advisory On Malicious Scripts Executed Via A Fake YouTube Channel
13 May	Active Exploitation of SAP's NetWeaver Visual Composer Metadata Uploader
14 May	May 2025 Monthly Patch

16 May	Critical Vulnerabilities in Multiple Fortinet Products
20 May	Critical Vulnerability in WordPress Crawlomatic Plugin
20 May	Joint Advisory on Enhancing Cyber Defences Amidst the Tariff Changes
22 May	Joint Advisory on Safeguarding Online Accounts
26 May	Multiple Vulnerabilities in Atlassian Data Center and Server
26 May	High-Severity Vulnerability in VMware vCenter Server
26 May	Multiple Vulnerabilities in Cisco Unified Intelligence Center, Unified Contact Center Express, and Identity Services Engine
27 May	Active Exploitation of High-Severity Vulnerability in Commvault Software
29 May	Securing Your Cloud Environment when using SaaS Products
30 May	Security Flaw in Microsoft's OneDrive File Picker
2 Jun	Ongoing Botnet Campaign Targeting ASUS Routers
4 Jun	Active Exploitation of Zero-Day Vulnerability in Google Chrome
5 Jun	Critical Vulnerability in Hewlett Packard Enterprise StoreOnce Software
5 Jun	Critical Vulnerability in IBM Tivoli Monitoring
6 Jun	High-Severity Vulnerability in Apache Tomcat CGI Servlet
6 Jun	Critical Vulnerability in Cisco ISE
11 Jun	June 2025 Monthly Patch
19 Jun	Active Exploitation of Critical Vulnerability in Langflow
20 Jun	Multiple Vulnerabilities in Major Linux Distributions
24 Jun	Multiple Vulnerabilities in Advantech Products
26 Jun	Critical Vulnerabilities in Cisco Identity Services Engine (ISE) and ISE Passive Identity Connector (ISE-PIC)
26 Jun	Joint Advisory Against Using NRIC Numbers For Authentication
30 Jun	High-Severity Vulnerability in Notepad++
30 Jun	Active Exploitation of Critical Vulnerabilities in Citrix NetScaler ADC and NetScaler Gateway
1 Jul	Active Exploitation of Zero-Day Vulnerability in Google Chrome
4 Jul	Ongoing Campaign by SCATTERED SPIDER
8 Jul	Choosing the Right Authentication Methods
9 Jul	July 2025 Monthly Patch
10 Jul	Critical Vulnerability in FortiWeb
10 Jul	Ongoing ClickFix Campaign
11 Jul	Critical Vulnerabilities in Multiple SAP Products

11 Jul	Protecting Yourself and Your Organisation from Data Breaches
14 Jul	Critical Vulnerability Affecting Multiple Printer Models
16 Jul	Multiple Vulnerabilities in Alcatel-Lucent OmniAccess Stellar Products
17 Jul	Multiple Vulnerabilities in VMware Products
18 Jul	High Severity Zero-Day Vulnerability in Google Chrome
22 Jul	Critical Vulnerabilities in Microsoft SharePoint
24 Jul	Remediation Guide for a Compromised SharePoint Environment related to CVE-2025-53770 and CVE-2025-53771
1 Aug	Critical Vulnerability in WordPress Theme
1 Aug	Defending Against Scams Targeting National Day Celebrations
7 Aug	Critical Vulnerabilities in Trend Micro Endpoint Security Products
8 Aug	Critical Zero-Day Vulnerabilities in Adobe Experience Manager
14 Aug	August 2025 Monthly Patch
15 Aug	Critical Vulnerability in FortiSIEM
16 Aug	Advisory on New Endpoint Detection and Response (EDR) Killer Tool Used by Multiple Ransomware Groups
17 Aug	Critical Vulnerability in Cisco Secure Firewall Management Centre
18 Aug	Ongoing Dire Wolf Ransomware Campaign
21 Aug	Active Exploitation of Cisco Smart Install Client Vulnerability
25 Aug	High-Severity Zero-Day Vulnerability in Apple Products
27 Aug	Critical Vulnerability in Docker Desktop for Windows
27 Aug	Critical Vulnerability in NetScaler ADC and NetScaler Gateway
4 Sep	Critical Vulnerability in FreePBX Servers
9 Sep	Critical Vulnerability in SAP S/4HANA
10 Sep	September 2025 Monthly Patch
12 Sep	Critical Vulnerabilities in SAP NetWeaver
15 Sep	High-Severity Vulnerability in Samsung Android Devices
19 Sep	Active Exploitation of Zero-Day Vulnerability in Google Chrome
22 Sep	Compromised SonicWall Backup Firewall Preference Files
23 Sep	Ongoing Supply Chain Attack Involving npm Packages
26 Sep	Active Exploitation of Multiple Vulnerabilities in Cisco Products
2 Oct	Active Exploitation of CVE-2025-32463 in the Sudo Command-line Utility

6 Oct	Active Exploitation of Zero-Day Vulnerability in Oracle E-Business Suite
8 Oct	Vulnerability in DuckDuckGo Browser for Android
8 Oct	Critical Vulnerability in Redis
15 Oct	October 2025 Monthly Patch
17 Oct	Multiple High-Severity Vulnerabilities Affecting F5 Products
24 Oct	Active Exploitation of High Severity Vulnerability in Oracle E-Business Suite
5 Nov	Critical Vulnerability in React Native CLI NPM Package
12 Nov	November 2025 Monthly Patch
12 Nov	Joint Advisory On Safeguarding Against The Dangers Of Streaming Devices
17 Nov	Critical Vulnerability in FortiWeb Web Application Firewall
18 Nov	Active Exploitation of Zero-Day Vulnerability in Google Chrome
21 Nov	Active Exploitation of Vulnerability in FortiWeb
22 Nov	Critical Vulnerability Affecting Grafana Enterprise
24 Nov	Active Exploitation of Critical Vulnerability in Oracle Identity Manager
28 Nov	Critical Vulnerability in ASUS AiCloud Routers
4 Dec	Critical Vulnerability in React Server Components and Next.js
10 Dec	Critical Vulnerabilities in Multiple SAP Products
10 Dec	Critical Vulnerability in Ivanti Endpoint Manager
10 Dec	December 2025 Monthly Patch
12 Dec	Critical Vulnerabilities in Multiple Fortinet Products
14 Dec	Zero Day Vulnerabilities in Apple WebKit
16 Dec	Critical Vulnerabilities in Adobe ColdFusion and Experience Manager
18 Dec	Critical Vulnerability in Cisco Products
19 Dec	Vulnerability in Linksys Router
22 Dec	Critical Vulnerability in Hewlett Packard Enterprise OneView Software
22 Dec	Critical Vulnerability in WatchGuard Fireware Operating System
27 Dec	Scammers Impersonating CSA, the SPF, and the MHA
29 Dec	Vulnerability in SmarterTools Software
30 Dec	High Severity Vulnerability in MongoDB Server

3.4.2 Unveiling of Safe App Portal Pilot

CSA unveiled the "Safe App Portal" Pilot, an online tool that aims to provide clear and actionable safety and security insights on mobile apps. It is designed to help developers build more secure apps, strengthen the baseline security of

mobile apps, and enhance public confidence in Singapore's digital ecosystem.

It offers three core functions: App Scan, Safety Rating, and App Report. This portal evaluates app safety and security risks in alignment with established industry standards, including those from the Open Web Application Security Project (OWASP), MITRE Corporation, and Android security guidelines.

More information about the playbooks is available via https://www.csa.gov.sg/news-events/press-releases/csa-unveils-safe-app-portal-pilot.

3.4.3 Quantum-Safe Handbook & Quantum Readiness Index

CSA released a Quantum-Safe Handbook and Quantum Readiness Index (QRI).

Quantum computing is expected to transform industries by enabling new breakthroughs; however, it also introduces the "quantum threat" (the expectation that threat actors will misuse the quantum computers to break the existing cryptography that underpins today's digital infrastructure). To address this risk, organisations need to transit to quantum-safe solutions, a process known as quantum-safe migration.

The Quantum-Safe Handbook provides guidance for organisations, in particular Critical Information Infrastructure (CII) owners and government agencies, in preparing for the quantum-safe transition, as it explains what is at stake, highlights key areas of focus, and sets out practical considerations and resources for organisations to begin building readiness.
The QRI helps organisations translate awareness into action, as it is a self-assessment questionnaire that complements the Quantum-Safe Handbook. It helps system owners and security practitioners gauge their organisation's state of readiness, prioritise key actions, and facilitate informed discussions with senior management.

More information about this is available via https://www.csa.gov.sg/news-events/press-releases/csa-releases-a-quantum-safe-handbook-and-quantum-readiness-index/.

3.4.4 Singapore Cyber Landscape 2024/2025

The Singapore Cyber Landscape (SCL) 2024/2025 publication reviews Singapore's cybersecurity situation in 2024 against a dynamic backdrop of rapid digitalisation, and charts Singapore's efforts in building a safer cyberspace in the past decade. This edition of the SCL also marks a milestone for CSA, which celebrated its 10th anniversary in 2025.

In line with global trends, Singapore 's cyber landscape has faced, and continues to face attacks from Advanced Persistent Threat (APT) activity, which continuously increase in both scale and sophistication. One such group targeting Singapore is UNC3886, focusing on high-value, strategic targets, including critical infrastructure.

This SCL also highlights a notable rise in local threats, as well as the nation's efforts in creating a safe and trustworthy cyberspace, such as initiatives to combat new and emerging cyber threats.

More information about the publication, including a downloadable copy, is available via https://www.csa.gov.sg/resources/publications/singapore-cyber-landscape-2024-2025.

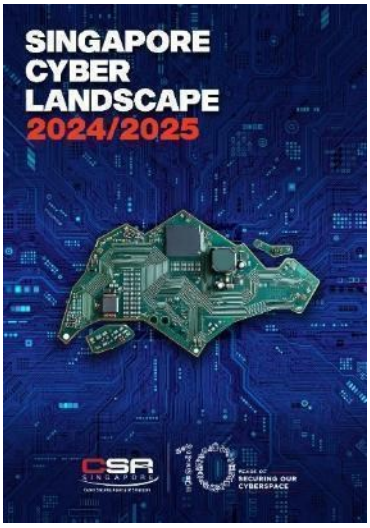


Figure 4: Singapore Cyber Landscape 2024/2025

4. Events organised & hosted

4.1 Drills & Exercises

4.1.1 ASEAN CERT Incident Drill 2025

The ASEAN CERT Incident Drill (ACID) is an annual exercise that Singapore has been convening since 2006, to strengthen cybersecurity preparedness and cooperation within the region.

On 21 and 22 October 2025, SingCERT successfully conducted the 20th iteration of ACID. To mark this special occasion, ACID was organised physically for the first time at the ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE) where the physical facility of the ASEAN Regional CERT is co-located. Themed "Securing Network Devices at the Edge", the scenario for ACID focuses on cyber incidents affecting network edge devices, such as VPN appliances and secure remote access gateways, which often act as the first line of defence. As organisations increasingly rely on network edge devices, the drill enabled participants to learn practical techniques to secure these devices.

Ten ASEAN Member States (AMS), five ASEAN Dialogue Partners and Timor Leste participated in the drill. Participants used the ASEAN Regional CERT's Information Sharing Mechanism (ISM), a centralised communication channel to facilitate cyber threat information sharing, technical exchanges, and cyber exercise coordination, for the first time.

This year's ACID also included a Tabletop Exercise (TTX) developed and moderated by SingCERT, as well as a workshop on strengthening defences against Advanced Persistent Threats (APT), titled "Upskilling Blue Teams: Defending Against

APTs". The TTX saw participants working together to deal with a simulated scenario affecting multiple countries' critical systems, while the workshop gave an overview of the APT cyber landscape and cybersecurity skillsets required for effective blue teams and provided case studies of recent incidents, as well as an interactive walkthrough on how to detect Tactics, Techniques and Procedures (TTPs), which are commonly used by APT actors to compromise a system.

More information about ACID can be found via https://www.csa.gov.sg/news-events/press-releases/certs-from-asean-member-states-gather-in-singapore-for-the-first-time-to-participate-in-the-asean-cert-incident-drill--acid-.

4.2 Conferences and Seminars

4.2.1 Singapore International Cyber Week 2025

The Singapore International Cyber Week (SICW) is Singapore's most established annual cybersecurity event, providing a platform for political leaders, policy makers and thought leaders from around the world to discuss, network, strategise and form partnerships in the cyberspace.

The milestone 10th edition of SICW was held from 21 to 23 October 2025, with the theme "Shaping the Next Era of Global Cybersecurity". It explored the impact of cyber developments on international security and the digital economy and focused on the shifting global environment and reaffirmed the vital role of having an inclusive dialogue in shaping the next era of global cybersecurity. SICW 2025 successfully concluded with more than 14,000 participants from over 90 countries and regions, along with more than 300 exhibitors.

More information about SICW can be found via https://www.sicw.gov.sg.

4.2.2 Cybersecurity Awareness Alliance

One of the ways in which CSA drives cybersecurity awareness efforts, is through the Cybersecurity Awareness Alliance - a collaboration between public and private sector organisations as well as trade associations to raise awareness and adoption of cybersecurity measures. Alliance members actively give talks to schools, businesses, and the community at various platforms.

4.2.3 5th Counter Ransomware Initiative Summit

Singapore hosted the 5th International Counter Ransomware Initiative (CRI) Summit on 24 October 2025 at Marina Bay Sands, in conjunction with the Singapore International Cyber Week 2025. The 5th CRI Summit brought together nearly 150 international representatives from 60 countries, international organisations and private sector entities, reflecting strong global cooperation in the fight against ransomware. This is the first time the Summit is held outside the United States of America (US). Singapore together with Australia, Germany, the United Kingdom (UK), and the US co-chairs the CRI.

The Summit underscored the CRI's commitment to cooperate in combating ransomware and advancing efforts for cybersecurity. Singapore will continue to contribute to the CRI efforts to strengthen international cohesion and collaboration on counter-ransomware policies.

More information about the 5th CRI Summit can be found at https://www.csa.gov.sg/news-events/press-releases/singapore-hosted-the-5th-counter-ransomware-initiative-summit/

5. International Collaboration

5.1 Drills & Exercises

5.1.1 Asia Pacific Computer Response Team (APCERT) Cyber Security Drill 2025

The Asia Pacific Computer Response Team (APCERT) Cyber Security Drill tests the response capabilities of leading Computer Security Incident Response Team (CSIRT) within the regions.

The annual APCERT Cyber Security Drill was held on 29 July 2025 with the theme "When Ransomware Meets Generative AI". This drill reflects emerging real-world cybersecurity threats posed by the malicious use of Generative AI and evaluates the response capabilities of member teams in responding to real incidents and issues that exist on the internet. It also allowed participating teams to review its procedures against evolving Generative AI-enabled threats, emphasising the importance of proactive preparedness in an era of rapidly advancing technologies. As a member of the APCERT Drill Working Group, SingCERT was involved in the conducting of the drill as a part of the Exercise Controller Team.

5.2 Conferences, Seminars & Presentations

5.2.1 Forum of Incident Response and Security Teams (FIRST)

The Forum of Incident Response and Security Teams (FIRST) is an organisation and recognised global leader in incident response. FIRST brings together a wide variety of security and incident response teams including product security teams from the government, commercial, and academic sectors. The Forum is also beneficial to both newly established and matured National CSIRTs as it serves as a platform for networking and collaboration. More details about the organisation can be found at https://www.first.org.

As a member of FIRST, SingCERT attended the FIRST Conference at Copenhagen, Denmark from 22-27 June 2025.

5.2.2 APCERT Annual General Meeting (AGM) and Conference 2025

The APCERT AGM and Conference is an annual event where CERTs from the Asia Pacific region gather to exchange information on the latest cybersecurity issues and incident response methodologies. SingCERT attended the APCERT Annual General Meeting (AGM) and Conference held in Sydney, Australia from 25-27 November 2025.

6. Future Plans

SingCERT will continue with its work in facilitating detection, resolution, and prevention of cybersecurity related incidents. Planning and discussions are in progress for the following workstreams in the year 2026:

S/n	Description	Category
1	Singapore Cyber Landscape 2025	Publications
2	11th Singapore International Cyber Week (SICW)	Events Organising & Hosting
3	21st iteration of ASEAN CERT Incident Drill (ACID)	Events Organising & Hosting

Sri Lanka CERT|CC

Sri Lanka Computer Emergency Readiness Team | Coordination Centre

1. Highlights of 2025

1.1 Summary of major activities

During the year 2025, Sri Lanka CERT carried out a wide range of operational and capacity-building activities to strengthen national cybersecurity resilience. This included conducting extensive training programs, reaching 3,359 government officers and 1,280 police officers across the country, while also enhancing internal expertise through 19 overseas training opportunities for staff. The organization actively supported law enforcement by undertaking 37 digital forensic investigations, including 28 court cases. Proactive threat communication remained a priority, with 18 cybersecurity alerts issued to address emerging risks. Public awareness efforts were significantly expanded through 114 social media posts, 39 awareness videos, 21 newsletters, 21 press releases, and 21 TV and radio programs. In addition, Sri Lanka CERT strengthened organizational security across sectors by conducting 10 network security assessments, 132 application security assessments for 76 organizations, and providing 6 managed security services. Governance and risk management were also reinforced through 23 IT General Control Reviews and 19 risk assessments for Critical National Information Infrastructure (CNII) entities, alongside assessments for non-CNII organizations. Operationally, the CERT handled 8,080 social media-related incidents and 2,851 cybersecurity incidents, demonstrating its central role in national incident response. Furthermore, Sri Lanka CERT contributed internationally as the country coordinator for GLACY-e and as a member of the T-CY Plenary, while also initiating the implementation of an Information Security Management System (ISMS) internally.

1.2 Achievements & milestones

Sri Lanka achieved several significant milestones in advancing its national cybersecurity posture. The country became a member state of the UN Convention Against Cybercrime, reinforcing its commitment to global cybercrime cooperation. Sri Lanka CERT was also elected as a Steering Committee Member of APCERT for the 2026–2028 term, highlighting its growing regional leadership. A major national milestone was the official launch of the National Cyber Security Operations Center (NCSOC), further strengthened by Cabinet approval to onboard 37 Critical Information Infrastructure providers.

The Cabinet of Ministers also approved and launched the National Cyber Security Strategy (2025–2029), providing a strategic roadmap for the country's cybersecurity development. Progress was made toward advanced threat capabilities with the approval to establish the Malware Analysis and Threat Hunting Lab (MATHLAB). Collectively, these milestones demonstrate a strong commitment by Sri Lanka to enhancing institutional capacity, strengthening international collaboration, and building a robust and forward-looking cybersecurity ecosystem.

2. About CSIRT

2.1 Introduction

Sri Lanka Computer Emergency Readiness Team (Sri Lanka CERT) (Pvt) Ltd is a State-Owned Enterprise that serves as the national focal point for civilian cybersecurity in Sri Lanka and currently operates under the Ministry of Digital Economy, the primary government body responsible for leading the nation's digital transformation, strengthening digital governance, and expanding the digital economy under the leadership of His Excellency the President of Sri Lanka. Sri Lanka CERT is mandated to protect the nation's information infrastructure and strengthen national cyber resilience through coordinated prevention, detection, response, and recovery efforts against cybersecurity threats and vulnerabilities affecting government organizations, critical information infrastructure, the private sector, and citizens.

2.2 Establishment

Sri Lanka CERT was established on 1 July 2006 as a subsidiary of the Information and Communication Technology Agency of Sri Lanka (ICTA) to address emerging cybersecurity risks associated with Sri Lanka's digital transformation. In 2018, the organization was separated from ICTA and restructured as an independent institution operating under the relevant line Ministry, enhancing its operational independence and expanding its national-level responsibilities.

2.3 Constituency

The primary mandate of Sri Lanka CERT is to handle cybersecurity incidents at the national level, including malware infections, phishing campaigns, ransomware attacks, data breaches, website defacements, and other emerging cyber threats. In addition to incident response, Sri Lanka CERT provides a comprehensive range of technical advisory and assurance services to government institutions, businesses, and citizens. These services include vulnerability assessments, network security assessments, penetration testing, IT General Controls (ITGC) reviews, and digital forensic investigations. Through these efforts, Sri Lanka CERT supports the protection of digital assets and contributes to the continuous improvement of the nation's overall cybersecurity posture.

3. Activities & Operations

3.1 Incident handling reports

Sri Lanka CERT, as the national focal point for cybersecurity incident reporting and response, continued to receive a significant volume of cyber security and online safety related complaints during 2025. During the year 2025, a total of 12,659 cyber security and social media related incidents were reported to Sri Lanka CERT.

Social media incidents remained the largest category of reported cases, with 9,375 incidents in 2025. The most common issues were hacked accounts (2,867) and fake accounts (2,676), highlighting ongoing account security weaknesses and misuse for impersonation, harassment, and fraud. Reports of harassment and abusive content included 40 cases of child sexual harassment, 38 of child non-sexual harassment, and 1,009 involving adult sexual harassment, reflecting persistent risks to women and children. Hateful or abusive content accounted for 1,514 incidents, while harmful acts reached 632, indicating widespread online hostility and intimidation. False information was reported in 585 incidents, contributing to misinformation. Additionally, 32 incidents involved suicide or self-harm content, 2 related to mental health issues, and 9 involved copyright violations, emphasizing the need for responsible digital behavior and timely interventions.

The continued dominance of social media related incidents highlights the growing need for enhanced digital literacy, stronger platform-level safeguards, and effective reporting and takedown mechanisms.

In 2025, a total of 3,284 cybersecurity incidents were reported, reflecting ongoing technical threats to individuals and organizations. Financial scams (1,817) and general scams (523) remained the leading categories, highlighting the persistent risk of cyber-enabled fraud driven by social engineering. Technical incidents included 551 technical issues, 205 internal inquiries, and 148 cases of phone or laptop loss, underscoring the growing reliance on digital devices and the need for stronger asset protection and incident response. Malware incidents, 9 infections, 4 malicious software cases, and 5 ransomware attacks remained low in volume but posed significant operational and financial risks. Infrastructure related incidents, including 7 website compromises, 2 DDoS attacks, 10 data breaches, and 3 cases of data loss or deletion, highlighted ongoing system vulnerabilities and the importance of proactive security measures.

The cyber threat landscape in 2025 demonstrates that cyber security challenges in Sri Lanka are increasingly human centric, combining technical risks with social media misuse and technology facilitated harms. These trends highlight the importance of continued public awareness programs, strengthened institutional response capabilities, improved collaboration with digital platforms, and the implementation of national cyber security policies and strategies to ensure a safer and more resilient digital environment.

3.2 Publications

The Cabinet of Ministers–approved National Cyber Security Strategy (2025–2029) was officially published by Sri Lanka CERT, providing a comprehensive national framework to guide cybersecurity development, strengthen institutional coordination, and enhance the country's resilience against evolving cyber threats.

3.3 New services

As part of its continued efforts to strengthen national cybersecurity capabilities, Sri Lanka CERT introduced key new services, including the establishment of the National Cyber Security Operations Center (NCSOC) and the Malware Analysis and Threat Hunting Laboratory (MATHLAB). The NCSOC serves as a centralized platform for real-time monitoring, detection, and coordinated response to cyber threats across Critical Information Infrastructure (CII) organizations. By enabling continuous security monitoring and enhanced situational awareness, the NCSOC significantly improves the country's ability to detect, prevent, and respond to cyber incidents in a timely and efficient manner.

Complementing this capability, MATHLAB is being established to strengthen advanced threat analysis and proactive defense mechanisms. The lab focuses on malware analysis, threat intelligence generation, and threat hunting activities to identify sophisticated and emerging cyber threats. Through these services, Sri Lanka CERT enhances its technical capabilities to support organizations in mitigating risks, improving incident response, and building a more resilient national cybersecurity ecosystem.

4. Events organized / hosted

4.1 Training

- Conducted cyber security capacity building sessions for 3,359 government officers and 1,280 Police officers across the country.
- Sri Lanka CERT staff is provided with 19 overseas training programs which enhanced the organization's ability to address emerging threats effectively.

4.2 Conferences and seminars

Sri Lanka CERT successfully organized its annual Cybersecurity Conference for the 16th consecutive year in 2025, continuing its longstanding commitment to fostering knowledge sharing, collaboration, and awareness among cybersecurity professionals, policymakers, and industry stakeholders.

5. International Collaboration

5.1 International partnerships and agreements

Sri Lanka strengthened its international partnerships and engagements in cybersecurity by becoming a member state of the UN Convention Against Cybercrime, demonstrating its commitment to global cooperation in combating cyber threats. Further enhancing its regional leadership, Sri Lanka CERT was elected as a Steering Committee Member of APCERT for the 2026–2028 term. Sri Lanka also participates in the Counter Ransomware Initiative, strengthening international cooperation to combat ransomware threats and enhance collective cyber resilience. In addition, Sri Lanka also participates in global policy and legal discussions as a member of the T-CY Plenary, further reinforcing its role in shaping international cybercrime frameworks and collaboration.

5.2 Capacity building

5.2.1 Training

Sri Lanka actively contributes to international capacity-building efforts by representing the country as the coordinator for GLACY-e, a joint initiative of the European Union and the Council of Europe.

6. Future Plans

6.1 Future projects

- NCSOC – Phase II: Expansion of the National Cyber Security Operations Center (NCSOC) to enhance advanced threat detection and response capabilities.
- Establishment of Dedicated Cybersecurity Training Center Facility: Development of a specialized training facility to strengthen national cybersecurity skills and capacity building.
- Facilities for CERT to Conduct Security Assessments on Advanced Technologies: Establishment of advanced labs to assess emerging technologies and related security risks.
- Establishment of Sectoral CSIRTs – EduCSIRT (Education Sector): Creation of a dedicated CSIRT to support and secure the education sector.
- Establishment of Sectoral CSIRTs – MediCSIRT (Health Sector): Formation of a sector-specific CSIRT to enhance cybersecurity within the healthcare sector.
- Procurement of a Phishing Prevention Tool: Implementation of advanced tools to detect and prevent phishing attacks at scale.
- Facilitating Cybersecurity Higher Education and Certification for Government Employees: Enabling government staff

to pursue higher education and professional certifications in cybersecurity.

7. Conclusion

In 2025, Sri Lanka CERT continued to play an important role in strengthening the nation's cybersecurity posture through a balanced approach encompassing operational excellence, capacity building, policy development, and international collaboration. The organization's proactive efforts in incident response, public awareness, and technical service delivery have significantly contributed to enhancing the resilience of government organizations, critical infrastructure, businesses, and citizens against an increasingly complex and evolving cyber threat landscape.

Key milestones achieved during the year, including the launch of the National Cyber Security Operations Center (NCSOC), the publication of the National Cyber Security Strategy (2025–2029), and strengthened global partnerships, demonstrate Sri Lanka's growing commitment to building a secure and trusted digital ecosystem. At the same time, the increasing volume and complexity of cyber incidents, particularly those driven by social engineering and online misuse, highlight the need for continued vigilance, innovation, and collaboration.

Looking ahead, Sri Lanka CERT remains focused on advancing its capabilities through strategic initiatives such as the expansion of NCSOC, establishment of sectoral CSIRTs, development of advanced technical laboratories, and investment in human capital. These forward-looking efforts will further enhance national readiness to prevent, detect, and respond to cyber threats.

Overall, the progress achieved in 2025 reflects a strong foundation for the future, positioning Sri Lanka to effectively navigate emerging cybersecurity challenges while supporting the country's broader digital transformation agenda.

TechCERT

TechCERT

1. Highlights of 2025

1.1 Summary of major activities

In 2025, TechCERT continued to strengthen its position as a trusted cybersecurity service provider in Sri Lanka, supporting organizations in safeguarding their digital infrastructure against evolving cyber threats. Building on the experience and industry partnerships, TechCERT expanded and delivered a wide range of services. As the demand for cybersecurity continued to grow across industries, TechCERT successfully engaged with major local enterprises and organizations while maintaining an efficient and collaborative working model to ensure timely delivery of services. Throughout the year, we remained committed to enhancing cyber resilience by assisting businesses in improving their security posture and aligning with recognized cybersecurity standards and best practices.

TechCERT Cyber Security Drill

TechCERT conducted three cyber security drills involving organizations from key sectors including banking, finance, telecommunications, manufacturing, and large conglomerates.

- TechCERT Cyber Security Drill for Financial Sector organizations was conducted on 25th June 2025.
- TechCERT Cyber Security Drill for Banking Sector organizations was conducted on 06th August 2025.
- TechCERT Cyber Security Drill for Telecommunications Sector and Other Sectorial organizations was conducted on 17th September 2025.

TechCERT Annual Cyber Security Training and Awareness Sessions

The annual training program was delivered through a series of in-person seminars conducted for selected participants representing each of TechCERT's Managed Security Services clients.

- TechCERT annual training 2025: "Deep Dive into the App Threat Spectrum"
  - Practical demonstration on how modern attackers exploit APIs to compromise web applications
  - Showcase of techniques used in real world scenarios and common vulnerabilities affecting both web and API platforms
- In addition, regular information security awareness sessions were organized for employees of leading banks,

financial institutions, insurance companies, telecommunications providers, and other corporate organizations.

SWIFT Customer Security Program Independent Reviews

TechCERT continued conducting independent security reviews aligned with the SWIFT Customer Security Programme (CSP), further strengthening its ongoing efforts of five years in supporting financial institutions in meeting SWIFT security requirements. Building on the experience and refinements made in previous years, the engagement reflected continued improvements in methodology and assessment practices. During 2025, a leading bank in Sri Lanka partnered with TechCERT to carry out an independent review as part of its SWIFT CSP compliance efforts.

Payment Card Industry – Data Security Standard (PCI DSS) Version Upgrade

The year 2025 marked the adoption of PCI DSS v4.0.1. TechCERT upgraded all its PCI DSS service offerings to align with the latest version of the standard. PCI DSS v4.0 introduced new requirements, some of which became mandatory after March 2025. To support organizations during this transition period, TechCERT proactively provided specialized consulting services to clients who were in the process of upgrading their environments to comply with the new version of the standard and meet the mandatory requirements effective after March 2025.

Security Assessments & Incident Responses

TechCERT Conducted nearly 10000 Security Assessments on various IT infrastructures and responded to nearly 700 Cyber Security incidents.

1.2 Achievements & milestones

TechCERT ISO 27001:2022 Certification

TechCERT has successfully achieved ISO/IEC 27001 certification following the implementation of the required security controls and compliance measures.

2. About TechCERT

2.1 Introduction

TechCERT, being Sri Lanka's pioneering Computer Emergency Readiness Team, plays a vital role in helping both the public and local organizations safeguard their computer systems and networks from cyber threats. By 2025, TechCERT had continued building on over two decades of experience since its establishment as a project of the LK Domain Registry. With a mission to provide a strong cyber security safety net, TechCERT supports entities ranging from general public to large enterprises in responding to cyber incidents and strengthening their overall digital security posture.

TechCERT maintains collaborative relationships with several national and international cybersecurity communities,

including APCERT. Through these partnerships, the organization stays informed about emerging threats, vulnerabilities, and global cyber security trends. This cooperation also enables TechCERT to participate in coordinated responses to cyber incidents that may require multinational support, ensuring effective handling of complex cyber security events.

Beyond incident response, TechCERT actively contributes to improving cyber security awareness and resilience across Sri Lanka. TechCERT regularly publishes security advisories, conducts cybersecurity awareness programs, and organizes workshops related to cybercrime prevention and safe internet usage. In addition, we provide specialized cybersecurity consultancy services, working closely with organizations to design and implement integrated security solutions across diverse IT environments through the expertise of its experienced team of security professionals.

2.2 Establishment

Founded in 2006, TechCERT began as an initiative of the LK Domain Registry together with its academic partners, with the objective of strengthening cybersecurity support for organizations across Sri Lanka. The initiative was created to provide a reliable safety net that could assist both large and small organizations in responding to cyber-attacks and handling cyber emergency situations. As the organization expanded its activities and responsibilities, TechCERT was later incorporated as an independent limited by guaranteed entity while remaining affiliated with the LK Domain Registry, a transition that was formally completed on 5 September 2016 under company registration number GA 3238.

2.3 Resources

TechCERT currently has an expansive technical team of qualified and experienced professionals. The details of the academic/professional qualifications held by all members of the technical team are given below (the majority of the team members have multiple qualifications in different areas of information security, computer systems security, network security etc.):

Name	Designation	Qualification
Prof. Gihan Dias	Chairman	PhD, MSc, BSc Eng (Hons), MIE(SL), CEng
Prof. Shantha Fernando	Director	PhD (TU Delft), MPhil (Moratuwa), MCS (SL), BSc Eng (Hons) (Moratuwa), IET (UK), MIE (SL), CEng
Kushan Sharma	Chief Executive Officer	MBA (Colombo), MSc in Computer & Network Security (Moratuwa), BSc Eng. (Hons)(Moratuwa), C|EH, Certified ISMS Auditor (ISO27001), AMIE(SL), MCS(SL), CPISI (PCI DSS V3.2.1)
Kasun Chathuranga	Chief Technology Officer	MSc in Information Systems Security

		(Moratuwa), BSc Eng. (Hons) in Electrical Engineering, MIEEE, AMIE (SL)
Kalana Guniyangoda	Principal Engineer	MSc in Computer & Network Security (Moratuwa), BSc IT (Hons), GCFA, CHFI, IOS Forensic with Belkasoft, Windows Forensics with Belkasoft, Microsoft Certified: Azure Fundamentals
Geethika Wijerathne	Head of HR & Administration	MSc in Information Systems Management (UOC), PMP, PGDip in ISM (UOC), Chartered Qualification in HRM (CIPM)
Sahan Nanayakkara	Principal Engineer	BICT UCSC, MISM UOC, CPISI (PCI DSS v4.0), ISO 27001: 2013 Lead Auditor, CISM (ISACA), CPISI, CPSCM
Chalana Gunasekara	Principal Engineer	BSc Eng. (Hons) in Computer Engineering, AMIE (SL)
Akila Thuduwewaththa	Senior Manager – Business Operations	BSc (Hons) in Marketing Mgt (UK)
Hirushan Thilanka	Lead Security Engineer	Master of Information Security (UCSC), BSc in Information Systems (UCSC)
Vijan Herath	Project Manager	MSc in Project Management, BSc in Computer Science, HND in Computing (UK), ORACLE HCM (Cert), Project Management & SCRUM Immersion (Cert), CPISI (PCI DSS V3.2.1), PMP Basics (Cert), SFC (Cert), SCDM-FTM
Pubudu Ranasinghe	Senior Information Security Engineer	BSc (Hons) Information Technology (Sp. Cyber Security) - SLIIT, RHCSA (Red Hat 8.0)
Nisal Priyanka	Associate Lead Security Engineer	MSc in Cyber Security (SLIT) BSc (Hons) Information Technology (Sp. Cyber Security) - SLIIT, PGD in Cyber Security
Chamitha Gunawardena	Senior Information Security Engineer	BSc (Hons) Information Technology (Sp. Cyber Security) - SLIIT, ISO 27001: 2013 Lead Auditor, CPISI (PCI DSS V3.2), CCSK
Udeshika N. Alupotha	Senior Information Security Engineer	MSc Information Security (UoC), BSc (Hons) Information Technology (Sp. Cyber Security) – SLIIT, ISO 27001: 2013 Lead

		Auditor, CPISI (PCI DSS V4.0)
Kavindu Viraj Rathnayake	Information Security Engineer	BSc (Hons) Information Technology (Sp. Cyber Security) – SLIIT, NSE 1,2,3 Certification, EC-council Cisco LABS Crash Course, Palo Alto Networks unit
Amal Hewagama	Associate Lead Security Engineer	MBA sp. Project Management (Cardiff Metropolitan), MSc in cybersecurity (SLIIT), BCS PGD, PGD in networking (NSBM), RHCSA, NSE 1,2, Certification, Qualys vulnerability management, CCNA
Lasitha Bandara	Information Security Engineer	BSc (Hons) Information Technology (Sp. Cyber Security) – SLIIT, CPISI, PNPT
Kawya Nayanathara	Information Security Engineer	BSc (Hons) Information Technology (Sp. Cyber Security) – SLIIT, ISO 27001: 2013 Lead Auditor, Foundation Level Threat Intelligence Analyst (arcX)
Priyasuthan Pushparajah	Senior Information Security Engineer	BSc (Hons) Information Technology (Sp. Cyber Security) - SLIIT
Ravindu Pabasara Illeperuma	Information Security Engineer	BSc (Hons) Information Technology (Sp. Cyber Security) – SLIIT, Certified in Cyber Security (ISC2) NSE 1, 2 Certifications, Microsoft Certified Azure Fundamentals
Ravindu Thomas	Information Security Engineer	BSc (Hons) Information Technology (Sp. Cyber Security) – SLIIT, ISO 27001: 2013 Lead Auditor, SWIFT Certified Auditor, Network Security Expert 3
Tharaka Rathnayaka	Information Security Engineer	BSc Eng Hons, Computer Science & Engineering Specializing in Cyber Security (Moratuwa)
Dinethra Hewage	Information Security Engineer	BSc (Hons) Information Technology (Sp. Cyber Security) – SLIIT, eJPT
Sahan Dasanayake	Information Security Engineer	Bachelor of Science (Hons) in Computer Science specializing in Cyber Security (UOK)
Sharadi Gajanayake	Information Security	Bachelor of Science (Cyber Security) in Edith

	Engineer	Cowan University, Microsoft Certified - Azure AI Fundamentals, Microsoft Certified - Azure Security Engineer Associate
Charith Nanayakkara	Information Security Engineer	BSc (Hons) Information Technology (Sp. Cyber Security) – SLIIT, (CC) Certified in Cyber Security by ISC2
Vishvadini Kurukulasooriya	Information Security Engineer	BSc Eng Hons, Computer Science & Engineering Specializing in Cyber Security (Moratuwa)
Anjana Rusitha Kahawevitharana	Senior Information Security Analyst	MSc in Cybersecurity (UCSC), Bachelor of Science (Kelaniya), Bachelor of Information Technology (UCSC), Bachelor of Law (OUSL), ISO 27001: 2013 Lead Auditor
Inuka Wanigasekara	Information Security Engineer	BSc (Hons) Information Technology (Sp. Cyber Security) – SLIIT, eJPTv2, CRTA, CC, PMAT, Mobile Application Penetration Testing
Udesha Ranaweera	Information Security Engineer	MSc in Network & Information Security (Kingston, UK) – Reading, BSc Eng. (Hons) (Peradeniya), AMIE(SL), AZ-104, RHCSA, CIMA Operational Level Completed
Thejan Wijayasinghe	Associate Information Security Engineer	BSc (Hon.) in Industrial Information Technology C|EH, AWS Cloud Practitioner Essentials, C|HFI – Reading, C|ND - Reading
Chamika Kusal	Associate Information Security Engineer	BSc (Hons) Information Technology (Sp. Cyber Security) – SLIIT, Alison Basics of Security Management, Cisco Networking Basics Course
Surekha Sulakshani	Associate Information Security Engineer	Bachelor of Information and Communication Technology (Hons) (Kelaniya)
Wathsala Dewmina	Associate Information Security Analyst	BSc (Hons) Computer Science (University of Westminister), CPTS, eJPT, PT1 (TryHackMe), CRTA, AD-RTS, Professional Certificate in Cyber Security- IIT, Network

2.4 Constituency

TechCERT's constituency comprises its member organizations, private sector organizations, selected government organizations and the public of Sri Lanka. In accordance with its mandate, TechCERT provides effective incident response to malicious cyber threats, widespread security vulnerabilities, identifies and responds to cyber security incidents, conducts training and awareness to encourage best practices in information security and disseminates cyber threat information among Sri Lankan organizations and the public.

3. Activities & Operations

3.1 Scope and definitions

Customers can select from a wide and continuously expanding range of cybersecurity services, including digital forensic investigations, penetration testing, and web and server security assessments, among others. In addition, TechCERT's Managed Security Services offering encompasses a variety of specialized engineering and consultancy services, as outlined below.

- API Security Assessment
- Assumed Breach Assessment
- ATM / POS Security Assessment
- Cloud Security Assessment
- Compromise Assessment
- Cyber Security Drill
- Cyber Security Posture Assessment
- Cyber Security Strategy Development
- Digital Attack Surface Review Assessment
- Digital Forensic Readiness Review
- Digital Forensic Investigation
- Firewall Security Assessment
- Managed Security Services
- Mobile Application Security Assessment
- Threat Hunting
- Vulnerability Assessment
- Web Application Security Assessment

- Physical and Environment Security Checks
- Ransomware Readiness Assessment
- Red Team Exercise
- Review of Cyber Security Incident Management
- Risk Based Vulnerability Assessment
- Router / Switch Security Configuration Assessment
- Security Code Review
- Security Incident Response
- Security Policy Gap Assessment/Security Policy Review
- Security Risk Assessment
- Server Security Configuration Evaluation/Assessment
- SWIFT Security Audit
- Training and Awareness
- Wireless Security Assessment
- Approved Scanning Vendor (ASV) Scan
- Wireless Network Vulnerability Assessment
- Card Data Discovery
- Firewall Security Configuration and rule review
- Network & Security Architecture Review
- Operation Security Assessment
- PCI DSS Certification & Consultancy
- Penetration Testing
- Incident Response Service
- Compromise Assessment
- Incident Response Readiness Check/Review
- Incident Response Training
- PDPA Readiness Review
- Social Engineering Readiness Review
- ISO 27001:2022 Gap Assessment
- ISO 27035 Gap Assessment
- Application Security Architecture Review
- IT Systems Optimization Review
- IOT/IIOT Security Assessments
- External Attack Surface Review Monitoring
- Active Directory Penetration Testing
- LLM Penetration Testing
- Identity and Access Management Configuration Review

3.2 Incident handling reports

During 2025, TechCERT received and handled cybersecurity incident reports from a diverse range of entities, including organizations in the banking, telecommunications, and finance sectors, as well as corporate institutions and members of the public. These reports covered various types of cyber threats and security concerns observed across different environments. The following section presents the statistics related to the cybersecurity incidents reported to TechCERT during the year 2025.

Activity Type	Count
Server Security Compromises	177
Malware Infections	132
Ransomware Related Incidents	144
Social Network Related Incidents	68
Phishing Incidents	17
Website Defacement	23
Other Incident Responses	115

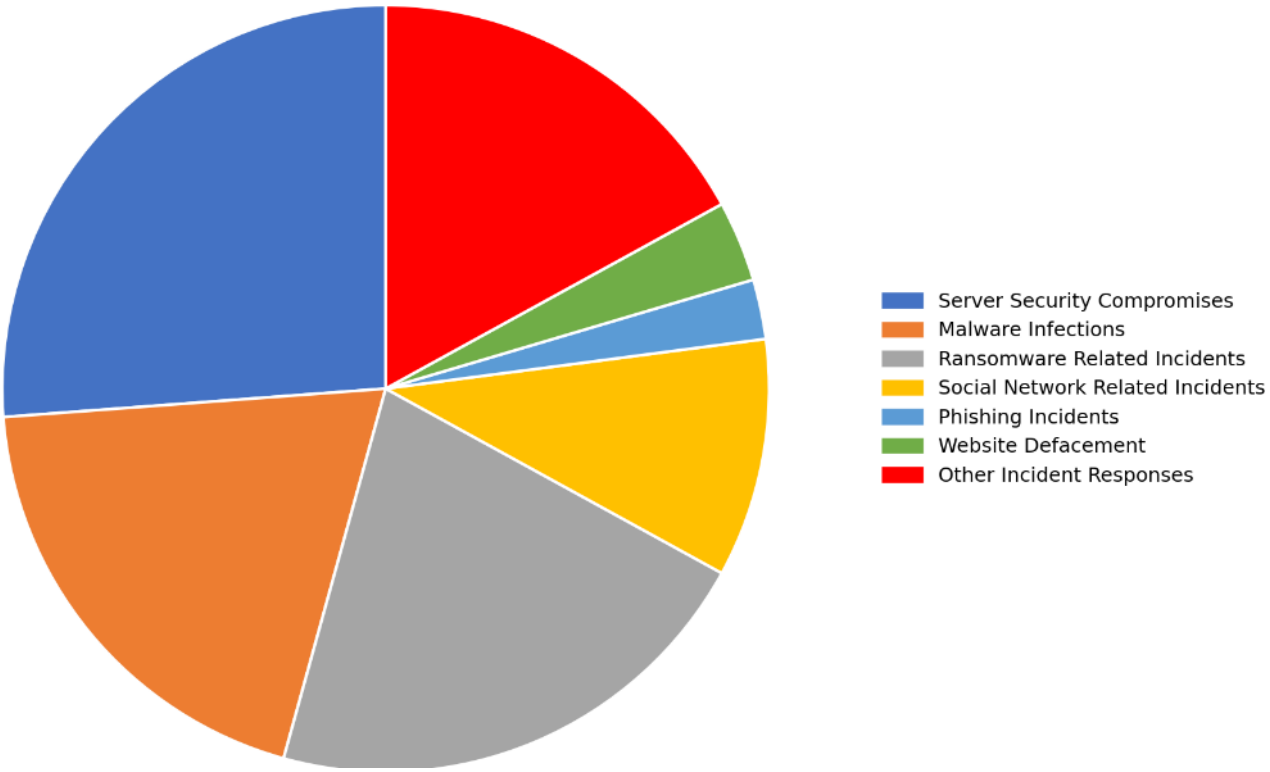


Table 1. Number of Responded Incidents

3.3 Abuse statistics

Server compromises, malware infections, and ransomware incidents continue to represent some of the most critical cybersecurity threats affecting organizations in Sri Lanka. Among the various incident types observed during the year, server security compromises remained in the most frequent and consistently reported category.

3.4 New services

Listed below are services commenced by TechCERT in 2025:

- Assumed Breach Assessment
- Red Team Exercise
- LLM Penetration Testing
- Active Directory Penetration Testing
- Identity and Access Management Configuration Review

4. Events organized / hosted

4.1 Drills & exercises

Apart from being an effective way of sharing knowledge and practical insights with members and clients of TechCERT, these exercises also provide an opportunity to evaluate the existing skills, experience, and readiness of participants. Such initiatives help assess how well individuals and teams respond to simulated cyber incidents while strengthening their overall cybersecurity capabilities. The drills conducted by TechCERT during 2025 are listed below.

- TechCERT Cyber Security Drill 2025– Finance Sector
- TechCERT Cyber Security Drill 2025– Telecommunications Sector and Other Sectors
- TechCERT Cyber Security Drill 2025– Banking Sector

4.2 Conferences and seminars

Cocktail Networking Event – "A Toast to a Secure Digital Future"

As part of the TechCERT's 20-year milestone in cybersecurity, a themed networking and knowledge-sharing event titled "A Toast to a Secure Digital Future" was conducted. The event brought together industry stakeholders to celebrate the organization's journey in strengthening the cybersecurity landscape while also providing insights into emerging cyber threats.

The session included a technical demonstration and discussion under the theme "Modern Cyber Threats Unfolded –

Real-World Insights, Emerging Attack Trends, and TechCERT's Proactive Response."
This event served as both a knowledge dissemination platform and an industry engagement opportunity, aligning with the objectives of conferences and seminars aimed at raising awareness and strengthening cybersecurity collaboration.

5. International Collaboration

5.1 Capacity building

5.1.1 Training

TechCERT enlisted its workforce in a number of external and internal training sessions to enhance their skillset. TechCERT also launched its new internal training program titled "Vanguard", focused at expanding the technical knowledge of all employees. Mentioned below is the list of training sessions undergone by TechCERT employees:

- Internal Training workshops covered under the Vanguard training program so far:
- Introduction to Artificial Intelligence
- Introduction to Kubernetes (K8s) & Conducting a Nessus Scan on Kubernetes-Hosted Applications
- LLM Penetration Testing : OWASP Top 10 – 2025
- Other internal staff skill development training workshops:
- MS Windows Evidence Analysis
- Incident Management Awareness
- Qualys Vulnerability Assessments – Demo
- Information Security Policy Awareness
- Modern Cyber Threats Unfolded - Real - World Insights, Emerging Attack Trends and TechCERT's Proactive Response.

5.1.2 Drills & exercises

To fortify its own employee's collective knowledge, TechCERT participated in the annual APCERT Cyber Drill as follows:

- APCERT Cyber Drill 2025: When Ransomware Meets Generative AI

6. Future Plans

6.1 Future projects and Operation

TechCERT remains committed to strengthening its role in safeguarding the nation's cyber ecosystem and supporting the development of a secure digital environment in Sri Lanka. With a forward-looking vision, the organization has identified several strategic priorities aimed at enhancing service delivery, strengthening national cyber resilience, and expanding cyber security awareness initiatives.

- Achieve sustainable organizational growth while ensuring the efficient and effective delivery of services to

stakeholders and member organizations.

- Continue providing assistance, guidance, and awareness to citizens on the evolving landscape of cyber security threats and digital risks.
- Enhance and maintain the information security posture of member organizations through proactive support, advisory services, and collaborative initiatives.
- Expand the TechCERT Annual Cyber Security Drill to address a broader range of emerging cyber security topics and threat scenarios.
- Conduct additional Cyber Security Drills to engage a larger and more diverse group of participants and strengthen national preparedness.
- Increase information security awareness initiatives targeting university students and the general public to promote responsible digital practices.
- Strengthen and develop the TechCERT team by providing opportunities for staff to acquire new skills, knowledge, and professional expertise in the field of cyber security.

7. Conclusion

In 2025, TechCERT continued to meet and exceed the needs of its patrons by promptly and effectively responding to the evolving cyber threat landscape within Sri Lanka. Key challenges addressed during the year included a significant number of compromised servers, malware infections, and a continued rise in ransomware-related incidents. Recognizing the importance of proactive awareness, TechCERT remained committed to ensuring that its clientele are well informed prior to incidents, thereby minimizing potential operational impact. The organization also strengthened its capabilities by expanding its skilled workforce, welcoming new professionals while enhancing the expertise of existing staff through continuous knowledge sharing and skill development. Maintaining its commitment to consistency, quality, and operational excellence, TechCERT continued to deliver reliable cybersecurity services to all stakeholders. Building on its experience in overcoming challenges, TechCERT remains focused on strengthening cybersecurity preparedness across the nation while prioritizing employee wellbeing through flexible work arrangements and necessary support. As Sri Lanka's leading cybersecurity service provider, TechCERT remains committed to continued growth and to confidently addressing future challenges.

ThaiCERT

Thailand Computer Emergency Response Team

1. Highlights of 2025

1.1 Summary of major activities

- Cybersecurity Incident Response and Digital Forensics: ThaiCERT actively supported agencies by responding to 86 cybersecurity incidents, achieving an average response time of 24 hours. In 2025 ThaiCERT conducted digital forensics for 34 agencies to identify attack root causes and utilized a "Cyber Mobile Response Team" van equipped with advanced tools (like NDR and EDR) to support on-site incident command, threat containment, and evidence collection.
- Vulnerability Management: ThaiCERT provided Vulnerability Assessments (VA) and Penetration Testing for 90 agencies across government, public health, and critical infrastructure sectors. By simulating attacks and analyzing security weaknesses, which categorized vulnerabilities based on NIST severity standards and provided detailed remediation reports to help organizations proactively strengthen their systems.
- Threat Monitoring & Information Sharing: Operating a 24/7 Security Operations Center (SOC), ThaiCERT monitored and analyzed over 116 billion attack attempts and issued over 261,000 proactive alerts. Moreover, ThaiCERT managed Web DDoS protection for 550 critical government websites. A major milestone was the expansion of the Malware Information Sharing Platform (MISP), sharing over 62 million Indicators of Compromise (IOCs) across 223 participating agencies to build a proactive national defense shield.
- Public-Private Partnerships (PPP) & Sectoral CERTs: ThaiCERT drove the establishment of Sectoral CERTs across key industries, including energy, transport and logistics, public health, and finance (such as MOF-CSIRT). The team also regularly hosted the Thailand CERT Community (THCC), bringing together various sectors to exchange threat intelligence, share best practices, and build a unified national defense.
- Capacity Building and Awareness: To cultivate a culture of cybersecurity, ThaiCERT organized extensive training programs and awareness campaigns that reached over 4,500 participants from more than 40 agencies. Notable initiatives included free cybersecurity upskilling projects for SMEs, the "Hack Health" hackathon for hospital personnel, and the "Board Cyber Forum" targeted at corporate executives in the capital market

1.2 Achievements & milestones

- Proactive Defense: Expanded the Malware Information Sharing Platform (MISP) to share over 62 million threat indicators (IOCs) across 223 agencies and actively monitored over 116 billion attack attempts.
- Rapid Incident Response: Successfully handled 86 cybersecurity incidents with an average response time of just 24 hours and completed 90 Vulnerability Assessments (VA) to pre-emptively secure systems.
- National Partnerships: Established specialized "Sectoral CERTs" for critical infrastructure (such as Energy, Transport, and Finance) and partnered with 16 agencies to launch the "DE-fence Platform" against online scams.
- Capacity Building: Trained over 4,500 personnel across more than 40 agencies using interactive Tabletop Exercises (TTX) and extensive upskilling boot camps.
- Global Recognition: Officially announced Thailand's readiness to co-host the prestigious 39th FIRSTCON cybersecurity conference in Bangkok in 2027.

2. About CSIRT

2.1 Introduction

ThaiCERT (Thailand Computer Emergency Response Team) is the national cybersecurity incident response team of Thailand, operating under the National Cyber Security Agency (NCSA). ThaiCERT plays a crucial role in enhancing Thailand’s cybersecurity resilience by coordinating incident response efforts, providing threat intelligence, and supporting organizations in mitigating cyber threats.

As the central point of contact for cybersecurity incidents in Thailand, ThaiCERT works closely with government agencies, private sector, and critical information infrastructure organizations to detect, prevent, and respond to cyber threats. It also collaborates with international cybersecurity communities to strengthen global cyber defense efforts.

Through proactive monitoring, security advisories, and capacity-building initiatives, ThaiCERT aims to improve the overall cybersecurity posture of the country and ensure a safer digital environment for all stakeholders.

2.2 Establishment

ThaiCERT (Thailand Computer Emergency Response Team) was established in 2000 as the national CERT of Thailand. It was originally operated under the Electronic Transactions Development Agency (ETDA). However, in 2019, with the enactment of the Cybersecurity Act, ThaiCERT became part of the National Cyber Security Agency (NCSA), which is responsible for national cybersecurity policy, coordination, and incident response.

ThaiCERT's primary role is to coordinate cybersecurity incident response efforts, provide threat intelligence, and support government agencies, businesses, and critical information infrastructure organizations in handling cyber threats. It also

collaborates with international cybersecurity organizations to enhance Thailand’s cyber resilience.

2.3 Resources

ThaiCERT comprises a team of over 60 professionals dedicated to cybersecurity operations, incident response, and national resilience initiatives. The team is structured into the Cyber Operation Office and the Cyber Coordination Office, ensuring the seamless management of threats and strategic collaboration.

2.4 Constituency

ThaiCERT's responsibilities encompass a diverse range of stakeholders, including critical information infrastructure (CII) organizations in sectors such as finance, energy, public health, and transportation, which are vital for national stability. The agency provides support to government entities at all levels in managing and responding to cyber incidents. Additionally, ThaiCERT promotes the establishment of Sectoral CERTs specialized cybersecurity response teams within specific sectors to enhance coordination and incident management efforts.
ThaiCERT also addresses the private sector's growing cybersecurity needs by offering guidance and resources to mitigate cyber threats. Furthermore, it collaborates with international partners to strengthen cyber threat intelligence and improve national cybersecurity capabilities.

3. Activities & Operations

3.1 Scope and definitions

ThaiCERT’s scope includes cybersecurity incident monitoring, threat intelligence sharing, incident response, and capacity building to enhance Thailand’s cyber resilience. It collaborates with government, private sectors, critical information infrastructure, and international partners. A cybersecurity incident threatens the confidentiality, integrity, or availability of systems, while incident response involves detecting and mitigating such threats. Critical Information Infrastructure (CII) refers to services that are important to national security, military security, economic security, and public order in the country. ThaiCERT aims to strengthen both national and global cybersecurity efforts.

3.2 Incident handling reports

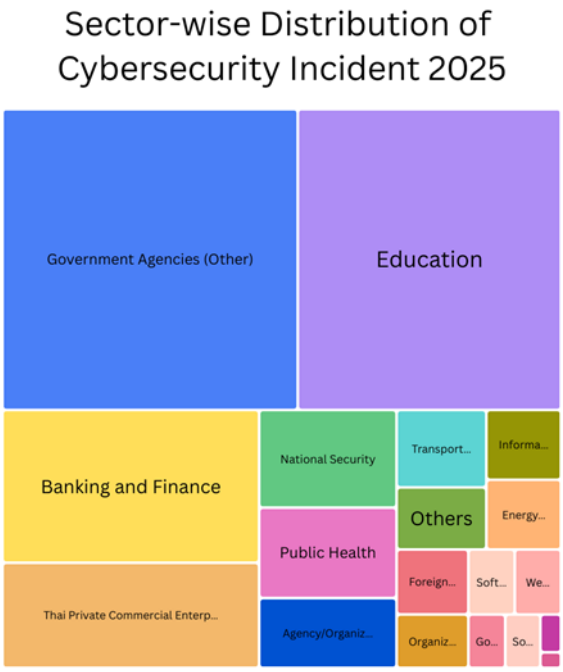
ThaiCERT remains proactive in monitoring and responding to cyber threats. Based on recent data, 3,384 cybersecurity incidents were handled and categorized into primary threat types. The most frequent threat was Intrusion Attempts, with 1,133 cases accounting for approximately 33.48% of all incidents. Information Content Security followed at 908

cases (26.83%), and Fraud made up 706 cases (20.86%) of the total. Availability issues remained a concern, with 559 incidents accounting for 16.52%. Other recorded threats included Malicious Code (73 cases or 2.16%) and Intrusions (5 cases or 0.15%). Notably, there were no reported incidents involving Abusive Content during this period.

In terms of proactive measures, ThaiCERT actively monitored over 116 billion attack attempts and issued 261,642 notifications to warn agencies of potential cyber threats. To build a robust proactive defense shield, we expanded the Malware Information Sharing Platform (MISP) to share over 62 million Indicators of Compromise (IOCs) across 223 participating organizations, allowing them to block malicious activities preemptively. Furthermore, to strengthen cybersecurity defenses and identify system weaknesses before they could be exploited by attackers, ThaiCERT conducted 90 vulnerability assessments (VA) and 24 penetration tests (Pentests) for various government and critical infrastructure entities. Additionally, we fostered incident readiness by organizing Tabletop Exercises (TTX) for more than 12 agencies and over 500 participants, ensuring proactive preparation against complex cyber attacks.

3.3 Abuse statistics

ThaiCERT recorded a diverse range of cybersecurity incidents across multiple sectors, totaling 3,384 reported cases. The Government Agencies (Other) sector was the most affected, with 964 cases accounting for approximately 28.49% of incidents. This was followed by the Education sector with 859 cases (25.38%) and Banking and Finance with 427 cases (12.62%). Thai Private Commercial Enterprises represented 8.57% of the total with 290 cases, while National Security accounted for 4.34% (147 cases). The Public Health sector reported 136 cases (4.02%), followed by Agency/Organization under Cyber Act with 103 cases (3.04%). Finally, sectors such as Transport and Logistics and Energy and Public Utilities represented 2.25% and 1.65% of incidents, respectively.



3.4 Publications

i. ThaiCERT annual report. ThaiCERT releases annual reports summarizing its activities and findings every year.

ii. Monthly report

- IOC (Indicators of Compromise) Monthly Report: This report includes details on specific IoCs identified, trends, and analysis of their potential impact.
- Credential Leak Monthly Report: This report includes the number of leaked accounts, affected sectors, and analysis of the sources and potential impact of these leaks. The information can be used for proactive protection.
- Cyber Attack Monthly Report: This report provides an overview of cyber-attacks that occurred during the month. It includes information on the types of attacks, targeted sectors, and the tactics and techniques used by attackers.

3.5 New services

- "DE-fence" Platform: A joint effort with 16 agencies to block fraudulent calls and scam SMS links.
- Fake Web/App Takedown: Uses AI to automatically hunt and shut down scam websites, fake apps, and compromised APIs.
- Government Website Protection (GWP): A dedicated service protecting 150 critical government websites from being crashed by DDoS attacks.
- DNS Security: Blocks users from accidentally accessing malicious websites, cutting off a major entry point for malware.
- On-the-Ground & Technical Support

- Cyber Mobile Response Van: A rapid-deployment vehicle packed with advanced tech that drives directly to an attacked organization to contain the threat and gather evidence.
- Temporary Security Scanners: ThaiCERT can temporarily install advanced threat-hunting tools (like network monitors and hacker decoys) inside an agency's network during high-risk periods.
- 24/7 Helpdesk App: A round-the-clock support center that agencies can reach via 6 channels, including the newly launched "THCert HelpDesk" mobile app, LINE, and Facebook.

4. Events organized / hosted

4.1 Training

- Cyber Boot Camp: A hands-on training program for new cybersecurity personnel focusing on real-world incident scenarios, malware analysis, and the use of SOC/XDR tools.
- Hack Health (Cybersecurity Hackathon for Hospitals 2024): An event organized in Chiang Mai to raise awareness, elevate medical data security, and train hospital administrators in cyber threat prevention.
- SME Cybersecurity and PDPA Training: A free online and onsite training project organized in collaboration with partners like Thammasat University to help Small and Medium Enterprises (SMEs) build cyber resilience.
- Security Operation Center (SOC) Management Training: Specialized technical training designed to support the establishment of Sectoral CERTs in the transport, logistics, and energy sectors.
- MISP System Usage Workshops: Practical training for government and private agencies on how to actively share and utilize Cyber Threat Intelligence (CTI) through the Malware Information Sharing Platform.
- Deception System Training: Workshops teaching IT personnel how to set up proactive hacker traps, decoys, and analyze attacker behaviour.
- NIST Cybersecurity Framework Training: Capacity-building training specifically targeted at public hospital personnel in Health Region 1 to effectively handle cyber threats.
- Partnered Training Initiatives: ThaiCERT co-organized various training programs, including AI skills training with Microsoft, cloud security with Huawei, youth cyber awareness with OBEC, and national security training with ISOC.

4.2 Drills & exercises

- Thailand’s National Cyber Exercise (NCX) 2024 / 2025: The country's premier, large-scale annual cyber drill that tests incident response, decision-making (War Room format), and technical defense capabilities among government, private, and critical infrastructure sectors.
- Interactive Tabletop Exercises (TTX):
  - Tabletop Exercise Game of Cyber Warz: An innovative digital simulation platform using realistic graphics and animations to train over 500 participants across more than 12 agencies in cyber warfare response.

  - Sasin TTX: A specific tabletop simulation held at the Sasin School of Management to help business executives develop organizational Cyber Resiliency.
  - Cyber Wargame Simulations: Co-organized with the Digital Government Development Agency (DGA) to test practical response skills.
- National Skill Competitions:
  - Thailand Cyber Top Talent 2025 (and Women Thailand Cyber Top Talent): A massive national competition using "Strategic Gamification" to upskill current IT professionals and discover new cybersecurity stars.
  - Software AI & Cyber Operations Contest 2025

4.3 Conferences and seminars

- Thailand International Cyber Week 2025: Co-hosted with VNU Asia Pacific alongside Cybersec Asia 2025, this major event served as a collaborative platform featuring academic seminars, innovation exhibitions, CTF competitions, and business matchmaking.
- Cyber Security Forum 4/2025 (Risk & Self-Assessment): A dedicated national forum focused on analyzing and assessing cybersecurity risks to shape future national policies and protection measures.
- TH-CERT Community Meetings: A continuous series of public-private consultations and seminars designed to share in-depth threat intelligence, track the cyber landscape, and build a unified national defense shield.
- Board Cyber Forum 2025 (Cyber Defense with AI and Innovation Strategies): A specialized seminar specifically targeted at corporate executives and board members in the capital market to teach them crisis management and AI defense strategies.
- Energy CERT Forum 2024: Co-hosted to discuss "The Future of Energy: Innovation, Policy and Cybersecurity," focusing on risk management for the critical energy infrastructure.
- Policy & Workforce Seminars: Hosted strategic forums such as the "Cybersecurity and Cyber Safety for a Digital Workforce" seminar, and public consultations for developing the "National Cybersecurity Industry Promotion Plan".
- Thailand-Israel Cybersecurity Workshop: The 1st workshop of its kind co-hosted with the Embassy of Israel to transfer knowledge and practical experience from Israeli cyber experts to Thai agencies

5. International Collaboration

5.1 International partnerships and agreements

ThaiCERT and the National Cyber Security Agency (NCSA) place a strong emphasis on international collaboration, actively engaging in both bilateral and multilateral frameworks to address increasingly complex global cyber threats. In the 2025 fiscal year, conducted a total of 900 international cooperation activities, comprising 600 bilateral and 300 multilateral engagements.

i. Bilateral Partnerships and Agreements ThaiCERT actively partnered with national CERTs and government agencies worldwide to share threat intelligence and operational strategies:

Israel: Co-hosted the 1st Thailand-Israel Cybersecurity Workshop with the Embassy of Israel to transfer practical experience and defense strategies from Israeli cyber experts to Thai agencies.

- Lao PDR & Malaysia: Welcomed delegations from LaoCERT and Malaysia's NACSA to exchange operational experiences, threat management structures, and discuss future regional threat intelligence sharing.
- South Korea: Partnered with KrCERT/CC and KISA by participating in the 2025 APISC Security Training Course under the TRANSITS-1 curriculum in Seoul.
- Netherlands: Collaborated with the Clingendael Academy for specialized "Cyber Diplomacy" training to strengthen capabilities in international cybersecurity policy and global norms.
- Bhutan: Welcomed Bhutanese government delegates to share knowledge on NCSA's mission, SOC operations, and incident response frameworks.
- Russia: Held a Thailand-Russia bilateral meeting on information security alongside the Kuban Cyber Security Conference.

ii. Multilateral Cooperation Frameworks Thailand is deeply integrated into **regional and global cybersecurity initiatives**:

- United Nations (UN) & ITU: Participated in the 11th UN Open-Ended Working Group (OEWG) on ICT security in New York, partnered with UNIDIR and the Canadian government for a Cybersecurity Capacity Building Programme, and engaged with the International Telecommunication Union (ITU).
- FIRST (Forum of Incident Response and Security Teams): ThaiCERT participated in FIRSTCON25 in Denmark and officially announced Thailand's readiness to co-host the 39th FIRSTCON in Bangkok in 2027.

ASEAN Initiatives:

- Actively advanced the ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC) as a fully established regional training hub.
- Participated in the 16th ANSAC Meeting to drive the establishment of the ASEAN Regional CERT.
- Engaged in the China-ASEAN Cybersecurity Seminar in Beijing and ASEAN defense-civil society network building.

iii. International Corporate Partnerships (MOUs & Agreements) To elevate national infrastructure to global standards, ThaiCERT established agreements with major international technology providers:

- Palo Alto Networks (MoU): Signed an agreement to establish a Cloud Center of Excellence (Cloud COE) to elevate cyber risk management in cloud environments.
- Google Cloud Security: Partnered to enhance the cybersecurity capabilities of Thai government agencies, regulators, and Critical Information Infrastructure (CII).
- TikTok: Formed a collaboration to combat fake news, online scams, and promote safe internet use to drive the regional digital economy.
- Salesforce: Collaborated to develop concrete measures and operational guidelines for preventing and responding to cyber threats

5.2 Capacity building

5.2.1 Training

- Cybersecurity Capacity Building Programme: NCSA co-organized this training in Bangkok with UNIDIR, supported by the Government of Canada, to enhance the cyber capabilities of government agencies, critical information infrastructure (CII), the private sector, and academia.
- Cyber Diplomacy Training: NCSA representatives attended this specialized training hosted by the Ministry of Foreign Affairs in collaboration with the Clingendael Academy (Netherlands) to strengthen capabilities in international cybersecurity policy and global norms.
- 2025 APISC Security Training Course: Thai delegates travelled to Seoul, South Korea, to participate in this advanced course under the TRANSITS-1 curriculum, organized jointly by KrCERT/CC and KISA.
- Cybercrime Investigation Training Course: Participated in a training focused on investigative techniques for online scams and fraud, organized by UNODC.
- ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC): Thailand continued to strongly support and host this regional training hub, which successfully trained 1,474 participants from ASEAN member states to handle complex digital threats.

5.2.2 Drills & exercises

- 2025 APISC Security Training Course: Thai delegates travelled to Seoul, South Korea, to participate in this advanced course under the TRANSITS-1 curriculum, organized jointly by KrCERT/CC and KISA.
- Cybercrime Investigation Training Course: Participated in a training focused on investigative techniques for online scams and fraud, organized by UNODC.
- ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC): Thailand continued to strongly support and host this regional training hub, which successfully trained 1,474 participants from ASEAN member states to handle complex digital threats.

5.2.3 Seminars & presentations

- 2025 APISC Security Training Course: Thai delegates travelled to Seoul, South Korea, to participate in this advanced course under the TRANSITS-1 curriculum, organized jointly by KrCERT/CC and KISA.
- Cybercrime Investigation Training Course: Participated in a training focused on investigative techniques for online scams and fraud, organized by UNODC.
- ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC): Thailand continued to strongly support and host this regional training hub, which successfully trained 1,474 participants from ASEAN member states to handle complex digital threats.
- Workshop for Regional CERT Cooperation and Cybersecurity Standards in ASEAN: Participated in this collaborative workshop held in Japan.

5.3 Other international activities

- **FIRSTCON25 (Denmark)**: ThaiCERT participated in this global conference in Copenhagen alongside experts from over 130 countries. Here, Thailand officially announced its readiness to co-host the 39th FIRSTCON in Bangkok in 2027.
- **Singapore International Cyber Week 2025**: The NCSA Secretary-General attended ministerial-level meetings in Singapore to discuss international standards, AI threats, and regional cooperation frameworks.
- **United Nations (UN) Engagement**: Representatives travelled to the UN Headquarters in New York for the 11th session of the Open-Ended Working Group (OEWG) on ICT security to discuss global cyber cooperation policies.
- **ASEAN & Bilateral Forums**: Actively engaged in the 16th ANSAC Meeting in Cambodia to drive the ASEAN Regional CERT, the World Internet Conference Asia-Pacific Summit in Hong Kong, and the Kuban Cyber Security Conference in Russia.
- **Hosting International Delegations**: ThaiCERT hosted bilateral knowledge-sharing visits from several international bodies, including LaoCERT (Lao PDR), NACSA (Malaysia), the ITU, JICA, and government agencies from Bhutan.
- **Global Corporate Partnerships**: Signed MOUs and collaborative agreements with major global tech providers, including Palo Alto Networks (to establish a Cloud Center of Excellence), Google Cloud Security, TikTok, and Salesforce.

6. Future Plans

6.1 Future projects

To build a robust physical and structural foundation for national defense, ThaiCERT and NCSA have outlined several major projects for 2026:

- Establishing the National Cyber Security Operation Center (NSOC): NCSA plans to establish the NSOC to serve as a central hub, working alongside ThaiCERT, to continuously monitor, track, analyze, and process cyber threat intelligence, as well as issue timely alerts to critical agencies.
- Thailand National Cyber Academy: NCSA is setting up this academy to serve as a comprehensive national hub for knowledge, data, and capacity building for both professionals and the public. As part of this, ThaiCERT plans to develop and roll out two certification-level cybersecurity training programs for the general public in 2026.
- Penetration Testing Laboratory (Cyber Security Lab): A dedicated lab will be established to conduct comprehensive system testing, risk assessments, and vulnerability detection. This facility will also serve as a hands-on training environment for cybersecurity personnel.
- Drafting the National Cyber Incident Response Plan: To handle the growing severity of attacks, ThaiCERT is drafting a national framework for managing cyber crises, which will guide emergency response, recovery operations, and the establishment of dedicated response teams.

- Upgrading the Cyber Threat Management Center and Help Desk: The Help Desk will be enhanced to support multi-channel incident reporting and provide faster mitigation guidance. Concurrently, the threat management center will be upgraded with new dashboards, network Intrusion Detection Systems (IDS), and expanded SIEM hardware to handle growing threat data.
- Legal Amendments and Policy Drafting: By September 2025, NCSA is drafting amendments to the Cybersecurity Act to expand its regulatory coverage to include Cloud Service Providers and Data Centers. ThaiCERT is also preparing for the enforcement of the Cloud Security Standards in September 2026 and will begin drafting the next National Cybersecurity Policy and Master Plan for 2028-2032.

6.2 Future Operation

In terms of operational strategy, ThaiCERT's actions in 2026 will focus heavily on proactive defense, advanced threat readiness, and deeper cross-sector integration:

- Proactive Defense & Expanding MISP: ThaiCERT will shift further toward "Proactive Protection" by expanding the Malware Information Sharing Platform (MISP) to cover the entire country. Which will utilize the international "Traffic Light Protocol" to safely filter and control the sharing of Indicators of Compromise (IOCs) across networks.
- Preparing for Advanced & Quantum Threats: Operations will specifically target emerging and highly complex threats. This includes developing response frameworks for the post-Quantum era (where quantum computers might break current encryption), countering Ransomware 2.0, and defending against AI-driven threats like "Deepfake-as-a-service".
- Zero Trust & Supply Chain Management: Future operations will emphasize the adoption of "Zero Trust" security architectures and place a heavy focus on Vendor Risk Assessments to mitigate vulnerabilities originating from third-party supply chains.
- Sectoral CERT Expansion & GCI Elevation: ThaiCERT will continue to push for and support the establishment of Sectoral CERTs across all critical national sectors. These efforts are directly tied to an operational goal of elevating Thailand's ranking in the Global Cybersecurity Index (GCI) through international collaboration.
- Targeted Data Protection Integration: Following up on initial efforts, NCSA will deepen its collaboration with the Personal Data Protection Committee (PDPC). In 2026, we plan to expand joint operational assessments to 35 high-risk government agencies to actively prevent personal data leaks caused by cyber threats.
- Broadening Awareness: Operations will expand beyond critical infrastructure to cover broader societal risks, including protecting Cybersecurity MSMEs, domestic cybersecurity industries, and implementing measures against cyberbullying.

7. Conclusion

Looking ahead to 2026, ThaiCERT and the National Cyber Security Agency (NCSA) are committed to moving beyond simply "reacting" to incidents. Instead, their operations will focus intensely on "proactive defense" to protect critical

infrastructure and citizens from highly sophisticated threats, particularly those seamlessly utilizing AI technology.

The ultimate strategic goal is to build sustainable "Cyber Immunity" for the country. To achieve this, the agencies will focus on the following key pillars:

- Strengthening organizations, government agencies, and national readiness in parallel.
- Enhancing preparedness to effectively address rapidly evolving cyber threats.
- Promoting sustainability and shared trust across all public and private sectors.

Through these integrated, multi-sectoral efforts, Thailand aims to successfully establish a "Safe, Secure, and Trusted Cyberspace" that protects public interests, builds confidence, and supports long-term digital resilience for everyone.

TWCERT/CC

Taiwan Computer Emergency Response Team / Coordination Center

1. Highlights of 2025

1.1 Achievement & Milestones

TWCERT/CC is committed to strengthening Taiwan's capability to respond to and handle cybersecurity incidents. Over the past year, TWCERT/CC has accomplished the following:

- Received and assisted in handling 599 cybersecurity incident reports from the private sector.
- Published 12 e-newsletters and 42 cybersecurity articles to enhance cybersecurity awareness among enterprises and the public.
- Reviewed and assigned 150 CVE IDs issued on the Taiwan Vulnerability Note (TVN).
- Operated an online malicious file analysis service, scanning 2,301 suspicious files.
- As the convener of the APCERT Training Working Group, organized six online training sessions, engaging 25 APCERT member teams.
- Released *Practical Guidelines for PSIRT Implementation* to assist local enterprises in building and operating effective PSIRT functions.

2. About TWCERT/CC

2.1 Introduction

TWCERT/CC provides services to government agencies, critical infrastructure (CI) providers, and local enterprises, including incident reporting and coordination, product vulnerability disclosure, the Virus Check service, and cybersecurity awareness campaigns. It also fosters intelligence sharing with domestic and international CERTs/CSIRTs, cybersecurity organizations, academic institutions, civil communities, government agencies, and private enterprises. Through these efforts, TWCERT/CC strengthens national cybersecurity defenses and jointly safeguards Taiwan's digital

environment.

2.2 Establishment

Established in 1998, TWCERT/CC merged with TWNCERT in 2024 and is now operated by the National Institute of Cyber Security (NICS) under the Ministry of Digital Affairs (MODA). With an expanded scope of service covering government, industry, and academia, TWCERT/CC enhances its capabilities in cyber threat monitoring, as well as incident coordination and response.

2.3 Constituency

TWCERT/CC is dedicated to enhancing the cybersecurity incident reporting and response capabilities of Taiwan's government agencies, critical infrastructure providers, and the private sector. It collaborates with various stakeholders, including CERTs and ISACs across sectors such as finance, telecommunications, energy, transportation, healthcare, high-tech parks, and academia, as well as MSSPs, law enforcement agencies, and both domestic and international cybersecurity vendors and organizations.

3. Activities & Operations

3.1 Scope and definitions

Key responsibilities of TWCERT/CC:

Incident Response and Early Warnings

TWCERT/CC coordinates cybersecurity incident response for Taiwan’s government agencies, CI providers, and private sector, analyzing and generating early warning intelligence to counter cyberattacks. It also provides the Virus Check service to assist the public in detecting the risk levels of suspicious files. Additionally, as a CVE Numbering Authority (CNA), TWCERT/CC reviews and assigns CVE IDs to vulnerabilities that meet the criteria.

Information Sharing

TWCERT/CC compiles cybersecurity intelligence from domestic organizations, establishing diverse channels for information sharing to foster cross-sector collaboration in cybersecurity.

Awareness Enhancement

TWCERT/CC strengthens the cybersecurity joint defense system by promoting the Taiwan CERT/CSIRT Alliance and raises public awareness through e-newsletters, articles, and awareness videos.

International Collaboration

TWCERT/CC establishes communication channels for domestic and international incident response organizations and facilitates cooperation among global CSIRTs, vendors, and other cybersecurity entities.

3.2 Incident handling reports

In 2025, TWCERT/CC received 599 cybersecurity incident reports from various sources, including enterprises, private organizations, government and individuals. Reports from private organizations accounted for the majority, making up 47.58% of the total.

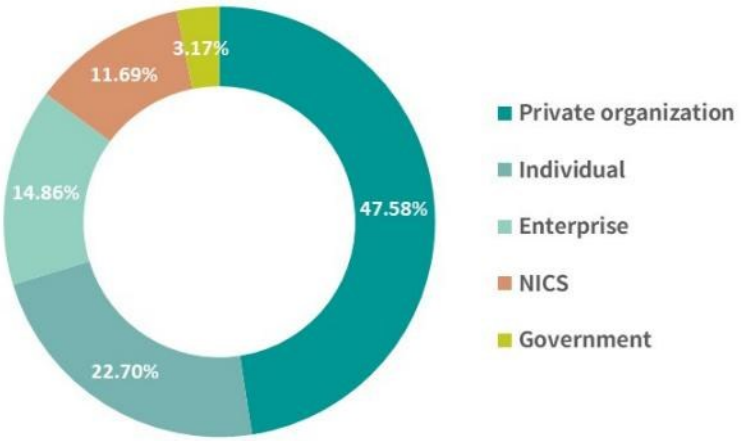


Figure 1. Incident Report Sources

3.3 Abuse statistics

Incident Reports

Among the 599 incident reports received in 2025, the majority involved third-party vulnerability reports at 51.09%, followed by third-party hacking reports at 14.19%, primarily concerning suspected ransomware attacks affecting other enterprises. Phishing website incidents accounted for 12.02% of all reports.

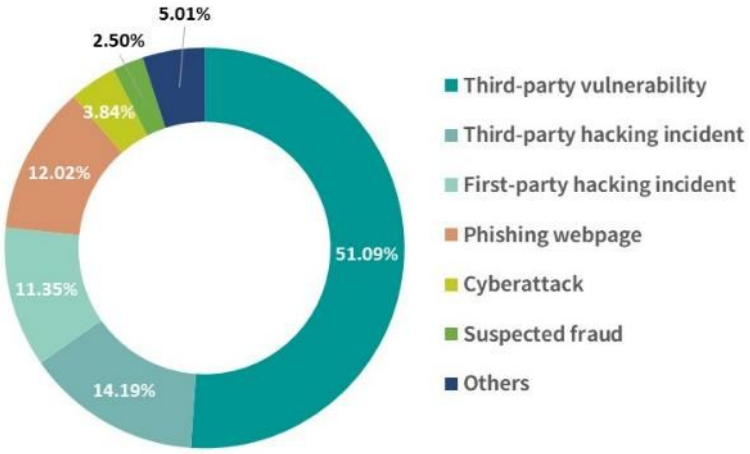


Figure 2. Reported Incident Categories

Domestic Cyber Information Sharing

TWCERT/CC integrates domestic resources and shares cybersecurity intelligence through its system with N-ISAC members, the Taiwan CERT/CSIRT Alliance, government agencies, and private enterprises.

In 2025, TWCERT/CC shared 1,177 pieces of cyber information. Intrusion incidents accounted for the largest portion at 63.47%, followed by vulnerability intelligence at 32.88%. IoCs and early warnings made up 3.06% and 0.59%, respectively.

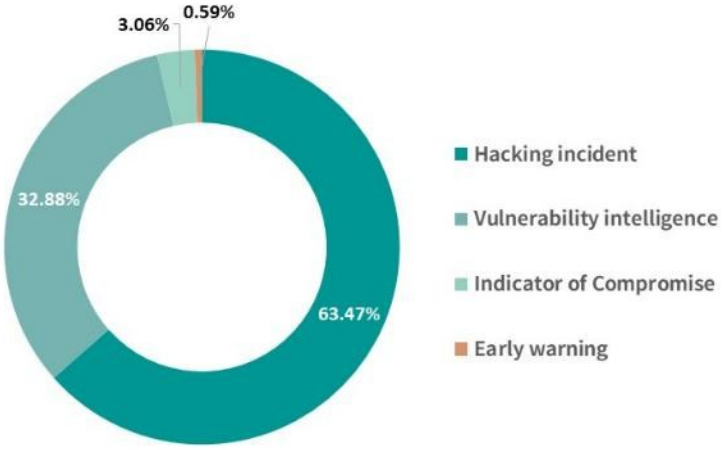


Figure 3. Domestic Cyber Information Sharing

CVE Assignment

In 2025, TWCERT/CC received vulnerability reports from various sources and assigned a total of 150 CVE IDs.

Virus Check

TWCERT/CC provides an online scanning service, allowing users to upload suspicious files for malware detection. The

service first obtains the hash value of the submitted file and searches the threat intelligence to determine whether it is a known malware. It then conducts both static scanning and dynamic analysis to assess potential risks.

In 2025, we analyzed 2,301 suspicious files. Of those, 651 were identified as risky through static scanning, while 974 were determined to be risky through dynamic analysis.

3.4 Publications

E-newsletters and Cybersecurity Articles

TWCERT/CC publishes monthly e-newsletters and articles to provide the latest cybersecurity news, vulnerability alerts, and threat analyses. This helps the public stay informed and enables enterprises to respond to attacks and deploy defenses promptly. The newsletters also compile training resources and relevant information to facilitate public participation, aiming to enhance cybersecurity awareness and better prepare for potential risks.

In 2025, a total of 12 newsletters and 42 cybersecurity articles were released, covering the rapid evolution of hacking techniques and emerging defense challenges. Key trends highlighted include the increasing sophistication of social engineering and phishing attacks, the potential weaponization of both AI and open-source vulnerabilities, the rise in targeted attacks against government agencies and critical industries, and the emergence of fileless malware and interactive intrusion, emphasizing the importance of timely protection and incident response capabilities

3.5 New services

Practical Guidelines for PSIRT Implementation

In response to the increasing risks of product vulnerabilities and supply-chain threats, as well as growing international cybersecurity requirements (such as the EU CRA and the US NIST framework), TWCERT/CC developed the *Practical Guidelines for PSIRT Implementation* to serve as a reference for enterprises in establishing and operating a PSIRT. The guidelines are based on the FIRST PSIRT Services Framework and incorporate a PDCA (Plan-Do-Check-Act) cycle for continuous management, outlining processes for vulnerability management and incident response. It aims to strengthen enterprises' ability to respond to security incidents throughout the product lifecycle while enhancing overall cybersecurity governance maturity and external trust.

4. Events organized / hosted

In 2025, TWCERT/CC organized a blue team exercise for enterprises and hosted its annual conference to expand the exchange of cybersecurity incident response and threat intelligence among local enterprises. These efforts aimed to promote incident reporting within local businesses and enhance cybersecurity awareness.

Blue Team Exercise for Enterprises

On September 12, TWCERT/CC hosted a blue team exercise with 40 companies and 80 cybersecurity professionals. Using the cyber range and guided by instructors, participants practiced real-world cybersecurity incident investigation techniques and strengthened their ability to respond to and analyze cybersecurity incidents.

2025 TWCERT/CC Annual Conference

On December 3, TWCERT/CC held the **2025 Taiwan Cybersecurity Incident Response Annual Conference, which was attended by 927 participants.** The conference focused on challenges in incident reporting and response in the era of AI-driven attacks, as well as product security, featuring insights and experiences shared by experts from both industry and government-affiliated organizations.

5. International Collaboration

5.1 International partnerships and agreements

TWCERT/CC actively participates in the member activities of international organizations, including regular meetings, working group activities, annual conferences, and other collaborative initiatives. Currently, TWCERT/CC is involved with the following international organizations:

- APCERT
- FIRST

5.2 Capacity building

5.2.1 Training

As the convener of the APCERT Training Working Group, TWCERT/CC coordinated member teams and organized 6 online training sessions in 2025:

Date	Topic	Trainer
Feb. 24	Ransomware Trends and Case Studies	KrCERT/CC
Apr. 29	Centralized Threat Monitoring/Threat hunting	NRD Cyber Security
Jun. 24	Using AI to Enhance Incident Response in CERTs	Cybersecurity Malaysia
Aug. 26	Introduction to Malware Analysis Methods	Huawei PSIRT
Oct. 28	Cybersecurity exercises for Taiwan's government agencies and critical infrastructures	TWCERT/CC
Dec. 30	Impact of AI on Cyber Threat Intelligence (CTI)	CERT-In

5.2.2 Drills & exercises

On July 29, the APCERT Drill, titled **"***When Ransomware Meets Generative AI",* was held. TWCERT/CC successfully completed the scenario-based exercise within the allocated time.

6. Conclusion

Looking ahead, TWCERT/CC will continue to strengthen its core services in cybersecurity incident reporting, vulnerability disclosure, and threat intelligence sharing, enhancing response efficiency and cross-organization collaboration to help private sector address increasingly complex attacks and supply-chain risks. At the same time, TWCERT/CC will promote the practical implementation of PSIRTs, supporting enterprises in integrating product security incident response throughout the entire lifecycle in alignment with international cybersecurity standards and regulatory requirements. By deepening public-private partnership, expanding international cooperation, and optimizing system platforms, TWCERT/CC aims to improve information sharing and service accessibility, thereby reinforcing overall cybersecurity resilience and trust.

Activity Reports from APCERT Partners

APNIC

Asia Pacific Network Information Centre

1. About the Organization

APNIC (Asia-Pacific Network Information Centre) is a non-profit Regional Internet Registry (RIR) established in 1993. It manages IP address space and Autonomous System Numbers (ASNs) for the Asia-Pacific region. APNIC supports Internet stability and security through capacity building, collaboration with CERTs/CSIRTs, engagement with law enforcement, and information sharing across the security community.

2. Activities & Operations in 2025

2.1 APNIC Community Honeynet Project

- Continued operating the APNIC Community Honeynet Project, providing threat data to APNIC members through DASH, ShadowServer, and the MISP community.

2.2 APNIC60 Conference

- Hosted the FIRST-TC Da Nang event as part of the APNIC60 Conference in Da Nang, Vietnam.

2.3 Sponsorship for security community events

APNIC provided sponsorship for security community events in the region:

- Phoenix Summit 2025 – Dhaka, Bangladesh
- ACAD CSIRT Summit – Bandung, Indonesia
- CERT Kiribati Cyber Drill & Security Bootcamp 2025 – Tarawa, Kiribati
- MNSEC 2025 – Ulaanbaatar, Mongolia
- Team Cymru RISE Asia Pacific – Kuala Lumpur, Malaysia

3. Collaboration with APCERT members/partners

The following is some of the activities of APNIC members that APNIC supported or participated

- CERT Vanuatu – Cybersecurity Bootcamp 2025 (May 2025)
- CERT Tonga – Training and TWICT Cybersecurity Bootcamp (July 2025)
- KrCERT/CC - APISC Security Training Course (August 2025)
- BtCIRT – Cyber security workshop and Annual Conference (October 2025)
- APCERT – APCERT Annual General Meeting and Conference (November 2025)

CERT-GIB

Computer Emergency Response Team Group-IB

1. About the Organization

CERT-GIB (https://group-ib.com/) is the Computer Emergency Response Team created by the global cybersecurity company Group-IB. It is launched with the mission to immediately contain cyber threats, regardless of when, where they take place, and who is involved. CERT-GIB combines the power of human intelligence with technological prowess to offer the most effective response and remediation actions.

Group-IB adopted a decentralized operational strategy enabling collective action against cybercrime and comprehensive coverage of threat actors across all geographies for information exchange as the only effective long-term solution. Group-IB's GLOCAL strategy ensures the most robust response to cybercrime worldwide through its Digital Crime Resistance Centers (DCRCs), which deliver immediate, comprehensive, localized expertise and intelligence support. DCRC network spans multiple strategic locations, including Singapore, the Netherlands, UAE, Saudi Arabia, Vietnam, Malaysia, Thailand, Italy, Uzbekistan, Chile, and Egypt.

Group-IB introduced the Cyber Fusion Center (CFC) as an intelligence-driven evolution of the traditional SOC, designed to unify threat intelligence, hunting, and response into a single, proactive ecosystem. By fusing internal telemetry with external intelligence, the CFC moves beyond the reactive nature of a traditional SOC to anticipate and disrupt attacks during the adversary's reconnaissance phase.

Aside from being an APCERT member, CERT-GIB is a member of Trusted Introducer, Anti-Phishing Working Group (APWG), FIRST, OIC-CERT, Europol European Cybercrime Centre's (EC3) Advisory Group on Internet Security, and a strategic partner of Afripol and the International Multilateral Partnership Against Cyber Threats (IMPACT).

2. Activities & Operations in 2025

2.1 Operations

Operation Secure with INTERPOL

In early 2025, Group-IB played a pivotal role in Operation Secure, a major INTERPOL-led initiative that successfully dismantled infostealer infrastructure in Asia, protecting over 216,000 potential victims. The operation resulted in 32

arrests and the takedown of more than 20,000 malicious domains and IPs. Group-IB's High-Tech Crime Investigations and Threat Intelligence teams provided the mission-critical data that fueled the operation, specifically identifying compromised user accounts, analyzing the command-and-control (C2) infrastructure for malware like Lumma and Risepro, and tracking dark web and Telegram channels used to sell stolen data. By sharing this actionable intelligence with INTERPOL and local agencies in Vietnam, Sri Lanka, and Hong Kong, Group-IB enabled law enforcement to seize 41 servers and 100GB of criminal data, effectively disrupting the Malware-as-a-Service (MaaS) ecosystem.

Operation ALTDOS takedown with the Royal Thai Police and Singapore Police Force

In early 2025, Group-IB played a critical role in a joint operation with the Royal Thai Police and the Singapore Police Force that led to the arrest of a prolific cybercriminal responsible for over 90 data leaks worldwide, including 65 in the Asia-Pacific region. Operating under aliases such as ALTDOS, DESORDEN, GHOSTR, and 0mid16B, the individual exfiltrated more than 13TB of personal data and blackmailed victims by threatening to notify regulators and the media. Group-IB's High-Tech Crime Investigation and Threat Intelligence teams provided the essential breakthrough by using dark web monitoring technologies to correlate the cybercriminal's shifting digital personas, writing styles, and attack patterns across multiple years. By identifying the technical link between these aliases and tracking the individual's infrastructure—including the use of SQL injection tools and compromised RDP servers—Group-IB enabled law enforcement to execute raids that resulted in the seizure of electronic devices and luxury goods purchased with criminal proceeds.

GoldFactory — Mobile banking app phishing in APAC

Group-IB uncovered a mobile-app phishing campaign in the Asia-Pacific region tracked back to GoldFactory, notorious for stealing facial recognition data. The group is injecting legitimate banking apps with malicious code, combining hooking frameworks, remote access trojans, social engineering, and real-time streaming to hijack devices and steal from users across Southeast Asia. The activity involves distributing modified banking applications that act as a conduit for Android malware, with the first cases detected in Thailand and subsequently spreading to Vietnam and Indonesia.

Immediate Era — Singapore investment scam

Group-IB identified a large-scale scam operation that misappropriates the images and likeness of Singapore officials, including Prime Minister Lawrence Wong, to deceive citizens into engaging with a fraudulent investment platform. The scam campaign relies on paid Google Ads, intermediary redirect websites, and highly convincing fake webpages. Group-IB's analysis revealed that 28 verified advertiser accounts, 52 intermediary domains, and 119 malicious domains impersonating mainstream news outlets were used in the operation.

2.2 Anti-Phishing and Anti-Scam Activities

In 2025, CERT-GIB detected more than 96,000 phishing websites, marking a 17% increase over the previous year. In APAC, the most targeted industries were financial services, government and telecommunications, accounting for 62.33%, 32.22%, and 4% of phishing websites, respectively.

CERT-GIB also detected more than 150,000 scam resources, with nearly 82% of observed scams in APAC targeting the financial institutions.

One of the key responsibilities of CERT-GIB is not only to detect violations, but also to take down violating resources. CERT-GIB actively interacts with domain name registrars, TLD administrators, ISPs, as well as with other CERT and CSIRT teams to eliminate the violations.

In 2025, CERT-GIB responded to more than 26,000 phishing resources and 118,000 scam resources, achieving successful takedowns of 99% of these.

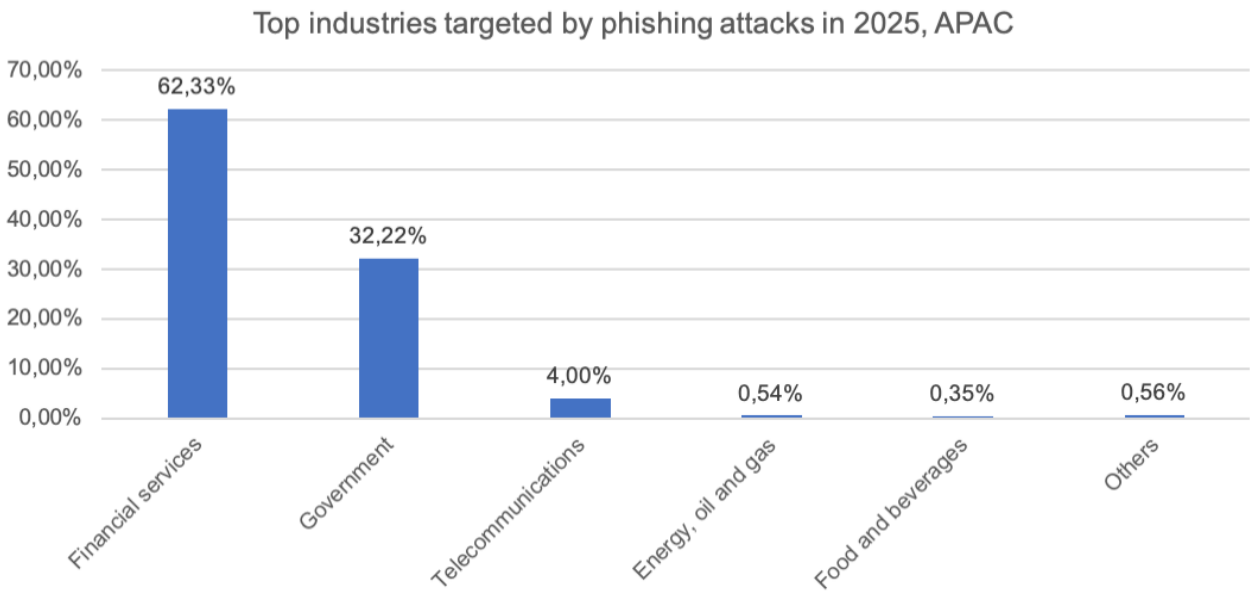


Figure 1. Top industries in APAC targeted by phishing attacks in 2025

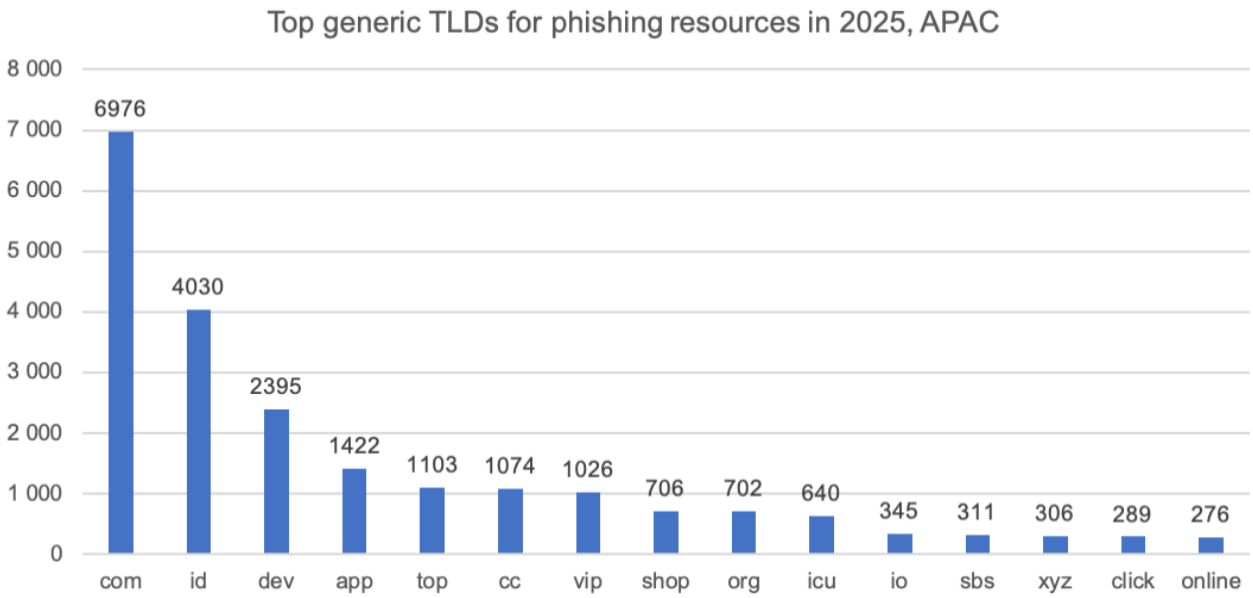


Figure 2. Top generic TLDs for phishing resources in 2025, APAC

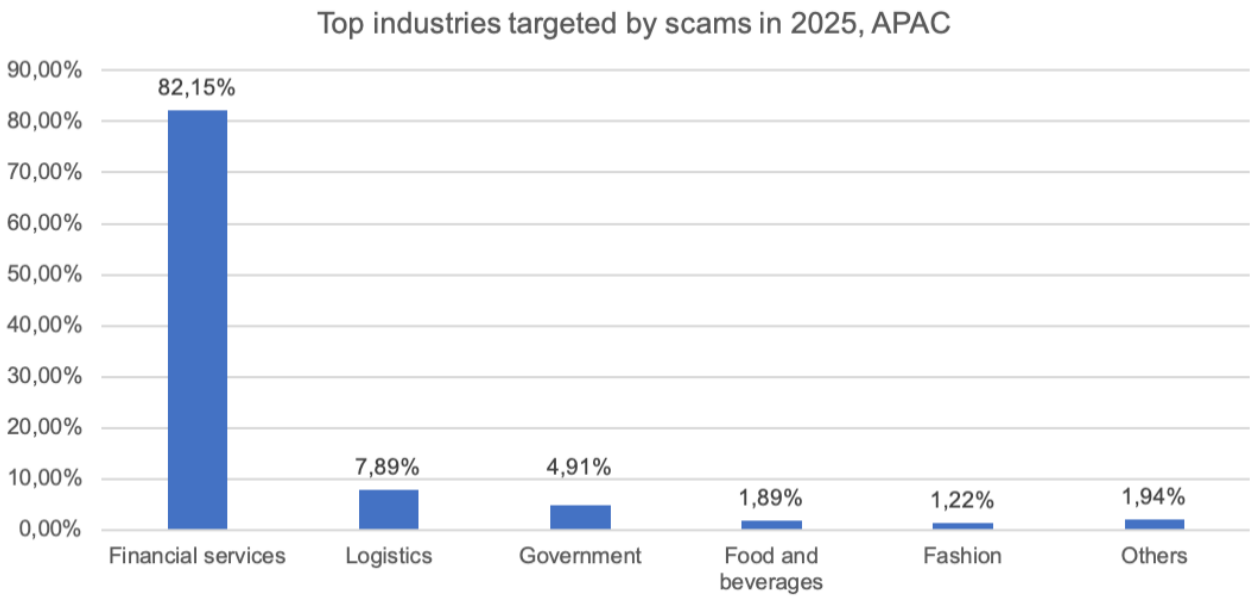


Figure 3. Top industries in APAC targeted by scams in 2025

2.3 Activities

No.	Description	Date
1	Operation ALTDOS takedown with the Royal Thai Police and Singapore Police Force.	February 2025
2	Cybersecurity Malaysia (CSM) Symposium in Cyberjaya, Australia.	5 February 2025
3	APAC Intelligence Insights Webinar.	19 February 2025
4	Fraud & Financial Crime Summit NSW in Sydney, Australia.	20 February 2025
5	Special Lecture by Group-IB Strategic Adviser Craig Jones to Senate of Thailand in Bangkok.	28 March 2025
6	APAC High Tech Crime Trends Webinar.	3 April 2025
7	Cyber Voyage Guard Day in Shenzhen, China.	26 April 2025
8	Fraud Protection Roundtable in Mumbai, India.	16 May 2025
9	Brunei Cybersecurity Association Visit in Kuala Lumpur, Malaysia.	20 May 2025
10	Operation Secure with INTERPOL.	June 2025
11	National Australia Bank (NAB) Interbank Event in Melbourne.	5 June 2025
12	Cyberwarrior X Royal Thai Armed Forces Event in Bangkok.	15 July 2025
13	ASEAN 5G & OT Security Summit in Malaysia.	16 - 19 July 2025
14	Cybersecurity, IT Assurance & Governance (CIAG) Conference organized by the Malaysia Chapter of ISACA (Information Systems Audit and Control Association) in	20 - 21 August 2025

	Kuala Lumpur.	
15	Royal Malaysia Police Force (PDRM) Special Dialogue in Kuala Lumpur.	26 August 2025
16	Thai CyberX by NCSA (National Cyber Security Agency) in Bangkok.	28 August 2025
17	International Economic Crime Conference (IECC) by the Singapore Police Force (SPF).	1 September 2025
18	CySec Brunei in Bandar Sri Begawan.	3 - 4 September 2025
19	CISO Roundtable in Melbourne, Australia.	11 September 2025
20	APAC Intelligence Insights Webinar.	23 September 2025
21	Smart Banking Summit in Hanoi, Vietnam.	25 September 2025
22	Singapore Digital Crime Resistance Center (DCRC) and Cyber Fusion Center (CFC) Showcase in Singapore.	22 October 2025
23	GovWare in Singapore.	21 - 23 October 2025
24	Royal Malaysia Police Force (PDRM) Workshop in Kuala Lumpur.	28 October 2025
25	Malaysia Ministry of Defence (MINDEF) Technology Updates Workshop in Kuala Lumpur.	5 November 2025
26	CISO NZ Summit.	18 November 2025
27	Annual Group-IB Security (GSEC) Day in Hanoi, Vietnam on 11 December 2025; and in Ho Chi Minh City, Vietnam.	18 December 2025
28	CyberDSA in Kuala Lumpur, Malaysia.	30 September - 2 October 2025

FIRST

Forum of Incident Response and Security Teams

1. About the Organization:

FIRST brings together Internet security teams and experts from across the world, to share knowledge and insights, ensuring a safer Internet for all. Founded in 1990, FIRST consists of security practitioners from corporations, government bodies, universities and other institutions, representing 115 economies in the Americas, Asia, Europe, Africa, and Oceania.

FIRST gives the global incident response community a place to build trust and work together. It also provides valuable opportunities to build capability, such as:

- technical colloquia for security experts,
- hands-on classes,
- annual incident response conference,
- publications and web services,
- special interest groups, and
- community and capacity building.

2. Activities and Operations in 2025:

- FIRST membership has grown to 837 member teams in 115 different countries with 204 liaisons and four associate members.
- In the past year FIRST has hosted and supported 15 events including the FIRST Cyber Threat Intelligence Conference, CVE/FIRST VulnCon 2025, and the FIRST Annual Conference 2025 held in Denmark.
- In June 2025, FIRST launched the FIRST CORE sponsorship initiative to expand the impact of the FIRST community and capacity building activities: https://www.first.org/global/core/

3. Collaboration with APCERT members/partners:

FIRST has been an APCERT Strategic Partner since 2021 and the two organizations have a strong shared membership leading to mutual engagement across our events and activities.

- In 2025, the FIRST Suguru Yamaguchi Fellowship Program included participation from APCERT members **CERT-PH** and **CERT VU**.
- In September 2025, the **APNIC**/FIRST Technical Colloquium was held as part of the APNIC60 Conference in Da Nang, Vietnam – https://www.first.org/events/colloquia/apnic25/
- In September 2025, FIRST supported the ITU Regional Cyber Drill for Asia and the Pacific Region hosted by the Mongolia Ministry of Digital Development, Innovation and Communications in Ulaanbaatar, Mongolia.
- During the APCERT Annual General Meeting and Conference in November 2025, held in Sydney, Australia, FIRST Board members delivered a presentation on its role in the worldwide incident response community.

FIRST continues to work with the Asia-Pacific cybersecurity community through events, mentorship, information sharing, training, advisory support, and community engagement. FIRST looks forward to building even stronger collaboration and engagement with APCERT and the wider community in 2026.

FSI-CERT

Financial Security Institute – Computer Emergency Response Team - Korea

1. About FSI-CERT

1.1 Introduction

FSI-CERT (Financial Security Institute – Computer Emergency Response Team) is a non-profit organization established by South Korean financial institutions. As the nation's dedicated financial security agency, we manage a comprehensive cyber incident response framework for the financial sector.

Our work covers threat intelligence sharing, early warnings, and root cause analysis—including digital forensics and malware analysis. We also focus on rapid response and effective damage control to protect the financial ecosystem.

1.2 Establishment

FSI-CERT was founded in April 2015 as South Korea's specialized financial security agency. Our mission is to build a safe and trustworthy financial environment that enhances user convenience and drives the industry forward.

1.3 Organization (Resources)

We currently have a team of over 300 professionals across 4 divisions and 14 departments. FSI-CERT provides specialized security services, including:

- Integrated security monitoring and cyber threat response.
- Research on financial security policies and new technologies.
- Support for digital finance transformation and autonomous security management.

2. Activities and Operations

2.1 Activities Summary

2.1.1 Enhancement of Financial Fraud Prevention

In October 2025, FSI-CERT launched the AI-based Anti-Phishing Sharing & Analysis Platform (ASAP). This platform centralizes fraud intelligence from both financial and non-financial sectors. By using AI for advanced analysis and data enrichment, ASAP allows us to respond quickly to sophisticated voice phishing attacks.

2.1.2 Financial Software Supply Chain Security

We have deployed a Software Supply Chain Security Platform for the financial sector. This platform encourages collaboration among stakeholders and improves vulnerability management for both open-source and commercial software. It also uses SBOM (Software Bill of Materials) to analyze supply chain risks, helping the industry manage these threats more effectively.

2.1.3 Operation of Financial Sector Attack Surface Management System

FSI-CERT operates an ASM system tailored for the financial sector. It proactively monitors network-based attack paths that adversaries might exploit. By identifying vulnerable assets and detecting early signs of anomalies before an attack occurs, we significantly strengthen the defensive capabilities of financial institutions.

2.1.4 Dark Web Threat Intelligence Collection and Response

We continuously monitor dark web marketplaces for stolen financial data, hacking tools, and other illicit content. This monitoring enables us to respond swiftly to cyber threats and security incidents originating from the dark web.

2.1.5 Financial Sector Bug Bounty Program

FSI-CERT runs a year-round Bug Bounty Program to discover new vulnerabilities and strengthen industry-wide defenses. We have expanded the program to include widely-used financial software, IT solutions, and information security products.

2.1.6 Malware Collection, Analysis, and Response

We collect malware samples from various channels to protect the financial sector. Using a dedicated analysis system, we profile advanced threats—including ransomware and APTs—through correlation analysis and threat clustering.
Key findings, such as threat actor identification and behavioral patterns, are shared with financial institutions and relevant agencies. We also actively distribute information on intrusion attempts, financially motivated malware, and distribution infrastructure to our partners.

2.2 Incident Response

2.2.1 Cyber Incident Response for Financial Institutions

In the event of a cyber incident at a financial institution, FSI-CERT conducts digital forensics and detailed incident analysis. We also perform preventive forensic analysis on high-risk endpoints to identify potential threats before they escalate.

Figure 1. Incident Response Process

2.2.2 Malware Response and Intelligence Sharing

We collect and analyze malware targeting financial institutions and share critical threat intelligence. This includes Indicators of Compromise such as C2 server addresses, distribution sites, and malicious file hashes. Our large-scale analysis results are systematically managed to provide deep insights through correlation analysis.

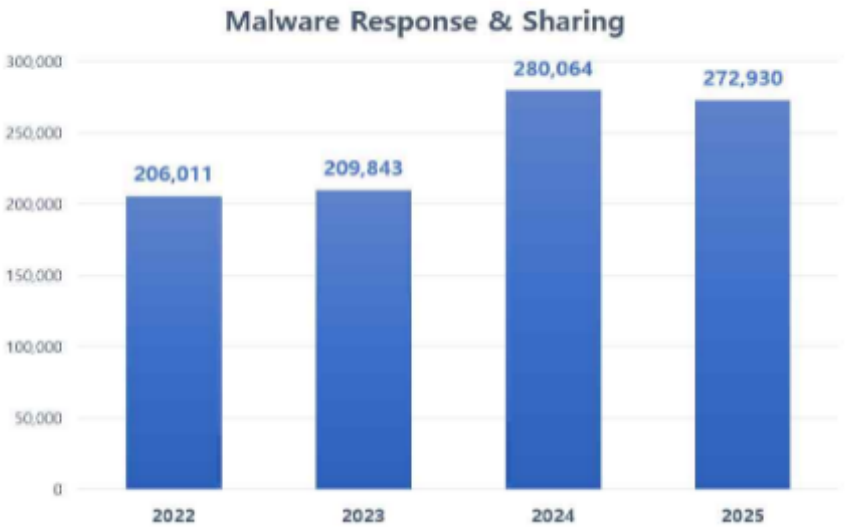


Figure 2. Malware Intelligence Sharing

2.2.3 Cyber Incident Response Exercises

FSI-CERT operates CATS (Cyber Attack Training Simulation), a realistic training platform. It allows financial institutions to run independent drills against various scenarios, including DDoS attacks, server intrusions, and spear-phishing, helping them strengthen their response capabilities and security awareness.

Figure 3. Cyber Incident Response Exercise

2.2.4 DDoS Emergency Response Center Operations

If a DDoS attack exceeds a financial institution's own mitigation capacity, our center steps in. We use on-premises and cloud-based scrubbing centers (both domestic and international) to filter out malicious traffic, ensuring only "clean" traffic reaches the institution.

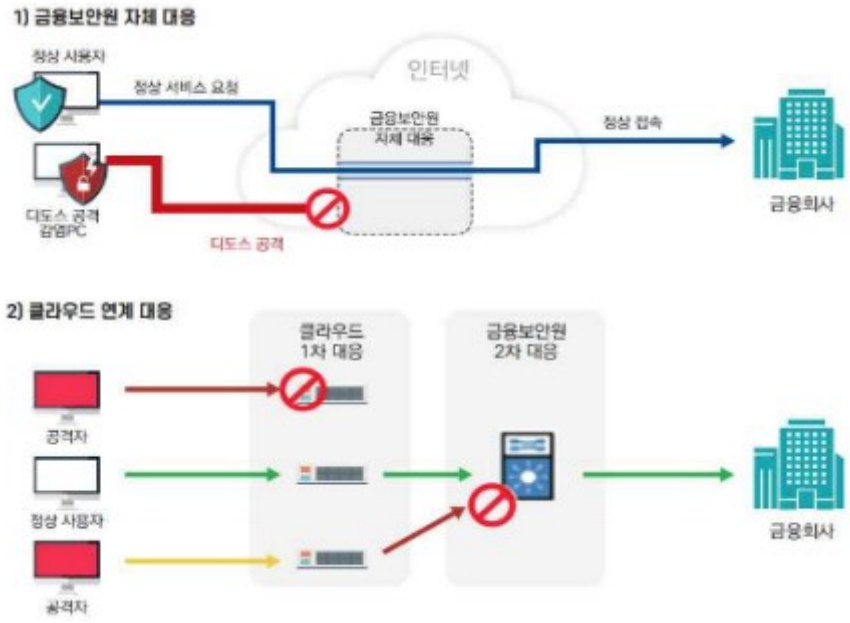


Figure 4. DDoS Attack Response Architecture

2.3 Integrated Security Monitoring for the Financial Sector

FSI-CERT operates a next-generation security monitoring system powered by AI, big data, and cloud technology. In 2026, we are advancing these capabilities by integrating Attack Surface Management (ASM) and developing a specialized threat intelligence platform for the financial sector.

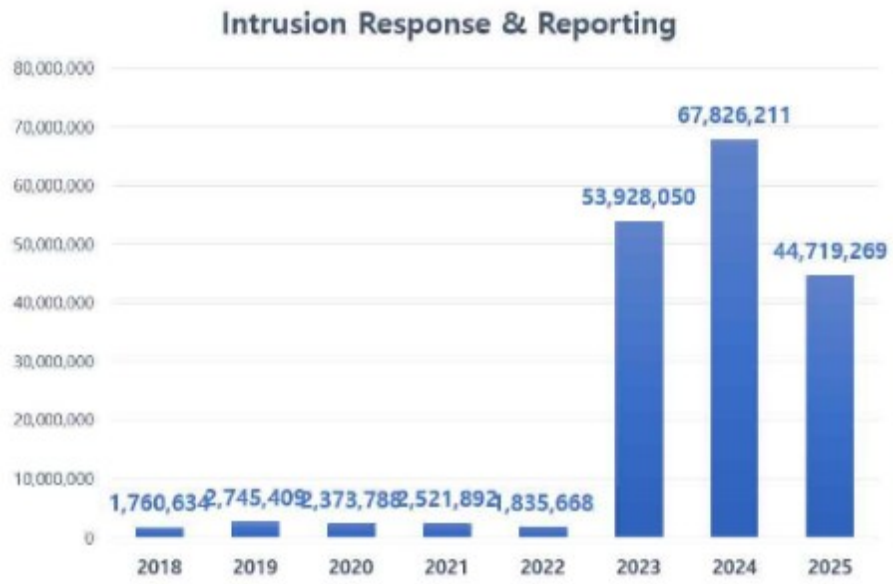


Figure 5. Electronic Incident Response

2.3.1 Voice Phishing Fraud Intelligence Response

Using an advanced detection system, we identify and block phishing and pharming sites. We also manage a sector-wide sharing framework to block malicious apps and infrastructure used in voice phishing. To strengthen this defense, we maintain active MOUs with the National Police Agency, telecom providers, and cybersecurity firms.

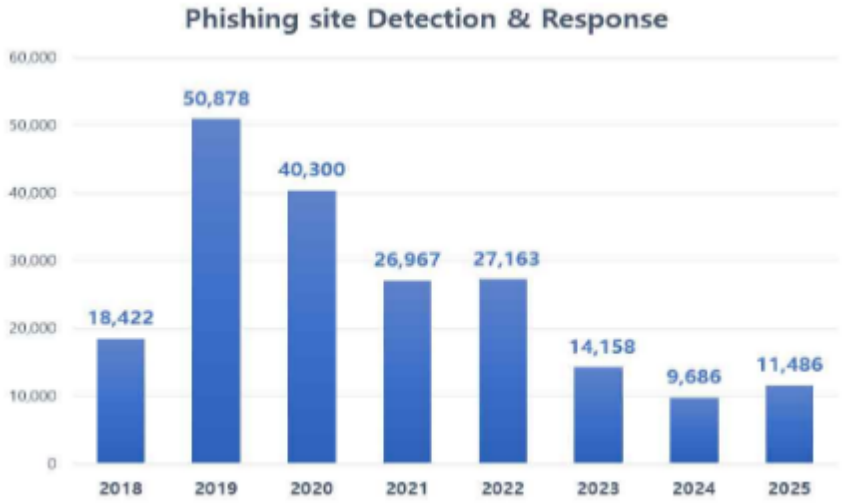


Figure 6. Phishing and Pharming Site Detection

2.4 Vulnerability Assessment and Analysis

We help financial institutions find and fix security gaps through comprehensive assessments of their infrastructure and web services. In 2026, we are expanding our elite white-hat hacker team to provide specialized penetration testing and stay ahead of emerging threats.

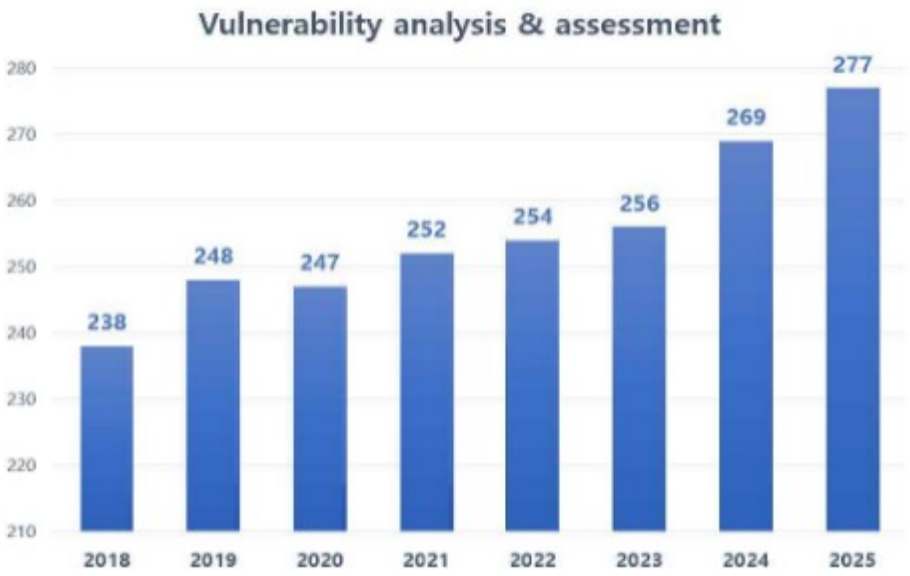
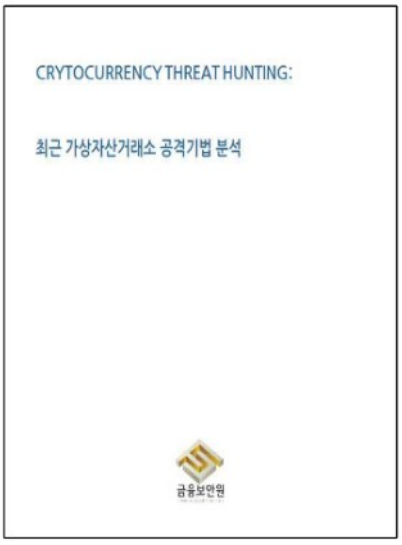


Figure 7. Vulnerability Assessment

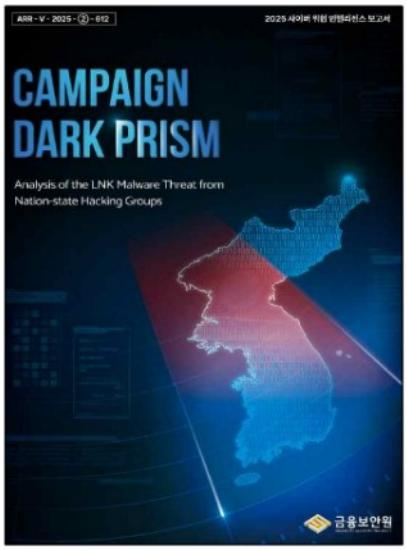
3. Publications

FSI-CERT publishes annual research and Cyber Threat Intelligence (CTI) reports.



CRYPTOCURRENCY THREAT HUNTING: Analysis of Recent Attack Techniques Targeting Cryptocurrency Exchanges (2025.9.)

While past cryptocurrency exchange breaches typically exploited technical vulnerabilities within the exchanges' own systems, recent attacks have evolved into compound campaigns combining technical exploitation with social engineering techniques. This report examines and analyzes recent cryptocurrency exchange breach cases to highlight the primary attack techniques of threat actors persistently targeting cryptocurrency exchanges and their methods of laundering stolen funds.



CAMPAIGN DARK PRISM : Analysis of the LNK Malware Threat from Nation-state Hacking Groups (2025.12.)

Over the past several years, threat actors have shifted away from traditional document-based attack vectors toward techniques exploiting Windows shortcut (LNK) files, conducting sophisticated cyber operations against government agencies, financial institutions, defense-related organizations, and private enterprises. This report presents in-depth technical analysis of approximately 200 LNK malware samples attributed to nation-state threat groups, independently collected by FSI between January 2024 and September 2025, including analysis of evolving adversary TTPs and C2 communication traffic. Just as a prism disperses a single beam of light into its constituent colors, the title "Campaign: Dark Prism" reflects the intent to capture the multi-layered threat landscape emanating from LNK malware — a single, common attack vector wielded by nation-state threat actors.

4. Events Organized / Hosted

- Financial Sector Voice Phishing Response Council
- Financial Information Security Conference (FISCON 2025)
- 2025 Financial Security Academy
- Financial Sector Bug Bounty Program
- Financial Security Threat Analysis Competition (FIESTA 2025)

- Financial Sector Threat Intelligence Working Group Meeting (Quarterly)
- Sector-wide Malware Practitioners' Committee Meeting (Quarterly)
- Financial Sector SW Supply Chain Security Practitioners' Committee Meeting (Quarterly)

5. Collaboration With APCERT Partners

FSI-CERT participated in APCERT Online Training (Topic: ATM Cyber Attack, 2020) and will continue to actively participate in various APCERT seminars to share diverse information and research findings related to financial cybersecurity.

6. Conclusion

As threats from the dark web, cloud vulnerabilities, and cyber warfare grow, FSI-CERT is committed to advancing our security framework. By integrating AI and big data into our operations, we will continue to provide a resilient and secure foundation for the financial industry.

FSI-CERT Contact Information

- Tel : +82-2-3495-9410
- Email : cert@fsec.or.kr
- Website : https://www.fsec.or.kr/en

KZ-CERT

The National Computer Emergency Response Team of the Republic of Kazakhstan

1. About the Organization

1.1 Introduction

KZ-CERT is a single center for the users of national information systems and the Internet segment of Kazakhstan which provides collection and analysis of cyber incident reports as well as consultative and technical assistance to Kazakhstani users in preventing of cyber threats.

1.2 Establishment

KZ-CERT was established in 2011 on the basis of the "Center for Technical Support and Analysis in Telecommunications" republican state enterprise on the right of economic management.
On January 28th, 2013, the government of Kazakhstan adopted a decree to rename the "Center for Technical Support and Analysis in Telecommunications" RSE on REM as the "State Technical Service" RSE on REM. Eventually, in 2020, the "State Technical Service" RSE on REM had undergone its final reformation into the "State Technical Service" joint-stock company (JSC STS) by another governmental decree.
In 2017, the National Coordination Center for Information Security (NCCIS) was established as a structural unit of the JSC STS. It combines the operation of both KZ-CERT and the Government SOC.

1.3 Resources

The National Coordination Center for Information Security (NCCIS), which is a structural subdivision of STS JSC, currently employs more than 80 people of various profiles. KZ-CERT, in turn, as a functioning unit of NCCIS, comprises around 20 employees.

2. Activities & Operations in 2025

2.1 Awareness-raising

One of the key areas of our work is raising awareness on cyber threats and promoting a culture of information security among various segments of the population. In 2025, our organization carried out educational events and cyber drills for employees of government agencies in Kazakhstan, the quasi-government sector, critical information and communication infrastructure (CICO) facilities, and Security Operations Centers. As part of these events, we address key issues of digital security, including:

- Cyber threats, attacks, and countermeasures – an overview of contemporary threats, attack methods, and effective defense strategies;
- Data protection in the digital reality – approaches to ensuring the security of personal and professional information in the context of digital transformation;
- Cyber hygiene basics and common internet fraud schemes – recommendations for safe online behavior and common scams;
- Digital defense: protection from cyberattacks, basics for public servants – practical advice on information security for government employees;
- Cybercrime: how to avoid digital fraud – strategies for protection against online threats and scammers;
- Cyber hygiene guide for schools – safe digital practices adapted for teenagers;
- Safe internet for children – educating children and parents on the basics of internet safety;
- The secrets of the internet: safety in the digital age – how to protect privacy and minimize digital risks;
- Key aspects of information security – understanding threats and the necessary protective measures for every user.

2.2 Internal operations

In 2025, within this initiative, KZ-CERT implemented a series of events aimed at increasing digital literacy, protecting against cyber threats, and strengthening information security in Kazakhstan.
As part of the ongoing activities to cover the cybersecurity issues in our country, the meetings that involve Kazakhstan's government agencies and Security Operations Centers have been held to discuss matters related to enhancing the level of information security in these organizations that play a significant role in domestic policy.

2.3 Incident handling

In 2025, KZ-CERT has handled over 61 thousand cybersecurity incidents. The majority of incidents are associated with the creation and distribution of malware. Figure 1 shows a more detailed information on their types.

Figure 1. 2025 incidents statistics. Source: https://cert.gov.kz/

2.4 Operations: 2025 Cybersecurity incidents and threats

As a National Computer Emergency Response Team of Kazakhstan, KZ-CERT continuously monitor, analyze, and respond to cybersecurity incidents and threats across the country. The following section provides an overview of the significant incidents and emerging threats identified during the reporting period.

2.4.1 Botnet

At the beginning of the current year, numerous events associated with the Phorpiex botnet – one of the most persistent and active cyber threats currently observed (accounting for approximately 90% of the total number of detected botnets) – were identified within the infrastructure of JSC "STS" This malware is commonly used for cryptocurrency wallet theft, spam distribution, sextortion campaigns, and the propagation of ransomware According to international and internal intelligence sources, more than 1000 IP addresses located in Kazakhstan were identified in connection with botnet activity, indicating a significant level of infection within the national network segment.

In several public sector organizations, malicious files (for example, "voldriver.exe") associated with a new variation of the botnet – Twizt – were detected This variant utilizes a peer-to-peer architecture and is capable of operating without centralized command-and-control infrastructure, which significantly increases its resilience and complicates detection and mitigation efforts.

The continued activity of botnets may be attributed to the compromise of new information systems as well as the ongoing evolution of command-and-control mechanisms and management algorithms for infected devices This situation highlights the need to strengthen protective measures, improve the level of cybersecurity awareness among

public sector personnel, and implement additional monitoring and incident response mechanisms.

Countering botnet threats such as Phorpiex and its Twizt modification requires a multilayered approach to protecting information infrastructure It is necessary to ensure monitoring coverage across all network ports and protocols through attack detection and prevention solutions, implement behavioral traffic analysis, and extend signature-based detection capabilities beyond standard rule sets Effective measures include the deployment of SIEM platforms as well as the timely acquisition and integration of Indicators of Compromise (IoC) from trusted intelligence sources Network segmentation should be enforced, routing from compromised nodes should be restricted, and connections to peer-to-peer networks commonly utilized by malware should be blocked.

It is also necessary to review and update existing security policies, maintain up-to-date antivirus protection, and train personnel to identify indicators of anomalous network activity. Regular security audits of internal infrastructure are recommended in order to detect potential involvement in botnet activity.

In addition, particular attention should be given to remote workplaces and workstations generating a high volume of outbound requests that may indicate signs of compromise.

2.4.2 Data breaches

During 2025, data breaches became one of the most significant and widespread information security threats. Multiple large-scale incidents involving the compromise of sensitive information affecting both government institutions and private organizations were identified across various online resources. The total volume of compromised data amounts to tens of millions of records. In several cases, the data became publicly accessible through open sources or was distributed via messaging platforms and specialized forums.

Organization in the transport sector

An incident involving the potential unauthorized transfer of internal documents was identified in an organization operating in the transport sector. Although no direct evidence of large-scale data exfiltration to the Internet was obtained, analysis of user directories, graphical files, and system artifacts (including registry data and USB device connection logs) revealed indications of possible involvement by certain employees. One document was subsequently published on a Telegram channel and further disseminated online, suggesting the possibility of a targeted data leak.

Organization in the emergency medical services sector

A database leak involving approximately 800,000 records associated with an information system used in emergency medical services was identified. An open web resource contained links to official web resources of the system as well as information regarding the database structure, including records of ambulance stations. As proof of access, the threat actors published samples of 10,000 records for each city, indicating that they possessed full access to the dataset.

Organization in the e-commerce and digital services sector

As a result of the compromise of a web resource belonging to an organization operating in the e-commerce and digital services sector, threat actors obtained access to a substantial dataset containing approximately 4.5 million records. The leaked materials included files and databases with various names suggesting links to telecommunications services, educational platforms, and contact data processing services. The majority of the records relate to citizens of neighboring countries, however information concerning citizens of the Republic of Kazakhstan was also identified, creating additional

risks for national stakeholders.

Organization in the healthcare sector

Particular attention should be given to a large-scale data breach presumably originating from a major information system used in the healthcare sector. The dataset is estimated to contain approximately 16 million records. A similar dataset had previously appeared for sale in December 2024, which may indicate a prolonged compromise and the possibility that the same data has been repeatedly resold to different threat actors.

Organization providing financial services

An incident was recorded in which a file containing 228,682 records with personal client data belonging to a financial services organization became publicly accessible. The dataset included partially masked bank card numbers, card expiration dates, payment system identifiers, client names, cities of residence, and phone numbers. The combination of this information significantly increases the likelihood of financial fraud and targeted phishing campaigns against affected clients.

Organization in the mass media sector

A leak involving more than 5.3 million records was identified on the web resource of an organization operating in the media sector. The dataset covers the period from 2016 to 2025 and includes both internal website information and personal user data. The scale of the dataset and the extended period of data accumulation indicate a potentially significant impact associated with the future misuse of this information.

Organization in the construction sector

A leak involving approximately 294,762 records related to an organization operating in the construction sector in the Republic of Kazakhstan was also identified. Analysis indicates that the majority of the records are clearly associated with residents and organizations located within the country, as evidenced by address information and references found in regional sources. The compromise affected both contact information and data enabling the identification of individuals and organizations.

The combination of the incidents described above confirms that data breaches represent one of the most significant and relevant cybersecurity threats in the last year. The scale of compromised datasets, the diversity of affected data categories, and the involvement of both public and private organizations highlight the need to prioritize data protection measures, strengthen vulnerability monitoring processes, improve the security posture of web applications and database infrastructure, and conduct systematic efforts aimed at preventing insider threats and improving employee cybersecurity awareness.

2.4.3 Ransomware

During the first quarter of 2025, several incidents involving data encryption within the IT infrastructure of various organizations were recorded. Analysis indicates the use of modern ransomware families such as Mimic, as well as the abuse of built-in encryption tools including BitLocker.

Data encryption in a financial sector organization

On January 12, 2025, following a compromise of the infrastructure of a financial sector organization, several servers were

encrypted using BitLocker. On January 14, a compromise of the organization's web resource was also detected, resulting in redirection to an external malicious website.

The intrusion into the infrastructure was carried out through Remote Desktop Protocol (RDP) access using an administrator account, which enabled the attackers to encrypt servers and workstations. In addition, the attackers gained access to the administrative panel of a website hosted within the corporate network. The system lacked up-to-date security patches and contained a known vulnerability in the content management system (CMS) being used. Insufficient information security controls, outdated operating systems (Windows Server 2003/2012 and Red Hat Linux 4), the absence of SIEM-based monitoring, and the lack of a structured information security policy significantly exacerbated the impact of the incident.

Data encryption in a local executive body

On April 28, 2025, numerous virtual machines were encrypted within the infrastructure of an organization, including critical services such as Active Directory (AD), DHCP, and DNS. The malware disrupted system operations and a ransom note was received. Backup copies were either unavailable or inaccessible.

The attackers gained initial access through a compromised account belonging to an employee responsible for system maintenance. Using RDP access, they penetrated the domain controller server, cleared event logs, and subsequently initiated data encryption. An additional factor that facilitated the attack was the use of an outdated and vulnerable version of a CMS deployed on one of the organization's web resources.

Data encryption in an organization in the education sector

On February 7, 2025, a ransomware incident occurred within the infrastructure of an organization operating in the education sector, resulting in disruption of the normal operation of information systems. The investigation revealed that key factors contributing to the successful attack included the absence of a formalized and implemented information security policy, the presence of open network ports, the lack of regular audits of user and administrator accounts, and improperly organized backup storage procedures, which complicated system recovery.

It was additionally determined that not all IP addresses involved were connected through the centralized Internet gateway, reducing the level of traffic visibility and increasing the infrastructure's exposure to external threats. The combination of these factors created conditions that allowed the attackers to successfully encrypt data and disrupt the integrity and availability of critical services.

2.5 Activities: Events and Cyber Drills

KZ-CERT recognizes the importance of cooperation with teams and organizations that have similar competency and constituency. Therefore, our Team is always open to invitations and opportunities to participate in various events dedicated to the information security matters.

International cooperation plays a big role in establishing communications with the global IT and cybersecurity communities, circulating important information, as well as maintaining the status of a national computer emergency response team on the global stage through the participation in different international information security conferences

and other events.

2.5.1 Cyber Drills and Trainings

The Standoff at the St. Petersburg International Economic Forum (SPIEF)

In June 2025, the "Standoff" cyber range at the St. Petersburg International Economic Forum (SPIEF) in Russia hosted a cybersecurity event featuring 12 teams from various countries. The goal of the Standoff was to evaluate the cybersecurity resilience of the virtual state's infrastructure in the logistics sector by investigating simulated cyber incidents, detecting malicious activity, and responding to threats. KZ-CERT secured 1st place in the competition;

OIC-CERT Cyber Drill

In September 2025, KZ-CERT participated in the 13th Regional Arab, OIC and Africa Cyber Drill event organized by OIC-CERT as part of the 17th Annual Conference held in Rabat, Morocco. The primary goal of these drills was to enhance the capabilities in defending against cyber threats and to promote cooperation in cybersecurity across member states. KZ-CERT successfully earned 2nd place in the competition;

CyberTask Cyber Drill

As part of the 13th Regional Arab, OIC and Africa Cyber Drill and the 17th Annual Conference organized by OIC-CERT in Rabat, Morocco, KZ-CERT participated in the CyberTask Cyber Drill. The exercise focused on investigating a cyber-attack against an AI-powered automation system, analyzing SIEM logs, network traffic, and forensic evidence to trace attacker activity. KZ-CERT members achieved 1st place, demonstrating the high level of expertise and preparedness;

CyberLab (MyCERT) Cyber Drill

During the same conference, KZ-CERT also took part in the CyberLab Cyber Drill, which focused on threat hunting and monitoring on a SIEM system, providing practical experience in detecting and responding to cyber threats in real-time. KZ-CERT showcased its capabilities and secured 2nd place in the rankings;

Positive Technologies Cyber Drill

KZ-CERT participated in the Positive Technologies Cyber Drill “Compromise of Medical Data” as part of the same OIC-CERT event in Rabat, Morocco. The exercise focused on investigating and responding to simulated attacks targeting medical information systems, providing practical experience in detecting breaches and mitigating threats. KZ-CERT achieved 2nd place in the team ranking and 1st place in the individual ranking.

Equinor CTF

In November 2025, KZ-CERT successfully participated in the Equinor CTF 2025, securing an impressive 3rd place finish. Throughout the competition, our team demonstrated high-level expertise in incident response, digital forensics, and log analysis.

FIRST CTF

In June 2025, KZ-CERT competed in the 37th Annual FIRST Conference CTF, which was held in Copenhagen, Denmark, securing 14th place out of 100 teams. The primary goal of the competition was to challenge participants with a diverse range of realistic attack-and-defense scenarios, requiring the team to demonstrate versatility, rapid problem-solving, and a comprehensive understanding of the modern threat landscape.

2.6 Cooperation

Every year KZ-CERT maintains efforts to conclude agreements with strategically important partners in the field of cybersecurity in order to formalize mutually beneficial cooperation in responding to threats and incidents of information security. Thus, in 2025, KZ-CERT has concluded 1 Memorandum of Understanding in the field of cybersecurity.

Apart from that, KZ-CERT Team members also actively attended various international conferences and meetings to gain valuable experience, stay updated on emerging cyber threats, and learn best practices from global cybersecurity experts. The following events can be mentioned in this regard:

- The 27th Big National Forum "Infoforum-2025" in Moscow, Russia;
- The "The Field of Cybersecurity in OIC Countries: Challenges and Prospects" workshop in Islamabad, Pakistan (as a speaker);
- The OSCE Workshop on Gender Issues in Cybersecurity and ICT, organized by the Transnational Threats Department in Astana, Kazakhstan;
- The "Mobile World Congress" event in Barcelona, Spain;
- The 37th Annual FIRST Conference and 20th Annual NatCSIRT Meeting in Copenhagen, Denmark;
- The "Positive Hack Days" International Cybersecurity Festival in Moscow, Russia;
- The 10th Annual CAMP Meeting in Seoul, South Korea;
- The 3rd Cybersecurity Summit for Central Asia in Tashkent, Uzbekistan;
- The "SOC-Forum" event in Moscow, Russia;
- The 13th Regional Cybersecurity Week General Meeting and the 17th Annual OIC-CERT Conference in Rabat, Morocco.

OIC-CERT

Organisation of The Islamic Cooperation – Computer Emergency Response Teams

1. About CSIRT

1.1 Introduction

The Organisation of the Islamic Cooperation - Computer Emergency Response Team (OIC-CERT) was established through the Organization of the Islamic Cooperation (OIC) Resolution No 3/35-INF Collaboration of Computer Emergency Response Team (CERT) Among the OIC Member Countries. It was passed during the 35th Session of the Council of Foreign Ministers of the OIC in Kampala Uganda on 18-20 June 2008.

In 2009 through the Resolution No 2/36-INF Granting the Organization of the Islamic Cooperation –Computer Emergency Response Team an Affiliated Institution Status, the OIC-CERT became an affiliate institution of the OIC during the 36th Session of the Council of Foreign Ministers of the OIC Meeting in Damascus, Syrian Arab Republic on 23-25 May 2009.

Vision

Envisioning the OIC-CERT to be a leading cybersecurity platform to make the global cyber space safe.

Mission

A platform to develop cybersecurity capabilities to mitigate cyber threats by leveraging on global collaboration.

1.2 Membership

As of Dec 2024, the OIC-CERT has a network and strategic collaboration with 68 members from 30 OIC countries. This comprised of 27 Full Members & 22 General Members as well as in support from 6 Commercial Members, 4 Professional Members, 3 Fellow Member, 1 Affiliate Member, and 1 Honorary Member.

The membership categories are as follows:

1.2.1 Full Members

These are CERTs, Computer Security Incident Response Teams (CSIRTs) or similar entities that are located and/ or having

the primary function within the jurisdiction of the OIC CERT member countries that are wholly or partly owned by the government with the authority to represent the country's interest.

1.2.2 General Members

These are other related government organizations, non-governmental organizations or academia that deal with cybersecurity matters. However, these parties do not have the authority to represent the country's interest.

1.2.3 Affiliate Members

These are not-for-profit organizations that deal with cybersecurity matters from non-OIC-CERT member countries.

1.2.4 Commercial Members

These are industrial or business organizations that deal with cybersecurity matters from the OIC and non-OIC member countries.

1.2.5 Professional Members

Individual professionals, mainly in the cybersecurity domain, are not restricted to the OIC community.

1.2.6 Fellow Members

These are individuals who are considered as co-founders of the OIC-CERT and have actively represented their organization as an OIC-CERT member for a minimum period of 5 years.

1.2.7 Honorary Members

Individuals or organizations who have demonstrated extraordinary contribution, support, and exemplary leadership to the OIC-CERT.

Details of the members can be found at www.oic-cert.org

2. Events & Activities organized / hosted

2.1 Business Plan

The OIC-CERT Business Plan is structured around strategic pillars, each led by specific board member countries to align cybersecurity activities with global trends which are as follows:

i. Pillar 1: Organizational Structure led by the Chair and Secretariat
ii. Pillar 2: Cyber Governance led by Egypt & Brunei
iii. Pillar 3: Cybersecurity Talent Development led by Indonesia, Malaysia, UAE, Uzbekistan & Qatar
iv. Pillar 4: Cybersecurity Innovation, R&D and Technology led by Azerbaijan & Morocco
v. Pillar 5: Cybersecurity Partnership and Collaboration led by Oman

2.2 Training & Awareness

2.2.1 Online Training

To raise awareness of cybersecurity within the OIC-CERT member states, eight (8) sessions of online training were conducted in 2025 by OIC-CERT Board members as follows:

Date	Topic	Host
5 Mar	Online training "Quantum Computing Threats to the Digital World"	CyberSecurity Malaysia
18 Jun	Webinar titled "Securing Tomorrow: Building Trust in Southeast Asia's Digital Future"	CyberSecurity Malaysia
28 Aug	OIC-CERT Webinar titled: Red Team Rising: Building Uzbekistan's Next Generation of Cyber Talent.	UZCERT
24 Sep	Online workshop "Securing Digital Identities: The Role of Identity Brokers in Modern Cybersecurity"	National Cyber and Crypto Agency (BSSN)
8 Oct	Online workshop "Transferring Cybersecurity Awareness & Education Initiatives Across Borders"	NCSA Qatar
30 Oct	Online workshop "OSINT/Dark Web Investigation: Cyber Threat Intelligence: Using OSINT & Dark Web Data for Security Operations"	National Cyber and Crypto Agency (BSSN)
5 Nov	OIC-CERT Webinar titled: "Building Government Cybersecurity Workforce Capacity: UZCERT's Experience and Best Practices"	UZCERT
16 Dec	Online training "Using AI to Support Incident Response in National CSIRTs"	CyberSecurity Malaysia

2.2.2 Awareness posters and presentations

The UAE, as the Awareness Pillar Lead under the OIC-CERT Business Plan, has published a series of cybersecurity awareness posters covering critical topics as follows:

- Cybersecurity Fundamentals
  - Password security, MFA, phishing awareness.
  - Secure browsing, mobile security, device encryption.
  - safe social media practices, privacy settings, personal data protection.
- Industry-Specific Cybersecurity, includes:
  - Financial cybersecurity, online banking fraud
  - Healthcare data protection, ransomware threats.
  - Government & public sector security, compliance awareness.
- Emerging Threats & Cybercrime, includes:
  - Deepfakes, AI-driven cyber threats, misinformation.
  - IoT security, connected devices vulnerabilities.

- Cybersecurity in remote work, cloud security.
- Advanced Security & Future of Cyber Awareness, includes:
  - Ethical hacking insights, bug bounty, penetration testing
  - Youth & child online safety, digital parenting.
  - Cybersecurity careers & leadership interviews.

2.3 Drills & exercises

Cyber Drills

As in previous years, the OIC-CERT organized its international cyber drill for the members and partners, including APCERT members. In 2025, the drill with the theme "using AI in Cyber Defense Plan" on 17 Sep 2025 was jointly hosted by Oman National CERT and ITU-ARCC. The event was held in conjunction with the 13th Regional Cybersecurity Summit & the FIRST & ITU-ARCC Regional Symposium for Africa and Arab Regions held in Rabat, Morocco. The primary objective of the drill was to assess and strengthen the readiness of participating organizations in responding to sophisticated cyber-attacks. By simulating real-world scenarios, the exercise provided a platform to test incident response capabilities, foster collaboration among international partners, and highlight the role of artificial intelligence in enhancing cyber defense strategies

2.4 Conferences and seminars

OIC-CERT 17th Annual Conference, Rabat, Morocco

The OIC-CERT 17th Annual Conference was held in Rabat, Morocco from 15-19 September 2025 in conjunction of 13th Regional Cybersecurity Summit & the FIRST & ITU-ARCC Regional Symposium for Africa and Arab Regions with theme "Digital Sovereignty for Sustainable Economic Development". Regional Cybersecurity Week 2025 provided an exceptional platform for 50+ countries, various international organizations from (Smart Africa, ANCA, OIC-CERT, CREST, HD, WEF) head of national cyber security agencies, and policy experts along with diplomats to address the interconnected challenges of cybersecurity, digital sovereignty, and sustainable economic development.

2.5 Publications

2.5.1 OIC-CERT Journal of Cyber Security

The growth in cybersecurity research has encouraged the collaboration between the public sectors, academia, and industry practitioners. The OIC-CERT has a substantial pool of resources and expertise both from the academia and industry practitioners that can produce quality research papers in the field of cybersecurity and can be published as a journal contributing to the body of knowledge in cybersecurity. In 2025, OIC-CERT published Vol. 6, 2025 consisting of 8 papers.

The OIC-CERT Journal of Cyber Security (JCS) is an initiative under the OIC-CERT led by CyberSecurity Malaysia and the

Technical University of Malaysia Melaka, Malaysia (UTeM). The OIC-CERT welcomed contributions from all parties, especially the APCERT members, for this journal. More details at https://www.oic-cert.org/en/call-for-paper.html

2.5.2 Cyber Security Guidelines/Procedures

The OIC-CERT has published several cybersecurity guidelines in 2025. The guidelines are as follows:

- OT Security Guideline
- Risk Assessment Guideline
- Cloud Security Guideline
- Cybersecurity Governance Implementation Plans and Guidelines
- Departmental Cybersecurity Integration Index
- Cybersecurity Framework for Electric Vehicles and Fast Charging Stations
- Critical Information Infrastructure Identification and Designation

2.6 OIC-CERT Working Group (WG) & Study Group (SG)

OIC-CERT has established several specialized Working Groups (WGs) and Study Groups (SGs) to address emerging cybersecurity challenges, foster collaboration, and develop frameworks that align with global standards as follows:

WG/SG	Lead	Objective
Blockchain	UAE & Brunei	Explore good practices of blockchain security based on national application practices
Supply Chain	Egypt, Oman & Huawei	Adopt a supply chain security standard and best practices to guide the members to return supply chain security issues to the essence of technology and management
AI	Egypt & Oman	To gain insights into and discuss the hot topic of AI security and effectively transfer knowledge

2.7 OIC-CERT Global Cybersecurity Award

The OIC-CERT Global Cybersecurity Award is an initiative by the OIC-CERT to encourage international collaboration in the cybersecurity domain. The "OIC-CERT Award" recognizes innovative cybersecurity projects from around the world, not bound by country or region, which contribute to the uplifting of the ummah wellness while promoting the digital realm.

This initiative is in congruence with the OIC-CERT vision to be a leading international cybersecurity platform in having a safer cyber space. This will be achieved through its mission of developing cybersecurity capabilities to mitigate cyber threats by leveraging global collaboration.

The award recognizes the recipient for their exceptional efforts in supporting the OIC CERT's vision and mission. The 2025 winner was the Cyber Security Council, UAE, for their project entitled "ITU Global CyberDrill 2025."

3. International Collaboration

3.1 International partnerships and agreements

On 15 Sep 2025, OIC-CERT and Crest International (CREST) has signed the Memorandum of Understanding (MoU) to cooperate within the common visions and goals in the field of promoting and supporting cybersecurity innovation and industry development initiatives in Arab & Islamic countries.

On 16 Sep 2025, a joint meeting was also held together with the OIC-CERT Board, FIRST Board, and the African Network of Cybersecurity Authorities (ANCA). The discussions highlighted the objectives of the Regional Cyber Security Week, which include balancing sovereignty, strengthening cyber security resilience, public-private collaboration, inclusive governance, sustainable development integration, aligning cyber security strategies and frameworks, avoiding duplication of efforts, and strengthening regional capacities. The main goal of the meeting was to determine how respected regional and international organizations could contribute to the region's focus areas and priorities, and what the region expected from them.

3.2 Capacity building

Drills & exercises

The OIC-CERT members (Bangladesh, Brunei Darussalam, Malaysia, Jordan, Morocco, Pakistan and Uzbekistan) also successfully participated in the APCERT Drill that was held on 29 July 2025, with theme "When Ransomware Meets Generative AI."

4. Future Plans

- OIC-CERT 18th Annual Conference 2026 (TBC)
- OIC-CERT Cyber Drill 2026
- OIC-CERT Global Cybersecurity Award 2026
- OIC-CERT Journal of Cyber Security for Volume 7.

5. Conclusion

In 2025, the OIC-CERT strengthened its position as a global cybersecurity collaboration hub by expanding membership, delivering impactful training and awareness programs, and organizing international cyber drills and conferences. The year saw the publication of new cybersecurity guidelines and research contributions through the OIC-CERT Journal of Cyber Security, alongside strategic partnerships such as the MoU with CREST International.

Through its awareness programs, digital identity workshops, and regional conferences, OIC CERT helped reinforce digital trust among member states and partners. Its strong emphasis on AI driven cybersecurity, showcased through AI focused training sessions, cyber drills, and dedicated working groups, further advanced the region's preparedness for emerging threats. Additionally, OIC CERT's active engagement with global organizations—such as its MoU with CREST and participation in multinational cyber exercises—demonstrated its commitment to cyber diplomacy, fostering cooperation, shared standards, and strategic alignment across borders. Overall, 2025 positioned OIC CERT as a trusted leader advancing secure, resilient, and collaborative digital ecosystems.

Disclaimer on Publications

The contents of "Activity Reports from Members" and "Activity Reports from APCERT Partners" are written by each APCERT members and partners based on their individual analysis. Responsibility for the information and views expressed in each report lies entirely with the authors.

APCERT ANNUAL REPORT 2025

TLP:CLEAR

APCERT
Asia Pacific Computer Emergency Response Team