

ANNUAL REPORT 2022

APCERT Secretariat

E-mail: apcert-sec@apcert.org URL: <https://www.apcert.org>

Table of Contents

About APCERT	5
APCERT Activity Report	12
Activity Reports from Members	16
ACSC	17
AusCERT	26
BGD e-GOV CIRT	35
BruCERT	45
BtCIRT	53
CERT-In	61
CERT-PH	74
CERT NZ	87
CERT Tonga	95
CERT VU	100
CNCERT/CC	105
CyberSecurity Malaysia	112
GovCERT.HK	122
HKCERT	132
Id-SIRTII/CC	146
JPCERT/CC	156
KN-CERT	165
KrCERT/CC	169
LaoCERT	178
mmCERT	186
MNCERT/CC	196
SingCERT	202
Sri Lanka CERT CC	218
TechCERT	230
ThaiCERT	241
TWCERT/CC	244
TWNCERT	252
VNCERT/CC	264
Activity Reports from APCERT Partners	271
AfricaCERT	272
FSI-CERT	275
KZ-CERT	283
APNIC	289
OIC-CERT	290

From the Chair

The Asia Pacific Computer Emergency Response Team (APCERT) has been in existence for 19 years since the APCERT agreement was accepted in 2003 in Chinese Taipei and the inaugural Steering Committee (SC) was formed. Since then, there is no turning back. From the founding members of 15 CSIRTs from 12 economies, the APCERT membership has grown to 33 Operational Members from 24 economies, 4 Liaison Partners, 4 Strategic partners, and 4 corporate partners. The APCERT have gone through a lot since its inception, but the past three years were challenging because of the Covid-19 pandemic. However, we soldier on, come what may, in any way possible to achieve our vision of help create a safe, clean, and reliable cyber space for the Asia Pacific Region base on global collaboration.

This can be seen when we still strive to deliver our international activities and engagement despite the challenges. We adapted and continued to have our pinnacle event, the Annual General Meeting (AGM) and Conference albeit online for three consecutive years. The 2022 AGM and Annual Conference was held in conjunction with the 2022 FIRST Virtual Symposium: Asia Pacific Region giving the event more visibility and impact. We continued to have our Annual Cybersecurity Drill tradition – the 17th APCERT cybersecurity drill where 25 CSIRTs from 22 economies participated including external members from the economies of the OIC-CERT and Africa CERT. We also conducted a session with the Pacific Cyber Security Operational Network or PacSON by delivering an online lecture as part of their webinar series. We hope that this session will develop further cooperation with the Pacific Island nations of Micronesia, Melanesia, and Polynesia. Apart from these, APCERT also participated in the Asia-Pacific Economic Cooperation Telecommunications and Information Working Group (APEC TEL WG) meeting, the Asia Pacific Internet Organisation (APStar) retreat, and the ASEAN CERT Incident Drill.

Looking ahead, APCERT need to be ready against the oncoming challenges for 2023 and beyond. One such challenge is data leakage when information is exposed due to internal errors and data breach when an external source breaches the system in a cyberattack. It is important to note that data leakage could lead to serious concerns and repercussions such as identity theft, data breaches, and ransomware installation. Ransomware which began as malware can extorts payments through data encryption; denying legitimate users access to their data. These challenges can be escalated to the related working groups under APCERT for serious consideration and possible mitigation.

This would be our last term as the Chair of APCERT after four years thus we would like to take this opportunity to extend our deepest appreciation the APCERT SC members for their tireless efforts to strengthen cross border collaboration. To the working groups and members, we would like to thank you for enhancing awareness and competency in computer security incidents management in the Asia Pacific region.

Mohd Shamir bin Hashim
Chair, APCERT Steering Committee
CyberSecurity Malaysia

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 cybersecurity experts in the Asia Pacific region to improve the region's awareness on 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 cybersecurity capabilities and capacities in the region, including through education and training, to raise awareness and encourage best practices in cybersecurity. APCERT coordinates activities with other regional and global organisations, such as the:

- Asia Pacific Network Information Centre (APNIC: www.apnic.net);
- Forum of Incident Response and Security Teams (FIRST: www.first.org);
- Organisation of the Islamic Cooperation – Computer Emergency Response Team (OIC-CERT: www.oic-cert.net);
- Africa Computer Emergency Response Team (AfricaCERT: <https://www.africacert.org/>)
- Pacific Cyber Security Operational Network (PaCSON: <https://pacson.org/>)
- STOP. THINK. CONNECT program (www.stopthinkconnect.org/).

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/apnics-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 2022, APCERT consists of 33 Operational Members from 24 economies across the Asia Pacific region, 4 Liaison Partners, 4 Strategic Partners, and 4 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 NZ	Computer Emergency Response Team New Zealand	New Zealand
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	CyberSecurity Malaysia	Malaysia

Malaysia		
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	Republic of Korea
LaoCERT	Lao Computer Emergency Response Team	Lao People's Democratic Republic
mmCERT/CC	Myanmar Computer Emergency Response Team	Myanmar
MNCERT/CC	Mongolia Cyber Emergency Response Team / Coordination Center	Mongolia
MOCERT	Macau Computer Emergency Response Team Coordination Centre	Macau, China
MonCIRT	Mongolian Cyber Incident Response Team	Mongolia
SingCERT	Singapore Computer Emergency Response Team	Singapore
Sri Lanka CERT CC	Sri Lanka Computer Emergency Readiness Team Coordination Centre	Sri Lanka
TechCERT	TechCERT	Sri Lanka
ThaiCERT	Thailand Computer Emergency Response Team	Thailand
TWCERT/CC	Taiwan Computer Emergency Response Team / Coordination Center	Chinese Taipei
TWNCERT	Taiwan National Computer Emergency Response Team	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 2022, CyberSecurity Malaysia was elected as the Chair of the APCERT, and CNCERT/CC as the Deputy Chair. The terms of each Steering Committee (SC) member are as follows:

Team	Term	Other positions
ACSC	2022 - 2024	
CNCERT/CC	2022 - 2024	Deputy Chair
CyberSecurity Malaysia	2021 - 2023	Chair
JPCERT/CC	2021 - 2023	Secretariat
KrCERT/CC	2022 - 2024	
Sri Lanka CERT CC	2021 - 2023	
TWNCERT	2022 - 2024	

Working Groups (WG)

There are eight (8) Working Groups (**WGs**) in APCERT.

TSUBAME WG (formed in 2009)

Objectives

- Establish a common platform for Internet threat monitoring, information sharing and analyses for the Asia Pacific region and others
- Promote collaboration among the member CSIRTs using the platform
- Enhance the capability of global threat analyses by incorporating 3D Visualization features into the platform

Convener (1): JPCERT/CC

- Members (21): AusCERT, BruCERT, CERT-In, CERT-PH, CNCERT/CC, CyberSecurity Malaysia, GovCERT.HK, HKCERT, ID-SIRTII/CC, KrCERT/CC, LaoCERT, maCERT, mmCERT, MOCERT, NCA-CERT, Sri Lanka CERT|CC, TechCERT, ThaiCERT, TWCERT/CC, TWNCERT, VNCERT/CC

*TSUBAME WG was concluded at the end of March 2023.

Information Sharing WG (formed in 2011)

Objectives

- Improve information and data sharing within the APCERT, including improving members' understanding of the value of data sharing and motivating the APCERT members to exchange information and data
- Organize the members to establish and enhance the necessary mechanisms, protocols, and infrastructures to provide a better environment to share information and data
- Help members to better understand the threat environment and share data to improve each team's capability as well as the cybersecurity of their constituent networks
- Work as the Point of Contact (PoC) for the APCERT towards other organizations on information sharing

Convener (1): CNCERT/CC

Members (18): AusCERT, bdCERT, Bkav Corporation, CERT-In, CNCERT/CC, CyberSecurity Malaysia, GovCERT.HK, HKCERT, ID-CERT, ID-SIRTII/CC, JPCERT/CC, KrCERT/CC, Microsoft, SingCERT, Sri Lanka CERT|CC, TechCERT, ThaiCERT, TWNCERT, 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

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 and maintain policies, procedures and governance structures that together makes up the APCERT Operational Framework. The WG will periodically review and advise the Steering Committee if changes are required ensuring APCERT remains fit-for-purpose to realise its mission whilst continuing a culture of strong governance underpinned by clear policies

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 and face to face technical workshops to enhance fellow members' cyber security capabilities and capacities in mitigating cyber incidents more efficiently and effectively

Convener (1): TWNCERT

Members (11): CERT-In, CERT NZ, CNCERT/CC, HKCERT, ID-SIRTII/CC, JPCERT/CC, KrCERT/CC, MonCIRT, Sri Lanka CERT|CC, ThaiCERT, TWCERT/CC

Malware Mitigation WG (formed in 2016)

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

Convener (1): CyberSecurity Malaysia

Members (14): bdCERT, BGD e-GOV CIRT, Bkav Corporation, BruCERT, CERT-In, GovCERT.HK, HKCERT, ID-CERT, JPCERT/CC, KrCERT/CC, SecureWorks, SingCERT, Sri Lanka CERT|CC, TWCERT/CC

Drill WG (formed in 2017)

Objectives

- Serve as a permanent 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): Sri Lanka CERT|CC (until August 2022)

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

IoT Security WG (formed in 2017)

Objectives

- Identification of the threat landscape and security challenges in the IoT ecosystem
- Suggesting steps to address the security issues including vulnerabilities tailored for IoT
- Recommendations for securing the IoT ecosystem
- Developing incident response mechanisms/measures for responding to cyber physical security incidents
- Discussions on existing Security Standards and gaps for IoT ecosystem and considerations for adoption
- Development of mechanisms for sharing technical information related to IoT attacks and threats.

Convener (1): CERT-In

Members (7): BGD e-GOV CIRT, CERT NZ, HKCERT, IDSIRTII/CC, JPCERT/CC, Panasonic PSIRT, VNCERT/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

The APCERT has been dedicated to representing and promoting its activities in various international conferences and events. From January to December 2022, APCERT Teams have hosted, participated and/or contributed to the following events:

PacSON Session (10 May – Online)

On behalf of the APCERT, JPCERT/CC conducted an online lecture titled "CVD & CVE Introduction" as part of PaCSON's webinar series.

APEC TEL meeting (10, 13, 14 May – Online)

APCERT attended the TEL 64 SPSG meeting and the TEL 64 Plenary meeting to observe the progress of projects run by the working group and receive updates from the participating countries.

34th Annual FIRST Conference (26 June - 1 July – Dublin, Ireland)

<https://www.first.org/conference/2022/>

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

National CSIRT Meeting (1-2 July – Dublin, Ireland)

APCERT teams attended the 17th Annual Technical Meeting for CSIRTs with National Responsibility (NatCSIRT 2022) and exchanged various activity updates as well as recent projects and research.

APCERT Cyber Drill 2022 (25 August 2022)

<https://www.apcert.org/documents/pdf/APCERTDrill2022PressRelease.pdf>

The APCERT Cyber Drill 2022, the 17th APCERT cyber exercise drill, was successfully conducted to test the response capabilities of the participating APCERT Teams. 25 CSIRTs from 22 economies of APCERT (Australia, Bangladesh, Brunei Darussalam, People's Republic of China, Chinese Taipei, Hong Kong, India, Indonesia, Japan, Korea, Lao People's Democratic Republic, Malaysia, Myanmar, New Zealand, Philippines, Singapore, Sri Lanka, Thailand, Tonga, Vanuatu, and Vietnam) participated in the drill. From the external parties, 4 CSIRTs from 2 economies of OIC-CERT and AfricaCERT participated.

AP* Retreat (12 September – Online)

APCERT attended the meeting for key updates on upcoming events and Internet related organizations in the AP region.

APCERT Annual General Meeting (AGM) and Conference 2022 (18-21 October – Online)

The APCERT Annual General Meeting (AGM) and Conference were held online, followed by the 2022 FIRST Virtual Symposium: Asia Pacific Regions. The program overview is as follows:

- 18 October APCERT Annual General Meeting
- 19 October APCERT Closed Conference
- 20 October 2022 FIRST Virtual Symposium: Asia Pacific Regions (Plenary Sessions)
- 21 October 2022 FIRST Virtual Symposium: Asia Pacific Regions (Trainings)

ASEAN CERT Incident Drill (ACID) 2022 (27 October – Online)

ACID 2022, led and coordinated by SingCERT, entered its 16th iteration with participation including ASEAN CERTs and APCERT Teams. The drill was completed successfully, providing an opportunity for teams to improve their knowledge and skills on investigating and responding to a ransomware incident, which also involves a DDoS attack.

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 an 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 2022, the SC members held 5 teleconferences to discuss the APCERT operations and activities.

Date	Location
9 February	Teleconference
20 April	Teleconference
22 June	Teleconference
16 August	Teleconference
12 October	Teleconference

APCERT Training

The APCERT held five (5) training calls in 2022 to exchange technical expertise, information, and ideas.

Date	Title	Presenter
8 February	Latest Trends on Keyword Hacks & SEO Spam	Sri Lanka CERT CC
12 April	Cyber Security Incident Reporting and Handling Scheme for Taiwanese Government Agencies	TWNCERT
21 June	FIRST's EPSS Scores for Vulnerabilities	AusCERT
9 August	Cyber Threat Intelligence on a national level	ThaiCERT
6 December	Honeynet Data Analysis Through LebahNET	CyberSecurity Malaysia

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



Australian Cyber Security Centre

1. Highlights of 2022

1.1 Summary of major activities

Throughout 2022, the Australian Cyber Security Centre (ACSC) continued to improve Australia's cyber security resilience and provide cyber security advice to government, critical infrastructure, small and medium-sized enterprises and individuals.

In 2022, the deterioration of the global threat environment was reflected in cyberspace. This was most prominent in Russia's invasion of Ukraine. Destructive malware resulted in significant damage in Ukraine itself, but also caused collateral damage to European networks and increased the risk to networks worldwide.

The deterioration in the global threat environment was reflected domestically in Australia with high-profile cyber incidents at Optus and Medibank.

1.2 Achievements & milestones

In financial year 2021-2022 (1 July 2021 – 30 June 2022), the ACSC responded to over 1,100 cyber security incidents; took down over 29,000 brute force attacks against Australian servers; blocked over 24 million malicious domain requests and responded to 135 ransomware incidents.

This financial year saw the ACSC focus on delivering a range of initiatives that streamline—and where possible, automate—active cyber defence and intelligence sharing. The Australian government's 10-year investment known as REDSPICE (Resilience, Effects, Defence, Space, Intelligence, Cyber, Enablers) will further strengthen Australia's cyber defences and address future cyber threats.

CTIS

The ACSC's Cyber Threat Intelligence Sharing (CTIS) was released broadly to ACSC network partners in June 2022.

The CTIS service enables the sharing of threat intelligence at machine speed. Through the use of automation, participating entities receive cyber threat intelligence in a structured and timely manner.

The CTIS Data Model enables partners to share cyber threat intelligence through a common language and outlines standards to share data in alignment to the 5 Cs: Content, Context, Clarity, Communication and Confidence.

CTIS has facilitated the sharing of indicators of compromise amongst participating entities. This has enabled organisations to better protect themselves, strengthening the security of Australian organisations.

Key achievements of CTIS include:

- 25,341 indicators have been provided by the ACSC, including from victims who are not ACSC Partners.
- 741 have been provided by CTIS analysts working for ACSC's delivery partner, Deloitte.
- 2,261 have been shared with CTIS by ACSC Partners.

Australian Protective Domain Name System

The Australian Protective Domain Name System (AUPDNS) is dedicated to protecting government networks. The system uses verified threat intelligence to build a 'block list' of known malicious web domains.

Providing protection against malware, spyware phishing attacks, viruses, and malicious sites, AUPDNS monitors connections between an organisation's network and the internet. AUPDNS also stops malware already on devices from 'calling home', mitigating the damage from an attack. The information captured within AUPDNS also helps build the ACSC's cyber threat picture.

In the 2021–22 financial year, AUPDNS processed more than 36 billion queries, and blocked over 24 million domain requests. AUPDNS onboarded 171 organisations, including a number of state and local government agencies.

Domain Takedown Service

In response to the increasing threat posed by domains hosting malicious software, the ACSC launched the Domain Takedown Service pilot in 2021.

Upon detecting suspected malicious software, the service verifies maliciousness before issuing a takedown notification request to the relevant Domain Host. The service also operates 10 'honeypot' servers on Australian IP ranges, giving the ACSC the ability to directly report malicious domains for manual verification and takedown. The service only targets those attack types which fall under ASD's cyber security function as per the Intelligence Services Act 2001.

In 2021–22, the service focused on 4 lines of effort:

Line of effort	Number of notifications issues	Number of takedowns	Targeting success rate
Government (Australian, state & territory, local)	1,352	1,333	99%
Australian vaccine rollout	16,291	15,932	98%
Flubot text message malware	19,117	19,117	100%
Brute force attacks against Australian servers	29,446	29,278	99%

CI-UP

The ACSC's Critical Infrastructure Uplift Program (CI-UP) pilot concluded in June 2022 and transitioned to a business-as-usual offering.

In 2021-2022, the ACSC piloted CI-UP, a voluntary service provided by the ACSC to help protect Australia's essential services from cyber threats by raising the cyber security levels of critical infrastructure organisations.

Through close collaboration between the ACSC and partners, CI-UP evaluates the cyber security maturity of critical infrastructure and systems of national significance. A combination of Cyber Security Capability and Maturity Model (C2M2) and Essential Eight maturity models are used to deliver prioritised vulnerability and risk management strategies. Following the conclusion of the pilot in June 2022, the ACSC now provides 2 models for CI-UP service:

- CI-UP: A modular suite of cyber security maturity activities undertaken through close collaboration with the ACSC to deliver holistic cyber security maturity uplift for CI-UP partners.
- CI-UP (Self-Assessment): A self-assessment C2M2 evaluation tool enabling ACSC partners to access online resources through the ACSC Partner Portal.

2. About CSIRT

2.1 Introduction

The ACSC, within the Australian Signals Directorate (ASD), leads the Australian Government's operational cyber security activities. The ACSC brings together capabilities to improve the cyber resilience of the Australian community and help make Australia the most secure place to connect online.

2.2 Establishment

In 2017, the Australian Government conducted an Independent Intelligence Review, which identified the need to provide enhanced cyber security capabilities, as well as a single point of advice and support on cyber security.

As a result of this, on 1 July 2018, the ACSC formally became a part of ASD and incorporating CERT Australia and elements of the Digital Transformation Agency.

2.3 Resources

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

2.4 Constituency

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

3. Activities & Operations

3.1 Scope and definitions

The ACSC provides advice and assistance across the Australian economy, including to: critical infrastructure and systems of national interest; federal, state and local governments; small, medium and large business; academia; the not for profit sector, and the Australian community.

More specifically, the ACSC:

- Responds to cyber security threats and incidents across the whole-of-economy;
- Collaborates with the private and public sectors to share information on threats and increase resilience;
- Works with governments, industry and the wider community to increase awareness of cyber security; and
- Provides information, advice and assistance to all Australians.

Additionally, the ACSC manages services for the Australian Government. These include the ReportCyber website and the Australian Cyber Security Hotline.

- **The ReportCyber website** is the single portal for Australians to report cyber security incidents and provides additional assistance and referral pathways. During the 2021–22 reporting period, over 76,000 reports were made via ReportCyber, an increase of 13 percent from the previous financial year. All relevant reporting is referred to the appropriate state or territory law enforcement agency for assessment and potential investigation.
- **The Australian Cyber Security Hotline '1300 CYBER1'** (1300 292 371). The hotline, which is contactable 24/7, provides advice to Australian organisations impacted by cyber security incidents. Since the beginning of the 2021–22 reporting period, ACSC has seen an increase in the number of calls to 1300 CYBER1. The number of calls in the 2021–22 reporting period totaled more than 25,000, an average of 69 calls per day. This is an increase of 15 percent from the last financial year.

3.2 Incident handling reports

ACSC's incident response capabilities span the full spectrum of cyber security incidents, ranging from national crises to incidents affecting individual members of the public. In order to manage the broad range of cyber incidents, the ACSC uses a Cyber Incident Categorisation Matrix (see Figure 1) to triage the immediate defensive response to mitigate a

cyber-incident. This allows the ACSC to focus its resources more effectively, ensuring consistent messaging and the appropriate response measures are activated.

Sustained disruption of essential systems and associated services	C6	C5	C4	C3	C1	C1
Extensive compromise	C6	1	14	28	2	C1
Isolated compromise	4	28	72	75	26	C2
Coordinated low-level malicious attack	C6	C6	15	40	33	C3
Low-level malicious attack	4	116	146	137	64	C3
Unsuccessful low-level malicious attack	1	29	35	62	152	35
	Member(s) of the public	Small organisations Sole traders	Medium-sized organisations Schools Local Government	State Government Academia/R&D Large organisations Supply chain	Federal Government Government shared services Regulated critical infrastructure	National security Systems of national significance

Figure 1

3.3 Abuse statistics

During the 2021–22 financial year, the ACSC responded to over 1,100 cyber security incidents, an average of 21 cyber security incidents per week. Compared to the 2020–21 financial year, this is a decrease of 36 per cent. This does not mean that the cyber security threat to Australian organisations has decreased, especially as the number of cybercrime reports has increased. The expansion of Australia's commercial incident response sector means incidents which may have previously required an ACSC response may now be being handled by in-house or contracted incident response teams.

3.4 Publications

Throughout 2021-2022 the ACSC published:

- 41 alerts and 14 advisories on cyber.gov.au, which collectively saw more than 393,000 visits;

- In response to Russia's invasion of Ukraine, the ACSC issued an Advisory urging Australian organisations to adopt an enhanced security posture. This was updated 10 times and received more than 57,000 views, plus a potential reach of almost 1 million people through social media.
- 13 new Step-by-Step Guides to help Australian individuals, businesses and organisations implement simple cyber security practices.

Other notable publications included:

- The 2021-2022 Annual Cyber Threat Report. The Report provides an overview of key cyber threats impacting Australia, how the ACSC is responding to the threat environment, and crucial advice for Australian individuals and organisations to protect themselves online.
- A major update in July 2021 to the Essential Eight Maturity Model. First published in June 2017 and updated regularly, this supports the implementation of the Essential Eight. It is based on the ACSC's experience in producing cyber threat intelligence, responding to cyber security incidents, conducting penetration testing and assisting organisations to implement this model. In recognition of the degrading cyber threat environment, in March 2022 the Attorney-General's Department mandated the Essential Eight for all non-corporate Commonwealth entities through amendments to the Protective Security Policy Framework.
- In response to the Log4j vulnerability, the ACSC published Log4j: What Boards and Directors Need to Know in January to assist Australian company boards in understanding the significance of the Log4j vulnerability and how their organisations can prepare.

3.5 New services

The ACSC has continued to provide high-quality cyber security services and advice to industry partners in an effort to make Australia the safest place to connect online. These include CTIS, AUPDNS, Domain Takedown Service and CI-UP.

4. Events organized / hosted

4.1 Training

ASD leads or supports over 12 skills based training programs to achieve recruitment requirements and to contribute to the national skills pool. ASD has supported a range of initiatives:

- Girls Programming Network - an extra-curricular program run by girls for girls and is aimed at Year 4-12 students of all programming abilities. This is delivered in partnership with the National Computer Science School and with the support of volunteers.
- Sponsor the Australian Women in Security Network (AWSN) to deliver a range of leadership and training initiatives from cadet to CISO programs to engage and retain women and girls in security careers.

- Sponsored-partnership with Australian cyber-startup OKRDY and AWSN, to launch the Women in Security Mentoring Program - an AI, values-based mentoring matching platform.
- Infosect to deliver highly technical scholarships for women in 2022 to undertake code review, reverse engineering and network security training.

4.2 Drills & exercises

The ACSC led 24 cyber security exercises, involving over 280 Australian organisations, to strengthen Australia's cyber resilience.

In April 2022, ACSC coordinated Exercise Blue Dawn, a simulated ransomware cyber security incident for its Network partners within the ACSC Partnership Program. This exercise was a cross-sector activity that identified participants' strengths and weaknesses, and provided examples on how to improve their holistic organisational responses.

As a result of the exercise, participants overwhelmingly indicated that they would review and further develop their organisation's incident response and preparedness plans. Of the participants, 98 per cent agreed that Exercise Blue Dawn enhanced their ability to perform their roles under similar circumstances, and that their participation was appropriate and beneficial to their roles.

4.3 Conferences and seminars

The ACSC's Joint Cyber Security Centres hosted 367 events with partners over financial year 2021-22.

5. International Collaboration

5.1 International partnerships and agreements

ACSC maintains strong international relationships with global cyber security counterparts in order to share information, mitigate incidents and enhance Australia's cyber security resilience. Cooperation with partners provides opportunities for leveraging capability, expertise and threat visibility.

5.2 Capacity building

Throughout the 2020-21 reporting period, ACSC contributed to expanding international partnerships by:

Leading regional capacity building through the Pacific Cyber Security Operational Network (PaCSON). The ACSC is the permanent PaCSON Secretariat and leads the Communications and Partners working groups. PaCSON member countries include Australia, the Cook Islands, Fiji, Kiribati, the Marshall Islands, Nauru, New Zealand, Niue, Palau, Papua New Guinea,

Samoa, the Solomon Islands, Tokelau, Tonga, Tuvalu and Vanuatu. The United States Cybersecurity and Infrastructure Security Agency and the Reserve Bank of Fiji are partners. During this reporting period, the ACSC managed PaCSON community teleconferences and PaCSON Executive Committee meetings every month to facilitate regular cyber threat information sharing. PaCSON also facilitates information-sharing through the Traffic Light Protocol, and the ACSC shared several ransomware profiles during this reporting period. The ACSC has received positive feedback from the PaCSON community on proposed future capacity building initiatives and training resources.

5.2.1 Training

The ACSC supported DFAT to deliver five 'Cyber Bootcamps' to the Association of Southeast Asian Nations (ASEAN). This collaboration boosted regional cyber resilience by sharing insights on Australia's cyber Threat landscape and response arrangements.

5.2.2 Drills & exercises

In 2022, the ACSC participated in the annual APCERT drill. The drill provided an opportunity to collaborate with APCERT members to ensure we are well prepared to respond to a potential cyber security incident.

5.2.3 Seminars & presentations

The ACSC presented to a number of international partners as part of whole-of-government international engagement activities.

5.3 Other international activities

In 2022, the ACSC also:

- regularly engaged with national cyber security centres in the US, UK, Canada and New Zealand to collaborate on operational cyber security, cyber threats and to work to improve individual and collective cyber resilience.
- engaged with the International Watch and Warning Network, a global partnership of operational cyber security agencies that aims to increase joint global cyber preparedness through information sharing and cooperation.
- supported DFAT to deliver five 'Cyber Bootcamps' to the Association of Southeast Asian Nations (ASEAN) countries, in collaboration with the ANU. In conjunction with each Cyber Bootcamp, the ACSC boosted regional cyber resilience by sharing insights into Australia's cyber security ecosystem and the ASEAN regional threat environment.
- participated in the Australian delegation at Singapore International Cyber Week.
- participated in the International Counter Ransomware Initiative with 30 other nations.

6. Future Plans

6.1 Future projects

The Australian Government's \$9.9 billion REDSPICE investment over the next decade will be used to enhance the ACSC's capabilities to further protect Australians from cyber adversaries.

7. Conclusion

In 2022, the deterioration of the global threat environment was reflected in cyberspace. We saw cyberspace become a battleground with Australia's prosperity particularly attractive to cybercriminals. Ransomware remains the most destructive cybercrime accounting with the number of incidents reported increasing by over 75 per cent.

The work and response from the ACSC is more important than ever. In the face of rising threats to the digital-dependent Australian economy, cyber defence must be a priority for all Australians. The most effective means of defending against cyber threats continues to be the implementation of the Essential Eight cyber security strategies. To support this, the ACSC launched several new initiatives in 2021–22 to improve Australia's cyber resilience, such as a CTIS platform which automates sharing of indicators of compromise. The Australian Government's ten-year investment in ASD, known as REDSPICE, will further harden Australia's cyber defences in 2022–23 and beyond.

AusCERT

Australian Computer Emergency Response Team

1. Highlights of 2022

1.1 Introduction

AUSCERT highlights are always in the being part of the Cyber security community and contributing the local, regional and global arena. This has been done at different levels by being an active member of the community. Participation in regional cyber incident drills is always a highlight of any year. In the year 2022 there are a few contributions and changes that AUSCERT are proud of these being listed in the section below.

1.1 Achievements & milestones

1.1.1 Streamlining in External Security Bulletin reporting

The creation of AUSCERT Impact and Vector assessments of PSIRTs security advisory was done in an era when assessment frameworks were little known in the industry. In 2022 the format of analysis has now aligned with CVSS3.1 to allow for timely reporting. This has also allowed AUSCERT to also follow the ever-increasing volume of PSIRT security advisories.

1.1.2 Contribution to APCERT

Every year AUSCERT contributes back to the APCERT community in being part of several working groups. In 2022 was marked with an increase in the work performed in several Working Groups that AUSCERT is part of. Especially rewarding was the tasks in the APCERT Drill WG, and APCERT Membership WG.

1.1.3 Tertiary Education Capstone Projects

2022 has marked the first time AUSCERT has engaged final year Cyber Security Masters student in their capstone projects. The results of the capstone projects are being assimilated in provided service that are increasing AUSCERT's capacity and capability in early warning notifications.

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

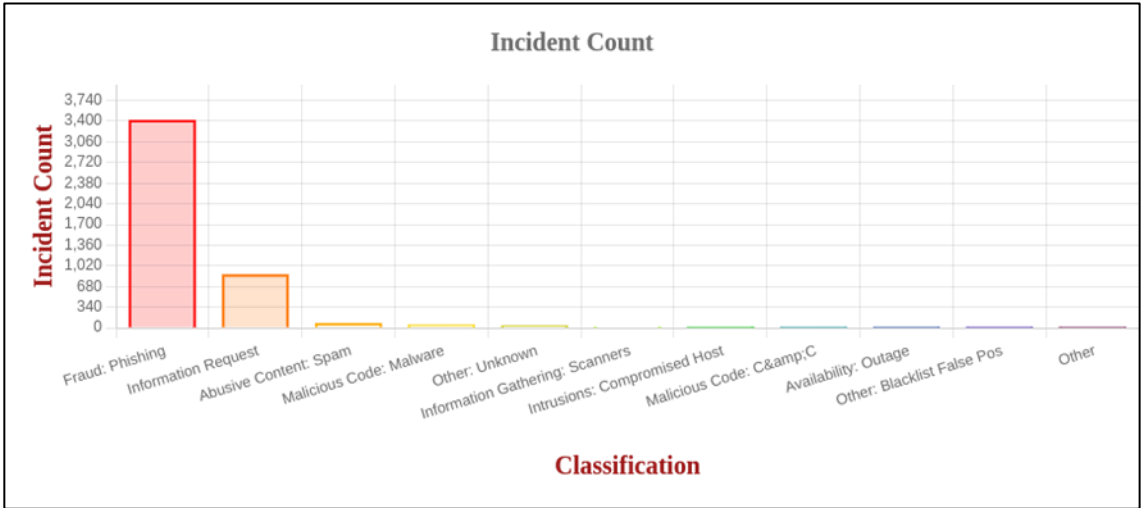
AUSCERT monitors and evaluates global cyber network threats and vulnerabilities and remains on-call for members after hours. AUCERT publishes the Security Bulletin Service, drawing on material from a variety of sources, with recommended prevention and mitigation strategies.

Services provided are listed as:

- Incident Management [3.2],
<https://www.auscert.org.au/services/incident-management-service/>
- Early Warning Service
<https://www.auscert.org.au/services/early-warning-service/>
- Malicious URL Feed
<https://www.auscert.org.au/services/malicious-url-feed/>
- Security Bulletin Service [3.3]
<https://www.auscert.org.au/services/security-bulletins/>
- Member security incident notification's (MSINs)[3.4]
<https://www.auscert.org.au/services/security-incident-notifications/>
- Phishing take-down
<https://www.auscert.org.au/services/phishing-take-down-service/>
- Leaked Credential Service
- AUCERT's member only Slack
- AUCERT Conference
<https://conference.auscert.org.au/>

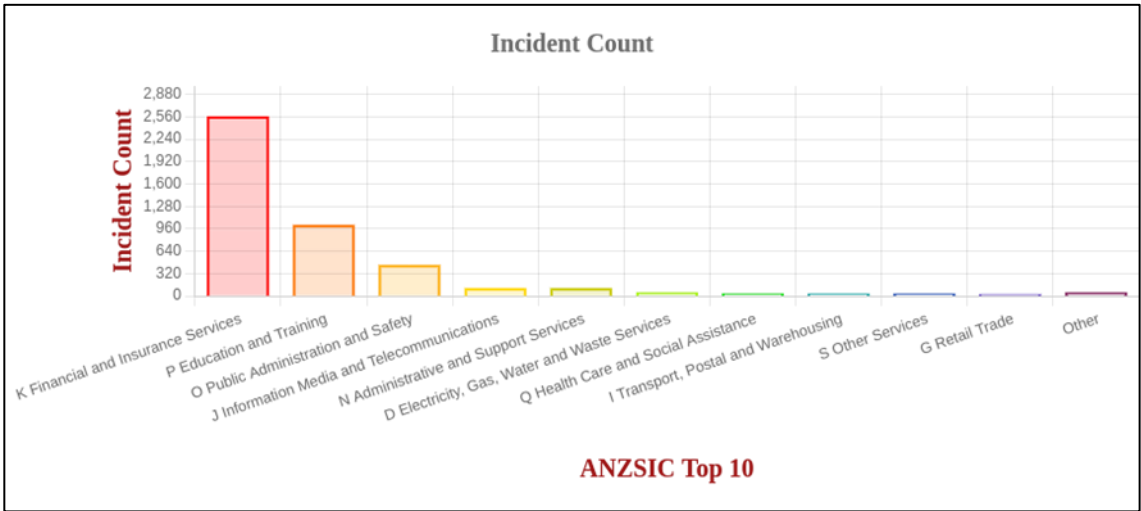
3.2 Incident Management

AUSCERT's Incident Management Service (sometimes referred to as incident response) includes incident coordination and incident handling, both of which are standard inclusions as part of AUCERT's membership services. As a 24/7 membership benefit, it is perhaps AUCERT's most focal service offering.



The diagram above shows the statistics of incidents that required handling for the calendar year of 2022. Overall, AUSCERT serviced 4490 tickets which resulted in just under 18 tickets per business day of operation. A vast majority of the work is around handling of phishing sites.

Incidents have happened across a wide varied range of industry. The following diagram shows the top 10 industries with respect to the number of incident tickets handled.

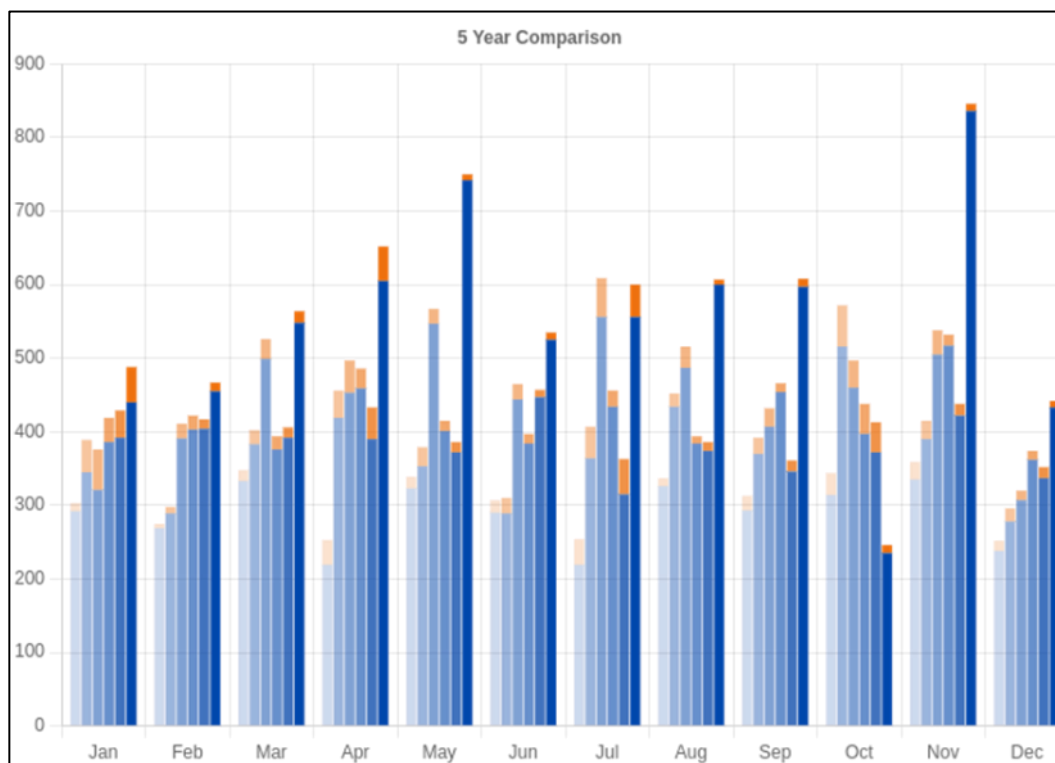


The industry definition used is the Australian and New Zealand Standard Industrial Classification (ANZSIC) and further details can be found at: <https://www.abs.gov.au/statistics/classifications/australian-and-new-zealand-standard-industrial-classification-anzsic/latest-release>

3.3 Security Bulletins

AusCERT distributes security advisories and bulletins to its members by email and publishes a portion of them to its public website. Bulletins are published in a standardised format with a consistent approach to classifications of

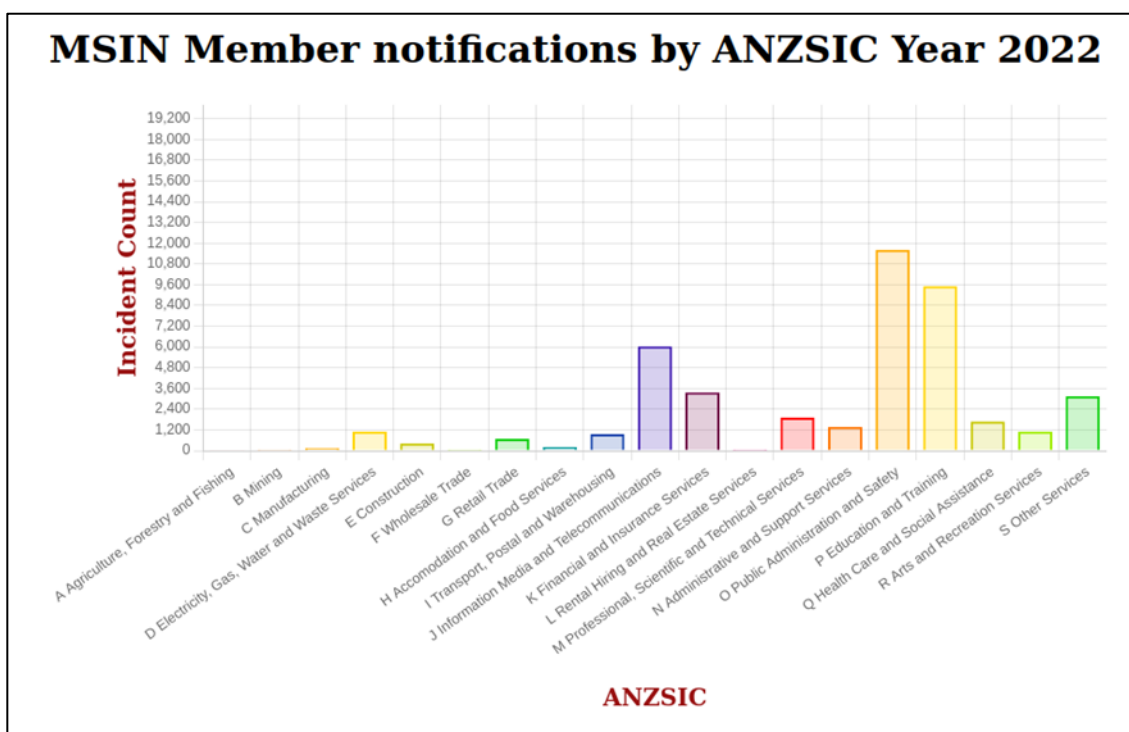
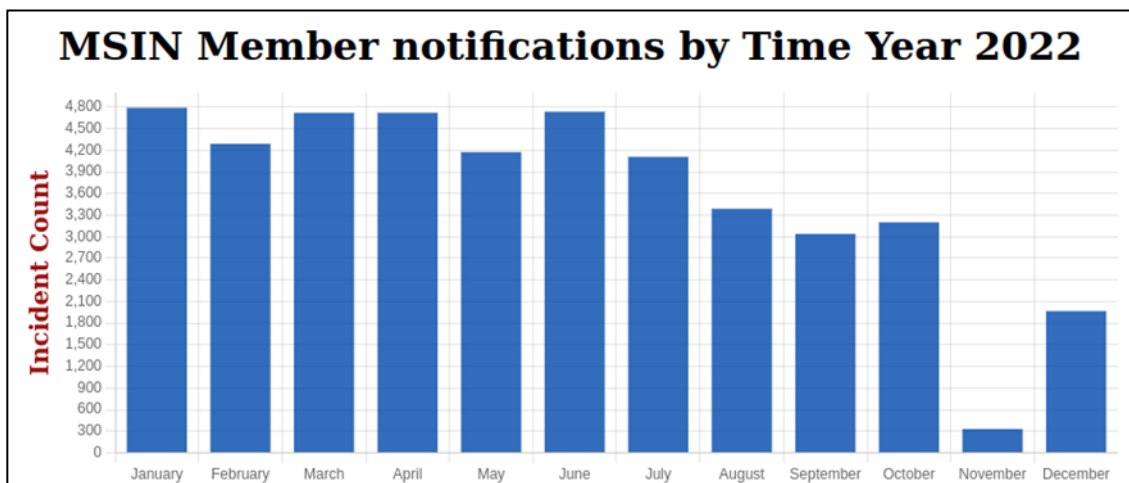
vulnerabilities, impacts and affected operating systems. In 2022, 6562 External Security Bulletins (ESBs) and 233 AusCERT Security Bulletins (ASBs) were published.



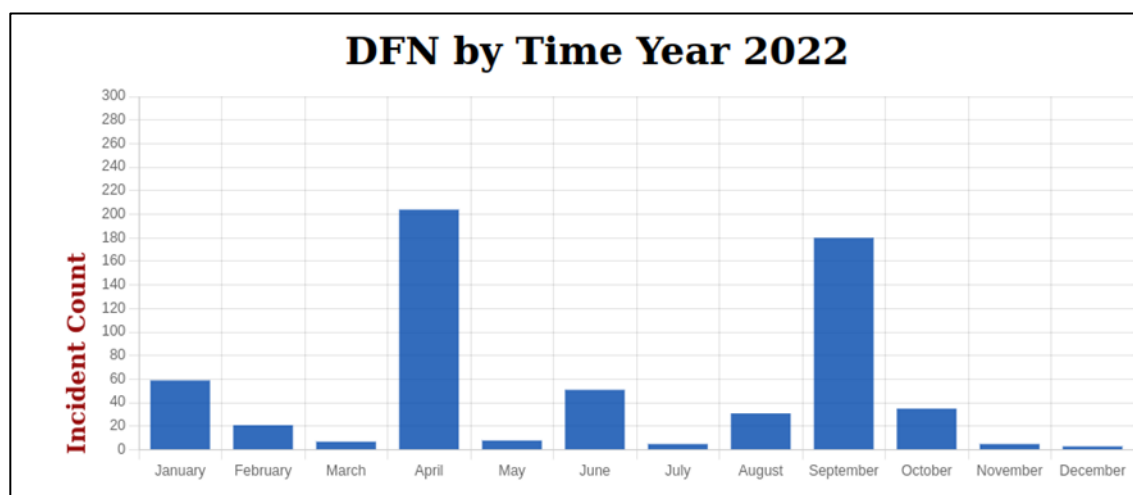
The marked increase as can be seen from the 5-year comparison chart is due to streamlining the process of security bulletin publication.

3.4 Member Security Incident Notifications

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).



An extension of the MSIN is a notification of edge hardware that is vulnerable as notified by a PSIRT's advisory. This notification is done in a similar manner as MSINs but are different as the source of information is different.



3.5 Publications

3.5.1 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.

3.5.2 Week in Review

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

3.5.3 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.

3.5.4 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.

3.5.5 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.

3.5.6 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 Conferences and seminars

4.1.1 AusCERT Conference

The AusCERT Conference 2022, took place from 10th May -13th May 2022 at the Star hotel Gold Coast with the theme of "Rethink, Reskill, Reboot" that was also broadcasted online. The conference included 50 presenters of ranging topics on cyber security.

5. International Collaboration

5.1 International partnerships and agreements

AusCERT maintains relationship and membership with Asia Pacific Computer Emergency Response Team (APCERT) and the Forum of Information Response Security Teams (FIRST)

5.2 Drills and Exercises

5.2.1 APCERT Drill 2022

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 "Data Breach through Security Malpractice". The drill fosters communication between the CERTs in the region and beyond. In all, 25 CERT/CSIRT teams from APCERT participated

5.2.2 ACID 2022

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 host AUSCERT Conference that brings together the Cyber Security community of Australia at the professional level. Although the year of 2022 has seen record numbers of External Security Bulletins being processed,

the numbers of phishing takedown have also dramatically increased. The streamlining of processes has enabled the handling of these influx of work. An increase in volume of work was also seen is in the notification of security events that have impacted the constituency. MSINs and credential dump advisories have therefor increased in part due to the ever increasing ransomware attacks affecting higher profile victims. 2022 has allowed AUSCERT to relook at some processes in handling increased volumes and background work has started to improve the capacity of AUSCERT in 2023.

BGD e-GOV CIRT

Bangladesh e-Government Computer Incident Response Team

1. Highlights of 2022

1.1 Summary of major activities

- BGD e-GOV CIRT has successfully organized National Cyber Drill, Inter University Cyber Drill and Cyber Drill for Financial organizations.
- Total 522 cyber security incidents registered in our tracking system.
- Total Nine (9) IT security audits performed.
- Organized stakeholder consultation on Data Protection Act, 2022 (DRAFT).
- Provided Digital Forensics service to a total 7 organizations. Total number of analyzed cases were 11 and total number of investigated artifacts were 36.
- Provided 40 cyber sensor analysis reports (from January 2022 - December 2022) to multiple Critical Information Infrastructures.
- "Cyber Threat Intelligence Report" provided to 60 government and non-government organizations.

1.2 Achievements & milestones

- BGD e-GOV CIRT has successfully participated in OIC-CERT Cybersecurity Drill 2022 and achieved 2nd position.

2. About CSIRT

2.1 Introduction

Bangladesh Government's Computer Incident Response Team (BGD e-GOV CIRT) is acting as the National CERT of Bangladesh (N-CERT) currently with responsibilities including receiving, reviewing, and responding to computer security incidents and activities. Under the Government of People's republic of Bangladesh, BGD e-GOV CIRT reviews and takes

necessary measures to resolve the issue with broad cybersecurity ramifications, conducts research & development and provides guidance on security vulnerabilities. BGD e-GOV CIRT also works with various government units, Critical Information Infrastructures, financial organizations, law enforcement agencies, academia & civil society to help to improve the cybersecurity defense of Bangladesh.

2.2 Establishment

The process to establish BGD e-GOV CIRT was started on November 2014 and team starts operation on February 2016.

2.3 Resources

Currently 17 people are working in BGD e-GOV CIRT.

2.4 Constituency

Constituency of BGD e-GOV CIRT are all governmental, semi-governmental, autonomous bodies, ministries & institutions of Bangladesh. Currently BGD e-GOV CIRT is acting as National CERT of Bangladesh with a mandate to serve whole of Bangladesh.

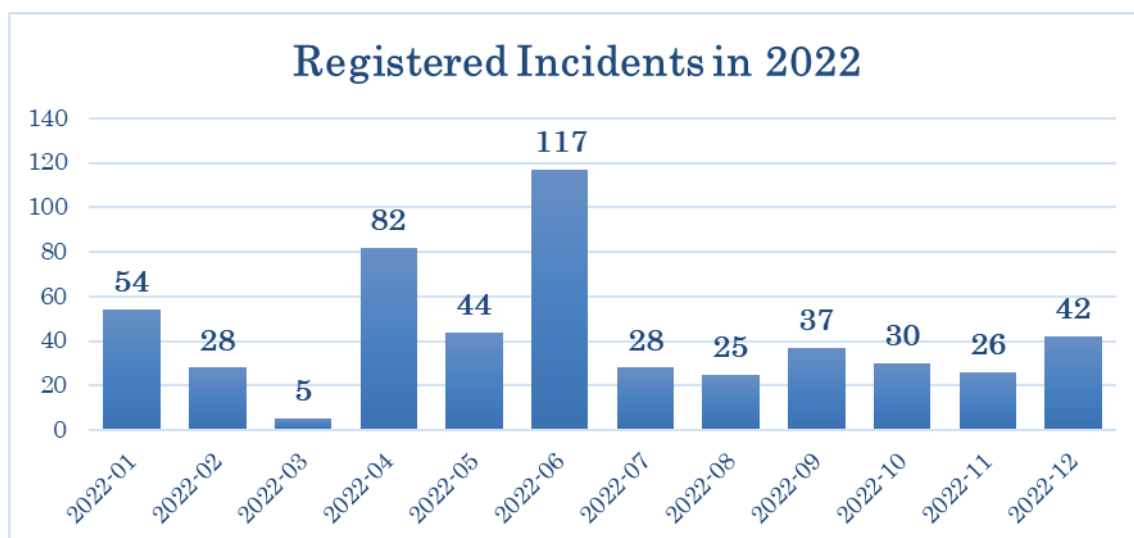
3. Activities & Operations

3.1 Scope and definitions

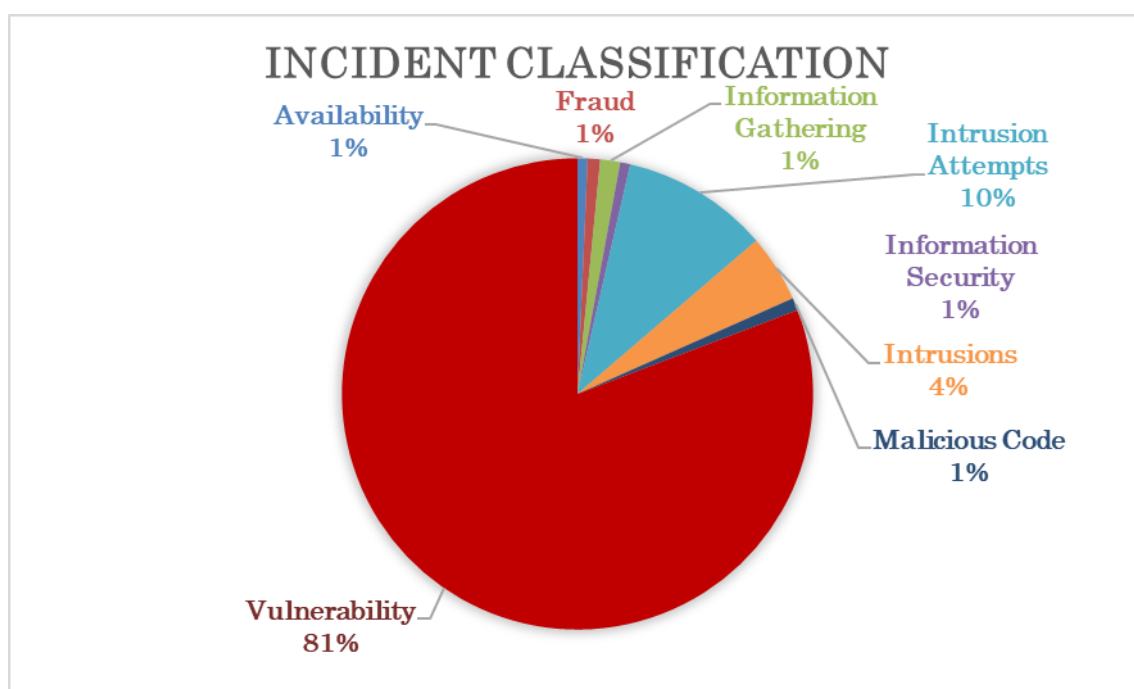
BGD e-GOV CIRT provide technical assistance and facilitate to manage cyber security in Bangladesh government's e-Government network and related infrastructure. BGD e-GOV CIRT also serve as a catalyst in organizing national cyber security resilience initiatives among various stakeholders. BGD e-GOV CIRT works for establishment the national cyber security incident management capabilities in Bangladesh.

3.2 Incident handling reports

BGD e-GOV CIRT receives information regarding cyber security incidents, triage incidents and coordinate response. Activities related to incident handling includes and not limited to Vulnerability Assessment, Penetration Test, Incident Analysis, Security Threat Notification and Incident Coordination etc.



3.3 Abuse statistics



3.4 Publications

- Ransomware Prevention & First Response Guideline has been published.
- Digital Forensic Guideline 2.0 has been published.
- Critical Information Infrastructure Guideline Implementation Workbook 1.0 has been published.
- Report on Sectorial Threat Intelligence for Banks July 2022 has been published.

- “Cyber Threat Landscape Report 2022” has been published.
- Ransomware State of Bangladesh was published in September 2022.
- Horizon Scanning Report for Bangladesh Telecom Operators was published in Q1,2022.
- Publishing a monthly cyber security magazine for stakeholders.

4. Events organized / hosted

4.1 Training

- Daylong workshop on BGD e-GOV CIRT operations for ICT Division, Ministry of Post, Telecommunications and IT.
- Organized 4 days long training program on Cyber Security for high officials of ICT Division, Ministry of Post, Telecommunications and IT.
- Organized 4 days long training program on Secure Computer User for officials of Bangladesh Army.
- Organized 3 days long training program on Information Systems Auditing for officials of Bangladesh Police.
- Organized 3 days long training program on Advance Cyber Security for personnel from WZPDCL.
- Organized 3 days long training program on Basic Cyber Security for personnel's from Bangladesh Computer Council.
- Organized 3 days long training program on Basic Cyber Security for personnel's from PKSF.

4.2 Drills & exercises

- Arranged National Cyber Drill 2022.
- Arranged Inter University Cyber Drill 2022.
- Arranged Financial Cyber Drill 2022.

5. International Collaboration

5.1 Capacity building

5.1.1 Training

- BGD e-GOV CIRT team participated in the RSA Conference 2022.
- BGD e-GOV CIRT team participated in ICS 301 Live and CSET training in Idaho Falls, USA.
- BGD e-GOV CIRT team participated in cyber security training in Dubai, UAE and New Delhi, India.
- Advanced Incident Handling training organized by Carnegie Mellon University, USA.

5.1.2 Drills & exercises

- Participated in the annual FIRST CTF 2022.
- Participated in the annual APCERT CTF 2022.
- BGD e-GOV CIRT has successfully participated in OIC-CERT Cybersecurity Drill 2022 and achieved 2nd position.

6. Future Plans

6.1 Future Operation

- Arrange Cyber Drills for different sectors.
- Perform risk assessment to critical infrastructure (CIs).
- Provide training about Industrial Control System (ICS) in public sector.
- Perform vulnerability assessment and penetration testing on financial sectors.
- Training and workshop about cyber security for government organizations.
- Provide regular cyber sensor analysis reports (Intrusion, Suspicious activity) to Critical Information Infrastructure where Cyber sensor deployed.

7. Attachments (Photos)



Figure: Cyber security training for ICT Division officers'



Figure: Award giving ceremony for cyber drill winners



Figure: Workshop on "Using Social Media to Counter Radicalism" in presense of Australian Deputy High Commissioner



Figure: Advanced Incident Handling training organized by Carnegie Mellon University, USA



Figure: Celebrating success for achieving 2nd place in OIC-CERT Cyber Drill



Figure: Training on Information Systems Auditor



Figure: Training on cyber security



Figure: Training on Secure Computer User



Figure: BGD e-GOV CIRT joins at RSA 2022, USA.



Figure: Celebrating Cyber Security Week 2022



Figure: National Cyber Drill 2022 host team



Figure: University Cyber Drill 2022 host team



Figure: Participants on Cyber Security training in Dubai, UAE.

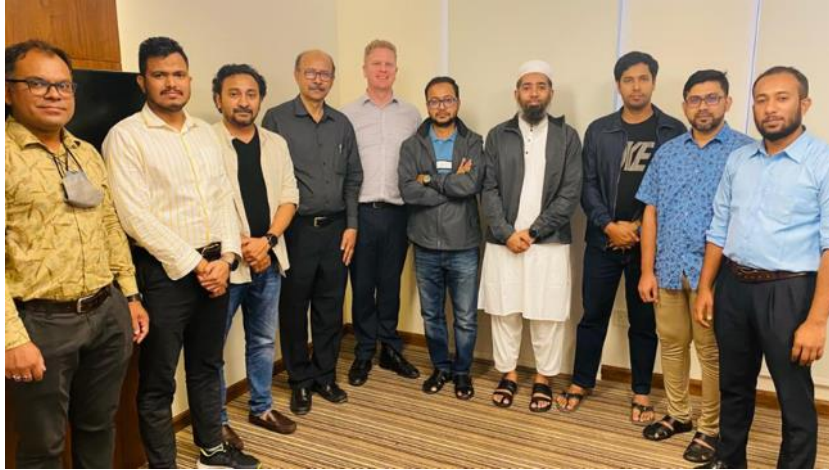


Figure: Participte on Cyber Security training in Dubai, UAE.



Figure: Participte on Cyber Security training in New Delhi, India.



Figure: Session on Digital Forensics at BUET

BruCERT

Brunei Computer Emergency Response Team

1. About BruCERT

1.1 Introduction

Cyber Security Brunei (CSB) is the national cyber security agency of Negara Brunei Darussalam, serving as an administrator that monitors and coordinates national efforts in addressing cyber security threats and cyber crime. It operates under the Ministry of Transport and Infocommunications (MTIC), with the Minister of MTIC as Minister-in-charge of Cybersecurity.

CSB provides cybersecurity services for the public, private and public sectors in Negara Brunei Darussalam. These cyber security services are intended to ensure the following interests:

- i. Increase awareness of cyber threats in the public and private sectors, especially the protection of the Critical Information Infrastructure (CII) in Negara Brunei Darussalam;
- ii. Improve the ability to respond to cyber incidents through effective cyber crisis management;
- iii. Enhance law enforcement capabilities in addressing cyber threats through the services of the National Digital Forensics Laboratory; and
- iv. Increase public awareness of cyber threats.

Brunei Computer Emergency Response Team (BruCERT) was established in May 2004. It was formed in collaboration with AITI, the Ministry of Communication, to become the nation's first trusted one-stop referral agency in dealing with computer-related and internet-related security incidents in Brunei Darussalam. It is now under Cyber Security Brunei.

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 organization 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 has a strength of 66 staff (100% local) of which a majority is specialized in IT and the rest is administration and technical support. Its staff has undergone training on various IT and security modules, such as A+, N+, Linux+, Server+, Security+, SCNP, SCNA, CIW, CEH, CCNA, CISSP, BS7799 Implementer and SANS trainings such as GREM, GCIA, GCIH, GCFA, GPEN, where most of BruCERT workforce has gained certifications in.

1.4 BruCERT Constituents

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

Government Ministries and Departments

BruCERT provide Security incident response, Managed Security Services 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 work closely with EGNC in providing Incident Response and Security Monitoring since most of the government equipment resided at EGNC.



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

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) 2458002
- Email: cert@brucert.org.bn
- Reporting: reporting@brucert.org.bn

2. BruCERT Operation in 2022

2.1 Incidents response

For the year 2022, CSB's BruCERT, through the Cyber Watch Centre (CWC), has identified multiple instances of malicious behavior through the secure monitoring and intelligent sensors, located at the BruCERT constituent systems. Based on these findings, malware infections, are the most prevalent form of cyber threat in Brunei Darussalam which some instances involve "Ransomware" attacks. The second most common type of incident detected involved attacks on user accounts, including both user and privilege accounts. Figure 1 and Table 1 depict the statistics of these security incidents.

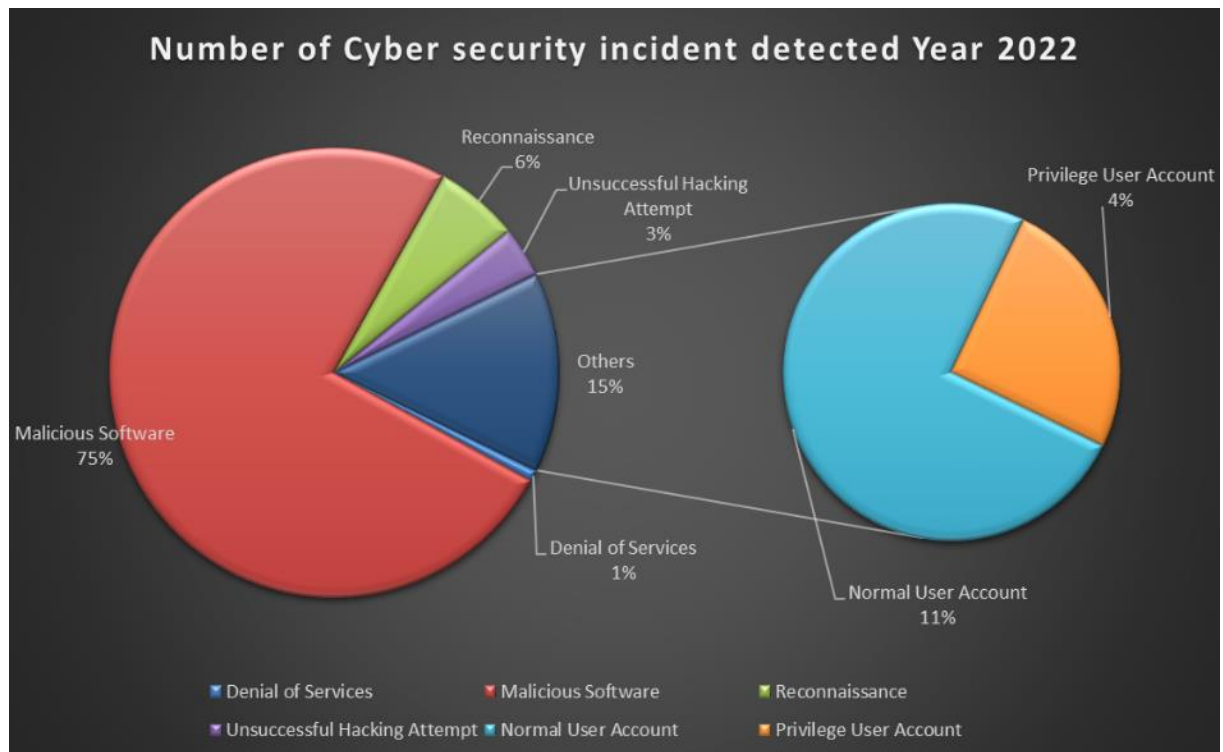


Figure 1

Types of Attacks	Count
Denial of Services	31
Malicious Software	3025
Reconnaissance	244
Unsuccessful Hacking Attempt	146
Normal User Account	434
Privilege User Account	146

Table 1

2.2 BruCERT Honey Pot

CSB's BruCERT had been deploying Honey Pot, a test web server to intentionally lure cyber attackers to compromise the server. From the logs extracted from the honeypot, BruCERT had identified that the most abused port number is 445 which is the SAMBA (SMB) followed by port number 22 which is used by Secure Shell Connection (SSH) for connectivity.

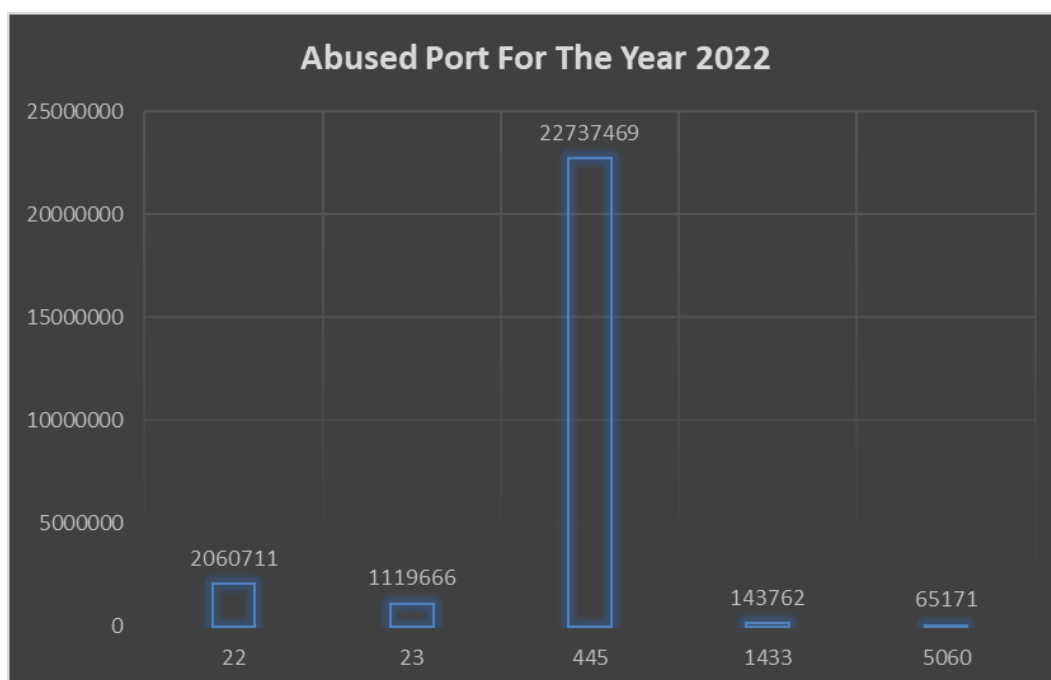


Figure 2

Port No	Count
22	2060711
23	1119666
445	22737469
1433	143762
5060	65171

Table 2

From BruCERT honey pot, it seems new variants of malware had been targeting the organizations using port 22 as well as port 445. This can be further support from the malware which was captured by BruCERT honeypot which is shown by Figure 4. In other configuration, BruCERT Honeypot managed to capture some of the malware hashes, as shown in Figure 3. Table 3 show the summary of the most detected malware attacking the Honeypot.

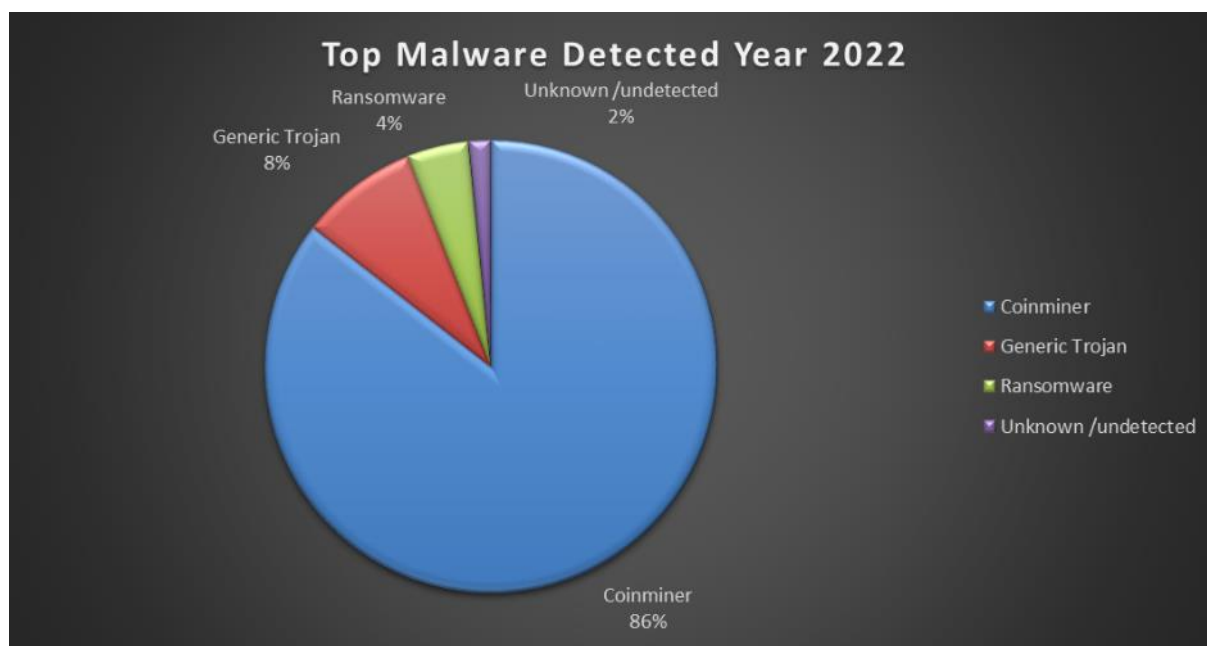


Figure 3

Malware Type	Total
COINMINER	37418
GENERIC TROJAN	3709
RANSOMWARE	1916
UNKNOWN	693
Grand Total	43736

Table 3

The year 2022, BruCERT has been receiving incident reports from the general public, including the private sector. During March 2022 and August 2022, BruCERT experienced a significant surge in incident reports received via email and the BruCERT hotline. The majority of these reports pertained to "Social Media Issues" and "Scam" activities. The former included instances of social media accounts such as Instagram, Facebook, WhatsApp, and Telegram being successfully compromised or taken over, with an increase in such incidents observed in Brunei Darussalam. Compromised social media accounts were often used as part of the "Scamming" activity. Since the outbreak of the Covid-19 pandemic, there has been a rise in scamming activity specifically targeting Bruneians, utilizing local Brunei. Please refer to Figure 4.

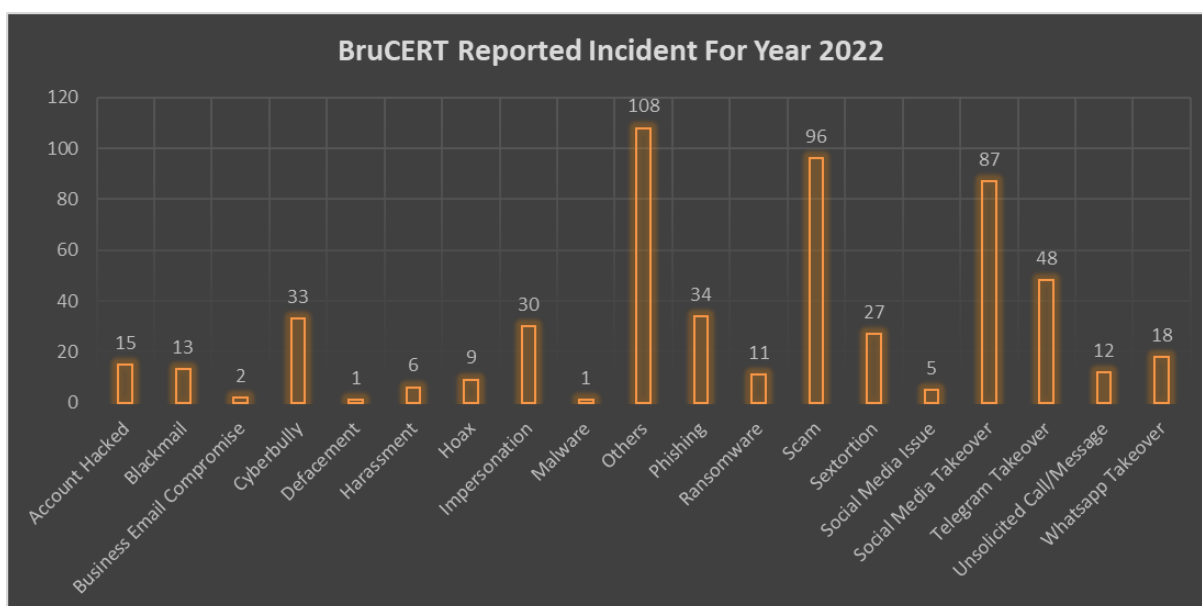


Figure 4

3. BruCERT Activities in 2022

3.1 Seminars/Conferences/Meetings/Visits

BruCERT attended and presented at various seminars, conferences and meetings related to the field of ICT security but some of the meetings are done through virtual meetings.

- On 18th October 2022 until 19th October 2019 - BruCERT delegates attended the APCERT AGM and Annual Conference 2022 which takes place online.
- On 6th November 2022 until 9th November 2022 - Three BruCERT delegates attended the OIC-CERT 10th GENERAL MEETING & 14th ANNUAL CONFERENCE (in conjunction with the 10th Regional Cybersecurity Summit & the FIRST & ITU-ARCC Regional Symposium for Africa and Arab Regions) which takes place at Muscat, Oman, hosted by OMAN CERT

3.2 Awareness Activities

Throughout 2022, CSB via BruCERT conducted various awareness-raising activities aimed at educating both the general public and public servants about the security threats present in the cyber world. Their main awareness website for this program is secureverifyconnect.info, which received a total of 42,049 website visits. The website experienced its highest traffic during May and June, when an advertisement for the BruCERT Capture the Flag (CTF) competition was published. (Figure 5)

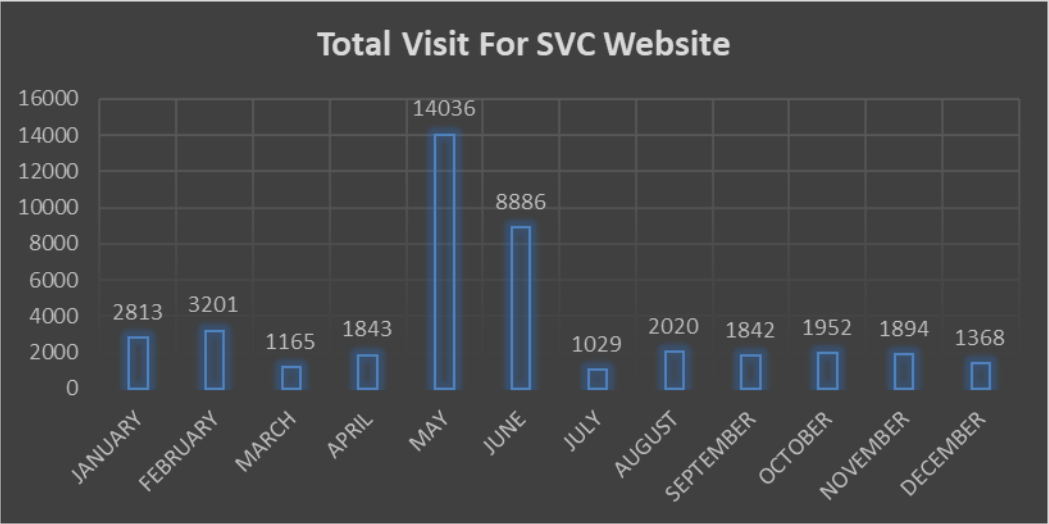


Figure 5

BruCERT awareness talk which was provided to schools, community as well as corporate/organization also took place almost every month in the year 2022.

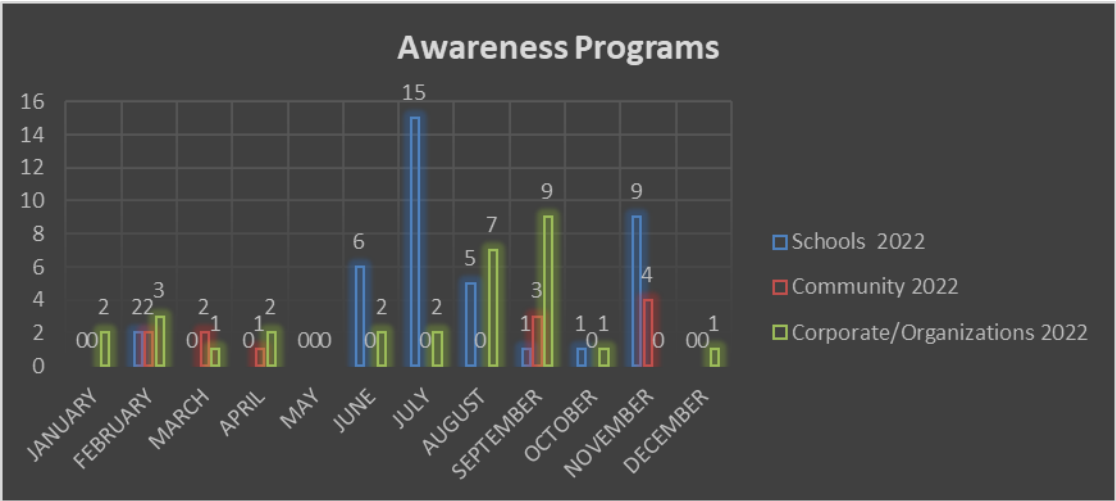


Figure 6

BtCIRT

Bhutan Computer Incident Response Team

1. Highlights of 2022

1.1 Summary of major activities

In 2022, the first ever Cyber Drill was conducted virtually in collaboration with the International Telecommunication Union (ITU). The second edition of the “National Cybersecurity Week” was also conducted successfully. In addition, BtCIRT became a member of Cybersecurity Alliance for Mutual Progress (CAMP) and Global Forum on Cyber Expertise (GFCE). A few workshops and training were also conducted in person while few were conducted online.

1.2 Achievements & milestones:

Key activities in 2022 included:

- Produced and aired three online banking and scam related awareness videos on national television and online platforms.
- Collaborated with ITU to conduct a joint ITU-Bhutan CyberDrill from 11-14 July that included a panel discussion, cybersecurity awareness for 30 leaders and parliamentarians, and workshops and Cyber-range simulation training for 30 technical officials.
- Membership to CAMP in July and GFCE in September.
- Organized the second “Cybersecurity Week” from 5-8 December, covering various programs; a full day seminar, a Cybersecurity Boot-Camp workshop and an Open Awareness program with awareness content published in BtCIRT Facebook page promoting cyber hygiene best practices.
- Published 79 Alerts and advisories on latest scams and threats
- Handled a total of 171 incidents in the past year

2. About BtCIRT

2.1 Introduction

The Bhutan Computer Incident Response Team (BtCIRT) is a part of the GovTech Agency (previously the Department of Information Technology and Telecom under the erstwhile Ministry of Information and Communications). 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 attacks and vulnerabilities.

2.2 Establishment

The BtCIRT was formally established on 20 May 2016 as the national focal point for coordinating and implementing cybersecurity activities and initiatives for Bhutan.

2.3 Resources

Currently, BtCIRT consists of seven working team members.

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. While BtCIRT 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 for contributing towards a 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 along with system administrators.
- Conduct periodic security assessment of government systems and provide services to non-government organizations on request.
- Represent Bhutan in international forums.
- Develop strategies, policies, standards, guidelines and baseline documents.

3.2 Incident Handling Report

A total of 171 incidents were handled in 2022, majority of which were vulnerabilities (62.6%), followed by fraud related incidents like phishing and scams (18.1%). The following graph provides the overview of the types of incidents handled:

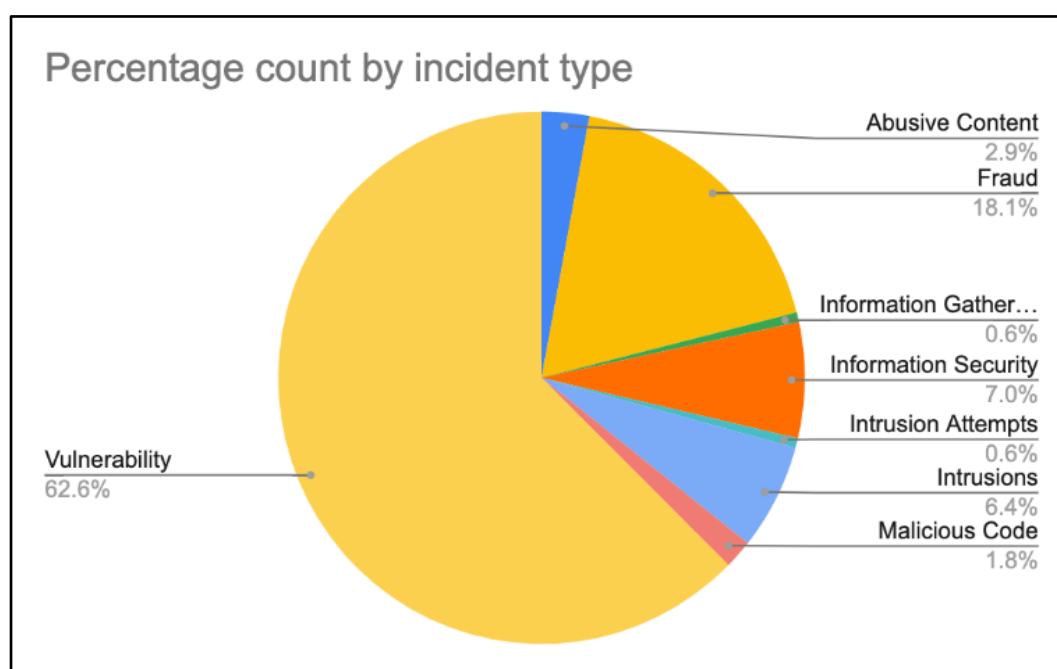


Figure 1: Percentage of Incident handled by Incident Classification type

3.3 Awareness creation programs

Awareness and advocacy is a very important mandate of BtCIRT. A number of awareness programs were implemented in 2022, as described in the following:

3.3.1 Cybersecurity awareness Animation Videos

In collaboration with the Tech Industry Development Division, a total of three animation videos were developed. The animation videos covered Online Banking security, How to Protect Online Accounts and Online scam related advisory and safety measures. The contents were aired on national television and shared through various social media platforms. A comic was also published highlighting cyberbullying issues in schools and the importance of providing support by parents, teachers and peers in helping students address such issues.



Figure 2: Awareness Videos produced

3.3.2 Participated in Cybersecurity and Cybercrime awareness discussions

- The panel discussion for 'End Violence Against Children advocacy' on 23rd August where BtCIRT participants contributed to the multi-sectoral discussion by sharing about the risks of children being online, including cyber bullying risks.
- A live Q&A session on 8th October by Bhutan Broadcasting Service covered prevalent scams in social media leading to compromise of accounts or loss of funds. A follow up in-depth discussion was also aired regarding the same on 20th October and was re-aired a couple of times.
- A panel discussion among youths and stakeholders was organized by RENEW on 12th June as a part of their youth talk series on the Digital Literacy theme, where issues related to digital technologies and challenges were discussed.

3.3.3 Awareness in Colleges

A cybersecurity awareness session was conducted in two colleges; one session for Royal Thimphu College (around 100) on 8th June, and two sessions for Khesar Gyalpo University of Medical Science (around 150) on 10th and 24th June. The sessions were attended by both students and faculty members.

3.3.4 Cyber Hygiene awareness at National Scout Center

Another Cyber Hygiene awareness session was conducted at the National Scout Center, Paro on 22nd June, for more than 140 scout students.

3.4 Security Advisory and Alerts

BtCIRT publishes latest cyber security news and vulnerabilities to keep the constituents well informed about the latest development in the area of cybersecurity on its website and Facebook page. A total of 79 alerts and advisories were

published in 2022. Of these alerts and advisories, a significant proportion were released to address critical patches released by software vendors to fix the vulnerabilities.

4. Events organized / hosted

4.1 Training/Workshops, Drills & exercises

4.1.1 Cybersecurity leadership workshop (January, 2022)

In collaboration with Nanyang Polytechnic International (NYPi) and Temasek Foundation in Singapore, a "Cybersecurity Programme for Leaders" for executives and chiefs from various government Ministries and agencies was conducted over 5 sessions in the month of January. The objective of the program was to cultivate cybersecurity leadership in the ministries/agencies and educate leaders on cybersecurity and showcased various cases from Singapore government experiences.

4.1.2 Email security and SSL Certificate workshop (24-25 May)

In the email security & SSL Certificate workshop where ICT officials from various government agencies were in attendance, the participants learned about email security, configuring SSL certificates, and concepts of vulnerability management.

4.1.3 Workshop on Incident Handling and Critical Information Infrastructure (12-13 July)

As a part of the Cyber Drill event, Incident Response Management and Identification of Critical Information Infrastructure workshops were conducted virtually over two days by external trainers supported by ITU. Over 30 ICT officials from government agencies, corporate and private sectors participated in the workshops each day.

4.1.4 Workshop on Building a Robust Cybersecurity Ecosystem (18th August)

In collaboration with the Government of Karnataka, a half day virtual workshop was conducted on sharing the learnings of Cybersecurity by both the governments. The workshop was attended by more than 100 ICT officials from various government, private and other agencies/organizations in Bhutan.

4.1.5 National Cybersecurity Week (5-9 December)

The 2nd edition of the National Cybersecurity Week was observed from 5-9 December, whereby several programs were conducted.

- **Cybersecurity Seminar (5th December)**

The speakers from Government agencies, Corporations and Private companies touched upon various cybersecurity efforts and issues. The seminar was also attended by ICT professionals from different backgrounds covering the full breadth of the cybersecurity ecosystem.

- **Cybersecurity Bootcamp (6-7 December)**

The Cybersecurity Bootcamp event hosted an Information Security Workshop and a Capture the Flag contest for 41 students from two colleges (College of Science & Technology and Jigme Namgyel Polytechnic College) and one Institute (Royal Institute of Management).



- **Awareness on Cybersecurity (8th December)**

An open cybersecurity awareness program was conducted targeting the general public to help with their understanding of prevalent cybersecurity threats and cybersecurity best practices in the online world. Awareness content was also published in the BtCIRT Facebook page throughout the week promoting cyber hygiene best practices.

4.1.6 Drills/Exercises

ITU-Bhutan joint National Cyber Drill

As a part of the National Cyber Drill, several programs under various themes were conducted from 11-14 July.

- **Reflect:** Panel Discussion and Awareness program for parliamentarians and secretaries
- **Learn:** Incident Response management and Identification of Critical Information Infrastructure Workshops for ICT professionals
- **Practice:** Four scenario based hands-on exercises simulating real life cyber attacks in Cyber Range platform for ICT professionals

5. International Collaboration

5.1 International partnerships and agreements

BtCIRT has been a member of Asia Pacific Computer Emergency Response Team (APCERT) and the Forum of Information Response Security Teams (FIRST) since 2016. In 2022, new partnerships were explored which resulted in successful

membership to CAMP on 11th August and GFCE on 25th August 2022.

5.2 Capacity building

5.2.1 Trainings

BtCIRT participated and benefited from the following international in-person trainings:

Event	Organizer/Trainer	Region	Date
Cybersecurity Course on Practical Penetration Testing	NYPi/Temasek Foundation & RGoB	Singapore	26 September-14 October, 2022
APNIC 54 Conference	APNIC	Singapore	12-15 September, 2022
Cybersecurity for Industry Control Systems	Cybersecurity and Infrastructure Security Agency (CISA)	USA	13-16 September, 2022
7th Annual CAMP Meeting	CAMP	South Korea	18-20 October, 2022

5.2.2 Drills and exercises

- Annual APCERT Drill themed “Data Breach through Security Malpractice” on 25th August.
- ITU-Bhutan joint National Cyber Drill, 14th July:
Participants learned to handle different types of cyber attacks, through four scenario-based exercises developed in the Cyber Range platform.

5.2.3 Seminars, Conference & Presentations

The BtCIRT had the opportunity to attend and participate in the following seminars and conferences:

- **APNIC 54 Conference**, 12-15 September:
A presentation with the title “Cybersecurity Initiatives and trends of Cyber Attacks in Bhutan” was presented during the conference in person in September 2022.
- **World Bank Cyber Talks**: Top Challenges for Cyber Resilient Development session, 7th November:
Top challenges for Bhutan were presented during the session.

6. Future Plans

BtCIRT will continue to work towards improving incident handling capabilities and work on areas to improve the overall cybersecurity maturity of Bhutan.

The future plans for BtCIRT include:

- Implementation of National Cybersecurity Strategy
- Strengthening cooperation and collaboration with more organizations internally and internationally

- Building relevant cybersecurity capabilities to defend and protect critical information infrastructure
- Cybersecurity awareness for leaders, users and general public

7. Conclusion:

BtCIRT will continue to focus on improving the relevant cybersecurity capabilities within the country and creating awareness on Cybersecurity and the importance of managing security risks to critical information assets.

CERT-In

Indian Computer Emergency Response Team

1. Highlights of 2022

1.1 Summary of major activities

- In the year 2022, Indian Computer Emergency Response Team (CERT-In) handled 13,91,457 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 653 security alerts, 38 advisories and 488 Vulnerability Notes were issued during the year 2022.
- CERT-In conducted 23 cyber security training and awareness programs for Government, Public, Critical Sector organisations to educate them in the area of Cyber Security with the latest security threats, needs and developments & deployment of techniques and tools in order to minimize security risk.
- CERT-In conducted 9 domestic cyber crisis exercises in 2022 for various organizations across Sectors and State Government Departments.
- CERT-In has contributed to 2 international exercise planning & scenario development and participated as a player in 6 International cyber security drills in 2022.
- CERT-In in collaboration with Cyber Security Agency (CSA), Singapore conducted an International cyber security exercise "Synergy" for 13 Countries as part of the International Counter Ransomware Initiative- Resilience Working Group in August 2022.
- CERT-In has trained & enabled sectoral entities to conduct sector specific exercise and drills.
- CERT-In was the convener of APCERT Internet of Things (IoT) Security technical working group. As a member of APCERT Drill WG, CERT-In has also contributed in APCERT drill 2022 design & execution.
- CERT-In conducted an online webinar on "Cyber Threat Hunting" for cyber security professionals from Government Cyber Security Agencies of IBSA Member States (India, Brazil, South Africa) on 3rd November 2022.

- CERT-In conducted a two-day joint online webinar on “Cyber Threat Hunting” in collaboration with ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE), Singapore for cyber security professionals from ASEAN Member states on 15 and 16 November 2022.

1.2 Achievements & milestones

- CERT-In became an Accredited Member of Task Force for Computer Security Incident Response Teams / Trusted Introducer (TF-CSIRT/TI) from 13 September 2022.
- CERT-In conducted one (1) International cyber security exercise “Synergy” for 13 Countries in 2022 as part of the International Counter Ransomware Initiative- Resilience Working Group.
- CERT-In has trained and enabled sectoral entities to conduct sector specific exercise and drills.
- 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.
- In 2022, CERT-In Signed bilateral agreements in the area of cyber security with The National Centre for Information Technology (NCIT), Republic of Maldives and renewed the agreements with Bangladesh Government Computer Incident Response Team (BGD e-Gov CIRT), People’s Republic of Bangladesh and Cyber Security Department, Socialist Republic of Viet Nam to enable information sharing and collaboration for incident resolution.

2. About CERT-In

2.1 Introduction

- CERT-In is a government organisation under Ministry of Electronics and Information Technology (MeitY), Government of India established with the objective of securing Indian cyber space. CERT-In provides Incident Prevention and Response services as well as Security Quality Management Services.
- CERT-In has been designated to serve as national agency for incident response under Section 70B of the Information Technology Act, 2000 (Amendment 2008). CERT-In operates 24x7 incident response Help Desk for providing timely response to reported cyber security incidents. 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.

- 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 organizations in the Government, Public and Private 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 2022 is given in the following table:

Activities	Incidents in 2022
Security Incidents handled	1391457
Vulnerability Notes Published	488
Advisories Published	38
Security Alerts issued	653
Security Drills	14
Trainings Organized	23

Table 1: CERT-In Activities during year 2022

3.3 Abuse statistics

In the year 2022, CERT-In handled 1391457 incidents. The types of incidents handled were Website intrusion & Malware propagation, Malicious Code, Phishing, Distributed Denial of Service (DDoS) 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	2022
Phishing	1714
Unauthorized Network Scanning /Probing	324620
Vulnerable Services	875892
Virus/ Malicious Code	161757
Website Defacements	19793
Website Intrusion & Malware Propagation	2164
Others	5517
Total	1391457

Table 2: Breakup of Security Incidents handled

3.3.1 Tracking of Indian Website Defacements

CERT-In has been tracking the defacements of Indian websites and suggesting suitable measures for hardening the web servers to concerned organizations. A total of 19793 numbers of defacements have been tracked.

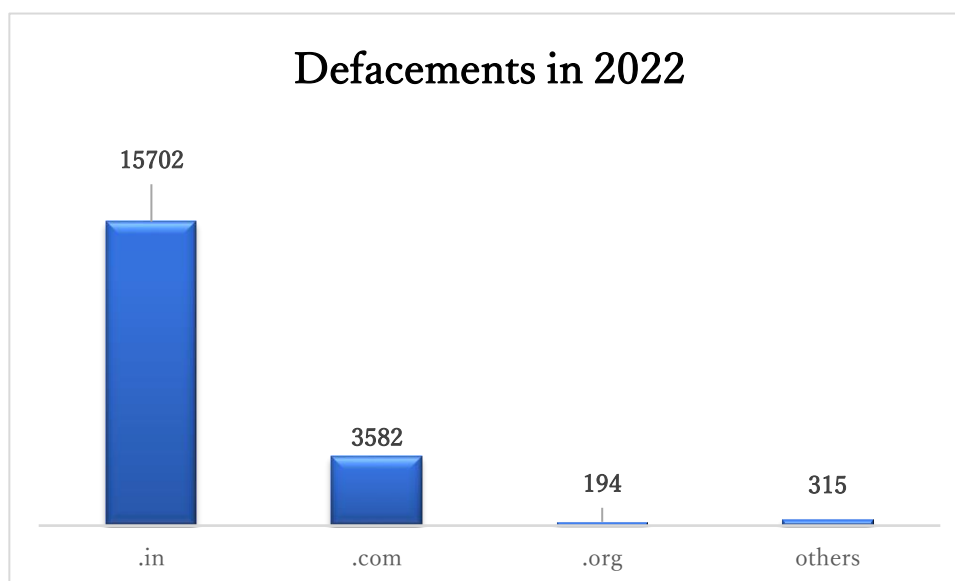


Figure 2: Indian Website Defacements tracked by CERT-In during 2022

3.3.2 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 ~94% 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 Swachhta Pakhwada' from 1-15 February 2022 and 'Special Cyber Swachhta Campaign 2.0' in October 2022, 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 28.04 lakh downloads recorded till December 2022. These FBRTs are available for Microsoft Windows and Google Android platforms.

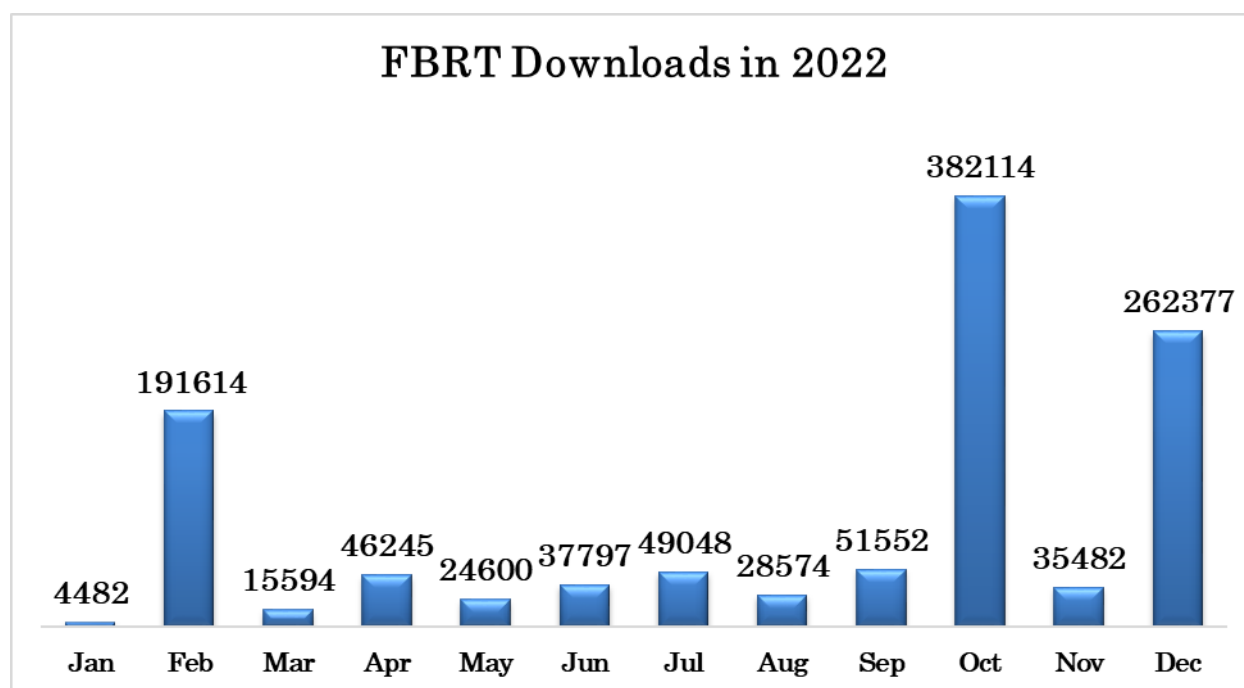


Figure 3: CSK Free botnet removal tools download statistics 2022

CSK also provide following security tools to users via web portal:

- Mobile Security Application – Android platform
- USB Pratirodh – Windows platform
- AppSamvid – Windows platform
- Browser JSGuard – Firefox and Google Chrome browsers

3.3.3 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 empaneled 150 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 empaneled 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 Auditee Organisations to Improve Outcome of Cyber Security Audits and Reducing Threat Exposure to cyber infrastructure.

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 empaneled 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.

3.3.4 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 operationalized 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.

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.

3.3.5 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. Realizing the need, Government has taken steps to 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.

3.3.6 Cyber Forensics

Cyber Forensics Lab 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.

3.3.7 CVE Numbering Authority (CNA)

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.

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.

4. Events organized / hosted

4.1 Training

In order to create security awareness within the Government, Public and Critical Sector organizations, CERT-In regularly conducts trainings / workshops to train officials of Government, critical sector, public sector, industry, financial & banking sector on various contemporary and focused topics of Cyber Security.

In 2022, CERT-In has conducted 23 trainings on various specialized topics of cyber security. A total of 6317 participants including system/Network Administrators, Database Administrators, Application developers, IT Managers, Chief Information Security Officers (CISOs)/ Chief information officers (CIOs), and IT Security professional have been trained. As part of services of CERT-In, for creation of awareness in the area of cyber security as well as training / upgrading the technical knowhow of various stakeholders, CERT-In observed the National Cyber Security Awareness Month (NCSAM) during October 2022 by organizing various events and activities for citizens as well as the technical cyber community in India with a theme of “See Yourself In Cyber”. The total outreach of National Cyber Security Awareness Month October 2022 is 71,16,57,905. CERT-In also observes “Safer Internet Day” on 1st Tuesday of February Month every year and carrying out various activities and awareness campaigns for sensitizing internet users on cyber frauds, crimes and safety measures.

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 9 such cyber security exercises in 2022.

Till 2022, CERT-In has conducted 74 Cyber security exercises of different complexities, including table top exercises, with participation from about 990 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.

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.

In 2022, CERT-In Signed bilateral agreements in the area of cyber security with The National Centre for Information Technology (NCIT), Republic of Maldives and renewed the agreements with Bangladesh Government Computer Incident Response Team (BGD e-Gov CIRT), People's Republic of Bangladesh and Cyber Security Department, Socialist Republic of Viet Nam to enable information sharing and collaboration for incident resolution. 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 an operational member of Asia Pacific Computer Emergency Response Teams (APCERT). CERT-In is the convener of "IoT Security working group" across APCERT to address security threats and evolve best practices to secure IoT devices.

CERT-In is also member of various other working groups under APCERT such as Information sharing working group, Drill working group, Malware Mitigation working group, Tsubame working group and Training Working Group. As a member of APCERT Drill WG, CERT-In has also contributed in APCERT drill 2022 design & execution.

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 became 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 officials attended the 54th Asia Pacific Network Information Centre (APNIC) Conference held in Singapore during 13th to 15th September 2022.
- CERT-In participated in the KISA – 2022 Global Cybersecurity Training Program from 20th to 24th June 2022.
- CERT-In participated in the webinars organized under "APISC Security Training Course" organized by KrCERT/CC of the Korea Internet & Security Agency and Asia Pacific Information Security Conference (APISC) Secretariat.
- CERT-In participated in the APCERT training "APCERT Training: Latest Trends on Keyword Hacks & SEO Spam" on 8th February 2022.
- CERT-In participated in the APCERT training "Cyber Security Incident Reporting and Handling Scheme for Taiwanese Government Agencies" on 12th April 2022.
- CERT-In participated in the APCERT training "FIRST's EPSS Scores for Vulnerabilities" on 7th June 2022.
- CERT-In participated in the APCERT training "Cyber Threat Intelligence on a national level" on 9th August 2022.
- CERT-In participated in the APCERT training "Honeynet Data Analysis through LebahNET" on 6th December 2022.
- CERT-In officials participated in the 301L ICS Cybersecurity Training provided by CISA in Idaho falls USA in June 2022.

5.2.2 International Drills & exercises

CERT-In has conducted 1, contributed in 2 international exercise planning & scenario development and participated as player in 6 International cyber security drills in 2022. Following are the brief of the exercises:

- CERT-In in collaboration with Cyber Security Agency of Singapore successfully designed & conducted the Cyber Security Exercise "Synergy" on 31 August 2022 for 13 Countries as part of the International Counter Ransomware Initiative - Resilience Working Group which is being led by India. The theme of the exercise was "Building Network Resiliency to counter Ransomware Attacks". The exercise scenario was derived from real life cyber incidents, in which a domestic level (limited impact) ransomware incident escalates to a global cyber security crisis.
- CERT-In participated in the APCERT Annual drill 2022 in August 2022 which was conducted with the objective to test the response capability of leading Computer Security Incident Response Teams (CSIRT) within the Asia Pacific economies. The theme of APCERT Drill 2022 was "Data breach through security malpractice". CERT-In also acted as exercise coordinator (EXCON) for international CERTs in the Drill.
- CERT-In participated in CSIRT Commonwealth Cyber Exercise in March 2022. It was a 2-day event simulating a large, wide-spread cyber security incident affecting numerous nations and organisations.
- CERT-In participated in India-UK Ransomware Resilience Exercise in March 2022.
- CERT-In participated in the 2nd Africa Cyber Drill 2022 and played in four scenarios on 08th & 09th September 2022.
- CERT-In participated in ASEAN CERT Incident Drill (ACID) – 2022 in October 2022. The theme of ACID Drill 2022 was 'Dealing with Disruptive Cyber-Attacks Arising from Exploitation of Vulnerabilities'.

5.3 Other international activities

- CERT-In participated in the Financial Stability Board (FSB) Working Group on Cyber Incident Response and Recovery (CIRR) meetings held during 14 – 15 June 2022 at Rome, Italy.
- CERT-In participated in the Forum of Incident Response and Security Teams (FIRST) Annual General Meeting (AGM) and NatCSIRT meetings held at Dublin, Ireland from 27 June to 1 July 2022.
- CERT-In participated in the APCERT AGM held on 18 October 2022
- CERT-In participated in the ICSJWG 2022 Fall Virtual Meeting on September 13 and 14, 2022 organized by CISA.
- CERT-In participated virtually in the Christchurch Call Summit 2022, held on 20 September 2022 in New York, USA.
- CERT-In participated in all the three sessions of the UN Ad-Hoc committee meetings on countering the use of ICTs for criminal purposes.

6. Conclusion

CERT-In is the national agency for incident response in the Indian constituency. 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:
 - +91-11-24368572
 - +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

PGP Key Details:

- User ID: incident@cert-in.org.in
- Key ID: 0xD8F1E992
- Key Type: RSA
- Expires: 2024-12-31
- Key Size: 4096/4096
- Fingerprint: A768 083E 4475 5725 B81AA379 2156 C0C0 B620 D0B4

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: 0x0808076C
- Key Type: RSA
- Expires: 2024-12-31

- Key Size: 4096/4096
- Fingerprint: EABE 086A 6FC4 CB47 3F29 A90B DE30 A071 275C CACF
- Email: csk@cert-in.org.in

PGP Key Details:

- User ID: csk@cert-in.org.in
- Key ID: 0x4EE11788
- Key Type: RSA
- Expires: 2025-05-31
- 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

PGP Key Details:

- User ID: international@cert-in.org.in
- Key ID: 0x4EE11788
- Key Type: RSA
- Expires: 2025-05-31
- Key Size: 4096/4096
- Fingerprint: 0A71 3343 F7E2 A8D7 09FA A71E 9ED3 D110 ECCB 2102

CERT-PH

Philippines National Computer Emergency Response Team

1. Highlights of 2022

1.1 Summary of major activities

- Successfully carried out the online CERT-PH Cyber Incident Drill (CCID) on October 24-26, 2022 with the theme "A Reinforced Cybersecurity: Revamping the Collaborative Competency of Government and Stakeholders in Responding to Threat Incidents". This was participated by participants from various organizations/government agencies and CIs.
- Conducted the online National Cyber Drill (NCD) 2022, with the theme "Building Cybersecurity Allies: Lifting Nation's Cyber Response Capacity and Creating a Digitally Prepared Community". This was the second open to public conduct of (NCD).

1.2 Achievements & milestones

- CERT-PH participated as a resource speaker in the APCERT Conference 2022- Topic: "Inclusion of Incident Response to Digital Transformation Program"
- A series of "Cybersecurity Essentials" trainings were conducted by CERT-PH to various regions around the Philippines.
- First FIRST - CERT-PH has signified its pursuit of becoming an official member of the Forum of Incident Response and Security Team (FIRST) through its first ever in-person attendance at the 34th FIRST annual conference held in Dublin, Ireland
- CERT-PH had the opportunity to participate and attend various international conferences, seminars, and capacity building activities. Involvement in these activities not only cultivated the competencies and skills of CERT-PH personnel but also fostered camaraderie among organizations in the cyber security community.

2. About CERT-PH

2.1 Introduction

The National Computer Emergency Response Team (NCERT) 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 ensures that systematic information gathering, dissemination, coordination, and collaboration among stakeholders are maintained, especially with computer emergency response teams (CERTs), to mitigate security threats and cybersecurity risks that may compromise the confidentiality, integrity, or availability of information. By conducting seminars and events to organizations, CERT-PH provides knowledge and awareness about the threats of cyber-related incidents and the importance of establishing CERTs by replicating the established processes, procedures, and protocols of NCERT, as well as making the necessary improvements and configurations to conform to the needs and requirements of their organization as far as applicable.

2.2 Establishment

CERT-PH was founded and began operations in 2018. The DICT Department Circular 003 issued in March 2020 enhanced the establishment of CERT-PH. NCERT is officially the Philippine National Computer Emergency Response Team (CERT-PH), and it is in charge of leading, administering, and supervising the numerous government, sectoral, and organizational CERTs. CERT-PH also monitors the implementation of the Information Security Incident Response Plan to ensure that cybersecurity incidents and events that are detected and reported receive an appropriate and timely response.

2.3 Resources

CERT-PH now has 22 full-time staff. The operational funding comes from the Department of Information and Communications Technology – Philippines.

2.4 Constituency

CERT-PH's constituency is composed of the National CERT, Government CERTs, and the Sectoral CERTs.

3. Activities & Operations

3.1 Scope and definitions

In order to effectively manage all its Constituency, the CERT-PH consists of four major sections. Their core functions are as follows:

3.1.1 National Security Operations Center Section

- Administers the operations of the Cybersecurity Management System Project (CMSP);
- Conducts regular network monitoring security testing, source code analysis, vulnerability and risk management, and escalation and resolution of cybersecurity-related incidents;
- Monitors the system for possible information security threats and injects countermeasures and remedies.

3.1.2 Incident Response Section

- 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.

3.1.3 Cyber Threat Monitoring Section

- 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 on monitoring and information sharing of cyber security incidents.

3.1.4 Digital Forensics Section

- Conducts Vulnerability Assessment and penetration testing to Government Agencies;
- Provides technical details and analysis of discovered vulnerabilities and criticality to systems owner;
- Examines and evaluates web and network assets to identify security deficiencies.

3.2 Incident handling reports

At the end of December 2022, the National Computer Emergency Response Team (CERT-PH) Incident Response (IR) section was able to handle a total of 1,129 cybersecurity-related incidents. This includes incidents caused by various attack vectors.

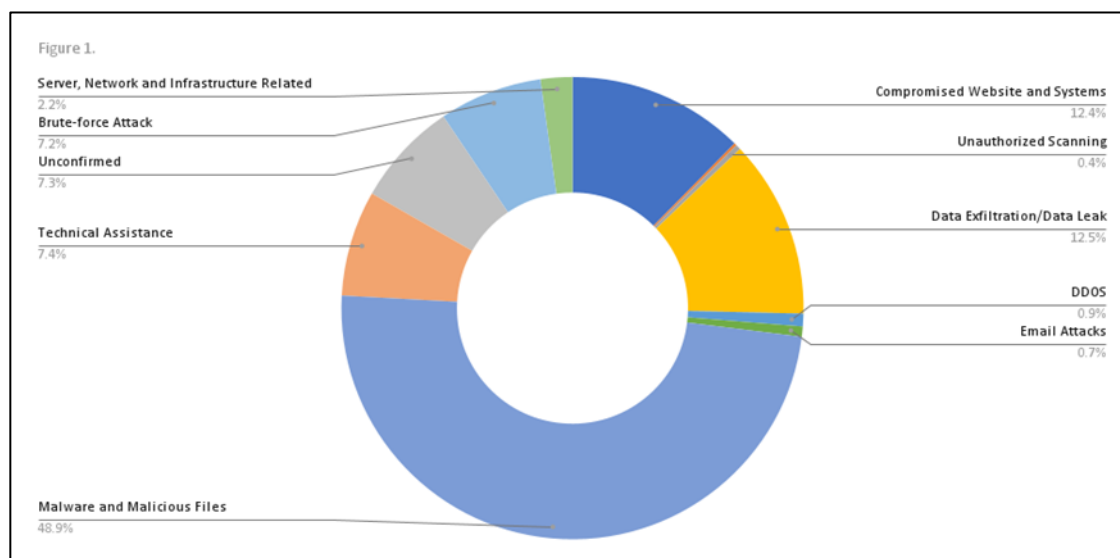


Figure 1. Incidents per Attack Category

This data represents the percentage of all recorded attack vectors that were monitored by CERT-PH during the year 2022. In this year, cases involving malware and malicious files were the most common types of incidents handled.

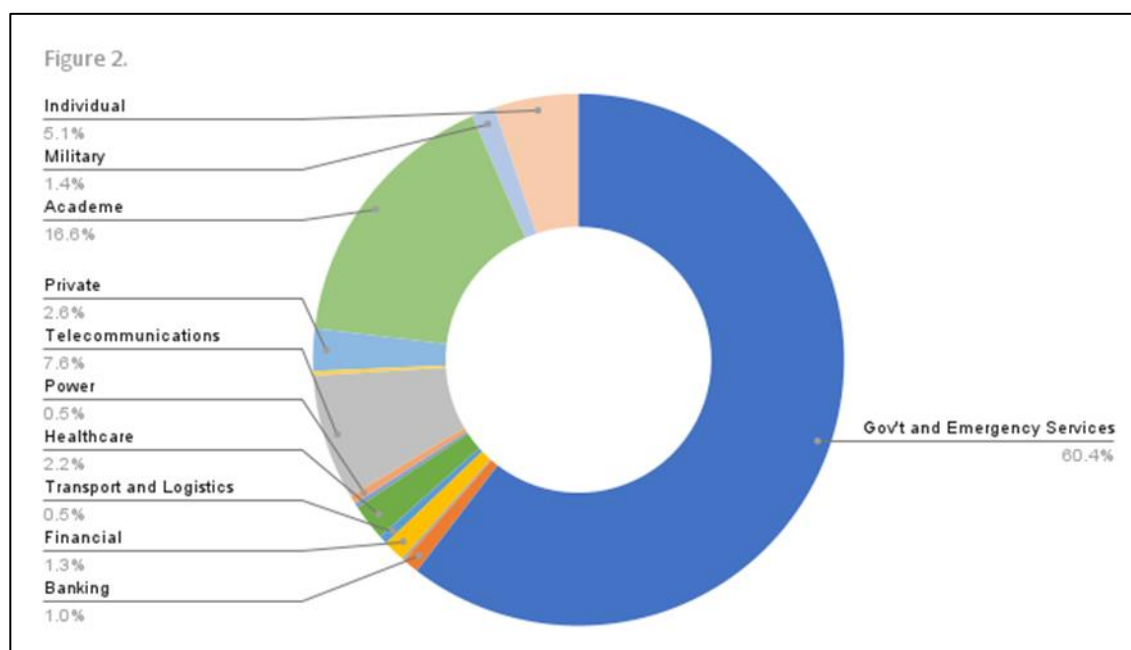
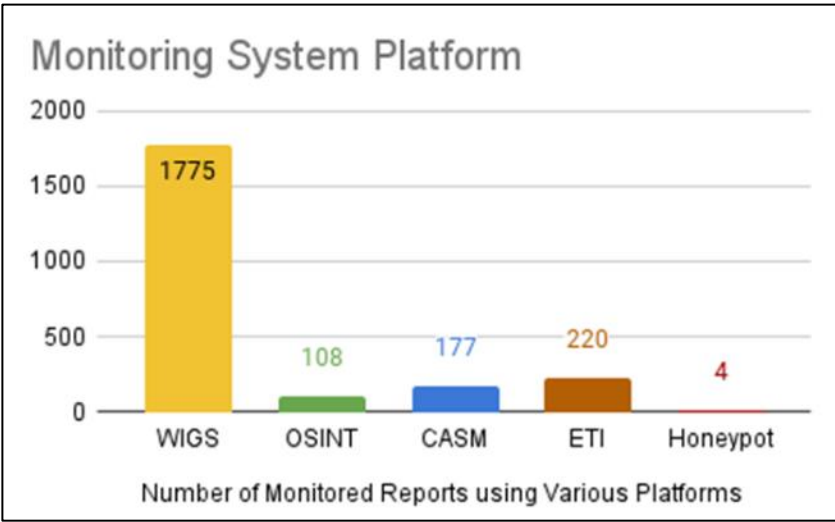


Figure 2. Incidents per Sector

This graph displays the sectoral distribution of all attacks monitored and handled by the CERTPH. As shown in the figure, agencies under the Government and Emergency Services sector have been the most popular target of cyberattacks.

3.3 Cyber Threat Monitoring and Information Sharing

From January to December 2022, a total of 2,284 Monitored Threats were created. CERT-PH through the Web Information Gathering System (WIGS) has monitored 1,775 threats, while the External Threat Intelligence System (ETI) has 220 monitored threats. Those monitored through Open Sources account for 108 monitored threats.



Recently the CERT-PH monitoring team has initiated the operation of its Honeypot monitoring which shows how attackers work and examines different types of threats the reports accounted for was 4. Lastly monitored threats within DICT and attached agencies monitored by the Cyber Attack Surface Management have 177 reports.

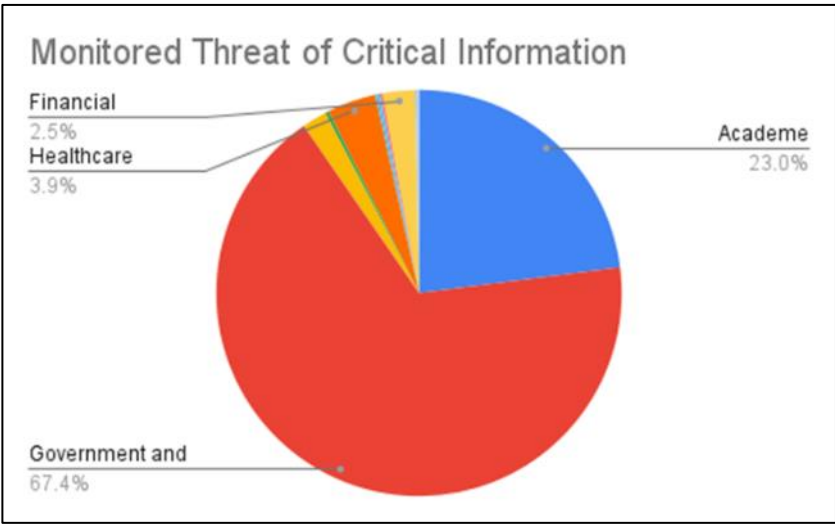


Figure 05. Monitored Threats per Sector

Based on CERT-PH Monitoring Systems the Government and Emergency Services which includes NGAs, LGUs GOCCs, and instrumentalities have a large number of monitored threats which accounted for

67.4%. Various monitored threats reported such as vulnerabilities, malware, alleged data leaks, and website defacement were either reported or escalated to the Incident Response Section.

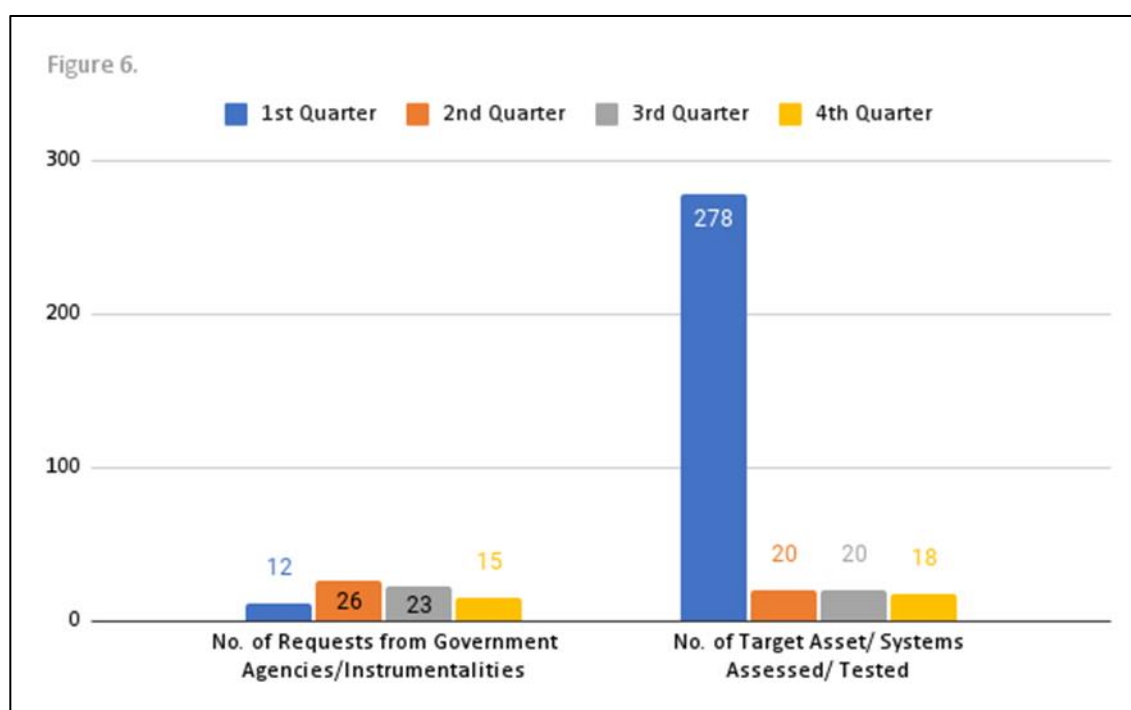
Cyber threat feeds and advisories are issued on a regular basis. Reports and information about the latest cyber threat news, topics, and articles from the web that may impact the Philippine government and cyberspace are gathered and analyzed to provide timely, actionable advice to our stakeholders so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

3.4 Vulnerability Assessment and Penetration Testing

The table below shows the number of requests for assessments or tests from government agencies or instrumentalities during each quarter of the year, as well as the total number of target assets or systems that were assessed or tested. This figure includes the total number of requests and assessments/tests across all four quarters.

	1st Qtr.	2nd Qtr.	3rd Qtr.	4th Qtr.	TOTAL
No. of Requests from Government Agencies/ Instrumentalities	12	26	23	15	76
No. of Target Asset/Systems Assessed/Tested	278	20	20	18	336

For the year 2022 (January-December), the CERT-PH has received and accommodated a total number of 76 requests from different Government Agencies and Instrumentalities.



Of these requests, vulnerability assessment and penetration testing services were conducted to a total of 336 web applications, network and mobile apps to discover any existing attack vectors that could be used by adversaries for potentially compromising the overall security, privacy, and operations of the Government and other Cybersecurity Bureau stakeholders. This also includes proactive engagements with various stakeholders.

4. Events organized/hosted

4.1 Seminars and Resource Speakerships

A total of 15 webinars were conducted by CERT-PH tackling several topics such as Establishing and Operating CERTs, Incident Response, Vulnerability Management, and Threat Monitoring.

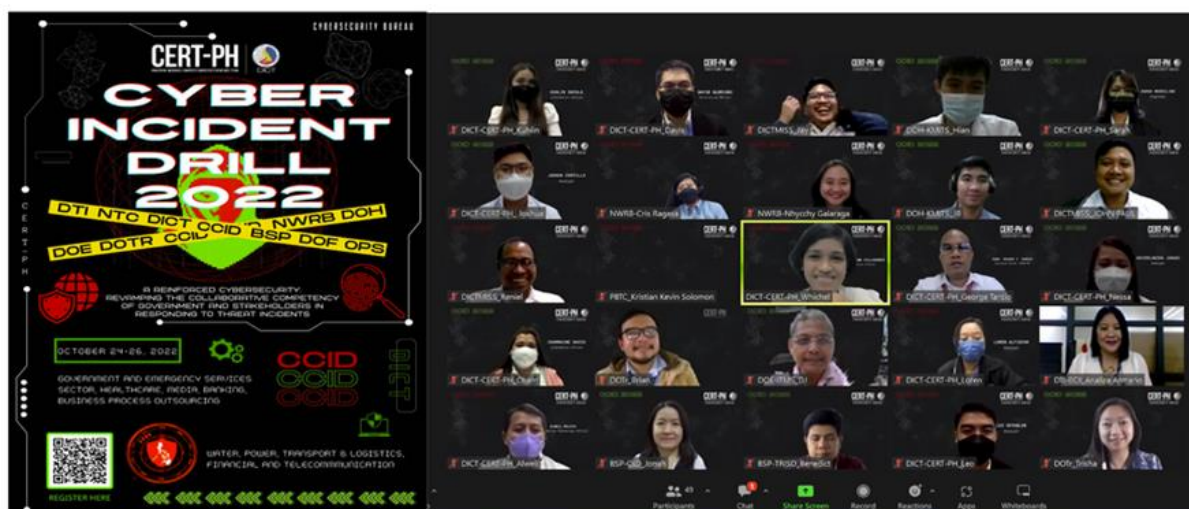
4.2 Drills & exercises

4.2.1 CERT-PH Cyber Incident Drill (CCID) 2022

CERT-PH has successfully conducted its annual CERT-PH Cyber Incident Drill (CCID) anchored on the theme "A Reinforced Cybersecurity: Revamping the Collaborative Competency of Government and Stakeholders in Responding to Threat Incidents" on October 24 - 26, 2022.

The three-day online activity coincides with the observance of National Cybersecurity Awareness Month which principally aims to solidify cybersecurity awareness and instill knowledge and confidence to our stakeholders in recognizing various security threats.

Joined by a total of 41 participants from 11 government agencies and instrumentalities, the CERT-PH has fueled its interest in achieving a wide-ranging and more collaborative involvement of stakeholders composed of the Sectoral Leads as well as the representatives from the Critical Information Infrastructures (CIIs).



Snap/Screen Shot taken during CCID 2022

4.2.2 National Cyber Drill (NCD) 2022

CERT-PH has successfully conducted the National Cyber Drill (NCD) 2022 held last November 28-29, 2022 and participated by representatives from the National Government Agencies (NGAs) and instrumentalities, Local Government Units (LGUs), Academes/ State Universities and Colleges (SUCs), Private sector as well as various entities and individuals of different occupations/ professions across the country. The conduct of NCD is pursuant to the Section 10 of the DICT Department Circular No. 003 series of 2020.



Snap/Screen Shot taken during NCD November 28-29, 2022

Anchored on this year's theme, "Building Cybersecurity Allies: Lifting Nation's Cyber Response Capacity and Creating a Digitally Prepared Community.", the drill is a continuous commitment of the DICT to robust the country's capacity to respond to any cyber-attacks. It has brought together over Six Hundred Twenty Three (623 participants) for the online two-day activity.

The opening day on November 28, 2022 was purposely carried out featuring a Basic Learning Path that is designed and

tailormade for the beginners or entry-level individuals for their optimal familiarity or awareness. A total of Three Hundred Fifty Six (356) participants have been able to embark on the scenario-based video table top platform that the CERT-PH diligently devised to inculcate the relevance of cybersecurity in this day and age.

The second day on November 29, 2022 showcased an Advanced or Extensive Learning Path intended for Intermediate Level and was participated by a total of Two Hundred Sixty Seven (267) individuals. In essence, the platform for this path allowed the participants to apply and exercise their incident handling response, and reporting capabilities through the Capture-the-Flag (CTF) format.

To put forward its persistent commitment in collaborating with the stakeholders, the NCD 2022 has been generally well-accepted by the public with its eye primarily set forth in conducting more interactive cyber drills for the succeeding years and building more cyber allies. This is tantamount to the mutual desire of lifting the nations' cyber response capacity and creating a digitally prepared community in the ensuing years.

4.2.3 Cyber Range

During the first six months of the Cyber Range Platform, CERT-PH was able to host fifteen online self-paced training classes and onboarded 108 learners from thirteen government entities. These trainees utilize video-based learning materials, hands-on labs, cyber ranges, and course assessments.

Additionally, the cyber range platform was utilized for the CERT-PH Cyber Incident Drill 2022, which focuses on traffic analysis and investigation.

5. International Participations

5.1 Conferences and Trainings

Below summarizes the local/ international conferences and training attended by the CERT-PH:

Country/ Region	Organization	Event	Date / Venue
Online	AJCCBC	Exercise for SOC Analysts	February 7-11,2022
Online	CISA	Industrial Control Systems	March 24, 2022
NCR- Makati	UNODC	Ransomware Investigation	May 17 – 19, 2022
Dublin, Ireland	FIRST	FIRST 34th Annual Conference	June 26-July 1, 2022
Online	APCERT	Cyber Threat Intelligence on a National Level	August 09, 2022
Online	Cybersecurity Alliance for Mutual Progress	CAMP 7th Annual Meeting (Virtual)	September 21,2022
Japan	National Center of Incident Readiness and Strategy for Cybersecurity (NISC)	15th ASEAN JAPAN Cybersecurity Policy Meeting	October 04-05, 2022
Seoul, South Korea	CAMP	CAMP 7th Annual Meeting (Seoul)	October 18-20, 2022
Online	APCERT	Annual General Meeting (AGM)	October 18-21, 2022
Online	APCERT	Closed Conference	October 19, 2022
Online	FIRST-APCERT	Regional Symposium	October 20-21, 2022
Online	JP-US-EU	Industrial Control Systems Cybersecurity Week for the Indo-Pacific Region	October 24-28, 2022
Bangkok, Thailand	ASEAN	24th AJCCBC Cybersecurity Technical Training – Incident Response and Malware Analysis	December 19-23, 2022

5.2 Capacity building

5.2.1 Training

Below summarizes the certification trainings gained by CERT-PH personnel:

Organization	Event	Date / Venue
Global ICT	CompTIA Network + Introduction	January 04, 2022
Global ICT	Network+ (batch1)	January 04-February 28, 2022
Trends Academy	Certified Incident Handler	February 16-18,2022
Trends Academy	Certified Ethical Hacker	March 7-11,202
Trends Academy	Cybersecurity Fundamentals Training for DICT	March 14-16,2022
Trends Academy	Computer Hacking Forensic Investigator (CHFI)	March 28-April 1,2022
USAID	Certified Information Systems Security Professional	August 8-12,2022

5.2.2 Drills & Exercises

Below summarizes the international exercises participated by the CERT-PH:

Country/ Region	Organization	Event	Date / Venue
Online	Asia Pacific Computer Emergency Response Team (APCERT)	APCERT Cyber Drill	August 25, 2022
Online	African CERT	Africa CERT Cyber Drill	September 8-9, 2022
Singapore	SingCERT	Singapore International Cyber Week 2022, Singapore Cyber Conquest 2022	October 17-20, 2022
Online	SingCERT	ASEAN CERT Incident Drill (ACID)	October 27, 2022
Online	Organisation of the Islamic Cooperation (OIC)	OIC Cert-Drill	November 07-08,2022

Bangkok, Thailand	AJCCBC	Cyber SEA Game 2022 Annual CTF cyber competition	November 10-11,2022
Online	International Telecommunication Union	ITU ASEAN Cyber Drill	December 5-9,2022

5.2.3 Seminars & presentations

Served as resource speaker to the following:

- OIC-CERT Webinar 2022: "Managing Security Operation Center (SOC) in Government Sector", on July 19, 2022
- APCERT Conference 2022: Inclusion of Incident Response to Digital Transformation Program on October 18-19, 2022

6. Future Plans

6.1 Projects

- Implementation of face-to-face activity for Hack4Gov for the Academe, Cyber Drills and National CERT Conference

6.2 Operation

- The CERT-PH plans to strengthen its frontline services by recommending to the management to transform from a section under Cybersecurity Bureau to a Service under the Philippine's Department of Information and Communications Technology Central Office
- Increase providing the services by recruiting additional members and providing 24/7 services

7. Conclusion

With the easement of the COVID-19 restrictions, CERT-PH pledges to continue to promote the importance of understanding Cybersecurity hygiene practices as well as promoting the incident response readiness of our stakeholders. Delivery of frontline services will be more proactive and aggressive to protect the Philippine National Cyber Space.

Contact Information

- Email Address: cert-ph@dict.gov.ph
- Hotline Number: (+632) 8920-0101 local 2378 (CERT)
- Mobile Number: +639214942917 / +639561542042

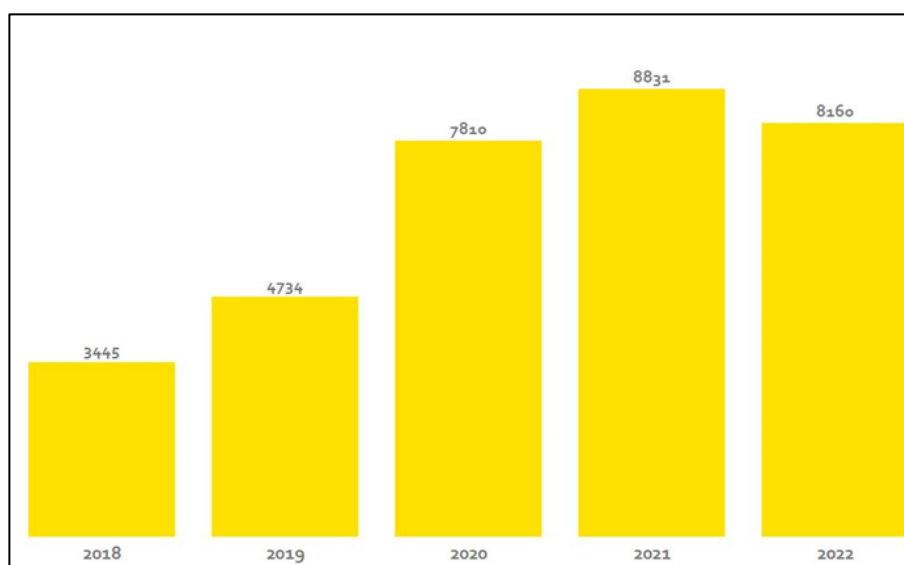
- Facebook: <https://www.facebook.com/Ncertgovph>
- Website: www.ncert.gov.ph

CERT NZ

Computer Emergency Response Team New Zealand

1. Highlights of 2022

In 2022, a total of 8,160 incidents were reported to CERT NZ, a 7.5% decrease on 2021.



- CERT NZ's key annual awareness-raising activity, Cyber Smart Week, was held for the sixth year running, on 10 to 16 October 2022.
- CERT NZ continues to strengthen its partnerships in the Pacific, including chairmanship of the capacity building working group as a member of the Pacific Cybersecurity Operational Network (PaCSON).

2. About CERT NZ

2.1 Introduction

CERT NZ is New Zealand's Computer Emergency Response Team, and works to support businesses, organisations and individuals who are affected (or may be affected) by cyber security incidents. CERT NZ provides trusted and authoritative

information and advice, while also collating a profile of the threat landscape in New Zealand. See www.cert.govt.nz for more information.

Anyone can report a cyber-security incident to CERT NZ, from members of the public, businesses, and government agencies to IT professionals and security personnel. We also receive incident notifications from our international CERT counterparts when they identify affected New Zealand organisations in their investigations.

2.2 Resources

CERT NZ is a branded business unit within the Ministry of Business, Employment and Innovation. It has 36 FTEs, including operations, communications & engagement, governance & analytical reporting staff. CERT NZ also has a contact centre to receive incident reports.

3. Activities & Operations

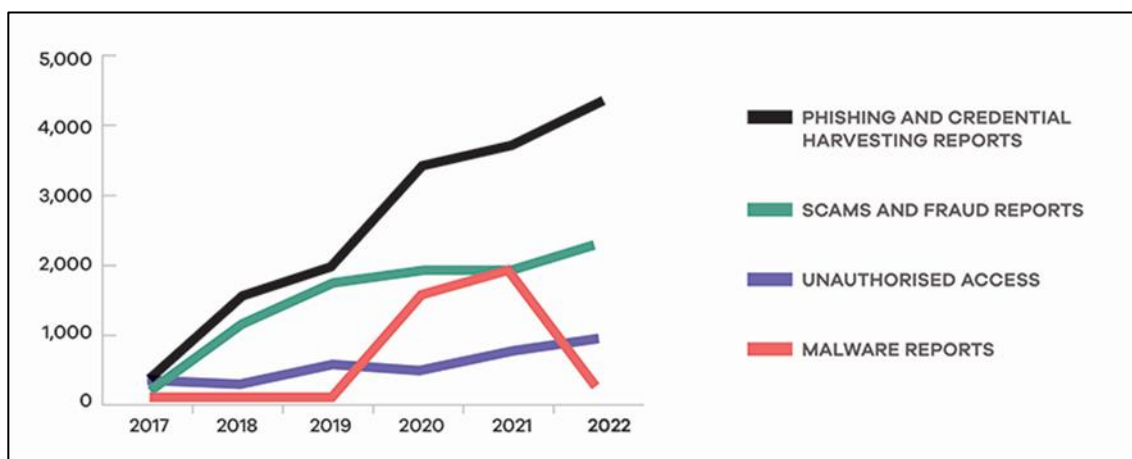
3.1 CERT NZ's key services are:

- Threat identification: We analyse the international cyber security landscape and report on threats.
- Vulnerability identification: We analyse data and report on vulnerabilities in New Zealand.
- Incident reporting: We triage reported incidents and assist businesses, organisations and individuals in getting help and pass some incidents on to appropriate organisations, with the reporter's consent.
- Response coordination: We lead the response to some incidents, coordinate the response to others and we support the national emergency response process.
- Readiness support: We raise awareness of cyber security risks, mitigations and impacts and deliver up-to-date, actionable advice on cyber security best practice.

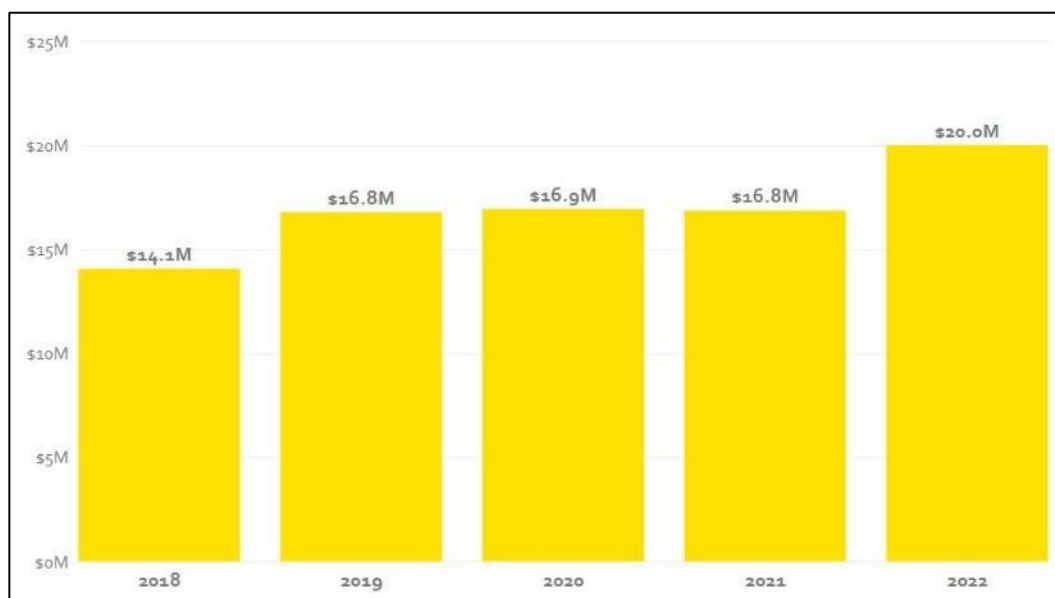
3.2 Top incident categories

'Malware' repots saw a drop in numbers from 2021, with 'Scams and Fraud' continuing their upward trend to be the second most common incident reported to CERT NZ in 2022, with 'Phishing & credential harvesting' remaining the top reported incident.

CERT NZ received 4,315 Phishing and credential harvesting reports in 2022, up 16% on 2021.



Of the reports received by CERT NZ in 2022 22% included a direct financial loss, with a combined total of \$20million.



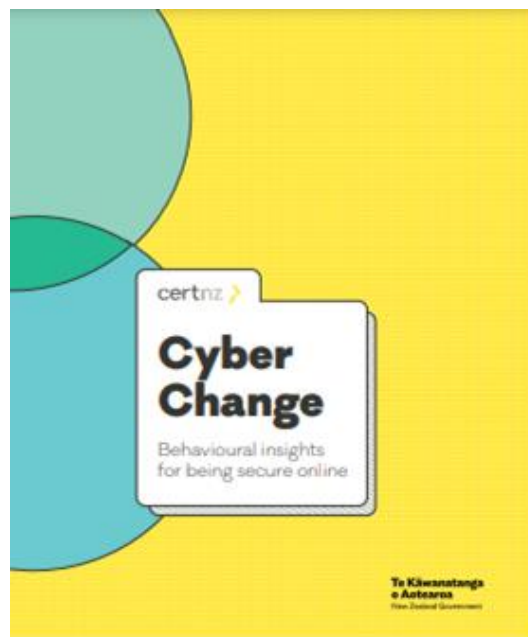
3.3 Publications

CERT NZ's rebranded the quarterly reporting, with the publication of the Cyber Security Insights report:

- Quarterly Report: Highlights document, focusing on selected cyber security incidents and issues
- Quarterly Report: Data Landscape document, providing a standardised set of results and graphs for the quarter.



In 2022 CERT NZ published Cyber security advice and information in eight different languages. CERT NZ also released research and guide on Cyber Change: Behavioural insights for being secure online.



A link can be found below:

<https://www.cert.govt.nz/assets/resources/cert-nz-cyber-change-behavioural-insights-2022-online-version.pdf>

2022 saw CERT NZ continue to publish their critical controls with some alterations. Updated critical controls will again be published in 2023.

3.4 Social Media

CERT NZ has built on their use of social media in 2022 as a way to reach our audience. We continue to run on our existing use of Twitter (@CERTNZ) and Facebook page <https://www.facebook.com/certnzgovt> and CERT NZ LinkedIn page <https://www.linkedin.com/company/certnz/>

4. Events organized / hosted

4.1 Campaigns

CERT NZ ran its sixth cyber security awareness campaign, Cyber Smart Week, in October 2022, which saw a new theme for our infamous robots, a 16-bit gaming theme. CERT NZ engaged with partners from across the government and private sectors to share the four simple steps all New Zealanders could take to be more secure online. During the campaign, CERT NZ worked with over 500 partner organisations, up from 290 in 2021, achieving a combined 13 million impressions. A wide range of resources – from graphics to editorial content – were available for partners to use and share, with the backing of CERT NZ.



CERT NZ ran password focused campaign for the second year running, Big Password Energy with supporting content including videos and posters.



A campaign focusing on 2FA and targeting four different small-business profiles was also launched in 2022, achieving 10 million impressions.



5. International Collaboration

5.1 Capacity building

CERT NZ's Pacific Partnership Programme has established a strong range of capacity building activities since its launch in December 2019.

The programme delivers two primary buckets of activities including business as usual (BAU) collaboration and standalone responsive programming.

The menu of BAU activities includes:

- Information and good practice sharing and development;
- Community development and engagement;
- Formal and informal mentorships activities;
- Direct incident response support;
- Community outreach;
- Contribution to PaCSON, including convenorship of the PaCSON Capacity Building Working Group; and
- Support, advice, and contributions to NZ, regional, and global cyber capacity building.

Responsive programming since January 2022 has included:

- The PaCSON Remote Session Series – with nine sessions for 235 participants in 2022, including one workshop in partnership with APCERT;
- Spearheading the development and delivery of the Cyber Smart Pacific annual regional awareness raising campaign;
- Support for the establishment of SamCERT;
- Trial translation of good practice materials;
- Sharing of CERT NZ Reporting templates; and
- Collaboration with CERT Tonga on a Cybersecurity Workforce Development Program



5.2 Other international activities

Key International engagements:

- APCERT IoT Working group
- PaCSOn AGM
- Business Link Pacific Cybersecurity Seminars
- CyberSafety Pasifika Partnership & Engagement Workshops
- Pacific Internet Governance Forum (PacIGF)
- APT Policy and Regulatory Forum
- GFCE Annual Meeting

6. Contact information

Website: www.cert.govt.nz

Twitter: @CERTNZ

Facebook: <https://www.facebook.com/certnzgovt>

LinkedIn: <https://www.linkedin.com/company/certnz/>

By post:

CERT NZ

PO Box 1473

Wellington 6140

By phone (to report an incident):

In New Zealand, call us on 0800 CERT NZ (0800 2378 69).

- From overseas, call +64 3 966 6295

CERT Tonga

Tonga's Computer Emergency Response Team

1. Highlights of 2022

1.1 Summary of major activities

- Tonga's Computer Emergency Response Team (CERT Tonga) under the Ministry of Meteorology, Energy, Information, Disaster Management, Environment, Communication and Climate Change (MEIDECC) was able to deliver awareness programs in organizations from Government, Private Sectors, Public Enterprises and Secondary schools.
- We continue to respond to incidents that were reported during the period, conducted IT helpdesk for the whole Ministry and handling the repatriation flight for the returning of the Tongan citizenships during lockdown period.

1.2 Achievements & milestones

- CERT Tonga established a memorandum of understanding with a domestic non-governmental organization known as the Tonga Women in ICT (TWICT). This enables us to conduct awareness sessions to secondary schools in October 2022.
- We signed an agreement with the Ministry of Business, Innovation & Employment – CERT NZ of the New Zealand government to a Cybersecurity Workforce Development Program (CWDP) for three (3) years.

2. About CSIRT

2.1 Introduction

CERT Tonga still operates under the Ministry of Meteorology, Energy, Information, Disaster Management, Environment, Communications and Climate Change (MEIDECC) and continue as the national Computer Emergency Response Team for the Kingdom of Tonga. We are engaging with international, domestic, public and private parties, acting within their statutory scope to collect information, knowledge and expertise to help improve understanding of developments, threats,

and trends and help parties to prevent and deal with incidents and make decisions in crisis.

On 24th of August 2022, the new director for CERT Tonga Mr. 'Esau Tupou commenced as the replacement of the former director Mr. Siosaia Vaipuna.

2.2 Establishment

The Government of the Kingdom of Tonga established CERT Tonga on 15th July 2016.

2.3 Resources

CERT Tonga consists of three established staff (Director, Senior Engagement Officer and Security Analyst), two contracted staff under the Cyber Security Workforce Development Program (CWDP) with CERT NZ (Secondment and Internship) plus three staff from the Media Division that they were previously under the Information Department and then transferred to the Prime Minister's Office (PMO) as the Digital Transformation Department and they are responsible for the e-government and Datacentre. The continuous support from handful volunteers from time to time yet existent.

2.4 Constituency

CERT Tonga's constituents are Government Ministries, the Private Sector, and the Public Enterprises as well as NGOs.

3. Activities & Operations

3.1 Scope and definitions

As mandated, CERT Tonga aims to:

- Serve as the Kingdom of Tonga's national point of contact for cyber security 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
- Establish and maintain an incident database
- Identify capacity building programs for staff
- Conduct incident handling
- Digital evidence handling
- Conducting risk analysis

- Provide security consultation and advice
- Research development
- Provide forensic services

3.2 Incident handling reports

During the year CERT has reported to number of incidents including:

- Compromised IP Address
- International Revenue Fraud Services (IRFS)
- Web-defaced
- Malicious activities with IP.

3.3 Publications

CERT Tonga publishes Advisories to assist constituents in resolving common threats and vulnerabilities observed to be exploited in the wild. We are also provided Monthly Security Bulletins of different vulnerabilities seen throughout each month. However, email advisory is sent out to our constituents' mailing list to notify any possible attacks and when it is detected.

We use the social media platforms, such as Facebook and Twitter to share our advisories, security bulletins as well as the security tips.

Additionally, we do have a website that we disseminate information there and for any press release on a specific event for CERT Tonga we used the Government portal.

4. Events organized / hosted

4.1 Trainings

CERT Tonga facilitating awareness trainings to Government ministries, public enterprises and including awareness outreach program to secondary school via the collaboration and coordination with the Tonga Women in ICT.

5. International Collaboration

5.1 International partnerships and agreements

- CERT Tonga became an Operational Member of APCERT and a member of the PaCSON (Pacific Cyber Security Operational Network).
- CERT Tonga continues to work closely with a Trustwave on a project running trainings and building staff's knowledge and capabilities.
- The agreement between CERT Tonga and the Ministry of Business, Innovation & Employment – CERT NZ on the Cyber Security Workforce Development Program
- CERT Tonga continues partnership with GetSafeOnline to provide cyber safety and security tips targeting businesses and individuals.

5.2 Capacity building

5.2.1 Trainings

- CERT Tonga attended online training courses provided by APNIC, remote session for PaCSON community and other online training to enhance the capacity and the capability of the staff.
- Trustwave from Australia also provided online training sessions specifically for CERT Tonga's staff. We also have invited relevant stakeholders to be a part of this trainings and it is the Tonga Police and the National Reserve Bank of Tonga.

5.2.2 Drills and exercises

CERT Tonga also participated in a Drill and exercises hosted by APCERT

5.2.3 Seminars & Presentations

CERT Tonga presented on Monthly Security Bulletins and Advisory online to PaCSON community.

6. Future Plans

6.1 Future projects

CERT Tonga continues managing, collaborating, and implementing the projects with the Trustwave via the support from the Government of Australia and the Cyber Security Workforce Development Program with CERT NZ.

6.2 Future Operation

CERT Tonga looks forward to continuing working with the global community, the Asia Pacific and Pacific region in the battle to ensure internet is a safe and secure space for everyone.

7. Conclusion

CERT Tonga recently joined APCERT and looks forward to maintaining the coordination, collaboration and sharing of information with other members of APCERT.

CERT VU

Computer Emergency Response Team Vanuatu

1. Highlights of 2022

1.1 Summary of major activities

- In 2022 CERTVU responded to around 450 cybersecurity-reported incidents.
- Our cybersecurity awareness campaign covers Radio talkback shows
- Radio talkback shows
- Through social media platforms
- Open-air awareness talks
- Through dissemination of flyers and brochures
- One-to-one awareness sessions with organizations
- Video clips awareness
- Music (Cybersecurity songs)
- Regular rural communities' awareness initiatives
- School's educational awareness talks
- CERTVU continues to strengthen its international and regional collaboration through its efforts in PacSON as the 2022/2023 Chair of the Pacific Cyber Security Operational Network (PaCSON), and Leader for the PaCSON awareness-raising group. Its efforts continue to see the yearly implementation of Cyber Smart Pacific week celebrated through the PaCSON community.

1.2 Achievements & milestones

- Cyber smart Pacific (<https://cert.gov.vu/cybersmart/>).
- The Vanuatu National Cyber Security Strategy of 2030 (<https://cert.gov.vu/index.php/resources/policies-and-strategies>).
- Introduction to the ISO 2001 capacity building program

2. About CSIRT

2.1 Introduction

CERTVU is the Vanuatu National Computer Emergency Response Team, it works to support the Government, Businesses, and Civil society in Vanuatu that are facing cyber security incidents. CERTVU provides trusted advisory information and continues to develop cybersecurity within Vanuatu awareness and capacity-building programs.

2.2 Establishment

CERTVU was established in 2018 within the office of the Government's Chief information officer under the Ministry for the Prime Minister as the Minister for Information and Telecommunication.

2.3 Resources

CERTVU sits within the Office of the Government Chief Information Officer (OGCIO) for the government of Vanuatu and its field with three dedicated staff which man the overall operation from Awareness Raising, Capacity building to Incident Response.

2.4 Constituency

CERTVU is a national cert therefore its serves entire Vanuatu. The Government, the business, and the civil society

3. Activities & Operations

3.1 Scope and definitions

CERTVU is mandated to provide

- Collaborate with the regional and international CERTs
- Vulnerability identifications
- Issuance of security advisories and alerts
- Provide cyber security awareness campaigns
- Conduct incident report handling and incident response coordination
- Cyber readiness through cybersecurity awareness programs

- Continues support to the established cybersecurity collaboration framework
- Identify and implement capacity-building programs nationally
- Provide forensic services to the Vanuatu Police Force

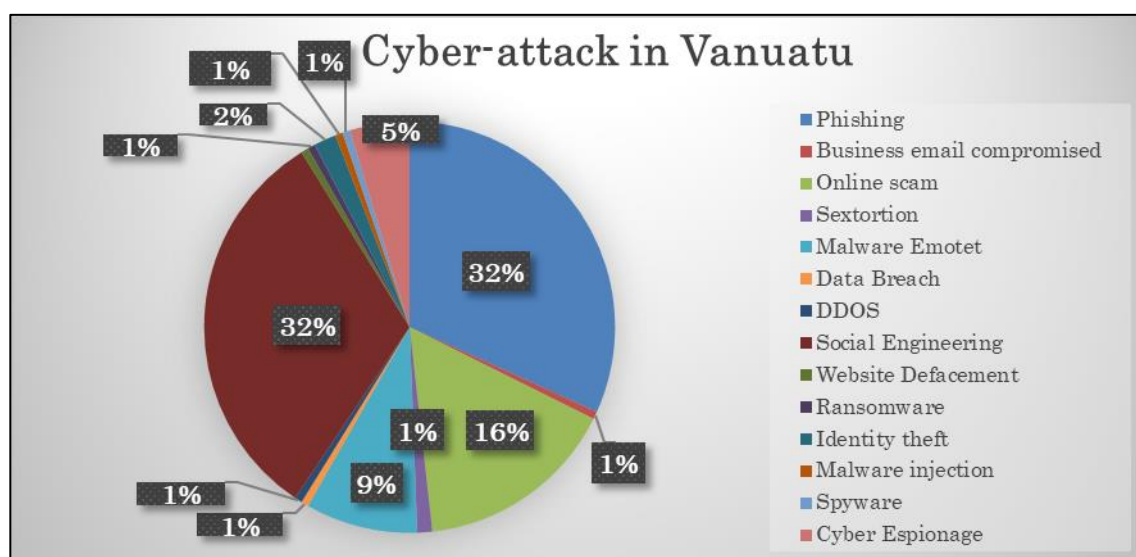
3.2 Incident handling reports

Top five of the cybersecurity incidents reported to the CERTVU

- Phishing and credential harvesting
- Ransomware attack
- Malware attack
- Web defacement
- Online Money scams

3.3 Abuse Statistics

The CERT Vanuatu continues to see similar abuse trends compared to 2018, 2019, 2020, and 2021. Notably, Ransomware Email compromised activities have increased over the last three years. Below is a summary of threats identified.



3.4 Publications

- Publish press release on the 2nd National ISO/IEC 27001 Information Security Management System Standards Capacity Building Workshops.
- Publish Press Release on Vanuatu attending the Cybercrime Conventional Committees' 26th Plenary Meeting at the Council of Europe Hemicycle.

- Publish security advisories on the different cyber threats and Vulnerabilities.

3.5 New services

CERTVU is embarking on the Cybersmart Pacific initiative as in effort to spread meaningful educational awareness throughout the pacific on cyber security.

4. Events organized/hosted

4.1 Training

- CERTVU in collaboration with the Vanuatu Bureau of Standards to deliver workshops on ISO 27001 introductory capacity building
- Joint Cyber Security Training with International Partners on Incident Response and SIEM Implementation.
- Joint Cyber Security Training with International Partners on Critical Infrastructure Security.
- Joint Cyber Security trainings through the PaCSON Capacity Building Programs.

5. International Collaboration

There are continuous collaboration through the PaCSON Platform.

5.1 International partnerships and agreements

- CERT NZ Partnership
- ACSC Partnership
- CERT Tonga Partnership
- AUSCERT Partnership

5.2 Capacity building

5.2.1 Training

- Cybersecurity by the Trustwave LTD
- Continues involvement with the PaCSON Capacity Building Working Group.

5.2.2 Drills & exercises

PaCSO AGM Capacity Building workshop on Emergency Communication (Table Top Exercise.)

5.2.3 Seminars & presentations

- PaCSO AGM Presentation
- PION Annual Workshop Presentaion

5.3 Other international activities

The COVID-19 Pandemic has hindered most of our 2020, 2021 and 2022 International Activities.

6. Future Plans

6.1 Future projects

The CERTVU is committed to continuing to implement the Vanuatu National Cybersecurity Strategy.

7. Conclusion

As a new Member of the APCERT, CERT Vanuatu, through the Government of Vanuatu, continuous its critical operations to ensure its Cyberspace and the Internet is a safe environment for its constituents to dwell, share information and do business to enhance business benefits in Vanuatu.

Cyber Security and the role of a CERT are prioritized in Vanuatu thus enabling Vanuatu to continue to implement and enforce its National Cyber Security Strategy of 2030. With the guiding priorities outlined in the [Vanuatu National Cyber Security Strategy \(NCSS\)](#), empowered by its NCSS Implementation Matrix, Vanuatu continues to respond to Cyber incidents, develop its Cybercrime Act No. 22 of 2021, and operating under a Cyber Security Memorandum of Understanding between CERT Vanuatu, The Vanuatu Police Force (VPF), the Telecommunications Radiocommunications and Broadcasting Regulators' Office (TRBR), Vanuatu Internet Governance Forum (VanIGF) and the Vanuatu Bureau of Standards (VBS). This partnership enables Vanuatu to enforce a multi-stakeholder approach.

Finally, Vanuatu values the need to develop a robust Cyber Security framework. This allows Vanuatu to focus on developing various legal frameworks, namely, the Data Protection and Privacy Policy and Bill (Legislation) and its Harmful Digital Communications Policy and Bill (Legislation).

CNCERT/CC

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

1. Highlights of 2022

1.1 Summary of major activities

2022 has been an exciting and special year for CNCERT/CC in many ways. Looking back, we would like to highlight the work that has been done especially during this year. We successfully hosted several international conferences and seminars, with an effort of enhancing understanding and cooperation among different organizations, such as the Online Conference on CNCERT International Partnership and the Cybersecurity Forum for Technology Development and International Cooperation of Wuzhen Summit. We also organized cross-border online trainings to exchange technical experience. Besides, we actively participated in cybersecurity drills, such as APCERT Drill 2022 and ACID 2022. We have made further collaboration with both global and regional partners. Respectively, the work done in emergency response, cross-border incident handling and other fields has been proceeding.

1.2 Achievements & milestones

In the past year, CNCERT/CC has improved information sharing in the following ways. After the conference call of Information Sharing Working Group last year, two proposals were made. Firstly, use a tag [APCERT Info] in email subject when sharing information with members, making it easier to be recognized by APCERT members and ADE. With supports of APCERT members, now periodic reports all have the tag in the email subject, including ETDA's Cyber Threat Intelligence, CNCERT/CC's weekly report, CyberSecurity Malaysia's Malware Monthly Trend Report, and JPCERT/CC's monthly report. Secondly, add a column in APCERT AccessLine to show the number of reports shared and number of likes received by APCERT members on a quarterly basis.

CNCERT/CC has maintained and promoted the APCERT Data Exchanger platform, with 31 APCERT members having registered and 23 members uploaded PGP keys. Over 730 thousand cyber threat data were shared via this platform in 2022. Meanwhile, CNCERT/CC continues to improve the "Chatroom" and "Feedback" functions in the platform. Now platform users are able to review the content, type, time, etc. of the information shared by APCERT members through

ADE and APCERT mailing lists. And the new functions can provide statistical support for APCERT Membership Awards calculation.

2. About CSIRT

2.1 Introduction

The National Computer Network Emergency Response Technical Team/Coordination Center of China (known as CNCERT/CC) is a non-governmental 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 2001 and became a member of FIRST and one of the founders of APCERT. As of 2022, CNCERT/CC has established "CNCERT/CC International Cooperation Partnership" with 285 teams in 82 countries and regions.

2.3 Resources

CNCERT/CC, which is based in Beijing, the capital of China, has spread branch offices in 31 provinces, autonomous regions, and municipalities in mainland China.

2.4 Constituency

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

3. Activities & Operations

3.1 Scope and definitions

CNCERT/CC coordinates with key network operators, domain name registrars, cybersecurity vendors, academia, civil society, research institutes and other CERTs to jointly handle significant cybersecurity incidents in a systematic way. With an important role in the industry, CNCERT/CC initiated the foundation of Anti Network-Virus Alliance of China (ANVA) and China Cyber Threat Governance Alliance (CCTGA).

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 Publications

During the year of 2022, CNCERT/CC has published weekly, monthly, and annual reports, as well as other released information, which were reprinted and cited by massive authoritative media and thesis at home and abroad.

Title	No. of Issues	Description
CNCERT Weekly Reports (Chinese)	52	Emailed to over 400 organizations and individuals and published on CNCERT's Chinese website (https://www.cert.org.cn/)
CNCERT Weekly Reports (English)	52	Emailed to relevant organizations and individuals and published on CNCERT's English website (https://www.cert.org.cn/publish/english/115/index.html)
CNCERT Monthly Reports (Chinese)	7	Issued to over 400 organizations and individuals on a regular basis and published on CNCERT's Chinese website (https://www.cert.org.cn/)
CNVD Vulnerability Weekly Reports (Chinese)	52	Published on CNCERT's Chinese website (https://www.cert.org.cn/)
Articles Analyzing Cybersecurity Threats	12	Published on journals and magazines

Table 1: Lists of CNCERT's publications throughout 2022

4. Events organized / hosted

4.1 Training

4.1.1 China-Vietnam Network Security Online Training

On 1st March, CNCERT/CC organized China-Vietnam Network Security Online Training, with the aim of implementing the "Initiative on China-ASEAN Network Security On-site Training" approved by China and ASEAN, and facilitating the development of China-ASEAN Information Harbor. During the training, participants exchanged technical experience covering not only such management experience as cybersecurity policy, situational awareness, and incident response, but also phishing incident analysis, critical information infrastructure protection, vulnerability emergency response and management, and threat prevention. VNCERT/CC invited nearly 200 local partners to participate in the training. Through this training, CNCERT/CC and VNCERT/CC have enhanced understanding and deepened mutual trust. VNCERT/CC expressed its willingness to carry out in-depth cooperation with CNCERT/CC in cybersecurity, enhance personnel exchanges, and cooperate in handling cross-border incidents.

4.2 Conferences and seminars

4.2.1 2022 Online Conference on CNCERT International Partnership

On 14th December, 2022 Online Conference on CNCERT International Partnership was held. More than 80 representatives from over 40 organizations at home and abroad attended the conference. On the theme of "Working Together for a Brighter Future in Cybersecurity Cooperation", the conference included two sessions: "Cross-border Collaboration" and "Technical Experience". Guest speakers from CNCERT/CC, aeCERT of UAE, Pakistan Information Security Association, HKCERT, Ministry of Post and Telecommunications of Cambodia, CyberSecurity Malaysia, Asia-Pacific Network Information Center (APNIC) and Kaspersky ICS-CERT exchanged their views on international cooperation of emergency response, regional collaboration experience in cybersecurity incidents, best practices and IOT & industrial cybersecurity.

4.2.2 China-ASEAN Network Security Emergency Response Capacity Building Seminar

On 8th December, the China-ASEAN Network Security Emergency Response Capacity Building Seminar hosted by CNCERT/CC was held online. More than 40 representatives from more than 10 organizations at home and abroad attended the meeting. Representative from CNCERT/CC attended and delivered the welcome speech.

Air Vice Marshal Amorn Chomchoey, Secretary-General of Thailand National Cybersecurity Agency (NCSA) and Mohd Zabri Adil Talib, Acting Head of Cyber Security Responsive Services Division of Cybersecurity Malaysia, delivered the opening remarks on behalf of ASEAN. During the meeting, CNCERT/CC and other representatives from Cyber Security Brunei, Indonesia National Cyber and Crypto Agency, CamCERT, LaoCERT, Malaysian Communications and Multimedia Commission, Malaysia National Cyber Security Agency, mmCERT, Singapore Cyber Security Agency, Thailand NCSA and

VNCERT/CC introduced their national cybersecurity situation, policies and new challenges in the past year.

4.2.3 Sub-forum of Wuzhen Summit of the 9th World Internet Conference: Cybersecurity Forum for Technology Development and International Cooperation

Hosted by CNCERT/CC, the Cybersecurity Forum for Technology Development and International Cooperation of 2022 World Internet Conference Wuzhen Summit was held in Wuzhen, Zhejiang Province on 10th November. Themed on "Promote In-depth Exchange and Cooperation in Securing Cyberspace", the forum was honored by the (tele)presence of world-renowned Internet pioneers, heads of international organizations, senior officials from cybersecurity administration of China and other countries, founders and executives of well-known enterprises who shared their experience and best practices through 3 keynote sessions: "Promote International Cybersecurity Cooperation in an in-depth manner", "Implement Data Governance for Compliance under New Circumstances", and "Jointly Seek Development of New Technologies and Applications in Cybersecurity". Apart from that, one panel was organized for discussions on the latest cybersecurity development trends, policies and strategies, technological opportunities and challenges in pursuit of a peaceful, secure, open, cooperative and orderly cyberspace.

4.2.4 2022 CNCERT Annual Conference in Beijing

On 16th August, CNCERT/CC held the 19th CNCERT Annual Conference in Beijing. Focusing on the theme of "Jointly Safeguarding the Security of Digital Information Infrastructure", the conference invited representatives from government, research institutes and cybersecurity companies to discuss and exchange new trends, hot topics and ideas in cybersecurity, with a view to deepening cooperation in digital security and assuring strong cybersecurity safeguards for the development of digital economy.

5. International Collaboration

5.1 Capacity building

5.1.1 Drills & exercises

- **APCERT Drill 2022**

On 25th August, CNCERT/CC participated in APCERT Drill 2022 and completed it successfully. The theme of this year's APCERT Drill is "Data Breach through Security Malpractice". This exercise reflects real incidents and issues that exist on the Internet. The participants handled a case of ransomware incident triggered by data leakage. 25 CSIRTs from 21 economies of APCERT, as well as 4 CSIRTs from 2 economies of OIC-CERT and AfricaCERT participated in the drill.

- **ASEAN CERT Incident Drill (ACID) 2022**

On 27th October, CNCERT/CC participated in the ASEAN CERT Incident Drill (ACID) 2022. The theme of this drill is "Dealing with Disruptive Cyber-Attacks Arising from Exploitation of Vulnerabilities". The participating teams

investigated, analyzed, reported and recommended remediation and mitigation measures towards cyber incidents. 15 CSIRTS from 10 AMS and 5 key Dialogue Partners participated in the drill.

5.2.2 Seminars & presentations

- **The ASEAN Regional Forum (ARF) Workshop on Countering the Use of ICTs**

The ASEAN Regional Forum (ARF) Workshop on Countering the Use of ICTs for Criminal Purposes was held on 15-16 March 2022 via videoconference, co-chaired by China, Russia, and Thailand. ARF representatives from both the public, private sectors and academia exchanged views on trends, policies and measures to prevent and combat the use of ICTs for criminal purposes as well as best practices and lessons learnt. The Workshop also emphasized the importance of the inclusion of civil society, private sector and academia in advancing cooperation under the ARF Work Plan on Security of and in the Use of ICTs. Representative from CNCERT/CC delivered a presentation on capacity building, and introduced cybersecurity exchanges and cooperation activities of CNCERT/CC.

- **The Second ASEAN-China Cyber Dialogue**

On 19th October, the Second ASEAN-China Cyber Dialogue was held in Singapore. Wang Lei, Coordinator for Cyber Affairs of the Ministry of Foreign Affairs of China, and Kyaw Soe Naing, Ministry of Transport and Communications of Myanmar, co-chaired the Dialogue. Delegates from relevant departments of China, including CNCERT/CC, and all ASEAN Member States attended the Dialogue. All parties had an in-depth exchange of views on general situation in cyberspace, protection of critical infrastructure, policies and mechanism building and pragmatic cooperation. The two sides agreed that under the current circumstance, it's important to strengthen solidarity and collaboration, oppose division, uphold multilateralism, and ensure the peace, security and resilience of cyberspace through dialogue and cooperation.

6. Future Plans

In the coming year, as the convener of Information Sharing Working Group, CNCERT/CC aims to achieve the following outcomes: First, organize teleconferences to facilitate communication between members, and motivate members to share information within APCERT. Second, maintain and update the ADE, add new data types, and continue to improve "Chatroom" and "Feedback" functions according to member's feedback. Third, design and distribute the Third Questionnaire about Information Sharing to all APCERT members, recognize new requirements of members and figure out ways to improve it.

7. Conclusion

There can be no doubt that 2022 was a year of challenge and achievement in the field of cybersecurity. We respond to those difficulties and manage to realize our yearly missions and activities.

As we move forward, we strive to make further contributions to APCERT community, fulfill the role of the Deputy Chair and the convener of Information Sharing Working Group. And most importantly, we will remain united in our commitment to APCERT to fostering a safe, clean, and reliable cyber space.

CyberSecurity Malaysia

CyberSecurity Malaysia

1. Highlights of 2022

1.1. Summary of major activities

21 Feb-3 Mar 2022	Participated in the APRICOT 2022/ APNIC 53 (online)
17 Mar 2022	Organized the Safer Internet Day (SID) 2022: Malaysia Edition in cooperation with the Indonesian National Cyber and Crypto Agency (BSSN), Cyber Security Brunei (CSB), and the Cyber Security Agency of Singapore (CSA) (online)
14-16 Mar 2022	Participated in the World Police Summit Dubai, United Arab Emirates (UAE)
21-23 Mar 2022	Participated in the Gulf Information Expo & Conference (GISEC) 2022 Dubai, UAE
23 Mar 2022	Organized the Cyber Security Dialogue with industry players at the Royale Chulan Hotel Kuala Lumpur, an initiative under the CyberSecurity Malaysia's Cyber Security Collaboration Program (CCP)
23 Mar 2022	Participated in Cyber-Security for Smart City webinar organized by the Malaysia Smart Cities Alliance Association (MSCA) and the Malaysian Industry-Government Group for High Technology (MIGHT) (online)
28 -30 Mar 2022	Participated in the Cybersecurity Innovation Series (CSIS) Conference, Egypt Edition Cairo, Egypt
10 -13 May 2022	Participated in the 21st Annual AusCERT Information Security Conference (online)
26 Jun-1 Jul 2022	Participated 34th FIRST Annual Conference, Dublin Ireland
25 Aug 2022	Participated in the APCERT Cyber Drill "Data Breach through Security Malpractice"
15-16 Sep 2022	Participated in the 4th Cybersecurity Innovation Summit 2022 Tunisia & presented the OIC-CERT 5G Security Framework
18 Oct 2022	Chaired the APCERT Annual General Meeting (AGM) (online)
17-21 Oct 2022	Organized the Cyber Security Malaysia - Awards, Conference & Exhibition (CSM-ACE) 2021 in

	Cyberjaya, Malaysia
7 Nov 2022	Participated in the OIC-CERT Cyber Drill with the theme "The Rapid Evolving of Cyber Threats Landscape in Parallel with Innovation in Cybersecurity Industry"
6-9 Nov 2022	Organized the OIC-CERT 10th General Meeting & 14th Annual Conference 2022 with the theme "Cybersecurity Innovation and Industry Development", Muscat, Sultanate of Oman

2. About CyberSecurity Malaysia

2.1 Introduction

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

i. Cybersecurity Responsive Services

- Security Incident Handling
- Digital Forensics

ii. Cybersecurity Proactive Services

- Security Assurance
- Information Security Certification Body

iii. Capacity Building and Outreach

- Info Security Professional Development
- Outreach

iv. Strategic Studies and Engagement

- Government and International Engagement
- Strategic Research

v. Industry and Research Development

2.2 Establishment

CyberSecurity Malaysia started with the formation of the Malaysian Computer Emergency Response Team (MyCERT) on 13 January 1997 under the Ministry of Science, Technology, and Innovation Malaysia. In 2018, with the restructuring of the government administration, CyberSecurity Malaysia was transferred to the Ministry of Communications and

Multimedia Malaysia which later became the Ministry of Communications and Digital. CyberSecurity Malaysia is committed in providing a broad range of cybersecurity innovation-led services, programs, and initiatives to help reduce the vulnerability of digital systems, and at the same time strengthen Malaysia's self-reliance in the cyberspace

2.3 Cybersecurity Incident Management

CyberSecurity Malaysia managed security incidents through MyCERT, a department within CyberSecurity Malaysia. The agency is a leading point of reference for the Malaysian Internet community when faced with cybersecurity incidents. MyCERT facilitates the mitigation of cyber threats for Malaysia's Internet users particularly on cyber intrusion, identity theft, malware infection, and cyber harassment, among others

MyCERT operates the Cyber999 Cyber Incident Reference Centre and Cyber Threat Research Centre that provide technical support for incident handling, and malware advisories and research, respectively. More information about MyCERT can be found at <https://www.mycert.org.my/>

2.3.1 Cyber999 Cyber Incident Reference Centre

MyCERT operates the Cyber999 Cyber Incident Reference Centre, providing an avenue for Internet users and organisations, to report or escalate cybersecurity incidents that threatens personal or organizational security, safety, or privacy. Channels for reporting cyber abuses and grievances to MyCERT's Cyber999 cyber incidents reference centre are available at MyCERT's website at <https://www.mycert.org.my/portal>

MyCERT's Cyber999 cyber incident reference centre, has responded to 7,292 incidents in 2022 and most being malicious codes and online fraud

2.3.2 Cyber Threat Research Centre

Another valuable service from MyCERT is the malware research with the establishment of the Cyber Threat Research Centre. The centre has been in operation since December 2009 and functions as a research network for analyzing malware and cybersecurity threats. The centre conducts research and development work for mitigating malware threats, producing advisories, monitoring threats, and collaborating with other malware research entities

2.3.3 Constituency

CyberSecurity Malaysia's constituency is the Internet users in Malaysia. Cybersecurity incidents within Malaysia that are reported either by the Malaysian public or international organisations will be resolved by assisting the complainants with technical matters. If an incident involves international cooperation, CyberSecurity Malaysia will request trusted parties in the country or constituency, of which the origin of the case, to assist in resolving the security issues

3. Activities & Operations

3.1. Incident Handling Reports and Abuse Statistics

CyberSecurity Malaysia receives reports from various parties within the constituency such as home users, private sectors, government sectors, and security teams from abroad (foreign CERTs), Special Interest Groups, as well as through the internal proactive monitoring by CyberSecurity Malaysia

CyberSecurity Malaysia through MyCERT had proactively produced 56 advisories and 20 alerts to inform the constituency on issues relating to cybersecurity. The specific list of the advisories, alerts and summary reports can be viewed at <https://www.mycert.org.my/portal/advisories>

Most of the incidents reported were related to fraud and followed by the intrusion. Figure 1 shows the reported incidents managed by MyCERT

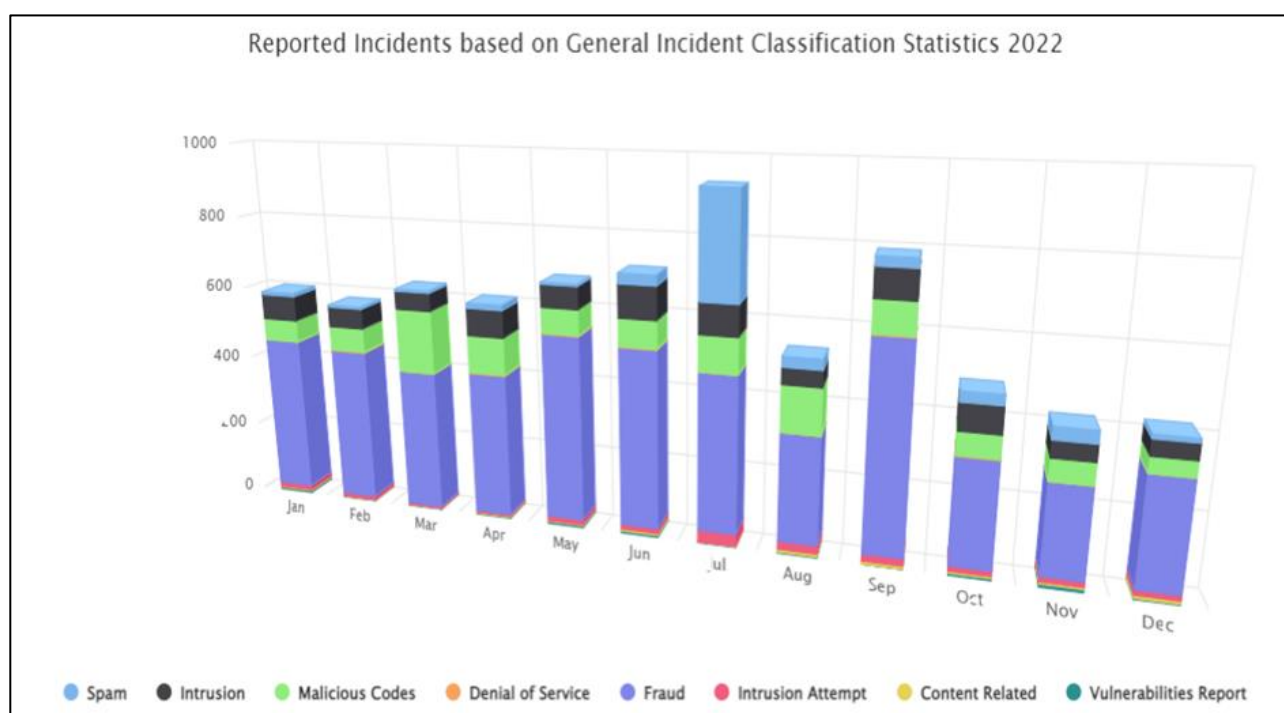


Figure 1 2022 Reported Incident

More information on incidents reported to CyberSecurity Malaysia can be viewed at:

<https://www.mycert.org.my/portal/statistics-2022>

3.2 Cyber Threat Research Centre

The centre operates a distributed research network for analysing malware and cybersecurity threats. The centre had also established collaboration with trusted parties and researchers in sharing threat research information

Other activities by the centre includes

- Conducting research and development work in mitigating malware threats
- Producing advisories on the latest threats
- Threat monitoring via the distributed honeynet project
- Partnership with universities, other CERT's, and international organisations

3.3. The LebahNET Project

LebahNET is a Honeypot Distributed System where a collection of honeypots is used to study the exploits functioned as well as to collect malware binaries. Honeypots are computer software mechanism 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/>

The URLs of the LebahNET project are:

- LebahNET portal at <https://dashboard.honeynet.org.my/dashboard/12/2022>
- Kibana portal at <https://es.honeynet.org.my/> by using guest authentication

Username: guest

Password: guest2021!

4. Events Involvement and Achievements

CyberSecurity Malaysia actively participated in cybersecurity events such as trainings, seminars, conferences, and meetings. Some of the major participations are as follows

4.1 Cyber Drills

CyberSecurity Malaysia, participated in three (3) international cyber drills in 2022 namely the APCERT Drill, ACID Drill, and the OIC-CERT Drill.

4.2 Trainings

Several workshops or hands-on training were conducted by CyberSecurity Malaysia in 2022.

17-20 & 23-26 May 2022	<i>Certified Penetration Tester training and certification under the Malaysian Technical cooperation Programme (MTCP)</i>
14-17 & 20-21 Jun 2022	This training aims to raise awareness and provide exposure to participants on the importance of cybersecurity. In addition, participants sit for the ' <i>Certified Penetration Tester</i> ' examination to obtain professional certification
1 Jul 2022	<i>Cybersecurity & Ethics Webinar</i> : This training provides exposure to the police on digital evidence and cryptocurrency handling procedures while at the same time strengthening cooperation between the two parties
5 Jul 2022	<i>Examination and Analysis of Electronic Evidence Online Training</i> : This training program assess the participants' level of knowledge on various aspects of electronic evidence as well as improve their skills in handling cases related to electronic evidence
3 Aug 2022	<i>Cyber Crime Prosecution Course</i> : This course exposed participants to the prosecution of cybercrime cases in Malaysia, in addition to improving their knowledge and skills on investigation techniques
23-26 & 29-30 Aug 2022	<i>"Digital Security Professional Development & Lifelong Learning Program"</i> under MTCP: A national program focusing on enhancing relevant cybersecurity capabilities for participating countries and provides validation for participants who have demonstrated capabilities in the cybersecurity capacity building through desktop exercises and examination
25 Aug 2022	<i>The Digital Evidence and Cryptocurrency Handling Procedures Course</i> : This training to provide exposure for the police on digital evidence and cryptocurrency handling procedures and strengthen cooperation between the two parties

4.3 Presentations

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

- i. 14 – 16 March 2022 - Dato' Ts. Dr. Haji Amirudin was invited to become a panelist at the forum entitled "Cross-border partnerships to defend the cyberspace: Mitigating next-generation cybercrime through technology and intelligence" at the International Conference World Police Summit for law enforcement and professionals during the Dubai Expo 2020, UAE

- ii. 17 March 2022 - Dato' Ts. Dr. Haji Amirudin became a panellist at the forum entitled "Speed challenges on cyber and the Future of Policing" at the INTERPOL Young Global Police Leaders Program (YGPL) during the Dubai Expo 2020, UAE
- iii. 21 March 2022 – Ts. Mohd Shamir Hashim became a presenter at the opening address at Telecom Cybersecurity Program during GiSEC 2022 Dubai, UAE entitled "the OIC-CERT 5G Security Framework- Building a coordinated effort to harness deep tech for digital transformation"
- iv. 28 – 29 March 2022 - Ts. Mohd Shamir Hashim became a speaker at the Cybersecurity Innovation Series (CSIS) - Egypt Edition, Egypt entitled "the OIC-CERT 5G Security Framework- Building a coordinated effort to harness deep tech for digital transformation"
- v. 16 September 2022 – Ts. Mohd Shamir Hashim became a moderator at the CSIS Tunisia Chapter, Tunisia entitled "Addressing the Shortage in Talent as Cyber Threats Continue to Evolve Rapidly"
- vi. 19 October 2022 - Sharifah Roziah became a speaker at the APCERT Closed Conference 2022 entitled "How Security Incidents are Responded and Handled Across Different National CSIRTs: Findings from an Online Survey"

4.4 Research Papers

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

- i. Mitigating Malware Threats at Small Medium Enterprise (SME) Organisation: A Review and Framework – IEEE
- ii. RENTAKA: A Novel Machine Learning Framework for Crypto-Ransomware Pre-Encryption Detection – IJACSA
- iii. A Proposal in Having a Cyber Resilience Strategy for the Critical National Information Infrastructure Sectors in Malaysia – OIC-CERT
- iv. Incident Response Practices Across National CSIRTs: Results from an Online Survey – OIC-CERT
- v. A Theoretical Comparative Analysis of DNA Techniques Used in DNA Based Cryptography – UMT
- vi. SPA on Modular Multiplication in Rabin-p KEM - MSCR
- vii. How National CSIRTs Operate: Personal Observations and Opinions from MyCERT – IEEE
- viii. GSMA 5G CyberSecurity Knowledgebase & Nesas Whitepaper - Huawei Technologies Malaysia
- ix. Analysis of Permutation Functions for Lightweight Block Cipher Design - Society for Cryptology Research - MSCR
- x. LAO-3D: A Symmetric Lightweight Block Cipher Based on 3D Permutation for Mobile Encryption Application – MDPI
- xi. Statistical Analysis of 3D RECTANGLE Encryption Algorithm - Research World International
- xii. Crypto-Ransomware Early Detection Framework Using Machine Learning Approach – Academia Industry Networks
- xiii. How national CSIRTs leverage public data, OSINT and free tools in operational practices: An empirical study – Henry Stewart Publications

4.5 Social Media

In 2022, CyberSecurity Malaysia received continuous invitations to speak in cybersecurity events at the local radio and television stations. CyberSecurity Malaysia also actively disseminates cybersecurity concerns through social media such as the Facebook and Twitter, which as of now the Facebook Page has about 56,243 followers and the CyberSecurity Malaysia Twitter has 7,638 followers.

5. International Collaboration

The Malaysia Cybersecurity Strategy 2022 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 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. The National Institute for Research and Development in Informatics – ICI Bucharest
- ii. The Association of Information Security Professionals, Singapore
- iii. The Ministry of Information Communication Technology and Postal Services, Republic of South Sudan
- iv. The National Revenue Authority (NRA) Republic of South Sudan
- v. Courtesy visit by EUROCHAM Malaysia
- vi. The Republic of Botswana
- vii. Presidential Advisor of International Relations & Program Coordinator, Somalia
- viii. Cyber Security Brunei

5.2 International Roles

Amongst the international roles and contributions by CyberSecurity Malaysia

- i. The Permanent Secretariat of the Organization 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 members countries
- ii. The lead for the Capacity Building Initiatives in the OIC-CERT
- iii. Co-Lead the OIC-CERT 5G Security Working Group with the objective of developing a security framework to be adopted by OIC member countries

- iv. The Chair of the APCERT
- v. Member of the Forum of Incident Response and Security Teams (FIRST)
- vi. The Convenor for the APCERT Malware Mitigation Working Group – addressing malware infection among Internet users and cyber threat general issues. The main objectives are to provide an overview of the cyber threats landscape by doing collaborative research to mitigate the cyber threats and sharing regular reports or data on malware attacks and focus on the impact analysis and remedial action

6. Future Plans

CyberSecurity Malaysia strives to improve the service capabilities and encourage 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 proactively be intensified

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 Understandings (MoU) and agreements

CyberSecurity Malaysia in conjunction with Aerosea Exhibitions Sdn. Bhd will be organizing an international event known as the Cyber Digital Services, Defence and Security Asia (CyberDSA'23). This event is scheduled to take place from 15 August to 17 August 2023, at the Kuala Lumpur Convention Centre. Held concurrently with this prestigious show are The Cybersecurity Malaysia ACE Awards (CSM-ACE) and Sibersiaga. The CSM-ACE which is an annual event providing awareness, trainings, and awards to information security professionals, and the National ICT Security Discourse to boost the cybersecurity awareness among the youth. At the international arena, CyberSecurity Malaysia as the Permanent Secretariat of the OIC-CERT, continues to spearhead collaborations and organize international events such as the OIC-CERT Annual Conferences and Trainings.

With such understanding, CyberSecurity Malaysia supports newly established local and international CSIRT by providing consultation and assistance especially in becoming members to the international security communities such as the APCERT, FIRST and OIC-CERT.

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 Malaysia Cybersecurity Strategy 2020 that emphasized on 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 an important facet in mitigating other cybersecurity issues. As the cyber

environment does not conform to the physical boundary of the countries, international relations will remain an important initiative. With the rapid development of the internet, the economies are now dependent on public network applications such as online banking, online stock trading, e-business, e-governments, and the protection of the various national information infrastructures. CyberSecurity Malaysia will continue to establish and support cross border collaboration through bilateral or multilateral platforms such as the APCERT and the OIC-CERT and will continuously pursue new cooperation with cybersecurity agencies regionally and globally in the effort to make cyberspace a safer place.

GovCERT.HK

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

1. Highlights of 2022

1.1 Summary of Major Activities

Throughout the year, the Government Computer Emergency Response Team Hong Kong (GovCERT.HK) continued to strengthen the cyber security resilience, promote security awareness and raise the defensive capabilities through the collaboration with different stakeholders.

1.2 Achievements and Milestones

Strengthening Cyber Security Resilience

In 2022, the number of organisations participated in the Partnership Programme for Cyber Security Information Sharing (Cybersec Infohub) have nearly doubled. To enable more effective sharing in the collaborative platform, we implemented a new feature of information sharing between private groups and introduced new threat intelligence (TI) feeds. Furthermore, numerous member events, including meetings, workshops and webinars, were successfully organized so as to build a closer bonding among members from a wide spectrum of industries.

Awareness and Capability Building

We launched the "Build a Secure Cyberspace Promotional Campaign 2022" with the theme "Fact Check After Receiving, Think Twice Before Sharing", held webinars and a contest with Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) and Hong Kong Police Force (HKPF), to raise the public awareness of false information on the Internet. We also organized a series of school visits and security talks for non-governmental organisations (NGOs) to raise their awareness on cyber security and to prevent them from falling prey to cyber pitfalls.

Collaboration with Stakeholders

We actively participated in the Asia Pacific Computer Emergency Response Team (APCERT) activities and worked closely with the Computer Emergency Response Team (CERT) community in handling threat information and coordinating incidents. We also supported our working partners for organizing various events for nurturing cyber security talents,

such as the Capture the Flag (CTF) Challenge 2022 and the Cyber Youth Programme 2022 organized by HKCERT and the Hong Kong Internet Registration Corporation Limited (HKIRC) respectively.

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, 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 organizing activities for public awareness promotion and capability development, with a view to enhancing information and cyber security in the region.

2.2 Establishment

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

2.3 Resources

GovCERT.HK is an establishment under 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 that the government's information infrastructure is well protected.

3. Activities and Operations

3.1 Security News Bulletins

GovCERT.HK published the following security bulletins to raise the awareness among government users and the general public:

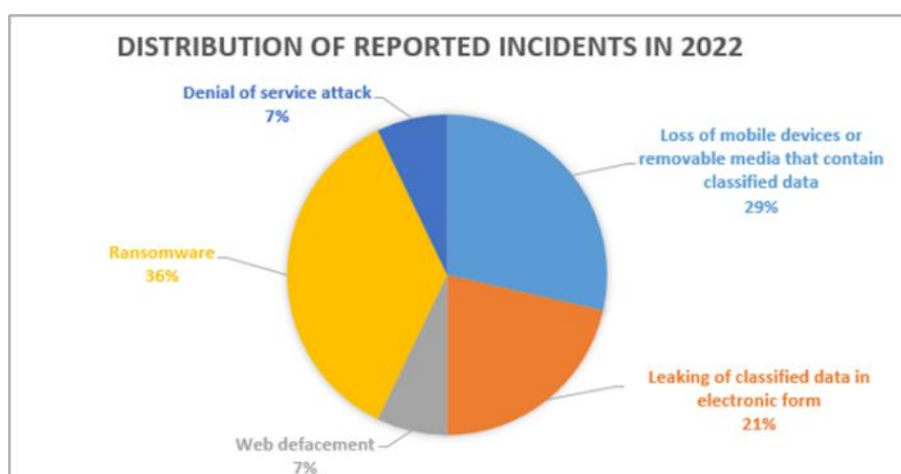
- “Security Vulnerabilities and Patches” to registered subscribers through emails on every working day;
- “Security Industry News” to registered subscribers through emails on every working day; and
- “Weekly IT Security News Bulletins” with summary of security news and product vulnerabilities to registered government subscribers through emails and posted to the GovCERT.HK website as public information.
- (www.govcert.gov.hk/en/secbulletins.html)

3.2 Alerts and Advisories

In 2022, GovCERT.HK issued over 220 security alerts about known security vulnerabilities reported in common products. For those vulnerabilities with higher severity level, we proactively requested government departments to take prompt and appropriate preventive measures against potential information security risks.

3.3 Incident Handling Reports

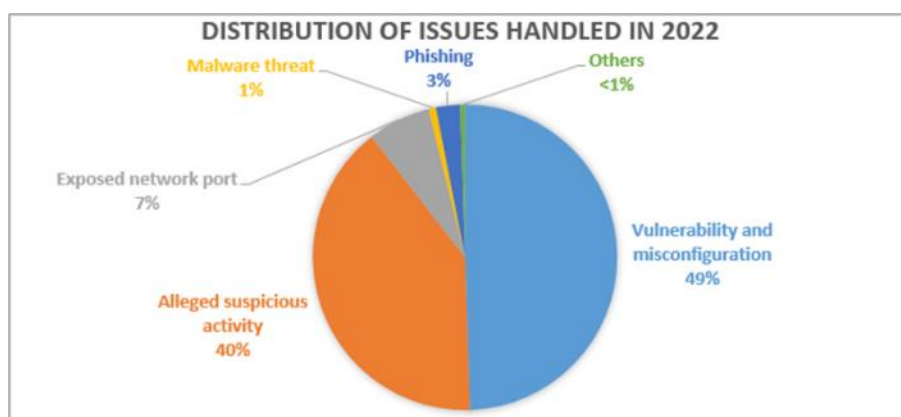
GovCERT.HK handled 14 reported incidents related to government installations, with the incident types shown below:



Relevant statistics on information security incidents in the Government are available on the Government’s Public Sector Information Portal for public access. (www.data.gov.hk/en-data/dataset/hk-ogcio-sec_div_01-information-security-incident)

3.4 Abuse Statistics

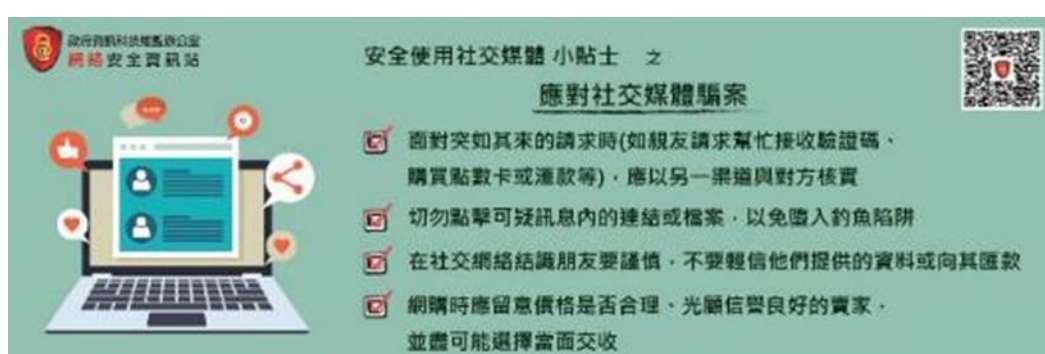
GovCERT.HK assisted government departments to take effective and prompt measures to prevent and reduce the risks and impacts of cyber attacks on their information systems, with the types of security issues shown below:



3.5 Publications and Mass Media

To actively 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” every week, covering a wide range of topics such as phishing attacks, cyberbullying, digital identity, password management, online shopping, using social media and instant messaging, in a lively and interesting way. (www.cybersecurity.hk/en/media.php#Radio)



- We published practical guidelines and infographics with themes such as safe use of social media, firewall setup and cyber security good habits to educate small and medium enterprises and the public to protect themselves against cyber attacks. (www.cybersecurity.hk/en/resources.php)



- We organized "Fact Check after Receiving, Think Twice before Sharing" Folder Design Contest. Many creative designs promoting digital etiquette and proper attitude to protect personal information were received.



Winning Entries



- We published a series of posts on the OGCIO Facebook page, with updates and tips on the latest cyber security topics such as phishing, scams, virtual assets and devices security, to enhance communications with the public. (www.facebook.com/OGCIOHK)



3.6 GovCERT.HK Technology Centre

We continued to operate the GovCERT.HK Technology Centre, which provided relevant facilities and equipment to develop the capability of government staff to tackle evolving cyber threats, identify and remediate from potential security weaknesses in a controlled environment.

4. Events Organized/Hosted

4.1 Training

In 2022, we organized various webinars and training featuring the latest IT security technologies and solutions, as well as the latest cyber security threats and how to deal with them. Some 2,100 government staffs participated in the events with topics such as endpoint security, zero trust security, continuous testing, promotion of various security solutions, and automated vulnerabilities assessment.

4.2 Drills and Exercises

Inter-departmental Cyber Security Drill

GovCERT.HK joined hands with the Cyber Security and Technology Crime Bureau (CSTCB) of HKPF to organize the annual inter-departmental cyber security drills to enhance government department's incident handling capabilities and test their familiarity with the predefined incident response procedures. In 2022, the drill was enhanced with hands-on technical exercises in addition to table-top drills.

Cyber Health Check Exercise

We launched a cyber health check exercise to evaluate the effectiveness of existing security controls and identify potential weaknesses in government Internet-facing systems and mobile applications through a series of technical assessments. The exercise aimed at enhancing the government security posture by adding an extra layer of security verification to government departments' own standing assessment processes.

Anti-Phishing Campaign

We conducted a phishing drill exercise to raise government staff awareness about phishing and improve their capability in defending against phishing attacks.

APCERT Drill

As an Operational Member of the APCERT, GovCERT.HK participated in the APCERT Drill with the theme of "Data Breach through Security Malpractice".

4.3 Conferences and Seminars

Build a Secure Cyberspace Promotional Campaign

A series of promotional activities under the theme "Fact Check after Receiving, Think Twice before Sharing" were organized for businesses, organisations, schools and the public to raise their cyber security awareness and strengthen their cyber security postures. Two webinars were organized in May and September 2022 under the campaign.



School visits and security talks for NGOs

To promote cyber security awareness and cyber etiquette, we organized a total of 24 visits 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

GovCERT.HK continued to partner with the RTHK to produce two online InfoSec Tours with topics of “Internet Etiquette” and “Beware of Email and SMS scams”, which delivered information security message in a relaxing way and equipped the public to be a smart Internet user.



Cybersec Infohub engagement activities

To encourage the engagement and effective discussion among different sectors, various activities such as sector-specific closed group meetings, technical professional workshops and webinars were arranged under the Cybersec Infohub partnership programme with positive responses received.



5. Local and International Collaboration

5.1 Local Collaboration

Promoting Sharing Cyber Security Information and Collaboration

We continued to promote and operate the Cybersec Infohub with HKIRC to promote closer collaboration and build trust among local information security stakeholders. The programme has attracted over 1 420 organisations and more than 2 460 representatives from various local sectors as of the end of 2022.



Nurturing Cyber Security Talents

We continued to support our working partners to organize various programs and campaigns to attract the young generation to develop their professional skills in cyber security and join the information security industry in a long run. GovCERT.HK supported the following events:

- Cyber Security Expo 2022 with the theme on technology application and cyber security by CSTCB
- CTF Challenge 2022 by HKCERT
- Cyber Youth Programme 2022 including certified training courses and game-aided learning platform by HKIRC

Supporting the Small and Medium Enterprises (SMEs)

We also supported our working partners to provide free online training packages and professional advice for SMEs to cope with cyber attacks and minimize the business impacts and financial losses affected by security incidents. GovCERT.HK supported the following initiatives:

- “SME Cyber Security Connection Programme” including engagement with various SME associations and publication of “Incident Response Guidelines for SME” by HKCERT
- “Cybersec Training Hub” with free training resources online by HKIRC

5.2 International Collaboration

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

GovCERT.HK participated in the following events in 2022:

- 2022 China Cybersecurity Week
- APCERT Annual General Meeting and Conference
- APCERT Drill

- APCERT on-line training sessions
- APISC Security Training
- AusCERT Conference
- CNCERT/CC Online Conference for International Partnership
- FIRST Annual Conference

6. Future Plans

GovCERT.HK will optimize its services and raise cyber security awareness of government staff and the general public through various activities:

- Review and streamline its operations appropriately to cope with the increasing security threats of emerging technologies;
- Forge closer ties with local, regional, and international cyber security partners and the CERT community;
- Organize cross-boundary cyber security drills to enable prompt and efficient response to cyber security incidents; and
- Support our partners to organize various programs to promote cyber security awareness and nurture cyber security talents.

7. Conclusion

A secure and stable cyber environment is essential to smart city development. GovCERT.HK has been working closely with government departments and working partners in implementing various measures and projects on all fronts, covering community support, talent development and co-operation with the Mainland of China and international communities, etc. We also collaborate proactively with different stakeholders to jointly enhance the awareness of various sectors on cyber security and their defensive capabilities in this regard. Adopting a multi-pronged approach, GovCERT.HK will continue to strive for maintaining a secure and reliable cyberspace.

HKCERT

Hong Kong Computer Emergency Response Team Coordination Centre

1. Highlights of 2022

1.1 Summary of Major Activities

- Organized the “Build a Secure Cyberspace 2022” campaign with the Government and Hong Kong Police Force.
- Organized the “Hong Kong Cyber Security New Generation Capture the Flag Challenge 2022”.
- Published an Incident Response (IR) Guideline and a one-page infographic for the guideline.
- Organized the “Small and Medium Enterprise (SME) Cyber Security Connection Programme”.
- Launched the Open Threat Intelligence Campaign
- Presented in different international conferences and local press briefing.
- “Year Ender” in local media briefing to call on public to raise awareness of information security
- 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 digital transformation.

1.2 Achievements & Milestones

- Organized the “Build a Secure Cyberspace 2022” campaign with the Government and Hong Kong Police Force. The campaign involved 2 public webinars, a Folder Design Contest and an award presentation ceremony. Over 1,000 participants joined the contest and over 1,200 participants joined the 2 webinars.
- Organized “Hong Kong Cyber Security New Generation Capture the Flag Challenge 2022”. It involved 3 workshops, a 48-hours online contest and a public webinar with award ceremony. 434 teams and more than 1100 participants from universities, secondary schools and security practitioners joined the contest. The contest was the second time expanded to have open group category and international teams invited.
- Published the “Incident Response Guideline for SMEs” and a one-page infographic for the guideline to guide organisations how to deal with common cyber attacks
- Published security advisories on latest phishing and ransomware attacks patterns and emerging cyber threats

- Collaborate with Cybersec infohub to launch the Open Threat Intelligence Campaign and provide automatic integration of threat intelligence feeds by means of machine-to-machine (M2M) sharing
- Continued the Healthcare Cyber Security Programme and Critical Infrastructure Cyber Security Programme. The which covered almost all public and private hospitals of Hong Kong.
- Launched the SME Cyber Security Connection Programme, which engaged 11 organisations from different sectors of SMEs in Hong Kong and organized 9 webinars .The topics of webinars covered the latest cyber security threats and the guideline for incident response.

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), which is a government subverted 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 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 defense 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 and Operations

3.1 Incident Handling

During the period from January to December of 2022, HKCERT had handled 8,393 security incidents which was 9% increase of the previous year (see Figure 1).

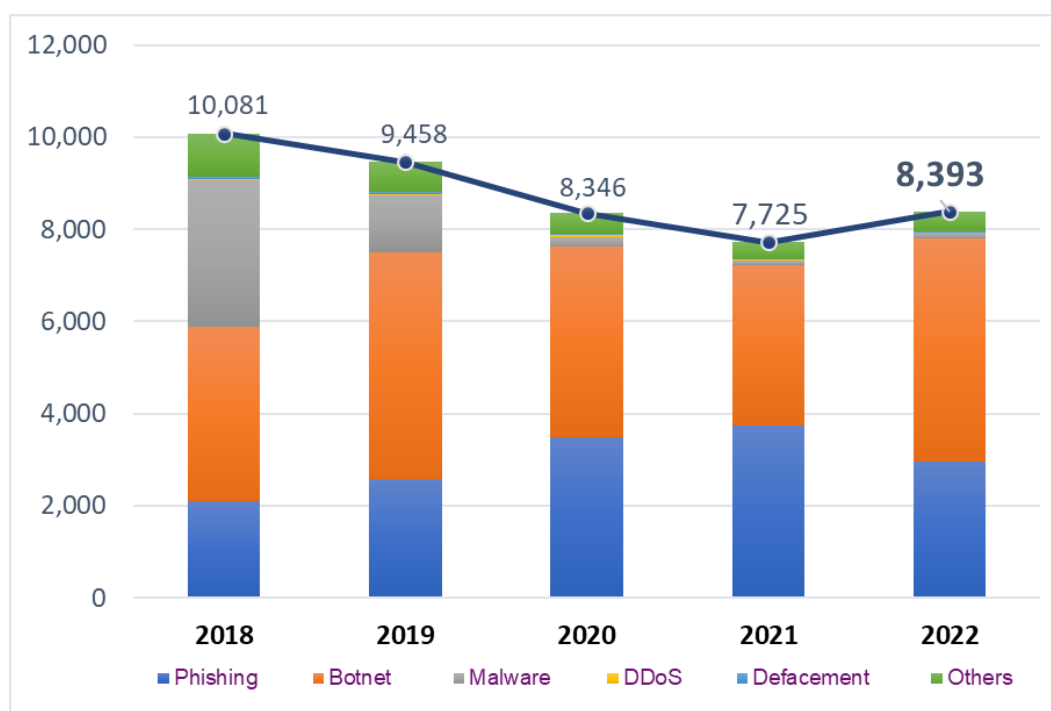


Figure 1. HKCERT Security Incident Reports

While the number of overall security incidents handled by HKCERT reported a rise after three consecutive years of decline since 2018, increasing 9% year-on-year to 8,393 in 2022. Phishing (2,946 cases or 36%) went down 21% but total phishing URLs was increased by 4%. On the other hand, botnets (4,858 cases or 58%), remaining the top source of reported incidents increased 40%. The increase of botnet cases was partly due to cybercriminals abusing a red-team kit, Cobalt Strike, to launch sophisticated attacks.

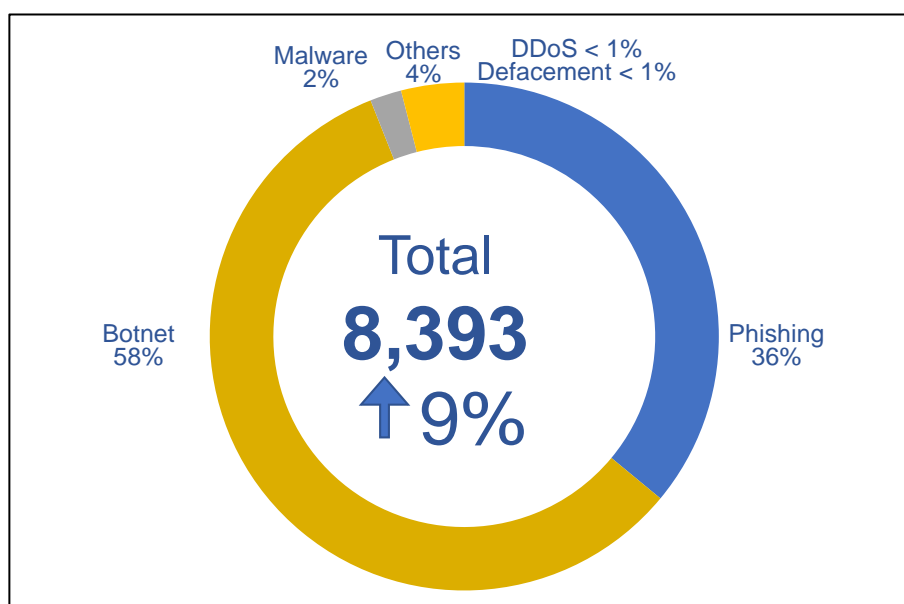


Figure 2. Distribution of Incident Reports

3.2 Watch and Warning

During the period from January to December of 2022, HKCERT published 350 security bulletins for the vulnerabilities of major software (see Figure 3) on the website. In addition, HKCERT have also published 35 security advisories, topics include zero trust architecture, analysis of malware and browser's anti-phishing feature, incident response guideline for SME, security risk of emerging technologies such as NFT, QR Code, artificial intelligence, etc.

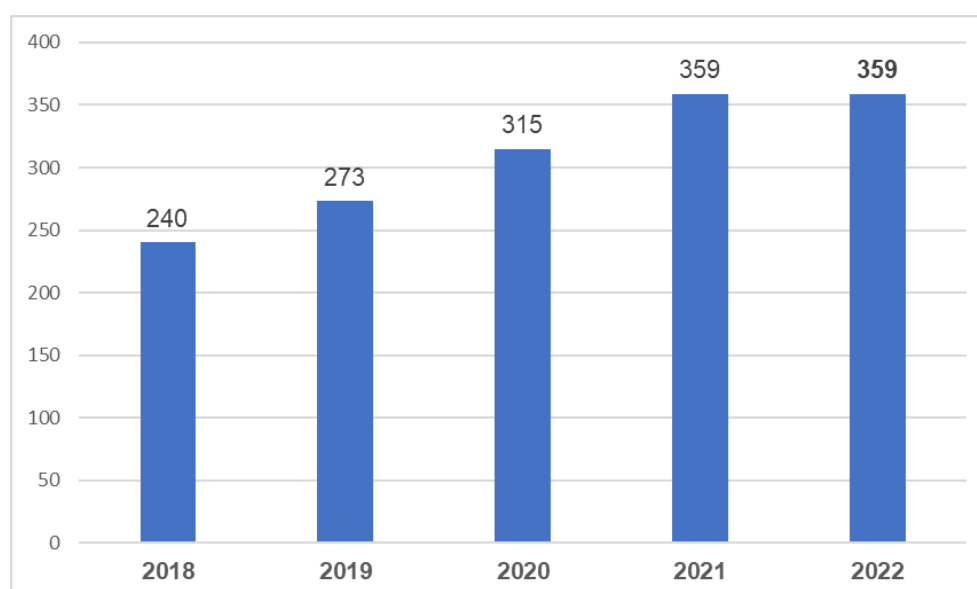


Figure 3. HKCERT Published Security Bulletins

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 reached a high count of 3,684 in 2022 Q3. The major botnet remained as Mirai.

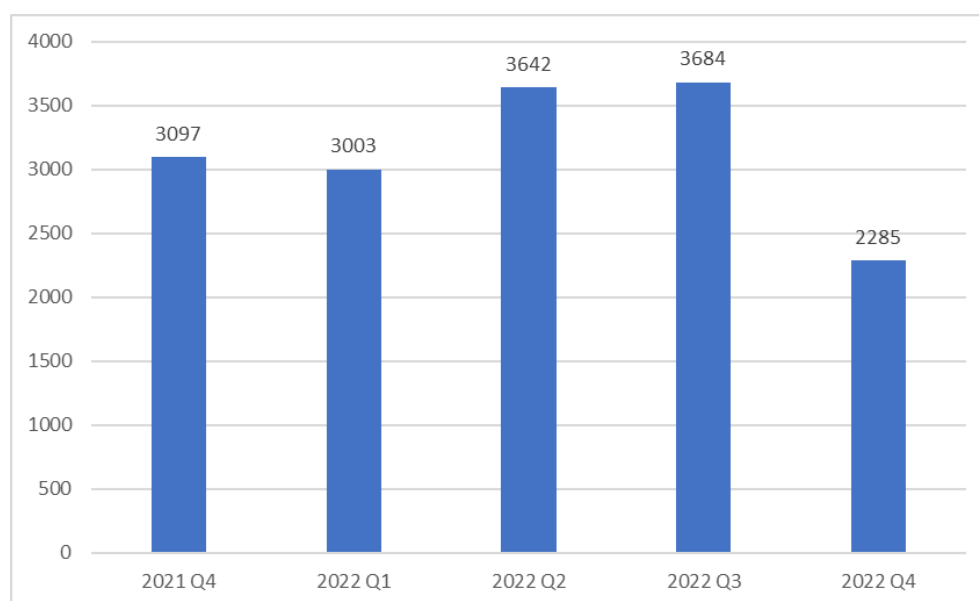


Figure 4. Trend of Bot related security events in the past year

(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 quarter (see Figure 5) (see <https://www.hkcert.org/statistics>).

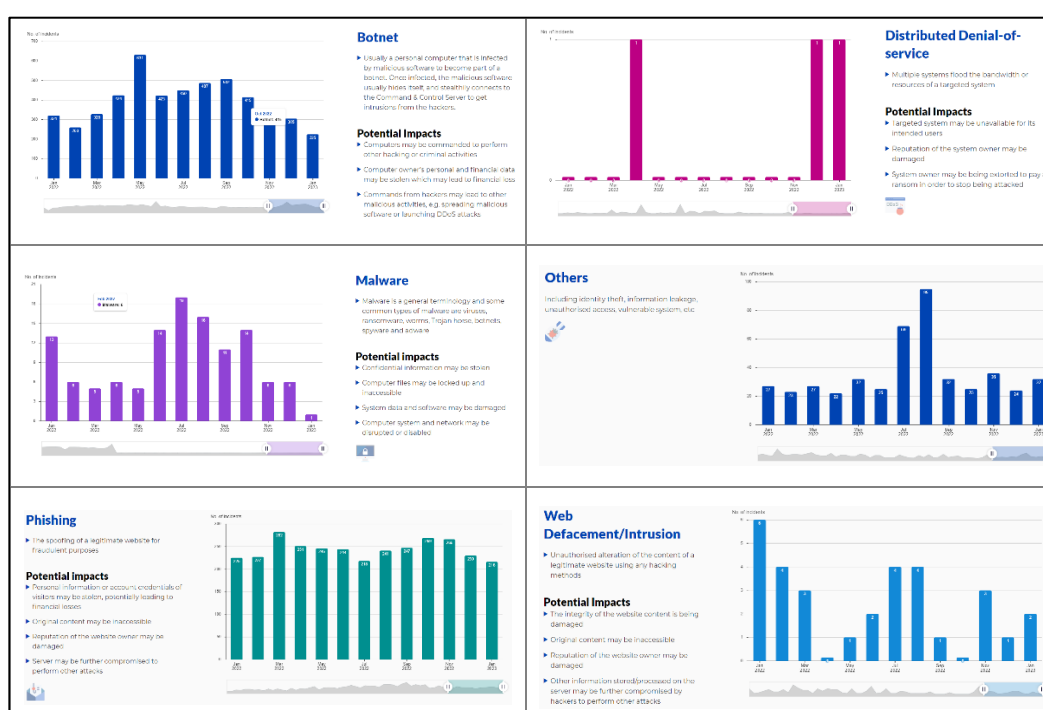


Figure 5. Charts in HKCERT website showing the statistics of different types of incident reports.

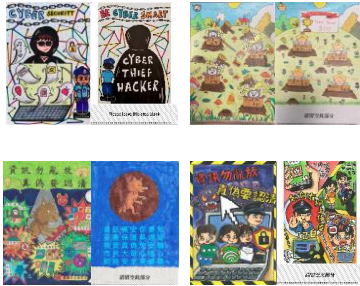
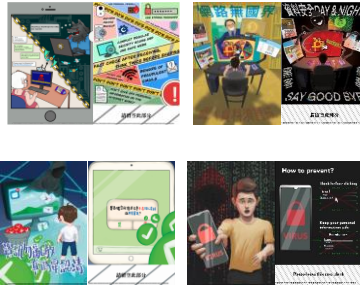
4. Events organized and co-organized

4.1 Build a Secure Cyberspace 2022

HKCERT jointly organized the “Build a Secure Cyberspace 2022” campaign with the Government and Hong Kong Police Force. The campaign involved 2 public webinars, and a Folder Design Contest. An award presentation ceremony was organized in Sep 2022.



For the Folder Design Contest, HKCERT received about more than 1,000 applications from Open Group, Secondary School and Primary School Group. A professional judge panel selected winners with most creative and outstanding design (see Figure 6).

Primary Group Champion	Secondary Group Champion
	

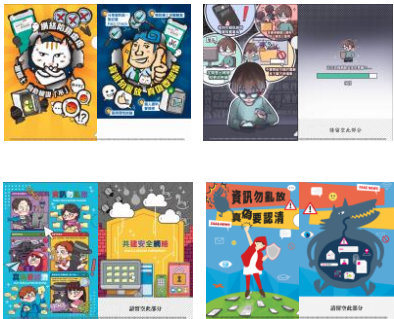
Open Group Champion


Figure 6. Champion entries of Primary School, Secondary School, Open Categories

Use this link to access the winning entries online:

<https://www.cybersecurity.hk/en/contest-2022.php>

4.2 Capture the Flag Contest

HKCERT jointly organized the “Hong Kong Cyber Security New Generation Capture the Flag Challenge 2022” with partner associations in information and education sectors. The 48-hours contest was opened to secondary and tertiary institutions. It was a success with 434 teams and more than 1,100 participants from universities, secondary schools and open categories. This year we also invited 10 teams from overseas countries to compete with local participants. A public webinar with award ceremony was organized in December 2022.



Use this link to access the webinar playback and winning entries online:

- <https://www.hkcert.org/event/hong-kong-cyber-security-new-generation-capture-the-flag-challenge-2022-webinar-and-award-ceremony>

4.3 Small and Medium Enterprise (SME) Cyber Security Connection Programme

HKCERT launched the SME Cyber Security Connection Programme to raise the security awareness of SMEs in Hong Kong, 11 SMEs associations were engaged and 9 webinars were delivered. Topics included the latest cyber security threats and incident response guideline. A discussion session was held to understand the pain point of SMEs on cyber security and explained the services of HKCERT to support their cyber security effort

4.4 Proactive Approach to Promote Awareness for Different Sectors in HK

HKCERT proactively approached several sectors in HK to promote cyber security awareness, e.g. banks, government, retail, manufacturing, SMEs, education, etc.

4.5 Media Promotion, Briefings and Responses

HKCERT attended several media interviews from local media, radio and TV programme to share the cyber security issues and provide security advice on user awareness, phishing, online scam and emerging technologies such as metaverse and NFT. HKCERT issued media messages for security hot topics and generated more than 200 reports of media coverage.

5. Collaboration

5.1 International Collaboration

HKCERT participated in a number of international coordination and collaboration events in year 2022:

- Participated in the NatCSIRT Conference 2022 and presented "HK SME Cyber Security Connection Programme"
- Participated in the OIC-CERT Webinar 2022 and presented "Raise Cyber Security Awareness and Capacity in HK"
- Participated in the HITCON 2022 (Online)
- Participated in the 2022 APCERT Cyber Security Drill Exercise
- Participated in the APCERT AGM and Conference 2022
- Presented "Safeguarding IoT Devices in Digital Age – How HKCERT Adds Values to the Industries"
- CNCERT International Partnership Conference
- Presented "Safeguarding IoT Devices in Digital Age – How CERT can Improve Cyber Readiness"

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 organize joint events regularly.

- HKCERT continued to actively participate in the Cyber Security Information Sharing platform ‘Cybersec Infohub’ which comprised of over 300 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 had held the Advisory Group Meeting in September 2022. The meeting solicited inputs 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 based on this plan to prepare the annual work plan and budget to solicit funding support from the government.

6.3 HKCERT Incident Response Guideline for SMEs

HKCERT had launched the “Incident Response Guideline for SMEs” (<https://www.hkcert.org/security-guideline/incident-response-guideline-for-smes>) in Jul 2022. The guideline covered information of 3 areas to aid user to handle cyber attacks. These 3 areas include (1) Maintain and maximize their systems’ defenses with limited resources, (2) Minimize

business and financial impacts in cyber incidents, and (3) Prevent and minimize the reoccurrence of similar cyber attacks

6.4 HKCERT “Open Threat Intelligence Campaign

HKCERT had launched the Open Threat Intelligence Campaign and used Cybersec infohub as an integrated intelligence sharing platform to provide automatic integration of threat intelligence feeds with organizations’ security systems by means of machine-to-machine (M2M) sharing. The objective is to help organisations enhancing their cyber security defense capabilities by leveraging HKCERT threat intelligence for early identification or proactive blocking of suspicious network activities.

6.5 Analysis of Latest Malware Behavior

HKCERT studied and analyzed the infection vector and malicious behavior of the 2 malware: QBot and AgentTesla. Advisories were published to raise situational awareness of users for the prevention and detection measures.

6.6 Security Guidelines and Advisories for Emerging Cyber Threats

HKCERT published different security guidelines and alerts in response to the emerging cyber threats and incidents happened in other regions, such as vulnerabilities in Apple, Microsoft, remote access device and storage device, protection of sensitive information in social media, NFT, AI, etc.

6.7 Analysis of Browser’s Anti-phishing Feature

HKCERT studied and analyzed the performance of anti-phishing feature of common browsers. The objective is to allow users understand the limitation of technology and emphasis the importance of security awareness against phishing.

6.8 Research on IoT and OT security

HKCERT collaborated with local universities to conduct researches on the security of drone and operation technology. The researches were successful and HKCERT published a video of drone hacking to raise the security awareness of IoT device.

6.9 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.

6.10 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.

6.11 Year Ender Press Briefing

HKCERT organized a year ender press briefing to media in February 2023 to review cyber security landscape of 2022 and provided an outlook to 2023 to warn the public for better awareness and preparedness. It received very good press coverage.



Figure 7. HKCERT at the Year Ender press briefing.

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 2023/2024. We shall work closely with the Government to plan for the future services of HKCERT and seek their support.

7.3 Enhancement Areas

In the coming year, with the increasing trend of phishing attack, HKCERT will launch the “Be Smart, Spot the Phish” campaign. It involves a roving exhibition through booth and vehicle to different regions of Hong Kong and explains how to tackle phishing attack to the citizens of Hong Kong. Also, a themed web page about phishing with preventive measure and latest phishing samples for raising the situational awareness will also be launched as part of the campaign.

HKCERT will continue to organize the Capture the Flag (CTF) contest, HKCERT will continue to partner with different associations to organize another CTF in 2023 for the participants from universities, secondary schools, and open categories.

8. Conclusion

In 2022, the number of overall security incidents reported to HKCERT recorded a rise (9%). Phishing URLs increased by 4% with cyber criminals exploiting the surge of online activities amid pandemics. Botnet also recorded an increase (40%). The increase of botnet cases would be due to cybercriminals abusing to use a red-team kit, Cobalt Strike

In 2023, 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 organize major international seminars and competitions, including the Information Security Summit and the Hong Kong Cyber Security New Generation Capture the Flag Challenge, 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 2023:

- i. Phishing attacks for identity or credential theft: In 2022, phishing attacks were consistently ranked among the top security incidents handled by HKCERT. Credential phishing is a common first step in identity theft by hackers to

obtain sensitive personal information from users. Hackers are also using new techniques to bypass multiple authentication security measures.

- ii. Attacks using artificial intelligence (AI): AI systems have a deeper and wider range of potential cyber security risks than traditional systems. For example, if multiple services use the same AI model, and the model is tampered with by an attack, all services using the model will be affected. Hackers can also use AI to create fake messages, such as images and sounds, to blackmail, create pornographic videos, spread rumors and even bypass biometric authentication to steal people's identities.
- iii. The low cost of cybercrime services will attract more criminals: as the business model for cybercrime changes, cyber attacks have evolved into a service format, significantly lowering the hurdles to launch an attack. Cybercrime services can be very inexpensive, for example, you can buy 1,000 stolen accounts for less than US\$1.
- iv. Web 3.0: The core concept is "decentralization", the most familiar application of which is cryptocurrency and metaverse. 12% of phishing links handled by HKCERT in 2022 involved cryptocurrency. The Hong Kong Monetary Authority has brought virtual currency exchanges under regulation and required virtual asset service providers to obtain a license on 1 June 2023, demonstrating that the security risks of Web 3.0 cannot be ignored.
- v. Widespread application of IoT creates more opportunities for attacks: digitization drives the development of "Industry 4.0", helping enterprises to improve their operational efficiency through smart manufacturing. "Industry 4.0" is one of the key elements of Hong Kong's new industrialization, which integrates IT and operational technology (OT) systems and often applies different IoT devices to connect IT and OT systems to the Internet, increasing the number of entry and exit points or network interfaces, bringing new IS risks and threats.

Id-SIRTII/CC

Indonesia Security Incident Response Team on Internet Infrastructure Coordination Center

1. Highlights of 2022

1.1 Summary of major activities

2022 will be the year of the revival for more active collaboration activities after the Covid-19 pandemic that occurred since the beginning of 2020 made everything go into a vacuum for almost the last three years. Id-SIRTII/CC/NCCA continues to operate normally in full, while continuing to provide services such as notification of security incidents/alerts, making security appeals, consulting, and assisting in responding to cyber incidents. Indonesia was also involved in several face-to-face international programs and collaborations, such as capacity building programs, focus group discussions, cybersecurity policy strategy working groups, and participated for annual activities with international forums.

1.2 Achievements & milestones

NCCA involves a comprehensive set of measures designed to protect the national digital assets, including computer systems, networks, and sensitive data, from various cyber threats. This service includes a range of services such as digital forensic, IT security assessments (ITSA), security monitoring, threat hunting & intelligence, and incident response, to help identify, prevent, and respond to security breaches. Id-SIRTII/CC as well as the National CSIRT is to establish CSIRTs in several government agencies and build communication and coordination mechanisms for established CSIRT.

2. About CSIRT

2.1 Introduction

Id-SIRTII/CC (Indonesia Security Incident Response Team on Internet Infrastructure/Coordination Center) was formed on May 4th, 2007 by the Minister of Communication and Information Decree number no 26 in 2007. Id-SIRTII/CC has a national responsibility in cybersecurity. From the establishment until 2018, Id-SIRTII/CC assumed the function as the

National CSIRT and Coordination Center for national incident handling and works under the Directorate of Telecommunication of the Ministry of Communication and Information. Based on Presidential Decree Number 53 in 2017, Id-SIRTII/CC merged and moved to the National Cyber and Crypto Agency - NCCA (Badan Siber dan Sandi Negara - BSSN).

In April 2018, NCCA officially started carrying the strategic roles as the top-level authority for cybersecurity-related activities in Indonesia. The agency is directly under the purview of the President, which is the merging of Id-SIRTII/CC, Information Security Directorate under Ministry ICT, and the National Crypto Agency (Lembaga Sandi Negara - LSN). In May 2021, based on President Decree Number 28/2021, Id-SIRTII/CC is currently operating under the Directorate of Cyber Security Operation, NCCA.

2.2 Establishment

Id-SIRTII/CC was established on May 4th, 2007, and then merged with National Crypto Agency to develop a new national agency named NCCA, based on the Presidential Decree Number 53 in 2017. Now, NCCA officially started its operation in April 2018. In May 2021, based on President Decree Number 28/2021, Id-SIRTII/CC is currently operating under the Directorate of Cyber Security Operation, NCCA.

2.3 Resources

NCCA, as the new national agency, has several main functions such as detection, monitoring, response and mitigation, cooperation, collaboration, and as the national security operation center, covering the areas of government, Critical Information Infrastructure (CII), digital economy and public. As an active member of the Forum for Incident Response and Security Teams (FIRST), Asia-Pacific Computer Emergency Response Team (APCERT), and also Organization of Islamic Countries Computer Emergency Response Team (OIC-CERT).

2.4 Constituency

Id-SIRTII/CC constituencies are:

- Ministries and Government agencies
- Law enforcement agencies (LEAs)
- National Defense
- CII Operators
- Cybersecurity communities
- Internet Service Providers (ISP)
- Network Access Providers (NAP)
- Local Internet Exchange Operators
- Other Sector CERT / CSIRT in Indonesia¹⁰⁸

3. Activities & Operations

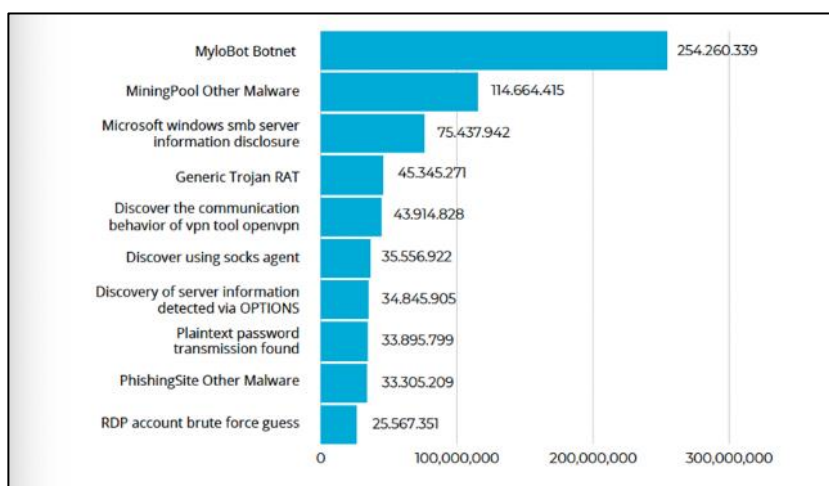
3.1 Scope and definitions

In 2022, Id-SIRTII/CC under Directorate of Cyber Security Operation, NCCA conducted security monitoring activity at national level, and the report can be summarized as follows:

- In 2022, we received 236 cyber security incident report from various sectors. The monitoring and incident response team also delivered 1.433 cyber security notifications. NCCA conducted ITSA to various national stakeholders, and 1.950 vulnerabilities found in 457 assessed electronic system. NCCA also collaborated in Digital Forensics Laboratory service as we processed 406 digital evidences in year 2022.
- As a national CSIRT, NCCA encourage the central and regional government, as well as vital infrastructure sectors to establish their own CSIRT. This CSIRT establishment is mandated in Indonesian Government National Mid-Term Development Program 2020-2024, that at least 121 CSIRT will be established in 2024. NCCA launched 81 sectoral CSIRTs in 2022 and it has exceeded the target figure.
- NCCA recorded 976.429.996 traffic anomalies, which are dominated by MyloBot Botnet. Anomalies traffic that occurs every month in 2022 has decreased, this is indicated due to a decrease in traffic on sensors, a decrease in the number of Indicators of Compromise (IoC), and recommendations sent by BSSN have been followed up by stakeholders and Internet Service Providers (ISP). The graph is shown in the following figure.



Traffic anomaly graph

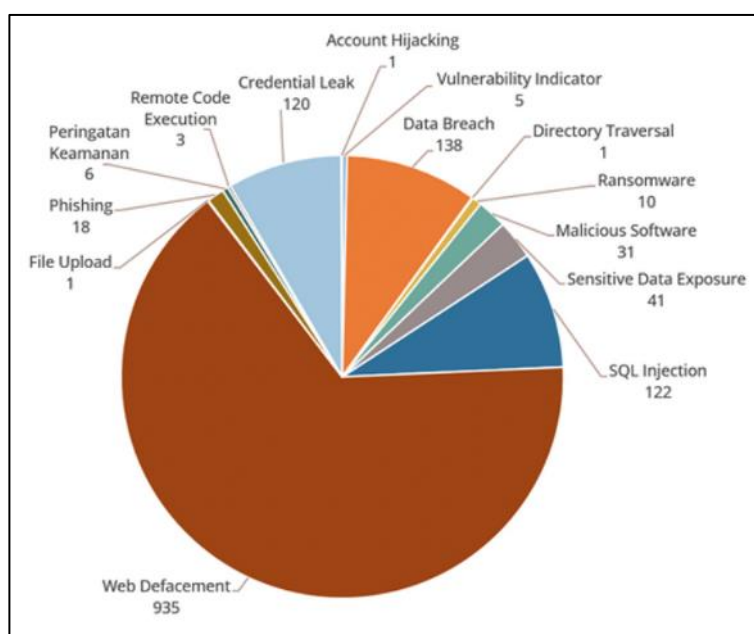


Top 10 traffic anomaly category

- NCCA also received 236 complaint reports in total. Most of the reports came from the government's sector with 108 (45%) reports. This report that received consisted of 13 categories with the 3 highest categories being Misconfiguration (37%), Cybercrime (21%), and Ransomware (15%).

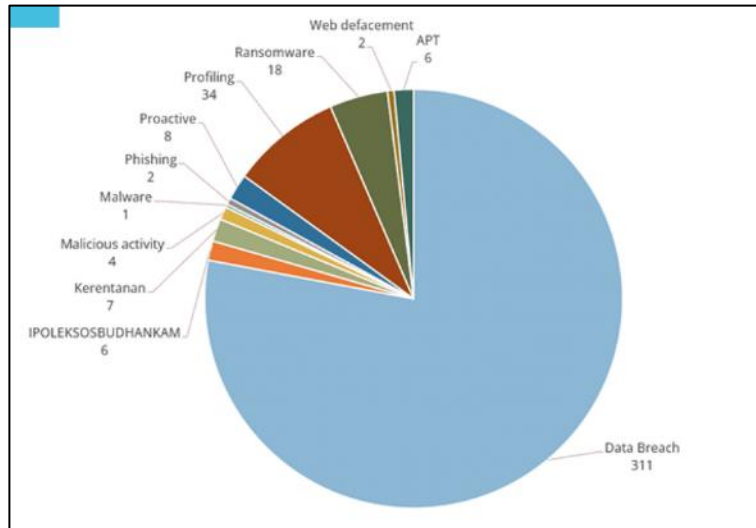
3.2 Incident handling reports

As a National CSIRT, NCCA sends several incident indication notifications to stakeholders who are indicated to be affected. The total incident indication notifications sent during 2022 were 1,435 with 127 notifications being responded and 1,308 notifications not being responded. The following is a graph of the types of notifications sent to stakeholders:



Notification category

- Based on Threat Intelligence conducted by NCCA, there were 399 alleged cyber incidents in the form of data breach, vulnerability, malicious activity, malware, phishing, ransomware, social, web defacement, and APT. The following is a graph of alleged incidents by category:



Category based on Threat Intelligence

3.3 Publications

Every month Id-SIRTII/CC publishes National Monitoring Monthly Report, from January to December in 2022. Id-SIRTII/CC also published its annual report named Cybersecurity Landscape 2022, that's published in Id-SIRTII/CC and BSSN website, published security guidelines, and security advisory.



Id-SIRTII/CC September 2022 monthly report.



Id-SIRTII/CC Cyber Security Landscape 2022



Security Guidelines



Security Advisory

3.4 New services

Currently there is no new services.

4. Events organized/hosted

4.1 Training

As the Deputy Chair of OIC-CERT, Indonesia conducted the OIC-CERT 5th Pillar: Capacity Building, and in 2022 we conducted four online capacity building program

- Conducted a Workshop Network Forensics (With Hands-On)
- Conducted a Workshop on Incident Management for Decision-Makers
- Conducted a Webinar: "Managing SOC in Government Sector"
- Conducted a Webinar: "Promoting Electronic Certificate In Digital Transformation"

4.2 Conferences and seminars

- Conducted a webinar for "Indonesia Cybersecurity Monitoring Annual Report 2021" publishing.

4.3 Events involvement

In national scale, the year 2022 was a special year for Indonesia as the host of G20 Summit in Bali. To support Indonesian Presidency, NCCA took the role in cyber security and protection during the event.



Indonesia also became the host for Inter-Parliamentary Union (IPU) The 144th General Assembly, and NCCA took the responsibility for the cyber security and protection during the event. The other international event conducted in Indonesia was ASEAN Para-Games 2022 as NCCA involved in protecting the cyber security area.

Other than the international events, NCCA also involved in many national events in 2022, such as:

- National Data Protection Task Force
- Indonesian Independence Day in The Presidential Palace
- Annual Session of the People's Consultative Assembly (MPR)
- National Police Recruitment

5. International Collaboration

5.1 Capacity building

5.1.1 Training

- Collaborated with Middlebury Institute of International Studies to conduct training English Communication for Cybersecurity Professional, MIIS, Embassy of US

- Collaborated with Nuffic Neso to conduct training Evidence-based Cybersecurity Policy Making Training Program StuNedTM_25
- Participated in Industrial Control Systems (ICS) 301L and Cyber Security Evaluation Tool (CSET) oleh Embassy of United States of America
- Participated in ILEA Computer and Network Intrusion Course (CNIC)
- Participated in Cyber Bootcamp (National Security College, The Australian National University), Agustus 2022, Jakarta
- Participated in Singapore ASCCE Webinar on "UN Cyber Discussions: A Primer"
- Participated in 24th AJCCBC Cybersecurity Technical Training ASEAN-Japan Cybersecurity Capacity Building Centre, in Bangkok Thailand
- Participated in APCERT Training: HoneyNet Data Analysis Through LebahNET
- Participated in APCERT Training: Cyber Threat Intelligence on a National Level
- Participated in APCERT Training: Cyber Security Incident Reporting and Handling Scheme for Taiwanese Government Agencies

5.1.2 Drills & exercises

- Participated in NISC International Cybersecurity Online Workshop & TTX
- Participated in ITU – UAE "Cyber Protective Shield" Cyber Drill
- Participated in ASEAN-Japan Policy Meeting & TTX, Jepang and Indonesia (Bali, August 2022)
- Participated in Africa-CERT Annual Cyber Security Drill 2022
- Participated in Singapore ACID Drill Test, SINGAPURA in October 2022
- Participated in Arab Drill Test - Saudi Arabia
- Participated in ITU-ASEAN CyberDrill
- Participated in ASEAN-Japan (NISC) Table Top Exercise in Tokyo, Japan
- Participated in APCERT 2022 Cyber Security Drill

5.1.3 Seminars & presentations

- Participated in United Nations Office on Drugs and Crime (UNODC) Bilateral Meeting on Ransomware
- Participated in Singapore Sharing Session on Ransomware
- Participated in China Network Security Conference and Seminar (CNCERT)
- Participated in United Nations Office on Drugs and Crime (UNODC) Bilateral Meeting on Ransomware in Kuala Lumpur, Malaysia
- Participated in FIRST Conference & NatCSIRT Annual Technical Meeting 2022, in Dublin – Ireland
- Participated in OIC-CERT Annual Meeting 2022 in Muscat, Oman

6. Future Plans

6.1 Future projects

In line with the mission in 2022 that establishing regional CSIRT is still one of our main focuses as a National CSIRT. This establishing can make better collaboration and coordination in cyber security will be form. The collaboration covered all sectors, especially the critical infrastructure sector and the government.

Based on the results of the 2022 OIC-CERT Board Election, Indonesia once again holds the role as Deputy Chair of OIC-CERT. We still hold the role of carrying out the Capacity Building pillar, so we plan to hold several more training activities in the form of webinars and workshops.

6.2 Future Operation

- Collaborating with relevant ministries and stakeholders about establishing CSIRT, especially the critical infrastructure sectors.
- On a national scale, Indonesia will hold several international events, and the NCCA will be involved as the security task force in the cyber security area.

7. Conclusion

Id-SIRTII/CC-NCCA will continue to try hard to produce as much as possible in creating safe and good cybersecurity in accordance with APCERT's vision to create a safe, clean, and reliable cyberspace in the Asia Pacific region. One of the steps that will be taken is to improve communication and collaboration with various stakeholders as an effort to create secure cybersecurity.

Office Address

Jl.Harsono RM 70 Ragunan, Pasar Minggu, Jakarta Selatan 12550

URL:

- <https://www.idsirtii.or.id/>
- <https://www.bssn.go.id/>

E-mail:

- info@idsirtii.or.id
- bantuan70@bssn.go.id

Telp. +62 21 780 5814 or +62 21 788 33610

JPCERT/CC

Japan Computer Emergency Response Team / Coordination Center

1. Highlights of 2022

1.1 Summary of major activities

Response to Re-emergence of Emotet Malware Infection

JPCERT/CC has received many reports regarding the infection of the malware Emotet, which has been confirmed to resume its activities. The number of reports has increased in particular since the first week of February 2022. JPCERT/CC published an alert including features and trends on the infection activity. The article was updated 12 times during the year to contain the latest information. In addition, a YouTube video was released to explain the attack vector and the number of infected devices in Japan. JPCERT/CC released v2.3.2 of EmoCheck, an Emotet detection tool for Windows OS on May 27, 2022.

- [Updated] Alert Regarding Re-emergence of Emotet Malware Infection Activities
<https://www.jpcert.or.jp/english/at/2022/at220006.html>
- How to check Emotet infection and respond (Japanese)
<https://www.youtube.com/watch?v=nqxikr1x2ag>

JPCERT/CC Resumes Active International Collaborative Activities with Border Reopening

Since around the end of FY2019, due to the spread of COVID-19 and subsequent travel restrictions imposed by countries around the world, many international conferences and events have been canceled and held only virtually. From around the middle of this year, travel restrictions have gradually been eased, and many international conferences are returning to their pre-COVID form. Japan's border control measures have been relaxed as well, and JPCERT/CC started to resume active exchanges with overseas, such as sending staff overseas to participate in international conferences, and welcoming CSIRT personnel visiting from overseas to hold meetings. For example, our staff members travelled to attend FIRST Conference, BlackHat USA, the Internet Governance Forum, Virus Bulletin etc. to listen to onsite presentations and exchange opinions face-to-face with security experts. JPCERT/CC will continue to further enhance international collaborations.

1.2 Achievements & milestones

JPCERT/CC now oversees 6 CNAs as a Root CNA

JPCERT/CC has been working to streamline the global distribution of vulnerability information as a Common Vulnerability and Exposure (CVE) Numbering Authority (CNA). Following the establishment of a policy to authorize key product developers as CNAs and assign CVE IDs in a more decentralized manner, JPCERT/CC has been supporting the stable operation of the CVE Program as a Root CNA through efforts such as inviting product developers in Japan to become a CNA. The CVE Program welcomes the recent addition of new CNAs from Japan, and JPCERT/CC is pleased to have more partners with which it can address vulnerability information and share values on vulnerability coordination and information distribution. Going forward, JPCERT/CC will continue to focus on the recruitment and development of CNAs. In addition, JPCERT/CC will work to build even more effective distribution channels for vulnerability information through activities geared to the popularization of the CVE Program, such as establishing an implementation system in Japan including localization.

2. About JPCERT/CC

2.1 Introduction & Establishment

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 has been conducting incident handling operations, vulnerability handling operations, engaging in malware and threat analysis, working on control system security, publishing security alerts and advisories to the wide public, organizing forums and seminars to raise awareness of security issues, and supporting the establishment and operations of CSIRTs in Japan and overseas.

2.2 Constituency

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

3. Activities & Operations

3.1 Incident Handling Reports

In 2022, JPCERT/CC received 58,389 computer security incident reports from Japan and overseas.

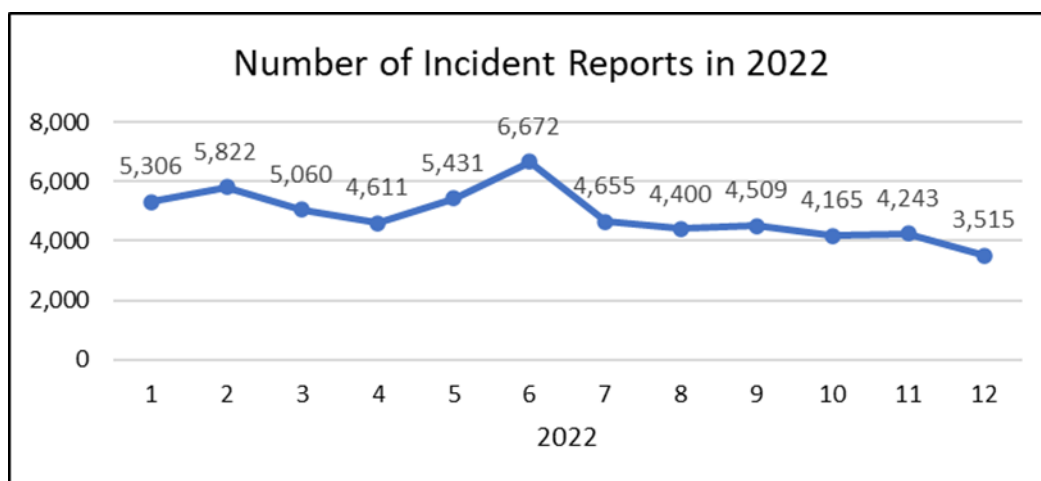


Figure 1. Number of Incident Reports (2022)

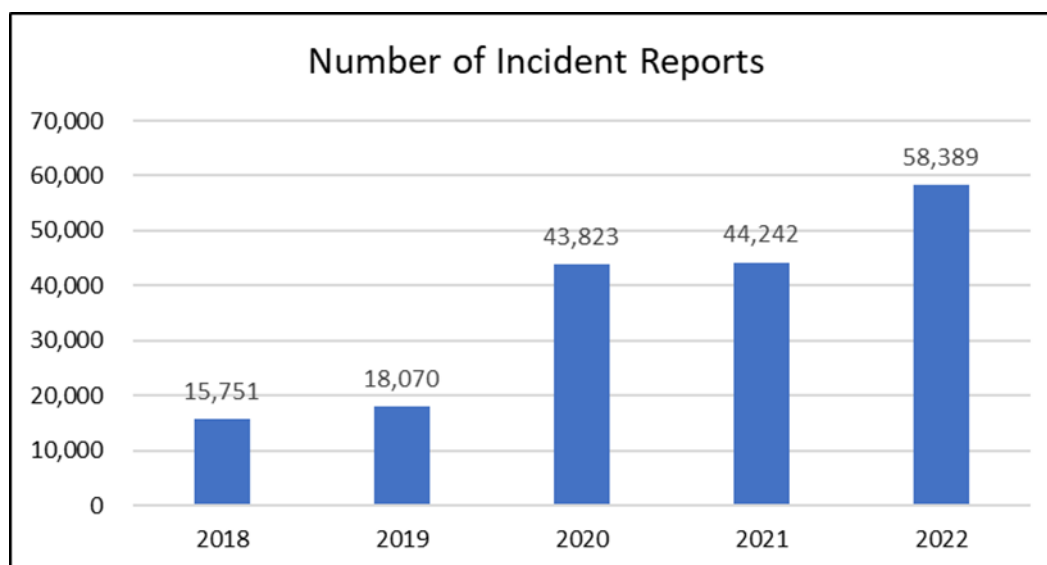


Figure 2. Incident reports to JPCERT/CC (2018-2022)

3.2 Abuse statistics

Incidents reported to JPCERT/CC during the last quarter of 2022 were categorized as in Figure 3. More than 70% of the reports were on phishing site, followed by scan and website defacement.

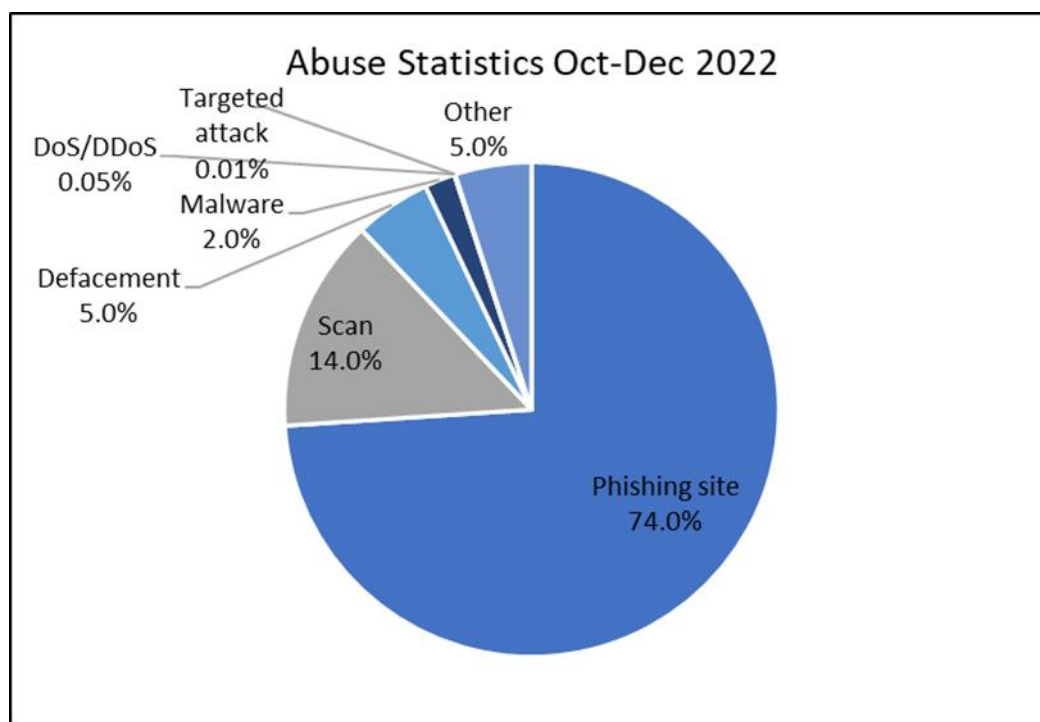


Figure 3. Abuse Statistics of Oct-Dec 2022

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 2022, 48 security alerts were published.

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).

For products that affect a wide range of developers, JPCERT/CC coordinates with CERT/CC, ICS-CERT, CPNI, NCSC-FI and NCSC-NL.

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.

In 2022, 18,094 vulnerabilities coordinated by JPCERT/CC were published on JVN. 8,073 were cases published with IPA through the Information Security Early Warning Partnership, and 10,021 were published through partnerships with overseas coordination centers, developers, researchers, etc.

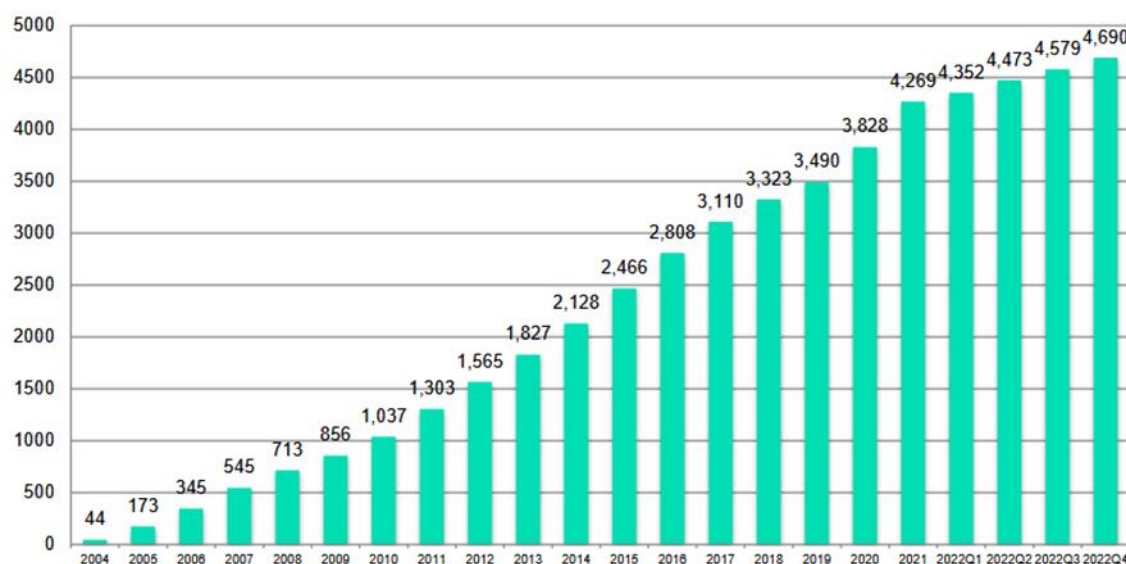


Figure 4. Number of vulnerabilities published on JVN by year

In June 2010, JPCERT/CC became a CVE Numbering Authority (CNA). Since then, JPCERT/CC has been releasing Japan Vulnerability Notes (JVN) and JVN iPedia entries that contain reserved CVE Identifier numbers.

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

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

JPCERT/CC 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 Official Blog

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

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

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.

JPCERT/CC on Twitter

https://twitter.com/jpcert_en

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

JPCERT/CC GitHub

<https://github.com/JPCERTCC>

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

3.4 Services

Industrial Control System Security

Since 2008, JPCERT/CC has been working on awareness raising of industrial control system (ICS) security in Japan, and since January 2013, JPCERT/CC's incident handling service was extended to cover the ICS area. JPCERT/CC has provided presentations at seminars and has supported cyber incident exercises for engineers of Japanese asset owners. Furthermore, JPCERT/CC released an ICS security assessment tool "J-CLICS", developed in collaboration with experts from ICS vendors and asset owners. The tool has been translated into English and published on JPCERT/CC's website.

<https://www.jpcert.or.jp/english/cs/jclics.html>

TSUBAME (Internet Threat Monitoring Data Sharing Project)

<https://www.apcert.org/about/structure/tsubame-wg/index.html>

The TSUBAME project is designed to collect, share and analyse Internet traffic data, in order to better understand the Internet threats mainly in the Asia Pacific region. It deploys sensors widely in the region, collecting and sharing the data with all participating teams. The TSUBAME project aims to establish a common platform to promote collaboration among CSIRTs mainly in the Asia Pacific region.

*JPCERT/CC continues the project, but the activities with APCERT TSUBAME Working Group concluded at the end of March 2023.

Demonstration Test: Internet Risk Visualization – Mejiro

<https://www.jpcert.or.jp/english/mejiro/>

JPCERT/CC has launched a demonstration test to visualize risks on cyber space based on data provided by multiple sources in comparison to the number of IP addresses assigned to each economy. Users can select a region and specify a period to perform analyses from various angles and obtain a more accurate picture of the situation.

3.5 Associations and Communities

Nippon CSIRT Association

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

The Association is a community for CSIRTs in Japan. JPCERT/CC serves as a member of the Steering Committee and the Secretariat for the Association.

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

4.1 Trainings, Seminars and Workshops

JPCERT/CC offers trainings, seminars and workshops for technical staff, system administrators, network managers, etc. JPCERT/CC hosts the JSAC in January (held annually since 2018) and the Control System Security Conference in February (held annually since 2009).

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. JPCERT/CC also supports CSIRTs who wish to become a member of FIRST. In 2022, JPCERT/CC supported several 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. JPCERT/CC is also the convener of the TSUBAME Working Group, which aims to establish a common platform for Internet threat monitoring,

information sharing & analysis within the region.

5.2 Capacity building

5.2.1 Drills & Exercises

JPCERT/CC participated in the following drills in 2022 to test our incident response capability:

- APCERT Drill 2022 (25 August)
- ASEAN CERTs Incident Drill (ACID) 2022 (27 October)

5.2.2 Seminars & presentations

In 2022, JPCERT/CC delivered presentations at the following international cyber security events:

- ASEAN Cyber Crisis Regional Workshop (June, Online)
- 2022 FIRST Virtual Symposium: Asia Pacific Regions (October, Online)
- TWIGF (September, Online)
- 17th Annual IGF Meeting (December, Addis Ababa)

...and more

5.2.3 Other international activities

Below are some of the international events that JPCERT/CC attended in 2022:

- ITU Global Policy Dialogue and Briefing (April, Online)
- NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) Locked Shields 2022 (April, Online)
- BlackHat Asia 2022 (May, Online)
- M3AAWG 54th General Meeting (June and October, Online)
- RightsCon (June, Online)
- 2022 FIRST Conference (June, Dublin)
- 17th Annual NatCSIRT Meeting (June, Dublin)
- USENIX Security Symposium & SOUPS (August, Boston)
- BSidesLV (August, Las Vegas)
- BlackHat USA 2022 (August, Las Vegas)
- DEFCON30 (August, Las Vegas)
- Virus Bulletin 2022 (September, Prague)
- APriGF 2022 (September, Online)
- BlackHat Europe 2022 (December, Online)

...and many more

6. Future Plans

6.1 Future projects/operation

Broaden engagement in multiple areas

While striving to maintain the robust collaboration among CERTs, JPCERT/CC will make efforts to participate in wider communities such as Internet governance and cyber norms, as well as to collect information on global cyber security policy trends.

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

KN-CERT

Korea National Computer Emergency Response Team

1. Highlights of 2022

1.1 Summary of major activities

- Founded the National Cyber Security Collaboration Center
- Became a full member of NATO CCDCOE
- Held 2022 Cyber Conflict Exercise(CCE)
- Hosted 2022 International Conference on Building Global Cyberspace Peace Regime(GCPR)
- Established the reliability verification system for quantum encryption communication devices
- Supported World Forestry Congress, and World Gas Conference for cyber security measures

2. About KN-CERT

2.1 Introduction

The Korea National Computer Incident Response Team (KN-CERT) of the National Intelligence Service of the Republic of Korea has been serving the mission of safeguarding national cyber security for the past 19 years since its establishment in 2004.

2.2 Establishment

On January 25th, 2003, the entire Internet of the ROK was paralyzed by the slammer Worm. This Incident has raised the need for a comprehensive and systematic response taken at the national level for cyber security, which led to the establishment of the KN-CERT on February 20, 2004.

2.3 Opening of the National Cyber Security Collaboration Center

Cyber threats encroaching in both public and private sectors worldwide ask for an international response system for sharing attack information and analysis. In response to this, the KN-CERT founded the National Cyber Security Collaboration Center.

The KN-CERT will secure a base of operation equipped with conference rooms, training facilities, and a central control room in the Pangyo area where IT corporations are concentrated to improve the collaborative response to cyber threats.

3. Activities & Operations

Policy establishment and consulting

- Establishment of cyber security policies, strategies, and guidelines
- Security assessments and consulting for information communications networks

Threat detection and response

- Continuous security monitoring of critical information and communications networks
- Real-time cyber threat detection and issuance of warnings

Incident investigation and damage control

- Attribution of cyber campaigns
- Provision of support for recovery and preventing recurrence

Information sharing and cooperation

- Information sharing for domestic and foreign cyber threats and responses
- Raising public awareness and establishing cooperative channels at home and abroad

Education and training

- Cyber security education for national and public organizations
- Cyber attack response training for public organizations and infrastructure

4. Education and Training

4.1 Cyber Security training

The KN-CERT offers a professional cyber security training program through the cyber security training center in order to improve the professional skills and cyber crisis response of the cyber security officers working for national public institutions.

In 2022, The KN-CERT held training sessions for 1,500 cyber security officers with 30 courses including cyber security policy, cyber security management, security control, and malicious code analysis.

4.2 Cyber Incident Response Training

- The KN-CERT conducts drills to improve the capabilities of national and public organizations in responding to cyber incidents and attacks against the industrial control system(ICS).
- For cyber incident response training(Cyber Guard), from July 5, 2022 to August 25, the KN-CERT conducted three training sessions according to the steps of camouflaged hacking email warning in real-time based on virtualization.
- From August 9 to 12, 2021, 57 ICS management organizations participated in the ICS cyber incident response drills.
- Just as in 2021, the KN-CERT participated in 2022 Locked Shields, the world's biggest cyber defense exercise to further enhance its defense capabilities against cyber attacks and strengthen its international cooperation system.
- South Korea joined NATO CCDCOE to exchange information about counter-cyber attack know-how and cyber security strategy policies with other NATO countries in 2019 led by the National Intelligence Service and became a full member in 2022.

5. Partnership

5.1 Security support for international events

During World Forest Congress and World Gas Conference held in May 2022, the KN-CERT supported security control, starting from a preliminary review for the vulnerabilities of the promotion and participation registration website to cyber attack detection during the event. At the end of the conferences, the KN-CERT helped them delete the sensitive information stored in their business laptops to safely close the events.

5.2 Joining NATO CCDCOE

In February 2022, South Korea became a full member of NATO CCDCOE for the first time in Asia. The KN-CERT prepared to join NATO CCDCOE to acquire the response strategies against global cyber threats, how to protect key infrastructures, and how to respond to cyber infringement incidents since 2019 by dispatching personnel to co-research cyber policies and participating in NATO's cyber defense training. In 2022, NATO acknowledged South Korea as a full member of its CCDCOE.

5.3 International Conference on Cyber Security

The KN-CERT hosted a conference about the new development in cyber security strategies befitting the values of democracy. This online and offline Conference was held from September 20 to 21, 2022 and about 250 experts and professionals at home and abroad participated in the conference, including James Louis, the deputy head of the CSIS.

KrCERT/CC

Korea Internet Security Center

1. Highlights of 2022

1.1 Summary of major activities

In 2022, the Korean public and companies alike were affected by a number of cyber attacks and threats, both small and large. KrCERT/CC has made substantial efforts to improve the response system that can quickly respond to accidents and prevent cyber threats against Koreans and Korean companies. In addition, as a national CERT in the private sector, KrCERT/CC is currently issuing TTPs reports that disclose the actions of attacker groups that can be of actual help to domestic companies, using the capacities and information held by KrCERT/CC. The TTPs report is a series of documentation of attackers' TTPs(Tactics, Techniques, Procedures) confirmed during the course of tracking threats confirmed in attacks that affected the Korean public and Korean companies. Among these reports, "TTPs#4 Operation Muzabi" is listed as kimsuky sub technique and contributor in MITRE ATT&CK.

1.2 Achievements & milestones

In 2022, KrCERT/CC made great efforts to prevent cyber threats, improve security and enable quick responses to attacks for the Korean public and Korean companies. We tried to improve the existing security service in a way that allows it to be more easily used and started new services in response to the drastically evolving environment.

In 2022, the following main activities were taken:

Pre/massive blocking of voice phishing using hacking tracking technologies

KrCERT/CC's hacking tracking technology was applied to the detection of voice phishing attacks and communication patterns, in an attempt to rule out the possibility of voice phishing. Through cooperation with police and 3 telecommunications service providers, we detected the pattern of attacks and blocked the relay that illegally made international voice phishing calls look like they were coming from a general phone number. Additionally, to prevent the collection of illegal information through the installation of malware, we detected the pattern of malware app communication, and blocked communication between the malware app installation smartphone monitoring server and

the malware app.

Launching of the smishing check service that reflects the needs of Koreans:

The spread of malware apps through a new type of smishing attack (text message phishing) using domestic messenger service caused financial losses for many Koreans, and thus it was necessary to implement a plan to resolve the concerns of the public. KrCERT/CC developed and test-operated a real-time smishing check service using a platform that is very accessible for Koreans (Kakaotalk open chat).

Customized security checkup for companies based on their importance and risk level:

Due to an increase in cyber threats attacking the non-face-to-face business environments of companies, KrCERT/CC operated a customized security checkup service to prevent them. Depending on the importance level of business for companies, we performed hacking simulations and inspected security vulnerabilities, and also supported inspection of vulnerabilities in homepage and mobile app service operated by companies, thus enhancing the level of security for overall IT infra of companies. In addition, we published and distributed guidebooks discussing the main cases of vulnerabilities confirmed and the countermeasures for companies to use.

Improvement of company service security through a vulnerability reward program:

In a joint effort with a domestic company, KrCERT/CC hosted a bug bounty program to improve the security level of small and medium companies. We hosted the event in which software developed by small and medium companies was opened to white hat hackers to report 977 cases of new vulnerabilities, and selected 199 critical cases from these to give rewards. The participating small and medium companies used security action consulting and security solutions from KrCERT/CC to quickly take care of vulnerabilities of the product and improved the security level of the company service.

Cyber drill platform development:

In 2022, KrCERT/CC implemented the cyber drill platform and started its test operation in order to consistently monitor the response systems for incidents at private companies and encourage the reinforcement of security measures. Service is limited to small and medium companies and the training areas include hacking email sending, DDoS attacks, and web vulnerability inspection. In addition, it is possible for the company to select a desired drill time and use the drill scenario prepared by themselves, as well as to check the results immediately.

Pre inspection of public app frequently used by Koreans:

Through collaboration with the Ministry of Interior and Safety and the Board of Audit and Inspection, KrCERT/CC has been operating a software development security system since 2012 to improve the security of digital government services, and supporting security vulnerability assessments of software for homepages and mobile apps in the public sector. Notably, in 2022, we helped in the security assessment of 250 mandatory public apps for Koreans including KORAIL Talk, Government 24, TheGeoganghohum and so on, thus successfully removing security vulnerabilities from about 94,000 software programs.

AI technologies applied to automated collection and analysis of incidents:

In the past, responses to incidents relied heavily on the abilities of experts, but there is currently a shift toward automated analysis technologies such as AI. Due to the need to use automated analysis tools and DB, KrCERT/CC also developed FENS(Feature Engineering Normalization System) for internal use. As a result, we have been able to quickly identify incidents by dangerous attacker groups and improve the accuracy of analysis.

One-stop support for victimized companies from recovery to post-management:

KrCERT/CC implemented a support system to prevent repeated occurrence of incidents, thus providing a reliable post-management service as well as speedy disaster recovery for small and medium companies that lack the response capacity and professional security manpower.

Cause analysis	Provides means of accurate cause analysis through visits by professional security staff.
Recovery supports	Professional technical measures, and intimate monitoring supports
Post management	Provides customized training and consulting to prevent the occurrence of the same or similar incidents

[Table 1] Support Process to Prevent Repeated Occurrence of Incidents

Expanding the incident detection area through implementing a big data based detection system:

KrCERT/CC is currently operating multiple detection and analysis systems that can detect attacks in their early phases. In 2022, we made a shift from the old individual system based operation to the big data based integrated detection system (Data Lake) that is newly introduced and implemented. As a result, through system integration and collaborative probing, the rate of incident detection for domestic companies who failed to detect hacking was increased by 265%(2021: 3,012 → 2022: 8,011) compared to the previous year.

Supply of AI and big data sets that can be immediately applied to sites:

The Cyber Security Big Data Center operated by KrCERT/CC implemented the cyber security AI data sets required by the private sector to support intelligence improvement of products and business to handle incidents. Notably, through the test operation of data sets implemented for 30 organizations and companies with direct impacts on the quality of Koreans' life such as airlines, smart homes, medical services and so on, we verified the effectiveness of the data sets in terms of detection performance improvement, efficient manpower use and response time reduction, and also discovered cases of excellent performance.

Remodeling of the portal to enable all Koreans to use it easily:

KrCERT/CC improved user accessibility to the portal(www.boho.or.kr, www.krcert.or.kr) that is operated as a service for Koreans. The level of importance and frequency of use for the content were analyzed to reconstruct the screen layout. Notably, improvements were made to facilitate easy use by elderly users and the handicapped, thus acquiring web accessibility quality certification.

Legal system improvement to prevent incidents and spreading of damages:

To enhance the ability to prevent incidents, KrCERT/CC upgraded the legal basis for the existing bug bounty award program from an Enforcement Decree to an Act, and to prevent the spread of damages due to incidents, KrCERT/CC improved the incident response procedures in terms of reporting information sharing, and speedy cause analysis and so on. In addition, to prevent the spread of damages due to smishing, we implemented the legal basis for blocking the telephone numbers used for smishing.

2. About CSIRT

2.1 Introduction

The Korea Computer Emergency Response Team/Coordination Center (KrcERT/CC) is Korea's national CSIRT, which is responsible for the private sector. Formed under the Korea Internet & Security Agency (KISA), KrcERT/CC is composed of three divisions with ten teams. KrcERT/CC carries out various responsive and preventive programs designed to minimize cybersecurity damage by enabling a 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 former Korea Information Security Agency (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 the so-called 'slammer worm' in 2003. At that time, KrcERT/CC had difficulties in communicating efficiently with a telecommunication carrier, which marked a turning point for the Korean Government in terms of recognizing the importance of cooperation with security incident response teams and businesses such as ISPs. 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 Resources

As of February 2023, 160 employees from 3 divisions work for KrcERT/CC.

2.4 Constituency

KrCERT/CC serves as the focal point of coordinating responses to security incidents in 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 telecommunications sector and home users. At the international level, KrCERT/CC cooperates with many leading and national CSIRTs, international organizations, and security vendors.

3. Activities & Operations

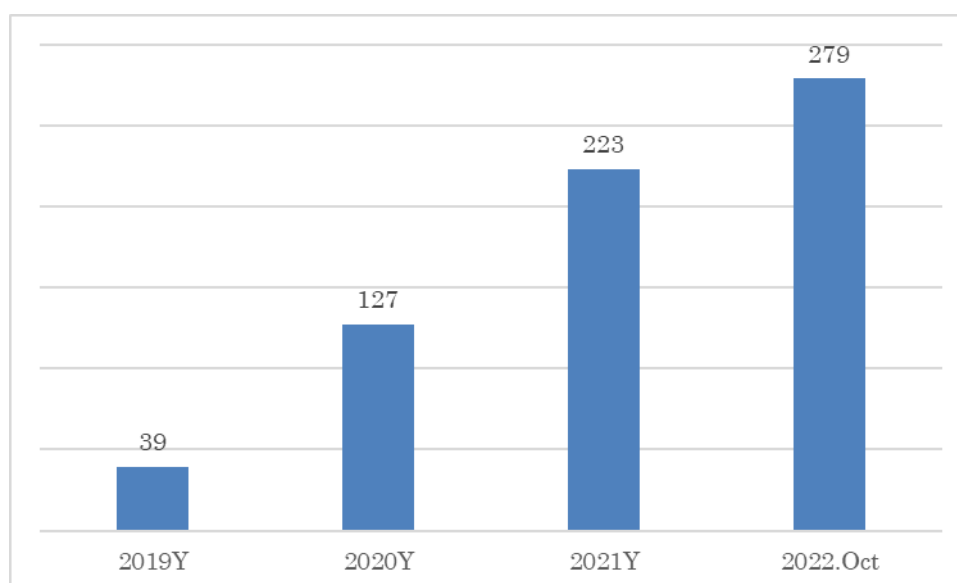
3.1 Scope and definitions

KrCERT/CC works for a safe and 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 related to cyberattacks in the private sector.

3.2 Incident handling reports & Abuse statistics

The scope of incident response by KrCERT/CC covers every type of cyber security for Korean people and companies, but not all related statistics are disclosed. However, please note the following statistics regarding several cases of incidents disclosed.

- Ransomware: Recently, there has been a sudden increase in the number of cases of damage due to ransomware, in which the attackers demand money in return for providing the password for files locked through hacking. Compared to the previous year, the number of reported ransomware attacks has increased by about 1.5 times. In total, 40% of ransomware attacks are reported by the manufacturing industry.



[Picture 1] Ransomware reports to KrCERT/CC

As HTTP-based malware distribution has been increased since 2006, KrCERT/CC has maintained a detection and response system against web-based malware. Additionally, it monitors the spread of malware through file-sharing and free software distribution. The web-based malware detection system inspected 77,000 domains in 2006 and has continued to expand the number of domains it checks, reaching 4.1 million in 2021. In the past, the distribution and type of malware relied on homepages such as drive-by download and so on, but now it has evolved toward malvertising, email attachments and so on, and the target is shifting from an unspecific large number of users to specifically targeted users.

Year	2019	2020	2021	2022
Distribution site	566	738	2,584	4,354
Landing site	7,733	5,296	4,459	9,307
Total	8,299	6,034	7,043	13,661

[Table 2] Detection of Distribution sites, Landing sites

* 4.1 million domestic domains: 3.2 million ccTLD(.kr, Korean) and 0.9 million gTLD(.com, .name, etc.)

To prevent the spread of cyberattacks, KrCERT/CC started the service in 2011 to notify users of an infected PC of malware through pop-up windows, as there was a danger of DDoS attacks, spam mail sending and so on. As mobile malware began to spread widely starting in the second half of 2012, and the number of mobile malware began to soar rapidly in 2013, we expanded the scope to mobile devices as well, notified the users of infected devices(PC and mobile) and provided guidance on anti-virus software and inspection to take necessary security measures. In 2022, we discovered 212,953 devices infected with malware(PC and mobile), informed owners about the infections and let them take

protection measures.

Year	2019	2020	2021	2022
Notification	297,208	436,025	179,544	212,953

[Table 3] Malware infection notifications

3.3 Publications

In 2022, KrCERT/CC published one report of trends of malware distribution, and 6 technical reports such as attacker strategy analysis and incident analysis and so on and distributed the 2023 cyber threat forecasts report. The report is available at the homepage of KrCERT/CC: www.boho.or.kr (or www.krcert.or.kr).

3.4 New services

In 2022, the following new services were provided:

- Pre/massive blocking of voice phishing using hacking tracking technologies
- Launching of smishing check service reflecting opinions of Korean
- AI technologies applied to automated collection and analysis of incidents
- One-stop support for victimized companies, from recovery to post-management
- Expansion of incident probing area by implementing a big data based detection system

4. Events organized / hosted

4.1 Training

KrCERT/CC is offering training by hiring internal or external speakers to share information and exchange knowledge among employees. The following are the details of internal training that took place in 2022.

- IoT Vulnerability Inspection System Function and Utilization Plans(Feb)
- NFT Service Infra Structure and Security Vulnerability Response Plans(Apr)
- Threat Intelligent Based Attack Surface Management(ASM) Roles and Technologies (May)
- Dirty Pipe Vulnerability Analysis and Attacker's Trace Analysis (May)
- Cyber Security Latest Trends(Law/System) (May)
- Introduction to Zero Trust/Overseas Trends and Cases of Introduction(May)
- Metaverse Security (Security Vulnerability Aspects)(May)

- Latest Trends and Methodologies of Hacking Simulation(May)
- Main Market's Malware Detection and Analysis Status(Jun)
- Status of Domestic Software Development Security Law Systems(Jun)
- Digital Forensic vs Incident Response(Jun)
- SIEM/SOAR Tech Trends(Jun)
- Ukraine Cyber War Trends(Jul)
- Source Code Security Vulnerability Diagnosis Procedures and Methodologies(Jul)
- Cyber Threat Information Based Big Data Analysis(Aug)
- Next AI Tech Introduction and Cyber Threats Archive(Aug)
- Change in the Pattern of Domestic Account Stealth Attacks(Aug)
- Latest Web Attack Technology Practice(Aug)
- Detailed Criteria for Source Code Security Vulnerability Diagnosis (Aug)
- Sharing incident case of Public Organizations' WAS(Sep)
- Introduction to Threat Intelligence Based Incident Response Strategy(Sep)
- Homepage/Mobile App Security Vulnerability and Diagnosis Method (Nov)
- Log4j Vulnerability and Web Application(Nov)
- Trends of Code Signature Certificate Related Incident(Dec)

We also offered APISC Security online course and offline training for external organizations(October).

4.2 Drills & exercises

Private Sector Cyber Crisis Response Drills : 1st and 2nd Half

4.3 Conference

- 27th Hacking Prevention Workshop(Dec, KrCERT/CC)
- 2022 AI Security Conference(Nov, KISA)
- 14th CODEGATE(Nov, KISA)
- Mydata Global Conference 2022(Nov, KISA)
- 12th Software Development Conference(Nov, KrCERT/CC)
- 1st Ransomware Resilience Conference(Sep, KISA)
- 2022 Blockchain Meetup Conference(2022 BCMC)(Jul, KISA)
- 11th International Information Protection Conference on the Day of Information Protection(Jul, KISA)
- 28th Information Communication Network Information Protection Conference (NetSec-KR 2022)(Apr, KISA)

5. International Collaboration

5.1 International partnerships and agreements

- Cyber Threat Alliance(CTA)

5.2 Capacity building

5.2.1 Training

- APCERT – Latest Trends on Keyword Hacks & SEO Spam(Feb)
- APCERT - Cyber Threat Intelligence on a national level(Aug)

5.2.2 Drills & exercises

- 2022 APCERT Cyber Drill(Aug)
- 2022 ASEAN Cyber Incident Drill(Oct)

5.2.3 Seminars & presentations

- VirusBulletin 2022(Sep)

6. Future Plans

6.1 Future projects

In the future, KrCERT/CC will introduce chatbots to its portal(www.boho.or.kr, www.krcert.or.kr) to improve accessibility and repair the companies' incident reporting systems. In addition, we will strengthen profiling and thus reinforce the analysis system and will also expand the scope of supports for the security of small and medium companies and launch a cyber drill platform as an official service.

7. Conclusion

As mentioned in the introduction, in 2022, a series of small and large cyber incidents resulted in many resources consumed domestically and overseas. Due to this situation, despite the scarce resources, in 2022, KrCERT/CC successfully managed to pursue various new prevention, response and recovery projects for the Korean people and companies. In the future, we will make greater efforts to create a safe cyber space for Koreans.

LaoCERT

Lao Computer Emergency Response Team

1. Highlight of 2022

1.1 Summary of Activities

- Co-host the Seminar on The Importance of Critical Information Infrastructure (CII) in Digitalisation Development and its challenges on 27 June 2022, Vientiane Capital, Laos. More than 80 people participate from Banks, ISPs, Private sectors and related Ministries.
- Organized Lao Digital Week event on 21 – 25 December 2022 at Km 6 Conference Hall, Vientiane Capital, Laos. Participants from all IT Private and Government sectors
- Organize the Lao Cyber Security Hacking Challenge on 22 December 2022 during the Digital week event.

1.2 Achievements & milestones

- Disseminated the use of social media security to students in high school around Vientiane Capital.
- Drafting the Cyber Security Law
- Drafting the National Cybersecurity Strategy

2. About LaoCERT

2.1 Introduction

Lao Computer Emergency Response Team (LaoCERT) is the national CERT of Lao PDR, under, Ministry of Post and Telecommunications 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

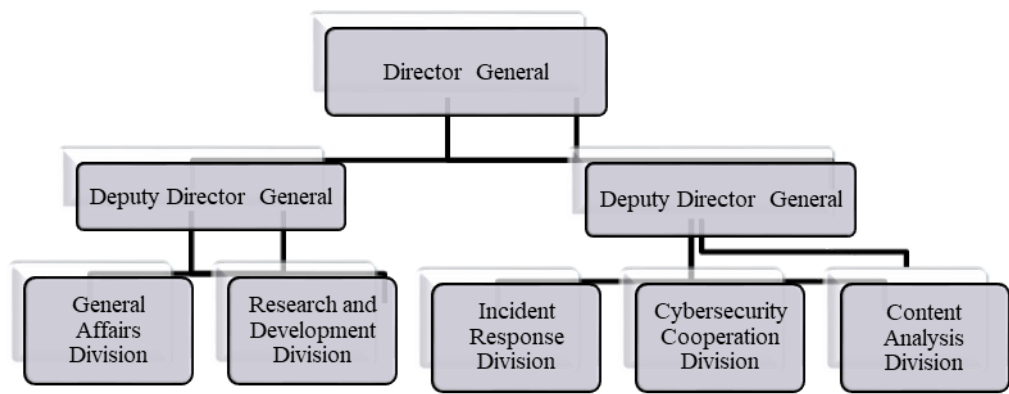
was a member of APCERT in 2014. This annual report will describe activities and operation of LaoCERT in 2022.

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 announcement to become the national CERT equivalent department in 2016, directly under to the Ministry of Post and Telecommunications. Currently, the Ministry of Post and Telecommunications has become 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 Resource

Department/LaoCERT currently contains 30 staffs, 8 females and divide into 5 Divisions.



Department/LaoCERT Organization Charts

2.4 Constituency

Department/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 Laos PDR.

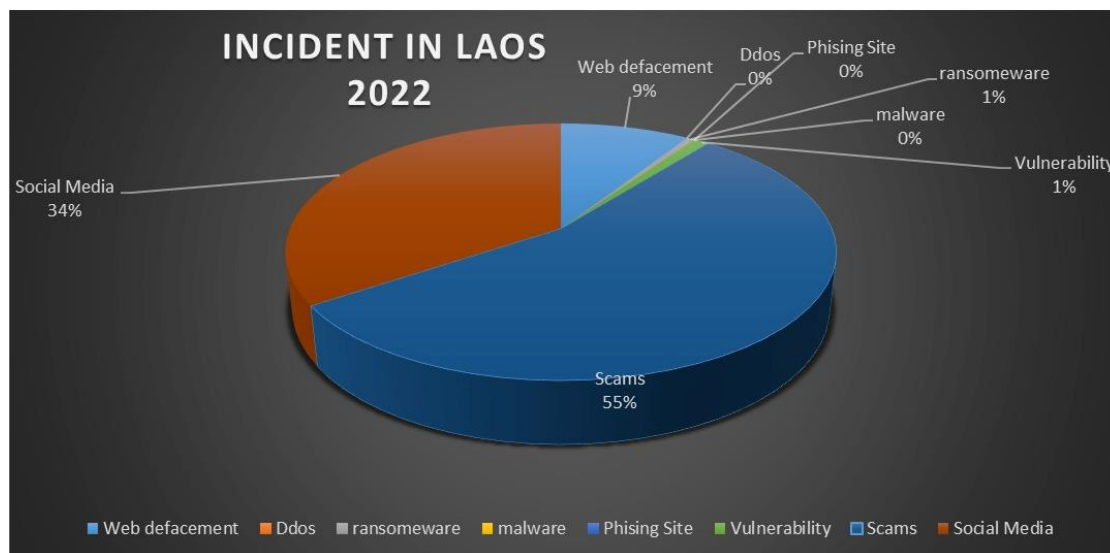
3. Activities & Operations

3.1 Scope and definition

Department/LaoCERT aim to awareness raising 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.

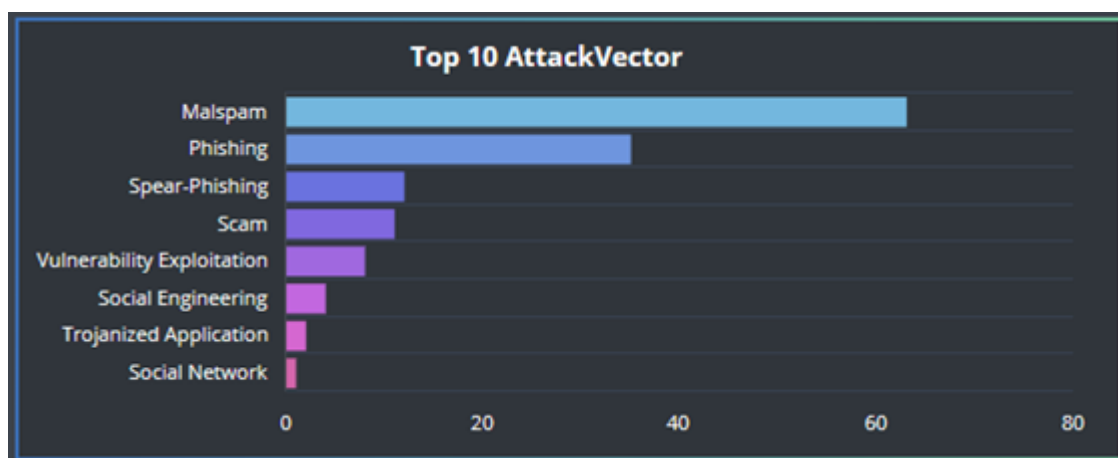
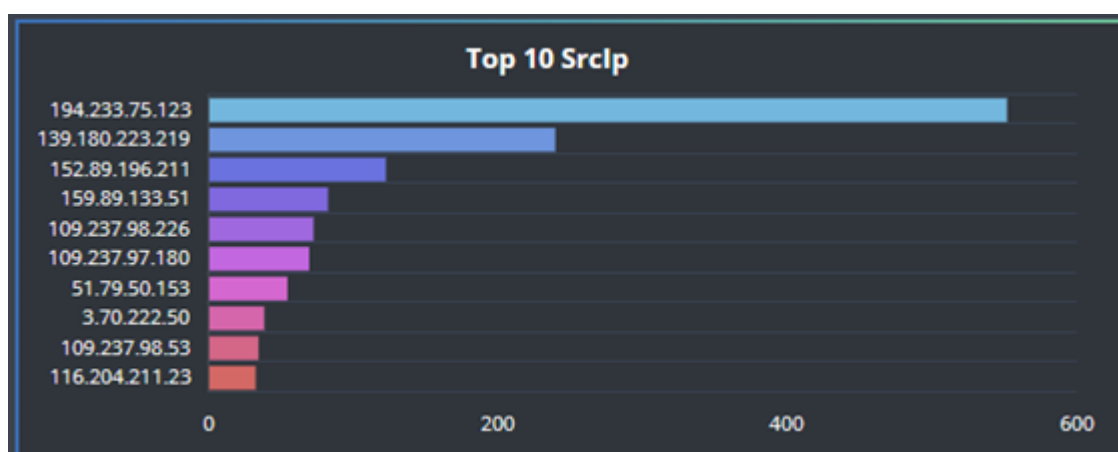
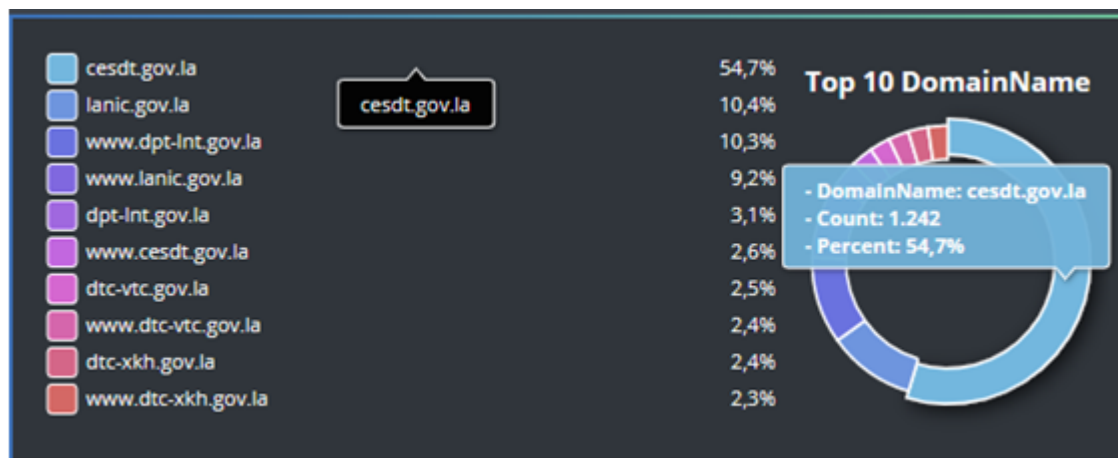
3.2 Incident handling report

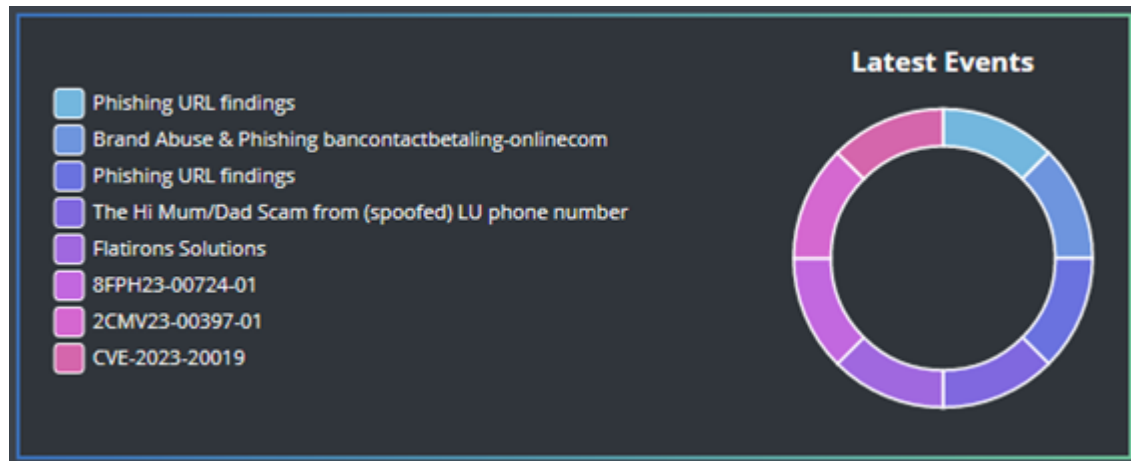
The following graph shows the statistic of incidents that happened in 2022.



3.3 Abuse Statistics

The following graph shows Abuse Statistics in 2022:





Top 10 of Web attacks

3.4 Publication

- Website: www.laocert.gov.la
- E-mail: admin@lacert.gov.la
- Tel: +85621 254508 (08:00-16:00) Working hour
- Incident report: report@laocert.gov.la

3.5 New Services

- Advisory on the use of Social Media Security.
- Coordinating to provide information that related cybercrime.

4. Events organized / hosted

4.1 Training

- Training on the Zimperium Mobile Threat Defense Application and Honeywell Secure Media Xchange on 25 March 2022, Vientiane Capital, Lao PDR.
- Training on Restrospect Lab, on 07, 14 and 21 November 2022 via online platform.

4.2 Conferences and seminars

- Co-Organized Seminar on Cyber Security and Critical Information Infrastructure Protection on 1 April 2022 in Vangvieng District, Vientiane Province, Lao PDR.
- Co-host the Seminar on The Importance of Critical Information Infrastructure (CII) in Digitalisation Development and its challenges on 27 June 2022, Vientiane Capital, Laos.

5. International Collaboration

5.1 International partnership and agreement

In 2022, LaoCERT did not sign any agreement on cooperation plan due to the pandemic of COVID-19 and other inconveniences, however, we are now planning to prepare the contract for joint activities in cybersecurity field with ASEAN countries, international organizations and the national CERT.

5.2 Capacity Building

5.2.1 Training

The following has shown the statistic for attended the training in 2022:

- The Cybersecurity Executive Awareness Course via on 27-29 April 2022.
- The 20th Online ASEAN-Japan Cybersecurity Building Centre Training (AJCCBC) on 09-13 May 2022.
- APCERT Online Training on 07 June 2022.
- The 21st Online ASEAN-Japan Cybersecurity Building Centre Training (AJCCBC) on 13-17 June 2022.
- The 22nd Online ASEAN-Japan Cybersecurity Building Centre Training (AJCCBC) on 01-05 August 2022.
- APCERT Online Training on 09 August 2022.
- The International Security in Cyberspace Seminar for ASIA-Pacific Partners training on 19-23 September 2022 in Germany.
- The 23rd AJCCBC Technical Cybersecurity Training on 03-07 October 2022 in Bangkok, Thailand.
- The 24th AJCCBC Technical Cybersecurity Training on 19-23 December 2022 in Bangkok, Thailand.

5.2.2 Drills and Exercises

The following has shown the statistic for participated Drills and Exercises in 2022:

- APCERT Cyber Drill on 25 August 2022.
- ASEAN CERT Incident Drill (ACID) 2022
- ASEAN Plus Three CERTs Cyber Security Drill
- Attend The 12th Singapore Cyber Conquest on 18-20 October 2022 in Singapore

- ASEAN-ITU Cyber Drill on 05-09 December 2022.

5.2.3 Seminar and presentation

The following has shown the statistic for participated the Seminar and Workshop in 2022:

- The Webinar on the Development of Effective Coordination at the National Level for the Participation in International Discussions on ICTs Security on 20 January 2022.
- The 1st ASEAN-Japan Cybersecurity Working Group Meeting on 15 February 2022 via Video Conference.
- The UK Workshop on Identifying Critical National Infrastructure Dependencies on 17 February 2022 via online Platform.
- Attend the research study on covid-19 related cybercrime in Asia on 07-09 March 2022 in Sri Lanka.
- The 2nd ASEAN-Japan Cybersecurity Working Group Meeting (Video Conference) on 07 June 2022.
- The ASEAN Partner CERTs Information] Sharing on Emoted and Local Cyber Threat Landscapes on 14 June 2022 via online.
- The Seminar on TikTok Southeast Asia Dialogues - Unlocking the Creator Economy in Southeast Asia on 15 June 2022 via online.
- The 3rd ASEAN-Japan Cybersecurity Working Group Meeting on 02-05 August 2022 in Bali, Indonesia.
- The Global Forum on Cyber Expertise (GFCE) on 13-15 September 2022 in Hague, Netherlands.
- The Digital Diplomacy workshop on 20-22 September 2022 at the ASEAN- Singapore Cybersecurity Centre of Excellence (ASCCE) in Singapore.
- The 15th ASEAN-Japan Cybersecurity Policy Meeting on 04-05 October 2022 in Japan.
- The APCERT Annual Meeting via Video Conference on 18-19 October 2022.
- The 07th Singapore International Cyber Week (SICW) and ASEAN Ministerial Conference on Cybersecurity (AMCC) on 18-20 October 2022.
- The CAMP 7th Annual Meeting on 17-20 October 2022 in Seoul, South Korea
- The FIRST-APCERT Regional Symposium on 20-21 October 2022
- The China-ASEAN Digital Security Forum via Video Conference on 28 October 2022The Seminar on Industrial Control Systems Cybersecurity Week for the Indo-Pacific Region on 24-28 October 2022 via online.
- The ASEAN Cybersecurity Coordinating Committee Meeting on 11 November 2022 via Video Conference.
- The China-ASEAN Digital Security Forum on 15 November 2022 via Video Conference.
- The International Law of Cyber Operations course on 28 November – 02 December 2022, at the ASEAN- Singapore Cybersecurity Centre of Excellence (ASCCE) in Singapore.

6. Future Plans

- Continue to provide training and seminar on Cybersecurity to provincial 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 Cyber Security Law.
- Drafting National Cyber Security Strategy
- Expanding the awareness raising on Cyber Crime Law and data protection Law.
- Establish a Cyber Security Operations Center (SOC) and now is under the coordination and set up the room.
- Planning for Establishing Government Threats Monitoring (GTM).
- Planning to set up the Network Monitoring System.

7. Conclusion

Department/Lao Computer Emergency Response Team (LaoCERT) still keep continuing to develop a team including to improve the technical capabilities of staff both quality and quantity with the concentrate on incident handling, network security, development the cybersecurity legislation and enhance the cooperation among domestic and international cybersecurity organizations in order to promote and organize the cybersecurity activities as well as to provide a workshop-seminar and training which aim to improve the technical skill of staff as well as to disseminates awareness-raising on legislation and Law and instruction on how to use social media or computer network securely without cyber-attacks.

mmCERT

Myanmar Computer Emergency Response Team

1. Highlights of 2022

1.1 Summary of major activities

Due to the situation of post Covid-19 pandemic, physical activities were allowed in the midst of this year while ongoing the virtual events. In spite of the challenges and constraints, mmCERT keeps on serving to response and handle cyber incidents and to provide technical assistant to its constituency. mmCERT continues on collaboration with international and regional organizations both onsite and online.

For the purpose of effective incident response services, mmCERT had contributed in APCERT Drill, ACID Drill, ASEAN-Japan Cyber Remote Exercises and Tabletop Exercise yearly. In terms of capacity building, mmCERT encourages international, regional, and local trainings and knowledge sharing sessions, webinars, and forums.

mmCERT had successfully launched a new service of "Penetration Testing Lab" to provide secure attempt for government organizations.

1.2 Achievements & milestones

- Organized "Myanmar Cyber Security Challenge-2022" on 1st October, 2022.
- Myanmar acted as host country virtually for 13th ANSAC meeting in 11th October 2022.
- Myanmar represented as co-chair in 2nd ASEAN-China Cyber Dialogue at Singapore on 19th October 2022.
- Myanmar performed as host country virtually in "The 3rd Meeting of ASEAN Cybersecurity Coordinating Committee (ASEAN Cyber-CC)" on 11th November 2022.
- ITCSD participated in "Youth, Literature and Art Show" during 26th to 29th December 2022 at MICC-2, Nay Pyi Taw.
- Cyber Security Policy is approved by the meeting of the Government of the Union of Myanmar No. (9/2022) held in December, 2022.

2. About CERT

2.1 Introduction

Myanmar Computer Emergency Response Team (mmCERT/cc) is a national computer emergency response team of Myanmar for handling cyber security incidents in Myanmar. It is an operational member of APCERT in 2011.

2.2 Establishment

Myanmar Computer Emergency Response Team (mmCERT) was formed by e-National Task Force on 23rd July, 2004 according to the Initiative of ASEAN Integration (IAI) agreement. mmCERT was wholly government funded organization under Information Technology Department, Ministry of Communications, Posts and Telegraph (MCPT).

On December 15th 2010, mmCERT extended its service coordination center (cc). and in 2011, mmCERT/cc become an operational member of APCERT.

In 2015, Information Technology and Cyber Security Department (ITCSD) was formed under the Ministry of Communication and Information Technology (MCIT) in order to accelerate E-Government Services and to enhance the cyber security of government agencies and private sectors. And mmCERT/cc was restructured under National Cyber Security Center (NCSC), ITCSD.

In 2016, The Ministry of Communication and Information Technology (MCIT) was changed the name to the Ministry of Transport and Communications (MOTC). The Ministry of Transport and Communications (MOTC) is a leading Ministry of Information Technology and Cyber Security Department Activities in Myanmar.

mmCERT/cc is currently operating as a sub-division under NCSC of MOTC.

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 National Cyber Security Center under Information Technology and Cyber Security Department (ITCSD). As human resources of mmCERT is inadequate to handle cyber issues at present and thus it has been planned to extend the organization structure and to recruit more professionals.

2.4 Constituency

mmCERT formerly handled computer incidents of government agencies and MPT, state-own telecom operator. Since establishment, mmCERT/cc has been serving for disseminating security information and advisories and providing technical assistance to government agencies, telecom operators, internet service providers (ISP), universities and

individual users in Myanmar. It has been planned to extend the constituency to financial institutions, banks, online services/shopping, research and development center and vendors.

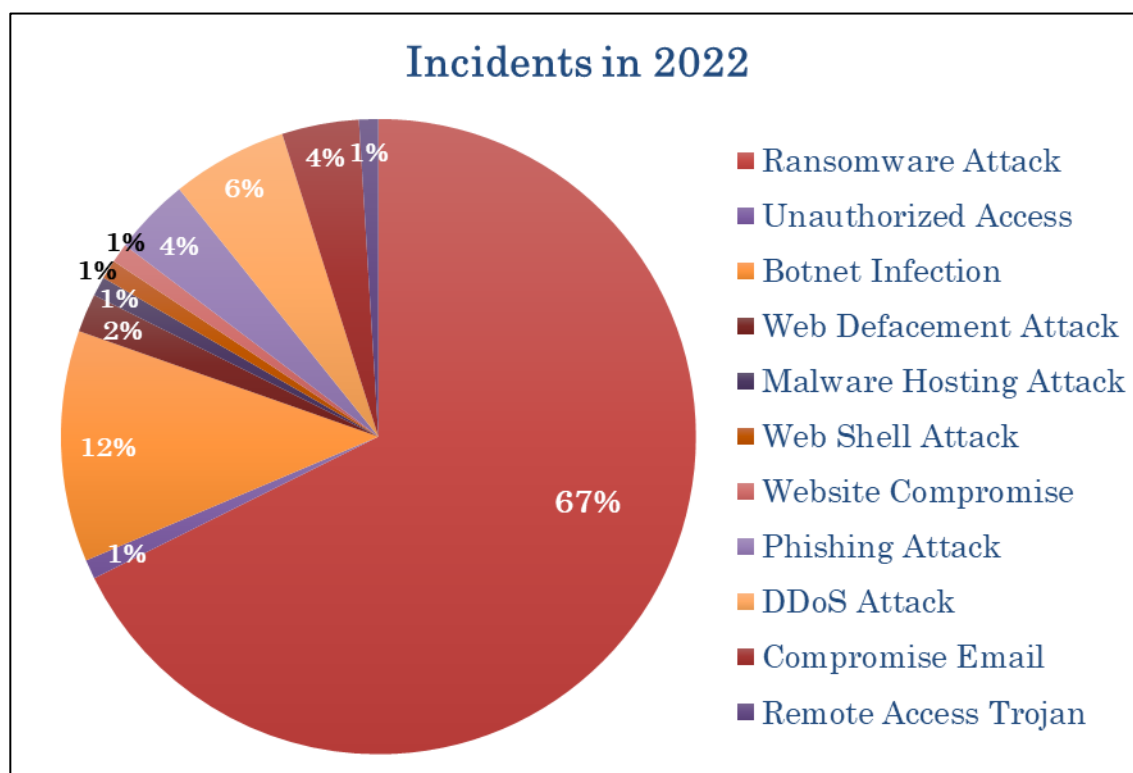
3. Activities & Operations

3.1 Scope and definitions

- Creates National IT image by cooperating with international CERT teams for cyber security and Cyber-crime
- Disseminates Security Information and Advisories
- Provides technical assistance
- Cooperates with law enforcement organizations for cyber crime

3.2 Incident handling reports

Being facing with many challenges since previous years, it is significantly fewer in the number of incidents reported to mmCERT from individuals and private sectors. The following graph shows the incidents handled by mmCERT in 2022. According to the results on incident analysis by mmCERT, ransomware attacks remains prominent incident case for Myanmar.



3.3 Publications

- “STOP Ransomware Guide” was released on its Facebook page and website from Version 1.1 to 1.4 according to timely changes of encryption method of the developer.
<https://ncsc.gov.mm/wp-content/uploads/2022/06/STOPRansomwareGuide1.4.pdf>
- “PlugX Removal Guide (Version 1.0)” was also released to help the victims of PlugX RAT to know the tactic of this RAT and eradication method.
<https://ncsc.gov.mm/wp-content/uploads/2022/06/PlugXRemovalGuideVersion1.1.pdf>
- “Guidebook for Suspicious Mails (Version 1.0)” was shared for the knowledge of phishing mail attack and provides the preventive measures to wide range of aspects from individual to enterprises and government organizations.
https://ncsc.gov.mm/wp-content/uploads/2022/12/Guidebook-for-Suspicious-Mails-Version-1.0_with-cover.pdf
- “Cyber Security for Mobile Devices”
This is the compilation of infographics by ASEAN Member States and Japan to share best practices and exchange public education resources. With the increased use of smartphones and other smart devices, this booklet is intended to increase public awareness of cybersecurity and to adopt measures to protect our devices and data.
<https://ncsc.gov.mm/wp-content/uploads/2022/06/Cyber-Security-for-Mobile-Devices2021.pdf>

Current events and activities of mmCERT can be known from mmCERT website and NCSC website. The update cyber trends, cyber incidents and articles were also translated into Myanmar language and published appropriately. CVE for computer network and system can also be reviewed in mmCERT website. Trending security and cyber threat news and articles can be seen frequently in mmCERT Official Facebook Page and Website.

- <https://www.mmcert.org.mm>
- <https://www.ncsc.gov.mm>
- <https://www.facebook.com/mmcert.team/>
- https://www.youtube.com/@NCSC_Myanmar

3.4 New services

In this year, Penetration Testing Labs was introduced that intends to check, identify and advise about cyber security vulnerabilities in network security systems and Web servers of Union Ministries and Government Agencies. In this year, the penetration testing and security audit were provided as per request.

To provide prompt assistance for incidents, mmCERT/cc provides contact point as follow:

- Incident report: infoteam@mmcert.org.mm and incident@ncsc.gov.mm
- (+ 95 67 3422272) (24 x 7 services)
- <https://www.facebook.com/mmcert.team> (24 x 7 services) (Messenger)

4. Events organized / hosted

4.1 Training

- Incident Handling – Intrusion Detection Courses are provided three times in May, July and November at Training Center of ITCSD. There were 78 attendees from ministries and government organizations.
- Information and Communications Technology Course for “Officer Capacity Building Training (2/2022)” was offered at Information & Public Relation Department (Nay Pyi Taw) in July 2022. There were total 22 attendees from district and division branch offices in this training.

<https://ncsc.gov.mm/en/ict-subject-in-iprd/>

- The Cyber Security Training was provided for IT staffs of Union Election Commission in November 2022. There were 30 attendees in this training.

<https://ncsc.gov.mm/en/uec-training/>

4.2 Drills & exercises

- Myanmar Cyber Security Challenge-2022 was held at Nay Pyi Taw on 1st October, 2022.



- “Cyber Security Quiz” was conducted “Youth, Literature and Art Show” during 26th to 29th December 2022 at MICC-2, Nay Pyi Taw. There were 1,353 participants for this quiz and the remarkable mark holders were presented gifts. The six participants who got highest mark in Basic Education High School and University Level were awarded prizes.



4.3 Conferences and seminars

- It was attempted for encouraging participants from government and private CII Sectors to join the “ASEAN-JAPAN CIIP Workshop” was held as the first day of ASEAN-JAPAN Cybersecurity Working Group Meeting on 2nd August 2022 in Bali, Indonesia. There were total 30 persons who joined this workshop from Myanmar.

<https://ncsc.gov.mm/en/asean-japan-ciip-workshop/>

- Myanmar acted as host country virtually for 13th ANSAC meeting on 11th October 2022.

<https://ncsc.gov.mm/en/13ansac/>



- Myanmar represented as co-chair in the 2nd ASEAN-China Cyber Dialogue at Singapore on 19th October 2022.

- Myanmar performed as host country virtually in “The 3rd Meeting of ASEAN Cybersecurity Coordinating Committee (ASEAN Cyber-CC)” on 11th November 2022.

<https://ncsc.gov.mm/en/3rd-meeting-of-asean-cyber-cc/>



4.4 Other activities

To raise cyber security awareness through youngers, parents, governmental personals and citizens, ITCSD participated in “Youth, Literature and Art Show” during 26 to 29 December 2022 at MICC-2, Nay Pyi Taw. Cyber Security Awareness Booklets were distributed and Cyber Security Quiz was conducted during these days.

<https://ncsc.gov.mm/en/youth-and-literature-art-show/>

5. International Collaboration

5.1 Capacity building

5.1.1 Training

- Joined “APT Myanmar Network Security Online Workshop” hosted by Asia Pacific Telecommunity (APT) on 6~7th July 2022.
- NCSC virtually attended Network Security Workshop organized by APNIC foundation in July, 2022.
- Member of mmCERT/cc enrolled “AJCCBC & UK Home Office E-Learning Syllabus” from July to September, 2022.
- Members of ITCSD attended CYDER Course, Network Forensic and Malware Analysis in February, May, August, October and December 2022.
- Members of NCSC attended “ASCCE-UK Digital Diplomacy Course” provided by ASCCE and UK, Singapore in September 2022.

- Member of NCSC attended “Executive Course on International Law of Cyber Operation” provided by ASCCE, Singapore in 28th November to 2nd December 2022.

5.1.2 Drills & exercises

- mmCERT/cc conducted ASEAN-JAPAN Remote Cyber Exercise in June to improve Incident Handling and Responding skills.
- Participated in “Tabletop Exercise” at ASEAN-JAPAN Cybersecurity Working Group Meeting, Indonesia on 3rd August 2022.
- Also joined APCERT Drill in August 2022.
- mmCERT/cc participated in ACID Drill in October 2022.

5.1.3 Seminars & presentations

- Virtually presented about “Exchange of policies and mechanism building” at the 2nd ASEAN-China Cyber Dialogue on 19th October 2022.
- Virtually joined China-ASEAN Network Security Emergency Response Capacity Building Seminar on 8th December 2022.
- Virtually attended the “2nd ASEAN-Russia Dialogue on ICT Security-related Issues” on 15th December 2022 and presented the topic of “Exchange of information on threats, attacks and incidents in the information sphere”.
- Conducted “Sharing Sessions” hosted by SingCERT twice a year among ASEAN Member States. mmCERT/cc also shared “Local Threat Landscape” in these sessions.

5.2 Other international activities

- Closely coordinated with ASEAN-JAPAN Working Group Meeting and conducted their activities.
- Joined “First Meeting of the BIMSTEC Expert Group of Cyber Security Cooperation” on 14~15th July, 2022 in India.



- Myanmar hosted 13th ANSAC meeting on 11th October 2022 and the 3rd Meeting of ASEAN Cyber-CC on 11th November 2022.

- Myanmar co-chaired in the 2nd ASEAN-China Cyber Dialogue at Singapore on 19th October 2022.



- NCSC also sent the students to participate in 12th Singapore Cyber Conquest on 19th October 2022.
- NCSC arranged the participants to join the Cyber SEA GAME 2022 - ASEAN Cybersecurity Competition by AJCCBC in November 2022.

6. Future Plans

6.1 Future projects

- Public Key Infrastructure Project will be implemented.
- It is planned to Cyber Security Awareness Raising Workshops for CIOs and ACIOs from government agencies.
- Cyber Security Awareness Video Competition Project has been planned to enhance the cyber security knowledge among younger ages.

6.2 Future Operation

- Being a developing team, mmCERT/cc is striving hard to be a developed and matured team by elaborately doing Incident Handling, Cyber Security Researches, efficiently providing Technical Advisories, Trainings, Seminars and Workshops to Constituencies.
- Coordination with government ministries and agencies to establish CSIRT and ISAC in the future.
- Incident Handling Courses will be extended to get effective capacity building through government agencies.
- Public Awareness Activities such as workshops, seminars and discussion will be organized to enhance ICT knowledge and to know the importance of cyber security aspects.
- Cyber Security Awareness Movies will be produced for broadcast media and other social media platforms.

- Cyber Range Platform will be implemented to strengthen the cyber security skills for the students from universities in terms of internship program at NCSC.
- Web-Penetration Testing will be carried out for government agencies upon their requirements.
- Security Operation Center of NCSC monitors, detects, protects and responds the cyber incidents by adapting the Security Operation Center Platform. It serves as 24/7 protection for government agencies as per demands.
- And then mmCERT/cc will continue to international and regional co-operations for CERT Activities and operate research on Log Data Analysis as much as possible.

7. Conclusion

Being an age of post pandemic of work and life, there may be many transitional processes all over the world. Despite bad things of last year, our people had got the advantages of understanding the needs for using of ICT and the importance of cyber security for their real life.

mmCERT/cc proceeds with not only handling and responding of incidents but also capacity building and awareness raising throughout the country. We continue to closely collaborate with government agencies and CII sectors in terms of information sharing on cyber issues and to build safer cyber space within our constituency. On the other hand, we keep on maintain relationships with regional and international organizations related with cyber security in order to ensure proactive cyber resilience and to affirm the safe and trusted global cyber environment.

MNCERT/CC

Mongolia Cyber Emergency Response Team/Coordination Center

1. Highlights of 2022

1.1 Summary of major activities

All of the activities of MNCERT/CC moved back to in-person after the global Covid-19 pandemic. MNCERT/CC has successfully organized its annual event and cyber security competition on-site. Mongolian the biggest cyber security event MNSEC2022 has covered larger scope of participants than the last few years and continued for two days for the public.

“Haruulzangi U18” CTF among high school senior grade students and “Haruulzangi 2022” CTF among security specialists had been held successfully by MNCERT/CC.

“Red Team” bug bounty drill among banking and financial sector was a new activity organized by MNCERT/CC in 2022.

1.2 Achievements and milestones

One of the main activities of MNCERT/CC was providing its member organizations with threat intelligence and indicator information, recommendations, consulting, and training.

MNCERT/CC continued the cooperation with NCFTA IFA system and provided its constituency with stolen credentials including credit/debit cards, email accounts with accompanying passwords and user login accounts with respective passwords related to our constituency.

We continued providing our member organizations with threat intelligence, indicators, threat actor information using MISP open-source threat intelligence and sharing platform.

One of the key achievements of this year was continuation of “HaruulZangi” cyber security competition which was held on-site in three stages. Winners of the contest expressed their impression that the missions were more exciting and challenging than the past years.

MNSEC 2022 event included an offsite networking day beside the official event and covered 348 participants which are a relatively large percentage of the security sector for Mongolia.

2. About MNCERT/CC

2.1 Introduction

“Mongolian Cyber Emergency Response Team / Coordination Center” (MNCERT/CC) is a non-governmental organization which established in 2014 and has been performing its function under the guidance and regulation of Mongolian National Security Council. MNCERT/CC is responsible for incident response and monitoring, disclosing the cyber security related information and knowledge to public, developing and broadcasting the methodology to prevent from cyber threats, providing its member organizations with cyber security details and training, as well as acting as coordinator to defend Mongolian cyber environment.

2.2 Establishment

“MNCERT/CC” was established on March 15th, 2014 and founded on following grounds:

Based on the component of information security of the Mongolian National Security Concept and National program for Cyber security, the 48th resolution was approved by Mongolian State Great Hural (State Great Assembly) in 2010:

- Objective 2.2 “Establish a system to respond on cyber threats and incidents, develop national CERT, expand cooperation with organizations that have similar operations (e.g., APCERT, FIRST, CERT/CC) (Implementation date 2010-2012, financial source – foreign loan & aid)”
- Objective 4-1 “To strengthen capacity of the organization obligated to provide security on state’s data and information (Implementation date 2010-2015, financial source – foreign loan & aid)”

2.3 Resources

According to the Non-governmental organizations code of Mongolia, the founders of MNCERT/CC have appointed the steering committee with nine members and consultant team with three members. The members of steering committee and consultant team consists of the professionals and researchers in information technology field especially in cyber security and a legal advisor. Under steering committee, the executive team including CEO, operational manager, incident handler, analyst and legal advisor performs its activity.

2.4 Constituency

Our constituencies are:

- Internet Service Provider Companies
- Banks

- Mobile Operator Companies
- Universities
- MonCIRT and DCERT
- General public

3. Activities & Operations

3.1 Scope and definitions

MNCERT/CC's constituency covers various types of organizations such as business companies, private sector organizations, banks, universities, non-governmental organizations, and general public. MNCERT/CC provides services such as cyber security related discussion, training, security information and feed, recommendation, consulting, research and analysis report and coordination with other local and international CSIRTs for its member organizations as well as provides and improves cyber security awareness for general public.

4. Events organized / hosted

4.1 Training

4.1.1 Members meeting and training

MNCERT/CC is expanding into a forum for creating a community of security professionals, where security professionals from member organizations can discuss the problem they face every day, share their experience and have free conversations. MNCERT/CC initiates a discussion and presents specific topics at monthly member meeting such as NIST cyber security framework, Bug bounty approaches, MITRE ATT&CK Use Cases and Applications, Data privacy act developed in Mongolia, Kubernetes Security configuration and Money laundering of Crypto economy, Modern identity and access management and CTF final round tasks.

4.2 Drills & Exercises

4.2.1 "Red Team" drill

MNCERT/CC and the Mongolian Banking Association jointly organized the Red Team cyber drill on July 1-3, 2022. 2 trainers with international certificates (OSCE, CEH, CPISI, GREM) and 16 specialists from 4 organizations participated in the training. Training instructors shared their experience and skills with participants, including vulnerability scanning methodologies and commonly used tools. Also, each team is given instructions and suggestions for detecting system vulnerabilities.

A total of 16 participants were divided into 3 teams depending on their skills and experience and searched for vulnerabilities in the online banking system production environment of two banks and the testing environment of one bank.

As a result, four of High-Level Vulnerability and 7 of Medium Level Vulnerability were detected respectively.

At the end of the training, the participants shared their knowledge and experience by discussing the vulnerabilities they discovered and how they were discovered.

4.2.2 “Haruulzangi 2022” National Cyber Security Competition

MNCERT/CC organizes a cyber security contest named “Haruulzangi” in order to promote the real-life challenges and proper knowledge of cyber security to students and cyber security engineers. We have successfully organized “Haruulzangi 2022” competition between 10th September to 6th October of 2022.

The HaruulZangi Cyber Security Competition has been organized with two main sections of Cyber Probability Analysis and Ethical Attacks and Defenses. The competition seeks to create opportunities for the identifying, executing, and presenting hacking activities in an ethical manner consistent with relative laws and regulations and to raise awareness of the need and requirements for the confidentiality and protection of sensitive information assets.

Today, the HaruulZangi competition has developed into Mongolia's largest CTF competition among IT security engineers and specialists.

The 1st stage was held virtually while the 2nd and final stage were held physically. Out of 168 teams of 342 members, 10 teams qualified from the 1st stage to final. The champions and finalists of the previous HaruulZangi competition competed which makes it a fierce competition.

It is distinguished by its inclusion of tasks that can appear in real cases (Information Security Case Management), Blockchain, Zero-Knowledge-Proof tasks, Crypto, Forensic, Web, and Programming tasks.

4.2.3 “Kharuul Zangi U18 2022” National Cyber Security Competition

MNCERT/CC has initiated and organized cyber security competition named “Kharuul Zangi U18” among the high school students under the age of 18 on 28th May to 5th June. The competition goal is to provide knowledge of possible danger caused by the cyber crime and to increase cyber threat awareness for high school senior grade students.

Totally 138 competitors of 46 teams have challenged for the competition. 1st stage of the competition had been held online while the final 2nd stage had been onsite. High school senior grade students had great interests to this kind of competition and had informed to be more prepared for next Kharuul Zangi U18.

4.3 Conferences and seminars

4.3.1 MNSEC 2022 Virtual Event

MNCERT/CC has been organizing the MNSEC cybersecurity conference since 2014. MNSEC2022 was held on 5th and 6th of October at the Shangri-La Ulaanbaatar Hotel Ballroom. The main goals of the conference are to share information, gain knowledge and experience, and learn from others, for amateurs and professionals in the cybersecurity field, and build professional connections with one another. The MNSEC has been extended over the years and has become the

biggest cybersecurity conference and meeting in Mongolia.

By attending the conference, the cybersecurity professionals, students, and researchers are sharing their knowledge and experience and building professional networks with fellow professionals, and for the organizations, MNSEC is offering sponsor options with the benefit of promoting their products, increasing their market share and headhunting opportunity for the young talents.

The MNSEC2022 was an onsite conference after the Covid-19 pandemic. Furthermore, the number of attendees and active participation were indicating that attendees were waiting for the onsite MNSEC conference for a long time of two years. The conference program consisted of 2 days of full schedule that had 13 speeches and other fun & team building activities. The total number of attendees was 348.

The speeches were about Kubernetes security, building Quantum Resistant organizations and securing your data in the future, Getting started in bug bounty, the Cyber threat landscape in Mongolia, Top risks in Information Technology, Checkpoint Maestro Hyperscale Network security, Table Top Exercises and Cyber Drills for Increasing Incident Response Preparedness, Cyber threat intelligence information sharing, Cyber Security Architecture, Android app security, SOC process improvement, Modern penetration testing approaches and Password analysis of Mongolian internet users. In other words, regardless of their knowledge base and position, everyone who attended the conference could learn something new within their interested areas.

5. International Collaboration

5.1 International partnerships and agreements

- APCERT
- TEAM CYMRU
- FIRST
- APWG
- MICROSOFT
- NCFTA

5.2 Capacity building

5.2.1 Training

- MNCERT/CC attended to Japan-US-EU Industrial Control Systems Cybersecurity Week (FY2021).
- MNCERT/CC attended to an Interactive Virtual Training for Financial Institutions in Mongolia held by Mandiant on 13th - 16th December 2021.

5.2.2 Seminars & presentations

- MNCERT/CC attended to APCERT VIRTUAL AGM 2022.

6. Future Plans

6.1 Future Operations

MNCERT/CC planned the following activities in 2023.

Events, conferences, and drill to participate are as follows:

- APCERT Annual General Meeting 2023.
- APCERT Drill 2023.

Local activities to organize are as follows:

- MNSEC 2023 Cyber Security Event
- "Haruulzangi 2023" CTF Contest among security specialists
- "Haruulzangi U18 2023" CTF Contest among high school pupils
- Local cyber drill among member organizations
- Local training for our constituency.

7. Conclusion

After the covid-19 pandemic situation, 2022 was the year of coming back to in-person activities, building the security community in Mongolia.

We are looking forward the year 2023 to be a more progressive year in both local and international stage and greater collaboration with APCERT and other international organizations.

SingCERT

Singapore Computer Emergency Response Team

1. Highlights of 2022

The Singapore Computer 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 four initiatives aimed at promoting cybersecurity awareness and fostering a more secure cyberspace in 2022:

i. Internet Hygiene Portal

Provides visibility on the cyber hygiene of digital platforms and furnishes enterprises with easy access to resources and self-assessment tools.

ii. Cybersecurity Certification Programme

Recognises organisations with good cybersecurity practices.

iii. Inter-agency Counter Ransomware Task Force (CRTF) Report

Blueprint to drive Singapore's efforts to foster a resilient and secure cyber environment, domestically and internationally, to counter the growing ransomware threat.

iv. 6th Edition of Singapore Cyber Landscape

Highlights facts and figures on significant cyber threats and incidents in Singapore for 2021.

2. About SingCERT

2.1 Introduction

The Singapore Computer 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/Explore/who-we-are/our-identity/about-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.

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/Explore/who-we-are/our-identity/about-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/reporting>). 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 2022, SingCERT received reports of 4,649 incidents, a 6.27% decrease from the 4,960 incidents reported to SingCERT in 2021. This resulted in an average of 12.74 incidents per each business day of operation. 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	1,095	1,119	1,129	1,306	4,649

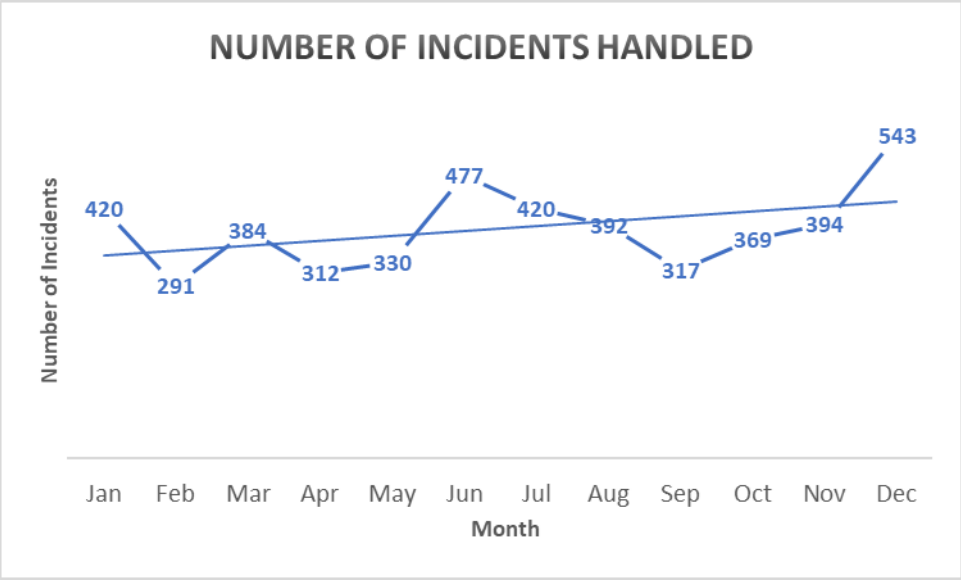


Figure 1: Number of Incidents Reported to SingCERT (2022)

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 2022, phishing was, once again, the most prevalent cyber threat that was reported to SingCERT in Singapore, comprising over 65% 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. In some cases, scammers even impersonated government bodies as well as high ranking government officials to conduct scams.

Cyber Incident Category	# Handled in 2021	# Handled in 2022
Phishing	3004	3060
Intrusion Attempt/Attack	823	576
Malware	614	641
Others	411	287
Vulnerability	108	85

Table 1: Breakup of Cyber Incidents handled (2021 vs 2022)

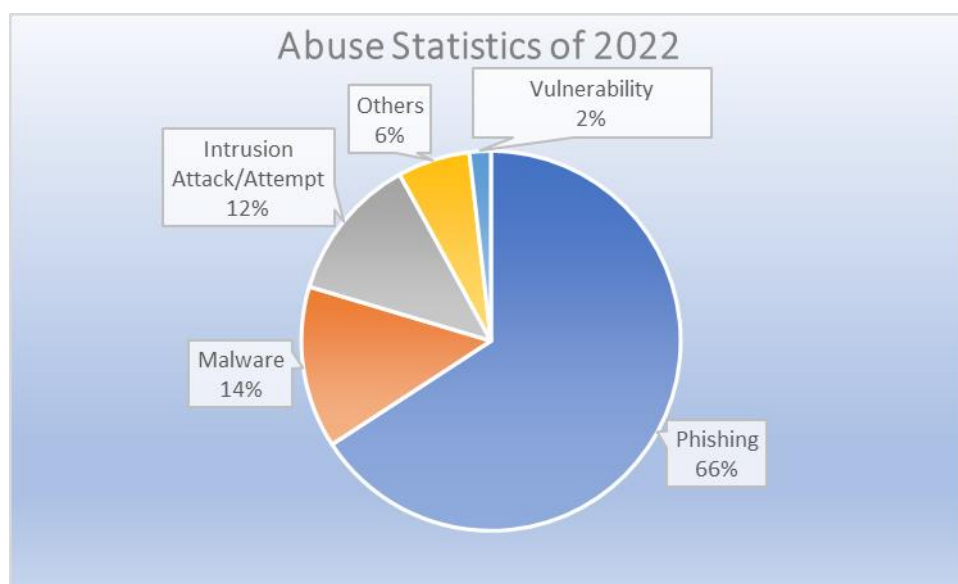


Figure 2: Abuse Statistics (2022)

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 2022, SingCERT published a total of 98 alerts and advisories, in addition to 52 Security Bulletins, on SingCERT's website. This represented a 20% increase from the 81 alerts and advisories published in 2021. The chart below shows the month-by-month comparison between 2021 and 2022.

	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Total
2021	8	6	9	10	5	3	11	6	8	6	5	4	81
2022	2	7	11	4	6	5	6	13	12	13	9	10	98

Table 2: Month-by-month comparison of Alerts and Advisories Published (2021 to 2022)



Figure 3: Comparing the Number of Alerts and Advisories Published (2021 to 2022)

Of the 98 alerts and advisories, 80 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 2022 are tabulated below:

Date	Title
10 Jan	Vulnerability in Apache HTTP Server
12 Jan	January 2022 Monthly Patch Release
9 Feb	February 2022 Monthly Patch Release
10 Feb	Critical Vulnerability in SAP Internet Communication Manager (ICM)
10 Feb	Critical Remote Code Execution Vulnerabilities in WordPress PHP Everywhere Plugin
11 Feb	Zero-Day Vulnerability in Apple iPhone, iPad, and Mac
14 Feb	Zero-Day Vulnerability in Adobe Commerce and Magento Open Source Platforms
23 Feb	Deadbolt Ransomware Attacks on Asustor NAS Devices
27 Feb	Strengthening Your Cybersecurity Posture Amidst Developments in the Russia-Ukraine Conflict

3 Mar	Critical Vulnerabilities in Cisco Expressway Series and Cisco TelePresence Video Communication Server (VCS) Products
7 Mar	Zero-Day Vulnerabilities in Firefox
8 Mar	Dirty Pipe Vulnerability in Linux Kernel
8 Mar	Increased Malicious and Scam Activity Exploiting the Russia-Ukraine Conflict
9 Mar	March 2022 Monthly Patch Release
18 Mar	High Severity Vulnerability in CRI-O
22 Mar	Protect your Organisation from Business Email Compromise
25 Mar	Protect your Industrial Control Systems' Safety Instrumented Systems
26 Mar	High-Severity Zero-Day Bug in Google Chrome
28 Mar	Critical Vulnerability in Sophos Firewall
31 Mar	Zero-Day Vulnerability in Spring Framework
4 Apr	Vulnerabilities in Rockwell Automation Logix Controllers
7 Apr	Multiple Critical Vulnerabilities in VMware Products
13 Apr	April 2022 Monthly Patch Release
26 Apr	Joint Advisory on Tech Support Scam
5 May	Critical Vulnerability in BIG-IP iControl REST
11 May	May 2022 Monthly Patch Release
14 May	Joint Advisory on Magniber Ransomware Distributed Through Fake Windows Operating System (OS) Updates
17 May	Zero-Day Vulnerability in Apple Products
19 May	Vulnerabilities in VMware Products
26 May	Protecting Your Website from Cyber-Attacks

1 Jun	"Follina" Microsoft Support Diagnostic Tool Vulnerability
3 Jun	Zero-day Remote Code Execution Vulnerability in Atlassian Confluence
15 Jun	June 2022 Monthly Patch
24 Jun	Importance of Using Strong Passwords, and Ways to Safeguard Your Passwords and Accounts
30 Jun	Increase in DDoS Activities Globally
5 Jul	SQL Injection Vulnerability in Django
6 Jul	Active Exploitation of Windows LSA Spoofing Vulnerability
13 Jul	July 2022 Monthly Patch
21 Jul	Unauthorised Access Vulnerabilities in Cisco Nexus Dashboard
21 Jul	Critical Vulnerability in Atlassian's Confluence Server and Confluence Data Center
28 Jul	Multiple Vulnerabilities in Samba
3 Aug	Critical Vulnerability in VMware Products
4 Aug	Critical Vulnerabilities in Cisco Products
4 Aug	Critical Vulnerability in DrayTek Routers
10 Aug	August 2022 Monthly Patch
10 Aug	Active Exploitation of Microsoft Windows Support Diagnostic Tool (MSDT) Vulnerability
10 Aug	Active Exploitation of RARLAB's UnRAR Vulnerability
11 Aug	Multiple Vulnerabilities in Device42 Asset Management Appliance
18 Aug	Zero-Day Vulnerabilities in Apple Products
18 Aug	Active Exploitation of High Severity Vulnerability in Google Chrome
19 Aug	Importance of Proper Segregation and Management of Enterprise Data

24 Aug	Critical Vulnerability in GitLab
24 Aug	Active Exploitation of Vulnerabilities in Apple, Google, Microsoft, Palo Alto and SAP products
29 Aug	Critical Vulnerability in Atlassian's Bitbucket Server and Data Center
3 Sep	Active Exploitation of High-Severity Vulnerability in Google Chrome
7 Sep	Critical Vulnerability in Zyxel NAS Products
9 Sep	Active Exploitation of Critical Vulnerabilities in D-Link Routers
13 Sep	New Shikitega Malware Targeting Linux Servers & Internet-of-Things (IoT) Devices
13 Sep	Active Exploitation of a Critical Vulnerability in Apple Products
14 Sep	September 2022 Monthly Patch
14 Sep	Active Exploitation of a Zero-Day Vulnerability in WPGateway Plugin
15 Sep	Multiple BIOS Vulnerabilities in Lenovo Products
21 Sep	Evolved ChromeLoader Malware Threat Targeting Chrome Browsers
26 Sep	Multiple Vulnerabilities in Sophos Firewall
28 Sep	Remote Code Execution Vulnerabilities in WhatsApp
30 Sep	Zero-day Vulnerabilities Affecting Microsoft Exchange Server
3 Oct	Specialised Malware Targeting Unsigned vSphere Installation Bundles (VIBs) in VMWare ESXi
4 Oct	Active Exploitation of Vulnerable Redis Servers
10 Oct	Critical Vulnerability in Fortinet Products
11 Oct	Critical Vulnerability in vm2 Sandbox
12 Oct	October 2022 Monthly Patch
13 Oct	Critical Vulnerabilities in Aruba EdgeConnect Enterprise Orchestrator

17 Oct	Active Exploitation of Critical Vulnerability in Zimbra Collaboration Suite
18 Oct	Critical Vulnerability in Apache Commons Text Library
19 Oct	Importance of Securing Your Application Programming Interface (API)
25 Oct	Active Exploitation of Zero-day Vulnerability in Apple Products
26 Oct	Critical Vulnerability in VMware Cloud Foundation
26 Oct	Critical Vulnerabilities in Cisco AnyConnect Secure Mobility Client for Windows
29 Oct	Active Exploitation of a Zero-day Vulnerability in Chrome Web Browser
2 Nov	High Severity Vulnerabilities in OpenSSL
2 Nov	Critical Vulnerability in ConnectWise Recover and R1Soft Server Backup Manager
4 Nov	Multiple Vulnerabilities in Splunk Enterprise Products
9 Nov	November 2022 Monthly Patch
9 Nov	Critical Vulnerabilities in VMware Workspace ONE Assist
9 Nov	Critical Vulnerability in Citrix ADC and Citrix Gateway
11 Nov	Vulnerabilities in Apple Products
23 Nov	Joint Advisory on the Distribution of Ransomware "Deadbolt" Targeting QNAP NAS Devices
26 Nov	Active Exploitation of a Zero-day Vulnerability in Chrome Web Browser
1 Dec	Protecting Yourself Against Telegram Scams and Securing your Telegram Account
2 Dec	Joint Advisory on Scams Targeting Year-End Online Shopping and Festivities
3 Dec	Active Exploitation of a Zero-day Vulnerability in Chrome Web Browser
6 Dec	Vulnerabilities in American Megatrends, Inc. MegaRAC Baseboard Management Controller software
8 Dec	Critical Vulnerabilities in Android Operating System

13 Dec	Critical Vulnerability in Fortinet's FortiOS
14 Dec	December 2022 Monthly Patch
14 Dec	Active Exploitation of Zero-day Vulnerability in Apple Products
14 Dec	Active Exploitation of Zero-day Vulnerability in Citrix ADC and Citrix Gateway
15 Dec	Vulnerabilities in VMWare Product

3.4.2 Internet Hygiene Portal (IHP)

The IHP is an initiative under the Singapore's Safer Cyberspace Masterplan 2020, serving as a one-stop platform for enterprises, providing them easy access to resources and self-assessment tools so that they can adopt internet security best practices in their digitalization journey. The IHP uses non-intrusive internet health lookup tools to assess the internet security of websites, email services and domain configuration before providing actionable suggestions on how enterprises can adopt best practices and improve their overall internet security. In doing so, internet security is simplified to key indicators that matter.

For consumers, the IHP also provides visibility on the cyber hygiene of digital platforms by publishing an Internet Hygiene Rating table with a simplified view of each digital platform's internet hygiene. This helps consumers make informed choices to better safeguard their digital transactions from cyber threats.

More information about the IHP is available via <https://ihp.csa.gov.sg>.

3.4.3 Cybersecurity Certification Programme

The cybersecurity certification programme for organisations developed by CSA recognizes organisations that have adopted and implemented good cybersecurity practices. The certification programme comprises two cybersecurity marks: Cyber Essentials and Cyber Trust. Cyber Essentials recognizes organisations that have put in place cyber hygiene measures. On the other hand, Cyber Trust is a mark of distinction that recognizes organisations with comprehensive cybersecurity measures and practices.

Both Cyber Essentials and Cyber Trust have different target organisations. Cyber Essentials targets Small and Medium Enterprises (SMEs), which typically have limited IT and/or cybersecurity expertise and resources, prioritize baseline security measures needed to safeguard their systems and operations from common cyber-attacks. Cyber Trust is targeted at larger corporations, such as MNCs, which tend to be more digitalized and need to make significant investments to manage and protect their IT infrastructure and systems.

These initiatives promote greater trust and transparency between organisations and their vendors and suppliers.

More information about the Cybersecurity Certification Programme is available via <https://www.csa.gov.sg/our-programmes/support-for-enterprises/sg-cyber-safe-programme/cybersecurity-certification-scheme-for-organisation>.

3.4.4 Inter-agency Counter Ransomware Task Force (CRTF) Report

The Counter Ransomware Task Force (CRTF) was set up to bring together Singapore Government agencies across relevant domains to strengthen Singapore's counter-ransomware efforts. The report released by the CRTF contains recommendations that serve as a blueprint to drive Singapore's efforts to foster a resilient and secure cyber environment, domestically and internationally, to counter the growing ransomware threat. The recommendations contained within the CRTF report are expected to be taken up by relevant Government agencies for further study and action.



Figure 4: Singapore's Counter Ransomware Task Force Report

More information about the Inter-agency CRTF report, including a downloadable copy, is available via <https://www.csa.gov.sg/News-Events/Press-Releases/2022/inter-agency-counter-ransomware-task-force-releases-report---a-blueprint-to-protect-singapore-from-ransomware-attacks>

3.4.5 Singapore Cyber Landscape 2021

The 6th edition of the Singapore Cyber Landscape publication was released on 29 Aug 2022. It reviews Singapore's cybersecurity situation in 2021 against the backdrop of global trends and events and highlights the nation's efforts in creating a safe and trustworthy cyberspace, such as initiatives to combat new and emerging cyber threats.

The publication provides an overview of the frequency and scope of cyber-attacks in Singapore, raising awareness of cyber threats among stakeholders, including the public and businesses so that they can take appropriate actions to defend against such threats.



Figure 5: Singapore Cyber Landscape 2021

More information about the publication, including a downloadable copy, is available via <https://www.csa.gov.sg/Tips-Resource/publications/2022/singapore-cyber-landscape-2021>

3.5 Drills & Exercises

3.5.1 ASEAN CERT Incident Drill 2022

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 27 October 2022, SingCERT successfully conducted the 17th iteration of ACID. Fifteen CERT teams from the ASEAN Member States (AMS) and ASEAN Dialogue Partners participated in the drill. The theme “Dealing with Disruptive Cyber-Attacks Arising from Exploitation of Vulnerabilities” was selected in light of the log4j vulnerabilities discovered in late 2021 which presented the potential for highly disruptive cyber-attacks due to the ubiquitous presence of its service. Participants were given a series of scenario injects that simulated an emerging triple extortion tactic employed by threat actors to extract a ransom from victim organisations. After the conclusion of the drill, participating CERTs feedbacked that the exercise was well-organized and helpful in providing incident response experience.

More information about ACID can be found via

<https://www.csa.gov.sg/News/News-Articles/2022/17th-iteration-of-asean-cert-incident-drill-tests-certs-preparedness-against-disruptive-cyber-attacks>

3.6 Conferences and seminars

3.6.1 Singapore International Cyber Week 2022

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, strategize and form partnerships in the cyberspace.

The 7th SICW was held from 18 to 20 October 2022, with the theme "Digital Security – A Shared Responsibility". The event aimed to sustain the momentum of conversations amongst top policy makers, industry leaders, top academia, and domain experts from ASEAN and across the world on key areas of cybersecurity, including emerging digital opportunities and threats, evolution of cyberspace and cybersecurity policies, implementation of cyber norms, Internet of Things (IoT) and Operational Technology (OT) security.

SICW 2022 continued to be held as a hybrid event with a series of inter-linked virtual meetings that allowed key leaders from governments, industry, academic and non-government organisations to explore the future of cyberspace cooperation from a broader range of perspectives. SICW successfully concluded with local and international attendees comprising a diverse mix of government officials, industry representatives, academics, and cybersecurity professionals.

3.6.2 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 organizations 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. International Collaboration

4.1 Training

SingCERT benefitted from the following APCERT training topics that were arranged by TWNCERT:

Date	Title	Presented by
8 Feb	Latest Trends on Keyword Hacks & SEO Spam	Sri Lanka CERT CC
12 Apr	Cyber Security Incident Reporting and Handling Scheme for Taiwanese Government Agencies	TWNCERT
21 Jun	FIRST's EPSS Scores for Vulnerabilities	AusCERT
6 Dec	Honeynet Data Analysis Through LebahNET	Cybersecurity Malaysia

4.2 Drills & Exercises

4.2.1 Asia Pacific Computer Response Team (APCERT) Cyber Security Drill 2022

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 25 August 2022 with the theme "Supply Chain Attack Through Spear-Phishing – Beware of Working from Home". The drill evaluates the response capabilities of member teams in responding to real incidents and issues that exist on the internet. 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.

4.2.2 ASEAN-Japan Cyber Exercise

The ASEAN-Japan Cyber Exercise seeks to continuously improve the capabilities and readiness for national coordination between ASEAN Member States (AMS) and Japan. CSA is a member of the ASEAN-Japan Cybersecurity Working Group which conducts two exercises annually, namely (a) the Remote Cyber Exercise, and (b) the Table Top Exercise. SingCERT participated in both the Remote Cyber Exercise conducted on 22-23 June 2022 and the Table Top Exercise held physically on 3 August 2022.

4.3 Conferences, Seminars & Presentations

4.3.1 Forum of Incident Response and Security Teams (FIRST)

The Forum of Incident Response and Security Teams (FIRST) is an organisation and recognized 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 Dublin, Ireland from 26 June – 1 July 2022, followed by the NatCSIRT meeting from 1 July – 2 July 2022.

4.3.2 APCERT Annual General Meeting (AGM) and Conference 2022

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) held on 18 October 2022 and the conference held on 19 October 2022. Both events continued to be held virtually due to the COVID-19 situation.

5. 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 work plan in the year 2023:

S/n	Description	Category
1	Singapore Cyber Landscape 2022	Publications
2	8 th Singapore International Cyber Week (SICW)	Events Organising & Hosting
3	18 th iteration of ASEAN CERT Incident Drill (ACID)	Events Organising & Hosting

Sri Lanka CERT|CC

Sri Lanka Computer Emergency Readiness Team | Coordination Centre

1. About Sri Lanka CERT|CC

1.1 Introduction

The Sri Lanka Computer Emergency Readiness Team | Coordination Centre (Sri Lanka CERT|CC) is the national centre for civilian cyber security in Sri Lanka, mandated to protect the nation's information infrastructure and to coordinate protective measures against, and respond to cyber security threats and vulnerabilities.

1.2 Establishment

As the national CERT of Sri Lanka, Sri Lanka CERT|CC acts as the central hub for the cyber security of the nation. It is the single trusted source of advice on the latest threats and vulnerabilities affecting computer systems and networks, and a source of expertise to assist the nation and member organizations, in responding to and recovering from Cyber-attacks. Sri Lanka CERT|CC was established on the 1st of July 2006 as a subsidiary of the Information and Communication Technology Agency of Sri Lanka (ICTA). ICTA is the Government Agency responsible for the development of IT Infrastructure and Policy in Sri Lanka. Thereafter, Sri Lanka CERT was made independent of ICTA in 2018 and was assigned to the Ministry of Digital Infrastructure and Information Technology. In the year 2019, Sri Lanka CERT was assigned to the Ministry of Defence and later reassigned to the Presidential Secretariat in October 2020. Currently, Sri Lanka CERT serves the Ministry of Technology under the purview of his excellency the President of Sri Lanka from 2021 onwards.

At the end of December 2022, the headcount comprised twenty-two (22) staff members. This included the Chief Executive Officer, Head of Research, Policy and Projects, Head of Human Resources and Administration, Chief Information Security Engineer, two Information Security Managers, three Lead Information Security Engineers, Senior Information Security Engineer, Information Security Engineer, five Associate Information Security Engineers, Program Manager, Project Manager, Admin & Account Assistant, three Call Centre officers, there were ten undergraduate interns assisting the operations. Eleven staff members were recruited during the year 2021.

All staff are highly skilled and experienced in different areas of information security and have achieved corresponding Information security certifications that are widely recognized in the industry, such as Microsoft MCSL, EC-Council

Certified Ethical Hacker (CEH) and Certified Hacking Forensics Investigator (CHFI), CISCO CCNA, CCSP, Red Hat Certified System Administrator (RHCSA), Red Hat Certified Engineer (RHCE), ISO 27001 Lead Auditor, ISO 27001 Lead Implementer, ISO 22301 Lead Auditor and Project Management Professional (PMP).

1.3 Constituency

Sri Lanka CERT|CC's constituency encompasses the non-defence cyber community of Sri Lanka (private and public-sector organizations, and the general public). Sri Lanka CERT|CC maintains a good rapport with the government and private sector establishments and extends assistance to the general public. In accordance with its mandate, Sri Lanka CERT | CC gives priority to requests for assistance from the government. Requests from the private sector are accommodated where possible.

2. Vision & Mission

2.1 Vision

"To be Sri Lanka's flagship organization and trusted source of advice on threats and vulnerabilities to Information Systems through proactive prevention and effective action."

2.2 Mission

- To be the single and the most trusted point of contact for Information Security in Sri Lanka.
- To protect Information Technology users in the Public and Private Sector Organizations and the General Public by providing up-to-date information on potential threats and vulnerabilities and by undertaking computer emergency response handling services.
- To act as the most authoritative national source for all ICT security-related issues across the nation.
- To link with other CERTS and CSIRTS around the world to share the knowledge and know-how relating to Information security.

3. Activities & Operations

3.1 Responsive Services

This service is triggered by events that are capable of causing adverse effects on constituents' Cyber Systems. Examples are Spam, Virus infections and unusual events detected by an Intrusion Detection System.

Sri Lanka CERT handles information security incidents. This service involves responding to a request or notification by a constituent on an unusual event that has been detected, which may affect the performance, availability or stability of the services or cyber systems belonging to that constituent.

3.2 Awareness Services

This service is designed to educate our constituents on the importance of information security and related topics ranging from information security fundamentals and best practices to recent issues, such as the latest cyber threats and attacks.

Alerts & Advisory

This service provides early warning signals to the constituents regarding Computer viruses, hoaxes, security vulnerabilities, exploits and other security issues, and where possible, provides short-term recommendations for dealing with the consequences of such attacks.

Currently, alerts are posted on Sri Lanka CERT | CC website. Constituents may also join the mailing list by subscribing to receive alerts via e-mail.

Seminars & Conferences

This service is provided with the intention of raising awareness about the most current information security issues, security standards and best practices. The aim is to help constituents significantly reduce the probability of being victims of a cyber-attack. Seminars can even be tailored to address specific information security-related issues through special requests.

Workshops

This service is aimed at increasing the constituents' awareness of information security. However, unlike seminars, these are more technically oriented and targeted at IT professionals, who perform daily tasks related to information security. Workshops will be arranged regularly, or on request, by Sri Lanka CERT | CC for its constituents addressing general topics. If desired, constituents may submit specific information security-related topics, so that the workshops are tailored to their needs.

Knowledge Base

The Knowledge Base is a passive service offered by Sri Lanka CERT | CC to interested constituents through documents, articles, news items, etc. published on the Sri Lanka CERT | CC website and the media. The aim of this service is to provide a range of knowledge resources to the constituency, enabling anyone from a home user to an IT professional to find useful information to help boost their understanding of information security.

3.3 Consultancy Services

This service is aimed at providing constituents with means of determining the adequacy of their information security systems and taking necessary steps to strengthen their defenses.

Technical Assessments

This service is aimed at reviewing and analyzing the security infrastructure and procedures adopted within an organization based on the experience of Sri Lanka CERT | CC's information security Team and certain predefined parameters. The end result is a detailed report on the weaknesses of the client organization's current ICT infrastructure, where improvements need to be made and how such improvements should be implemented.

Advisory for National Policy

As the primary authority on information security in Sri Lanka, Sri Lanka CERT | CC is responsible for developing, introducing and enforcing information security standards to its constituents.

3.4 Managed Services

Sri Lanka CERT | CC's managed security services offering is designed to strengthen the security posture of the organisation or business by providing the expertise and support that is needed to detect, prevent and remediate any cybersecurity-related threats to your IT infrastructure.

Vulnerability Assessments

Sri Lanka CERT | CC's vulnerability assessment service helps an organization improve its security posture by identifying vulnerabilities before they become security incidents. Our experts use a proven combination of industry tools, best practices and in-house techniques to probe the network/ devices for vulnerabilities and hence identify potential areas of risk.

Penetration Testing

Sri Lanka CERT | CC provides an internal and/or external penetration testing service that involves simulating real-world attacks to provide a current view of vulnerabilities and threats to the client's network infrastructure.

These assessments begin with a discovery process to develop a baseline profile of accessible services, ports and systems as targets for further internal or external penetration testing.

The process involves an in-depth analysis including manual probing to:

- Test identified components to gain access to the networks
- Network devices such as firewalls, routers, and switches
- Network services such as web, DNS, email, FTP, etc.
- Determine possible impact or extent of access by attempting to exploit vulnerabilities

A detailed report is provided with findings and recommendations

System Hardening

The purpose of system hardening is to eliminate as many security risks as possible. This is typically done by assessing the systems against the security best practices. There may be continuous changes to the information systems of the organization. As a result, it may introduce new vulnerabilities due to misconfiguration, and/or unnecessary software/services etc. A detailed report will be provided with findings and recommendations.

On-site and off-site consultation

This service mainly focuses on incident response. The main purpose of this service is to ensure that the client is not unduly burdened with day-to-day information security-related incidents.

- Over-the-phone consultancy
- On-site incident handling
- Timely response and mitigation to incidents occurring at customer premises
- Review of security policies and processes

3.5 Digital Forensics Investigations

Sri Lanka CERT | CC digital forensics team has been offering the service since the year 2010 and has well-experienced digital forensics investigators. Sri Lanka CERT|CC is equipped with globally acceptable tools and adheres to globally recognized digital forensics procedures.

Furthermore, Sri Lanka CERT | CC conducts digital forensics training programs and technical workshops for both local and international audiences. Sri Lanka CERT | CC has successfully conducted tailor-made digital forensics training programs for public and private sector organizations based on client requirements.

3.6 Research & Policy Development

Sri Lanka CERT | CC Research and Policy Development division was established with the intention of:

- Developing strategies and formulating policies related to information security and cyber security for the nation
- Conducting national-level surveys on the various domains related to information and cyber security
- Coordinating special national projects related to information security and cyber security.

4. Operational Performance (Routine Responsibilities & Projects)

4.1 Incident Handling Summary

Sri Lanka CERT|CC being the national contact point for all cybersecurity-related matters receives numerous incident reports/complaints relating to the country's national cyber-space from both domestic and international partners.

The types of incidents received by Sri Lanka CERT include incidents related to social networks, email compromise, phishing, website compromise, scams, malicious software issues and ransomware, privacy violations, financial frauds, compromised unique IPs extracted from the information collected by automated systems operated by international organizations. The majority of the reported incidents fall into the category of social media-related incidents and on average more than 1250 cases are reported each month. Among the social media incidents, Facebook incidents were the highest. Apart from that there is a notifiable increase in the number of reported scam incidents compared to the last year 2021

Table 1 depicts the distribution of various types of incidents reported to Sri Lanka CERT in the year 2022. All the incidents reported to Sri Lanka CERT have been resolved satisfactorily.

Incident Type	Number of Incidents in 2022
DDOS	4
Ransomware	67
Abuse/Hate/Privacy violations	181
Malicious Software issues	17
Phone Hacking	114
Scams	1427
Phishing	48
Website Compromise	261

Table 1: Number of reported incidents in the year 2022

4.2 Consultancy Services

Sri Lanka CERT continues to provide consultancy services in response to requests made by both the public and private sectors.

4.3 Information Security Managed Services

Sri Lanka CERT was able to deliver the following security-managed services;

- External penetration testing
- Internal penetration testing
- Device configuration reviews
- Network architecture reviews
- Application security assessments
- Server OS configuration reviews

4.4 Application Security Audits

Sri Lanka CERT performed Web and Mobile Application Security Audits was performed throughout the year. Continuous monitoring of web applications was conducted in order to identify potential cyber-attacks.

4.5 Digital Forensics

Sri Lanka CERT|CC has completed over sixteen digital forensic investigations of counterfeit payment devices over the last year. Our investigators have appeared in the courts to provide expert testimonies and provided expertise for law enforcement officers on identifying and seizing digital devices.

Sri Lanka CERT|CC also successfully completed several digital forensic investigations and Business Email compromise incidents for the private sector and facilitated our experts for their cooperate investigations.

4.6 Training / Education Services

In order to fulfil its mandate to create awareness and build Information Security skills within the constituency; Sri Lanka CERT continued to organize training programs and education sessions targeting various audiences including CIOs, Engineers, System Administrators, Banking and Telecom Sector Staff, Students, and General Public.

4.6.1 Awareness Program and Training Sessions

Sri Lanka CERT conducted the following training and awareness programs:

- General Cyber Security Awareness sessions for:
- Members of the Internet Society Sri Lanka
- Students of the Master of Public Management program - Sri Lanka Development Administration
- Defence Ministry (Office of Chief of Defence Staff)
- Hayleys Group

- Vidura International College
- Lions International Club - Athurugiriya and Kaduwela Youth Cub
- Uva Province - Parents and School children
- SLAS Officers
- Sri Lankan judicial officers (judges and high court judges)
- Ministry of Fisheries
- Sri Lanka Ports Authority
- Ruwanpura Vidyapeetaya
- Ruwanwella Rajasinghe Vidyalyaya
- Open-source Intelligence Analysis & Email Header Analysis for Sri Lanka Police - Criminal Investigation Department
- Digital data protection and crime scene protection for Sri Lanka Police - Criminal Investigation Department
- Internet-related complaints handling for Sri Lanka Police - Criminal Investigation Department
- Windows Forensics Investigation for Members of ISACA Sri Lanka Chapter
- Webinar on Business Email Compromise
- Awareness of Suicide Prevention - Impact of Digital Media for Sumithrayo
- Awareness session on Information Systems Auditing for Department of Management Audit - Treasury
- Workshop on Implementation of the Information and Cyber Security Policy for Senior Government Officers
- Awareness sessions at ICTA, DigitalGovActivation Forum
- Awareness session on Information and Cyber Security Policy for Senior Government Officers for IT staff of Sri Lanka Parliament
- Session on "Open Source Threat Intelligence" for Katana Police Academy
- Session on "Digital Forensic Procedures" for the Bar Association of Sri Lanka
- Workshop for CNII Operators on the Implementation of the Information Security Policy – In collaboration with Cyber4Dev

4.6.2 Awareness through Electronic/Print Media

Sri Lanka CERT|CC provided information for 7 newspaper articles during the year 2022. Furthermore, 11 voice cuts for radio programs and recorded content for 03 Television programs were provided. Sri Lanka CERT|CC issued 4 Media press releases which were published on both social media as well as official websites.

4.6.3 Security Alerts

- An Average of 1300 compromised IPs per month were informed to ISPs.
- 12 critical security alerts were published and sent to subscribers.

4.7 Publications

Website

The Sri Lanka CERT website publishes security-related awareness bulletins for the public via News Alerts and a Knowledge Base. Glossaries, case studies and FAQs are among some of the other published items.

E-mails

Disseminating security-related information via e-mail alerts to Sri Lanka CERT website subscribers.

Newsletters

Sri Lanka CERT|CC publishes and circulates the Cyber Guardian e-newsletter to a large number of students, through the 'SchoolNet' - the network connecting secondary schools in Sri Lanka.

Newspapers/media

Sri Lanka CERT continues to educate the general public through the electronic and print media about emerging cyber security threats and vulnerabilities with recommendations on how to safeguard against these attacks.

4.8 Infrastructure Development & Staff Capacity Building

4.8.1 Staff Capacity Building – International Initiatives

- Training conducted by Cyber4Dev
- Session on IT Risk Assessment
- Session on Development of M & E Framework
- CSIRT essential training for new NSCOC employees
- Workshop on Crisis Management and National Level Disaster Recovery Framework
- Session on Impact and severity assessment framework
- Training on creating organisation ISMS
- SIM3 Implementation Training
- Sri Lanka CERT staff members had the opportunity to participate in and represent Sri Lanka for the following training/ seminars/conferences as well.
- MWC2022 Barcelona
- African Cyber Security Resilience Conference
- The Role of the EU Cyber Ecosystem in Global Cybersecurity Stability, Brussels
- First Conference 2022, Ireland
- Study visits and Meetings with the Estonian Information System Authority
- 7th Singapore International Cyber Week (SICW) 2022

4.9 National Projects

Project Name	Project Status (Simple Description)
National Cyber Security Operations Center for real-time monitoring of cyber security incidents	Delivery of threat intelligence report to ISPs on a weekly basis Real-time monitoring of websites (availability of websites) - 500+ Website Security monitoring of selected websites through Open Source SIEM tools
Implementation of the National Certification Authority of Sri Lanka to issue certificates for Certificate Service Providers	Certificate Revocation List (CRL) was generated. The first CSR was signed with LankaPay.
National Surveys on Citizens' awareness of Information and Cyber Security	The pilot survey is completed
Development of a Web Portal to increase citizens' awareness of cyber security (www.onlinesafety.lk)	The tri-lingual web portal is in operation.
Development of National Vocational Qualification (NVQ) Standard for Information and Cyber Security	NVQ Level 6 (National Diploma) on Information and Cyber Security Technology was developed.

Table 2: National Projects

5. Achievements

5.1 Information and Cyber Security Policy for Government

Organizations

Cabinet approval was received to implement the Information and Cyber Security Policy in government organizations.

5.2 Memberships

Sri Lanka CERT continues to maintain memberships with the following professional organizations;

- (ISC)2 Colombo Sri Lanka Chapter is the local representative organization of the International Information Systems Security Certification Consortium.
- Membership for Threat Intelligence from ShadowServer.
- Membership of FIRST

- Membership of APCERT
- Membership of CAMP, Korea
- Membership of TF-CSIRT

6. International Collaboration

6.1 CAMP

- Actively Participated in CAMP Operations Committee(OC) meetings
- Leading processes and procedures relevant to the membership component in CAMP OC
- Participated in many online and offline discussions on CAMP AGM 2022
- Delivered a presentation for CAMP AGM 2022 on the topic 'Cyber Security Status of Sri Lanka'
- Participated in CAMP AGM 2022 (both online and offline)
- Participated in six GCCD cyber security webinars and a 3-day workshop (online)

6.2 APCERT

- Participated in APCERT steering committee meetings
- Continuing with the network monitoring project "Tsubame" with JPCERT|CC
- Organized and conducted meetings with the working group members as the Convener of the APCERT working group – Critical Infrastructure Protection. The working group successfully completed its tasks and produced a report on "Best practices for protecting ICS"
- Participated in APCERT working group teleconferences- Policy and Planning, Membership
- Lead the APCERT cyber drill 2022 working group discussions and its activities
- Organized and Participated in APCERT cyber drill 2022
- Participated in APCERT AGM Program Committee Meeting
- APCERT AGM and Conference 2022 (Teleconference)
- Presented the progress of the Critical Infrastructure Protection working group at the AGM
- Presented the status summary of the APCERT cyber drill 2022
- Contributed to several APCERT working groups
- Won the APCERT Best Contributor Award 2022

7. Future Plans

7.1 Future Projects to be Implemented

- Implementation of Information and Cyber Security Policy in the government organizations
- Drafting of the next version of the National Information and Cyber Security Strategy
- Establishment of a Sectoral CERT for the Education Sector (EduCERT)
- Information and Cyber Security Risk Assessment for Critical Information Infrastructure Providers

8. Conclusion

The year 2022 was a successful year as Sri Lanka CERT was able to receive Cabinet of Ministers approval for the Information and Cyber Security Policy for government organizations. Further Sri Lanka CERT was able to win the APCERT Best Contributor Award 2022.

The National Certification Authority has signed the first CSR for its first Certification Service Provider. Sri Lanka CERT carried out a considerable number of awareness sessions and workshops targeting government and private sector organizations and the general public etc.

Further, the preliminary processes have been initiated to draft the next National Information and Cyber Security Strategy. The implementation of the Information and Cyber Security Policy for government organizations is considered to be a top priority in the year 2023. The initial plans are in place for the successful and smooth rollout of the activities of the year 2023.

Therefore, Sri Lanka CERT believes that the organization is well-positioned to build on its success in the coming year 2023.

TechCERT

TechCERT

1. About TechCERT

TechCERT, Sri Lanka's first and largest Computer Emergency Readiness Team (CERT) helps the general public and Sri Lankan organizations keep their computer systems and networks secure. TechCERT celebrated 16 years of excellence on the 01st of September 2022. Originating as a pioneering project of the LK Domain Registry - it's now academic partner, TechCERT's goal is to provide a safety net for external entities, from the general public to large corporations against cyber-attacks and cyber emergency situations.

TechCERT has collaborative partnerships with several national and global information security organizations, such as APCERT that provide the latest data on computer and network security threats and vulnerabilities. TechCERT also works closely with these organizations on handling cyber security incidents that require multinational support. Issuing security advisories to the public, conducting security/cyber-crime related workshops and public awareness programs on safe use of computers and the internet, and providing engineering consultancy services are a few more items in its repertoire of services.

TechCERT, as a leader in providing Cyber Security Services, works with its members to develop and implement customized and fully integrated IT security technologies and services across a wide range of IT infrastructures. We provide a high quality of service by using not only industry standard systems and software, but even more importantly, our qualified and experienced staff of full-time security experts who are active in the security community.

1.1 Establishment

TechCERT was originally founded in 2006 and has its origins as a pioneering project of the LK Domain Registry and its academic partners, it seeks to provide a way of providing a safety net for large and small organizations against cyber-attacks and emergency situations. To improve its operations and to further develop TechCERT, it was incorporated as an independent not-for-profit organization, affiliated with LK Domain Registry, on 05th September 2016 (Company registration no. GA 3238)

1.2 Resources

TechCERT currently has a technical team of over 30 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 Deift), MPhil (Moratuwa), MCS (SL), BSc Eng (Hons) (Moratuwa), IET (UK), MIE (SL), CEng
Dileepa Lathsara	Chief Executive Officer	MSc, BSc Eng (Hons), CISSP, C EH, CEng, MIE(SL), BCS(UK), ACS(Aus), Certified ISMS Auditor (ISO27001), CPISI (PCI DSS V3)
Kushan Sharma	Chief Operating 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	Principal Engineer	MSc in Information Systems Security (Moratuwa), BSc Eng. (Hons) in Electrical Engineering, MIEEE, AMIE (SL)
Nalinda Herath	Principal Engineer	MSc in Information Systems Security (Moratuwa), BSc Eng. (Hons) in Computer Science & Engineering, ISO 27001 Lead Auditor, C EH, CCNA (Security), CCNA (Network), CPISI, ITIL, AMIE (SL)
Kalana Guniyangoda	Principal Engineer	MSc in Computer & Network Security (Moratuwa), BSc IT (Hons), GCFA
Geethika Wijerathne	Senior Manager - HR & Administration	MSc in Information Systems Management (UOC), PMP, PGDip in ISM (UOC)
Mishra De Silva	Head of Enterprise Business	MBA (Colombo), BBA (U.S.A), AS (U.S.A), MSLIM, CIMA Adv. Dip. MA
Vijan Herath	Project Manager	BSc in Computer Science, HND in Computing (UK), ORACLE HCM (Cert), Project Management & SCRUM Immersion (Cert), CPISI (PCI DSS V3.2.1)
Chathuranga Gunatillake	Lead Security Engineer	MSc Information Security (UCSC), BEng (Hons) Computer Networks & Security, MBCS, E NSA, C EH, CPISI (PCI DSS V3.2), ISO/IEC 27001 Lead Auditor, C HFI
Radheesha Bandara	Associate Lead	Master of Information Security (UCSC), BSc in Computer Systems &

	Security Engineer	Networking, RHCSA, CCSE, CCSA, CCNA – Routing & Switching, CCNA - Security, OCI Architect (Professional)
Milinda Wickramasinghe	Senior Information Security Engineer	MSc in Cyber Security (SLIIT), LLM in Intellectual Property & IT (Cardiff), BICT (UCSC), ISO 27001 LA, C EH, CPISI (PCI DSS v4.0), MCSSL
Ayodya Balasuriya	Senior Information Security Analyst	BSc in Information Systems, CPISI (PCI DSS V3.2), LLB(Hons)
Chalana Madusanka	Associate Lead Security Engineer	BSc Eng. (Hons) in Computer Engineering, AMIE (SL)
Hirushan Thilanka	Information Security Engineer	Master of Information Security (UCSC), BSc in Information Systems (UCSC)
Pubudu Ranasinghe	Information Security Engineer	BSc (Hons) Information Technology (Sp. Cyber Security) - SLIIT, RHCSA (Red Hat 8.0)
Nisal Priyanka	Information Security Engineer	BSc (Hons) Information Technology (Sp. Cyber Security) - SLIIT, PGD in Cyber Security, MSc in Cyber Security
Akalanka Perera	Information Security Engineer	BSc (Hons) in IT Specialized in Cyber Security
Chamitha Gunawardena	Information Security Engineer	BSc (Hons) Information Technology (Sp. Cyber Security) - SLIIT, CPISI (PCI DSS V3.2)
Dushyantha Pathirathna	Information Security Engineer	BSc (Hons) Information Technology (Sp. Cyber Security) - SLIIT
Lalindra Perera	Associate Information Security Engineer	BSc (Hons) Information Security, MSc Cyber Security and Forensics - Reading
Dinidhu Jayasinghe	Associate Information Security Engineer	BSc (Hons) Information Technology (Sp. Cyber Security) - SLIIT
Udeshika N. Alupotha	Information Security Engineer	BSc (Hons) Information Technology (Sp. Cyber Security) - SLIIT, MSc Information Security (UoC) - Reading
Sudeepa Shiranthaka	Associate Information Security Engineer	BSc (Hons) Information Technology (Sp. Cyber Security) - SLIIT
Kavindu Viraj Rathnayake	Associate Information Security Engineer	BSc (Hons) Information Technology (Sp. Cyber Security) - SLIIT
Shanuka Ashen Karunadasa	Associate Information Security Engineer	Undergraduate - BSc (Hons) Information Technology (Sp. Cyber Security) - SLIIT
Anjana Kawshan	Trainee Information	Undergraduate - BSc (Hons) Information Technology (Sp. Cyber

	Security Engineer	Security) - SLIIT
Lasitha Bandara	Trainee Information Security Engineer	Undergraduate - BSc (Hons) Information Technology (Sp. Cyber Security) - SLIIT
Kawya Nayanathara	Trainee Information Security Engineer	Undergraduate - BSc (Hons) Information Technology (Sp. Cyber Security) - SLIIT
Amal Hewagama	Information Security Engineer	BCS PGD, PGD in networking (NSBM), MBA sp. project management (Cardiff Metropolitan), MSc in cybersecurity (SLIIT) -reading
Arun Viraj Poobalan	Information Security Analyst	BSc (Hons) Information Technology (Sp. Cyber Security) - SLIIT, ISO 27001:2013 Lead Auditor
Priyasuthan Pushparajah	Associate Information Security Engineer	Undergraduate - BSc (Hons) Information Technology (Sp. Cyber Security) - SLIIT

1.3 Constituency

TechCERT's constituency comprises its member organizations, private sector organizations, selected government organizations and the general 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.

2. Highlights of Year 2022

The 1st of September 2022 marked the 16th anniversary of TechCERT. TechCERT was able to maintain a consistent delivery of services despite the ongoing economic crisis in Sri Lanka. To provide its employees a relief during the period of fuel scarcity and skyrocketing cost of living, TechCERT continued delivering services remotely. After the situation reverted to normal conditions, TechCERT switched to a hybrid mode of work. With the resilient support of its skilled and dedicated team members, TechCERT continued to secure major cyber security projects of leading corporates while competing with global brands. Below are few of the major activities that could be successfully completed during the year 2022.

TechCERT Cyber Security Drill:

Conducted 03 Cyber Security Drills for Banking, Financial, Telecommunication, Manufacturing sector organizations and Large Conglomerates.

- TechCERT Cyber Security Drill for Financial Sector organizations was conducted on 22nd of September 2022.
- TechCERT Cyber Security Drill for Banking Sector organizations was conducted on 20th of October 2022.

- TechCERT Cyber Security Drill for Telecommunications Sector and Other Sectorial organizations was conducted on 24th of November 2022.

TechCERT Annual Cyber Security Training and Awareness Session:

The TechCERT annual training was conducted through a series of in-person seminars for a set number of participants from each of TechCERT's Managed Security Services clients.

- TechCERT annual training 2022:
- Strengthening the Security Posture
- Dashing Through the Application Layer
- Incident Response with TechCERT
- TechCERT Cyber Security Drill 2022 – Finance Sector
- TechCERT Cyber Security Drill 2022 – Telecommunications Sector and Other Sectors
- TechCERT Cyber Security Drill 2022 – Banking Sector

SWIFT Customer Security Program Independent Reviews:

TechCERT continued the independent security reviews aligning with the SWIFT customer security program, while building upon and refining the process with experience from the previous year. Four major banks in Sri Lanka engaged with TechCERT to conduct independent reviews during the year 2022.

Security Assessments & Incident Responses:

Conducted more than 7000 Security Assessments on various IT infrastructures and responded to more than 300 Cyber Security incidents.

3. Activities & Operations

3.1 Scope and definitions

Customers can choose from a large repertoire of services ranging from Digital Forensics Investigations to Penetration tests to Web and Server Security Assessments and more. TechCERT's Managed Security Services include a range of engineering and consultancy services listed 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
- Network & Security Architecture Review
- Operation Security Assessment
- PCI DSS Certification & Consultancy
- Penetration Testing
- 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 Risk Assessment
- Server Security Configuration Evaluation
- SWIFT Security Audit
- Threat Hunting
- Training and Awareness
- Vulnerability Assessment
- Web Application Security Assessment
- Wireless Security Assessment

3.2 Security Assessment

Statistics related to the security assessments conducted by TechCERT during the year 2022 are given below:

Assessment Type	Count
External Vulnerability Assessments	3560
Internal Vulnerability Assessments	3215

Web-based Security Vulnerability Assessments	1407
Firewall Rule Review and Security Assessments	144
Other Assessments (DF investigations, Wireless, Network, etc.)	650

Table 3 Number of Conducted Security Assessments

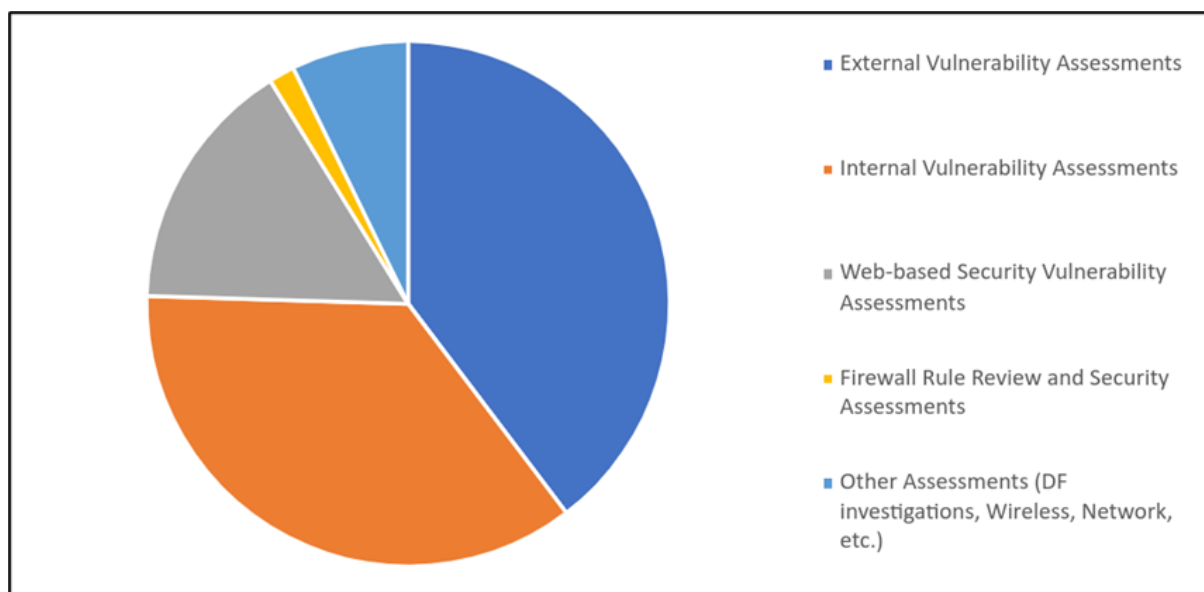


Figure 1 Number of Conducted Security Assessments

3.3 Incident handling

A broad range of entities reported Cyber Security incidents to TechCERT during the year 2022, including clients from the Banking sector, Finance sector, General Public and Corporations. The following are statistics related to the Cyber Security Incidents that were received by TechCERT in the year 2022:

Activity Type	Count
Server security compromises	190
Malware infections	176
Ransomware related incidents	92
Social network related incidents	32
Phishing incidents	15
Other incident responses	125

Table 4 Number of Responded Incidents

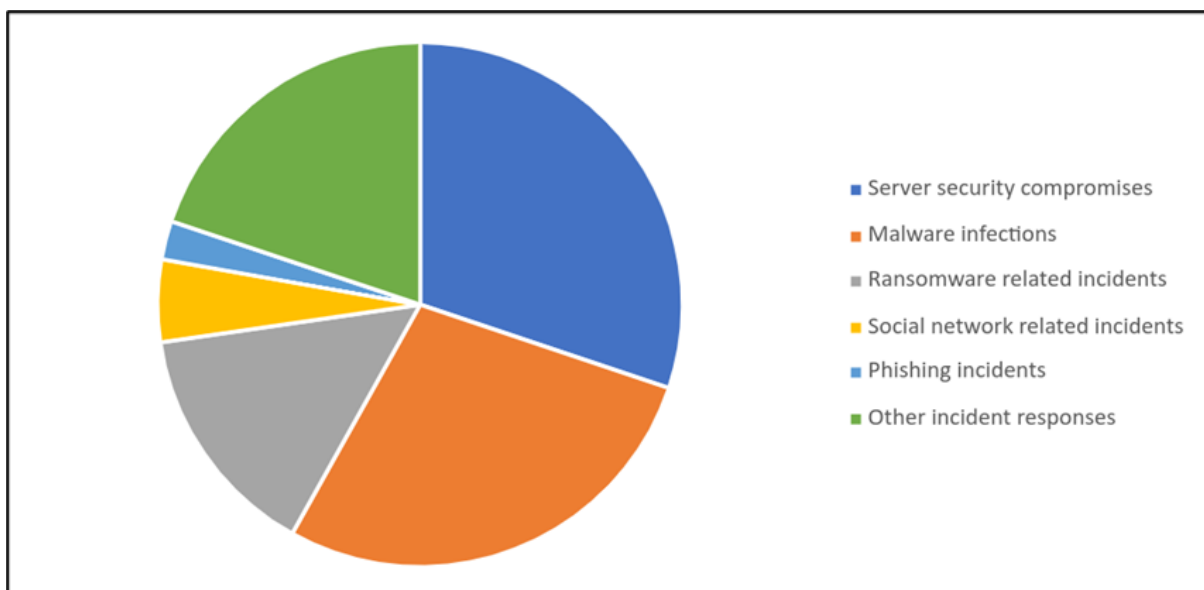


Figure 2 Number of Responded Incidents

3.4 Abuse statistics

Server compromise, Malware infections and Ransomware related incidents are some of the most serious and abundant cyber threats in Sri Lanka. The most consistent and common type of Cyber Security incident observed in 2022 was Server Security Compromises.

3.5 TechCERT New services

Listed below are services commenced by TechCERT in 2022:

- Assumed Breach Assessment
- Cyber Security Posture Assessment
- Cyber Security Strategy Development
- Digital Attack Surface Review Assessment
- Digital Forensic Readiness Review
- Review of Cyber Security Incident Management

4. Events organized / hosted

4.1 Training

In 2022, TechCERT conducted a number of training sessions for its member organizations and other customers. The trainings were conducted in-person. Given below is a list of training sessions conducted:

TechCERT annual training 2022:

- Strengthening the Security Posture
- Dashing Through the Application Layer
- Incident Response with TechCERT

4.2 Cyber Security Drills

In addition to being a proven method of spreading knowledge among customers and members of TechCERT, it also serves the important purpose of creating an effective means of grading each candidate on their pre-existing experience and expertise. Listed below are the drills that were hosted by TechCERT in 2022:

- TechCERT Cyber Security Drill 2022 – Finance Sector
- TechCERT Cyber Security Drill 2022 – Telecommunications Sector and Other Sectors
- TechCERT Cyber Security Drill 2022 – Banking Sector

4.3 Conferences and seminars

TechCERT upholds an active position in the local and international arena by partaking in various Conferences and/or Seminars. On occasion, team members of TechCERT who are experts in certain fields will speak at/coordinate these events. In 2022, TechCERT conducted a virtual seminar for the University of Moratuwa.

- Roadmap to a Secure Website – August 2022

5. International Collaboration

Collaboration with the Internet Assigned Numbers Authority (IANA) during 2022:

- Mr. Dileepa Lathsara was selected to become one of the IANA Crypto Officers. His duty involves key aspects of managing the Root Zone Key Signing Key of DNSSEC.

6. Capacity building

TechCERT greatly values the contribution its employees provide, and as such seeks to enhance their knowledge both for the betterment of TechCERT and their own professional development. Mentioned in the following sections are the efforts taken by TechCERT to furthering this goal in the year 2022.

6.1 Training

TechCERT enlisted its workforce in a number of external and internal training sessions to enhance the skill set of said workforce. Mentioned below is the list of training sessions undergone by TechCERT employees:

- TechCERT - SISA - 355th CPISI- PCI DSS v4.0 Implementation e-Workshop – April
- Internal Training workshops on subjects such as:
- Firewall Security Assessment
- Mobile Application Security
- API Security
- Wireless Security Assessment

6.2 Drills & exercises

To fortify its own employee's collective knowledge, TechCERT participated in the annual APCERT Cyber Drill as follows:

- APCERT Cyber Drill 2022: Data Breach through Security Malpractice

7. Future Plans

7.1 Future projects and operation

The past year contained a multitude of challenges brought on by the economic crisis and the residual effects of the COVID 19 Pandemic. Most professionals postulate, that a few years will have to pass before the economy of Sri Lanka can recover. It must be accepted that conditions will be harsh until this period passes. Despite this, TechCERT has set forth a number of ambitions it hopes to achieve in the near future.

- Continue providing assistance and awareness to the citizens of the country on the ever-rising stream of cyber security threats.
- Promote the advancement of the overall information security posture of our member organizations
- Advance the nature and content of training sessions conducted by TechCERT.
- Introducing new services such as Security Posture Assessments to the local sphere.

- Increase interaction with fellow cyber security organizations in the international sphere.
- Strengthen the team at TechCERT and enable them to garner new skills and talents.

8. Conclusion

In 2022, TechCERT responded promptly and effectively to constantly evolving cyber threats in Sri Lanka. These included a high number of compromised servers and malware infections. TechCERT remains confident in its ability to assist its customers during information security emergencies and has a clear plan in place to further develop and strengthen its workforce. This includes providing external training and workshops, acquiring advanced tools and equipment, and fostering global collaboration. With its talented and skilled workforce, and its commitment to consistent quality of service, customers of TechCERT can be assured of receiving nothing but excellence.

In conclusion, 2022 was a year of significant challenges for the local environment, with the Pandemic and Economic Crisis leading to fuel shortages, power outages, and police curfews. Despite these difficulties, TechCERT remained committed to the wellbeing of its employees by implementing a primarily remote work model. TechCERT also made progress in improving its core capabilities and fulfilling its role as a CERT. With the expansion of its workforce, TechCERT is poised to continue growing and exploring new opportunities in the future.

ThaiCERT

Thailand Computer Emergency Response Team

1. About CSIRT

1.1 Introduction and Establishment

Founded in 2000, ThaiCERT, a non-profit government funded organization, is the Computer Security Incident Response Team (CSIRT) for Thailand, providing an official point of contact for dealing with computer security incidents in the Internet Community of Thailand. Apart from coordination and handling the reported incidents, ThaiCERT also provides an advisory service to both organizations and individuals, releasing cybersecurity alerts and news, and organizes academic trainings for the public to enhance knowledge and to raise awareness to people on information security. With the increase of security incidents in the Internet Community of Thailand, ThaiCERT expanded its service not only to the governmental units but to the private organizations as well. Currently, ThaiCERT is an operational security organization under the public organization Electronic Transactions Development Agency (ETDA), which falls under the supervision of the Ministry of Digital Economy & Society, Thailand.

1.2 Constituency

The constituents of ThaiCERT are all public, private and home sectors of Internet users in Thailand. ThaiCERT also provides the incident coordination service to other international entities, where the sources of attacks originate from Thailand.

2. Activities & Operations

2.1 Incident handling reports

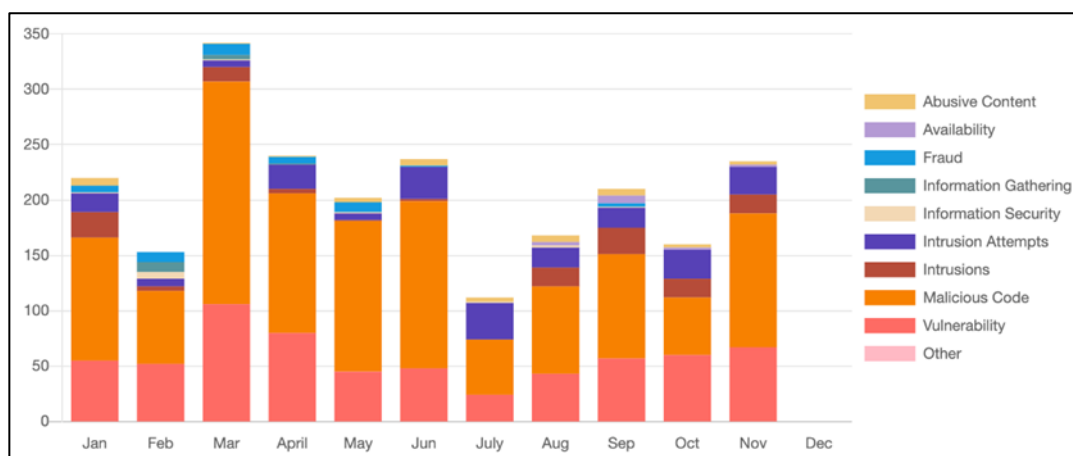


Figure 1: The proportion of reported incidents by incident type in 2022
(Due to data processing issue, we exclude statistics of December.)

Via triage, ThaiCERT handled a total of 2,279 reported incident cases (tickets) in 2022. According to the reported incidents in 2022, classified by the eCSIRT incident classification, Malicious Code dominated with 52%, followed by Vulnerabilities at 28% and Intrusion Attempt at 9%. All such information was handled and notified to the relevant parties through e-mail channels.

3. Events organized / hosted

3.1 Training

Organized:

- AJCCBC Trainings, Jan, Feb, May, Jun, Aug, Oct, and Dec 2022
- Cyber SEA Game, Nov 2022

Trainer:

- APCERT Training: Cyber Threat Intelligence on a national level, Aug 2022
- 2022 APISC Security Training Course, Aug 2022

3.2 Drills, exercises

Participated:

- APCERT Drill 2022, Aug 2022
- ASEAN-Japan Table Top Exercise 2022, Aug 2022

3.3 Conferences and seminars

Participated:

- 21st Annual AusCERT Information Security Conference, May 2022
- APCERT AGM & Conference 2022, Oct 2022
- FIRST-APCERT Regional Symposium for Asia-Pacific Region, Oct 2022
- APISC 2022 Special Seminar, Nov 2022
- 2022 Global Conference on CNCERT International Partnership, Dec 2022

TWCERT/CC

Taiwan Computer Emergency Response Team / Coordination Center

1. Highlights of 2022

1.1 Summary of major activities

In 2022, Taiwan Computer Emergency Response Team / Coordination Center (TWCERT/CC) has shared nearly 1.1 million cyber events and Indicators of Compromise (IOCs) to international and domestic CERT organizations, cyber security organizations, private enterprises and cybersecurity communities. TWCERT/CC shares intelligence to help foster Taiwanese and global defense capacity as well as strengthening the synergy of TWCERT/CC with its partners.

TWCERT/CC has shared several intelligence reports with its newsletter subscribers in 2022 including 12 cybersecurity intelligence newsletters and 263 domestic and global cybersecurity news articles. In addition, 70 seminars, events and contests were held to raise awareness of incident reporting to the public. TWCERT/CC serves as a security pillar for cybersecurity awareness to the public/private sectors in Taiwan.

As a CVE Numbering Authority (CNA) for Common Vulnerabilities and Exposures (CVE), TWCERT/CC has reviewed and assigned 101 CVE IDs in 2022. By assisting Taiwanese enterprises with vulnerability mitigation/remediation coordination, TWCERT/CC helps enterprises to reduce the risk and impact from potential cybersecurity incidents. TWCERT/CC was honorably evaluated as a Provider for CVSS3.1 and as a Contributor for CWE by MITRE in November of 2022.

TWCERT/CC has participated in 18 domestic and international cyber security conferences and seminars as well as an international drill. It has also hosted the 2022 Conference of Taiwan Cyber Security Notification and Response, working group meetings and security trainings for Taiwan CERT/CSIRT Alliance, and 8 cybersecurity conferences for Taiwan's enterprises. TWCERT/CC is proactively seeking opportunities to collaborate with its multilateral partners to raise the visibility of Taiwan CERT/CSIRT Alliance and participate in international events to contribute to the global community.

1.2 Achievements & Milestones

- TWCERT/CC has shared nearly 1.1 million cyber events and IOCs in 16 categories, where outbound attack, suspected system vulnerability and system intrusion were the three most common types of cybersecurity attacks in 2022.

- TWCERT/CC has Issued 12 monthly e-newsletters, 263 domestic and global cyber security news articles. In addition, 70 seminars, events and contests were held to raise awareness of incident reporting to the public.
- As a CVE Number Authority, TWCERT/CC reviewed and assigned 101 CVE IDs in 2022.
- TWCERT/CC has participated in 7 international and 18 domestic cybersecurity conferences and seminars, hosted the 2022 Conference of Taiwan Cyber Security Notification and Response and held regular meetings and trainings for Taiwan CERT/CSIRT Alliance.

2. About TWCERT/CC

2.1 Introduction

Taiwan Computer Emergency Response Team/Coordination Center (TWCERT/CC) is dedicated to responding to major cybersecurity incidents, analyzing cyber threats, publishing vulnerability information and exchanging cyber intelligence with trusted global partners. In the year 2022, TWCERT/CC accomplished several provisional goals and missions:

- Strengthened international cooperation with cybersecurity partner teams and enhanced intelligence gathering and sharing.
- Issued monthly e-newsletters regarding cybersecurity trends, cybersecurity tips and security advisories.
- Participated actively in international and domestic conferences and seminars as well as establishing Taiwan CERT/CSIRT Alliance.
- Assisted enterprises with cyber security incident response and coordination as well as raising cybersecurity awareness.
- Offered Virus Check, CVE reporting, Phishing Check services and cybersecurity incident reporting channels.

TWCERT/CC is a member of FIRST, APCERT and a Numbering Authority of the Common Vulnerabilities and Exposures (CVE®). Aside from its continuous participation to the events held by international cybersecurity organizations, TWCERT/CC also collaborates with other CERT organizations in the world to handle cybersecurity incidents and exchange cyber intelligence.

2.2 Constituency and Scope of Work

TWCERT/CC provides its cybersecurity services to enterprises and individuals in Taiwan, including incident reporting, handling and coordination, cybersecurity consultation as well as intelligence collection and dissemination.

TWCERT/CC is dedicated to increasing the overall cybersecurity capability in Taiwan. Therefore TWCERT/CC proactively promotes cybersecurity incident reporting and disseminates cybersecurity educational resources. TWCERT/CC continues to integrate resources and collaborate with cybersecurity organizations, academic institutions, civil communities, governmental institutions, private enterprises and global CERTs/CSIRTs. The emphasis of work is to establish a national cybersecurity collaborative defense mechanism, enhance self-protection capability in the cybersecurity industry, cultivate

cybersecurity human resources and strengthen public-private partnership on cybersecurity matters.

3. Activities & Operations

3.1 Incident Handling & Cyber Intelligence Sharing

TWCERT/CC regularly analyzes and disseminates cybersecurity incident reports and intelligence received from CERT partners, the public and private sectors in Taiwan, cybersecurity companies and individual researchers, to coordinate incident handling and help individuals and enterprises mitigate cyber threats.

In 2022, TWCERT/CC shared about 1.1 million cyber events and IoCs. The monthly statistics and the types of cyber intelligence are shown respectively in Figure 1 and Figure 2.

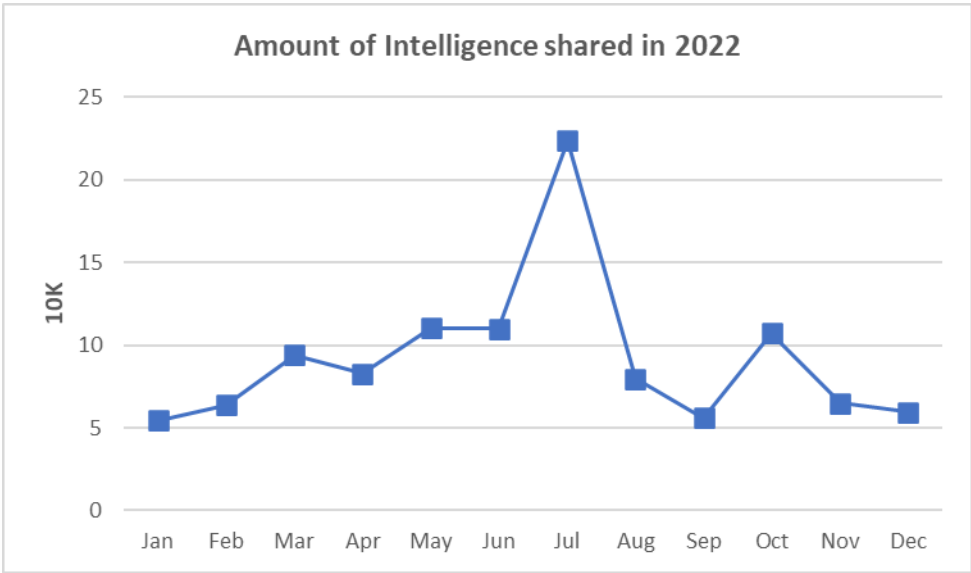


Figure1. Cyber intelligence shared by TWCERT/CC in 2022

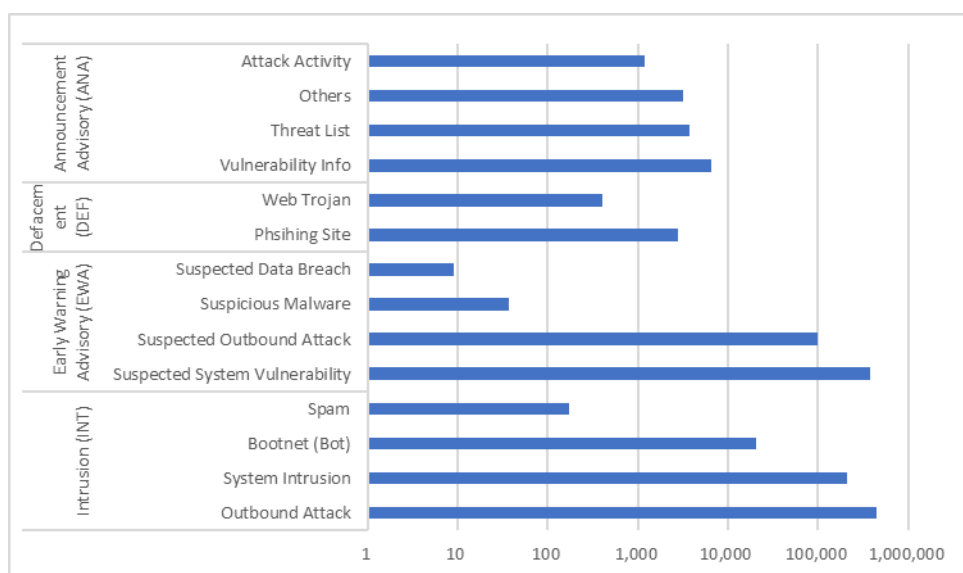


Figure2. Types of cyber intelligence shared by TWCERT/CC in 2022

TWCERT/CC consistently seeks progress on:

- **Prevention:** to provide advisories and early warnings to our constituency, so they can take preventative measures to lower the risk of cybersecurity breaches.
- **Reporting:** to issue immediate warnings for cybersecurity incidents so immediate remediation measure can take place.
- **Handling:** to provide technical support, consultation and coordination for threat mitigation and recovery.

3.2 Publications

As part of a continuous effort to raise public awareness for cybersecurity, TWCERT/CC releases a monthly e-newsletter regarding important cyber intelligence through email, TWCERT/CC official website, Facebook fan page and Pixnet blog. The e-newsletter contains information on TWCERT/CC's recent contributions, cybersecurity policies, emerging threats, cyberattacks, vulnerabilities, events, and the statistics of cybersecurity incident reports. In total, TWCERT/CC has issued 12 monthly e-newsletters, 263 domestic and global cyber security news articles.

3.3 Services

Common Vulnerability Disclosure

TWCERT/CC receives vulnerability reports from global researchers and maintains Taiwan Vulnerability Note (TV) to disclose vulnerability information. As a CVE Numbering Authority (CNA), TWCERT/CC reviews and assigns CVE IDs to those vulnerabilities that meets the criteria. In the year 2022, 101 vulnerabilities were assigned. The list of assigned CVE IDs as shown in Table 1.

Category	Amount	CVE ID
IOT devices	22	CVE-2021-44158, CVE-2022-22054, CVE-2022-23970, CVE-2022-23971, CVE-2022-23972, CVE-2022-23973, CVE-2022-25595, CVE-2022-25596, CVE-2022-25597, CVE-2022-26670, CVE-2022-26673, CVE-2022-26674, CVE-2022-40740, CVE-2022-21933, CVE-2022-21742, CVE-2022-25635, CVE-2022-26527, CVE-2022-26528, CVE-2022-26529, CVE-2022-32966, CVE-2022-32967, CVE-2022-47618
Software and Service	79	CVE-2022-22055, CVE-2022-22056, CVE-2022-22262, CVE-2020-12775, CVE-2022-32959, CVE-2022-32960, CVE-2022-32961, CVE-2022-32962, CVE-2022-35222, CVE-2022-25594, CVE-2022-26671, CVE-2022-26675, CVE-2022-26676, CVE-2022-26668, CVE-2022-26669, CVE-2022-26672, CVE-2022-32456, CVE-2022-32457, CVE-2022-32458, CVE-2022-32958, CVE-2022-35220, CVE-2022-35221, CVE-2022-35223, CVE-2021-45918, CVE-2022-35217, CVE-2022-35218, CVE-2022-35219, CVE-2022-38118, CVE-2022-38116, CVE-2022-32963, CVE-2022-32964, CVE-2022-32965, CVE-2022-35216, CVE-2022-38699, CVE-2022-39029, CVE-2022-39030, CVE-2022-39031, CVE-2022-39032, CVE-2022-39033, CVE-2022-39034, CVE-2022-39035, CVE-2022-39053, CVE-2022-39054, CVE-2022-38117, CVE-2022-39055, CVE-2022-39056, CVE-2022-39057, CVE-2022-39058, CVE-2022-39021, CVE-2022-39022, CVE-2022-39023, CVE-2022-39024, CVE-2022-39025, CVE-2022-39026, CVE-2022-39027, CVE-2022-40741, CVE-2022-40742, CVE-2022-40739, CVE-2022-38119, CVE-2022-38120, CVE-2022-38121, CVE-2022-38122, CVE-2022-39036, CVE-2022-39037, CVE-2022-39038, CVE-2022-41675, CVE-2022-41676, CVE-2022-39039, CVE-2022-39040, CVE-2022-39041, CVE-2022-39042, CVE-2022-46304, CVE-2022-46305, CVE-2022-46306, CVE-2022-46309, CVE-2022-48229, CVE-2022-43436, CVE-2022-43437, CVE-2022-43438

Table 1. CVE IDs assigned

Virus Check

Virus Check is an online file analysis service offered by TWCERT/CC where both static and dynamic analyses are conducted to determine the risk level of the file. When a file has high risk behavior but has low anti-virus detection rate, it is passed to TWCERT/CC's collaboration partners: Trend Micro, CyCraft Technology and TeamT5, for manual analysis. If a new type of malware is recognized, a corresponding virus signature is created to improve future detection of this malware.

Phishing Check

Phishing Check is an online phishing site report service for the general public. The service includes analysis and validation of the reported phishing webpages as well as reporting to relevant parties for take down requests. Phishing Check is dedicated to mitigating the impact of phishing websites and improve the overall cybersecurity capability in Taiwan.

Anti-Ransom

TWCERT has established the Anti-Ransom site containing critical information on ransomware preventive measures and response as well as post-incident recovery. Anti-Ransom is aimed at assisting individuals and enterprises to improve their cyber security capability in respond to the fast-growing threat of ransomware today.

4. Cybersecurity Event

4.1 Domestic Cybersecurity Events

TWCERT/CC actively participated in domestic cybersecurity events, including **organizing, co-organizing** CyberSec 2022 and 2022 Cyberspace conference, **participated** in Cryptology and Information Security Association (CISC) 2022, ICANN APAC-TWNIC Engagement Forum, 38th TWNIC IP Open Policy Meeting, ISACA ITAF Promotion Conference and HICON PEACE 2022. TWCERT/CC has also presented at ten domestic cyber forums for SMEs regarding cyber defense, case study and promoting cyber awareness.

TWCERT/CC has organized a Taiwan CERT/CSIRT Alliance Conference and three cybersecurity trainings for private enterprises in Taiwan, where topics such as cybersecurity drill, emerging cyber threats, vulnerability report, incident response were explored.

4.2 International Cybersecurity Events

TWCERT/CC has been actively engaged with its international partners and cyber security events. In 2022, TWCERT/CC participated in the following international conventions:

- 34TH Annual FIRST Conference
- APNIC 54
- NatCSIRT 2022 Annual Conference
- APCERT Annual General Meeting (AGM)
- APCERT Closed Conference
- FIRST-APCERT Regional Symposium

TWCERTCC has organized the TWCERT 2022 Annual Conference (figure 3). The theme was 'Cyber resilience and operational sustainability', where cybersecurity experts were invited from different fields of industry, government-sector and academic fields to share their valuable knowledge and experience with the audience. Broad cybersecurity topics are

discussed, such as supply chain cybersecurity, international cybersecurity trend, and industrial CISO summit. Several honorable guests were invited to share their expertise and experience from Ministry of Digital Affairs, American Institute in Taiwan, Ministry of Justice, CyCraft, Hong Hai Research Institute, Zyxel and Delta Electronics.

The Panel Discussion regarding 'international cybersecurity trend' was hosted by Kenny Huang, the CEO of TWNIC. Several international experts from CISA, MSTIC, MyCERT and CERT® Division of Carnegie Mellon University Software Engineering Institute were invited to share their experiences in coordinating cyber joint-defense in their constituency.



Figure 3. TWCERT 2022 Annual Conference

TWCERT/CC has participated in APCERT Cyber Drill 2022. The theme was 'Data Breach through Security Malpractice', where this exercise reflects real incidents and issues that exist on the Internet. This drill included the need for the teams to interact locally and internationally, with CSIRTs/CERTs and targeted organizations, for coordinated suspension of malicious infrastructure, analysis of malicious code, as well as notification and assistance to the affected entities. This incident response exercise, which was coordinated across 25 CSIRTs from 21 economies, reflects the collaboration amongst the economies in mitigating cyber threats and validates the enhanced communication protocols, technical capabilities and quality of incident responses that APCERT fosters in assuring Internet security and safety. TWCERT/CC was able to complete all injects within the given time limit.

TWCERT/CC has participated APNIC 54 and presented 'An Anatomy of TCP Middlebox Reflection Attack and Mitigation Measures' at APNIC 54 (figure 4). Distributed Denial-of-Service (DDoS) attacks leveraging a new amplification technique called "TCP Middlebox Reflection" are emerging as a serious threat to organizations. These attacks abuse vulnerable firewalls and content filtering systems to reflect and amplify TCP traffic to victims' devices. This presentation gives an in-depth anatomy and threat landscape of the TCP Middlebox Reflection attack and shares the verification and mitigation techniques to fend off such attacks.



Figure 4. TWCERT/CC's presentation at APNIC 54

5. Future Work

TWCERT/CC is dedicated to optimizing its services and raise awareness of cybersecurity with the following items:

1. Disseminate vulnerability information and cybersecurity incidents, monthly cybersecurity e-newsletter, and annual cybersecurity report.
2. Notify emerging cyber threats, policies to its constituency regularly.
3. Collect, analyze, and release the latest information regarding cybersecurity conferences, seminars, and trainings.
4. Actively engage with international and domestic cybersecurity partners and facilitate collaboration to improve its cybersecurity capability as a CERT organization.

6. TWCERT/CC Contact Information

- Website: <https://www.twcert.org.tw/>
- Facebook: <https://www.facebook.com/twcertcc/>
- E-Mail: twcert@cert.org.tw

TWNCERT

Taiwan National Computer Emergency Response Team

1. Highlights of 2022

1.1 Summary of major activities

TWNCERT (Taiwan National Computer Emergency Response Team) aims to support and enhance the government's ability to respond and deal with cyber security incidents. In 2022, TWNCERT issued more than sixteen hundred advisories to government agencies. TWNCERT also provided consulting and training services for government agencies and critical infrastructure sectors.

To strengthen the preparedness against cybercrimes, technology failures, and Critical Information Infrastructure incidents, TWNCERT conducted a national cyber security exercise, Cyber Offensive and Defensive Exercise (CODE) every two years and keeps conducting social engineering exercises, information system penetration exercises to help promote the preparedness of Taiwan government agencies.

Besides, TWNCERT launched a series of cyber security competitions in 2022 to nurture cyber security talents and promote cyber security awareness. There are more than two thousand students, and the general public participated.

1.2 Achievements & milestones

TWNCERT developed four online courses to improve cyber security protection and awareness among government agencies in 2022. More than sixteen thousand government staff attended the online and onsite training and took course exams. As the convener of the APCERT Training Working Group, TWNCERT convened six online training sessions. A total of twenty-three APCERT member teams participated in these programs.

2. About TWNCERT

2.1 Introduction

As a national CERT, TWNCERT acts as the point of contact for the CSIRTs in CI sectors in Taiwan and worldwide for the nation. We aim to enhance the government and CI sectors' ability to respond and deal with cyber security incidents and conduct technical and consulting services to government agencies.

2.2 Establishment

TWNCERT was established in 2001 and formed by the National Information and Communication Security Taskforce (NICST). TWNCERT is also known as the National Center for Cyber Security Technology (NCCST) domestically, led by the Administration for Cyber Security, Ministry of Digital Affairs, which is in charge of the cyber security policy of Taiwan. The formation of TWNCERT aims to create a government cyber response center that can help optimize the capability of continuous monitoring, task coordination, and incident response and handling in the face of cyber security threats.

2.3 Resources

TWNCERT currently has around 140 full-time employees, and the operation funding comes from the Department of Cyber Security of the Executive Yuan.

2.4 Constituency

TWNCERT dedicates to enhancing the capability of incident reports and response among government authorities and CI sectors. Moreover, TWNCERT coordinates information sharing with various stakeholders such as Financial ISAC, Academic ISAC, National Communications Commission ISAC, Energy ISAC, Transportation ISAC, Hygiene ISAC, High-Tech Park ISAC, major MSSPs, law enforcement agencies, other CSIRTs in Taiwan as well as cyber security industries in Taiwan and worldwide.

3. Activities & Operations

3.1 Scope and definitions

Our critical mission activities are:

Incident Response

Responsible for cyber security incident response in the government and CI sectors and effective practical assistance and support to related agencies to counter when facing threat situations or cyber attacks.

Information Sharing

National Information Sharing and Analysis Center (N-ISAC) provides a central resource for gathering information on cyber threats to critical infrastructure and providing two-way sharing of information between the private and public sectors.

Cyber Security Drill & Audit

Hold large-scale cyber offensive and defensive exercises, pairing with cyber security audits, cyber health checks, and penetration test services, to discover cyber security problems of the government and critical infrastructures in time.

Education & Training

Plan cyber security series competitions and training programs to enhance cyber security education effects and raise cyber security awareness.

Coordination and Collaboration

Build coordination and communication channels with domestic and foreign incident response organizations; Coordinate with international CSIRTs, cyber security vendors, and other cyber security organizations.

3.2 Incident handling reports

In 2022, TWNCERT received nearly one thousand reports on cyber security incidents from Taiwan government agencies. We also received about eleven hundred cyber security incident reports from international CERTs/CSIRTs and cyber security organizations. Moreover, more than seven hundred forty thousand cyber security incidents and critical information were shared among N-ISAC members, including CI sector ISACs, MSSPs, LEAs, and CSIRTs in Taiwan.

3.3 Abuse statistics

Government agencies

In 2022, TWNCERT received reports on cyber security incidents from government agencies. About 44.7% of the reported security incidents are in the category of Intrusion, as shown in Figure 1.

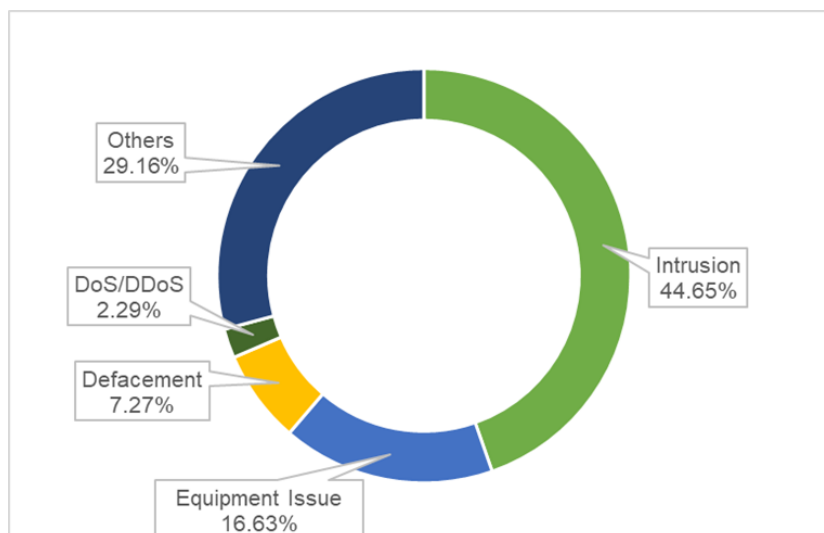


Figure 1. Security Incidents from Government Agencies

International incident report

In 2022, TWNCERT received about eleven hundred cyber security incident reports from international CERTs/CSIRTs and cyber security organizations. The incident reports were categorized as shown in Figure 2. About 83% of the incident reports were Malware Infected Systems, followed by Attack, and Phishing.

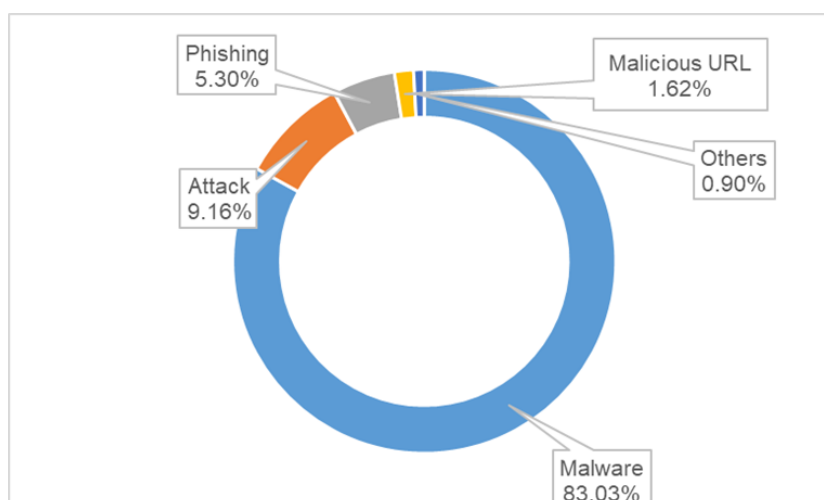


Figure 2. Category of International Incident Reports

N-ISAC information sharing

N-ISAC members shared more than seven hundred forty thousand cyber security incidents and critical information. The Early Warning is the most shared cyber security information in 2022, as shown in Figure 3.

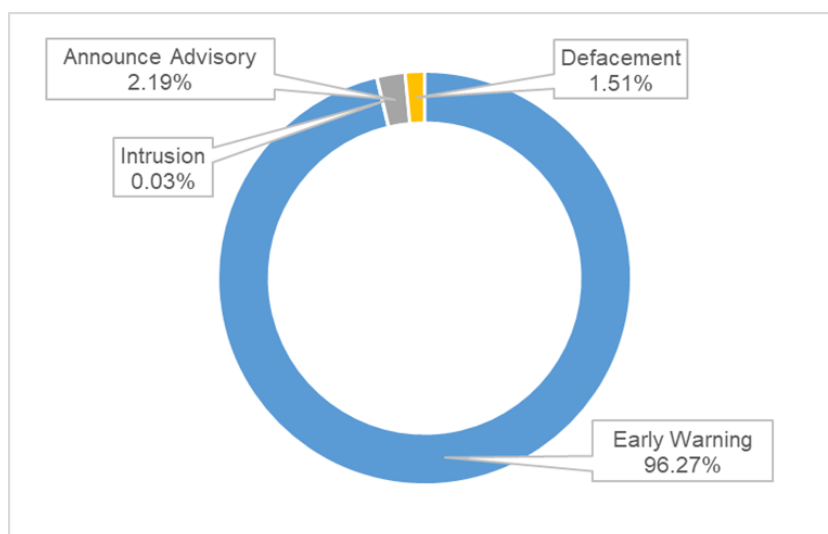


Figure 3. Distribution of N-ISAC Information Sharing

3.4 Publications

Website publication

TWNCERT collects and publishes cyber security advisories, news, and guidelines on the website. In 2022, TWNCERT published more than one hundred articles, including cyber security news and security alerts.

Advisory and Alert

In 2022, TWNCERT issued more than sixteen hundred advisories to government agencies. The categories were distributed as in Figure 4.

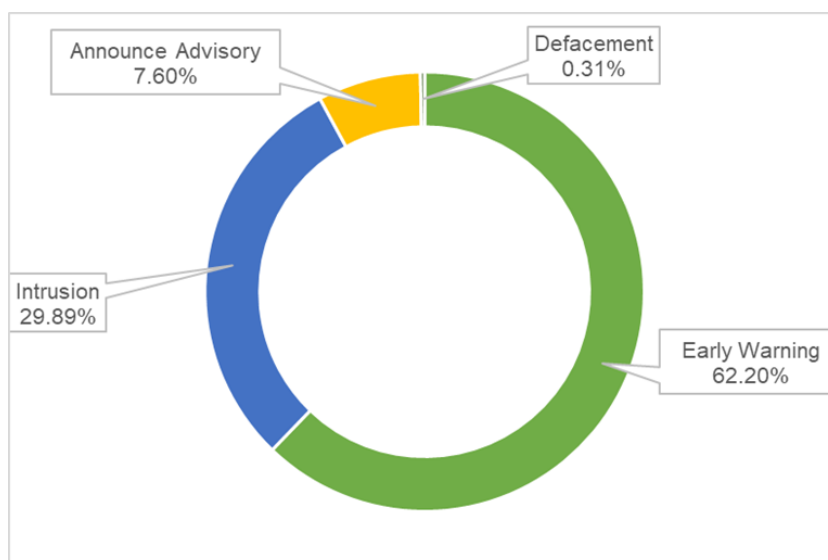


Figure 4. Distribution of Government Notice Advisories

International incident report

In 2022, TWNCERT shared more than twenty-six thousand incident reports to other national CERTs/CSIRTS, as shown in Figure 5.

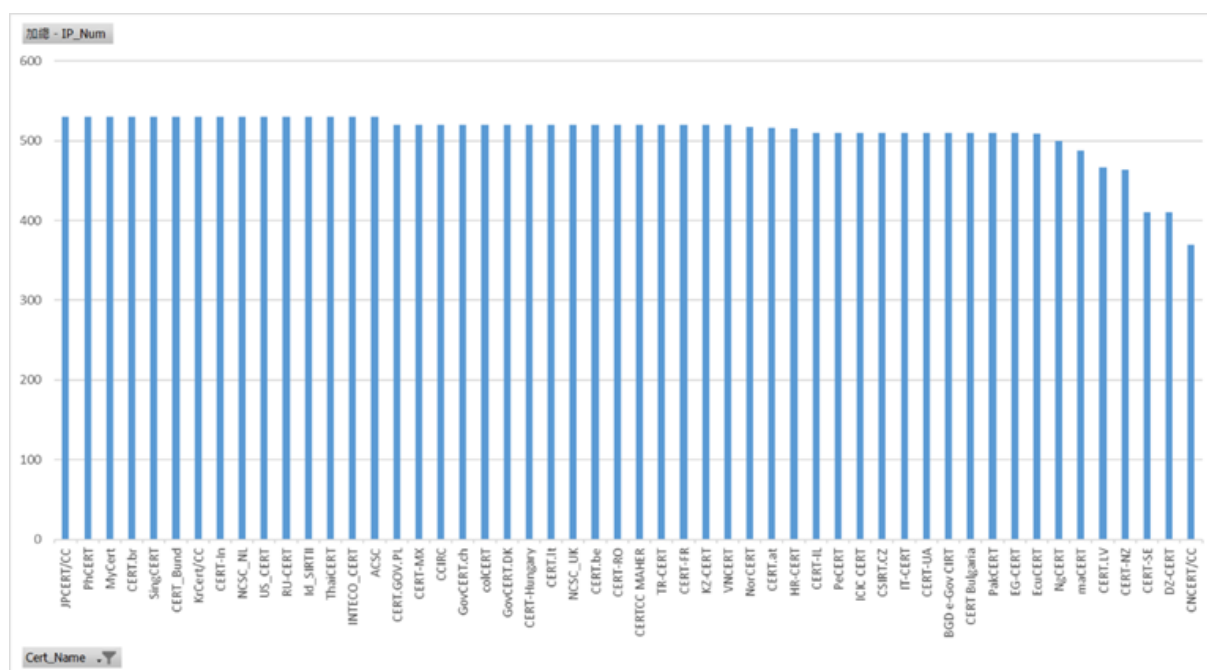


Figure 5. International Incident Report Sharing

4. Events organized/hosted

4.1 Training

TWNCERT developed four online courses to improve cyber security protection and awareness among government agencies in 2022. About sixteen thousand government staff attended the online and onsite training and took course exams.

4.2 Drills & exercises

Drill

To strengthen the preparedness against cybercrimes, technology failures, and Critical Information Infrastructure (CII) incidents, TWNCERT conducts Cyber Offensive and Defensive Exercise (CODE) once every two years as well as continuing to conduct social engineering exercises and information system penetration exercises to help promote the preparedness of Taiwan government agencies. There were twenty countries, and thirty-one public and private organizations attended the events in CODE 2021. CODE 2021 included a Red vs Blue confrontation live-action exercise in the energy CI sector, as shown in Figure 6.



Figure 6. CODE

Cyber security competition

To nurture cyber security talents and to promote public awareness of cyber security, TWNCERT launched a series of cyber security competitions in 2022. More than two thousand students and the general public participated.



Figure 7 Cyber Security Competition

4.3 Conferences and seminars

In 2022, TWNCERT held N-ISAC meetings in April and November. We discussed the recent cyber security issues and improved information sharing efficiency and effectiveness through the meetings.

During the N-ISAC annual meeting in November, experts from the public and private sectors in Taiwan were invited to share valuable insights and experiences with N-ISAC members. Moreover, we instructed the workshop for our ISAC members. The topics focused on the execution strategy for Critical Infrastructure and Key Resources Protection. Members learn how to process and share cyber security information, gain valuable experience, and build trust relationships with other sectors through the seminar.



Figure 8 N-ISAC Annual Meeting



Figure 9 N-ISAC Workshop

5. International Collaboration

5.1 International partnerships and agreements

TWNCERT is a member of the international organizations listed below and actively participates in member activities, including meetings, working groups, annual conferences, and other cooperation.

- Asia Pacific Computer Emergency Response Team (APCERT)
- Forum for Incident Response and Security Teams (FIRST)
- APEC TEL
- Meridian

5.2 Capacity building

5.2.1 Training

As the convener of APCERT Training Working Group, TWNCERT coordinated member teams for online training sessions bi-monthly. TWNCERT convened six online training sessions in 2022.

Date	Title	Presenter
2022/2/8	Latest Trends on Keyword Hacks & SEO Spam	Sri Lanka CERT CC
2022/4/12	Cyber Security Incident Reporting and Handling Scheme for Taiwanese Government Agencies	TWNCERT
2022/6/21	FIRST's EPSS Scores for Vulnerabilities	AusCERT
2022/8/9	Cyber Threat Intelligence on a national level	ThaiCERT
2022/12/6	Honeynet Data Analysis Through LebahNET	CyberSecurity Malaysia

Figure 10 APCERT Training Programs

5.2.2 Drills & exercises

TWNCERT participated in APCERT Drill under the theme "Data Breach through Security Malpractice" on August 25th and solved a set of drill scenarios within the given time limit.



Figure 11 APCERT Drill 2022

5.2.3 Seminars & presentations

Below is the list of international events that TWNCERT participated in.

- APEC TEL Conference (online)
- FIRST 2022AGM
- APCERT AGM 2022(online)

6. Future Plans

For the APCERT online training program, TWNCERT will continue to coordinate trainers and participants to provide bi-monthly online training, expand coordination with other APCERT Working Groups, and participate in APCERT activities such as APCERT Drill. Possible collaboration opportunities with other international organizations will also continue to be a pivotal emphasis to enhance the depth and broadness of the training program further.

7. Conclusion

TWNCERT will continuously enhance the collaboration with government agencies, particularly critical information infrastructure sectors, to build public-private partnerships and collaborate with local and global CSIRTs to strengthen cyber security awareness and incident handling capabilities. The essential elements of this strategy will be

- Enhance agency accountability and guide resource allocation
- Expand public-private partnerships and introduce quality services
- Defense-in-depth deployment and government-wide situation awareness
- Harden IT infrastructure and reduce cyber-attack surfaces

- Check and evaluate regularly, improve through lessons learned
- Cultivate future talents to raise the bar for cybersecurity

Within the region, TWNCERT dedicates to contributing to the APCERT mission and looks forward to domestic and international cooperation opportunities to establish safe and secure cyberspace for the prosperity of society.

VNCERT/CC

Viet Nam Cybersecurity Emergency Response Teams/Coordination Center

1. Highlights of 2022

In 2022, VNCERT/CC has focused on capacity building for CISRTs, development of the Vietnam CSIRTs Network and preparing for security conforming of IT/IS solutions, products. Besides, VNCERT/CC has some activities such as:

- Submitted to the Prime Minister for promulgation Directive 18/CT-TTg on stepping up incident response activities in Viet Nam.
- Launched the national network security coordination and troubleshooting platform, which enables quick and timely warning and troubleshooting.
- Developed and provided tools to check, review and support incident response activities for members of Vietnam CSIRTs Network.
- Evaluated SIM3 criteria for VNCERT/CC under EU's experts support.
- Implemented 02 tools to support child online protection.

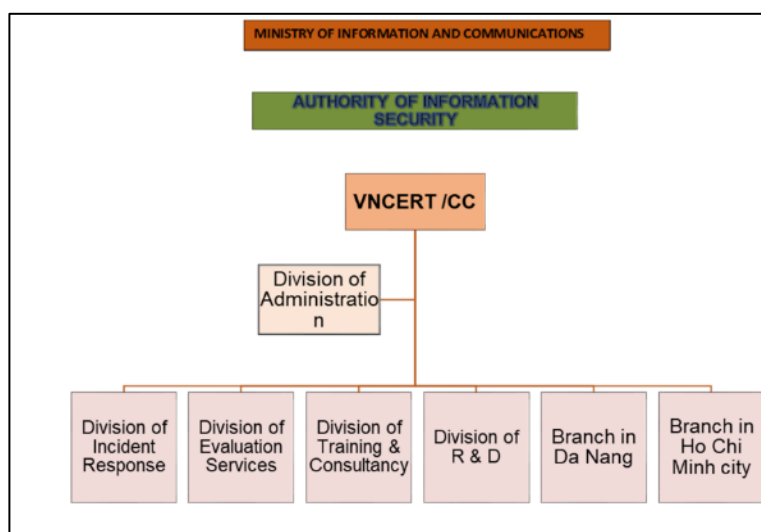
2. About VNCERT/CC

2.1 Introduction

- The Viet Nam Cybersecurity Emergency Response Teams/Coordination Center (VNCERT/CC) has been reorganized and renamed since 2019 from VNCERT (The Vietnam Computer Emergency Response Team), which was established in 2005 by the Prime Minister.
- VNCERT/CC has functioned as a coordinator of computer incident response activities nationwide; timely warnings of computer network security issues; coordination of the development of standards and technical regulations on computer network safety; security evaluation services; encourage the formation of CERT/CSIRT in agencies, organizations, and enterprises; being the contact point with the international CERT organizations (CERTs).
- VNCERT/CC has more than 70 employees at the Head Office and two branches.

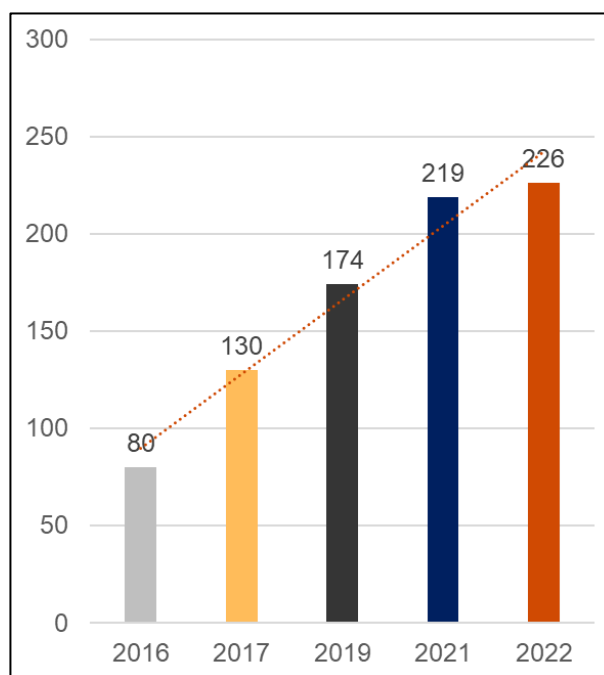


- VNCERT/CC is a member of the Forum of Incident Response and Security Teams (FIRST).



The organizational structure of VNCERT/CC

- VNCERT/CC is a leader and coordinator of the national CSIRTs Network of Vietnam (Vietnam CSIRTs Network) which consists of 226 organizational members with more than 4,000 staff members.



Number of Vietnam CSIRTs Network Members

2.2 Contact Information

- Website: <http://www.vncert.gov.vn/>
- E-mail: international@vncert.vn
- Tel: +84-24-3640 4421 (08:00-17:00 - Working hour)
- Incident report: ir@vncert.vn / ucsc@vncert.vn
- Hotline: + 84-86 810 0317 (24x7)

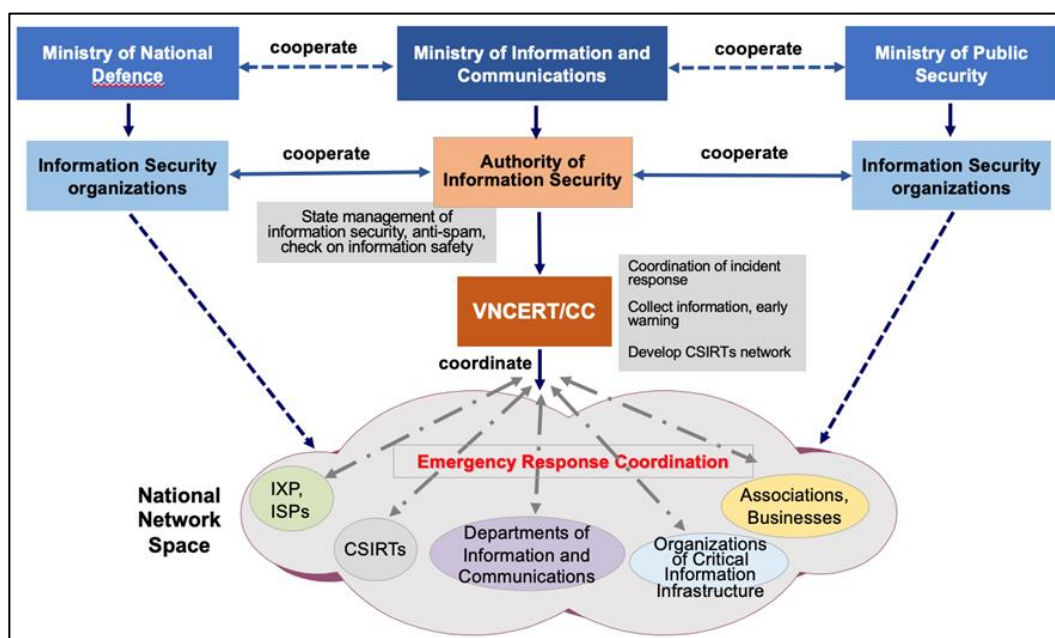
3. Activities & Operations

3.1 Scope and definitions

VNCERT/CC has the roles of:

- Operating activities of Vietnam CSIRTs Network with 226 members (including incident response center, information security center or information technology centers from Ministries, ministerial agencies, governmental agencies, telecommunication enterprises, Internet service providers, Finance Organizations, Banks, organizations in charge of national information systems).
- Receiving reports of security incidents and warning
- Coordinating national cybersecurity incident response activities.

- Promoting to build of CERTs/CSIRTs in Vietnam's organizations, enterprises, and agencies.
- Being the point of contact of Vietnam with the other CERTs in the world.
- Implementing and deploying the anti-spam activities.
- Receiving reports of incidents, harmful content, child abuse in the cyber as a being an operation member of the Viet Nam's Network for Child Online Protection (VN-COP), be established in 2021 with 24 members.



3.2 Incident handling reports

Security Incidents	2022
Phishing	668
Deface	1130
Malware	417
Vulnerability	53
Total	2223

3.3 New services

- Developed and coordinated the treatment of spam.
- Build an automatic DNC (Do not call) data-sharing system.
- Build an automatic IP blacklist data-sharing system.
- Coordinated the deployment of a number to receive reports of spam calls, scam calls.

4. Events organized/hosted

4.1 Training

Participated and/or organized:

- Supported 29 ministries, branches and localities to organize security real-combat exercises.
- Organized 09 cybersecurity Webinars.
- Organized a training on The Security Incident Management Maturity Model (SIM3) for the Vietnam CSIRTs Network with support from EU's Cyber4Dev.
- Connected with international organizations such as AJCCBC (Japan), KISA (Korea) to participate in skills training programs.

4.2 Drills & exercises:

Participated:

- VNCERT/CC participated in the ASEAN-Japan Remote Cyber Exercise on June 23, 2022, based on the theme "Cyberattacks on VPN devices installed in the government and Ransomware attack on healthcare institution". The exercise was held in both online and in-person formats. It was organized to 200 locations across the country for IT units of ministries, agencies, provinces and cities to join the event.
- VNCERT/CC participated in the APCERT cyber drill on August 25, 2022, based on the theme "Data Breach through Security Malpractice" and forwarded to organizational members of Vietnam CSIRTs Network participation at the same time as APCERT drill.
- VNCERT/CC participated in the ASEAN CERTs Incident Response Drill (ACID) on October 27, 2022, based on the theme "Dealing with Disruptive Cyber-Attacks Arising from Exploitation of Vulnerabilities".
- Organized:
- Organized 05 drills (03 international drills, 02 real combat drills) for information system for members of the Vietnam CSIRTs Network.

4.3 Conferences and seminars

VNCERT/CC cooperated with other organizations to organize annual events such as "Security World 2022", "National Information Security Day 2022" and organized other conferences for CSIRTs Network members and information security departments from all over the country.

VNCERT/CC organized the national network information security incident response conference in 2022 and the workshop on "Improving defense capacity through the deployment of security real-combat drills".

5. International Collaboration

5.1 International partnerships and agreements

Completed signing of a Memorandum of Understanding with CERT-In.



Exchanged information, connect with CNCERT, Cyber4Dev (EU), CyberCX (Australia).



5.2 Capacity building

5.2.1 Training

Attended online courses of foreign organizations, international organizations such as distance training conducted by Korean companies, AJCCBC Cyber Security Training, GCCD Cybersecurity Webinar...

5.2.2 Drills & exercises

Attended 3 drills of APCERT 2022, ASEAN-Japan 2022, and ACID 2022.

5.2.3 Seminars & presentations

Attended FIRST conference, NatCSIRT meeting, ASEAN-Japan meetings, CAMP meeting and other regional workshops in ASEAN.

5.3 Other international activities

Contacting and cooperating with international organizations and businesses for security data sharing, coordinating, protecting, mitigating, etc.

6. Future Plans

6.1 Future projects

Digital Forensic Lab.

6.2 Future Operation

- Develop technical human resources of VNCERT/CC;
- Continue to develop the Vietnam CSIRTs Network, improving the cybersecurity service quality and quantity for the community
- Develop cooperation with other CERTs in the world
- Project of Children Protection on Cyberspace.
- Improve Anti-spam.
- Continue to collaborate to exchange lessons and experiences on the development of legislation, laws, and information on developing an online social media management system among National CERT, international organizations, and related sectors in the field of cybersecurity.



7. Conclusion

The mission of VNCERT/CC is to assist Vietnam organizations and internet users in implementing proactive measures to reduce the risks of security incidents and to assist them in responding to such incidents when they occur.

Besides, VNCERT/CC is planning to provide more services to local communities and develop cooperation with all the incident response teams in the world to contribute to greater global cyber security.

VNCERT/CC is also interested in and looking to connect with government leaders on child protection issues online.



Activity Reports from APCERT Partners

AfricaCERT

Africa Computer Emergency Response Team

1. About the Organization

The objectives of AfricaCERT are to assist African countries in establishing and operating Computer Security and Incident Response Teams (CSIRTs) by providing expertise and advice in formulating initiatives, programs, and projects related to the launch of CSIRTs in African countries and to encourage and support cooperation among teams in the Africa Internet Service Region.

2. Activities & Operations in 2022

CSIRT Assistance

- Assistance for Ghana Commercial Bank for FIRST Membership
- Assistance for Rwanda Computer Security Incident Response Team (Rw-CSIRT) for FIRST Membership
- Assistance for gmCSIRT (Gambia) for Suguru Yamaguchi Fellowship Program

Publication for the GFCE

Cyber Incident Management in Low-Income Countries

- PART 1: A HOLISTIC VIEW ON CSIRT DEVELOPMENT
<https://cybilportal.org/publications/cyber-incident-management-in-low-income-countries-part-1-a-holistic-view-on-csirt-development/>
- PART 2: A GUIDELINE FOR DEVELOPMENT
<https://cybilportal.org/wp-content/uploads/2022/01/CSIRTs-In-Low-Income-Countries-Final-Report-part-2-v16.pdf>

Conferences and Trainings

- Cybersecurity Summit - Lomé 2022 on March 23 -24, 2022.
- Panel of Experts: Identify and implement key success factors to strengthen regional Cybersecurity collaboration.
<https://sommetybersecuritelome.com/en/agenda>
- African Cyber Resilience Conference. Keynote on Cyber Resilience
- <https://cyber4dev.eu/2022/05/02/african-cyber-resilience-conference-brings-delegates-from-partner-countries-to-mauritius/>
- <https://govmu.org/EN/newsgov/SitePages/Mauritius-hosts-the-African-Cyber-Resilience-Conference.aspx>
- Global Constellation Annual Conference: Linking Cybersecurity Capacity Research. Participation in the GFCE Session. November 2-3, 2022
- Global Cyber Policy Dialogues: Southern Africa meeting. October 31–November 1, 2022, in Pretoria (Tshwane). Speaker represented by Roland Aikpe from BJCSIRT.
- May 27: AfricaCERT Workshop: Incident Response 101.
- * Building an Effective Cyber Incident Response Team. CERT MU
- * WordPress intrusion case: Dynamic Log Analysis
- Luc SEMASSA, Senior cybersecurity analyst at bjCSIRT
- OSWE|OSCP|CEH|CSA
- Support for HackerLab 2022, an annual competition organized by BJCSIRT by providing 20 Access Code(s) CertMaster Learn for CompTIA Security+ (SY0-601) - Individual Access to some participating teams.
- Official CISSP Bootcamp
- Nov 21 – 25, 2022
- July 11 – 15, 2022
- Annual Africa Cyber Drill: 2nd Africa CYBER DRILL “Stay on Alert” September 8-9, 2022
- Third SADC Cyber Drill: 20-21 October 2022 – Co-Organizer

Collaboration

AfricaCERT Signed an MOU with Smart Africa. Nov 17, 2022

Smart Africa and Africa Computer Emergency Response Teams (AfricaCERT) signed a MoU to advance the cybersecurity ecosystem on the continent. Both organizations will work together to promote good practices and experiences sharing among Smart Africa member States to develop a comprehensive framework for cybersecurity, including better addressing legal and regulatory issues related to information security.

AfricaCERT to build a Community around MAUSHIELD

The Computer Emergency Response Team of Mauritius (CERT-MU), operating under the Ministry of Information Technology, Communication, and Innovation of the Republic of Mauritius, has launched a Cyber Threat Information

Sharing Platform known as MAUSHIELD. It is an automated platform for sharing cyber threat intelligence in real-time, securely, and confidentially. MAUSHIELD aims to facilitate cyber threat information sharing and better understand the different techniques cybercriminals use to carry out cyber-attacks. This will help organizations improve their defense capability and stay on top of current trends and emerging threats.

MAUSHIELD is open to the following national, regional, and international organizations or sectors:

- Public sector organizations
- Critical sectors
- Private sector organizations
- Small and Medium Enterprises
- Academia
- Non-profit organizations

To become a Member of MAUSHIELD, please register on the portal: (<https://maushield.govmu.org>)

3. Collaboration with APCERT Members/Partners

- Members from APCERT Economies participated in the 2nd Africa Cyber Drill.
- Participation in the Cybersecurity Forum for Technology Development and International Cooperation during the 2022 World Internet Conference held from November 9 to 11 in Wuzhen, Zhejiang Province, China.
- Participation of African team in the 2022 APISC training organized by KrCERT/CC from Aug 10 – Oct 31, 2022.

FSI-CERT

Financial Security Institute – Computer Emergency Response Team - Korea

1. About FSI-CERT

1.1 Introduction

FSI-CERT is an organization dedicated to cyber security in the financial sector. The institute is a non-profit corporation funded by member financial companies.

FSI-CERT operates a cybersecurity incident response system in the financial sector by coordinating a system sharing information on cybersecurity incidents, notifying intrusion attempts, analyzing the cause of incidents, and providing prompt response and prevention measures.

When security incidents occur, FSI-CERT deploys digital forensics and malware analysis to identify the cause of the incident and provides initial measures to limit damage and avoid any recurrences of such incidents.

1.2 History

FSI-CERT was founded on April 2015 to specialize as a cyber security organization for the financial sector. Its mission is to create a safe and reliable environment to enhance the convenience of customers and the development of the financial industry.

1.3 Organization

FSI-CERT has more than 300 employees working in 3 groups(12 departments), to conduct cyber security monitoring in the financial sector, cyber attack response, and vulnerability analysis/assessment.

1.4 Contact Information

- Tel: +82-2-3495-9431
- Fax: +82-2-3495-9399
- Email: cert@fsec.or.kr
- Website: <https://www.fsec.or.kr/en>

2. Activities & Operations

2.1 Summary of major activities

2.1.1 Response to the Lazarus Group's attack

In response to Lazarus Group's APT attack and attack on the spam mail blocking system's supply chain of financial companies, FSI-CERT identified and disseminated information to the financial sector on the cause of the compromise.

2.1.2 Monitoring and Response to dark web threats

FSI-CERT successfully responded to cyber threats and security incidents related to dark web by monitoring financial information and latest hacking-related information traded on the platform.

2.1.3 Bug-bounty program for the financial sector

FSI-CERT launched a bug bounty program to discover unprecedented security vulnerabilities and strengthen preemptive prevention activities against cyber infringement threats. The program was broadened to cover mobile apps of financial companies in addition to internet banking security software.

2.1.4 Operation of a next-generation financial ISAC system

The next-generation Financial Information Sharing and Analysis Center(ISAC) system operated by FSI-CERT leads security control technology by advancing the application of artificial intelligence(AI), producing and providing threat intelligence, and establishing private clouds.

2.1.5 Information sharing of voice phishing threats

FSI-CERT established a voice phishing fraud information sharing system between related and/or specialized institutes of the financial, communication, security, and public sectors using information sharing APIs to prevent and respond to advancing voice phishing threats.

2.1.6 Operation of an integrated analysis system for financial mobile app

To prevent compromise and ensure a safe user environment in financial applications, FSI-CERT developed and operated a system which classifies and manages mobile security function modules to analyze security threats and vulnerabilities.

2.2 Incident Response

2.2.1 Incident analysis and response

When cyber attacks occur in financial companies, FSI-CERT gathers digital evidence and utilizes digital forensics on scene to analyze the cause of the incident. FSI-CERT also establishes measures to prevent damage propagation and enhance financial companies' cyber threat response capabilities by conducting incident prevention digital forensic analysis on PCs that are likely to be targeted.

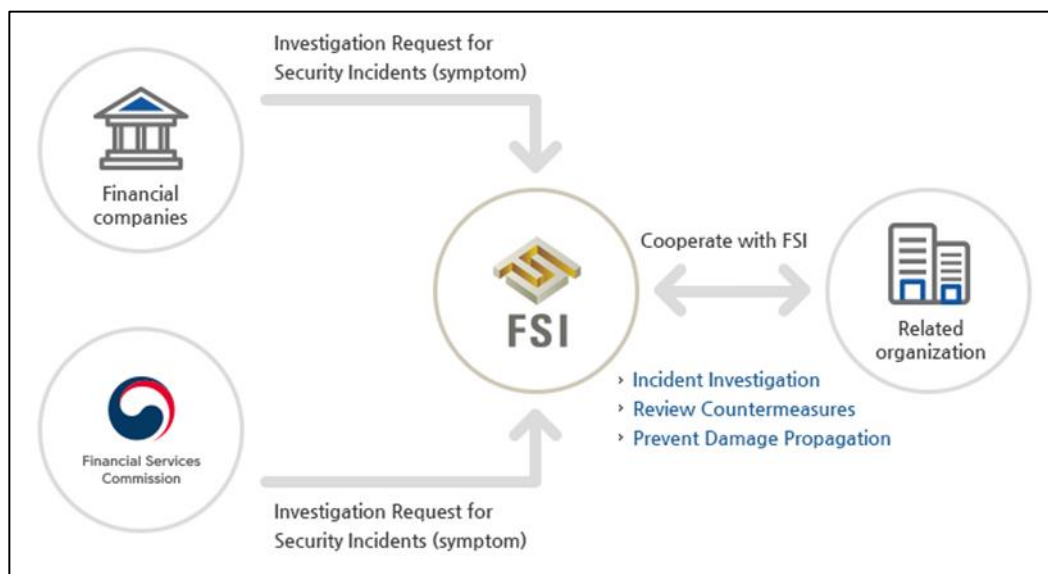


Figure 1. Incident Response Process

2.2.2 Collection, analysis, and response to malware

FSI-CERT shared information on cyber threats such as distribution sites, hash values, and IOCs(Indicator of Compromise) by collecting and analyzing cyber attack attempts on financial companies and also malicious codes that are spread for financial purposes.

Furthermore, FSI-CERT provided correlation analysis information by systematically managing a multitude of collected/analyzed results of malicious codes.

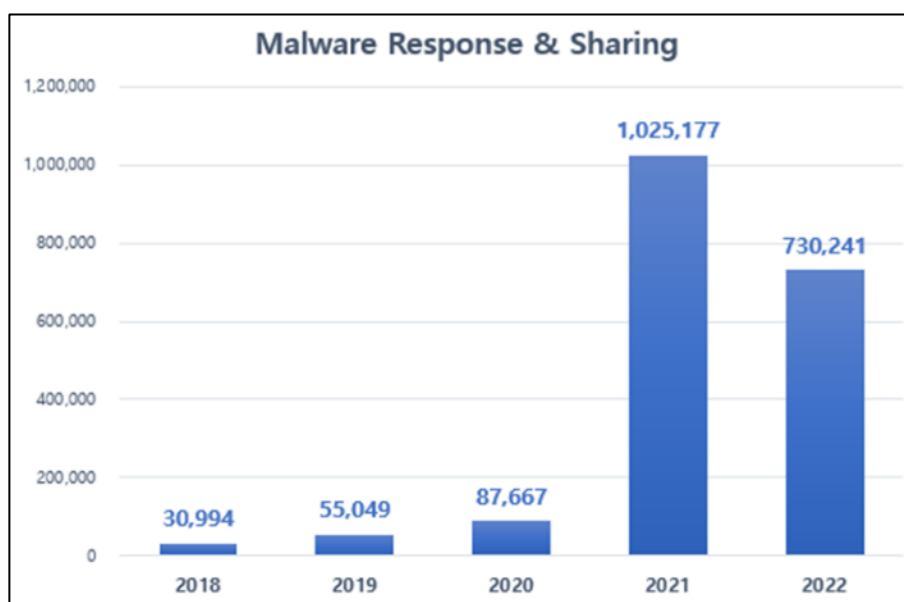


Figure 2. Total Malware Response and Sharing Cases

2.2.3 Simulation training on cyber security incidents

FSI-CERT conducted simulation training on cyber security incidents for financial companies. Through trainings on various types of cyber attacks such as DDoS attacks, server hacking, and APT attacks, FSI-CERT inspected the incident response system of financial companies and contributed to improving security awareness.

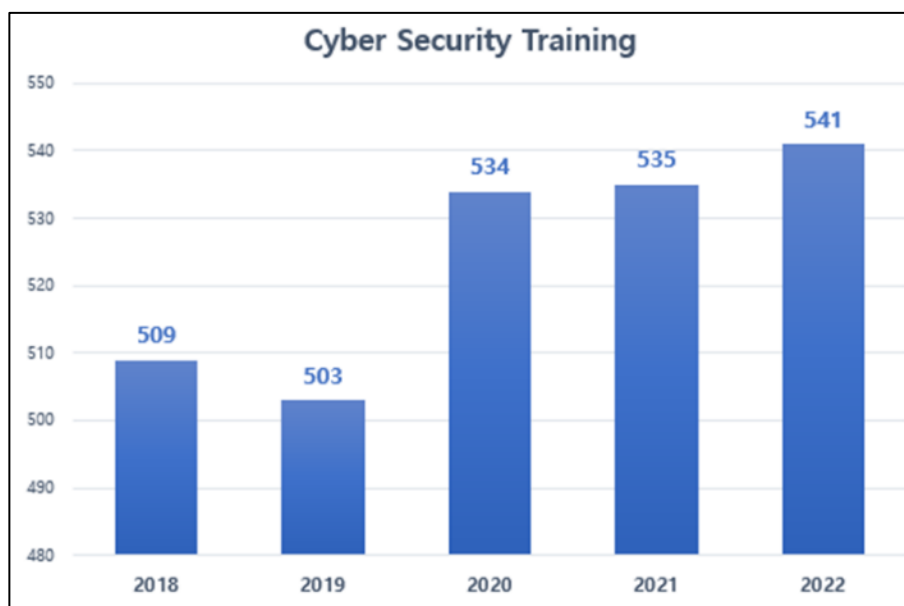


Figure 3. Total Cyber Security Training Sessions

2.2.4 Operation of DDoS Attack Emergency Response Center

When large-scale DDoS attacks to which financial companies cannot respond on their own occur, FSI-CERT filters DDoS attacks and sends back only the valid network traffic to financial companies. The cloud-based DDoS cyber shelters first block large-scale bandwidth attacks. Then the FSI CERT's DDoS attack emergency response center blocks application-layer attacks on critical services.

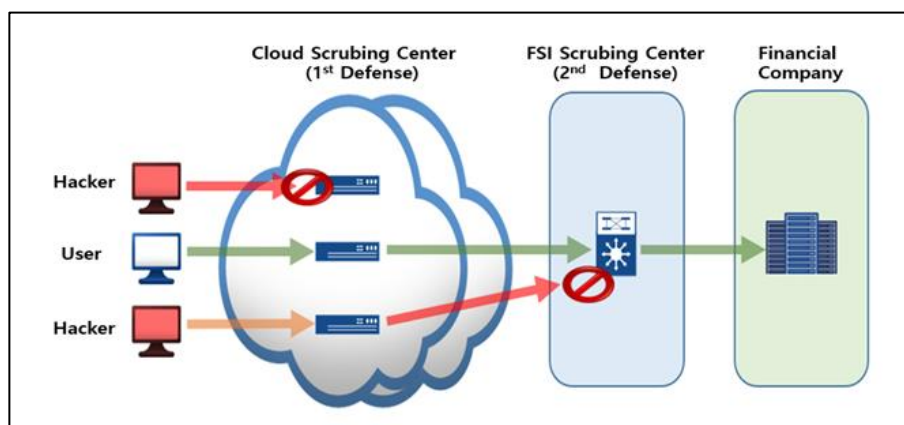


Figure 4. DDoS Attack Response Process

2.3 Operation of an integrated security monitoring system

FSI-CERT coordinates a financial ISAC, in which an AI and big-data based security monitoring system, operating nonstop, detects cyber threats against the entire financial industry.

In 2022, FSI-CERT produced and disseminated information on Lazarus Group's APT attack, Spring4Shell and Log4Shell vulnerability attack trends, etc., to financial companies.

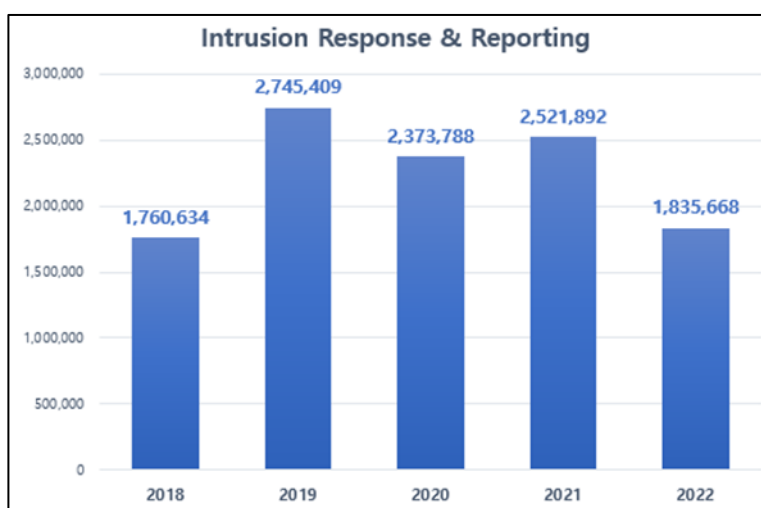


Figure 5. Total Intrusion Response and Reporting Cases

FSI-CERT protects financial assets from voice phishing by detecting phishing/pharming sites through a self-developed system and by blocking the spread of malicious applications through an information sharing system across the financial sector.

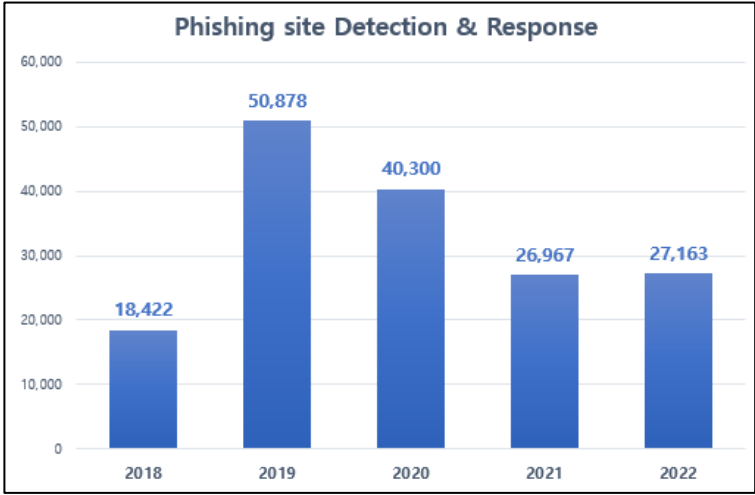


Figure 6. Total Phishing Site Detection and Response

2.4 Vulnerability analysis and assessment

FSI-CERT provides comprehensive inspections and vulnerability checks on digital financial infrastructure (ex. public webpages) of financial companies to find potential vulnerabilities and take necessary measures. In order to support the autonomous security system so that financial companies can self-inspect their vulnerabilities, technical support and training such as upgrading evaluation methods and inspection tools are provided.

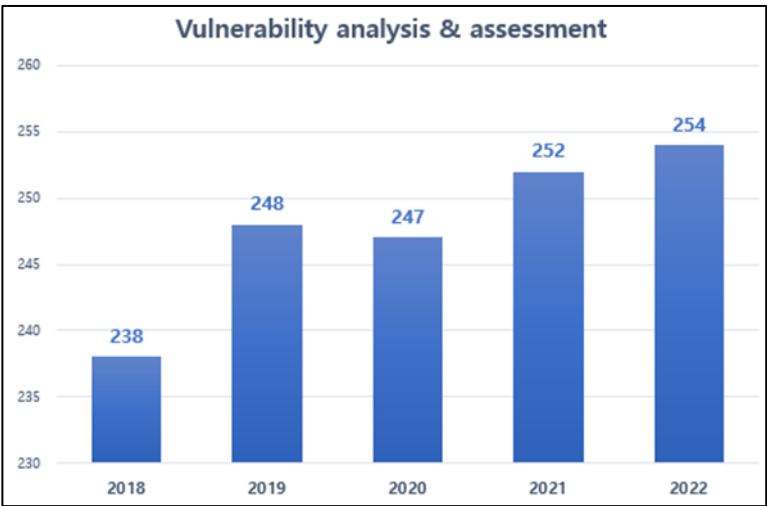


Figure 7. Total Vulnerability Analyses and Assessments

Areas : Areas of Inspection: information security management systems, servers, database, network, network equipment, information security system equipment, web applications, mobile applications, HTS(Home Trading System) applications, penetration testing etc.

3. Publications

FSI-CERT analyzes various cyber threat and uploads monthly financial security trend reports on the website, Also, FSI-CERT selects research topics and publishes cyber threat intelligence reports every year.



Voice Phishing App Distribution Group Profiling

This report analyzes malicious applications collected from January to September in 2021 and selects three major voice phishing malicious application distribution organizations. It also conducts research on the change in functions, profiling items, and profiling analyses of voice phishing malicious applications per distribution organization and studies further into additional distribution situations of such applications.

- Download: www.fsec.or.kr/bbs/detail?menuNo=244&bbsNo=6753

Malicious APK Deforming ZIP File Format Found under Experiment in the Wild

This report examines a number of analysis interruption techniques used in the process of analyzing malicious applications and suggests countermeasure techniques for a smooth analysis process.

- Download: www.fsec.or.kr/bbs/detail?menuNo=244&bbsNo=6879

4. Organized/Hosted Events

- Voice Phishing Response Meeting
- New Technology in Financial Security Seminar
- FISCON 2022 (Financial Information Security Conference)
- Financial Security Camp for university students
- Financial Security Seminar at Korea Fintech Week 2022
- FSI Data Challenge 2022
- Financial Sector Bug Bounty program
- FIESTA 2022 (Financial Institutes' Event on Security Threat Analysis)
- Financial Sector Threat Identification Working Group Meeting
- Financial Sector Malware Working-level Meeting

5. Conferences and Presentations

- 2022 Asia Pacific Summit, hosted by FS-ISAC(Singapore, August)

6. Collaboration with APCERT

At the 2020 APCERT online training session, FSI-CERT presented on the topic "ATM Cyber Attack." FSI-CERT looks forward to participating continuously in various seminars of APCERT to share research and information of the financial security sector.

7. Conclusion

Cyber security threats such as the dark web, cloud security threats, COVID-19, and cyber warfare are increasing day by day. Accordingly, FSI-CERT will continue to enhance cyber security systems—such as the financial ISAC(Information Sharing and Analysis Center), digital forensics, malware analysis, etc.—to combat such increasingly developing security threats. In addition, FSI-CERT will follow by its mission of providing a safe environment for the financial industry by incorporating new technologies (ex. big data, AI, etc.) into cyber security.

KZ-CERT

Kazakhstan Computer Emergency Response Team

1. About KZ-CERT

National Computer Emergency Response Team (KZ-CERT) is a single center for national information systems users and kazakhstani Internet segment providing collection and analysis of cyber incidents report as well as consultative and technical assistance to kazakhstani users in prevention of cyberthreats.

1.1 History

KZ-CERT was established in 2011 on the basis of republican state enterprise with the right of economic management "Center for Technical Support and Analysis in Telecommunications".

On January 28th, 2013, the government of Kazakhstan adopted a decree to rename the republican state enterprise with the right of economic management "Center for Technical Support and Analysis in Telecommunications" as the republican state enterprise with the right of economic management "State Technical Service". Eventually, in 2020, the RSE with REM "State Technical Service" had undergone its final reformation into the joint-stock company "State Technical Service" by another governmental decree.

Apart from that, in 2017, there was also an establishment of the National Coordination Center for Information Security which combines now the operation of both KZ-CERT and Government SOC.

1.2 Resources

Currently, KZ-CERT employs more than 20 people of various profiles.

2. Activities and Operation over 2022

KZ-CERT is responsible for detecting, processing and neutralizing the following computer incidents:

- brute-force attacks;
- botnets;

- malware;
- phishing, spam attacks;
- vulnerability exploitation;
- unauthorized access and modification of network infrastructure and information resource data.

2.1 Incident Handling Report

In 2022, KZ-CERT has handled 18 315 cybersecurity incidents. The majority of incidents managed are associated with the creation and distribution of malware. Figure 1 shows a more detailed information on their types.

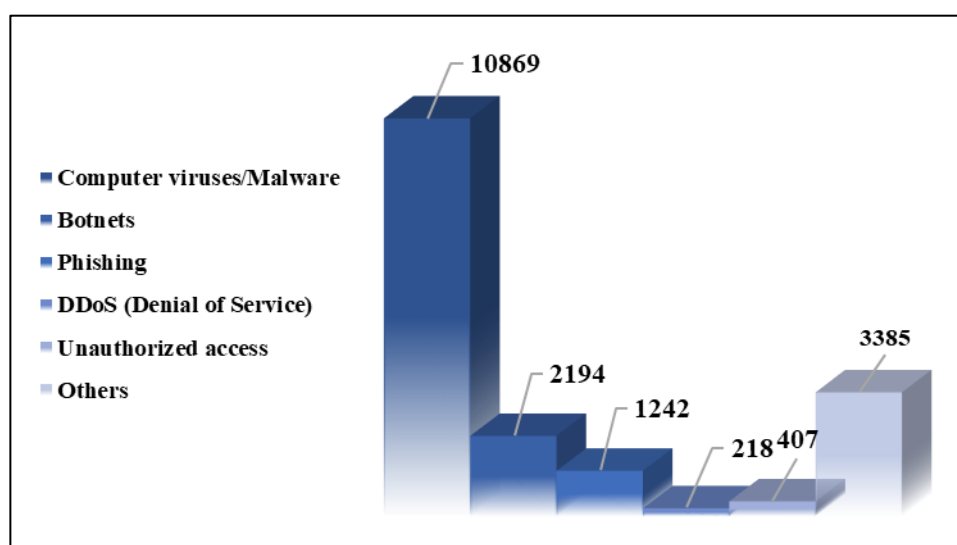


Figure 1. Types of the incidents handled by KZ-CERT over 2022

2.2 2022 Cyber Incident Case Example

On January 6th, 2023, at 9:42 AM KZ-CERT received an incoming report through the On-Call Service Telegram chat of the National Coordination Center for Information Security of JSC STS (head organization of KZ-CERT), which contained information on the computers of a quasi-public sector organization of Kazakhstan infected by encryption virus.

At 12:00 PM KZ-CERT sent its mobile unit to visit the organization for investigation.

During the course of investigation, it was detected that as part of the cyber incident response, employees of this organization isolated the infected hosts from the network.

As a result of the cyberattack, there was an infection in 1C (CIS accounting platform) server, a domain controller, the workstations of the Head of IT Department, network administrator, and a specialist, including also the data from the network share which is a common directory for all employees of the organization.

To complete the analysis of the incident, KZ-CERT Team requested images of the infected workstations and the firewall. The examination of the received infected workstations images disclosed the following:

- organization's local network was not connected to the Internet through the Unified Gateway for Internet Access ;
- 1C RDP port was open;
- the firewall was used without a valid license;
- 1C server shared the same subnet with the domain controller;
- weak passwords were used;
- system authorization credentials were unsafely stored in one of the devices;
- some workstations were running Windows 7 operating system which is no more supported by Microsoft and has vulnerabilities.

KZ-CERT Team has provided recommendations on eliminating the cyber incident and preventing possible attacks in future. You can find the detailed report with indicators of compromise on the FIRST MISP Portal (<https://misp.first.org>, ID 136788).

2.3 KZ-CERT Statistics on International Alert Exchange

In 2022, KZ-CERT sent 1061 alerts to the foreign organizations of 48 countries and received 666 alerts from the foreign organizations of 33 countries. The top 10 countries for notifying KZ-CERT and getting notified by KZ-CERT are presented in Figure 2 and Figure 3, respectively.

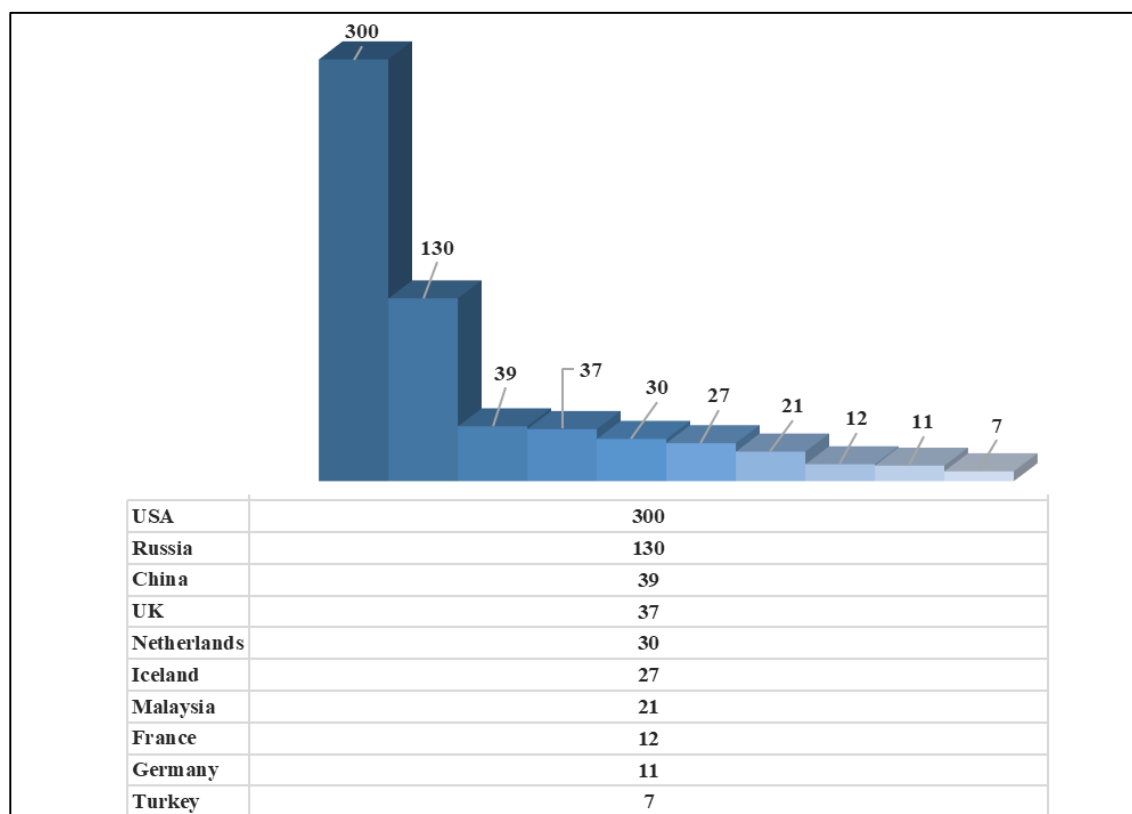


Figure 2. Incoming foreign alerts statistics over 2022

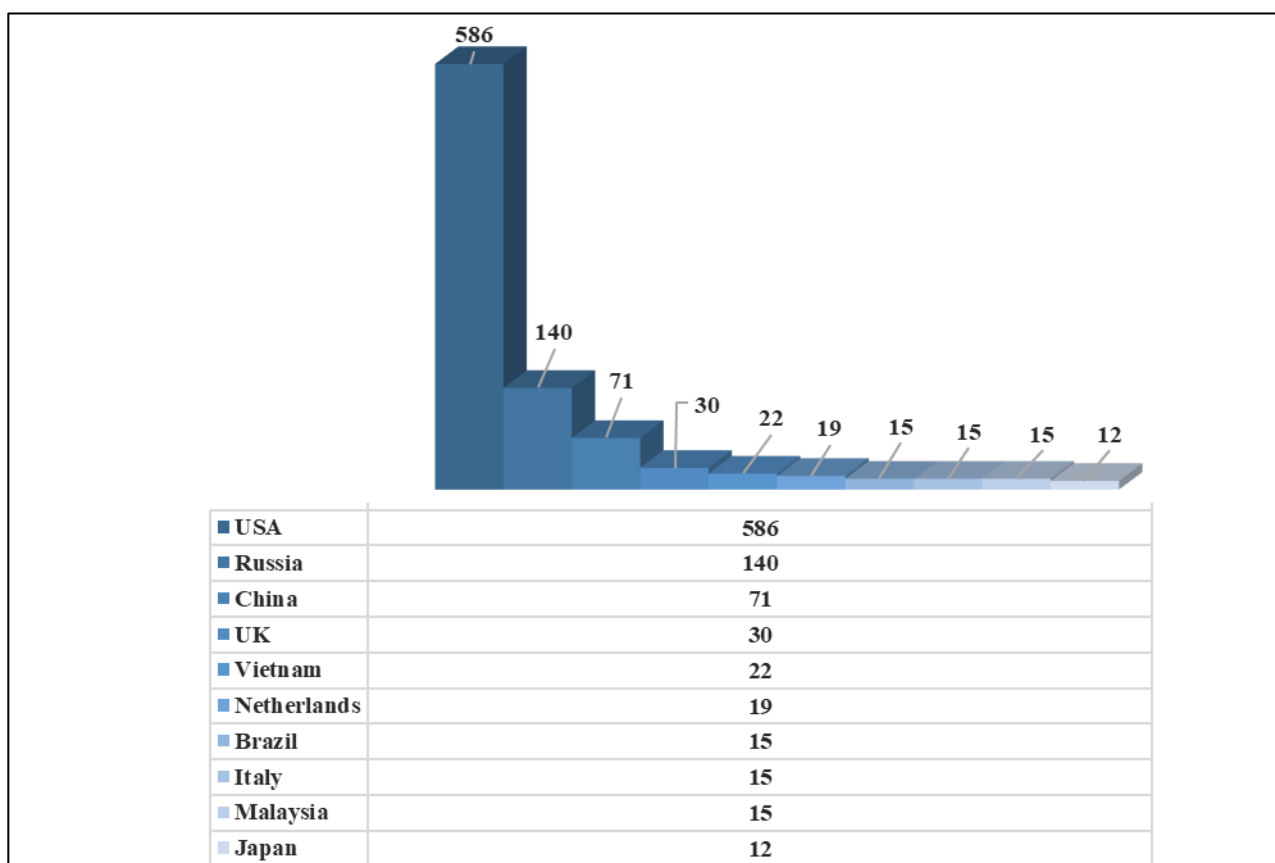


Figure 3. Outcoming foreign alerts statistics over 2022

2.4 Publications

The official website of KZ-CERT (cert.gov.kz), along with the newsfeed, features regularly published articles with recommendations on cyber hygiene and cybersecurity.

All materials are provided in three languages – Kazakh, Russian, and English.

For instance, you can find the following articles published in 2022:

- What does a cryptographer do and how to protect yourself? (cert.gov.kz/news/13/2042)
- Who you should take special precautions when shopping online (cert.gov.kz/news/13/2055)
- Guidance on receiving suspicious e-mails and text messages (cert.gov.kz/news/13/2054)
- Data leak: a guide for individuals and families (cert.gov.kz/news/13/2053)
- Configuring anti-spoofing controls (cert.gov.kz/news/13/2052)
- Basic tips for internet security (cert.gov.kz/news/13/2062)
- How to ensure data privacy in mobile applications? (cert.gov.kz/news/13/2058)
- Understanding patches and software updates (cert.gov.kz/news/13/2056)
- Recommendations for parents to ensure the safety of children on the internet (cert.gov.kz/news/13/2074)
- How to protect yourself from fraud on Instagram? (cert.gov.kz/news/13/2073)
- Kazakh Grafana users need an urgent update (cert.gov.kz/news/13/2079)

- Recommendations for owners of IP-addresses of Hikvision cameras (cert.gov.kz/news/13/2120)
- Recommendations for tourists on connecting to a public wi-fi network while traveling (cert.gov.kz/news/13/2128)
- Charity fraud (cert.gov.kz/news/13/2175)
- Spoofing (cert.gov.kz/news/13/2227)

2.5 Awareness-raising Activities

In 2022, KZ-CERT Team members organized visits to a number of educational institutions and state bodies in order to give lectures and provide trainings on cybersecurity. The program involved presentations on the following:

- computer viruses;
- malware protection methods;
- computer virology.

Apart from that, KZ-CERT Team members also contribute to awareness raising on cybersecurity through the national television. Accordingly, several appearances were made with the following topics:

- “Cyber Fraud and How to Protect Against It”
- “Information Security Threats”

3. Collaborations with APCERT members/partners and International Cooperation

KZ-CERT recognizes the importance of cooperation with similar teams and organizations. Therefore, we are 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 community, circulating important information, as well as maintaining the status of a national computer emergency response team on the global stage through the participation of employees in different international information security conferences and other events.

3.1 CyberDrills

The 10th Arab regional & OIC-CERT Cyber Drill 2022

On November 7, 2022, KZ-CERT Team members participated in the international Cyber Drill dedicated to National Arab CERTs, private CERTS. and critical sector security operation centers. The event was organized by the ITU Arab Regional Cybersecurity Center (ITU-ARCC) and the Organization of the Islamic Cooperation – Computer Emergency Response Team (OIC-CERT);

Arab States - CIS Inter-regional ITU CyberDrill

KZ-CERT Team members took part in the Arab States - CIS Inter-regional CyberDrill between September 14 and 16, 2022, in Almaty, Kazakhstan. The CyberDrill was held at the "KazHackStan 2022" conference and organized by the Telecommunication Development Bureau (BDT) of the International Telecommunication Union (ITU) at the invitation of the Ministry of Digital Development, Innovation and Aerospace Industry of Kazakhstan and the Center for Cyber Attack Analysis and Investigation (TSARKA). The CyberDrill was open to national CIRT/CSIRTs, ministries, regulators, telecommunication operators, universities and general education institutions, telecommunication equipment manufacturers, research and design institutes, software developers and other interested stakeholders of the ITU Member States, Sector Members, and Associates.

4. Events

In 2022, KZ-CERT has signed 3 Memorandums of Understanding/Cooperation in the field of cybersecurity.

Apart from that, Team members also actively attended various international conferences and meetings, including those hosted by organizations our Team shares the APCERT membership with. The following events can be mentioned:

- The 34th Annual FIRST Conference (in person, as a listener);
- The 17th Annual Technical Meeting for CSIRTs with National Responsibility (NatCSIRT 2022) (in person, as a listener);
- The KazHackStan 2022 conference (in person, as a speaker)
- FIRST Cyber Threat Intelligence Symposium (in person, as a listener);
- DEFCON (in person, 4th place in CTF contest)
- CAMP 7th Annual Meeting 2022 (in person, as a speaker);
- SCO and CICA Seminar On Combatting Cybercrime (online);
- OIC-CERT 10th General Meeting (in person, as a listener);
- Global Cybersecurity Forum 2022 (in person, as a listener).

APNIC

Asia Pacific Network Information Centre

1. About the organisation

APNIC is the Regional Internet Registry administering IP addresses for the Asia Pacific region. In addition, APNIC is also active in supporting capacity development and engagement activities related to cyber security. For more information about APNIC please visit <https://www.apnic.net>

2. Activities in 2022

The full report of APNIC's activities can be accessed on the official website:

https://www.apnic.net/wp-content/uploads/2023/03/APNIC_AR_2022_FINAL.pdf

3. Collaboration with APCERT members and partners

Here are some activities in 2022 which APNIC supported or contributed speaker/trainer:

- Presentation at MNSEC 2022 - organized by MNCERT/CC
- Invited instructor for APISC 2022 – organized by KrCERT/CC (KISA)
- Presentation at CNCERT/CC International Partnership Conference
- Table Top Exercise, collaboration with CERT NZ at PACSON AGM & Conference
- Linux forensics virtual workshop organized by CERT Tonga
- Invited instructor & speaker for Security Bootcamp 2022 organized by BtCIRT

4. Honeynet Project

APNIC operates a community honeynet project since 2019 and has been sharing relevant information with CERTs/CSIRTs and partners. For those who are interested please contact Adli Wahid (adli@apnic.net).

OIC-CERT

Organisation of The Islamic Cooperation – Computer Emergency Response Teams

1. About the OIC-CERT

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 2022, the OIC-CERT has a network and strategic collaboration with 59 members from 27 OIC countries. This alliance is further supported through the presence of 7 Commercial Members, 5 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 is 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 deals 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 deals with cybersecurity matters from non OIC-CERT member countries.

1.2.4 Commercial Members

These are industrial or business organizations that deals with cybersecurity matters from the OIC and non-OIC member countries.

1.2.5 Professional Members

Individual professionals mainly in cybersecurity not restricted to the OIC community.

1.2.6 Fellow Members

These are individual who are considered as co-founders of the OIC-CERT and have actively represent their organization as an OIC-CERT member for a minimum period of 5 years.

1.2.7 Honorary Members

Individuals or organizations who has demonstrated extraordinary contribution, support, and exemplary leadership to the OIC-CERT. Details of the members can be found at www.oic-cert.org

2. Activities & Operations

2.1 OIC-CERT 10th General Meeting & 14th Annual Conference, Muscat, Oman

After 2 years conducted the events virtually, the OIC-CERT 10th General Meeting & 14th Annual Conference was held in Muscat, Oman from 6-9 November 2022. The event organized in conjunction with the 10th Regional Cybersecurity Summit & the FIRST & ITU-ARCC Regional Symposium for Africa and Arab Regions with theme "Cybersecurity Innovation and Industry Development".

2.2 Online Trainings

To raise awareness on cybersecurity within OIC-CERT member states, 12 sessions of online trainings were conducted in 2022 as follows:

Date	Topic	Host
22 Feb	5G Security Framework Workshop	CyberSecurity Malaysia & Huawei
17 Feb	Webinar: Information Sharing and Analysis Center	CyberSecurity Malaysia & CISA
29 Mar	Arms Race: The Use of Neural Network Technology by Fraudsters	Group IB
16-17 May	Analyzing Network Artifacts	EG CERT
17-24 May	Certified Penetration Tester	CyberSecurity Malaysia
14-21 Jun	Certified Penetration Tester	CyberSecurity Malaysia
12-13 Jul	Network Forensic	NCCA
19 Jul	Managing Security Operation Center in Government Sector	NCCA
1 Aug	Risk & Threat Analysis on Internet of Everything (IoE)	CyberSecurity Malaysia
29-30 Aug	Analyzing Operating System Artifacts	EG CERT
23-30 Aug	Digital Security Professional Development & Lifelong Learning Program	CyberSecurity Malaysia
26 Oct	Emerging Threats in Social Media: Technology and Policy	UTeM

3. Events Involvement and Achievements

The OIC-CERT actively participated in cybersecurity events such as trainings, seminars, conferences, and meetings. The agency has contributed its competencies in the following events.

3.1 Cyber Drills

As in the previous years, the OIC-CERT organizes an international cyber drill for the members and partners. In 2022, Oman National CERT and ITU-ARCC organized the drill with the theme "The Rapid Evolving Of Cyber Threats Landscape In Parallel With Innovation In Cybersecurity Industry" on 7 Nov 2022. The event was held in conjunction of OIC-CERT 10th General Meeting & 14th Annual Conference. The objective of this drill is to measure the readiness of the participants in facing cyber-attacks.

Besides that, OIC-CERT members also participated in the APCERT Drill that was held on 25 Aug 2022.

3.2 OIC-CERT Journal of Cyber Security

The growth in cybersecurity research has encouraged the collaboration between the academia and industry practitioners. The OIC 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. 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.

In 2022, the OIC-CERT has published Volume 4, Issue 1 in Apr 2022. The journal consists of 7 papers. The OIC-CERT welcomed contribution from APCERT members for this journal. More details at <https://www.oic-cert.org/en/call-for-paper.html>

3.3 Cyber Security Guidelines/Procedures

The OIC-CERT has published several cyber security guidelines in 2022. The guidelines are as follows:

- Security Frameworks & Models for Organizational Architecture
- A guideline on security and privacy issues for social network owner
- Security Guidelines on Industrial Control System (ICS)
- Guideline on Internet of Things (IoT)
- Security Software Development Life Cycle (SSDLC) Guideline
- Cloud Security Guideline
- Wireless System Security Guideline
- Cloud Computing Security Guideline
- Promoting The Cyber Security Industry on a National Level
- OIC-CERT 5G Security Framework
- Awareness posters and presentations

3.4 Malware Trend Report

12 Monthly Malware Trend Reports have been published in 2022.

3.5 OIC-CERT 5G Security Working Group

OIC-CERT 5G Security Working Group was established in 2021 co-lead by Huawei (OIC-CERT Commercial member) and Malaysia. The WG consist of 10 members i.e., Bangladesh, Brunei, Indonesia, Pakistan, Somalia, Tunisia, Malaysia, Morocco, Oman and UAE.

The objectives of the WG are as following:

- Identifying 5G cybersecurity risks taking in account different perspectives from the stakeholders and maintaining a risk register
- Developing recommendations for our members, a 5G security standard that be a reference model for member states to develop their own National 5G cybersecurity standards
- Developing recommendations for developing an OIC-level 5G security framework that harmonize the requirements that allow for cross-recognition among OIC member states; and
- Develop an ISAC (Information Sharing and Analysis Centre) capability for CERT response in the era of 5G and Cloud for OIC member states under OIC-CERT

In 2022, the WG has done several rollout plan activities and developed the following documents:

- OIC-CERT 5G Security Framework Part 1: Cybersecurity Repository
- OIC-CERT 5G Security Framework Part 2: Baseline Security Technical Specification
- OIC-CERT 5G Security Framework Part 3: Cross-recognition Assurance Methodology

4. Collaboration with APCERT Members/Partners

4.1 OIC-CERT Malware Research and Coordination Facility

The Malware Research and Coordination Facility Project (Project) is facilitated by CyberSecurity Malaysia, which is the Permanent Secretariat of the OIC-CERT and the Convenor of the APCERT Malware Mitigation Working Group.

Analysis of the data provides early detection of malware, assists to provide awareness to the public, and for the cybersecurity personnel to act accordingly based on the shared information.

The Project uses LebahNET as the data source for research as the captured botnet activities are from the worldwide source and Kibana as the data analysis tool for the user to visualize the data from the LebahNET data.

5. Future Plans

5.1 Future projects

- OIC-CERT Cloud Security Working Group
- OIC-CERT Blockchain Working Group

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 2022

TLP:CLEAR