APCERT
Asia Pacific Computer Emergency Response Team

TLP: WHITE

APCERT ANNUAL REPORT 2021

TLP:WHITE

APCERT Annual Report 2021

APCERT Secretariat

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

CONTENTS

Message from the Chair 2021

The Asia Pacific Computer Emergency Response Team (APCERT), a collaboration of Computer Security Incident Response Teams (CSIRTs)/ Computer Emergency Response Teams (CERTs) within the Asia Pacific region, represents an international collaboration in information sharing for effective cybersecurity responses. The APCERT Annual Report is a compilation of the members' activities in an effort to provide some level of transparency of them mitigating cyber threats and information security incidents.

The past two tempestuous years have been challenging not only for the APCERT but the whole world. The Covid-19 pandemic has aghast the society at all levels. We are now living in a new norm where the people are reliant on digitally connected devices and systems much more than ever. This phenomenon increased the risks, vulnerabilities, and exposures to cyber threats, associated with the increase in remote working activities. CSIRTs/ CERTs must grab the bull by the horns to squarely face such risks and threats accordingly. The Covid-19 pandemic has somehow impacted the APCERT operations but despite the aleatory, it does not askew us from moving forward carrying out programmes that have been planned.

Because of such circumstances faced, it foundered us from having the APCERT Annual Conference 2020 in Colombo, Sri Lanka, costing us the opportunity for a physical meet and discovering the charm of Sri Lanka. However, the Steering Committee was steadfast in not breaking the tradition, thus the Annual General Meeting 2020 did proceed using an online platform. The same platform was also employed for the 2021 Annual General Meeting and Annual Conference. Now, we yen for physical meets for the Annual General Meeting and Annual General Meeting in 2022.

CSIRTs/CERTs organisations worldwide realise that international cooperation must be galvanized in mitigating cyber threats which bona fides as one of the pillars of cybersecurity framework. This led to the APCERT membership undergoing a meritorious growth, presently having 32 teams from 23 economies, 4 Corporate Partners, 4 Liaison Partners, and 4 Strategic Partners. We are happy to welcome the Forum of Incident Response and Security Teams (FIRST) as our newest Strategic Partner and sanguine about attracting new members in 2022 and beyond for omniscient

global cooperation.

The APCERT also continued with the Cyber Drill to edify the members' incident handing arrangements, an exemplary cross border collaboration in mitigating cyber threats and to validate and enhance any egregious communication protocols, technical capabilities, and quality of response. The APCERT Cyber Drill 2021, with the theme "Supply Chain Attack Through Spear Phishing – Beware of Working from Home", reflected real Internet incidents and issues that exist for supply chain attacks triggered by spear phishing. Participants are 22 CSIRTs/ CERTs (19 APCERT, 2 OIC-CERT and 1 Africa CERT) that took part in this exercise as follows:

1. Australia	2. Brunei Darussalam	3. Bhutan
4. Chinese Taipei	5. Hong Kong, China	6. India
7. Indonesia	8. Japan	9. Malaysia
10. Myanmar	11. Philippines	12. Republic of Korea
13. Singapore	14. Sri Lanka	15. Thailand
16. Tonga	17. Vietnam	18. Lao's People Democratic Republic
19. People's Republic of China	20. Kazakhstan	21. Tunisia

The APCERT Cyber Drill is an arch activity and a tradition that we hope to continue in the years to come. Our candour appreciation to KrCERT/CC for leading this initiative in 2021 and other members who have provided the necessary support to make this drill a success.

We would like to express our appreciation to every member for the camaraderie in supporting the APCERT activities, (be it the Steering Committee members, working groups team members, General members, Corporate members, Liaison members and Strategic Partners) and stirring the collaboration towards creating a safe, clean, and reliable cyber space in the Asia Pacific Region. We will strive to maintain a trusted contact of computer security network experts in the region to improve awareness and competency in cybersecurity.

Mohd Shamir bin Hashim
Chair, APCERT Steering Committee
CyberSecurity Malaysia

I. About APCERT

1. 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 of 56 economies. The list of those economies is available at:
https://www.apnic.net/about-APNIC/organization/apnics-region

2. 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_-_Sep_2020-1.pdf

As of December 2021, APCERT consists of 32 Operational Members from 23 economies across the Asia Pacific region, 4 Liaison Partners, 4 Strategic Partners, and 4 Corporate Partners.

Operational Members (32 Teams / 23 Economies)

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	CERT NZ	New Zealand
CERT-PH	Philippines National Computer Emergency Response Team	Philippines
CERT Tonga	Tonga Computer Emergency Response Team	Tonga
CNCERT/CC	National Computer network Emergency Response technical Team / Coordination Center of China	People's Republic of China
CyberSecurity Malaysia	CyberSecurity 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

Liaison Partners (4 Teams)

Team	Official Team Name	Economy
CISA	Cybersecurity and Infrastructure Security Agency	United States of America
FINCSIRT	Financial Sector Computer Security Incident Response Team	Sri Lanka
FSI-CERT	Financial Security Institute – Computer Emergency Response Team	Republic of Korea
KZ-CERT	Kazakhstan Computer Emergency Response Team	Kazakhstan

Strategic Partners (4 Teams)

Team	Official Team Name
AfricaCERT	Africa Computer Emergency Response Team
APNIC	Asia Pacific Network Information Centre
FIRST	Forum of Incident Response and Security Teams
OIC-CERT	Organisation of The Islamic Cooperation – Computer Emergency Response Teams

Corporate Partners (4 Teams)

Team	Official Team Name
Bkav	Bkav Corporation
Dell SecureWorks	Dell SecureWorks
Microsoft	Microsoft Corporation
Panasonic PSIRT	Panasonic Product Security Incident Response Team

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

At the APCERT AGM 2020, CyberSecurity Malaysia was elected as the Chair of the APCERT, and CNCERT/CC as the Deputy Chair.

Terms of each Steering Committee (SC) member are as follows:

Team	Term	Other positions
ACSC	2020 - 2022	
CNCERT/CC	2020 - 2022	Deputy Chair
CyberSecurity Malaysia	2021 - 2023	Chair
JPCERT/CC	2021 - 2023	Secretariat
KrCERT/CC	2020 - 2022	
Sri Lanka CERT|CC	2021 - 2023	
TWNCERT	2020 - 2022	

3. Working Groups (WG)

There are currently ten (10) Working Groups (WGs) in APCERT.

3.1 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 CSIRTs in the Asia Pacific region and others using the platform
  - Enhance the capability of global threat analyses by incorporating 3D Visualization features to the platform
- Secretariat (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

3.2 Information Sharing WG (formed in 2011)

- Objectives:
  - Improve information and data sharing within the APCERT, including by improving the members' understanding on the value of data sharing and motivating the members to exchange information
  - Organize the members to establish and enhance the necessary mechanisms, protocols, and infrastructures to provide a better environment for members to share information
  - 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 to 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

3.3 Membership WG (formed in 2011)

- Objectives:
  - Promote collaboration and participation by all the APCERT members
  - Establish the organizational bases to enhance the partnership with cross-regional partners and supporters
  - Guide activities such as checking and monitoring for sustaining the health of the membership structure
  - Promote harmony and cooperation among the members and partners
- 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

3.4 Policy, Procedure and Governance WG (formed in 2013)

- Objectives:
  - Promote the vision and mission of the APCERT through the development and coordination of policies and procedures for the APCERT and provision on advice regarding governance issues
  - In consultation with the SC, periodically review the Operational Framework to ensure it continues to achieve its intended effect, and provide advice to the SC
  - Review associated policies and procedures as they relate to the Operational Framework (also known as sub-documents), and supplement these with guidelines or other documents as needed
  - Identify and resolve issues relating to the APCERT policies, procedures, and governance, including referring them to the SC or APCERT membership where appropriate
  - Undertake other activities related to the policy, procedures, and governance of the APCERT as directed by the SC.
- Convener (1): ACSC
- Members (6): AusCERT, CyberSecurity Malaysia, HKCERT, JPCERT/CC, KrCERT/CC, Sri Lanka CERT|CC

3.5 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' cybersecurity 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

3.6 Malware Mitigation WG (formed in 2016)

- Objectives
  - Have a better understanding of the malware threats and analysis as well as the related potential impacts mainly within the participants' community
  - Educate and improve awareness, preparedness, and readiness in facing malware threats
- 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

3.7 Drill WG (formed in 2017)

- Objectives
  - To serve as a permanent Organizing Committee for the annual cyber drills and assist the Lead Organizing CERT
  - To maintain centralized documentation for the drills, their working documents, procedures, handbooks, and feedback
  - To allow continuous improvements
- Convener (1): KrCERT/CC (until August 2021)
- Members (11): ACSC, AusCERT, CERT-In, HKCERT, JPCERT/CC, SingCERT, Sri Lanka CERT|CC, TechCERT, ThaiCERT, TWCERT/CC, TWNCERT

3.8 IoT Security WG (formed in 2017)

- Objectives
  - Identification of the threat landscape and security challenges in IoT ecosystem
  - Proposing steps to address the security issues including vulnerabilities tailored for IoT
  - Recommendations for securing Internet of Things (IoT) ecosystem
  - Incident response mechanisms/measures for responding to cyber physical security incidents impacting human life
  - Discussions on existing Security Standards and gaps for IoT ecosystem and considerations for adoption
  - Development of threat sharing platform and threat sharing mechanism
- Convener (1): CERT-In

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

3.9 Secure Digital Payment WG (formed in 2017)

- Objectives
  - Build trust in secure usage of digital payments so as to ensure economic stability in the region
  - Study of vulnerabilities and security issues in digital payments
  - Recommendations for the security of digital payments ecosystem
  - Incident response mechanisms and measures for responding to cybersecurity incidents impacting digital payments
- Convener (1): CERT-In
- Members (5): BGD e-GOV CIRT, CNCERT/CC, HKCERT, JPCERT/CC, Sri Lanka CERT | CC

3.10 Critical Infrastructure Protection WG (formed in 2020)

- Objectives
  - Identify best practices for protecting ICS in CI sectors
  - Encourage CERT teams to prepare for the next era of cyber protection and incident handling with CI protection
  - Build the capabilities of the APCERT teams (through knowledge sharing activities) to face emerging threats
- Convener (1): Sri Lanka CERT | CC
- Members (5): ACSC(Observer), CNCERT/CC, CyberSecurity Malaysia, JPCERT/CC, TWNCERT

4. APCERT Website

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

II. APCERT Activity Report 2021

1. International Activities and Engagements

The APCERT has been dedicated to representing and promoting its activities in various international conferences and events. From January to December 2021, APCERT Teams have hosted, participated and/ or contributed to the following events:

- PacSON Session (14 April – Online)

On behalf of the APCERT, ThaiCERT conducted an online lecture titled "Microsoft Exchange Server Vulnerabilities" as part of PaCSON's webinar series.

- APEC TEL meeting (14, 18, 19 August – Online)

APCERT attended the TEL 63 SPSG meeting and the TEL 63 Plenary meeting to observe the progress of projects run by the working group and receive updates from the participating countries.

- APCERT Cyber Drill 2021 (25 August)

https://www.apcert.org/documents/pdf/APCERT_Drill2021_Press%20Release.pdf

The APCERT Cyber Drill 2021, the 16th APCERT cyber exercise drill, was successfully conducted to test the response capabilities of the participating APCERT Teams. 25 CSIRTs from 19 economies of APCERT (Australia, Bhutan, Brunei Darussalam, People's Republic of China, Chinese Taipei, Hong Kong, India, Indonesia, Japan, Korea, Lao People's Democratic Republic, Malaysia, Myanmar, Philippines, Singapore, Sri Lanka, Thailand, Tonga, and Vietnam) participated in the drill. From the external parties, CSIRTs from 2 economies (Kazakhstan and Tunisia) of OIC-CERT and AfricaCERT participated. The theme of the drill was "Supply Chain Attack Through Spear-Phishing - Beware of Working from Home -."

- AP* Retreat (13 September – Online)

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

- APCERT Annual General Meeting (AGM) and Conference 2021 (29-30 September – Online)

The APCERT Annual General Meeting (AGM) and Conference was held online. The whole event was for the APCERT community only.

- ASEAN CERT Incident Drill (ACID) 2021 (5 October – Online)

ACID 2021, led and coordinated by SingCERT, entered its 15th iteration with participation including ASEAN CERTs and APCERT Teams. The drill was completed successfully, providing an opportunity for teams to improve their skills on investigating and responding to ransomware incident, including malware analysis to uncover its characteristics, and subsequently escalating to the necessary parties for mitigation.

- FIRST & AfricaCERT Virtual Symposium for Africa and Arab Regions (7 December – Online)

The APCERT Cyber Drill was introduced at the FIRST African & Arab Symposium by KrCERT/CC as the representative of APCERT. The presentation focused on the importance of the cooperation among all APCERT members as the key to successful cyber exercise.

Other International Activities and Engagements

- DotAsia

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

- Forum of Incident Response and Security Teams (FIRST)

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

- STOP. THINK. CONNECT (STC)

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

- Asia Pacific Network Information Security Centre (APNIC)

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

- Africa Computer Emergency Response Team (AfricaCERT)

The APCERT and AfricaCERT signed a MoU in 2019.

2. APCERT SC Meetings

From January to December 2021, the SC members held 6 teleconferences to discuss the APCERT operations and activities.

Date	Location
27 January	Teleconference
17 Mar	Teleconference
2 June	Teleconference
3 August	Teleconference
7 September	Teleconference
1 December	Teleconference

3. APCERT Training

The APCERT held five (5) training calls in 2020 to exchange technical expertise, information and ideas.

Date	Title	Presenter
23 February	Implementing IoT Security Testing	HKCERT
6 April	Incident Management and Digital Forensics Investigation	CERT-PH
8 June	API Security	TWNCERT
13 July	For Operational Member on the APCERT DRILL	AusCERT
3 August	Zero Trust	SingCERT
2 November	How to automate advisories - CSAF Overview and Examples	CERT-Bund
7 December	Stop using Wi-Fi! It's DANGEROUS	ID-SIRTII/CC

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 the Activity Report on Chapter III and IV 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.

III. Activity Reports from APCERT Members

ACSC

Australian Cyber Security Centre – Australia

1. Highlights of 2021

1.1 Summary of major activities

Throughout 2021, Australian Signals Directorate's 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 2021, the ACSC continued a high-level of operational tempo, due to COVID-19-related cyber incidents.

1.2 Achievements & milestones

Throughout the 2020-1 reporting period, the ACSC actively worked across Australia to strengthen cyber security arrangements. The ACSC continued to work closely with government stakeholders, including the Australian Department of Home Affairs and the Australian Federal Police, to deliver the Australian Cyber Security Strategy 2020 objectives. This body of work will see an investment of $1.67 billion over the next ten years.

Key activities in 2020-21 included:

- Cooperating with federal entities to increase their cyber security posture, including conducting 14 cyber uplift activities. This effort assisted government agencies to better align themselves with the ACSC's Essential Eight Strategies to mitigate cyber security incidents, enhance basic cyber hygiene and business practices, and better equip agencies to respond to cyber security incidents.
- Publishing the Cyber Hygiene Improvement Programs (CHIPs) reports quarterly to Commonwealth, state and territory government agencies. These reports focus on measurable areas of cyber security, producing objective data to guide cyber security management.
- Engaging with the Digital Transformation Agency to support the Government Cyber Hubs Pilot as part of the Hardening Government IT Project (HGIT). The Hubs model is designed to uplift the cyber resilience of multiple Commonwealth entities and provide a cost-efficient way to implement a best practice, whole-of-government

approach to managing cyber threats across government systems.

- Partnering with 16 Australian government agencies to the Australian Protected Domain Name Service (AU PDNS), processing more than 5.5 billion queries and blocking over 400,000 malicious domain name requests.
- Updating the Australian Government Information Security Manual (ISM), aligning industry best-practices with the ACSC's Essential Eight Strategies.
- Updating the Information Security Registered Assessors Program (IRAP) policy and procedures. ACSC partnered with the Australian Cyber Collaboration Centre and Canberra Institute of Technology Solutions to deliver IRAP new starter training and examinations. The number of active assessors has grown by more than 20 per cent since the program reopened in January 2021.
- Improving the sharing of cyber security best practice information among federal government entities through the Chief Information Officer (CIO) / Chief Information Security Officer (CISO) and IT Security Advisor (ITSA) forums. During the reporting period, ACSC hosted three CIO/CISO forums and four ITSA forums.
- Providing technical cyber security advice and guidance to the Department of Defence in support of Australia's national naval shipbuilding enterprise, including the Future Shipbuilding and Future Submarine Programs.
- Responding to more than approximately 1,630 cyber incidents, assisting critical infrastructure, businesses and Commonwealth, state, territory and local governments.
- Publishing 27 Alerts and 12 Advisories on cyber.gov.au. Alerts provide timely notification on threats or activity with the potential to impact individuals, businesses, organisations, government, devices, peripherals, networks or infrastructure. Advisories provide information on current security issues, vulnerabilities, and exploits. There were more than 7.8 million visits to Alerts and Advisories on cyber.gov.au during the reporting period.
- Reporting over 1,500 cybercrime reports of malicious cyber activity related to the coronavirus pandemic. This included approximately 500 ransomware cybercrime reports, an increase of nearly 15% from the 2019-20 reporting period.
- Identifying that approximately one quarter of reported cyber security incidents impacted entities associated with Australia's critical infrastructure.
- Assessing that more than 75% of pandemic-related cybercrime reports involved Australians losing money or personal information.

2. About CSIRT

2.1 Introduction

The ACSC sits within the Australian Signals Directorate and leads the Australian Government's operational efforts on national cyber security. It collocates multi-agency Australian Government cyber security staff to improve the cyber security resilience of the Australian community.

Working with individuals, small to medium business, big business and critical infrastructure, the ACSC provides clear, timely and succinct advice during cyber incidents. The ACSC collaborates with small-medium sized enterprises, government, academic partners and cyber experts across Australia and overseas to investigate and deliver solutions to advanced cyber security threats.

2.2 Establishment

The ACSC commenced operations in 2014. 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, which itself had recently become an independent statutory agency within the Defence portfolio. This merger resulted in collocating cyber security experts from CERT Australia and the Digital Transformation Agency in a central location, providing whole-of-government cyber security services.

2.3 Resources

The ACSC consists of several hundred staff members, including those from partner agencies such as the Australian Criminal Intelligence Commission and the Australian Federal Police. The Department of Home Affairs Cyber Security Policy Division are also collocated within the ACSC to better inform policy development and advice for Government.

2.4 Constituency

The ACSC has a whole-of-economy remit. This includes providing cyber security advice and assistance to Australian governments, business and critical infrastructure, as well as communities and individuals.

3. Activities & Operations

3.1 Scope and definitions

The ACSC coordinates cyber security collaboration between the private and public sectors to increase cyber resilience and enhance information sharing. We provide advice and assistance across the whole of the 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:

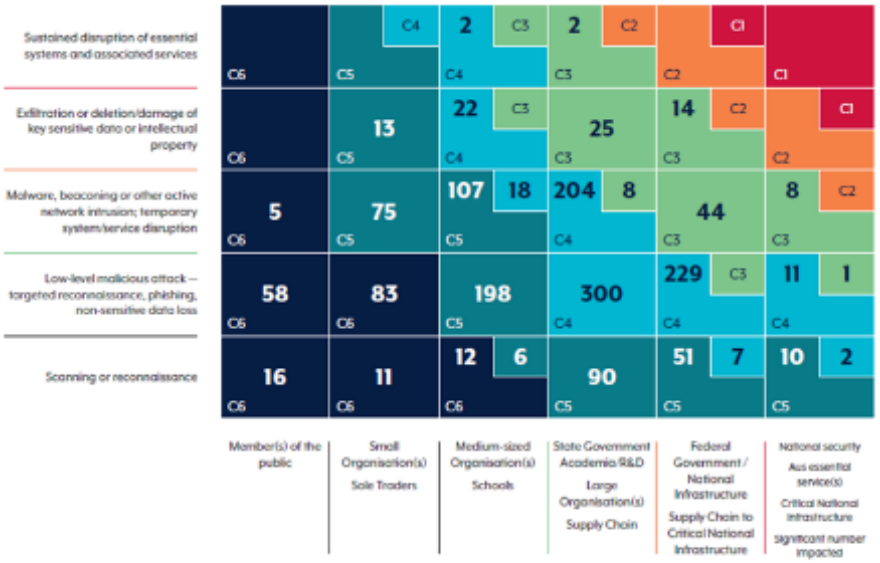
- Responds to cyber security threats and incidents across the whole-of-economy;
- Collaborates with the private and public sectors to share information on threats and increase resilience;
- Works with governments, industry and the wider community to increase awareness of cyber security; and
- Provides 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** allows the whole-of-economy to report cyber security incidents and provides additional assistance and referral pathways. During the 2020-21 reporting period, over 67,500 reports were made via ReportCyber. All relevant reporting was 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 2020–21 reporting period, ACSC has seen a significant increase in the number of calls to 1300 CYBER1. The number of calls in the 2020–21 reporting period totaled more than 22,000, an average of 60 calls per day. This is an increase of 310 per cent when compared with the previous reporting period, where ACSC received only 5,300 calls.

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.



Note: In order to manage the range and volume of reported incidents, the ACSC uses a cyber incident categorisation system to triage and prioritise responses to mitigate each incident. The ACSC categorises incidents based on severity of impact and extent of compromise. This allows the ACSC to focus its resources more effectively, and ensures a consistent approach and an appropriate level of response measures to each incident.

Figure 1

3.3 Abuse statistics

During the 2020-21 reporting period, the ACSC responded to 1630 cyber security incidents of varying significance. Although the 2020-21 reporting period saw a 28% decrease in cyber security incidents, a higher proportion were categorized as having a 'substantial' impact. This change is due in part to an increase in attacks by cybercriminals on larger organizations and the subsequent flow-on effects on victims. The majority of these incidents involved data theft, extortion and/or malicious cyber activity.

3.4 Publications

Throughout 2020-21, the ACSC used a variety of means to provide accurate and timely cyber security advice to Australians.

The ACSC produced:

- The 2020-21 Annual Cyber Threat Report. This report highlights key cyber threats affecting Australian systems and networks, using strategic assessments, statistics, trends analysis, and case studies to describe impact of malicious cyber activity on Australian networks.
- An updated version of the Australian Government Information Security Manual (ISM), the publication of advisory documents to cyber.gov.au, and the Partnership Portal. These ensure the advice provided remains relevant in a rapidly evolving threat environment.
- A new version of the Small Business Cyber Security Guide. This was developed to help small businesses protect themselves from the most common cyber security incidents.
- More than 40 step-by-step guides to support older Australians, families and businesses. These guides assist Australians in implementing sound cyber security practices, along with assistance to businesses to prevent and respond to ransomware attacks. The public consumption guides in particular provide individuals with reliable and practical information to evaluate and enhance their cyber security principles at home.

3.5 New services

In support of the whole-of-government approach to COVID-19, the ACSC provided technical advice and assistance to key private entities involved in the vaccine supply chain. Proactive support to assist with research and logistics was also provided, therefore reducing the risk of disruption to the vaccine distribution network.

ACSC also launched the Critical Infrastructure Uplift Program (CI-UP) pilot on 17 May 2021 to protect Australia's critical systems. This program aims to improve ACSC's understanding of the cyber security maturity of Critical Infrastructure and Systems of National Significance owners and operators. Over 100 entities had registered by the end of the 2020-21 reporting period.

4. Events organized / hosted

4.1 Training

ACSC provided essential support to critical infrastructure owners and operators throughout the 2020-21 financial year. Through the Joint Cyber Security Centers (JCSCs) and the Partnerships Program, ACSC has continued to provide high-quality cyber security services and advice to industry partners.

Key outcomes included:

- Expanding the reach and capabilities of the JCSC program. This was done by launching a Northern Territory (NT) Outreach Office in conjunction with the NT Government on 25 June 2021. This outreach office will improve ACSC's ability to engage with the NT Government and businesses, and will be crucial in developing strong partnerships with our NT partners.
- Engaging with critical infrastructure owners and operators through the Partnership Program and the JCSCs, including through information exchanges, sector specific working groups, and cyber security and threat briefings.
- Expanding the Partnership Program to include three tiers of membership: (i) Network, (ii) Business, and (iii) Home. The business and home membership tiers are designed to extend ACSC's services to smaller entities who previously might not have engaged with the program. By the end of the 2020-21 reporting period, the ACSC had: more than 1,700 network partners (a 230 per cent increase from the previous financial year); 2,000 business partners (a 190 per cent increase from the previous financial year); and tens of thousands of home partners.
- Initiating the next phase of the development of a Cyber Threat Intelligence Sharing (CTIS) capability, co-designed with industry partners to create a means to bi-directionally share cyber threat intelligence between the ACSC, industry and government stakeholders.

4.2 Drills & exercises

Through its National Exercise Program, the ACSC continued to conduct incident response cyber security exercises with critical infrastructure organisations, as well as cyber security training workshops for industry and government. COVID-19 continued to hinder the ACSC's ability to conduct in-person activities.

AquaEx, a major cyber exercise held in 2021, involved over sixty entities from Australia's critical infrastructure community. This exercise assisted the ACSC in updating its existing capability, threat and operational responses. Lessons learned evidenced the need to maintain pre-existing relationships and build trust between government and industry partners. Major outcomes included ensuring the presence of effective reporting avenues and the further development of incident response planning when engaging with industry partners.

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.

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). PaCSON is a community of 17 countries that delivers beneficial outcomes to the Pacific region. This group was designed to develop regional cyber security capability, including incident response, enhancing technical skills and knowledge, and reflecting best practice to strengthen cyber security defences. As PaCSON Secretariat, ACSC hosted the PaCSON Annual General Meeting virtually in May 2021. Additionally, ACSC supported the launch of the PaCSON website and portal during the reporting period, strengthening the connectivity and collaboration between PaCSON members.

5.2.1 Training

In 2021, the ACSC participated in four cyber bootcamps run by the Australian National University. These bootcamps were conducted with Indonesia, Thailand, the Philippines and Cambodia. The bootcamps provided the ACSC an opportunity to discuss Australia's perspective on cyber threats in the Indo-Pacific region, and informed partners as to how they can cooperate to mitigate these challenges.

6. Future Plans

6.1 Future projects

A key component of the Australian Cyber Security Strategy 2020 is the investment of $1.35 billion towards ACSC's Cyber Enhanced Situational Awareness and Response (CESAR) program. CESAR is designed to enhance protection and cyber resilience for all Australians, from providers of critical infrastructure to small-to-medium enterprises and individuals. The first year of CESAR implementation was a great success, and the ACSC now looks forward to focusing its efforts on enhancing the situational awareness of online threats faced by government, industry and the Australian public.

This package has enabled the ACSC to increase cooperation with government and industry partners. It has also facilitated the implementation of a number of pilot initiatives, such as strategic host-based detection and threat blocking. These initiatives deliver tangible benefits to Australia through detecting and blocking threats across government agencies.

7. Conclusion

As the ACSC moves into 2022, we remain steadfast in our resolve to continue our invaluable work with the APCERT community to collaborate on incident response and information sharing. We look forward to contributing meaningfully with you all to further build cyber resilience in our region.

AusCERT

Australian Computer Emergency Response Team – Australia

1. About CSIRT

1.1 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.

1.2 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.

1.3 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.

1.4 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).

2. Activities & Operations

2.1 Scope and definitions

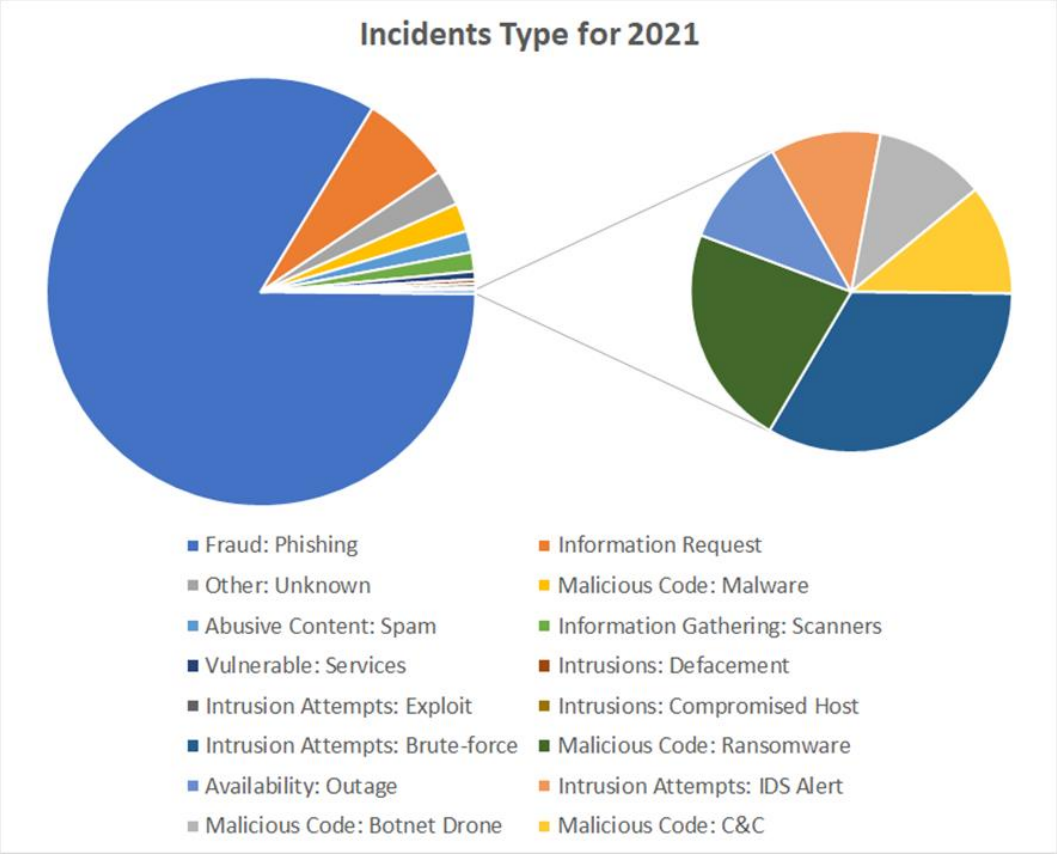
AusCERT monitors and evaluates global cyber network threats and vulnerabilities and remains on-call for members after hours. AusCERT publishes the Security Bulletin Service, drawing on material from a variety of sources, with recommended prevention and mitigation strategies.

Services provided are listed as:

- Incident Management [2.2], 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 [2.3] https://www.auscert.org.au/services/security-bulletins/
- Member security incident notification's (MSINs)[2.4] 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
- AusCERT's member only Slack
- AusCERT Conference https://conference.auscert.org.au/

2.2 Incident Management Service

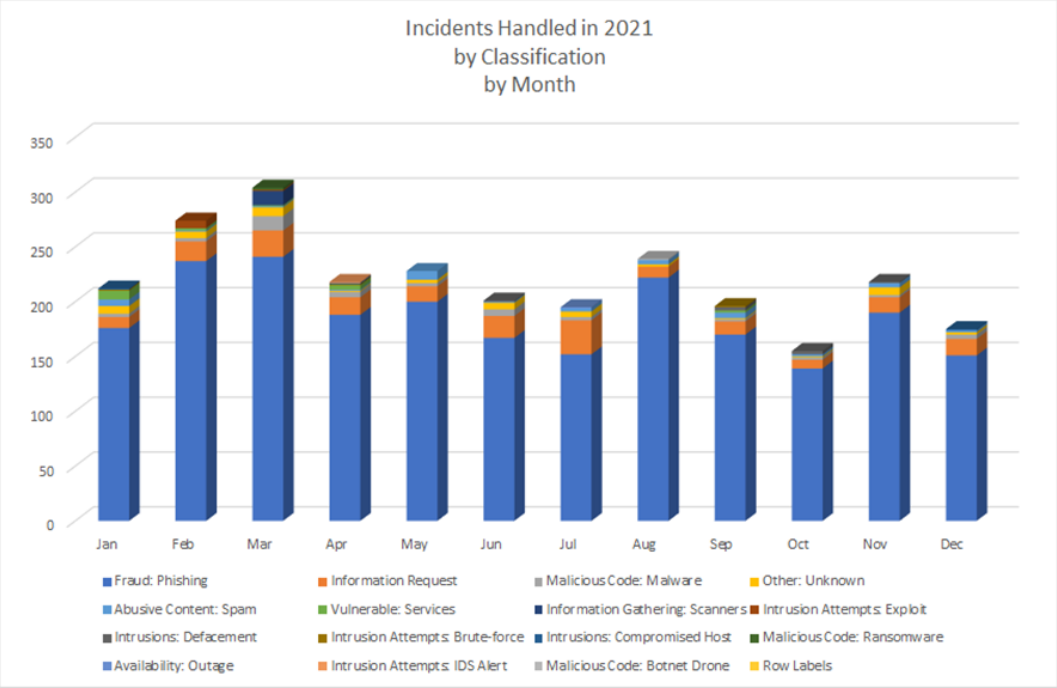
AusCERT's Incident Management Service (sometimes referred to as incident response) includes incident coordination and incident handling, both of which are standard inclusions as part of AusCERT's membership services. As a 24/7 membership benefit, it is perhaps AusCERT's most focal service offering.

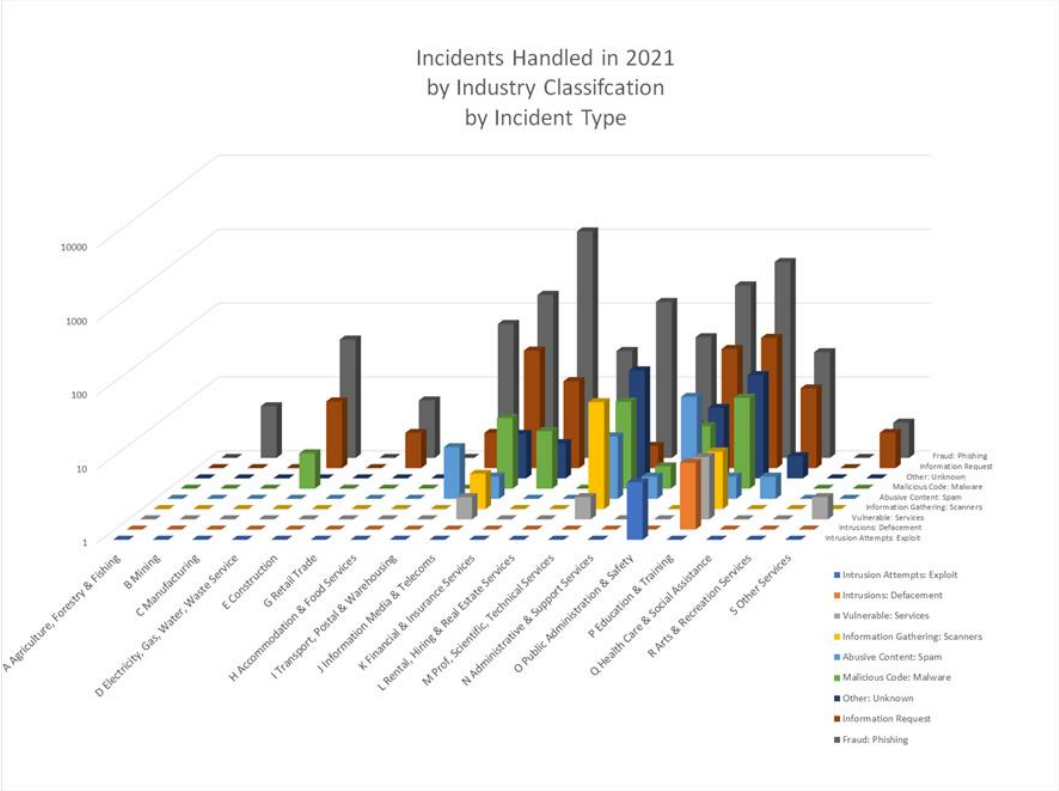


The diagram above is the statistics of incidents that required handling for the calendar year of 2021. Overall, AusCERT serviced 2795 tickets which resulted in an average of approximately 11 tickets per each business day of operation.

There are two further diagrams provided here which showcases the breakdown of incident classification types and incident classifications by month.

These tallies are sites that are located around the world that, when interacted with, affects the security of the constituency that AusCERT is serving. AusCERT members can utilise AusCERT's considerably large overseas and local contact networks for removal of phishing and malware sites.



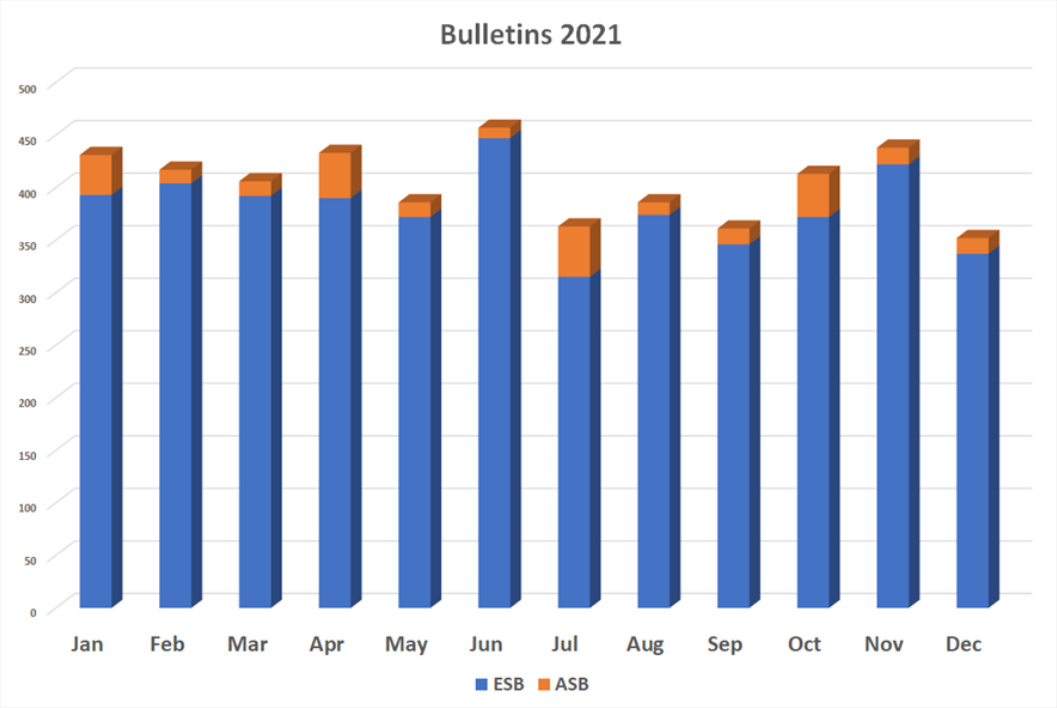


2.3 Security Bulletins

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.

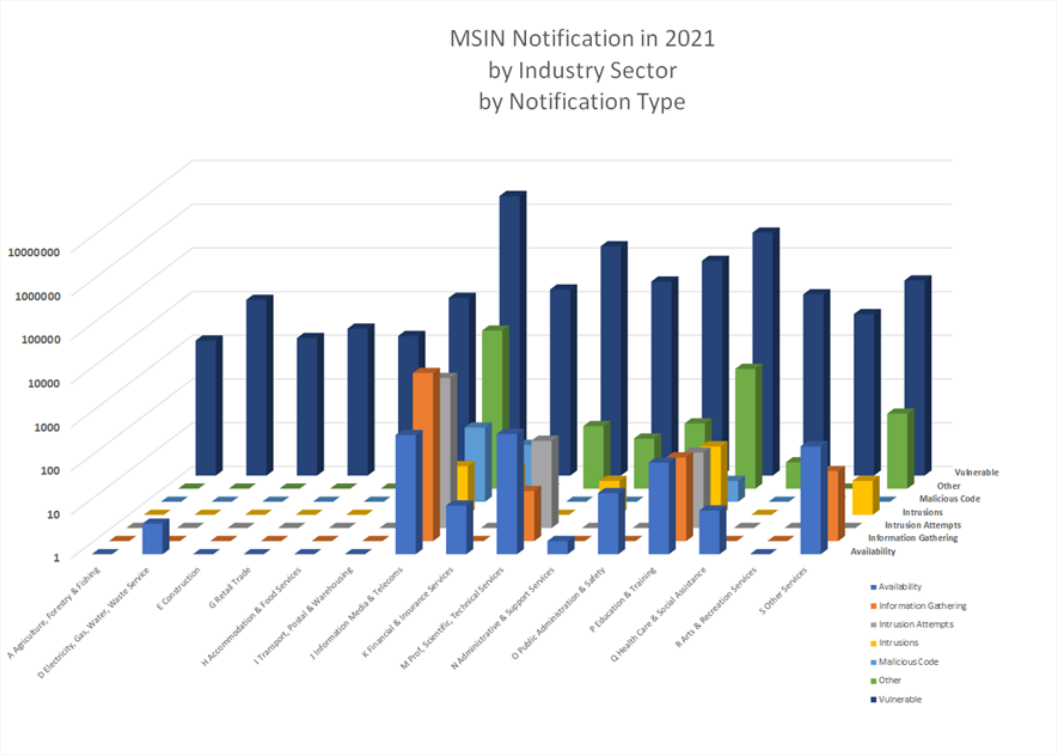
In 2021, 4564 External Security Bulletins (ESBs) and 279 AusCERT Security Bulletins (ASBs) were published.



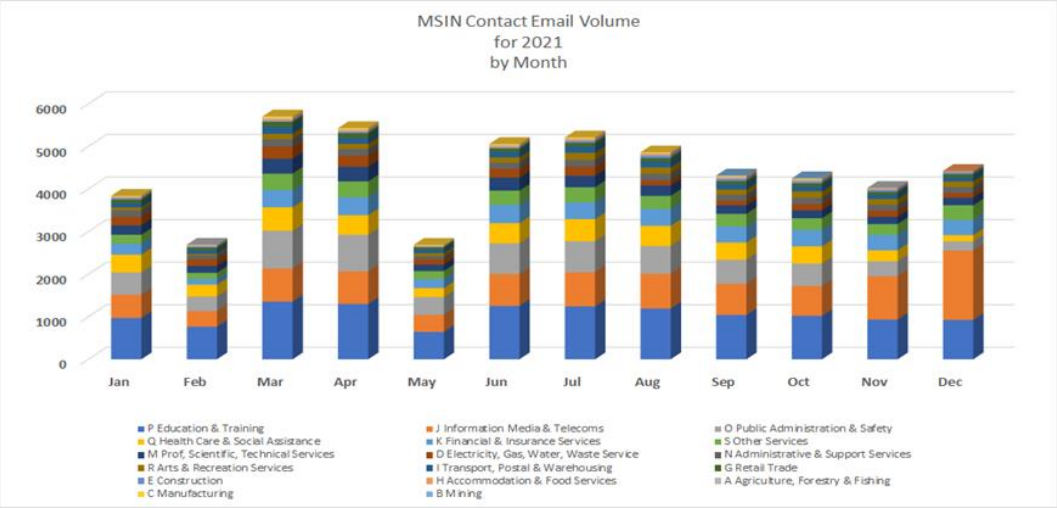
2.4 Member Security Incident Notifications

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).



The numbers of IoV far outweigh other categories and hence to be able to better display all the categories, the notifications are plotted on a logarithmic scale.



2.5 Publications

2.5.1 Week In Review

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

2.5.2 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.

2.5.3 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.

2.5.4 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. Events organized / hosted

3.1 Conferences and seminars

3.1.1 AusCERT Conference

The AusCERT Conference 2021, took place from 11th May -14th May 2021 in hybrid mode of both online and in-person with the theme of "SOARing with Cyber".

4. International Collaboration

4.1 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)

4.2 Drills & exercises

4.2.1 APCERT Drill 2021

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 "Supply Chain Attack Through Spear-Phishing". The drill fosters communication between the CERTs in the region and beyond. In all, 26 CERT/CSIRT teams from APCERT participated

4.2.2 ACID 2021

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.

5. Conclusion

AusCERT continues to deliver sought after computer security incident handling and early warning information to its constituency, whilst engaging members in cyber security.

As a membership-funded operation with an economy wide constituency, AusCERT has increased the breadth of its members organisations, enabling it to committed to its constituency quality services and support from AusCERT.

During 2021, and despite the continuing Covid-19 pandemic, AusCERT supported its operational capacity to provide timely information and maintain capability for the purpose of improving the cyber security posture of AusCERT's constituency.

Looking into the future 2022, and with the return to office mode of operation AusCERT will look into streamlining and automating processes that serve the two strategy points of Cyber Threat Intelligence and Incident Response.

BGD e-Gov CIRT

Bangladesh e-Government Computer Incident Response Team - Bangladesh

1. Highlights of 2021

1.1 Summary of major activities

- BGD e-GOV CIRT has successfully organized National Cyber Drill, Inter University Cyber Drill and also Cyber Drill for Financial organizations.
- Bangladesh has improved its rank to 32nd among 160 countries on the National Cyber Security Index (NCSI) in 2021.
- 873 cyber security incidents registered in our tracking system.

1.2 Achievements & milestones

- BGD e-GOV CIRT has successfully participated in OIC-CERT Cybersecurity Drill 2021 and achieved 2nd position.
- BGD e-GOV CIRT published "Cyber Threat Landscape Report 2021"
- Bangladesh Cyber Security Strategy 2021-2025 has been released.
- IT Audit Manual v1.0 is published

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 work 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 16 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.

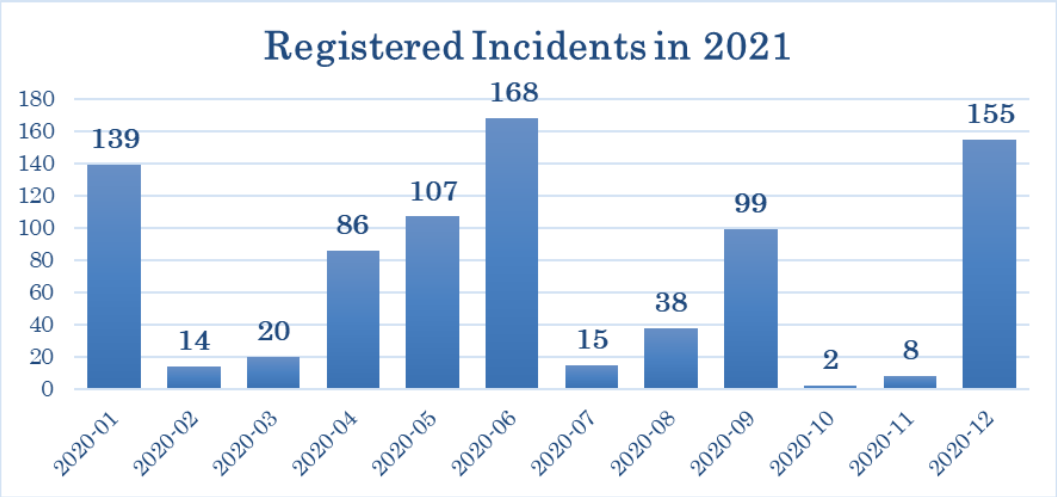
3. Activities & Operations

3.1 Scope and definitions

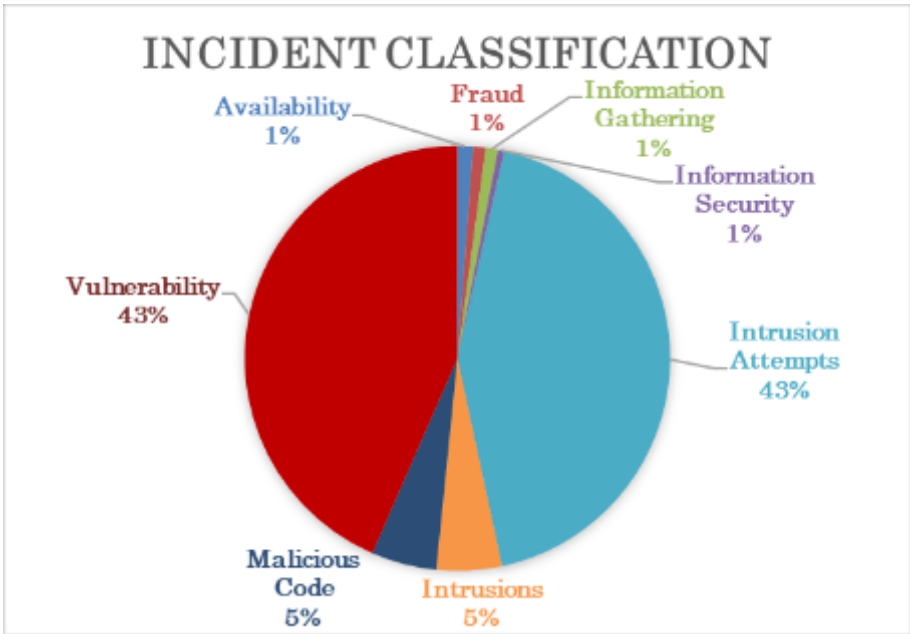
BGD e-GOV CIRT provide technical assistance and facilitate to manage cyber security in Bangladesh government's e-Government network and related infrastructure. BGD e-GOV CIRT also serve as a catalyst in organizing national cyber security resilience initiatives among various stakeholders. BGD e-GOV CIRT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

- BGD e-GOV CIRT published "Cyber Threat Landscape Report 2021"
- Bangladesh Cyber Security Strategy 2021-2025 has been released.
- IT Audit Manual v1.0 is published.

4. Events organized / hosted

4.1 Training

- Day long workshop on BGD e-GOV CIRT operations for ICT Division, Ministry of Post, Telecommunications and IT.
- Launching ceremony of "Bangladesh Cyber Security Strategy" and "CII Information Security Guideline, 2021"
- Seminar on "Digital Forensic Laboratory Guideline".
- Conducted training session for "Department of Women Affairs" on basic cyber security, digital security acts, cyber awareness.
- Conducted training session for "Bangladesh Institute of Bank Management" on cyber security, cyber security strategy, cyber awareness.
- Conducted training session for "Youth for Digital Awareness" on cyber security awareness.

4.2 Drills & exercises

- Arranged National Cyber Drill 2021.
- Arranged Inter University Cyber Drill 2021.
- Arranged Financial Cyber Drill 2021.

5. International Collaboration

5.1 Capacity building

5.1.1 Training

- Participated in the "3rd World Data Forum (UN)" in Switzerland.

5.1.2 Drills & exercises

BGD e-GOV CIRT has successfully participated in OIC-CERT Cybersecurity Drill 2021 and achieved 2nd position.

6. Future Plans

6.1 Future Operation

- Arrange Cyber Drills for different sectors.
- Perform risk assessment to critical infrastructure (CIIs).
- 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. Attachment (Photos)

Figure. Launching ceremony of “Bangladesh Cyber Security Strategy” and “CII Information Security Guideline, 2021”

Figure. Honorable minister of Maldives visited CIRT premises

Figure. Day long workshop for ICT division about cyber security

Figure. Cyber drill team for 9th Arab Regional & OIC-CERT Cyber Drill 2021

Figure. Training session at BIBM

Figure. Seminar on Digital Forensic Lab Guideline, 2021

Figure. National Cyber Drill organizer team

BruCERT

Brunei Computer Emergency Response Team – Negara Brunei Darussalam

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 66staff (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.

1.4.1 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.

1.4.2 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.

1.4.3 AITI

Authority for Info-communications Technology Industry of Brunei Darussalam (AITI) is an independent statutory body to regulate, license and develop the local ICT industry and manage the national radio frequency spectrum.

AITI has appointed ITPSS (Information Technology Protective Security Services), an IT local security company to become the national CERT in dealing with incident response in Brunei.

1.4.4 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.

1.4.5 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

2. BruCERT Operation in 2021

2.1 Incidents Response

In 2021, BruCERT had received a lot of reports from the public as well as from BruCERT security Intelligent sensors. Malware Infection is the most common cyberthreats upon Brunei Darussalam, there are few cases involving Ransomware. There is an increase in Reconnaissance as well as root level intrusion in Brunei. The statistic of the security incident is shown as Figure 1.

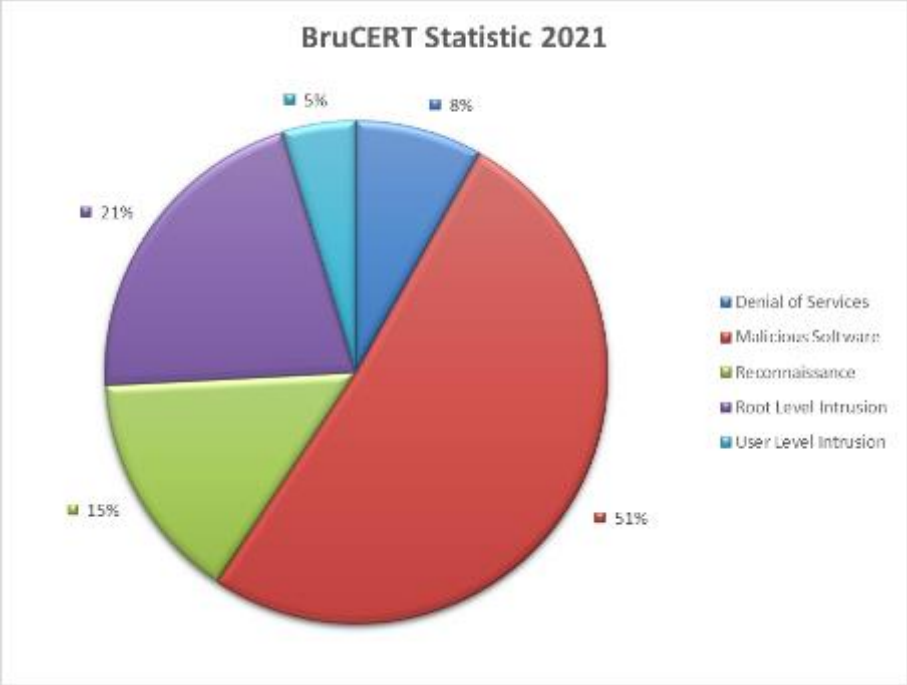


Figure 1

Types of Attack	Count
Denial of Services	309
Malicious Software	1939
Reconnaissance	562
Root Level Intrusion	798
User Level Intrusion	180

Table 1

2.2 BruCERT Honey Pot

The most abused port number is 1900 which is the UPnP followed by port number is 445, which in this case use by SAMBA (SMB). The third most abused port is port number 1433 which used by Microsoft SQL Server for database management It is assumed the attack on SMB might came from "WannaCry Ransomware", trying to exploit the vulnerability.

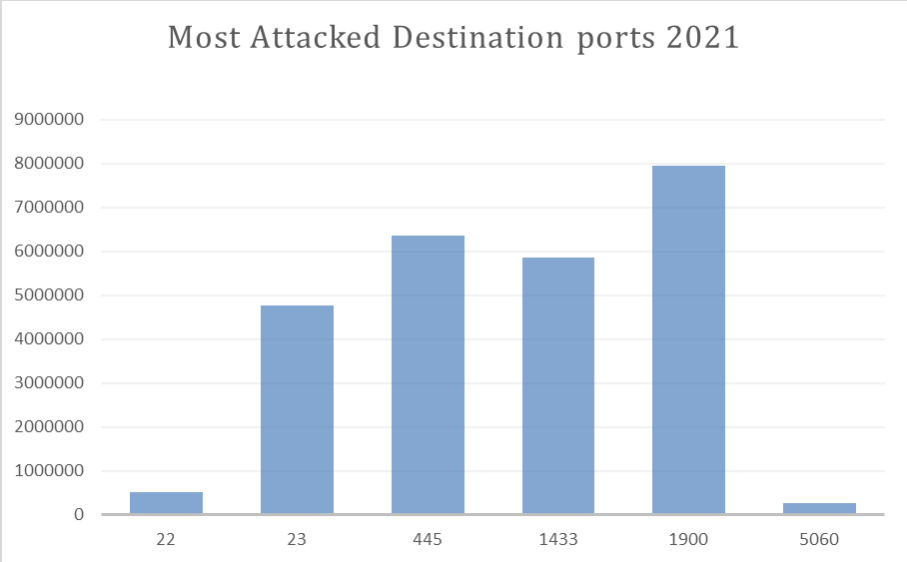


Figure 2

Port No:	Count
22	514573
23	4768959
445	6368525
1433	5863661
1900	7943676
5060	273847

Table 2

BruCERT honeypot managed to capture some of the malware hashes, in Figure 3 and Table 3, it shows the summary of the most detected malware in BruCERT Honeypot.

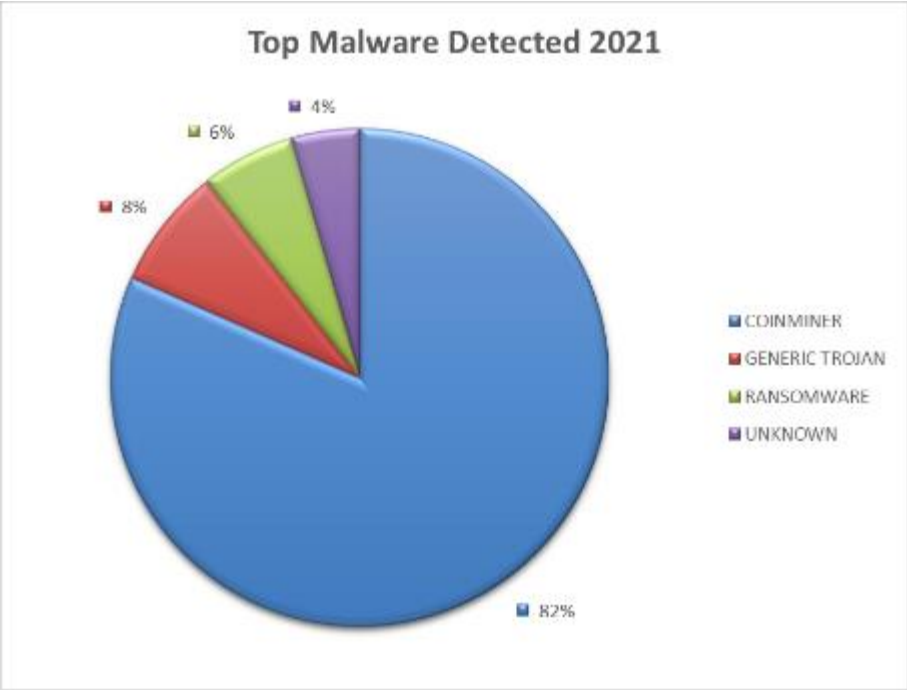


Figure 3

MALWARE TYPE	TOTAL
COINMINER	35740
GENERIC TROJAN	3445
RANSOMWARE	2674
UNKNOWN	1942
TOTAL	43801

Table 3

3. BruCERT Activities in 2021

3.1 Seminars/Conferences/Meetings/Visits

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

BtCIRT

Bhutan Computer Incident Response Team – Bhutan

1. Highlights of 2021

1.1 Summary of major activities

In 2021, although the COVID pandemic continued and the nation experienced a few lock downs and restrictions, BtCIRT was able to meet some critical targets for the year. The country's first ever "Cybersecurity Week" was successfully conducted. Articles and alerts on latest cyber trends, threats, vulnerabilities, and best practices were also published. Majority of the workshops and training were carried out online due to the pandemic.

1.2 Achievements & milestones:

- Production and airing of awareness videos on national television and online platforms
- First ever "Cybersecurity Week" from 20-25 December covering various programs including:
  - 3 simultaneous workshops,
  - Awareness programs through social media such as quizzes, talks and competitions to promote cyber hygiene,
  - In person awareness programs in banks, and
  - One day conference covering various topics on cybersecurity.
- 73 advisories published on latest scams and threats
- Critical Information Infrastructure identification framework developed
- 105 incidents handled

2. About BtCIRT

2.1 Introduction

Bhutan Computer Incident Response Team (BtCIRT) is a part of the Department of Information Technology and Telecom, Ministry of Information and Communications. The overall mission of BtCIRT is to enhance cyber security in the country by 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 central agency for cybersecurity activities and initiatives.

2.3 Resources

Currently, BtCIRT consists of 5 working team members.

2.4 Constituency

BtCIRT constituents are all government institutions which use 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:

- BtCIRT is a national contact in relation to cyber security issues.
- BtCIRT conducts end-user awareness at national level and disseminates information on threats and vulnerabilities and conducts security workshops related to various cyber security domains.
- BtCIRT actively monitors systems hosted in the Government Data Centre (GDC) for attacks and vulnerabilities and provides timely reports to the GDC operating team along with system administrators.
- BtCIRT also conducts periodic security assessment of government systems while for non-government organizations it provides services on request basis.
- Represent the country in international forums.
- BtCIRT also develops strategies, policies, standards, guidelines and baseline documents.

3.2 Incident Handling Report

105 incidents were handled in 2021, majority of which were vulnerabilities, followed by fraud and malware. The following graphs provide a number of incidents resolved on a monthly basis in 2021:

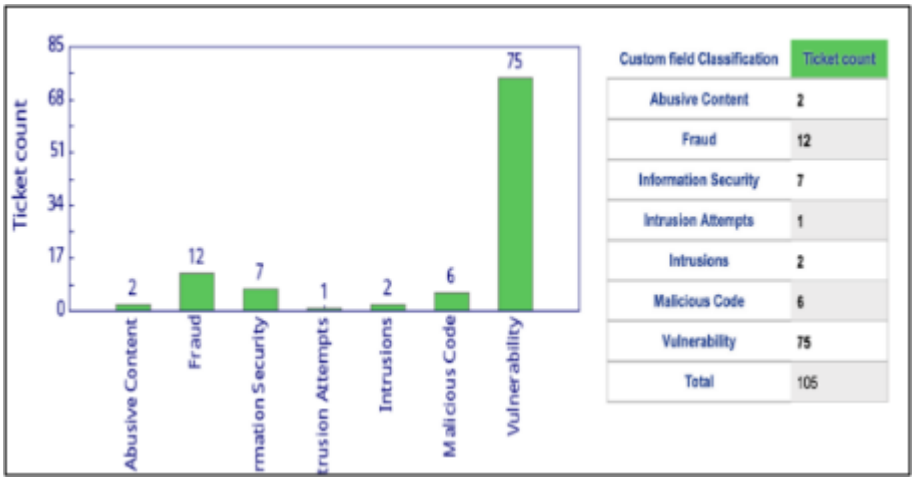


Figure 1: Incident Count by Classification

3.3 Critical Information Infrastructure(CII)

A Task Force was created with representation from critical sectors to carry out tasks related to research and study different global criterias and methodologies and develop a framework to identify CII sectors/services in Bhutan. Through a workshop among the taskforce members and a series of meetings with the members and stakeholders, a CII Identification Framework and Methodology was developed. The framework shall serve as a guide to identify future CII in the country.

3.4 Awareness creation:

i. BtCIRT developed 3 animation videos targeting school going children in our local language. The animation videos covered Online Predators, Privacy and Identity Theft and Gaming scams. The content was aired on national television (TV) and shared through various social media platforms.

ii. The team designed posters targeted towards school children, covering topics that are relevant to school going children. The posters were distributed to all Primary, Middle and Higher Secondary schools in the country.

iii. Videos related to WhatsApp OTP Scam were developed in-house and shared on BtCIRT Facebook page for advocacy.

iv. A 4-page article covering 'Online Safety Top Tips for High School students' was drafted for a local magazine that publishes content relevant to High school children and was distributed to all high schools for free.

v. BtCIRT participated in 2 panel discussions; one on WhatsApp OTP scam and general cyber hygiene, and the other one covering online scams, BtCIRT roles and initiatives and basic cyber hygiene.
vi. As a part of the Bhutan Cybersecurity Week, an Open Awareness Program was conducted in two local banks targeting the general public and a Cyber hygiene awareness program with high school students was also conducted.
vii. Other Social Media Activities such as quizzes and featuring of cybercrime victim stories were also conducted as part of the Bhutan Cyber security week.

3.5 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 73 alerts and advisories were published. 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

i. A week-long online training on Linux Forensics for System Administrators was conducted from 17-21 May 2021 in collaboration with APNIC.
ii. The following workshops were carried out as a part of the Bhutan Cybersecurity Week from 20-22 December 2021:
    - Network Security Workshop
    - Web Application Security Webinar
    - Mutually Agreed Norms for Routing Security (MANRS)
    - Cyber Security Awareness Workshop

5. International Collaboration

5.1 International partnerships and agreements

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

5.2 Capacity building

i. Trainings

BtCIRT participated and benefited from the following trainings:

Date	Title	Organiser/Trainer
6 - 10 September 2021	Online programme on Integrated Management Systems (IMS) – IT Service Management (ITSM) of ISO/IEC 20000-1, Information Security (ISMS) of ISO/IEC 27001 and Business Continuity (BCMS) of ISO 22301 Management Systems.	Malaysian Technical Cooperation Program
15-19 June 2021	Hands on Training on Fundamental Web and Application Security Issues for NREN Professionals	Institute of Information Technology (IIT) University of Dhaka Bangladesh
22 -26 November 2021	Integrated Cybersecurity for Safer Digital Worlds	Singapore Cooperation Program
6 – 10 September 2021	Second Workshop under the Asi@Connect 3rd call grant "Uplifting Resources to Deploy IPv6, DNS/DNSSEC, identity access management and monitoring of the network performance and its security" Network Security & Performance Workshop.	Lanka Education and Research Network (LEARN)

ii. Drills and exercises

BtCIRT participated in the following drills and exercises:

- ITU Global Cyber Drill 2021, September-November 2021
- Annual APCERT Drill themed "Supply Chain Attack Through Spear-Phishing - Beware of Working from Home," 25th August 2021

iii. Seminars, Conference & Presentations

A Cybersecurity Conference Day was conducted on 23rd December 2021 as a part of the Cybersecurity Week. The conference was conducted in a hybrid format, both online and offline. The morning sessions covered various cybersecurity topics by international speakers from Sri Lanka CERT, APNIC, CSA Singapore and local speakers from the bank and BtCIRT.

Figure 2: Group picture of the on-site participants

The evening session was a Panel Discussion on the topic "Emerging Cybercrimes and Cybersecurity Risks, and the State of Bhutan's Preparedness."

6. Future Plans

- BtCIRT also looks forward to collaborating with more organizations internally and internationally to strengthen its cooperation.
- Conduct awareness programs in schools and colleges and through media outlets
- Implement National Cybersecurity Strategy
- Identify Critical Information Infrastructure and conduct risk assessments

7. Conclusion

The BtCIRT will continue to focus on improving its visibility in the country and to create awareness on the importance of cybersecurity. Importance will be given to training and human resource development of ICT officials in the government and critical sectors to improve our cyber threat resilience.

CERT-In

Indian Computer Emergency Response Team – India

1. Highlights of 2021

1.1 Summary of major activities

i. In the year 2021, Indian Computer Emergency Response Team (CERT-In) handled 1402809 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.

ii. CERT-In tracks latest cyber threats and vulnerabilities. A total of 618 security alerts, 52 advisories and 390 Vulnerability Notes were issued during the year 2021.

iii. CERT-In conducted 19 cyber security training and awareness programs for Government, Public and Critical Sector organisations including topics such as cyber threat landscape, deployment of techniques and tools in order to minimize security risk.

iv. CERT-In has contributed to 3 international exercise planning & scenario development and participated as player in 7 International cyber security drills in 2021.

v. CERT-In conducted 9 domestic cyber crisis exercises in 2021 for various Sectors and State Government Departments.

vi. CERT-In contributed to design and execution of India-ITU Cyber Drill 2021 for Indian entities. CERT-In experts also participated as expert panelist on "Strengthening Cyber Defenses through Effective Information Sharing – A CIRT Perspective".

vii. CERT-In was the convener of two APCERT technical working groups namely Internet of Things (IoT) Security and Secure Digital Payments.

1.2 Achievements & milestones

i. CERT-In is the listed member in Task Force for Computer Security Incident Response Teams / Trusted Introducer (TF-CSIRT/TI) since 24th June 2021

ii. 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.

iii. CERT-In is conducting cyber security exercises comprising of table top exercises, crisis management plan mock drills and joint cyber security exercises with organizations from key sectors to enable participating organizations to assess their preparedness in dealing with cyber crisis situations. Till to date, a total of 64 such exercises have been conducted.

iv. In 2021, CERT-In Signed Memorandum of Cooperation (MoCs) in the area of cyber security with JPCERT/CC, Japan and Nigerian Computer Emergency Response Team (ngCERT), Nigeria to enable information sharing and collaboration for incident resolution.

2. About CERT-In

2.1 Introduction

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

ii. CERT-In has been designated to serve as National nodal agency for incident response under Section 70B of the Information Technology Act, 2000. 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.

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

2.2 Establishment

CERT-In has been operational since January 2004.

2.3 Constituency

The constituency of CERT-In is the Indian cyber community and Indian cyberspace. CERT-In provides services to the 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 Indicators of Compromise, Situational awareness of existing & potential cyber security threats and Security Guidelines to help organizations 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 2021 is given in the following table:

Activities	Incidents in 2021
Security Incidents handled	1402809
Vulnerability Notes Published	390
Advisories Published	52
Security Alerts issued	618
Trainings Organized	19
Cyber Security Mock Drills/Exercises	
a) Domestic Drills/Exercises	9
b) International Drills/Exercises	7

Table 1. CERT-In Activities during year 2021

3.3 Abuse statistics

In the year 2021, CERT-In handled 1402809 incidents. The types of incidents handled were Website intrusion & Malware propagation, Malicious Code, Phishing, Distributed Denial of Service attacks, Website Defacements, Unauthorized Network Scanning/Probing activities, Ransomware attacks, Data Breaches and Vulnerable Services.

The summary of various types of incidents handled is given below:

Security Incidents	2021
Phishing	523
Unauthorized Network Scanning /Probing/Vulnerable Services	1160333
Virus/ Malicious Code	209110
Website Defacements	27408
Website Intrusion & Malware Propagation	1489
Others	3946
Total	1402809

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 securing websites to concerned organizations. A total of 27408 numbers of defacements have been tracked.

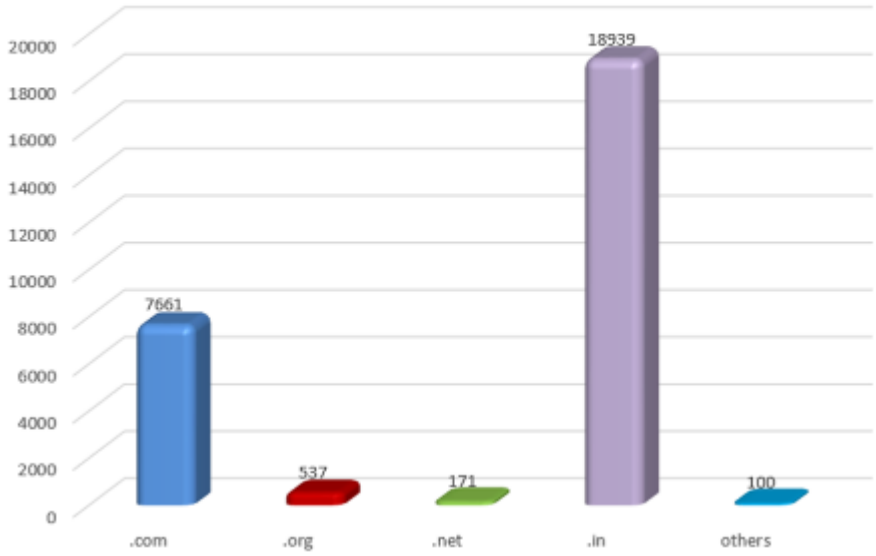


Figure 1. Indian Website Defacements tracked by CERT-In during 2021

3.3.2 Botnet Cleaning Initiatives

Botnet Cleaning and Malware Analysis Centre (Cyber Swachhta Kendra – https://www.csk.gov.in) 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 in collaboration with Internet Service Providers, antivirus companies, academia and Industry.

Currently, Cyber Swachhta Kenda (CSK) is covering ~94% of the subscriber base for notifications about botnet/malware infection. Organizations from various sectors including Communications (Internet Service Providers), Finance, Healthcare, Transport, IT & ITeS, Government, Academia, 'Industries & Manufacturing' and Energy are collaborating and being benefited by using CSK services.

CSK celebrated Cyber Swacchhta Pakhwada from 1-15 February 2021 and participated in Cyber Security Awareness Month in October 2021 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 tracked 44,36,41,608 botnet/malware infections in India and notified end users in collaboration with Internet Service Providers and organizations.

CSK provides two Free Bot Removal Tools (FBRT) developed in collaboration with “QuickHeal” and "eScan" with a cumulative of 16.74 lakh downloads recorded till December 2021.

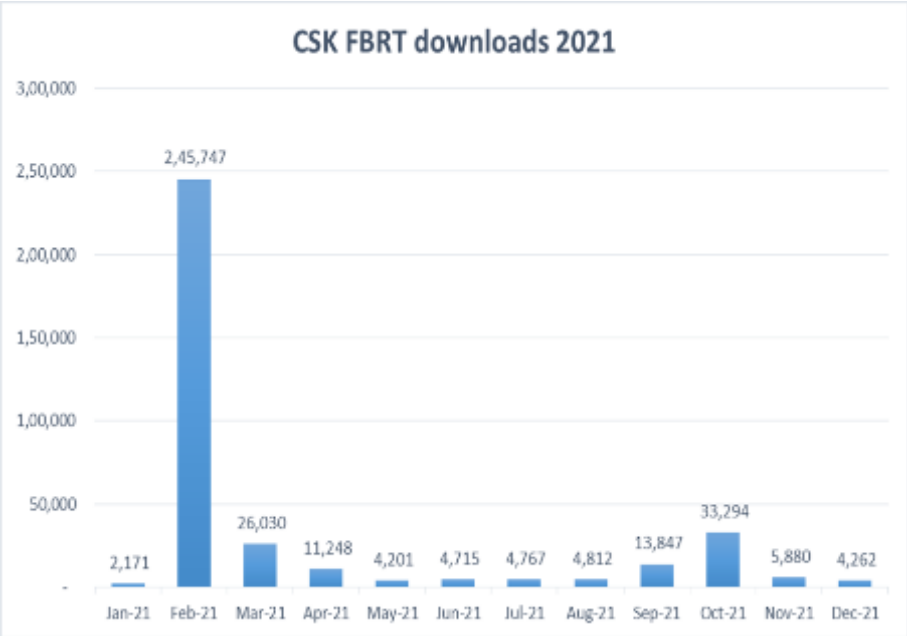


Figure 2. CSK Free botnet removal tools download statistics 2021

Botnets events processed by Botnet Cleaning and Malware Analysis Centre (Cyber Swachhta Kendra) during 2021.

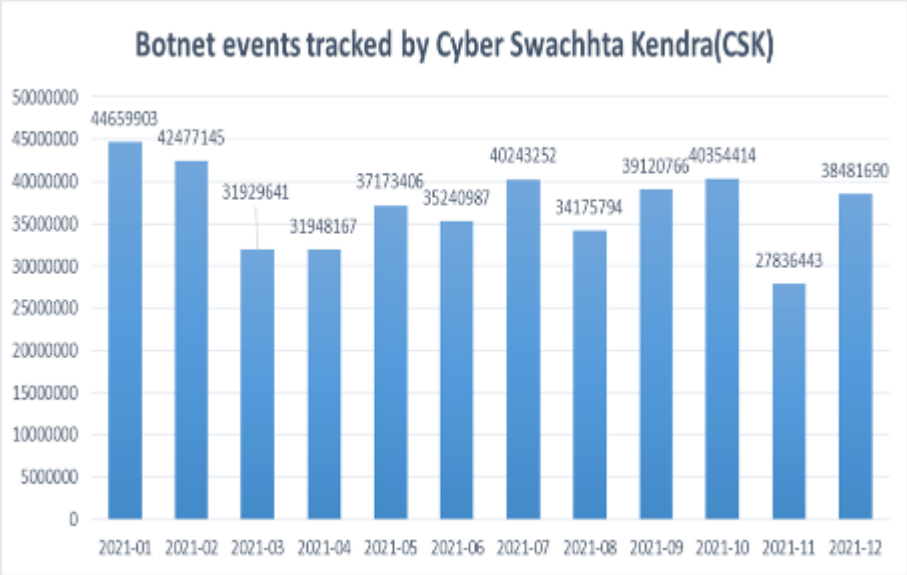


Figure 3. Botnet events tracked by Cyber Swachhta Kendra (CSK)

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 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 96 Information Security Auditing organizations, on the basis of stringent qualifying criteria, to carry out information security audit, including the vulnerability assessment and penetration test of the networked infrastructure of government and critical sector organizations. This list of CERT-In empanelled auditing organizations is being consulted frequently by the entities in Government and critical sectors for their auditing requirements.
- 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 empanelled technical IT security auditors are being used for technical as well as compliance audits.
- CERT-In has also carried out episodic security audits of key organizations for enhancing their security posture.

3.3.4 Cyber threat Intelligence Sharing

A core part of CERT-in mission as the Indian Cyber security responder with respect to Incident Response and Security Teams is to provide a trusted community platform for sharing cyber threat intelligence and situational awareness. Based on analysis, CERT-In releases Indicators of Compromises (IoC's) - operational, tactical and strategic, Alerts, Advisories & Vulnerability notes to update the Government and critical sector organizations about the threats and suitable necessary actions to counter those threats.

CERT-In has established its own Threat Intelligence eXchange platform based on STIX and TAXII standards and made operational. 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.

CISO's of various organizations are getting benefitted by the curated operational and tactical threat intelligence digest including Indicators of Compromise shared through an automated platform as well as email.

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.

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, 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.

Officers posted in Cyber Forensic Lab, CERT-In impart training through training workshops organized by CERT-In on computer forensics and mobile device forensics through lectures, demonstrations and hands on practical sessions, which covers seizing, preservation, processing and analysis of the raw data extracted from the digital items. CERT-In also supports other institutes in imparting trainings on various aspects of cyber forensics by delivering lectures along with demonstrations. The Cyber Forensics Laboratory, Indian Computer Emergency Response Team (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.

3.4 Publications

3.4.1 Working Group reports

CERT-In is the Convener of the IoT Security Working group across APCERT. The first report of the IoT Security working group was completed and circulated to the APCERT Operational Members and Partners.

3.4.2 Research Papers

- "Proactive Measures to Mitigate Cyber Security Challenges in IoT based Smart Healthcare Networks" published in IEEE Xplore Digital Library
- "The IoT Supply Chain Attack Trends- Vulnerabilities and Preventive Measures" published in IEEE Xplore Digital Library

4. Events organized / hosted

4.1 Training

i. 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. Due to the

COVID pandemic caused restrictions, CERT-In carried out online trainings/workshops on various issues relating to cyber security.

ii. In 2021, CERT-In has conducted 19 trainings on various specialized topics of cyber security. A total of 5169 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.

iii. 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 Cyber Security Awareness Month during October 2021 by organising various events and activities for citizens as well as the technical cyber community in India with a theme of "Do Your Part, #BeCyberSmart".

4.2 Drills & exercises

i. 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 2021.

ii. Till to date, CERT-In has conducted 64 Cyber security exercises of different complexities, including table top exercises, with participation from about 800 organizations covering various sectors of Indian economy from Government/Public/Private including Defense, Paramilitary forces, Space, Atomic Energy, Telecommunications(ISPs), Finance, Power, Health, Oil & Natural Gas, Transportation (Railways & Civil Aviation), IT/ ITeS/ BPO sectors and State Data Centers.

4.3 Conferences and seminars

CERT-In supported AVAR 2021 as a 'Supporting Partner'. The theme of AVAR 2021 Virtual was "Cybersecurity in Peril: The Changing State of Threat Actors"

5. International Collaboration

5.1 International partnerships and agreements

i. 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.

ii. In 2021, CERT-In signed bilateral agreements on cyber security cooperation with Japan and Nigeria 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.

iii. CERT-In is an operational member of Asia Pacific Computer Emergency Response Teams (APCERT). CERT-In is the convener of two working groups across APCERT namely “IoT Security working group” and “Secure Digital Payments working group” to address security threats and evolve best practices to secure these domains.

iv. 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.

v. CERT-In is a member of global Forum of Incident Response and Security Teams (FIRST). The membership in FIRST enables incident response teams to respond to security incidents more effectively in a reactive as well as proactive manner

vi. CERT-In is a listed member in the Task Force for Computer Security Incident Response Teams / Trusted Introducer (TF-CSIRT/TI) since 24th June 2021.

5.2 Capacity building

5.2.1 Training

i. CERT-In officials attended the KrCERT/CC's APISC training from 18th to 22nd October 2021
ii. CERT-In participated in the APCERT training “Implementing IoT Security Testing” on 23rd February 2021
iii. CERT-In participated in the APCERT training “Incident Management and Digital Forensics Investigation” on 6th April 2021
iv. CERT-In participated in the APCERT training “The OWASP API Security Top 10” on 8th June 2021
v. CERT-In participated in the APCERT training “Zero Trust (Sun Tze's way)” on 3rd August 2021
vi. CERT-In participated in the APCERT training “How to automate advisories - CSAF Overview and Examples” on 2nd November 2021
vii. CERT-In participated in the APCERT training “Stop using Wi-Fi! It's DANGEROUS” on 7th December 2021
viii. CERT-In participated in the JP-US-EU Industrial Control Systems Cybersecurity Week for the Indo-Pacific Region (FY2021) held during October 25-29, 2021
ix. CERT-In participated in the Cybersecurity Studies Course sponsored by George C. Marshall European Center for Security Studies during 30th November to 16th December 2021

5.2.2 International Drills & exercises

CERT-In has contributed in 3 international exercise planning & scenario development and participated as player in 7 International cyber security drills in 2021. Following are the brief of the exercises:

i. CERT-In participated in the APCERT Annual drill 2021 in August 2021 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 2021 was “Supply Chain Attack Through Spear-Phishing - Beware of Working from Home”. CERT-In also acted as exercise coordinator (EXCON) for international CERTs in the Drill.
ii. CERT-In participated in the 1st Africa Cybersecurity Drill and played in four scenarios from 30th June to 1st July 2021.

iii. CERT-In participated in the Arab Regional and Organization of The Islamic Cooperation – Computer Emergency Response Teams (OIC-CERT) Cyber Security Drill in September 2021.

iv. CERT-In participated in ASEAN CERT Incident Drill (ACID) – 2021 in October 2021. The theme of ACID Drill 2021 was 'Responding to Supply Chain Attacks Against Businesses'.

v. CERT-In participated in 6 days International Telecommunication Union (ITU) 2021 Global Cyber Drill in November 2021. The Drill was conducted in 6 different scenarios for each day.

vi. CERT-In contributed in the planning of Quantum Dawn VI exercise and also participated as player in the exercise in November 2021. Quantum Dawn is a global exercise series conducted by Securities Industry and Financial Markets Association (SIFMA). The objective of Quantum Dawn VI was to enabled key public and private bodies around the globe to practice coordination and exercise incident response protocols, both internally and externally, to maintain smooth functioning of the financial markets when faced with a series of sector-wide global cyber-attacks.

vii. CERT-In was actively engaged in coordination and planning of India-International Telecommunication Union India-ITU Cyber Drill 2021 in December 2021. CERT-In also participated as player in the exercise.

5.3 Other international activities

i. CERT-In participated in the APCERT AGM held on 29th September 2021

ii. CERT-In participated in the CISA Industrial Control Systems (ICS) Joint Working Group (JWG) meetings held in April and September 2021.

iii. CERT-In participated in the 14th Annual Cyber Security Week (CSW) of Sri Lanka organized between 25th to 29th October 2021

6. Conclusion

CERT-In is the National nodal agency for Incident response in the Indian constituency. CERT-In is working to enhance the security of Indian Cyber space. CERT-In looks forward to continuing to work with the APCERT community to make the Cyberspace safe and secure.

7. Contact Information

7.1 Postal Address:

Indian Computer Emergency Response Team (CERT-In)
Department of Electronics & information Technology
Ministry of Communication & information technology
Government of India
Electronic Niketan
6, CGO Complex, Lodhi Road
New Delhi – 110003, India

7.2 Incident Response Help Desk:

- Phone: +91-11-24368572
  +91-1800-11-4949 (Toll Free)
- Fax: +91-11-24368546
  +91-1800-11-6969 (Toll Free)

7.3 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: 2022-12-31
  - Key Size: 4096/4096
  - Fingerprint: A768 083E 4475 5725 B81A A379 2156 C0C0 B620 D0B4

7.4 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: 2022-12-31
- Key Size: 4096/4096
- Fingerprint: EABE 086A 6FC4 CB47 3F29 A90B DE30 A071 275C CACF

7.5 For queries related to botnet cleaning initiative:

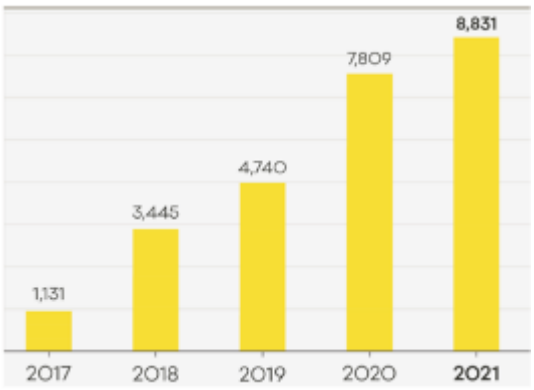
- Email: csk@cert-in.org.in
- PGP Key Details:
  - User ID: csk@cert-in.org.in
  - Key ID: 0x4EE11788
  - Key Type: RSA
  - Expires: 2022-05-31
  - Key Size: 4096/4096
  - Fingerprint: E204 D43D 0296 40FB 8DB9 0290 706D EF4D 4EE1 1788

CERT NZ

CERT NZ – New Zealand

1. Highlights of 2021

- In 2021, a total of 8,831 incidents were reported to CERT NZ, a 13% increase on 2020.



- CERT NZ's key annual awareness-raising activity, Cyber Smart Week, was held for the fifth year running, on 18 to 24 October 2021.
- This year the campaign saw a refresh of the iconic CERT NZ robots.
- 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 35 FTEs, including operations, communications & engagement, governance & analytical reporting staff. CERT NZ also has a contact centre to receive incident reports.

3. Activities & Operations

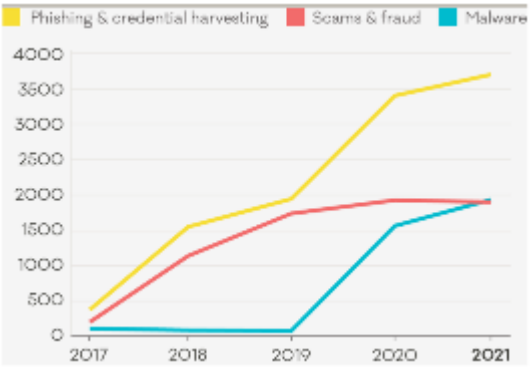
3.1 CERT NZ's key services are:

- 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.

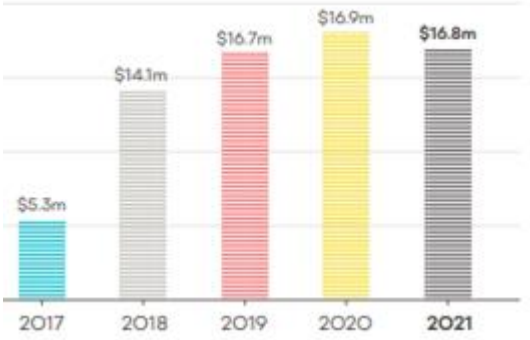
3.2 Top incident categories

'Malware' has continued its upward trend and overtaken 'Scams and fraud' as the second most common incident reported to CERT NZ in 2021, with 'Phishing & credential harvesting' remaining the top reported incident.

CERT NZ received 3,709 Phishing and credential harvesting reports in 2021, up 9% on 2020.



Of the reports received by CERT NZ in 2021 15% included a direct financial loss, with a combined total of $16.8million.



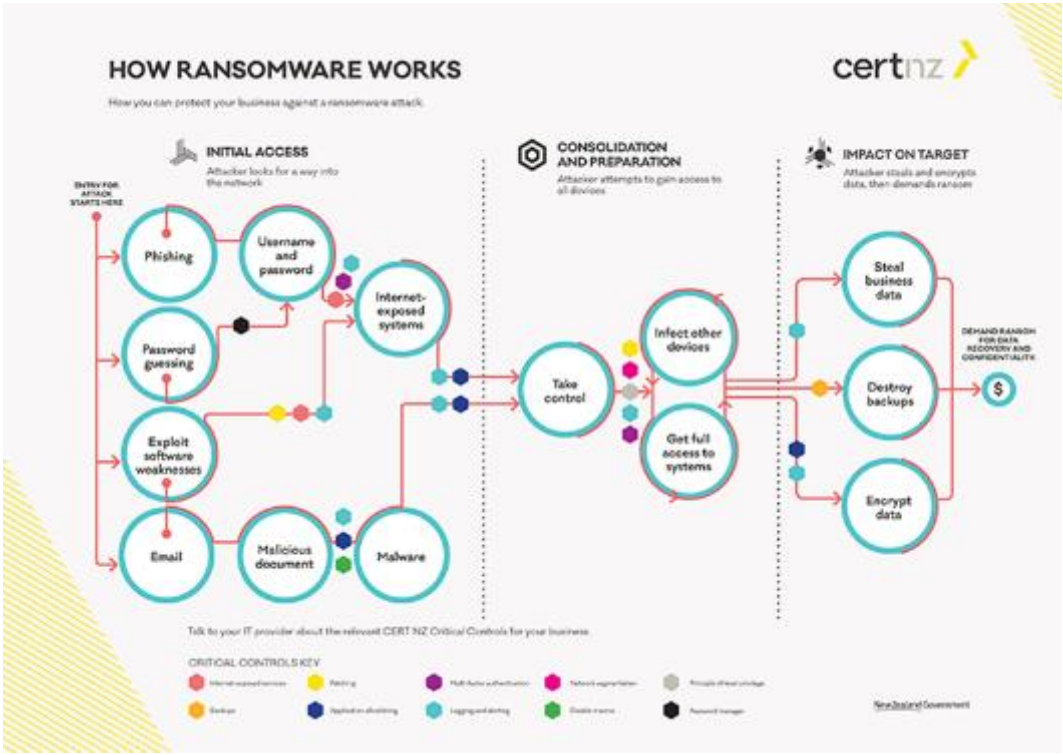
3.3 Publications

CERT NZ's quarterly reporting continued in 2021, with the publication of two reports each quarter:

- 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.

2021 saw CERT NZ publish updated critical controls which included two changes from 2020 with the addition of 'asset lifecycle management' and 'implement application control'. CERT NZ also published numerous pieces of content in response to people shifting to remote working arrangements due to the COVID-19 Pandemic.

With the growing prevalence of Ransomware CERT NZ published several new pieces of content to help organisations help understand it and how to best mitigate any attack.



The above diagram can be found at:
https://www.cert.govt.nz/business/guides/protecting-from-ransomware/
An IT Specialist version of the above diagram can be found at:
https://www.cert.govt.nz/it-specialists/guides/how-ransomware-happens-and-how-to-stop-it/

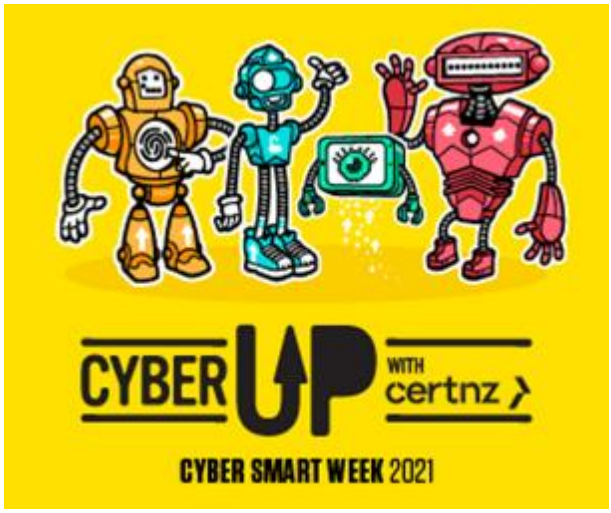
3.4 Social Media

CERT NZ has increased its use of social media in 2021 to reach our constituency. As well as building on our existing use of Twitter (@CERTNZ) and Facebook page https://www.facebook.com/certnzgovt CERT NZ launched a LinkedIn page to target businesses - https://www.linkedin.com/company/certnz/

4. Events organized / hosted

4.1 Campaigns

CERT NZ ran its fifth cyber security awareness campaign, Cyber Smart Week, in October 2021, which saw a refresh of the iconic CERT NZ robots. 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 290 partner organisations, up from 122 in 2020, achieving a combined 7 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 a password focused campaign in 2021, with supporting content including videos. Password perfect was a mini campaign targeting 54–64-year-olds to get better at creating strong passwords by using passphrases, stronger and easier to remember.

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 2021 has included:

- The PaCSON Remote Session Series – with nine sessions for 218 participants in 2021, 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
- 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

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-PH

Philippines National Computer Emergency Response Team – Philippines

1. Highlights of 2021

1.1 Summary of major activities

- Strengthened and expanded the services offered by CERT-PH by recruiting additional members
- Conducted the National Cyber Drill 2021, with the theme "Cybersecurity Starts with You: Building a Cybersecured Society," which is the first-ever National Cyber Drill conducted by CERT-PH that was open to the public.
- Secured the 8th spot in the 2021 Cyber Sea Games conducted by the ASEAN-Japan Cybersecurity Capacity Building Centre.
- Maintained continuous information sharing through the distribution of daily cyber threat feeds to various agencies, as well as security alerts to the general public.
- Procured different tools/systems for proactive monitoring and which will help in providing immediate response to different incidents.
- Participated in various training, drills, and exercises via online platforms

1.2 Achievements & milestones

- Applied for a Fellowship to the FIRST Suguru Yamaguchi Program
- Championed as Ease of Doing Business Partner by the Philippine Securities and Exchange Commission in providing assistance on the development of company registries, as well as for providing training and assistance on issues related to Cybersecurity incidents response.
- 3 CERT-PH Staff earned their certifications on EC Council Certified Ethical Hacker and 5 CERT-PH Staff earned their certifications on EC Council Certified Incident Handler.

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 23 full-time staff. The operational funding comes from the Department of Information and Communications Technology – Philippines.

2.4 Constituency

CERT-PH 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 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 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.

3.1.4 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.

3.2 Incident handling reports

From January 1 to December 31, 2021, CERT-PH responded to and handled all 1174 reported and monitored cybersecurity incidents within the required response timeframe.

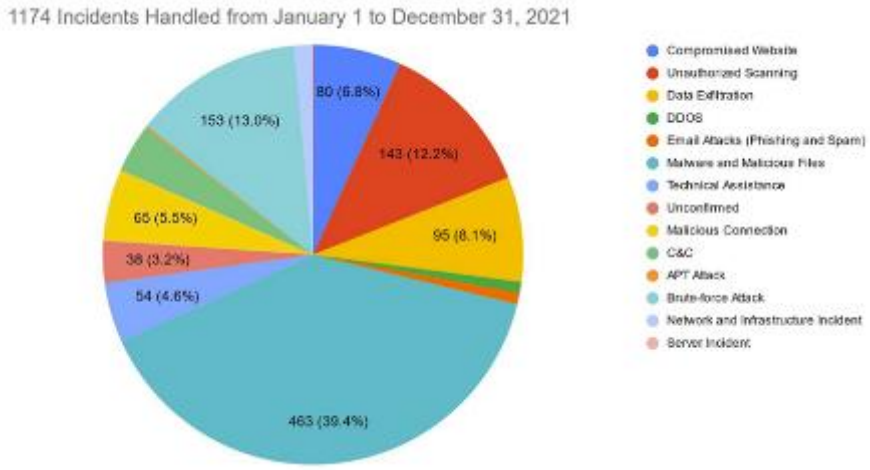


Figure 1. Incidents Per Sector (January 1 to December 31, 2021)

3.3 Vulnerability Assessment and Penetration Testing Assessment

	1ST QTR	2ND QTR	3RD QTR	4TH QTR	TOTAL
No. of Requests from Government Agencies/Instrumentalities	15	32	32	41	120
No. of Target Asset/Systems Assessed/Tested	19	416	860	505	1800

The CERT-PH received and accommodated a total of 120 requests from various Government Agencies and Instrumentalities in 2021. In response to these requests, vulnerability assessment and penetration testing services were performed on a total of 1,800 network and online systems to identify any existing attack vectors that adversaries could use to potentially compromise the overall security, privacy, and operations of the Government and other stakeholders.

3.4 Cyber Threat Monitoring and Information Sharing

In 2021, CERT-PH through the National Cyber Intelligence Web Monitoring System, monitored a total number of 83,861,811 events based on the country code of the Philippines and Geo-IP pointing to the Philippines. Of those, 73,509 were escalated for incident response for verification and remediation.

As indicated in Figure 2, HTTP Scanning had the most recorded attacks, accounting for

82.2 percent of all threats. HTTP Scanning refers to events that have been monitored on an asset that may be infected with malicious software or is potentially being utilized by someone from the organization that owns the IP address to conduct scanning activity that may constitute a threat to other organizations.

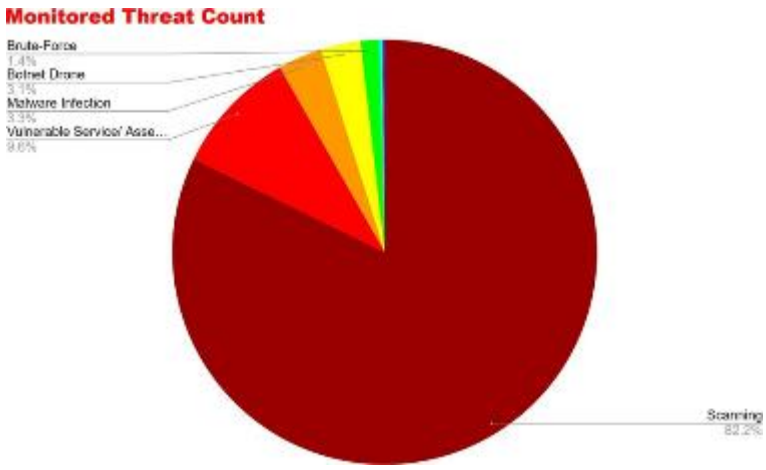


Figure 2. Monitored Threats (January to December 2021)

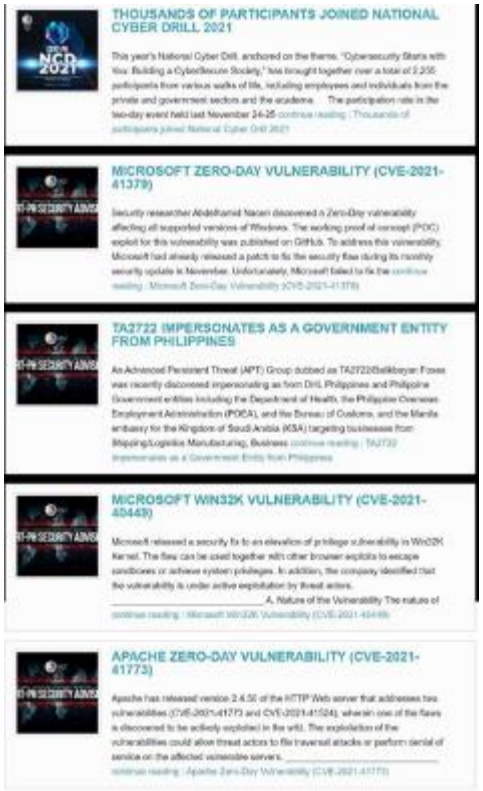


Figure 3. Some of the Issued CERT-PH Security Advisories in 2021

3.5 Cybersecurity Management System Establishment and Operation

In 2021, CERT-PH thru the Security Operations Center operations monitored around 7,931 incidents of which there are 248,625 alerts recorded from 10 connected National Government Agencies. Alerts are malicious activities detected through the Threat Protection System (TPS). After undergoing automatic investigation by the TPS, alerts are considered as incidents for further investigation by the analysts.

Based on the number of TPS incidents per attack stage category the Command & Control (C&C) is the most executed attack, accounting for 8,134 as shown in the table and with a percentage of 96.5% as shown in the chart.

Data Date Range: January 1, 2021- December 21, 2021

Attack Stage	Total TPS Incidents
Command & Control (C&C)	8134
Delivery	273
Installation	4
Lateral Movement	9
Unknown	6

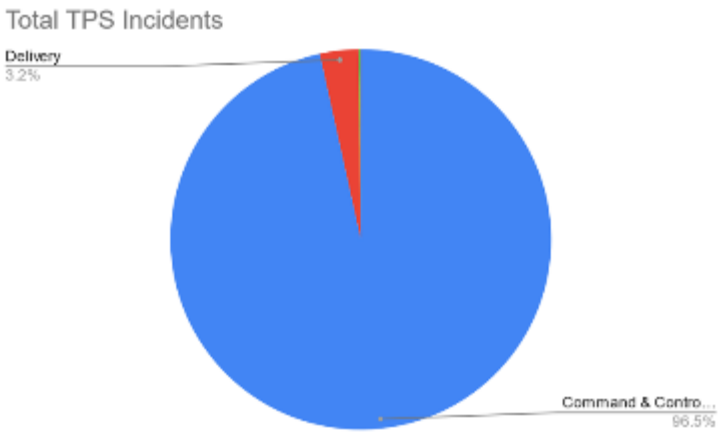


Figure 4. Total TPS Incidents in 2021

4. Events organized/hosted

4.1 Training

A total of 12 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

The CERT-PH Cyber Incident Drill (CCID) took place between June and August 2021. The CCID is a virtual exercise designed to strengthen the cybersecurity capabilities of the agencies designated as Sectoral Lead CERTs under the DICT Department Circular 003 s2020, as well as to improve coordination and collaboration within their respective sectors. This year's drill theme is "Enhancing the Collaboration Among CII Sectors Through Coordinated Incident Response."

The drill exercise included 65 teams that participated in the drill exercise, with a total of 138 people from the various CII Sectors.

Snap/Screen Shot taken during CCID 2021

Meanwhile, the National Cyber Drill 2021 was conducted last November 24-25, 2021 with the theme "Cybersecurity Starts with You: Building a CyberSecured Society," and brought a total of 2,255 participants.

NCD 2021 aimed at strengthening the country's cybersecurity landscape by enhancing public awareness and assessing the public's perspective on Cybersecurity and their capacity to protect themselves from cyber threats and cyberattacks.

The two-day exercise included a series of activities that have helped assess and improve the participant's knowledge and capacity for swift response and recovery. For day 1, a total of 1,752 individuals have registered to participate, while participants for day 2 reached 503.

Snap/Screen Shot taken during NCD November 24-25, 2021

5. International Collaboration

5.1 International partnerships and agreements

On December 2021, CERT-PH has submitted its application for the Fellowship on the FIRST　Suguru Yamaguchi Program

5.2 Capacity building

5.2.1 Training

Below summarizes the international trainings attended by the CERT-PH:

Country/Region	Organization	Event	Date/Venue
Japan - US	Japanese government (METI) and United States government (DHS/CISA, DOS and DOE)	Japan-US Industrial Control Systems Cybersecurity Week	March 8-12, 2021/ Online
ASEAN-Japan	ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC)	11th and 12th Cybersecurity Training on Digital Forensics and Malware Analysis	June 24-25, 2021/ Online
ASEAN-Japan	AJCCBC Technical Cybersecurity	17th AJCCBC Technical Cybersecurity Training	December 13-17, 2021/ Online
Southeast Asia and Pacific	United Nations Office on Drugs and Crime	Advanced Regional Ransomware Investigation Training Course	December 13-17, 2021/ Online

5.2.2 Drills & Exercises

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

Country/Region	Organization	Event	Date/Venue
ASEAN-Japan	National center of Incident readiness and Strategy for Cybersecurity (NISC)	ASEAN-Japan Remote Cyber Exercise 2021	June 09, 2021
Africa	AfricaCERT	Africa Cybersecurity Drill	June 30 - July 01, 2021
Global	Asia Pacific Computer Emergency Response Team (APCERT)	APCERT Drill 2021	August 25, 2021
Global	International Telecommunication Union (ITU)	ITU Global 2021 CyberDrill	November 3-5 and 9-11, 2021/Online
ASEAN-Japan	ASEAN-Japan Cybersecurity Capacity Building Centre	Cyber SEA Games	November 26, 2021/ Online

5.2.3 Seminars & presentations

Served as resource speaker to the following:

- APCERT Training: Incident Management and Digital Forensics Investigation on April 6, 2021
- Asia Pacific Regional Internet Conference on Operational Technologies (APRICOT) 2021 on February 2021 "CERT-PH Response and Countermeasures on Cyberthreats affecting ISP"

6. Future Plans

6.1 Projects

- Establishment of operational SOC intended for internal services offered by the Department of Information and Communications Technology
- Finalization of the budgeting requirements and documentation reports for the application for FIRST membership
- Procurement of additional tools for data gathering, vulnerability assessments, threat monitoring, and incident response to enhance CERT-PH capabilities
- Implementation of Cyber Range Platform for strengthening of cybersecurity skills of government workforce
- Expansion the information sharing to all its stakeholders.
- Encourage more organizations to establish their own CERT.

6.2 Operation

- Further expand its operation to the different stakeholders
- Strengthen its monitoring operation on the upcoming 2022 National Elections
- Deployment of the mobile SOC for requesting agencies and for emergency incidents.

7. Conclusion

Despite the ongoing threat posed by the COVID-19 epidemic, the world has gradually accepted a new normal way of life in which practically everything is done digitally. In terms of cybersecurity, this abrupt shift has resulted in a rapidly increasing number of incidents in 2021.

The past year has seen a significant increase in malicious online activity, including various forms of online scam efforts capitalizing on the crisis, phishing, identity fraud, and others, perpetrated by numerous cybercriminal groups and highly experienced attackers.

As the world transitions to a post-pandemic era of work, cybersecurity must be at the core of every organization's information solutions. Putting cybersecurity first is a proactive approach to dealing with potential threats.

While threats are constantly evolving, CERT-PH pledges to promote cybersecurity practices on a constant basis in order to mitigate risks and establish a stronger security operation. With the help of modern technologies, CERT-PH will also continue to initiate programs and projects that will avert incidents and reduce variables that will have a substantial impact on the nation's key information infrastructure and the general population.

CERT-PH will utilize the highest level of protection in order to prevent potential crises from exploding and causing long-term damage to intellectual property and systems. Similarly, CERT-PH promises to keep interacting, engaging, and collaborating with local and international groups and authorities in order to develop a more secure national cyber ecosystem.

8. 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 Tonga

Tonga Computer Emergency Response Team – Tonga

1. Highlights of 2021

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 and Public Enterprises.

CERT Tonga also continues to respond to incidents that were reported during the period.

1.2 Achievements & Milestones

- CERT Tonga continues partnering with GetSafeOnline in the Ambassador Scheme which trains volunteers on spreading information on cybersafety and cybersecurity.
- CERT Tonga continues its journey by providing awareness trainings to Government, Public Enterprise, Private Sectors, schools and not only here in the main island but also in the outer island.

2. About CSIRT

2.1 Introduction

CERT Tonga operates under the Ministry of Meteorology, Energy, Information, Disaster Management, Environment, Communications and Climate Change (MEIDECC) and is the national Computer Emergency Response Team for the Kingdom of Tonga. Working with international, domestic, public and private parties, acting within their statutory scope, collect information, knowledge and expertise to help improve understanding of developments, threats, and trends and help parties prevent and deal with incidents and make decisions in crisis.

2.2 Establishment

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

2.3 Resources

CERT Tonga team consist of 3 full time staff and liaison officers within domestic partner organizations. There are also a handful of volunteers who assist the team from time to time

2.4 Constituency

CERT Tonga's constituents are Government Ministries, Private Sector, and 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:

- Brute Force activities
- Botnet Activities
- Darknet Activities
- Microsoft Exchange Vulnerabilities

3.3 Publications

- CERT Tonga publishes Advisories to assist constituents in resolving common threats and vulnerabilities observed to be exploited in the wild. They also provide Monthly Security Bulletins of different vulnerabilities seen during the month. However, email advisory is also sent out to our constituents' mailing list to notify any possible attacks and when it was detected.
- With the use of social media platform, CERT Tonga uses Facebook and Twitter to share our advisories, security bulletins as well as security tips.

4. Events organized / hosted

4.1 Trainings

CERT Tonga providing awareness trainings to Government ministries, public enterprises and including awareness program outreach to the outer island.

5. International Collaboration

5.1 International partnerships and agreements

- CERT Tonga in an Operational Member of APCERT and a member of PaCSON (Pacific Cyber Security Operational Network).
- CERT Tonga continues to be partnered with GetSafeOnline to provide cyber safety and security tips targeting businesses and individuals.
- CERT Tonga continues to work closely with a Trustwave on a project running trainings and building staff's knowledge and capabilities.

5.2 Capacity building

5.2.1 Trainings

- CERT Tonga also joined Online Training courses with APNIC, sessions with PaCSON community, building the level of skills and knowledge of our staff.
- CERT Tonga also joined online trainings with Trustwave colleagues from Australia

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 looks forward to undertaking projects that are currently in progress with the assistance of donor partners and implementers.

6.2 Future Operation

We also look forward to continuing working with global community, the Asia Pacific and Pacific region in the fight to keep the internet secure.

7. Conclusion

CERT Tonga recently joined APCERT and looks forward to continuing to collaborate and sharing with the APCERT members.

CNCERT/CC

National Computer network Emergency Response technical Team / Coordination Center of China - People's Republic of China

1. About CNCERT

1.1 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.

1.2 Establishment

CNCERT/CC was founded in 2001 and became a member of FIRST and one of the founders of APCERT. As of 2021, CNCERT/CC has established "CNCERT International Cooperation Partnership" with 274 teams in 81 countries and regions.

1.3 Workforce power

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.

1.4 Constituency

As a national CERT, CNCERT/CC strives to improve the nation's cybersecurity posture and protect critical infrastructure cybersecurity. CNCERT/CC leads efforts to prevent, detect, warn and coordinate cybersecurity threats and incidents, pursuant to the guideline of "proactive prevention, timely detection, prompt response and maximized recovery".

1.5 Contact

E-mail: cncert@cert.org.cn

Hotline: +8610 82990999（Chinese）, 82991000（English）

Fax: +8610 82990399

PGP Key: http://www.cert.org.cn/cncert.asc

2. Events organized/co-organized

2.1 The Seminar on China-ASEAN Cyber Security Emergency Response Capacity Building and the Online Conference of CNCERT International Partners in the ASEAN Region

On 29th June, the China-ASEAN Seminar on Cyber Security Emergency Response Capacity Building hosted by National Computer Network Emergency Technical Processing Coordination Center (CNCERT/CC) and The Video Conference of CNCERT International Partners in the ASEAN region was held online. More than 30 representatives from more than 10 organizations at home and abroad attended the meeting and the representative with CNCERT/CC attended and delivered the welcome speech. The year of 2021 marks the 30th anniversary of China-ASEAN dialogue relations.

During the meeting, CNCERT/CC and representatives of Cambodia CERT, Lao CERT, Malaysia National Cyber Security Agency, CERT-PH, Singapore Cyber Security Agency, Thailand Digital Economy and Society Department and Indonesia National Cyber Security and Cryptography Agency introduced the national cybersecurity situation &policy and new challenges in the past year.

2.2 2021 CNCERT Annual Conference in Beijing

On 20th July, CNCERT/CC held the 2021 Annual Chinese Conference on Computer and Network Security in Beijing. Focusing on the theme "Rising up to Data Security Threats and Challenges with Joint Efforts", the conference invited representatives from government departments, important information system units, research institutes and network security industries to discuss and exchange new trends, problems and ideas of network security, so as to improve domestic data protection.

2.3 2021 Global Conference on CNCERT International Partnership in Emergency Response

On 16th August, Conference on CNCERT International Partnership in Emergency Response hosted by CNCERT/CC was held online. More than 90 representatives from over 40 organizations of nearly 20 countries and regions attended the conference. Lu Wei, Deputy Director General of CNCERT/CC, attended and delivered a speech.

With the theme of "Cooperation on Cybersecurity Emergency Response to

Olympics-related Incidents", the conference included two sessions: "International cooperation" and "Technical experience". Guest speakers from CNCERT/CC, Pakistan Information Security Association, AeCert of UAE, Africa Cert, Kazakhstan Kz-Cert, Indonesia Cert, Kaspersky ICS CERT, Asia-Pacific Network Information Center (APNIC) and Alibaba Aliyun exchanged their views on international cooperation of emergency response, regional collaboration experience in cybersecurity incidents, past practices and experience in cyber-security protection of large-scale sports events, as well as competition protection on the cloud.

2.4 Sub-forum of Wuzhen Summit of the 8th World Internet Conference: Cybersecurity Forum for Technology Development and International Cooperation

Hosted by the National Computer Network Emergency Response Technology Processing Coordination Center (CNCERT/CC), the World Internet Conference 2021 Wuzhen Summit on Cybersecurity Forum for Technology Development and International Cooperation was held in Wuzhen, Zhejiang Province on 27th September. Themed on "Building Consensus for a Closer Partnership in Cybersecurity", the forum was honored by the (tele)presence of Internet Hall of Fame Inductees, head of international organizations , senior officials from cyber-security administration of China and other countries, well-known enterprises who shared their experience and best practices through 4 keynote sessions: "International Cooperation in the Digital Era", "Cooperation in Emergency Response in the Time of COVID-19", "Stronger Protection of Critical Information Infrastructure" and "Trusted and Collective Governance of Cyberspace". Apart from that, two panels were organized for discussions on the latest cybersecurity development trends, policies and strategies, technological opportunities and challenges, as well as on international cooperation and prospects, in pursuit of a respectful, open, inclusive and mutually beneficial cyber cooperation landscape.

2.5 The 9th China-Japan-Korea CSIRT Annual Meeting for Cybersecurity Incident Response

From October 13th to 14th, the 9th China-Japan-Korea CSIRT Annual Meeting for Cybersecurity Incident Response was held online. Hosted by JPCERT/CC, this annual meeting has offered a platform for CNCERT/CC, JPCERT/CC and KrCERT/CC of KISA to exchange their thoughts and experiences in cybersecurity.

2.6 2021 Conference on CNCERT International Partnership with Africa

On 3rd November, the 2021 conference on CNCERT International Partnership with Africa was successfully held online. More than 30 representatives from 17 organizations in Africa attended the meeting.

The meeting consisted of three sessions: "emergency coordination", "technical experience" and "exchange and discussion". 10 guests from CNCERT/CC, African CERT, bjCSIRT, CERT-MU and China Unicom, Huawei, Qi Anxin, Nsfoucs, Eversec and Sangfor companies exchanged their views and opinions focusing on international cooperation and capacity building in emergency response, development of CERTs, cloud infrastructure security, AI-enabled threat detection and emergency response, cyber security attack and defense, industrial Internet security, ransomware response and disposal cooperation and other technical experience.

3. Drill attended

3.1 APCERT Incident Drill 2021

On 25th August, CNCERT/CC participated in the APCERT 2021 Drill and completed it successfully. The theme of this year's APCERT Drill is "Supply Chain Attack Through Spear-Phishing - Beware of Working from Home". This exercise reflects real incidents and issues that exist on the Internet. The participants handled a case of a supply chain attack triggered by spear phishing. 25 CSIRTs from 19 economies of APCERT participated in the drill.

3.2 ASEAN CERT Incident Drill (ACID) 2021

On 5th October, CNCERT/CC participated in ASEAN CERT Incident Drill (ACID) 2021. The theme of this drill is "Responding to Supply Chain Attacks Against Businesses". The participating teams investigated, analyzed, coordinated and recommended remediation and mitigation measures towards cyber incidents. More than 100 participants from 10 AMS and 5 key Dialogue Partners from China, Australia, India, Japan and South Korea participated in this year's drill.

4. Achievements

CNCERT's weekly, monthly and annual reports, as well as other released information, were reprinted and cited by massive authoritative media and thesis at home and abroad.

Table 5-1 Lists of CNCERT's publications throughout 2021

Title	No. of Issues	Description
CNCERT Weekly Reports (Chinese)	52	Emailed to over 400 organizations and individuals and published on CNCERT's Chinese website (http://www.cert.org.cn/)
CNCERT Weekly Reports (English)	52	Emailed to relevant organizations and individuals and published on CNCERT's English website (http://www.cert.org.cn/english_web/documents.htm)
CNCERT Monthly Reports (Chinese)	12	Issued to over 400 organizations and individuals on a regular basis and published on CNCERT's website (http://www.cert.org.cn/)
CNCERT Annual Reports (Chinese)	2	Published on CNCERT's website (http://www.cert.org.cn/)
CNVD Vulnerability Weekly Reports (Chinese)	52	Published on CNCERT's website (http://www.cert.org.cn/)
Articles Analyzing Cybersecurity Threats	12	Published on journals and magazines

CyberSecurity Malaysia

CyberSecurity Malaysia – Malaysia

1. Highlights of 2021

1.1 Summary of major activities

27 Feb 2021	Organised the Safer Internet Day (SID) 2021: Bicara Etika Siber in Cyberjaya, Malaysia
22 Feb - 4 Mar 2021	Participated in the APRICOT 2021/ APNIC 51 (online)
11 - 14 May 2021	Participated in the 20th Annual AusCERT Information Security Conference (online)
24 - 25 May 2021	Participated in the 16th Annual Technical Meeting for CSIRTs with National Responsibility (online)
6 - 9 June 2021	Participated in the 33rd FIRST Annual Conference (online)
21 - 30 Jun 2021	Conducted a capacity building training under the Malaysian Technical Cooperation Programme (MTCP) attended by selected APCERT members titled "Certified Penetration Tester" Technical Training (online)
25 Aug 2021	Participated in the APCERT Cyber Drill 2021 with the theme "Supply Chain Attack Through Spear-Phishing – Beware of Working from Home"
13 - 16 Sep 2021	Participated in the APNIC 52 (online)
10 Sep 2021	Conducted Awareness Talk on Cyber Wellness (online)
28 Sep 2021	Co-organised the OIC-CERT Cyber Drill with Oman National CERT.
1 Oct 2021	Chaired the APCERT Annual General Meeting (AGM) (online)
6 - 9 Oct 2021	Organised the the National ICT Security Discourse Competition (NICTSeD) 2021 - CyberSAFETM Challenge Trophy (online)
5 Nov 2021	Conducted Cybersafe Awareness Talk with Cyber Security Malaysia (online)
23 - 24 Nov 2021	Organised the OIC-CERT 13th Annual Conference & 9th Arab Regional Cybersecurity Summit 2021 with the theme "CERTs in an Evolving Cyber Security Landscape" (online)
14 - 16 Dec 2021	Organised the Cyber Security Malaysia - Awards, Conference & Exhibition (CSM-ACE) 2021 in Cyberjaya, Malaysia.

2. About Cybersecurity Malaysia

2.1 Introduction

CyberSecurity Malaysia is the national cybersecurity specialist agency under the Ministry of Communications and Multimedia Malaysia having the vision of being a globally recognised National Cyber Security and Specialist Centre. Some of the services provided are:

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. In 2018, with the restructuring of the government administration, CyberSecurity Malaysia was transferred to the Ministry of Communications and Multimedia Malaysia. CyberSecurity Malaysia is committed in providing a broad range of cybersecurity innovation-led services, programmes, and initiatives to help reduce the vulnerability of digital systems, and at the same time strengthen Malaysia's self-reliance in 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 cyberthreats 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 organisational 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/full?id=9eb77829-7dd4-4180-814f-de3a539b7a01

MyCERT's Cyber999 cyber incident reference centre, has responded to 10,016 incidents in 2021 and most being intrusion 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 analysing 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 16 advisories and 16 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.

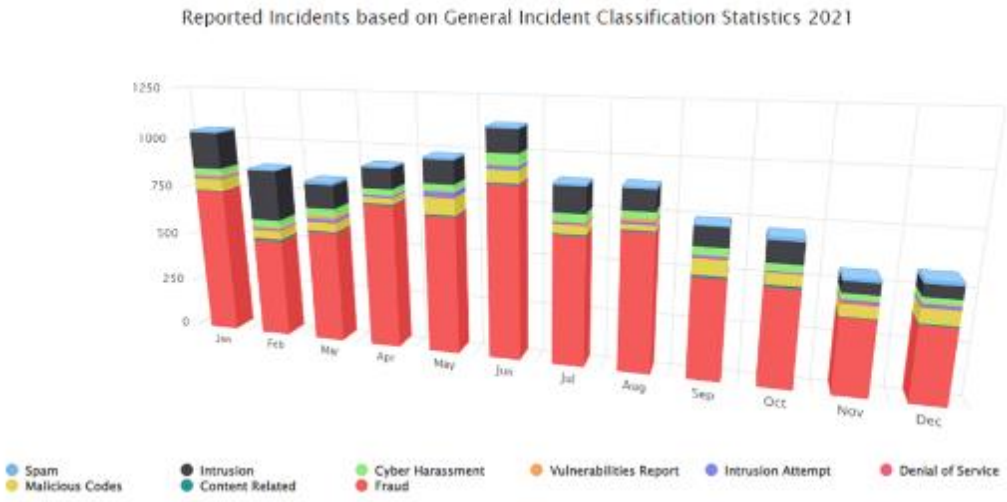


Figure 1. 2021 Reported Incident

Further information on incidents reported to CyberSecurity Malaysia can be viewed at: https://www.mycert.org.my/portal/statistics-2021

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/
- Kibana portal at https://es.honeynet.org.my/s/public/app/canvas#/workpad/workpad-5e83726d-0125-4bfd-a8e9-88b6e844ce24/page/1 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 2021 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 2021.

21-30 Jun 2021	Malaysian Technical Cooperation Programme (MTCP) 'Certified Penetration Tester' Technical Training (online) This training aims to raise awareness and provide exposure towards participants on the importance of cyber security. In addition, participants sit for the 'Certified Penetration Tester' examination to obtain professional certification.
9-12 Aug 2021	Forensic Training Program for Asia Pacific University (APU) (online) This training program attended by 60 lecturers and students, with the objective of further strengthening the country's cyber forensic capabilities. The participants were divided into four segments as follow: AI & Biometrics Training Cryptocurrencies Forensic Training Forensic Audit Training Forensic Web Reconstruction Training
28-29 Aug 2021	The Certified Cybersecurity Awareness Educator (CCASE) Training Program virtually CCAsE is a professional training and certification program that provides essential knowledge focusing on human cyber security aspects. Teachers will be ready and able to implement effective security awareness programs for their target audience especially school students.
23 Sep 2021	Global Digital Security and Forensic in the New Norm Webinar The event is aimed at fostering the global cyber security and digital forensics in the new norm through international cooperation among collaborators. The event itself provides unique sessions focusing on digital forensics and cyber security current issues and challenges.
23 Dec 2021	People, Process and Technology Certification: An Instrument of Compliance Webinar The event acted one of the platforms to promote CyberSecurity

Malaysia's roles and services and to enhance awareness of cyber security in the public. It offers an opportunity for the public to get basic information on CyberSecurity Malaysia's certification services. The event also provided insight on the current cyber security landscape and outlook for 2022. CyberSecurity Malaysia is utilizing this platform to also understand the stakeholders and CII needs and to gather information, strategize and position our offerings to meet the required demand.

4.3 Presentations

CyberSecurity Malaysia's representatives had been invited to give presentations and talks at international conferences and seminars. Among the participations include:

i. 13 Jan 2021 - Ts. Dr. Zahri Yunos, Chief Operating Officer was invited to present a paper entitled "Cyber Resiliency in Critical Infrastructure Environment" at the 18th International Bhurban Conference on Applied Sciences & Technology (IBCAST-2021) organised by the Centers of Excellence in Science & Applied Technology (CESAT) (online).
ii. 31 May 2021 - CyberSecurity Malaysia in collaboration with the National Financial Crime Center organised a cryptocurrency investigation from Australia's perspective seminar.

4.4 Research Papers

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

i. A Study on Privacy Issues in Internet of Things (IoT) - IEEE
ii. Modifications of Key Schedule Algorithm on RECTANGLE Block Cipher - Springer
iii. Lightweight Denial of Service (DoS) Detection System Algorithm (LIDSA) - IEEE
iv. People, Process and Technology for Cryptocurrencies Forensics: A Malaysia Case Study - Springer
v. Compromising the Data Integrity of an Electrical Power Grid SCADA System - Springer
vi. Developing Cyber Resilience Strategy for The Critical National Information Infrastructure Sectors in Malaysia - The University of Warwick, United Kingdom

vii. Practical Guideline for Digital Forensics Laboratory Accreditation – A Case Study - CyberSecurity Malaysia
viii. The Integration of Cyber Warfare and Information Warfare - CyberSecurity Malaysia
ix. Cyberbullying via Social Media: Case Studies in Malaysia - CyberSecurity Malaysia
x. Establishment of a Method to Measure the Awareness of OIC-CERT Members - CyberSecurity Malaysia
xi. Development of Examination Framework for Cyber Security Professional Competency Certification - CyberSecurity Malaysia
xii. New Vulnerabilities upon Grain v0 Boolean Function through Fault Injection Analysis - CyberSecurity Malaysia
xiii. Cryptocurrencies Investigation: A Methodology for the Preservation of Cryptowallets - IEEE
xiv. Comparison Multi Transfer Learning Models for Deep Fake Image Recognizer - IEEE
xv. A Review of Digital Forensics Framework for Blockchain in Cryptocurrency Technology - IEEE
xvi. Application of Knowledge-Oriented Convolutional Neural Network for Causal Relation Extraction in South China Sea Conflict Issues - IEEE
xvii. News Event Prediction using Causality Approach on South China Sea Conflict - IEEE
xviii. Formulation of Association Rule Mining (ARM) for an effective Cyber Attack Attribution in Cyber Threat Intelligence (CTI) - The Science and Information [SAI] Organization
xix. Security and Threats in the Internet of Things Based Smart Home - IEEE
xx. KSA for Digital Forensic First Responder: A job Analysis Approach - Academic Conferences International Limited
xxi. The Implementation of Hardware Security Based Zymkey 4i in HDVA – IEEE

4.5 Social Media

In 2021, 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 54,046 followers

and the CyberSecurity Malaysia Twitter has 7,175 followers.

5. International Collaboration

The Malaysia Cybersecurity Strategy 2020 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

Since the COVID-19 pandemic, there was no working visits conducted by CyberSecurity Malaysia. This activity will resume after the Covid-19 situation improves allowing international travelling.

5.2 International Roles

Amongst the international roles and contributions by CyberSecurity Malaysia are:

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.

This agency will continue to organise national events such as the Cyber Security Malaysia – Awards, Conference and Exhibition (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 organise 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 either 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 2021

1.1 Summary of Major Activities

As the COVID-19 epidemic continues to impact our daily lives, the public is becoming more dependent on e-services. On the other hand, the associated cyber threats grow in scale and sophistication and bring significant impacts on the smooth operation of e services. The Government Computer Emergency Response Team Hong Kong (GovCERT.HK) is committed to strengthening the security measures of the government systems and Internet infrastructure, as well as collaborating with various stakeholders to provide a reliable and secure cyber world for the community.

We attach great importance to information security and facilitate the protection by the departments of the Government of the Hong Kong Special Administrative Region of the People's Republic of China (the Government) of their information infrastructure and data assets against cyber threats by various effective measures, through such measures as monitoring cyber threat trends, conducting risk assessments, and providing security alerts and advice. Numerous webinars and trainings were also organised to raise the information security awareness of the government staff and refreshing their knowledge in dealing with the latest cyber security threats and evolving technologies. In addition, the annual inter-departmental cyber security drill was held to strengthen the capability of government departments to defend against emerging cyber attacks and foster cyber security collaboration among the GovCERT.HK, the Hong Kong Police Force (HKPF) and other government departments.

To strengthen the overall defensive capability and resilience of the city against cyber attacks, we continued to promote trusted partnership and closer collaboration among local cyber security stakeholders across different sectors for sharing cyber security information and providing actionable insights to the community via the Partnership Programme for Cyber Security Information Sharing (Cybersec Infohub, www.cybersechub.hk). The programme kept on a steady growth of membership base with some 870 organisations, which was more than double as compared with 2020.

Situational awareness helps organisations and individuals protect their assets in the cyber realm. In 2021, we continued publishing threat trends, early warnings and advice through the GovCERT.HK web portal (www.govcert.gov.hk) to enhance government departments' understanding of the cyber threat environment, the associated risks and impacts, and also the adequacy of the risk mitigation measures.

We also put a lot of efforts in promoting security awareness and raising defensive capabilities among local enterprises and the community by collaborating with various major cyber security stakeholders to hold cyber security publicity events regularly.

1.2 Achievements and Milestones

1.2.1 Cyber Security Information Sharing

With the objective to foster cross-sector collaboration for a better visibility of cyber threats, Cybersec Infohub has been receiving critical acclaim and support from the industry. In 2021, the participating organisations from a wide spectrum of industries have more than doubled and so has the number of posts shared in the collaborative platform. To facilitate users with different levels of background in utilising the information shared in the collaborative platform, we implemented a new user interface to suit the needs of business users as well as cyber security professionals. A lot of system enhancements and new features were also implemented to further strengthen the sharing capability of the platform and enhance the user experience. For example, the machine-to-machine sharing application programming interface was implemented to facilitate automatic integration of cyber threat information with the systems of member organisations for more timely responses when tackling potential cyber threats.

Furthermore, we successfully organised 10 member events, including thematic webinars, technical professional workshops and closed-group discussion, to build a better trust and closer bonding among members.

1.2.2 Liaison and Collaboration

We worked closely with the Computer Emergency Response Team (CERT) community and actively participated in the Asia Pacific Computer Emergency Response Team (APCERT) activities in handling threat information and coordinating incidents. We also supported our working partners in organising various events, such as the Capture the Flag (CTF) Challenge 2021, the Cyber Youth Programme 2021 and the Cyber

Security Competition 2020/21 organised by the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT), the Hong Kong Internet Registration Corporation Limited (HKIRC) and HKPF respectively.

1.2.3 Awareness Building and Public Education

Human element is often regarded as the weakest link in information security. To elevate the security awareness against phishing attacks in the Government, an "Anti-Phishing Resources Centre" was launched with interactive quizzes and lively promotional materials to refresh our government staff with the latest tactics and techniques to protect themselves from getting phished.

GovCERT.HK also endeavours in public education to enhance the knowledge and capability of the public to defend against cyber attacks. In 2021, we organised 16 school visits and several security talks for the elderly in response to the increasing adoption of digital technology.

2. About GovCERT.HK

2.1 Introduction

The Government Computer Emergency Response Team Hong Kong (GovCERT.HK) is a governmental Computer Emergency Response Team (CERT) responsible for coordinating incident responses for over 80 departmental Information Security Incident Response Teams (ISIRTs) of the Government.

Since its establishment, GovCERT.HK has profoundly shaped the management framework and coordination mechanism of incident handling, and empowered close collaboration with the industry, critical Internet infrastructure stakeholders and the global CERT community for timely exchange of cyber threat information and coordinated responses.

GovCERT.HK works closely with HKCERT and local industries on cyber threat intelligence sharing, capability development, public education and continuous promotion on cyber security through social and mass media. GovCERT.HK also actively collaborates with other governmental and regional CERTs, and international organisations in sharing cyber threat intelligence and incident information; participating in training events, workshops, forums and drills; and organising activities for public awareness promotion and capability development.

2.2 Establishment

GovCERT.HK was established on 1 April 2015 through the consolidation of internal information technology (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 Scope of Services

GovCERT.HK is the CERT for the Government, providing centrally managed incident response services and timely security advice, coordinating cyber security drills, promoting public awareness and capabilities, and engaging global CERT community with a view to enhancing information and cyber security in the region.

3.2 Security News Bulletins

In 2021, GovCERT.HK published the following security bulletins to raise the awareness among government users and the general public.

- "Security Vulnerabilities and Patches" information was consolidated on every

working day and disseminated to registered subscribers through emails;

- "Security Industry News" was gathered on every working day and top news with wide impact was compiled and disseminated to registered subscribers through emails; and
- "Weekly IT Security News Bulletins" was published every week to summarise selected recent security news and product vulnerabilities for security practitioners' reference. The Bulletins were distributed to registered government subscribers through emails and posted on the GovCERT.HK website as public information. (www.govcert.gov.hk/en/secbulletins.html)

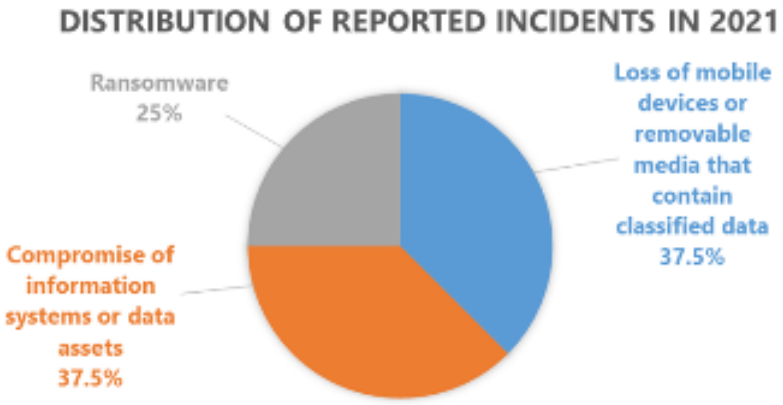
3.3 Alerts and Advisories

To meet the challenges of increasing cyber security threats, we continued to strengthen the collection and analysis of cyber risk information from more sources and make use of big data analytics to provide targeted and timely warnings to government departments, so that early warnings of vulnerabilities and threats could be issued and timely preventive measures could be taken. In 2021, GovCERT.HK issued over 170 security alerts for known security vulnerabilities in computing products that are widely used in government installations. For those vulnerabilities with greater potential impacts on the Government, we took proactive steps to ensure all government departments addressed the vulnerabilities in a timely manner so as to mitigate the risks of exploitation.

We also kept on analysing cyber security threats shared by various sources and identified by our detection capabilities. In response to any imminent threats posed to the Government, our security advisories would provide government departments with our latest observations and appropriate actionable advice.

3.4 Incident Handling Reports

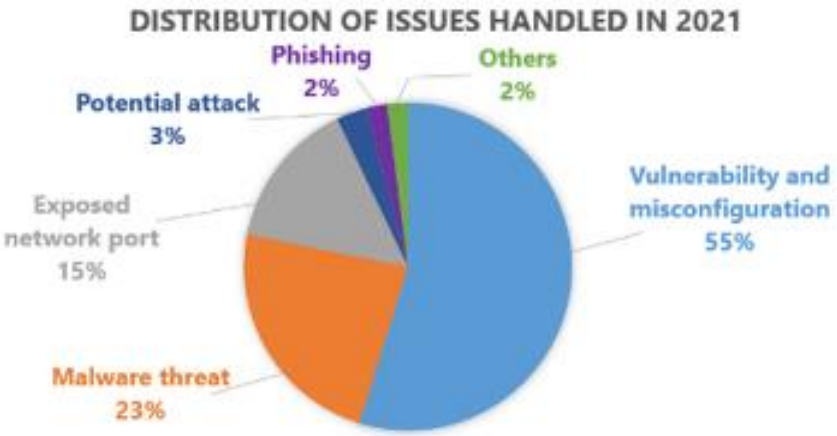
In 2021, GovCERT.HK handled eight reported incidents that were related to government installations. The following chart shows the types of reported incidents handled in 2021.



To facilitate public access to the statistics of information security incidents in the Government, relevant data has been made available on the Government's Public Sector Information Portal.
(www.data.gov.hk/en-data/dataset/hk-ogcio-sec_div_01-information-security-incident)

3.5 Abuse Statistics

In 2021, GovCERT.HK also dealt with around 200 cyber security issues by assisting government departments in taking effective and prompt measures to prevent and reduce the risks and impacts of cyber attacks on their information systems. The following chart shows the types of security issues handled in 2021.

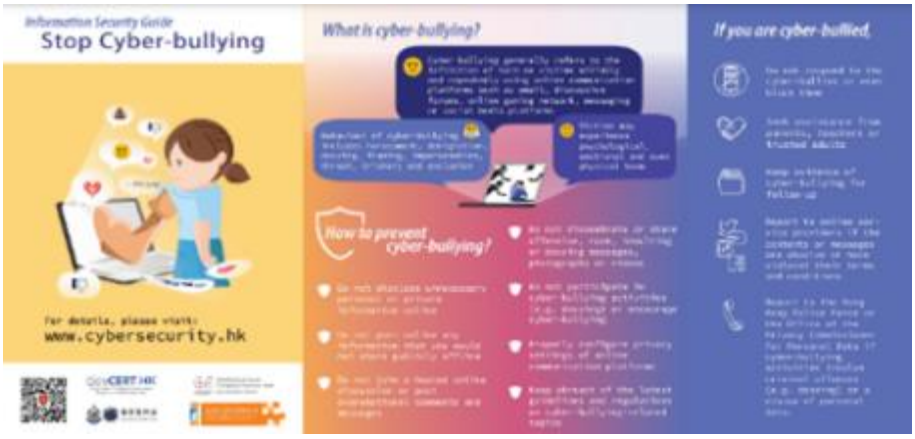


3.6 Publications and Mass Media

In this era of digital transformation, every generation starts adapting to digital living and relies more heavily on technologies. Associated with more digitalisation are more risks. To actively reach out to the targeted audience, we continued to launch various promotional activities through multiple channels such as radio broadcast, social media (like YouTube, Facebook and Twitter) and school visits to share tips and best practices against cyber threats.

- We partnered with Radio Television Hong Kong (RTHK) to broadcast radio episodes "e-World Smart Tips" every Saturday morning to help the public understand more about information security in various aspects and raise their awareness of the issue. The radio episodes in each month featured a specific theme and offered associated tips on mitigating the risks of cyber threats through daily life examples and in a lively and interesting way. In 2021, we covered a wide range of topics including Wi-Fi security, safe online shopping, phishing attacks, social networking security, Internet of Things (IoT) devices security, and more. (www.cybersecurity.hk/en/media.php#Radio)

- A set of practical guidelines with different themes were published to educate small and medium enterprises and the public to guard against cyber attacks. (www.cybersecurity.hk/en/resources.php#leaflets)



- To raise public awareness of Internet safety and etiquette, we organised the "Be Smart Online, Stay Away from Pitfalls" GIF Graphic Design Contest in 2021. Participants designed sets of innovative and creative GIF graphics to convey the message of Internet safety and etiquette. The winning entries are made as instant messaging stickers and now available at www.cybersecurity.hk/en/contest- 2021.php. Anyone may download them and share with his/her family and friends.

- By leveraging the OGCIO Facebook page, we have shared a series of posts with timely updates and tips on cyber security topics such as supply chain attack and cyber-bullying. The social media channel with highlighted key points and linked resources helped strengthen our communications with the public. (www.facebook.com/OGCIOHK)

3.7 GovCERT.HK Technology Centre

To facilitate the development of government staff's capability in more specialised knowledge and skills to tackle evolving cyber threats, our GovCERT.HK Technology Centre offers government departments a controlled environment with relevant facilities and equipment for tackling potential security issues. The overall security of government web applications and services is enhanced by making use of such tools to identify web vulnerabilities, misconfigurations, compromised passwords, etc.

4. Events Organised/Hosted

GovCERT.HK regularly organises awareness trainings and solution workshops to share the latest knowledge on security measures, best practices, skills and security solutions

with various levels of government users to continuously strengthen their knowledge on cyber attacks and enhance their information security skills, thereby strengthening their capabilities in guarding against cyber attacks.

4.1 Training

In 2021, we organised various webinars and trainings for government users as well as IT staff to raise their information security awareness and update their knowledge of the latest IT security technologies and solutions. Over 2 000 government staff members participated in these events, which covered a broad range of topics including security measures and best practices for remote working, defence against phishing, operating system security, promotion of various security solutions, etc.

To facilitate government departments' obtaining hands-on experience in various IT security solutions, different security solution vendors were invited to deploy their cutting-edge solutions to the Security Solution Showcases Platform. Also, the platform was upgraded to allow government departments to access remotely in order to encourage the acquisition of latest security solutions for protecting government information systems and data assets.

4.2 Drills and Exercises

4.2.1 Inter-departmental Cyber Security Drill

GovCERT.HK coordinates government departments to conduct the annual inter departmental cyber security drills to enhance their incident handling capabilities and test their familiarity with the predefined incident response procedures.

In 2021, we continued to organise the drill with the Cyber Security and Technology Crime Bureau (CSTCB) of HKPF to strengthen the cyber security incident response capability of the Government. Due to the epidemic situation, the drill was held online with around 40 government departments and 100 government incident response practitioners joined. It included a scenario-based table-top exercise and an incident response workshop.

4.2.2 Anti-Phishing Resources Centre

To further support the promotion of phishing awareness in the Government, a thematic web page of "Anti-Phishing Resources Centre" was launched in 2021. The resource

hub consolidates promotional materials, including interactive quizzes, infographics, animations, posters and etc., to promote to government users with the latest threat trend and phishing techniques.

4.2.3 APCERT Drill

As an Operational Member of the APCERT, GovCERT.HK participated in the APCERT Drill with the theme of "Supply Chain Attack through Spear-Phishing – Beware of Working from Home" in August 2021. GovCERT.HK played the role of Exercise Controller in addition to Player and Observer in the drill.

4.3 Conferences and Seminars

4.3.1 Build a Secure Cyberspace Promotional Campaign

To enhance the knowledge to avoid cyber pitfalls and build the law-abiding awareness of the public, a series of promotional activities under the theme "Be Smart Online, Stay Away from Pitfalls" were organised in 2021 for businesses, organisations, schools and the public to raise their cyber security awareness and strengthen their cyber security postures.

- Two webinars were organised under the "Build a Secure Cyberspace" promotional campaign in May 2021 and September 2021, aiming to raise public awareness of cyber security and introduce precautions against cyber attacks.

4.3.2 School visits, InfoSec Tours with RTHK

To promote cyber security awareness and cyber etiquette in the community, GovCERT.HK organised visits to primary schools, secondary schools and tertiary institutions to deliver information security talks to students, teachers and parents. GovCERT.HK also partnered with RTHK to deliver InfoSec Tours using pre-recorded talks on the platforms of RTHK and YouTube, aiming to deliver information security message in a relaxing way. (www.cybersecurity.hk/en/school-visit.php)

- A number of school visits were conducted in 2021, reaching out to students, teachers and parents to raise their awareness of cyber security and instil them with the proper attitude in using the Internet.
- In response to the increasing adoption of digital technology by the elderly in their daily lives, OGCIO also conducted security talks for them to raise their cyber security awareness.
- Two InfoSec Tours videos with topics of "Responding to the temptation of the online world" and "Study at home safely" were produced for broadcasting.

4.3.3 Cybersec Infohub engagement activities

To encourage the engagement and effective discussion among different sectors under the Cybersec Infohub partnership programme, various activities such as sector-specific closed group meetings, technical professional workshops and webinars were arranged in 2021 with positive responses received.

5. Local and International Collaboration

5.1 Local Collaboration

5.1.1 Cybersec Infohub

To foster closer collaboration among local information security stakeholders of different sectors to share cyber security information through the Cybersec Infohub programme, GovCERT.HK continued promoting and operating the programme side by side with HKIRC since September 2020. The programme has attracted some 870 participating organisations and more than 1 800 representatives from various sectors as of end of 2021.

We have always been encouraging exchanges of cyber security information within key industries with higher risks to cyber attacks, such as banking sector and Internet services providers. To enable closer collaboration in insurance sector, we collaborated with the Hong Kong Insurance Authority to motivate their members to actively participate in the programme and share information with other sectors.

5.1.2 Internet Infrastructure Liaison Group (IILG)

To help maintain the healthy operation of the Internet infrastructure of Hong Kong, GovCERT.HK continued to support the IILG which was established and led by OGCIO to foster closer liaison with the Internet infrastructure stakeholders, aiming to collaborate with the stakeholders for the smooth operation of the local Internet infrastructure. In 2021, the IILG collaboration mechanism was activated four times to support major events and take precautions against cyber threats.

5.1.3 Cyber Security Professional Awards (CSPA)

The CSPA 2021 was co-organised by CSTCB, GovCERT.HK and HKCERT, to recognise

the excellence of cyber security personnel in safeguarding cyber security of Hong Kong and serve as an opportunity to showcase their unique capabilities. The CSPA has been providing a platform for cyber security professionals across sectors to share their knowledge and experience, which also aims at building an intact cyber ecosystem.

5.1.4 Nurturing Cyber Security Talents

We reckon that cyber security talents are instrumental in creating a safe environment for the economy to thrive. We continue to collaborate with and support our working partners to organise various programmes and campaigns in order to attract the young generation to develop their professional skills in cyber security and join the information security industry in a long run.

To arouse cyber security awareness and enrich the knowledge of cyber threats among the students in Hong Kong, we supported CSTCB in holding the Cyber Security Competition 2020/21 with the theme “Cyber Security Starts from You”, which attracted over 12 000 participants. The competition included events such as cyber security quizzes, interactive games and a presentation.

We also supported CSTCB to organise the Cyber Security Expo 2022, taking the theme on technology application and cyber security, to feature a series of activities for the participants. Among the activities, Cyber Security Innovation Challenge for students was open for submission in October 2021 and it attracted more than 300 participating schools.

In addition, we supported HKCERT in organising "CTF Challenge 2021" to strengthen the cyber security skills and awareness of young people and nurture more talents, with some 310 teams to compete. CTF also encouraged problem solving through teamwork and creative thinking in coping with the cyber security tasks to gain real life experience.

Last but not least, we also supported HKIRC to organise the HKIRC Cyber Youth Programme 2021 with an aim to nurturing technology talents with professional knowledge and skills. Over 100 students joined a four-day cyber security course for free to get a taste of the latest cyber security equipment and tools, as well as to learn cyber security knowledge and skills.

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 strives 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 2021:

- 2021 China Cybersecurity Week
- Annual Technical Meeting for CSIRTs with National Responsibility
- APCERT Annual General Meeting and Conference
- APCERT Drill
- APCERT online training sessions

- APISC Security Training
- CNCERT/CC Annual Conference
- CNCERT/CC Online Conference for International Partnership
- FIRST Annual Conference

6. Future Plans

6.1 Upcoming Projects

In view of the rapid development of e-government services and the increasingly complex cyber threats, we will launch a comprehensive health check programme, in which additional and in-depth health checks will be conducted, and followed up with testing services for government Internet-facing systems and public-facing mobile applications. The programme aims at further strengthening the government security posture by adding an extra layer of security verification to government departments' own standing assessment processes. The proactive approach will improve the visibility of the overall security status of government systems, thus enabling the Government to formulate complete and pragmatic recommendations.

In addition, we will further support and facilitate the promotion of phishing awareness in the Government, by starting a new round of phishing drill campaign.

6.2 Future Operations

Facing the ever-increasing cyber attacks, GovCERT.HK is striving to collaborate with different stakeholders to further promote cyber security and nurture future talents such as liaising with HKCERT to organise another round of CTF Challenge for the community to increase their interests and knowledge in cyber security and a new promotional campaign to help small and medium enterprises in preventing and handling security incidents.

To enable a more fruitful sharing and closer collaboration in the Cybersec Infohub, we will further promote the programme, explore more collaboration opportunities with various industries, such as arranging closed group experience sharing session and leveraging the platform to enable more effective sharing of cyber threat intelligence.

7. Conclusion

The proliferation of cyber attacks, coupled with the growing cyber threats associated with artificial intelligence, blockchain, cloud computing and financial technology, has posed ever-increasing challenges on cyber security. GovCERT.HK will strive to work closely with various stakeholders, both locally and globally, to maintain a secure, stable and reliable e-government and cyberspace for a safer and better tomorrow.

Contact:

- cert@govcert.gov.hk

Websites:

- www.govcert.gov.hk
- www.cybersechub.hk
- www.cybersecurity.hk
- www.infosec.gov.hk

HKCERT

Hong Kong Computer Emergency Response Team Coordination Centre - Hong Kong, China

1. Highlights of 2021

1.1 Summary of Major Activities

- Organised the "Build a Secure Cyberspace 2021" campaign with the Government and Hong Kong Police Force. The campaign involved public webinars, and a GIF Graphic Design Contest.
- Organised the "Hong Kong Cyber Security New Generation Capture the Flag Challenge 2021". It involved a 48-hours online contest and a public webinar with award ceremony.
- 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 during the COVID-19 pandemic period.

1.2 Achievements & Milestones

- Organised "Hong Kong Cyber Security New Generation Capture the Flag Challenge 2021" with 319 teams and 941 participants from universities, secondary schools and open categories. The competition was the first time expended to have open group category and international teams invited.
- Launched the "Fight Ransomware" page
- Launched the online self-assessment tool "Check your Cyber Security Readiness"
- Published security advisories on latest phishing and ransomware attacks patterns and emerging cyber threats
- Continue the Healthcare Cyber Security Programme which covered almost all public and private hospitals of Hong Kong
- Launched the Critical Infrastructure Cyber Security Programme, which covered 7 organisations that provide essential public services to the citizens.

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 subvented organisation in Hong Kong, has operated the centre since then.

2.2 Organisation and Workforce Power

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

2.3 Mission and Constituency

HKCERT is the centre of coordination of computer security incident response for the constituency (local enterprises and Internet users) in Hong Kong.

The mission of HKCERT is to be the cyber threats response and defence coordinator in Hong Kong to protect the Internet environment and the economic and social interests of Hong Kong.

The objectives of HKCERT are to serve as a focal point in Hong Kong for information security incident reporting and responses; to provide a focal point in Hong Kong for cooperation and coordination with other Computer Emergency Response Teams (CERTs), and relevant bodies outside Hong Kong; to promote awareness of the community on computer security issues and the latest international best practices and standards; and to provide assistance to the community in the protection against computer security threats and the prevention of security attacks and in recovery actions for computer security incidents

3. Activities and Operations

3.1 Incident Handling

During the period from January to December of 2021, HKCERT had handled 7,725 security incidents which was 7% decrease of the previous year (see Figure 1). Referral cases accounted for ~97% of the total number of security incidents.

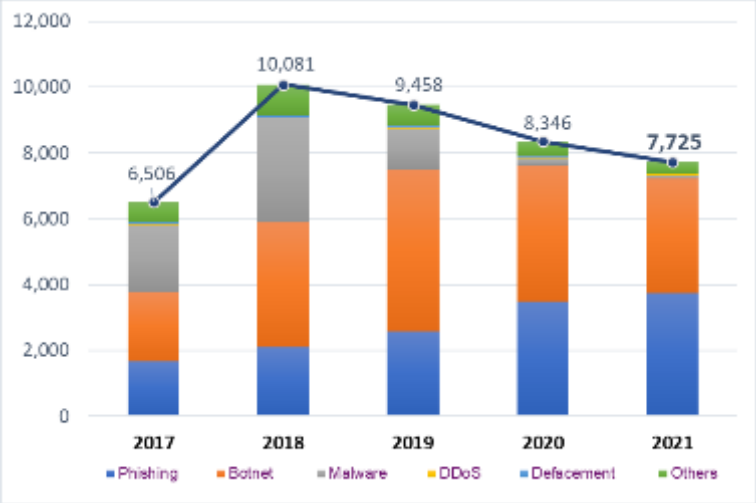


Figure 1. HKCERT Security Incident Reports

While the number of overall security incidents handled by HKCERT reported a drop for the third year running, falling 7% year-on-year to 7,725 in 2021. Phishing (3,737 cases or 48%) went up 7% with cyber criminals exploiting the surge of online activities due to the pandemic. On the other hand, botnets (3,479 cases or 45%), remaining the top source of reported incidents, and malware (112 cases or 2%) fell 16% and 38% respectively. The drop of malware cases was due to more malware targeting enterprises for higher return and the number of individual based reports dropped (see Figure 2).

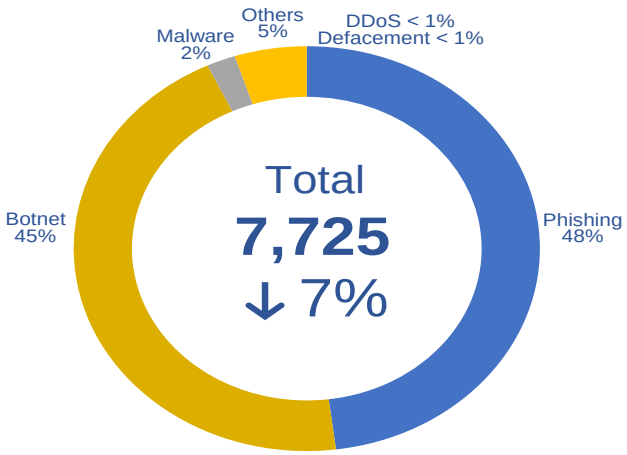


Figure 2. Distribution of Incident Reports

3.2 Watch and Warning

During the period from January to December of 2021, HKCERT published 359 security bulletins (see Figure 3) on the website. In addition, HKCERT have also published 39 security advisories, topics include the serious Log4J vulnerability, Microsoft MSHTML vulnerability, new trend of ransomware, new OWASP top 10, protect personal information in social media, malicious third party dependencies, security risks of online shopping, etc.

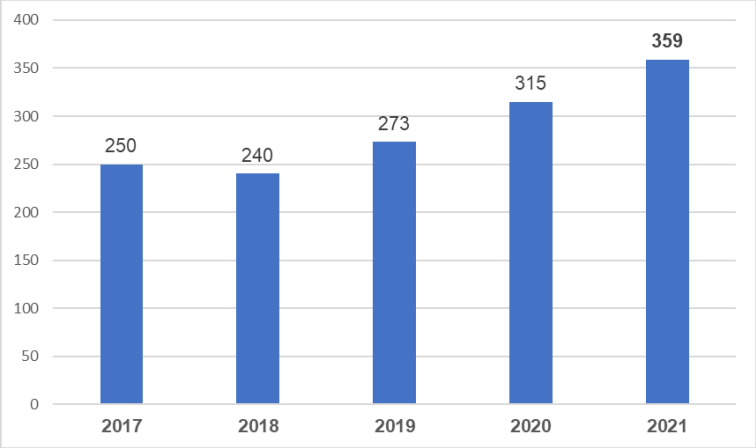


Figure 3. HKCERT Published Security Bulletins

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 6,042 in 2021 Q2, with a significant increase in Avalanche and Nymaim botnet events. The number dropped gradually to 3,097 in 2021 Q4. The major botnet remained as Mirai as depicted in Figure 5.

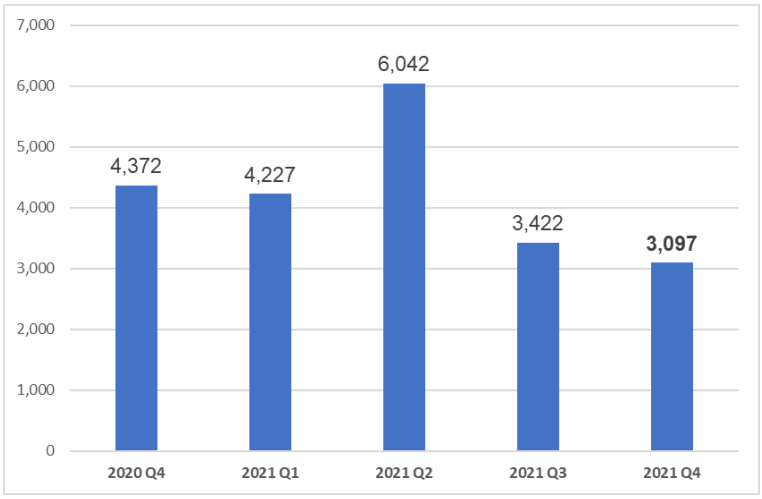


Figure 4. Trend of Bot related security events in the past year

(Source: data feeds from overseas security researchers, not from incident reports)

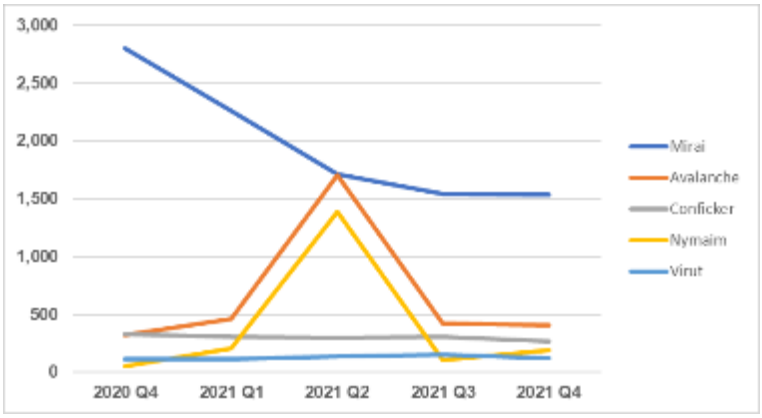


Figure 5. Trend of Top 5 Botnet Families in the past year

(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 6) (see https://www.hkcert.org/statistics).

Figure 6. Charts in HKCERT website showing the statistics of different types of incident reports.

4. Events organised and co-organised

4.1 Build a Secure Cyberspace 2021

HKCERT jointly organised the "Build a Secure Cyberspace 2021" campaign with the Government and Hong Kong Police Force. The campaign involved two public webinars, and a GIF Graphic Design Contest. A public webinar was organised in May 2021.

For the GIF Graphic Design Contest, HKCERT received about 151 applications from Open Group, Secondary School and Primary School Group. A professional judge panel selected winners with most creative and outstanding design (see Figure 7).

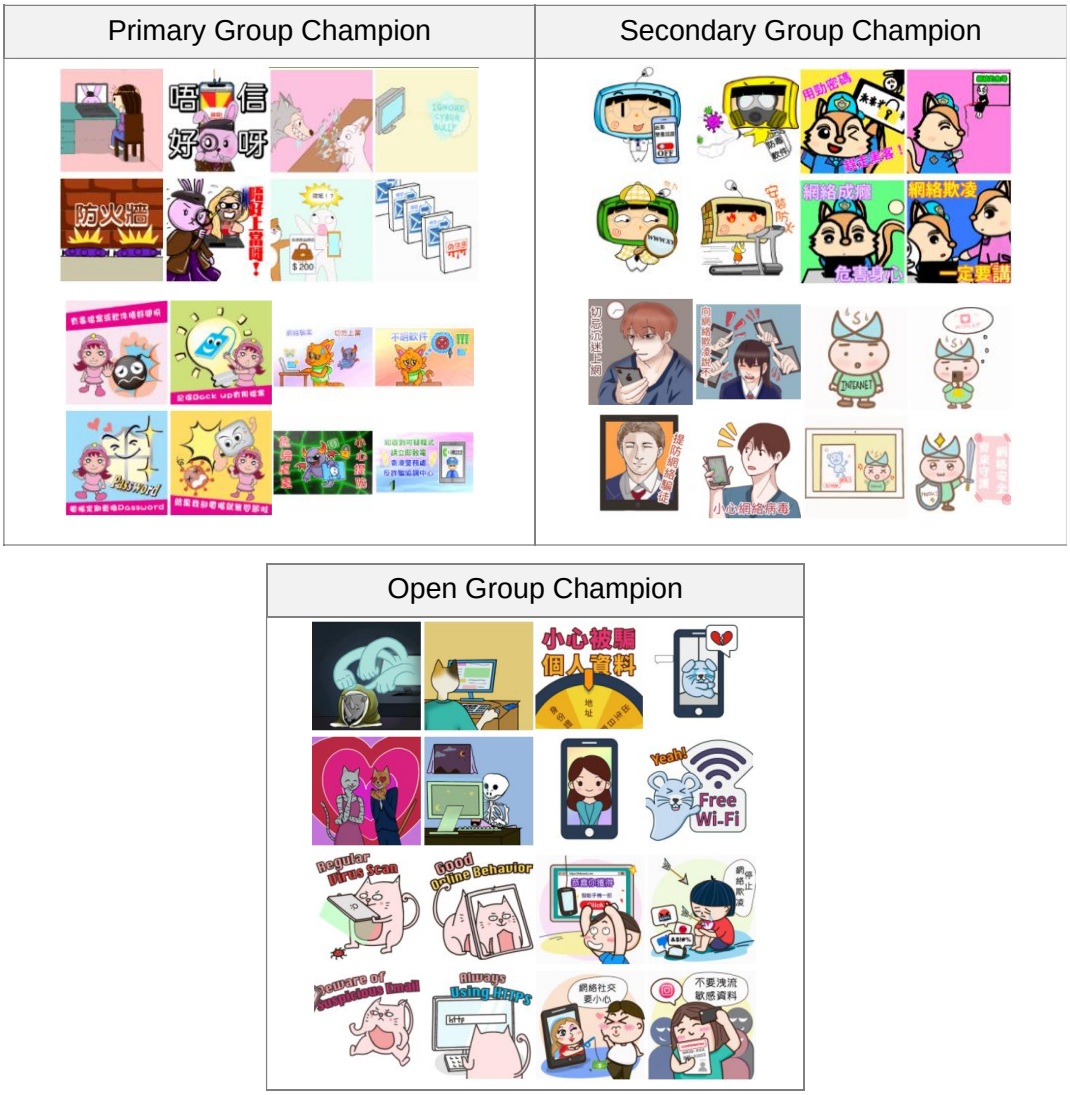


Figure 7. Champion entries of Primary School, Secondary School, Open Categories

Use this link to access the winning entries online:
https://www.cybersecurity.hk/en/contest-2021.php

4.2 Capture The Flag Contest

HKCERT jointly organised the "Hong Kong Cyber Security New Generation Capture the Flag Challenge 2021" with partner associations in information and education sectors. The 48-hours contest was opened to secondary and tertiary institutions. It was a success with 319 teams and 941 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 organised in December 2021.

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-2021-webinar-cum-award-ceremony
- https://www.hkcert.org/blog/hong-kong-cyber-security-new-generation-capture-the-flag-challenge-2021-award-presentation-ceremony-recognises-cyber-security-future-talents

4.3 New OWASP Top 10 Webinar

HKCERT arranged a webinar on Secure Coding Practices by sharing about latest OWASP Top 10 2021 version, what are the changes and the implications to application developer, with around 150 participants.

4.4 Speeches and Presentations

HKCERT was invited to deliver 26 speeches and presentations on various occasions for the Government, associations, SMEs, enterprises and schools.

4.5 Proactive Approach to Promote Awareness for Different Sectors in HK

HKCERT proactively approached several sectors in HK to promote cyber security awareness, e.g. telecom, retail and finance, etc.

4.6 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 advices on user awareness, ransomware and emerging technologies. HKCERT issued media messages 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 2021:

- Participated in the APCERT AGM and Web Conference
- Participated in the FIRST AGM and Web Conference
- Participated in the National CSIRT Annual Web Conference
- Participated in 2021 Global Conference on CNCERT International Partnership Web Conference
- Participated in the HITCON Annual and HITCON Pacific 2021 Web Conference
- Participated in the AusCERT Annual Web Conference
- Participated in APCERT Drill Exercise

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

5.2 Local Collaboration

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

- HKCERT continued to work closely with the government (GovCERT.HK) and law enforcement agency and held meetings to exchange information and to organise joint events regularly.
- HKCERT continued to actively participate in the Cyber Security Information Sharing platform 'Cybersec Infohub" which comprised of over 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 worked with HKPF and Interpol to conduct cyber hygiene operation. Misconfigured local servers which vulnerable to DDoS amplification attacks were collected and analysed. Owners of these servers were then notified the corresponding mitigation measures.
- HKCERT invited cyber security professors from local universities to form a vetting committee to vet and select the challenges to be used in the annual Capture the Flag contest.

6. Achievements & Milestones

6.1 Advisory Group Meeting

HKCERT had held the Advisory Group Meeting in September 2021. The meeting solicited inputs from the advisors 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 Ransomware Page

HKCERT had launched the "Fight Ransomware" page (https://www.hkcert.org/publications/fight-ransomware) in Nov 2021. The new page covered information of 6 areas to aid user to prevent and respond to the latest ransomware attacks. These 6 areas include (1) What is ransomware, (2) Infection method, (3) Ransomware's operation, (4) Prevention, (5) Incident handling and (6) Different decryption tools

6.4 HKCERT "Check Your Cyber Security Readiness" Self-assessment Tool

HKCERT had converted the paper checklist of "7 habits of cyber security for SME" to an interactive online self-assessment tool "Check Your Cyber Security Readiness". User will receive a score and appropriate recommendations based on his or her inputs, with actionable procedures from HKCERT or external resources. The tools can bring the following benefits to users: (1) Improve user experience, (2) Enhance the usability and (3) Better reporting.

6.5 Study of Latest Phishing and Ransomware Attacks Pattern

HKCERT studied the latest attacker techniques employed in phishing and ransomware attacks and summarised the patterns observed into two security advisories to raise situational awareness of users.

6.6 Security Guidelines and Advisories for Emerging Cyber Threats

HKCERT published different security guidelines and alerts in response to the emerging cyber threats, such as vulnerabilities in Log4j, Microsoft MSHTML, remote access device and storage device, how to protect sensitive information in social media, etc.

6.7 Healthcare Cyber Security Watch Programme

The programme was launched in December 2020 and 12 local healthcare organisations joined. In 2021, two more local private hospitals agreed to join which made the coverage of the programme almost all public and privates hospitals in Hong Kong.

6.8 Critical Infrastructure Cyber Security Watch Programme

The programme was launched in December 2021 and 7 local organisations that provide essential public services to the citizens in Hong Kong joined. The intelligence monitoring mechanism was established and dedicated private groups was setup to facility intelligence sharing within members.

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 organised a year ender press briefing to media in February 2022 to review cyber security landscape of 2021 and provided an outlook to 2022 to warn the public for better awareness and preparedness. It received very good press coverage.

Figure 8. 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 2022/2023. 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 success of the Capture The Flag (CTF) contest, HKCERT will continue to partner with different associations to organise another CTF in 2022 for the participants from universities, secondary schools and open categories.

HKCERT will proactively reach out to those SMEs through working with the trade associations in order to raise the cyber security awareness and capacity of the SME with HKCERT's services and resources.

HKCERT will provide a free-of-charge block-list based on the intelligence source from HKCERT incident response case handling and security researchers. SMEs which own security appliances that support External Dynamic List (EDL) technology can configure automatic block-list update. Once configured, the SME firewall can block upcoming attacks. It is an easy to use and low-cost solution to SMEs.

8. Conclusion

In 2021, the number of overall security incidents reported to HKCERT recorded a drop (7%) for the second year running. Phishing increased by 7% with cyber criminals exploiting the surge of online activities amid pandemics. On the other hand, botnet and malware fell 16% and 38% respectively. The latter was due to a drop of massive individual ransomware cases as cyber criminals moved to target enterprises for higher monetary return.

In 2022, HKCERT urges enterprises to quickly put in place cyber security strategy for the new technologies, in order to combat an anticipated surge in cyber attacks arising from accelerated digital transformation amid the pandemics and the use of emerging technologies such as 5G communication, Internet of Thing (IoT), Operational Technology (OT), Artificial Intelligence (AI) and widely use of QR code. Furthermore, HKCERT also urges enterprises to be ready for an escalation in supply chain attacks in which attackers leverage on the trust of an enterprise on its supply chain partners to bypass traditional defences, and the security risks of Cryptocurrency and Metaverse. HKCERT will also promote Incident Handling (Prevention and Response) and cloud security and groom the next generation cyber security talents.

ID-SIRTII/CC

Indonesia Security Incident Response Team on Internet Infrastructure/Coordination Center – Indonesia

1. Highlights of 2021

1.1 Summary of major activities

The condition of the COVID-19 pandemic that has occurred since the beginning of 2020 in Indonesia has presented several operational challenges for Id-SIRTII/CC - NCCA (National Cyber and Crypto Agency, considering that these conditions, especially the limitations of physical activity, pose extraordinary challenges both in terms of increasing incidents that occur and the process of responding to incidents that occur.

However, IdSIRTII-CC/NCCA continues to operate normally in full, while still providing services such as notification of security incidents/warnings, making security appeals, consulting, and assisting in response to cyber incidents. In addition, IdSIRTII-CC/NCCA is also involved in several international activities, such as a webinar at the OIC CERT forum which raised the issue of Incident Response during a Pandemic which brought together several stakeholders such as law enforcement and representatives from the National CSIRT of several countries. Then at the same forum, we also held several workshop sharing sessions for OIC CERT members, participating in training activities and various cyber exercises organized by the international community, IdSIRTII-CC/NCCA also appeared to organize these activities by involving the participation of countries in making it a success.

1.2 Achievements & milestones

The major achievement in 2021 for NCCA, especially Id-SIRTII/CC as the National CSIRT is to establish CSIRTs in several government agencies and build communication and coordination mechanisms for established CSIRT. By 2020, NCCA has established 15 CSIRTs in the government sector, and another 45 CSIRTs in local government by 2021.

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, and 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:

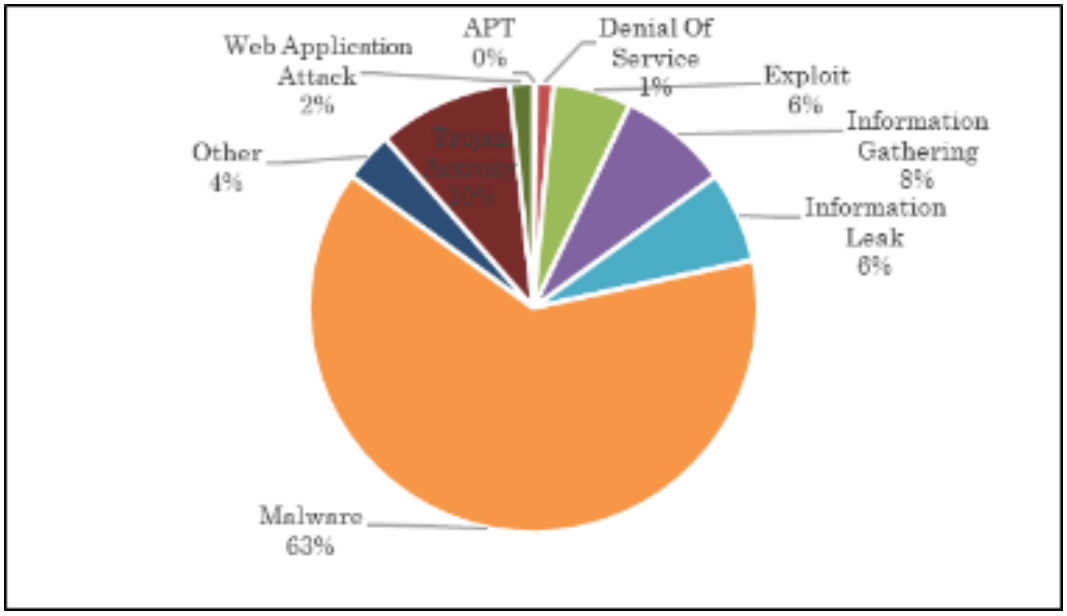
- Ministries and Government agencies
- Law enforcement agencies (LEAs)
- National Defence
- CII Operators
- Cybersecurity communities
- Internet Service Providers (ISP)
- Network Access Providers (NAP)
- Local Internet Exchange Operators
- Other Sector CERT / CSIRT in Indonesia

3. Activities & Operations

3.1 Scope and definitions

In 2021, 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:

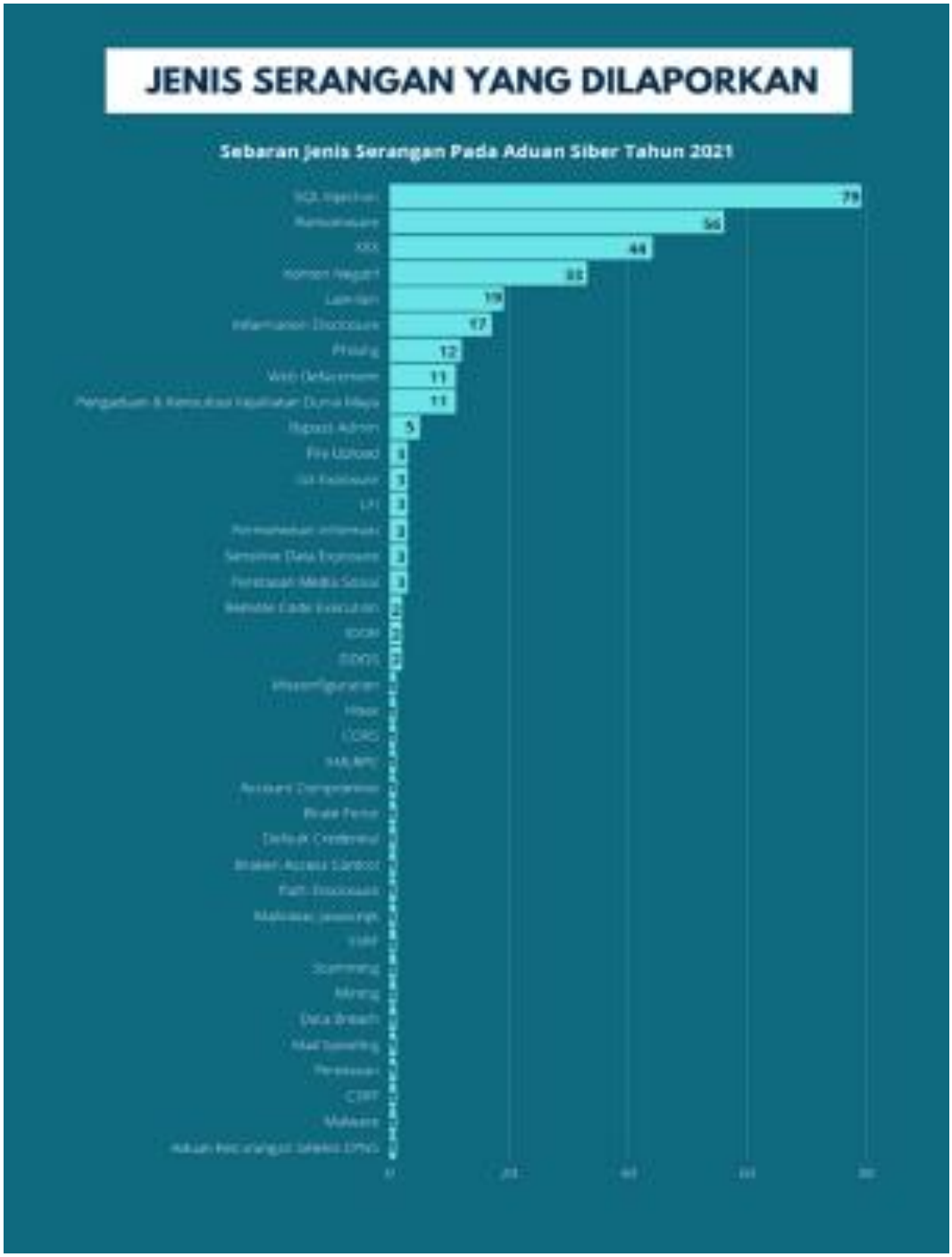
- Received 330 complaint reports in total. Most of the reports came from the government's sector with 81 (25%) reports. SQL Injection and Ransomware became the most attacks reported, 79 reports about SQL Injection and 56 about Ransomware.
- Id-SIRTII/CC recorded 1.637.973.022 traffic anomalies both from local and overseas, which are dominated by malware activity, the graph is shown in the following figure.



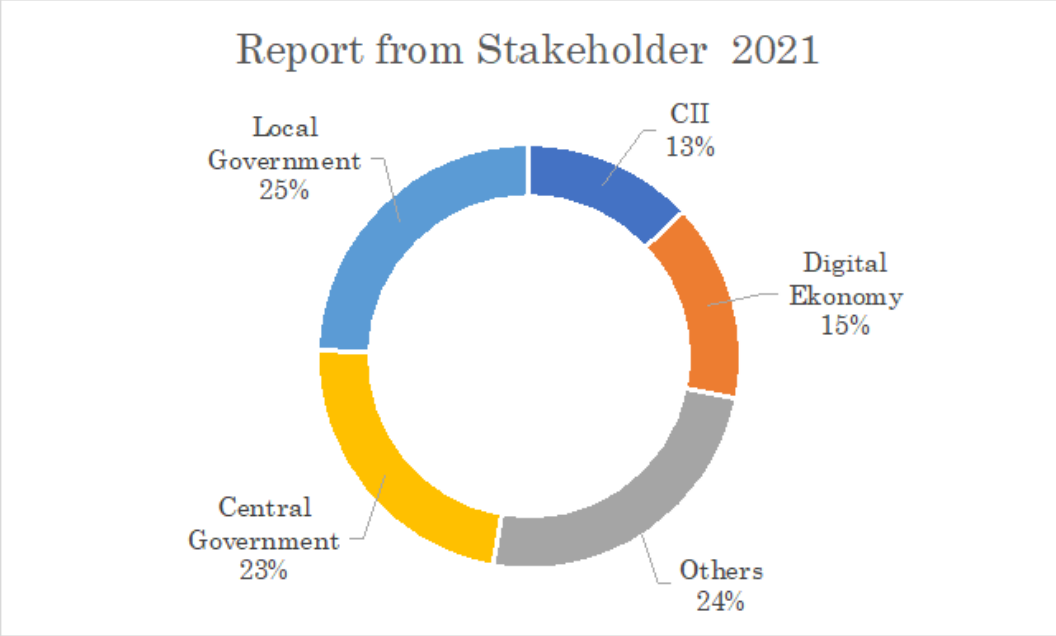
Traffic anomaly category.

3.2 Incident handling reports

Incident reports to Id-SIRTII/CC in 2021 were categorized as shown in Figure 2 (attack type) and Figure 3 (reported sector). About 25% of the reports came from the central government sector, 25% from other sectors, 23% from local government, 15% from the digital economy, and the rest was from the national critical infrastructure sector.



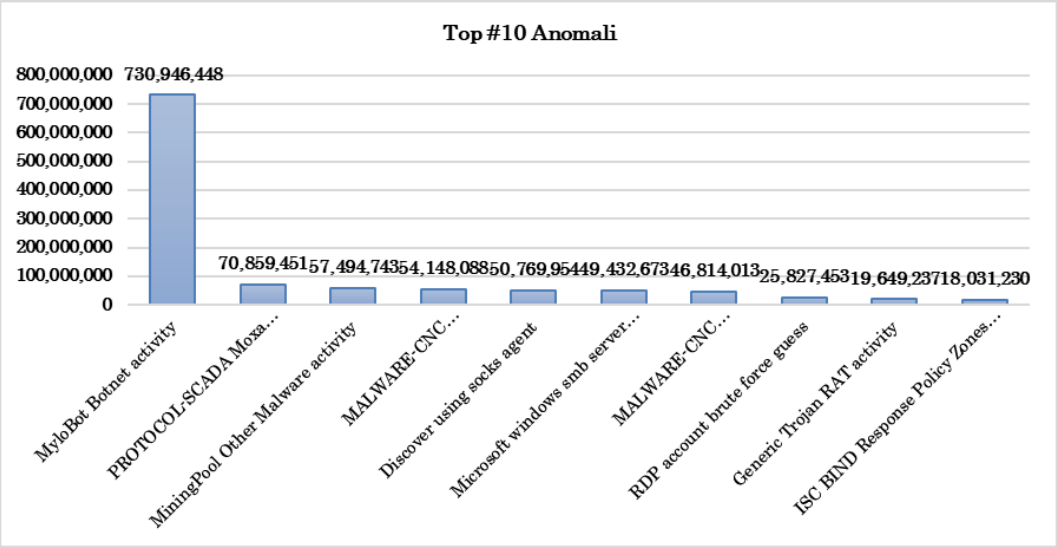
Reports in 2021 based on the reported attack type.



Reports in 2021 based on reported sector.

3.3 Abuse statistics

There are many anomalies activity in Indonesia, that has increased significantly in October 2021, this condition persists until December 2021.



Top 10 Anomalies in 2021

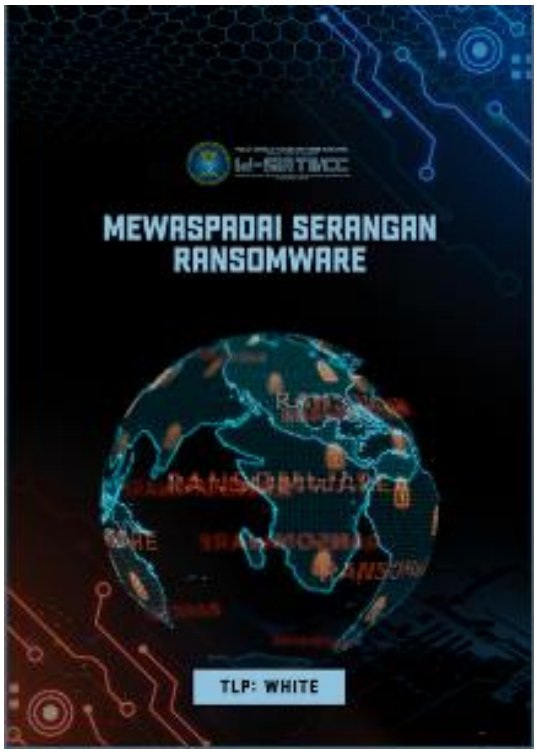
The histogram shows the number of traffic anomalies

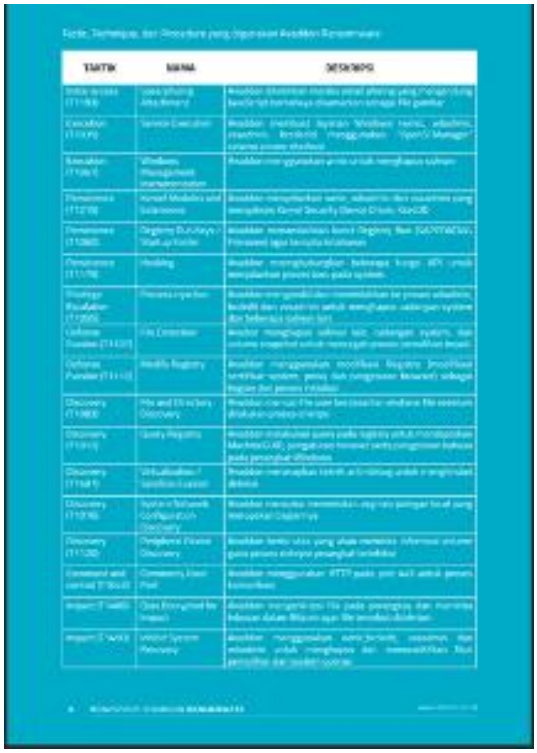
3.4 Publications

Every month Id-SIRTII/CC publishes National Monitoring Monthly Report, from January to December in 2021. Id-SIRTII/CC also published its annual report, that's published in Id-SIRTII/CC and BSSN website, published security guidelines, and security advisory.

Id-SIRTII/CC January 2021 monthly report.

Id-SIRTII/CC 2020 annual report.





Security Guidelines

Security Advisory

3.5 New services

Currently there is no new services.

4. Events organized/hosted

4.1 Training

- Conducted a Technical Assistance for Regional Government CSIRT (30 March)
- Conducted OIC-CERT Webinar "Data Breach: Mitigation and Lesson Learned" (29 June)
- Conducted OIC-CERT Technical Workshop "Malware Analysis" (17 November)
- Hosted APCERT Training "Wireless Network Security" (7 December)

4.2 Drills & exercises

- Conducted Coordination Forum of Indonesian Gov-CSIRT with Drill Test and Table Top (8 December)

4.3 Conferences and seminars

- Conducted a webinar for "Indonesia Cybersecurity Monitoring Annual Report 2020" publishing (1 March)

5. International Collaboration

5.1 Capacity building

5.1.1 Training

- Collaborated with Carnegie Mellon University to conduct technical training for Id-SIRTII/CC personnel with the theme "Unhiding Hidden Cobra" (15 February)
- Collaborated with Carnegie Mellon University to conduct technical training for Id-SIRTII/CC personnel with the theme "Industrial Control Systems (ICS) Training" (February-April)
- Participated in APCERT Training: Implementing IoT Security Testing (23 February)
- Participated in Japan-US Industrial Control System Cybersecurity Week FY2020 the year 2021 (8 March)
- Participated in FIRST Regional Virtual Lightning Talk Session (1 April)
- Participated in Carnegie Mellon University "Training of Trainer: Creating and Managing CSIRT" (2 November)

5.1.2 Drills & exercises

- Participated in NISC: International Cybersecurity Exercise 2021 (25 February)
- Participated in APCERT Drill Test 2021 (25 August)
- Participated in SingCERT ASEAN CERT Incident Drill (ACID) 2021 (8 September)
- Participated in OIC-CERT Cybersecurity Drill "Enhance Cyber Security Readiness" 2021 (28 September)
- Participated in ITU Cyber Drill (4 November)
- Participated in Taiwan Cyber Offensive and Defensive Exercise (CODE) 2021 (16 November)
- Participated in Egyptian First International Cyber Drill (22 Dec 2021)
- 5.1.3 Seminars & presentations
- Participated in CIT-CERT/CC Pakistan (C4P) Conference 2021 as a panelist (16 December)

6. Future Plans

6.1 Future projects

In line with the mission on establishing regional CSIRTs which become one of our major focuses, it leads to a plan on how a cybersecurity institution like NCCA and Id-SIRTII/CC as a National CSIRT, gain a good relationship with regional agencies, especially with the private sector and critical infrastructure sector, to collaborate in cybersecurity and to establish their CSIRTs.

Based on this objective, we plan to hold a series of activities that gather ideas and experiences from various countries in collaborating with relevant sectors in their respective countries to improve their national cyber security. As we know, as a national agency engaged in cybersecurity, it is essential to gain public trust and build collaboration with the private sector, especially the critical infrastructure sector.

6.2 Future Operation

- Collaborating with relevant ministries and stakeholders about establishing CSIRT, especially the critical infrastructure sectors.

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.

8. 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 – Japan

1. Highlights of 2021

1.1 Summary of major activities

- JPCERT/CC staff member is elected to the Board of FIRST

The Forum of Incident Response and Security Teams (FIRST) is the world's largest CSIRT community, and its activities are planned and operated by the 10 members on its Board of Directors. The directors serve a 2-year term, and half of them are elected each year through voting by participating organizations. The results of this year's online elections were announced at the Annual General Meeting held on June 10, and Yukako Uchida, Manager of Global Coordination Division who ran for the board from JPCERT/CC, was elected. Please refer to the link below for information about other board members.

FIRST.Org,Inc., Board of Directors
https://www.first.org/about/organization/directors

- JPCERT/CC now oversees 5 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.

1.2 Achievements & milestones

- Remote Operation of JPCERT/CC under the COVID-19 Pandemic

Even in the current global COVID-19 pandemic, JPCERT/CC's operation has been stable and successful thanks to our dedicated staff members working safely from home.

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 2021, JPCERT/CC received 44,242 computer security incident reports from Japan and overseas.

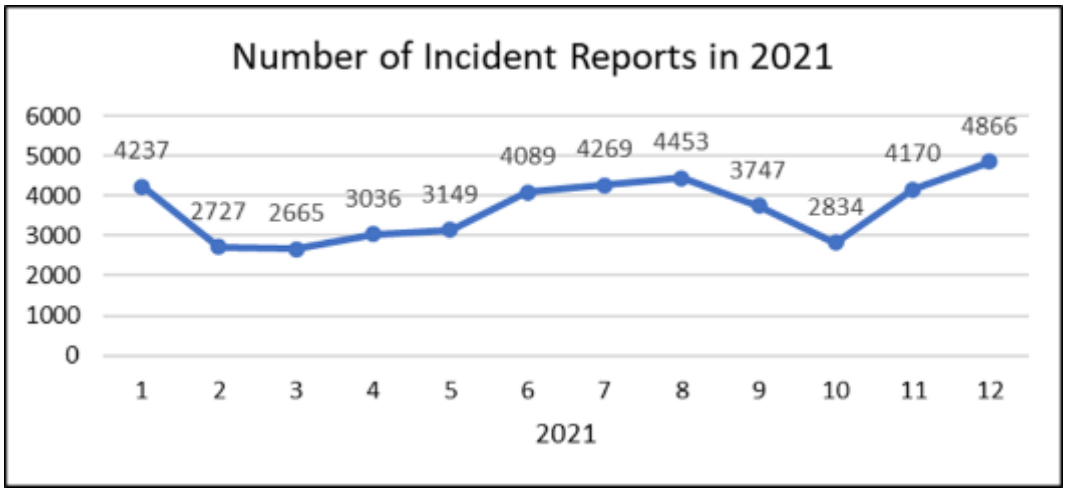


Figure 1. Number of Incident Reports (2021)

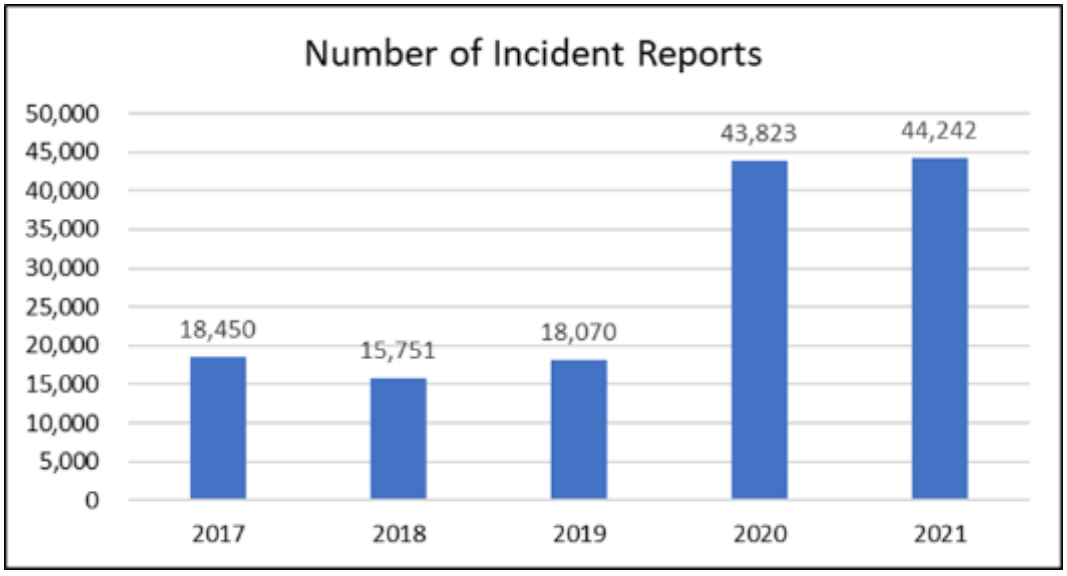


Figure 2. Incident reports to JPCERT/CC (2017-2021)

3.2 Abuse statistics

Incidents reported to JPCERT/CC during the last quarter of 2021 were categorized as in Figure 3. More than 70% of the reports were on phishing site, followed by scan and website defacement.

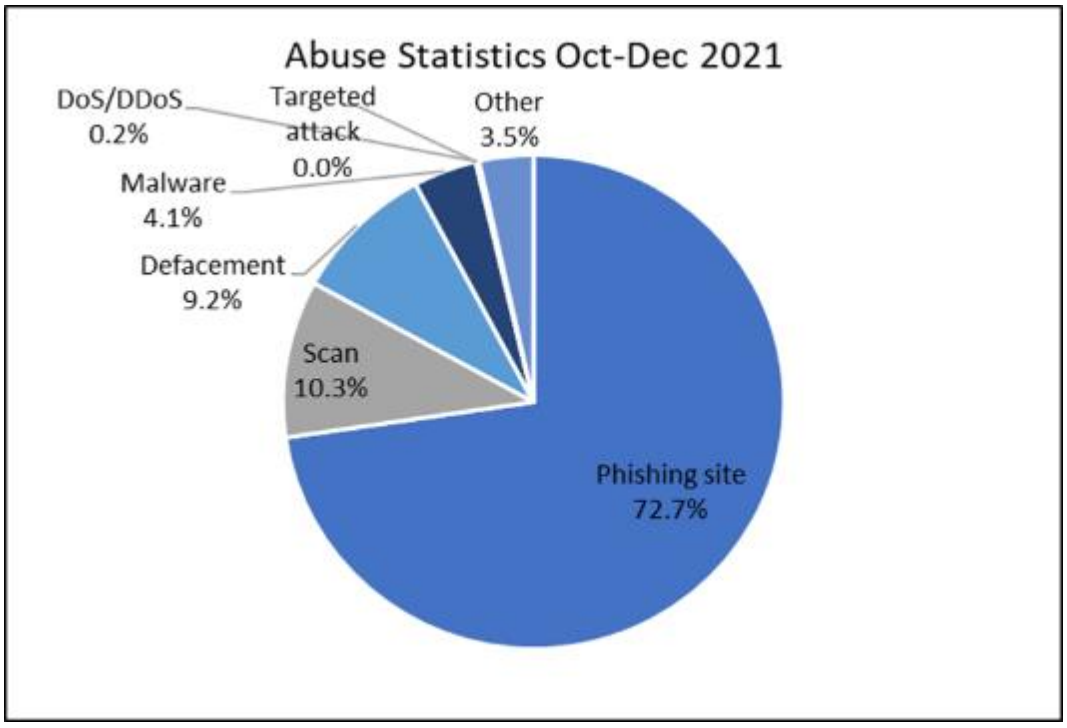


Figure 3. Abuse Statistics of Oct-Dec 2021

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 2021, 79 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 2021, 4,269 vulnerabilities coordinated by JPCERT/CC were published on JVN. 1,956 were cases published with IPA through the Information Security Early Warning Partnership, and 2,313 were published through partnerships with overseas coordination centers, developers, researchers, etc.

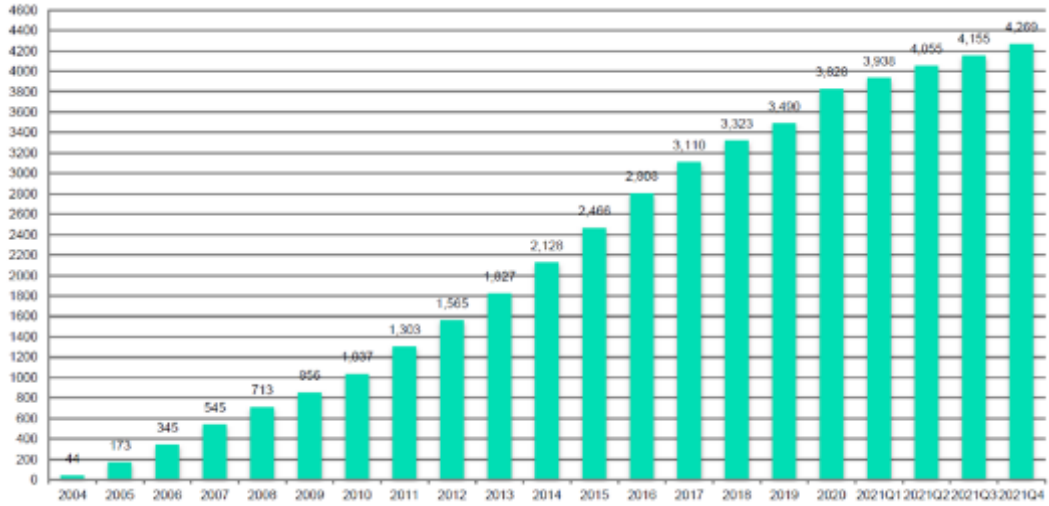


Figure 4. Number of vulnerabilities published on JVN by year

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. TSUBAME Working Group is active in APCERT, and observation results are exchanged among the teams.

- 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 Japan Security Analyst Conference 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 2021, JPCERT/CC supported 4 organisations to become a full member.

- 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 2021 to test our incident response capability:

- African Cyber Drill (30 June – 1 July)
- APCERT Drill 2021 (25 August)
- ASEAN CERTs Incident Drill (ACID) 2021 (5 October)

5.2.2 Seminars & presentations

In 2021, JPCERT/CC delivered presentations at the following international cyber security events:

- Global Digital Futures Policy Forum: Saving Cyberspace (April, Online)
- TWCERT/CC Annual Conference (November, Online)
- 16th Annual IGF Meeting (December, Online)

...and more

5.2.3 Other international activities

Below are some of the international events that JPCERT/CC attended in 2021:

- APRICOT 2021 (February-March, Online)
- NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) Locked Shields 2021 (April, Online)
- Blackhat USA 2021 (May)
- AusCERT2021 (May)
- 16th Annual NatCSIRT Meeting (June)
- OIC-CERT Webinar (June, Online)
- APSIG Webinar (July, Online)
- USENIX Security Symposium (August, Online)
- APNIC52 (September, Online)
- 2021 World Internet Conference (September, Online)
- APrIGF 2021 (September, Online)
- 31st Virus Bulletin Conference (October, Online)
- ICANN72 (October, 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

KrCERT/CC

Korea Internet Security Center – Korea

1. Highlights of 2021

1.1 Summary of major activities

In 2021, related Korean government departments, mainly the Ministry of Science and ICT, jointly prepared a “Ransomware Response Reinforcement Plan” to cope with ransomware attacks and announced it at the 42nd “Central Emergency Economy Countermeasure Headquarters meeting.” The government also established the “K-Cyber Security Alliance” and gathered collaborating expert groups in each field to achieve the common goal of “cybersecurity.”

1.2 Achievements & milestones

Damage by ransomware that steals victims’ data and demands money in return for decrypting it is increasing at home and abroad. Accordingly, the Ministry of Science and ICT and related government departments jointly announced a reinforcement plan, "Ransomware Response Reinforcement Plan." KrCERT/CC is a working organization that implements the reinforcement plan, increases the designation of critical information infrastructure, improves protection measures, and increases emergency inspections and cyber exercises. KrCERT/CC also supports the security enforcement of the entire cycle, from software and solution design to distribution, through the software development the Security hub, to keep the infrastructure supply chain safe. KrCERT/CC also established a basis for supporting data backup, encryption, and recovery to support the response capability of small and medium-sized businesses with a rather weak security system.

Nowadays, cyberattacks are spreading to all fields closely related to daily life, such as finance, healthcare, IT service, and manufacturing, and various types of damage caused by malware code infection and service shutdown are also affecting the people’s daily life. As a result, it is difficult for the government alone to respond to and prevent those attacks. Accordingly, KrCERT/CC launched “K-Cyber Security Alliance” (November 2021) by organizing private cooperative channels that have participated so far and decided to open the Cyber Threat Analysis & Sharing (C-TAS) system that has been operated since 2014 (January 2022). The “K-Cyber Security Alliance” aims at

preemptively responding to advanced cyber threats by strengthening cooperation and discovering policy agendas through exchanges between channels while maintaining the specialization of each information security cooperation channel. The Alliance is composed of three divisions: policy/system, detection/sharing, and response/capability. The cyber threat information analysis and sharing system has been completely reorganized as well to provide threat information and cyber threat trends, so that visitors can use the information easily.

2. About CSIRT

2.1 Introduction

As Korea's national CSIRT, the Korea Computer Emergency Response Team/Coordination Center (KrCERT/CC) is responsible for the private sector. Formed under the Korea Internet & Security Agency (KISA), KrCERT/CC is composed of three divisions and one center with fourteen teams. KrCERT/CC operates various responsive and preventive programs designed to minimize cybersecurity damage by enabling prompt response to incidents and to increase awareness in order to prevent incidents.

2.2 Establishment

KrCERT/CC started out in 1996 as a small team responsible for hacking incidents under the Korea Information Security Agency (formerly known as 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 made the Korean government realize the importance of cooperation with security incident response teams and businesses such as ISP. As a result, we came up with an organizational structure for an incident response team similar to that of the present in December 2003. With nationwide serious security incidents occurring in 2007, 2009, and 2013, the team was reformed in order to cope more effectively with such, and its size and budget were expended to today's KrCERT/CC (for analysis, response, and sharing). Domestically, it is usually called KISC or Korea Internet Security Center.

2.3 Resources

As of December 2021, 160 employees from 4 divisions work for KrCERT/CC.

2.4 Constituency

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

3. Activities & Operations

3.1 Scope and definitions

KrCERT/CC works for safe, reliable cyber space by preventing cyberattacks and enhancing countermeasures. Its mission is to guarantee rapid response to major Internet incidents nationwide to prevent and minimize damages and to cooperate closely with domestic (ISPs, antivirus companies) and foreign (FIRST, APCERT, etc.) partners in 24/7 Monitoring and Early Detection/Response with regard to cyberattacks in the private sector.

3.2 Abuse statistics

According to the survey among 150 corporate security managers in Korea, ransomware is the most worrisome cyber threat in 2022. As the concerns were true, ransomware damages are actually reported. According to the Ministry of Science and ICT, the number of ransomware hacking damage reports increased 76% from 127 cases in 2020 to 223 cases in 2021.

Number of ransomware report (MSIT)

Year	2019	2020	2021
Ransomware reports	27	127	223

As HTTP-based malware distribution has increased since 2006, KrCERT/CC has maintained a detection and response system against web-based malware. Furthermore, 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 continued to expand to 4.1 million in 2021.

Number of detection on malware distribution sites (KrCERT/CC)

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

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

Among such malware, credential stealer constituted 41.8%, downloaders, 12.2%, ransomware and crypto-miner, 5.3%, RAT, 4.2%, and DDoS attack, 4.2%.

3.3 Publications

In 2021, KrCERT/CC released three trend reports and Cyber Security Advisory 2022. KrCERT/CC also published one technical report on the responding method for vulnerability cases and vulnerability analysis, four analysis reports on the attacker strategy and cybersecurity incident, and one special report on ransomware. Those reports are available on the KrCERT/CC website (www.boho.or.kr).

3.4 New services

Presented as a measure to support small and medium-sized businesses among the aforementioned ransomware reinforcement measures, “Data Vault” is a service that supports data backup, encryption, and recovery to prevent data loss in the event of ransomware infection. Costs such as the cloud backup service fee will be supported for small and medium-sized businesses in 2022.

* Please note that this service is implemented by the Korea Internet & Security Agency, the parent organization of KrCERT/CC.

4. Events organized/hosted

4.1 Training

Online APISC incident response training: October

4.2 Drills & exercises

Cyber exercise to respond to cyber crisis in the private sector: First half and second half

5. International Collaboration

5.1 Capacity building

5.1.1 Drills & exercises

KrCERT/CC participated in the APCERT annyal drill and led the drill working group this year. The topic was a spear phishing attack targeting working from home.

5.1.2 Seminars & presentations

Due to the continued travel restrictions, KrCERT/CC participated in online conferences such as the cybersecurity session panel discussion of the World Internet Forum hosted by NASK, Poland and FIRST Africa & Arab Symposium and presented the mock training of APCERT and KrCERT/CC.

6. Future Plans

6.1 Future projects

The C-TAS system plans to provide an emergency propagation service to prevent damage from threats by providing customized information according to the work characteristics of security operators (cyber threat information) and managers (information security policy guide) and disseminating the information that requires corporate to respond using text message or social media's direct message.

6.2 Future Operation

In 2021, KrCERT/CC researched technology and established Honeynet to prevent and respond to cyber threats that were increasing after the COVID-19 pandemic due to home networks and corporate networks linked to the outside. Based on the research results in 2021, KrCERT/CC plans to operate Honeynet and conduct awareness improvement activities such as trend report publication and public alert issuance in 2022.

7. Conclusion

Last year, online activities increased, and quarantine in digital space became important due to the continuing COVID-19 pandemic. KrCERT/CC was busy checking vulnerabilities and responding to cyber security incidents to protect national life and corporate safety from the increasing threat of ransomware. We at KrCERT/CC believe that we did our best to play the assigned roles despite the ongoing difficulties.

mmCERT

Myanmar Computer Emergency Response Team – Myanmar

1. Highlights of 2021

1.1 Summary of major activities

Due to the Covid-19 conditions, there had constraints to physical activities and thus all events and seminars have to change to virtualize since the late 2020. Moreover, as Myanmar was faced many challenges in 2021, activities of mmCERT were inevitably slow down and the numbers of incident reporting to mmCERT from individual persons had decreased radically in 2021. In spite of these challenges and constraints, mmCERT keeps on serving to response and handle cyber incidents and to provide technical assistant to its constituency.

In addition, mmCERT joined and attended international meetings and activities such as ASEAN-Japan Working Group meeting, ITU events and other events of international communities.

And then, mmCERT had involved in APCERT Drill, Global Cyber Drill and ASEAN-Japan Cyber Remote Exercises yearly. mmCERT participated in international knowledge sharing sessions, webinars, and forums.

mmCERT had successfully launched a new service of XDR service to provide security for Government Organizations.

2. About CERT

2.1 Introduction

Myanmar Computer Emergency Response Team (mmCERT/cc) is a national CERT for handling cyber security incidents in Myanmar. Besides doing incident handling activities, mmCERT works to increase public awareness in cybersecurity and supports technical advisories in its community.

2.2 Establishment

mmCERT was established on 23rd July 2004 under Information Technology Department, Myanmar Posts & Telecommunications (MPT), Ministry of

Communications, Posts & Telegraph (MCPT). MPT was state-own telecom operator and mmCERT mainly handled computer incidents of MPT and government agencies.

On 15th December 2010, mmCERT extended its service coordination center (cc). In 2011, mmCERT became a member of APCERT.

In 2015, Information Technology and Cyber Security Department (ITCSD) was formed 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, Ministry of Transport and Communications (MoTC) was reformed by merging three ministries Ministry of Communications and IT, Ministry of Transport and Ministry of Railway Transportation. ITCSD was moved to Ministry of Transport and Communications (MOTC).

2.3 Resources

mmCERT members are recruited by Ministry of Transport and Communications (MoTC). The head of management is the director of National Cyber Security Center (NCSC) under Information Technology and Cyber Security Department (ITCSD). Being insufficient in human resources to handle the cyber issues, it has been planned to extend the organization structure and to recruit more professionals.

2.4 Constituency

Since establishment, mmCERT has been serving for propagating cyber 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 service to the constituency to financial institutions, banks, online services/ shopping, research and development center and vendors.

3. Activities & Operations

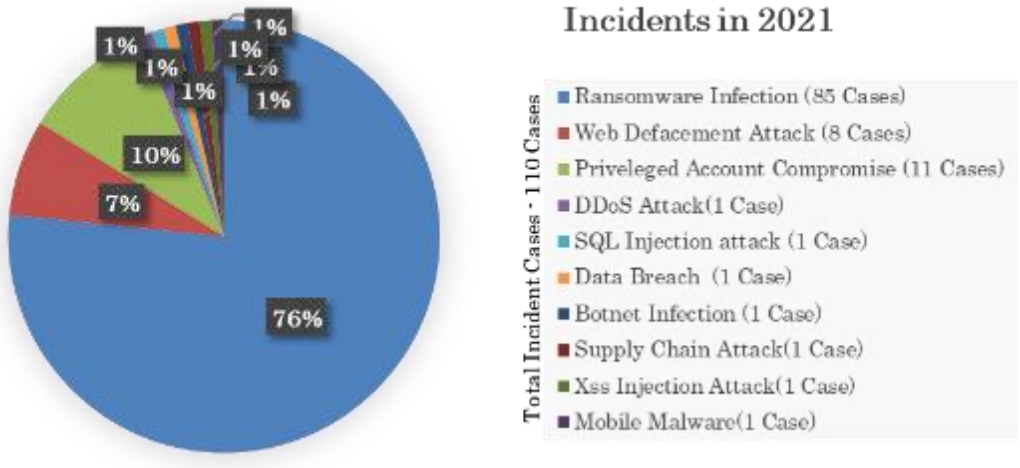
3.1 Scope and definitions

- Create National IT image by cooperating with international CERT teams for cyber security and Cyber crime

- Disseminate Security Information and Advisories
- Provide technical assistance
- Cooperate with law enforcement organizations for cyber crime

3.2 Incident handling reports

The following graph shows the incidents handled by mmCERT in 2021. According to the results on incident analysis by mmCERT, ransomware attacks were the most prominent incident cases in 2021.



3.3 Publications

3.3.1 Social Media

mmCERT releases reliable, accurate and timely information about emerging cyber threats and vulnerabilities in its official Facebook page:

- https://www.facebook.com/mmcert.team/

3.3.2 Website

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.

- https://www.mmcert.org.mm
- https://www.ncsc.gov.mm

3.3.3 Articles

mmCERT releases "STOP Ransomware Guidelines" on its Facebook page and website from Version 1.1 to 1.4 according to timely changes of encryption method of the developer.

"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.

Trending security and cyber threat news and articles can be seen frequently in the following mmCERT Official Facebook Page and Website:

- https://www.facebook.com/mmcert.team/
- https://www.mmcert.org.mm/

3.4 New services

In this year, Extended Detection and Response (XDR) Service was introduced which monitors the email servers and web servers of Union Ministries and Government Agencies and provides real time detection of cyber-attacks and minimization of losses.

To provide prompt assistance for incidents, mmCERT 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

"Myanmar Webinar on Data Privacy and Protection" was conducted with the aim to enhance understanding among policymakers, regulators and civil servants on the importance of data privacy and protection; emphasize the role of data privacy legislation; and to share information on international frameworks and good practices, including from ASEAN countries.

The event was co-organized with the Asian and Pacific Training Center for ICT for Development (APCICT) under the United Nations Economic and Social Commission for Asia and the Pacific and was held from 25th to 28th January 2021.

5. International Collaboration

5.1 Capacity building

5.1.1 Training

- Attended online training on Cybercrime and Digital Investigation on 25th January to 5th February 2021.
- Member of mmCERT attended the Defense Practice against Cyber-Attacks (JICA) in February 2021.
- AJCCBC online technical skill training related to incident response using a CTF format during 1st to 31st March 2021.
- mmCERT members attended ASEAN-JAPAN CYBERSECURITY CAPACITY BUILDING (AJCCBC) which provides CYDER Course, Digital Forensic and Malware Analysis in March, September and October 2021.
- Members of mmCERT joined APNIC Live eTutorial - Information Security for System Administrators on 7th to 8th July, 2021.
- Industrial Cybersecurity course on 13th July 2021.
- Participated in APCERT Training Program held on on 3rd August, 2021.
- Member of mmCERT attended the APISC Security Training Course at Seoul, Republic of Korea provided by KISA and KrCERT/CC in 18th to 22nd October, 2021.
- Attended AJCCBC Cyber Security Technical Training for Threat-Hunting exercise on 8th to 12th November 2021.
- ASCCE-Temasek Polytechnic Cyber Incident Response & Threat Analysis Course hosted by Asean-Singapore Cybersecurity Center of Excellence during 7th to 9th December, 2021.

5.1.2 Drills & exercises

- Participated in ASEAN –JAPAN Cyber Remote Exercise on 24th June, 2021.
- Participated in APCERT Drill in 25th August 2021.
- Joined in Table-top Exercises from APCERT Conference on 28th September 2021.
- Participated in ACID Drill on October 7, 2020.
- Participated in ITU 2021 Global CyberDrill Scenario-Based Exercises from November 2 to 4 and 9 to 11, 2021.

5.1.3 Seminars & presentations

- Attended the Countering COVID-19 Related Disinformation and Hate Speech in Southeast Asia Curriculum Workshop held by IFES on 27th to 28th January, 2021.
- Joined Sharing on the Evolving Ransomware Threat Landscape and Altdos hosted by SingCERT on 29th June, 2021.
- Attended Emerging Technology for Connectivity: Accelerating Digital Transformation in LDCs, LLDCs and SIDS organized by ITU on 5th to 9th July 2021.
- Participated in the 2021 3rd ASEAN-Japan Cybersecurity Working Group Online Meeting on 22nd September, 2021.
- Participated in APCERT Conference 2021 on 30th September, 2021.
- ASEAN Data Management Framework (DMF) Capacity Building Program on 11th to 12th October, 2021
- Participated in the workshop on Blockchain for the digital government that will be held at Vientiane Capital, Lao PDR on 13th October 2021.
- Joined JP-US-EU ICS Cybersecurity Week FY2021 on 25th to 29th October, 2021.
- Involved in Workshop on China-ASEAN & CJK 5G Network Security Technical and Industrial Communication and Training on 2nd to 3rd November, 2021.
- Attended the Asia and the Pacific Regional Dialogue on Digital Transformation: Gearing Up for Inclusive and Sustainable Development by ITU during 7th to 10th December, 2021.

5.2 Other international activities

- Joined the 2021 ASEAN-Japan Cybersecurity Working Group Meeting in 2021.
- Joined Second Online Open Consultation on the Draft Guidelines for utilization of the Global Cybersecurity Agenda (GCA) held by ITU on 1st March, 2021.
- Jointed the Global Cybersecurity Index (GCI) Report Launch event held by ITU on 23rd June, 2021.
- Participated in the 12th ASEAN Network Security Action Council (ANSAC) meeting on 15th September, 2021.
- Attended 1st ACMECS Coordinating Committee Meeting of Pillar 3 on 17th September 2021.
- Attended 7th ASEAN -India Network of Think-Thanks (AINTT) on 14th October, 2021.

- Attended Third ASEAN-India Track 1.5 Dialogue on Cyber Issues held on 20th October, 2021.
- Members of mmCERT participated the Cyber SEA GAME 2020 – ASEAN Cybersecurity Competition by AJCCBC on 26th November, 2021.

6. Future Plans

6.1 Future projects

To protect and support cyber security to Union Ministries and Government Agencies, mmCERT will focus on the following projects in near future:

- Government Secure Service Network
- Penetration Testing Labs
- Digital Forensics Lab
- Cyber Range Project

6.2Future Operation

Being a developing team, mmCERT 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.

Cyber Range Projects will encourage Computer and Technological Universities' Students and other young people who interest in cyber security to get effective Capacity Building and to enhance their skills.

Penetration Testing Labs which intends to check, identify and advise about cyber security vulnerabilities in network security systems and Web servers of Union Ministries and Government Agencies.

And then mmCERT will continue to enhance Public Awareness Activities and promote International and National Co-operations for CERT Activities and operate Research on Log Data Analysis as much as possible.

7. Conclusion

On proceeding of COVID-19 pandemic, Work from Home (WFH) – new normal working culture had been developed. Thus, mmCERT/cc have kept on expanding capacity and enhancing operations to combat emerging cyber threats and to ensure proactive cyber

resilience. mmCERT/cc will also collaborate with international parties to impose the safe and trusted cyber environment.

8. Contact Information

- E-mail: infoteam@mmcert.org.mm, technicalteam@mmcert.org.mm
- Tel: +95 67 3422272 (24 x 7 services)
- Website: https://www.mmcert.org.mm
- https://www.facebook.com/mmcert.team

MNCERT/CC

Mongolia Cyber Emergency Response Team / Coordination Center – Mongolia

1. Highlights of 2021

1.1 Summary of major activities

Due to the global Covid-19 pandemic, all of the activities of MNCERT/CC moved to virtual. MNCERT/CC has successfully organized its annual event and cyber security competition virtually. MNSEC 2021 cyber security virtual event has covered larger scope of participants than the past years.

"Kharuul Zangi 2021" cyber security virtual competition has been held successfully by MNCERT/CC. "Kharuul Zangi U18" cyber security competition among high school senior grade students was skipped in 2021 due to pandemic situation.

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. Totally, 68,431 of threat intelligence and indicator information provided by CIRCL and FIRST had been shared with our constituency in 2021.

One of the key achievements of this year was continuation of "Kharuul Zangi" cyber security competition which was held virtually in two stages. Winners of the contest expressed their impression that the missions were more exciting and challenging than the past years.

Key achievements continued to MNSEC 2021 event which has been organized virtually and made us a full of experience of hosting virtual event which was reached to 472 audiences.

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

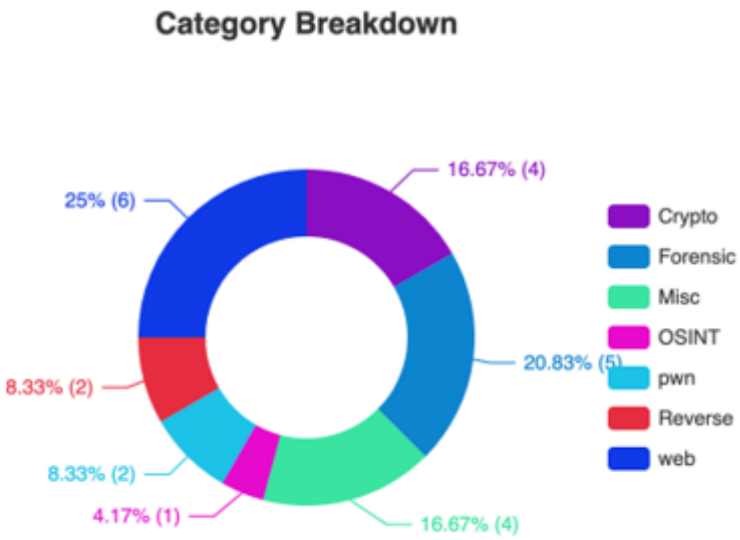
We have organized monthly meetings among IT engineers, cyber security officers and experts of member organizations. MNCERT/CC initiates a discussion and presents specific topics at each meeting such as MSOffice M365 security features, Malware pattern bypassing antivirus protection, Data loss prevention, Security on microservices and container, DevSecOps and Splunk system architecture. After the training, participants discuss information security related issues and problems faced to them. The goal of this meeting and training is to develop a security community within cyber security officers and experts as well as to share their experience.

4.2 Drills & Exercises

4.2.1 "Kharuul Zangi 2021" National Cyber Security Competition

MNCERT/CC organizes a cyber security contest named "Kharuul Zangi" in order to promote the real life challenges and proper knowledge of cyber security to students and cyber security engineers. We have successfully organized "Kharuul Zangi 2021" competition between 31st October to 13th November of 2021, in collaboration with Golomt Bank.

The 1st stage was held virtually while the final stage was held physically. Out of 83 teams of 171 members, 12 teams qualified from the 1st stage. Total of 24 tasks configured by dynamic scoring have been given to be completed at 1st stage. Category breakdown of 1st stage tasks is shown below.



At final stage, 12 teams participated at the contest and the competition was held as attack/defense style CTF by assigning a vulnerable server to each team.The tasks are shown in the following chart.

4.3 Conferences and seminars

4.3.1 MNSEC 2021 Virtual Event

Information technology (IT) benefits the business world by allowing organizations to work more efficiently and maximize productivity. Faster communication, electronic storage and the protection of records are advantages that IT can bring in the enterprise.

Nevertheless there are challenges to overcome in order to continue the development of IT sector. The lack of skilled human resource, legal environment, software and hardware infrastructure for the Information Technology sector in Mongolia and information security is one of them. Therefore, we have organized MNSEC 2021 event on 12th and 13th November of 2021 virtually.

Event consisted of 8 speeches from local and overseas cyber security experts including foreign speakers from Fortinet, Mandiant, DellEMC and YesWeHack and local speakers from MNCERT/CC, InfoSolution and System Center training center. After each speech, Q&A session was continued with the questions collected during the speech. Overseas speakers participated q&a session making online video calls using hopin.to platform.

The speeches covered following topics:

i. AI models in security
ii. Observations of cyber threats in Mongolia in 2021 including cyber espionage, cyber-crime, information operations and hacktivism.
iii. Analysis on new web app attacks
iv. Streamlining your SOC and bridge security gap with SIEM
v. Using polymorphic shellcode for antivirus evasion techniques
vi. How Crowdsourced Security Keep Us Resilient
vii. Supply chain attack: Case study
viii. How to Build Last line of defense against Cyber / Ransom Attack

In order to broadcast the event, we used hopin.to platform which allowed the broadcast only for registered participants. As shown the table below, Hopin.to shows us a report which said that the total of 472 participants registered, 456 of them had turnout and average spent time was 329 minutes. Total comments with questions reached to 284. Please find the mnsec2021 virtual event screenshots from the attachment below.

Main stage of the event

Speaking session

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 2021.

6. Future Plans

6.1 Future Operations

MNCERT/CC planned the following activities in 2022.

Events, conferences and drill to participate are as follows:

- APCERT Annual General Meeting 2022.
- APCERT Drill 2022.

Local activities to organize are as follows:

- MNSEC 2022 Cyber Security Event
- “Kharuul Zangi 2022” Cyber Security Contest among security engineers
- “Kharuul Zangi U18 2022” Cyber Security Contest among high school students
- Local cyber drill among member organizations
- Local training for our constituency.

7. Conclusion

Due to the covid-19 pandemic situation, 2021 was the year of experiencing online activities including meeting, event, competition and other communication. The more our activities go online, the more it requires to keep an eye on cyber security.

We are looking forward the year 2022 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- Singapore

1. Highlights of 2021

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.

Against the backdrop of the rising trend in cyber incidents, in part due to the global COVID-19 pandemic, CSA launched six initiatives aimed at promoting cybersecurity awareness and fostering a more secure cyberspace in 2021:

i. Singapore Cybersecurity Strategy 2021
   Outlines a blueprint for the creation of a safer and more secure cyberspace in Singapore.
ii. Operational Technology Cybersecurity Competency Framework (OTCCF)
   Provides guidance on the competencies to equip professionals in performing their jobs in OT industry sectors.
iii. SG Cyber Safe Cybersecurity Toolkits
   Helps enterprises take greater ownership of their cybersecurity.
iv. SG Cyber Safe Partnership Programme
   Partner with industry to further drive cybersecurity awareness to local businesses, individuals, and the wider community
v. 5th Edition of Singapore Cyber Landscape
   Highlights facts and figures on significant cyber threats and incidents in Singapore for 2020.
vi. Cybersecurity Awareness Campaign – “Better Cyber Safe Than Sorry”
   Increase awareness of cybersecurity and improve adoption of good cybersecurity practices in daily life.

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/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 website (https://www.csa.gov.sg/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, recently revamped with the launch of Cyber Aid. Cyber Aid is a tool that helps users with their cybersecurity incidents, as users are able to get clarity on the cybersecurity issues that they are facing, and advice on how to resolve them.

CSA also maintains a website – GoSafeOnline (https://www.csa.gov.sg/gosafeonline) - to provide individuals and businesses with information on cybersecurity trends and tips to protect themselves.

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 2021, SingCERT received reports of 4,960 incidents, a 5.85% increase from the 4,686 incidents reported to SingCERT in 2020. This resulted in an average of 13.59 incidents per each business day of operation. The table and graph below show the number of incidents that SingCERT handled.

	Jan – Mar	Apr – Jun	Jul – Sep	Oct – Dec	Total
Number of Incident Reports	1,250	1,142	1,200	1,368	**4,960**

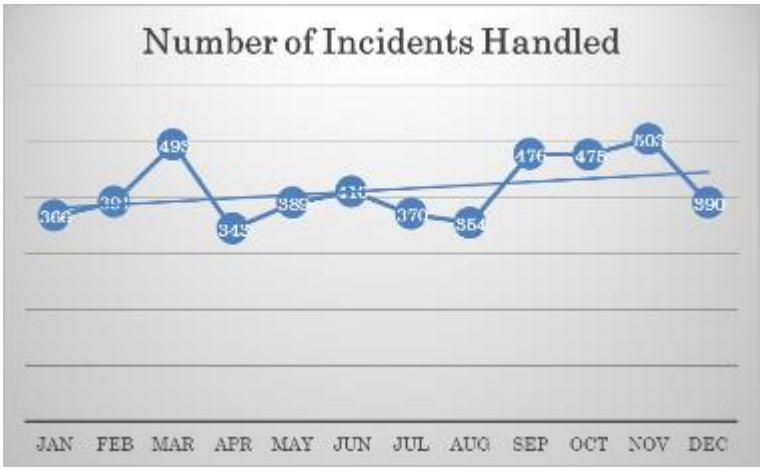


Figure 1. Number of Incidents Reported to SingCERT (2021)

3.3 Abuse statistics

SingCERT receives numerous incident reports on different types of cyber-attacks. As with the previous year, the most common types of cyber incidents handled by SingCERT are phishing, intrusion attempts / attacks, and malware infection.

In 2021, phishing was, once again, the most prevalent cyber threat in Singapore, comprising 60% of the incidents handled over the course of the year, a 42% increase from 2020's figure. 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 to conduct scams.

Cyber Incident Category	# handled in 2021
Phishing	3004
Intrusion Attempt/Attack	823
Malware	614
Others	231
Leaked Information	180
Vulnerability	108

Table 1: Breakup of Cyber Incidents handled (2021)

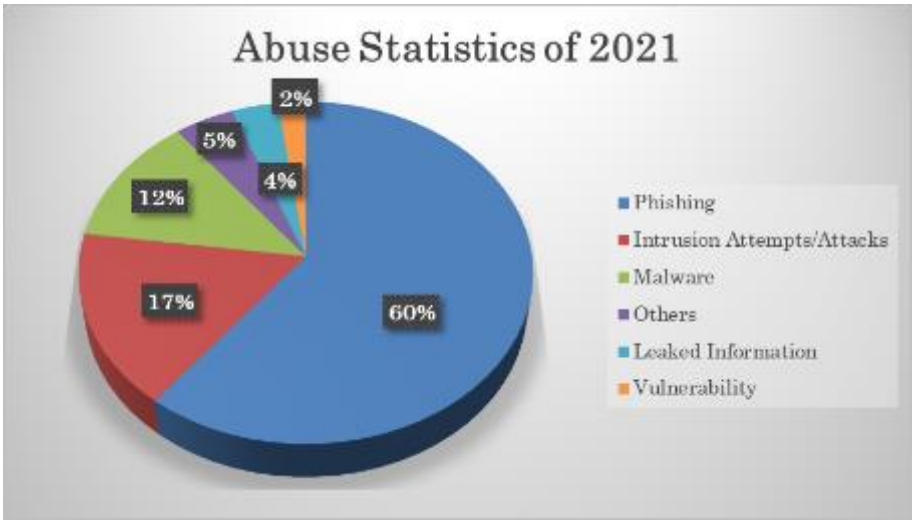


Figure 2. Abuse Statistics (2021)

3.4 Publications

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, vulnerabilities, and the recommended mitigation measures to adopt. SingCERT also publishes a weekly Security Bulletin on Wednesdays, which provides a summary of new vulnerabilities, the impacts and affected operating systems.

In 2021, SingCERT published a total of 81 alerts and advisories, in addition to 52 Security Bulletins, on SingCERT's website https://www.csa.gov.sg/singcert. This represented a slight increase from the 79 alerts and advisories published in 2020. The chart below shows the month-by-month comparison between 2020 and 2021.

	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Total
2020	10	5	8	6	8	11	6	2	5	5	9	4	79
2021	8	6	9	10	5	3	11	6	8	6	5	4	81

Table 2: Month-by-month comparison of Alerts and Advisories Published (2020 to 2021)

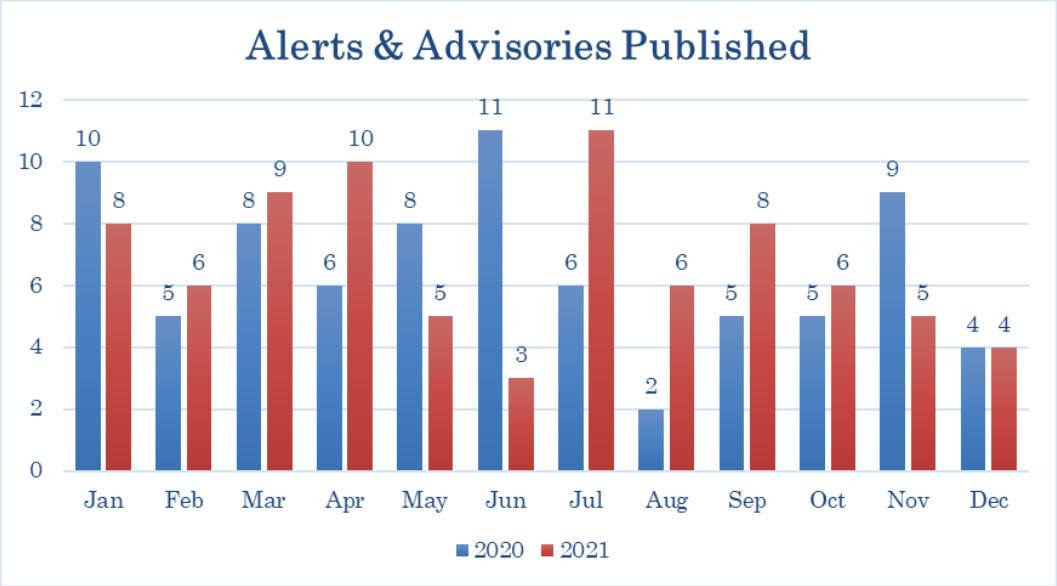


Figure 3. Comparing the Number of Alerts and Advisories Published (2020 to 2021)

Of the 81 alerts and advisories, 71 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 are tabulated below:

Date	Title
13 Jan	January 2021 Monthly Patch Release
15 Jan	High Severity Vulnerability in Cisco Connected Mobile Experiences
20 Jan	Strengthen the Security of Your Organisation's Cloud Services
21 Jan	Multiple Vulnerabilities in Dnsmasq
22 Jan	Critical Vulnerabilities in Oracle WebLogic Server
24 Jan	Probable Vulnerabilities Exploited in some SonicWall Secure Remote Access Products
25 Jan	Critical Vulnerability in SAP Solution Manager
28 Jan	Sudo Heap-based Buffer Overflow Vulnerability
10 Feb	February 2021 Monthly Patch Release
11 Feb	Active Exploitation in Accellion File Transfer Appliance (FTA)
18 Feb	Alert on AppleJeus Cryptocurrency Malware
24 Feb	Multiple High-Risk Vulnerabilities in VMware Products
24 Feb	Joint Cybersecurity Advisory on Exploitation of Accellion File Transfer Appliance
26 Feb	Multiple High Severity Vulnerabilities in SaltStack
3 Mar	Active Exploitation of Vulnerabilities in Microsoft Exchange Server
10 Mar	Patch/Mitigate Microsoft Exchange Product Vulnerabilities

10 Mar	March 2021 Monthly Patch Release
11 Mar	Multiple Critical Vulnerabilities in BIG-IP and BIG-IQ
15 Mar	Multiple Vulnerabilities Found in XStream
16 Mar	Multiple vulnerabilities in Netgear ProSAFE Plus networking switches
19 Mar	Critical Vulnerability in GitLab
26 Mar	Multiple Vulnerabilities in OpenSSL
29 Mar	Active Exploitation of Vulnerability in Apple iPhone, iPad and Watch
3 Apr	Vulnerabilities in D-Link DCS-2530L IP Camera (CVE-2020-25078 and CVE-2020-25079)
5 Apr	Possible Phishing Campaigns Arising from Facebook's Data Leak
6 Apr	Active Exploitation of Fortinet Vulnerabilities
14 Apr	April 2021 Monthly Patch Release
15 Apr	Multiple DNS Vulnerabilities affecting over 100 million devices
15 Apr	Critical Vulnerabilities in SAP Products
19 Apr	Critical Vulnerability in GitLab
21 Apr	Zero-Day Vulnerabilities in SonicWall Email Security
21 Apr	Zero-Day Vulnerability in Pulse Connect Secure (PCS)
24 Apr	Active Exploitation of QNAP Network Attached Storage (NAS) by Ransomware
4 May	Active Exploitation of Vulnerabilities in Apple iOS and iPadOS
6 May	Multiple Vulnerabilities in Exim Mail Transfer Agent
12 May	May 2021 Monthly Patch Release
25 May	Active Exploitation of Zero-Day Vulnerabilities in macOS and tvOS
28 May	Malicious Email Campaign by NOBELIUM
9 Jun	June 2021 Monthly Patch Release
17 Jun	Ransomware: A Growing Cybersecurity Threat to Businesses
25 Jun	Multiple Vulnerabilities in Dell's BIOSConnect and HTTPS Boot
2 Jul	Multiple Vulnerabilities in Windows Print Spooler Service
3 Jul	Kaseya Virtual System Administrator (VSA) Ransomware Attack
6 Jul	Critical Vulnerability in QNAP Network Attached Storage (NAS)
13 Jul	Zero-Day Vulnerability in SolarWinds Serv-U (CVE-2021-35211)
14 Jul	July 2021 Monthly Patch Release
21 Jul	CVE-2021-36934 Local Privilege Escalation Vulnerability in Microsoft Windows
21 Jul	Critical Vulnerability in Fortinet's FortiAnalyzer and FortiManager
22 Jul	Critical Vulnerabilities in Oracle WebLogic Server
23 Jul	Critical Vulnerability in Atlassian's Jira Data Center and Jira Service Management Data Center
26 Jul	PetitPotam NT Lan Manager (NTLM) Relay Attack
27 Jul	Active Exploitation of a Zero-Day Vulnerability in Apple Products

6 Aug	Multiple Vulnerabilities in Pulse Secure Products
11 Aug	August 2021 Monthly Patch Release
11 Aug	Multiple Vulnerabilities in SAP Products
24 Aug	Joint Advisory on ALTDOS
27 Aug	Critical Vulnerability in Atlassian's Confluence Server and Confluence Data Center
31 Aug	Multiple Vulnerabilities Affecting Bluetooth Devices
8 Sep	Zero-day Remote Code Execution Vulnerability in Microsoft MSHTML
9 Sep	Fortinet Fortigate VPN Credentials Leaked Online
10 Sep	Protecting Your Mobile Devices from Mobile Malware
14 Sep	Vulnerabilities in Apple iOS, iPadOS, MacOS and WatchOS
15 Sep	September 2021 Monthly Patch Release
22 Sep	Critical Vulnerability in VMware vCenter Server
23 Sep	Remote Code Execution Vulnerability in NETGEAR Routers
24 Sep	Critical Vulnerability in SonicWall Products
6 Oct	Critical Vulnerability in Apache HTTP Server
8 Oct	Vulnerabilities in Dahua's Cameras
13 Oct	October 2021 Monthly Patch Release
23 Oct	Bug Fix for the GPS Daemon (GPSD) Software
26 Oct	Critical Remote Code Execution Vulnerability in Discourse Platform
28 Oct	Vulnerability in OptinMonster
10 Nov	November 2021 Monthly Patch Release
11 Nov	Critical Vulnerability in WordPress Reset PRO Plugin
18 Nov	Remote Code Execution Vulnerability in NETGEAR Devices
18 Nov	Protect Your Systems and Data from Ransomware Attacks
19 Nov	Vulnerabilities in Drupal 8.9, 9.1, and 9.2
8 Dec	Vulnerability in FortiOS Products
10 Dec	Zero-Day Vulnerability in Apache Java Logging Library Log4j
14 Dec	Immediate Actions to Protect Against Exploitation of the Apache Java Logging Library Log4j Vulnerability
15 Dec	December 2021 Monthly Patch Release

3.4.2 Singapore Cybersecurity Strategy 2021

CSA launched the updated national cybersecurity strategy during the sixth edition of the Singapore International Cyber Week (SICW) held between 4 – 8 October 2021. The Singapore Cybersecurity Strategy 2021 outlines Singapore's plans to take a more proactive stance to address cyber threats, raise the overall level of cybersecurity across the nation, and advance international norms and standards on cybersecurity. The updated strategy also emphasises greater workforce and ecosystem development for businesses and citizens to capitalise on economic opportunities in the cybersecurity sector.

Figure 4. Singapore Cybersecurity Strategy 2021

The Singapore Cybersecurity Strategy 2021 was developed in consultation with Ministries, Government agencies, industry, and local and overseas academia. It comes five years after the launch of the first strategy in 2016 and seeks to address new and emerging cyber threats in the wake of strategic and technological shifts.

More information about the publication, including a downloadable copy, is available via https://www.csa.gov.sg/News/Publications/singapore-cybersecurity-strategy-2021

3.4.3 Operational Technology Cybersecurity Competency Framework (OTCCF)

The OTCCF, jointly developed by CSA and Mercer Singapore, maps out the various OT cybersecurity job roles and the corresponding technical skills and core competencies required. It also captures possible career pathways showing the options for vertical and lateral progression. The objective of this framework is to provide the foundation to attract and develop talent for the emerging OT cybersecurity sector in Singapore.

More information about OTCCF, including a downloadable copy, is available via https://www.csa.gov.sg/News/Publications/operational-technology-cybersecurity-competency-framework-(otccf)

3.4.4 SG Cyber Safe Cybersecurity Toolkits

The SG Cyber Safe Toolkits is tailored by CSA to help large enterprise leaders and Small Medium Enterprise (SME) owners take greater ownership of cybersecurity. The toolkits focus on the business reasons for business leaders and SME owners to invest in cybersecurity, such as rationalising investment in cybersecurity and how fostering a culture of cybersecurity would enable enterprises to reap the benefits of digital transformation. The toolkits simplify cybersecurity and enable business leaders to make informed trade-offs between security, system usability and cost.

More information about SG Cyber Safe Cybersecurity Toolkits is available via https://www.csa.gov.sg/Programmes/sgcybersafe/cybersecurity-toolkits

3.4.5 SG Cyber Safe Partnership Programme

Under the SG Cyber Safe Partnership Programme, CSA will partner the industry to further drive cybersecurity awareness to local businesses, individuals and the wider community. Under this programme, enterprises could develop training content, product and services, or community outreach programmes to raise awareness and encourage the adoption of good cybersecurity practices by businesses and the public.

More information about SG Cyber Safe Partnership Programme is available via https://www.csa.gov.sg/Programmes/sgcybersafe/partnership

3.4.6 Singapore Cyber Landscape

The 5th edition of the Singapore Cyber Landscape publication was released on 8 July 2021. The publication highlights the facts and figures of significant cyber threats and incidents in Singapore for 2020.

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

More information about the publication, including a downloadable copy, is available via https://www.csa.gov.sg/news/publications/singapore-cyber-landscape-2020

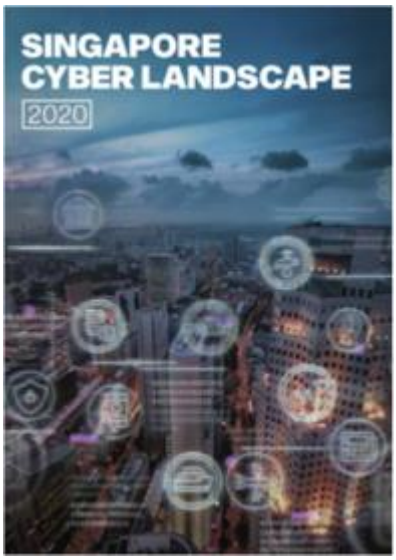


Figure 5. Singapore Cyber Landscape 2020

3.4.7 National Cybersecurity Awareness Campaign

As part of efforts to raise cybersecurity awareness among our constituents, CSA conducts an annual national cybersecurity awareness campaign to educate and raise awareness in the community and provide opportunities for members of the public to pick up cybersecurity tips.

Cybersecurity Awareness Campaign – "Better Cyber Safe Than Sorry"

On 28 June 2021, CSA launched the "Better Cyber Safe Than Sorry" campaign. The campaign builds on the momentum from past years and reinforces the adoption of good cybersecurity habits such as:

i. Using strong passwords;
ii. Enabling Two-Factor Authentication (2FA);
iii. Spotting signs of phishing;
iv. Updating software promptly; and
v. Installing anti-virus software.

To extend the reach of the campaign, CSA used a mix of out-of-home, digital and free-to-air media platforms. Out-of-home media channels included bus stop advertisements, bus wraps and Housing Development Board (HDB) lift stickers. Partnerships were also forged with popular e-commerce platforms such as Carousell and Shopee to amplify the campaign.

More information about the campaign is accessible via https://csa.gov.sg/gosafeonline/Resources/bettercybersafethansorry

3.5 Events organised & hosted

3.5.1 APCERT Training

CSA conducted a training session for the APCERT community at the invitation of APCERT on 3 Aug 2021. The session lasted 120 minutes and was attended by APCERT members. During the session, CSA demonstrated the value of Asset Based Cyber Defense (i.e., zero trust) in protecting corporate networks.

3.6 Drills & Exercises

3.6.1 ASEAN CERT Incident Drill 2021

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 5 October 2021, SingCERT successfully conducted the 16th iteration of ACID. Fifteen CERT teams from the ASEAN Member States (AMS) and ASEAN Dialogue Partners participated in the drill. The theme "Responding to Supply Chain Attacks Against Businesses" was selected in view of several high-profile supply chain attacks

such as the SolarWinds breach in December 2020 and the Kaseya breach in July 2021. Participants were given a series of scenario injects that simulated a supply chain attack originating from a compromised vendor's software which thereafter resulted in a ransomware incident involving the client organisation. After the conclusion of the drill, participating CERTs feedbacked that the exercise was well-designed and provided them with a good understanding of the different techniques employed by threat actors in a supply chain attack.

More information about ACID can be found via https://www.csa.gov.sg/News/News-Articles/csa-hosts-16th-iteration-of-asean-cert-incident-drill

3.7 Conferences and seminars

3.7.1 Singapore International Cyber Week 2021

The Singapore International Cyber Week (SICW) is Singapore's most established annual cybersecurity event, providing a platform for political leaders, policy makers and thought leaders from around the world to discuss, network, strategise and form partnerships in the cyberspace.

The 6th SICW was held from 4 to 8 October 2021, with the theme "Living with COVID-19 – Reimagining digital security risks and opportunities". The event aimed to sustain the momentum of conversations amongst top policy makers, industry leaders 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 (IoTs) and Operational Technology (OT) security, and coordinated cyber capacity-building.

Due to the ongoing COVID-19 pandemic, SICW 2021 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 nearly 2,000 local and international attendees comprising a diverse mix of government officials, industry representatives, academics and cybersecurity professionals. Details about the event can be found at https://www.sicw.sg.

3.7.2 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 participated and benefitted from the following APCERT training topics that were arranged by TWNCERT:

Date	Title	Presented by
23 Feb	Implementing IoT Security Testing	HKCERT
6 Apr	Incident Management and Digital Forensics Investigation	CERT-PH
8 Jun	The OWASP API Security Top 10	TWNCERT
3 Aug	Zero Trust	SingCERT
2 Nov	How to automate advisories – CSAF Overview and Examples	CERT-Bund

4.2 Drills & Exercises

4.2.1 Asia Pacific Computer Response Team (APCERT) Cyber Security Drill 2021

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 2021 with the theme "Supply Chain Attack Through Spear-Phishing – Beware Of Working From Home". The drill evaluated 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 part of the Exercise Controller Team conducting the drill.

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 23-24 June 2021 and the Table Top Exercise held virtually on 28 September 2021.

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 recognised global leader in incident response. FIRST brings together a wide variety of security and incident response teams including product security teams from the government, commercial, and academic sectors. The Forum is also beneficial to both newly established and matured National CSIRTs as it serves as a platform for networking and collaboration. More details about the organisation can be found at https://www.first.org.

As a member of FIRST, SingCERT attended the virtual FIRST Conference from 6-9 June 2021.

4.3.2 APCERT Annual General Meeting (AGM) and Conference 2021

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 29 September 2021 and the conference held on 30 September 2021. Both events were held virtually due to the ongoing COVID19 pandemic.

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 2022:

S/n	Description	Category
1	Singapore Cyber Landscape 2021	Publications
2	7th Singapore International Cyber Week (SICW)	Events Organising & Hosting
3	17th iteration of ASEAN CERT Incident Drill (ACID)	Events Organising & Hosting

Sri Lanka CERT|CC

Sri Lanka Computer Emergency Readiness Team Coordination Centre – Sri Lanka

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 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 1st of July 2006 as a subsidiary of 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 was 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.

The newly appointed CEO commenced his duties from 1st January 2021. At the end of December 2021, the headcount comprised of twenty-seven (27) staff members. This included the Chief Executive Officer, Head of Research, Policy and Projects, Head of Human Resources and Administration, Chief Information Security Engineer, seven Information Security Engineers, Associate Information Security Engineer, Program Manager, Project Manager, four Information Security Analysts, two Associate Information Security Analysts, , Admin & Account Assistant, three Associate SoC

Analysts and, three Trainee-Call Centre officers, there were seven undergraduate interns assisting the operations. Seven 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 SANS GCIH, Microsoft MCSE, EC-Council Certified Ethical Hacker (CEH) and Certified Hacking Forensics Investigator (CHFI),Certified Information Systems Auditor (CISA) by Information Security Audit and Control Association (ISACA), CISCO CCNA, CCSP and CISSP by International Information Systems Security Certification Consortium; (ISC)2.

1.3 Constituency

Sri Lanka CERT|CC's constituency encompasses the non-defense 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 constituents.

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, to provide 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 to 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 to take necessary steps to strengthen its defenses.

Technical Assessments

This service is aimed at reviewing and analysing 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 cyber security related threats to your IT infrastructure.

Vulnerability Assessments

Sri Lanka CERT | CC's vulnerability assessment service helps an organization to 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 an 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 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 organization 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
- Conducting research on cyber threats and issuing alerts on possible threats
- Coordinating special 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 cyber security 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, web site compromise, scams, malicious software issues and ransomware, privacy violations, financial frauds, compromised unique IP's extracted from the information collected by automated systems operated by international organizations. Majority of the reported incidents fall in to the category of social media related incidents and on average more than 1400 cases are reported each month. Among the social media incidents, Facebook incidents were the highest.

The Table 1 depicts the distribution of various types of incidents reported to Sri Lanka CERT in the year 2021. All the incidents reported to Sri Lanka CERT have been resolved satisfactorily.

Incident Type	No of Incidents 2021
DDOS	13
Ransomware	45
Abuse/Hate/Privacy violations	182
Malicious Software issues	10
Phone Hacking	7
Scams	322
Phishing	98
Website Compromise	282
Financial/Email frauds	115
Intellectual property violation	8
Server Compromised	13
Social media	16975
Other	144

Table 1: Number of reported incidents in year 2021

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

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 were performed throughout the year. Continuous monitoring of web applications was conducted in order to identify potential cyber-attacks.

4.5 Training/Education Services

In order to fulfill 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.

4.5.1 Awareness Program and Training Sessions

Sri Lanka CERT conducted the following training and awareness programs:

- General Cyber Security Awareness sessions for:
- Auditor General's department
- Ceylon Electricity Board
- Department of Railways
- University of Peradeniya
- Sri Lanka Institute of Information Technology (SLIIT)
- Airport & Aviation Services
- National Dangerous Drugs Control Board

- Department of Census & Statistics
- Western Province Intelligence Division
- Commission to Investigate Bribery or Corruption
- Western Province Intelligence Division
- Department of Examinations.
- Galle Police Station
- Election Commission
- Department of Public Trustee
- Malasna Devaraja school
- Application security and penetration testing session for SLIIT
- Social Media complains handling training for Crime Investigation Division of Sri Lanka Police
- Open-source intelligence training for CNI staff
- Online session on Social Media for better society
- Awareness session at CyberCon'21- Mozilla Campus Club of SLIIT
- Awareness session on "Why online privacy and security is important" for Sumithrayo NGO
- Session on Parental Controls at Hithawathi
- Session on "How to prepare for internships and industry as an undergraduate" at Sri Lanka Telecom
- Session on "Cyber security Advanced Threats and counter measures"
- Awareness session on "Ransomware / Phishing emails / Cyber frauds and scams/ Cyber Security best practices" for David Pieris staff
- Social Media complaints handling training sessions for law enforcement officers

4.5.2 Awareness through Electronic/Print Media

Sri Lanka CERT|CC provided information for 6 newspaper articles. Furthermore,02 videos for YouTube channels, 02 live radio programs and provided recorded content for 04 TV and 15 radio programs. Sri Lanka CERT|CC live streamed 4 sessions on social media platforms.

4.5.3 Annual Cyber Security Week 2021 (eCSW 2021)

The 14th Annual National Cyber Security Week (CSW) 2021 with the theme of "Striving with Hope" from the 25th to the 29th of October 2021. Taking place virtually owing to

the pandemic, year 2021 eCSW was packed with several keynote events. It was launched with the hacking challenge with 56 teams coming on onboard with 168 participants on the platform.

The 02nd Day of eCSW commenced with a series of workshops, two private workshops on defining the organization's critical information assets in the context of critical national infrastructure by international security experts and Memory forensic analysis by industry experts and 02 public workshops on Digital transformation and cyber resilience by ISC2 Colombo Chapter took place with over 400 participants. These workshops would enable and empower the development of strong cybersecurity policies and strengthen the threat resolution skills of cybersecurity professionals.

From the 27th of October onwards, eCSW flagship event launched its three-day conference featuring over 40 local and international experts sharing their insights on cybersecurity. Over the course of three days, there were in-depth discussions held on the current cybersecurity landscape in a series of panel discussions and presentations with over 1150 participants joining the session.

The 14th Annual eCSW was open to the public and free to attend whilst being streamed on Sri Lanka CERT Facebook page and YouTube Channel. As threats in the digital world evolve and cybersecurity becomes increasing borderless, international exchanges like the Annual Cyber Security Week are more important than ever and the exchange of insights and the upskilling of local cybersecurity professionals is essential if we are to safeguard our infrastructure and aid us collectively ensure our digital world is safer.

4.5.4 Security Alerts

- An Average of 1200 compromised IPs per month were informed to ISPs.
- 26 critical security alerts were published and sent to subscribers.

4.6 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.

4.7 Infrastructure Development & Staff Capacity Building

Staff Capacity Building – International Initiatives

- TLS/SSL live eTutorial (APNIC)
- Network Security & Packet Analysis live eTutorial (APNIC)
- Training on Understanding Exploits I & II (by Cyber4Dev)
- Training on Detecting Compromise (by Cyber4Dev)
- Training on Secure Logins (by Cyber4Dev)
- Training on NCSOC Planning (by Cyber4Dev)

4.8 National Projects

Project Name	Project Status (Simple Description)
National Cyber Security Operations Center for real-time monitoring of cyber security incidents	Publicly hosted websites of ICTA were added to the monitoring center. IT Infrastructure of Sri Lanka Customs was added for monitoring the security threats.
Implementation of National Certification Authority of Sri Lanka to issue certificates for Certificate Service Providers	Initial Certificate Revocation List (CRL) was generated.
Cyber Security Capacity and infrastructure development for building the capacity of staff and improving the infrastructure of Sri Lanka CERT	Purchasing of computer hardware and software were completed.
National Surveys on Information and Cyber Security to understand the cyber security landscape of Sri Lanka	Following Surveys were completed. • Public Officer's Information and Cyber Security Readiness • Critical Information Infrastructure Readiness • The Supply and Demand of Cyber Security Professionals
Development of a Web Portal to increase citizens' awareness on cyber security (www.onlinesafety.lk)	The tri-lingual web portal was launched.
Establishment of Cyber Security Call center to handle cyber security incidents	The Call Center was established
Development of National Vocational Qualification (NVQ) Standard for Information and Cyber Security	NVQ level 5 (National Diploma) on Information and Cyber Security Technology was developed.

Table 2: National Projects

5. Achievements

5.1 Cyber Security Bill

The Cyber Security Bill was drafted, revised, and submitted for review.

5.2 Information and Cyber Security Framework for Government

- Information and Cyber Security Implementation Guide drafted and reviewed.
- Minimum Information Security Standards (MISS) were developed and published.
- Web Application and Hosting Guidelines were drafted

5.3 National Cyber Security Index

National Cyber Security Index (NCSI) is a global index which measures the preparedness of countries to prevent cyber threats and manage cyber incidents. As per the latest ranking of the NCSI, Sri Lanka has advanced to 69th position (year 2021) from the 98th Position (year 2019) out of 160 countries.

5.4 Memberships

Sri Lanka CERT continues to maintain memberships with following professional organizations;

- (ISC)2 Colombo Sri Lanka Chapter the local representative organization of 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

- Participated in three (3) CAMP Operations Committee (OC) meetings
- Leading processes and procedures relevant to membership component in CAMP OC
- Participated in many online and offline discussions on CAMP AGM 2021
- Delivered a presentation for CAMP AGM 2021 on the topic 'Building Awareness on Information Protection During the Pandemic' (pre-recorded video)
- Participated CAMP AGM 2021

- Participated in many online and offline discussions on co-hosting CAMP Regional Forum 2021
- Co-hosted CAMP Regional Forum 2021 for Asia region
- Delivered the Welcome speech on behalf of Sri Lanka CERT during the Regional Forum
- Delivered a presentation during the Regional Forum on the topic 'Cyber Security Landscape of Sri Lanka'

6.2 APCERT

- Participated for five APCERT steering committee meetings
- Continuing with network monitoring project "TSUBAME" with JPCERT|CC
- Organized and conducted meetings with the working group members as the Convener of APCERT working group – Critical Infrastructure Protection
- Participated for APCERT working group teleconferences- Policy and Planning, Membership
- Conducted APCERT online training on "Latest Trends on Keyword Hacks & SEO Spam" for the APCERT members
- Participated for APCERT cyber drill 2021 working group discussions
- Participating APCERT cyber drill 2021
- Participated for APCERT AGM Program Committee Meeting
- Sponsored FIRST and APNIC to obtain the APCERT membership
- APCERT AGM and Conference 2021 (Teleconference)
- Appointed as a Member of the program committee of AGM
- Presented the progress of Critical Infrastructure Protection working group at the AGM
- Contributed to several APCERT working groups
- Proposed to have 2022 APCERT AGM in Sri Lanka

7. Future Plans

7.1 Future Projects to be Implemented

- Establishment of a Sectoral CERT for Education Sector (EduCERT)
- Information and Cyber Security Risk Assessment for Critical Information Infrastructure Providers

8. Conclusion

In the year 2021, there was an increase in the number of information security incidents while new challenges were posed by the pandemic. Despite these, Sri Lanka CERT was able to successfully perform its operations.

An increased focus was given towards securing sensitive government information assets. This included the development of policies, capacity building initiatives, improvements to information infrastructure and monitoring of key public facing resources.

Drafting the Cyber Security Bill, Developing the Information and Cyber Security Policy for government organizations and Monitoring of critical public facing resources are some of the activities carried out during the year as per the National Information and Cyber Security Strategy of Sri Lanka (2019:2023).

We believe Sri Lanka CERT is well positioned to build on its success in the coming year.

TechCERT

TechCERT – Sri Lanka

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 their 15th Anniversary on 01st of September 2021. Originating as a pioneering project of the LK Domain Registry and its 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 them on handling cyber security incidents that requires 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 the 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 over 30 full-time security experts who are active in the security community.

1.1 Establishment

TechCERT was originally formed 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 the 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 (most 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
Dr. 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 (PCI DSS V3), ITIL, AMIE (SL)
Kalana Guniyangoda	Principal Engineer	MSc in Computer & Network Security (Moratuwa), BSc IT (Hons), GCFA, C|HFI
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	Associate 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 Security Engineer	BSc in Computer Systems & Networking, RHCSA, CCSE, CCSA, CCNA – Routing & Switching, CCNA - Security, OCI Architect (Professional)
Dushan Chathuranga	Associate Lead Security Engineer	BSc Eng. (Hons) in Computer Engineering (Peradeniya), OCI Architect (Professional), AMIE(SL)
Dilusha Bandara	Senior Information Security Engineer	BSc in Information & Communication Technology, CCNA, C|HFI, RHCSA, MCSOAA, MCAF
Vishvajith Ihalagama	Senior Information Security Engineer	BSc Eng. (Hons) in Computer Engineering, C|EH, AMIE (SL)
Milinda Wickramasinghe	Senior Information Security Engineer	MSc in Cyber Security (SLIIT), LLM in Intellectual Property & IT (Cardiff), BICT (UCSC), ISO 27001 LA, C|EH, MCSSL
Asanka Dhananjaya	Senior Information Security Engineer	BSc Eng. (Hons) in Computer Engineering, ECSA, AMIE(SL)
Priyankara Bandara	Senior Information Security Engineer	MSc in Information Security (UCSC), BSc Eng. (Hons) in Computer Engineering (Peradeniya), C|EH, CPISI (PCI DSS V3.2), AMIE(SL)
Ayodya Balasuriya	Senior Information Security Analyst	BSc in Information Systems, CPISI (PCI DSS V3.2), LLB(Hons)
Chalana Madusanka	Information Security Engineer	BSc Eng. (Hons) in Computer Engineering, AMIE (SL)
Yenuka Sachintha	Information Security Engineer	BSc in Information Systems, C|EH
Darshana Kithulgoda	Information Security Engineer	Bachelor of Information Technology (UCSC), MSc in Information Technology specialized in Cybersecurity, SSCP
Hirushan Thilanka	Information Security Engineer	BSc in Information Systems
Pubudu Ranasinghe	Information Security Engineer	BSc Information Technology (Cyber Security) SLIIT, RHCSA (RedHat 8.0)
Roshli Perera	Information Security Engineer	BSc (Hons) in Information Technology (Specialized in Cyber Security), C|EH, MCASEA
Nisal Priyanka	Information Security Engineer	BSc (Hons) Informational Technology (Sp. Cyber Security) - SLIIT, PGD in Cyber Security
Janani Kehelwala	Information Security Engineer	MSc in Computer Science (Sp. Security Engineering), BSc (Hons) in Computer Security, C|EH
Akalanka Perera	Information Security Analyst	BSc (Hons) in IT Specialized in Cyber Security
Chamitha Gunawardena	Associate	BSc Hons in Information Technology (Cyber

	Information Security Engineer	Security), CPISI (PCI DSS V3.2)
Dushyantha Pathirathna	Associate Information Security Engineer	BSc (Hons) in Information Technology Specializing in Cyber Security (SLIIT)
Dilshan Umindu	Associate Information Security Engineer	BSc Hons in Information Technology (Cyber Security) - SLIIT, CPISI (PCI DSS V3.2.1)
Lalindra Perera	Associate Information Security Engineer	BSc (Hons) Computer Security
Dinidhu Jayasinghe	Associate Information Security Analyst	BSc IT. (Hons) Specialized in Cyber Security (SLIIT)

Table 1. Details of the Technical Team

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 the mandate of TechCERT, it 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 2021

The 1st of September 2021 marked 15 years of excellent service provided by TechCERT. TechCERT was able to successfully deliver services despite challenges due to the ongoing Covid-19 pandemic. To ensure the health and safety of employees and clients TechCERT started delivering services remotely aligning with health and safety guidelines introduced by the authorities of the country and specially by the customers. This enabled TechCERT to secure major cyber security projects and assignments of leading corporates while competing with the global brands. This milestone was mainly achieved with the support of the skilled and dedicated team members, who worked around the clock, to provide exceptional service to the customers. Below are a few of the major activities that could be successfully completed during year.

2.1 TechCERT Cyber Security Drill

Conducted 03 Cyber Security Drills:

- TechCERT Cyber Security Drill 2021 – Finance Sector
- TechCERT Cyber Security Drill 2021 – Telecommunications Sector
- TechCERT Cyber Security Drill 2021 – Banking Sector

2.2 TechCERT Annual Cyber Security Training and Awareness Session

Conducted 06 training and awareness sessions.

2.3 CPISI PCI DSS Implementation Workshop

Conducted 04 PCI DSS Implementation Workshops.

2.4 Security Assessments & Incident Responses

Conducted more than 6000 Security Assessments on various IT infrastructures and responded to more than 325 Cyber Security incidents.

2.5 International Memberships/Partnerships:

2.5.1 ATM Security Association

TechCERT obtained the membership of the ATM Security association on March 31st, 2021. TechCERT plans to utilize this membership to enhance its expertise on ATM Security and related threats which will in turn benefit TechCERT and its clientele.

2.5.2 SWIFT CSSP 2022

TechCERT successfully re-validated it's listing as a SWIFT CSP assessment provider and SWIFT Cyber Security Service Provider. TechCERT continues its role as a SWIFT CSP External Independent Assessor for the year 2022.

3. Activities and 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:

- Network Surveying and Vulnerability Assessments
- Penetration Tests
- Web Application Security Vulnerability Assessments
- Mobile Application Security Vulnerability Assessments
- Firewall Security Configuration Assessment and Rule Evaluation
- Operational Security Assessments
- Router / Switch Security Configuration Assessment
- Wireless Network Security Assessments
- Cloud Security Assessments
- Network Security Architecture Reviews
- Server Security Configuration Evaluation and Implementation
- Application Security Configuration/Vulnerability Assessments
- PCI Compliance Advisory Services
- Source Code Reviews
- Digital Forensics Investigations
- Vulnerability Research and Verification
- Physical and Environment Security Checks
- Information Security Policy Evaluations
- Preparation of IT Security Policy
- TechCERT - Cyber Security Drills
- Attending to Computer Security Incidents
- TechCERT Security Operations Centre (SOC)
- Information Gathering and Sending Threat Alerts
- SWIFT Compliance Assessments.

Additionally, the security assessments/services listed below were newly introduced within the year 2021.

- Secure Hard Disk Data Wiping
- Continuous Vulnerability Monitoring Services for Customers
- Risk-based Vulnerability Management
- ATM / POS Security Assessment

3.2 Security Assessment

Statistics related to the security assessments conducted by TechCERT during the year 2021 are given below:

Assessment Type	Count
External Vulnerability Assessments	4056
Web-based Security Vulnerability Assessments	1120
Internal Vulnerability Assessments	2944
Firewall Rule Review and Security Assessments	150
Other Assessments (DF investigations, Wireless, Network, etc.)	460

Table 2. Number of Conducted Security Assessments

3.3 Incident Handling

A broad range of entities reported Cyber Security incidents to TechCERT during the year 2021. 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 2021:

Activity Type	Count
Malware infections	103
Server security compromises	90
Social network related incidents	80
Ransomware related incidents	18
Phishing incidents	6
Other incident responses	40

Table 3. Number of Responded Incidents

3.4 Abuse Statistics

Malware infections, Social Network incidents and Server compromise 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 2021 was Malware Infections.

4. Events Organized / Hosted

4.1 Trainings & Awareness Sessions

In 2021, TechCERT conducted its annual Cyber Security Training and Awareness Sessions. They were conducted as a series of webinars due to the pandemic. Given below is a list of the training and awareness sessions conducted:

- Pre-Investigation Important Steps
- Staying Ahead of Payment Card Security Threats
- Securing Your APIs
- Mobile Application Security Awareness Session
- Current Security Concerns and Trends

In addition, TechCERT conducted a number of Incident Response skill development training sessions for its member organizations and other customers. They too were conducted via non-physical means.

Furthermore, TechCERT collaborated with SISA to organize and conduct 4 CPISI PCI DSS Implementation Workshops for TechCERT customers and employees. Listed below are the respective workshops:

- TechCERT - SISA – 320th Advanced Payment Security Implementation e-workshop (CPISI) 2.0 – February 2021
- TechCERT - SISA - 323rd Advanced Payment Security Implementation e-workshop (CPISI) 2.0 – March 2021
- TechCERT - SISA - 330th Advanced Payment Security Implementation e-workshop (CPISI) 2.0 – July 2021
- TechCERT - SISA - 338th CPISI Advanced Payment Security Implementation e-workshop - November 2021

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 2021:

- TechCERT Cyber Security Drill 2021 for Finance Sector organizations (26th of October 2021)

- TechCERT Cyber Security Drill 2021 for Banking Sector organizations (16th of November 2021)
- TechCERT Cyber Security Drill 2021 for Telecommunications Sector organizations (07th of December 2021)

4.3 Conferences and Seminars

TechCERT upholds an active position in the international arena by partaking in various Conferences and/or Seminars. On occasion, TechCERT will provide employees who are experts in certain fields to speak at/coordinate these events. Below is a list of the seminars/conferences conducted by TechCERT in 2021:

- Current Security Concerns and Trends (Nov 10, 2021)
- "The smart phone, cybercrimes related to it and how you can protect yourself." (TV program).

5. Capacity Building

TechCERT greatly values the contribution it's 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 2021.

5.1 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:

- APCERT Training: Stop using Wi-Fi! It's DANGEROUS
- On Demand APCERT Training: Latest Trends on Keyword Hacks & SEO Spam
- ACE Lab Webinar on the Modern Challenges in Data Recovery & Digital Forensics
- TechCERT AWS training

5.2 Drills and Exercises

To fortify its own employee's collective knowledge, TechCERT participated in a number of drills. They are as follows:

- OIC-CERT Cyber Drill 2021
- APCERT Cyber Security Drill 2021

- Oman National CERT Cyber Drill 2021
- AfricaCERT Cyber Drill 2021

6. Future Plans

6.1 Future Projects and Operation

The past year has been a difficult one for many as result of the COVID 19 pandemic, and the coming years will most probably be similar if not worse. Despite this, TechCERT has amassed a number of ambitions it wishes to achieve over the course of the next few years.

- Plan to target more local SMEs to benefit from our information sharing programs.
- Further our work on making the public of the country aware of rising cyber security threats through modes like TV programs.
- Collaborate with more international cyber security organizations on events such as conferences, webinars etc.
- Increase the scale of our annual Cyber Security Drill, to accommodate more customers and offer robust experiences.
- Leverage resources available to enhance the skill set and talents of the TechCERT team members.
- Introducing risk-based vulnerability management programs to Sri Lankan organizations.

7. Conclusion

Similar to the year 2020, this year was marred with challenges brought on by the pandemic. TechCERT operated entirely remotely with employees being required to leave their homes only at the most required instances. In spite of this, TechCERT succeeded at improving its core capabilities and fulfilling its duties as a CERT. This year marked the further expansion of its workforce. By bringing young and talented minds into the fold, TechCERT hopes to explore more and broaden its scope.

In 2021, TechCERT responded promptly and effectively to constantly evolving cyber threats in Sri Lanka. Many which were malware infections and compromised servers. TechCERT remains confident of its ability and readiness in assisting its members/customers during information security emergencies. TechCERT aims to develop the talents and strengths of its workforce, by means of external training and

workshops. Another goal is to acquire advanced tools and equipment that will better complement the skill sets of the employees. Through global collaboration, a talented workforce and consistent quality of service, customers of TechCERT are assured nothing but excellence.

ThaiCERT

Thailand Computer Emergency Response Team – Thailand

1. Highlights of 2021

1.1 Summary of major activities

Compared to 2020, ThaiCERT received less reports on incidents related to the Covid-19 relief program since the situation has improved. In 2021, one of the major reported incidents was the report of log4j vulnerabilities, which affect various products globally. ThaiCERT received and verified report of systems in Thailand affected by log4j and informed related parties to resolve the issues. Reported data breaches continued to have impact on major organizations in Thailand. In some cases, ThaiCERT works closely with related organizations such as the National Cyber Security Committee (NCSC) to help respond to the incident.

2. About CSIRT

2.1 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.

2.2 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.

3. Activities & Operations

3.1 Incident handling reports

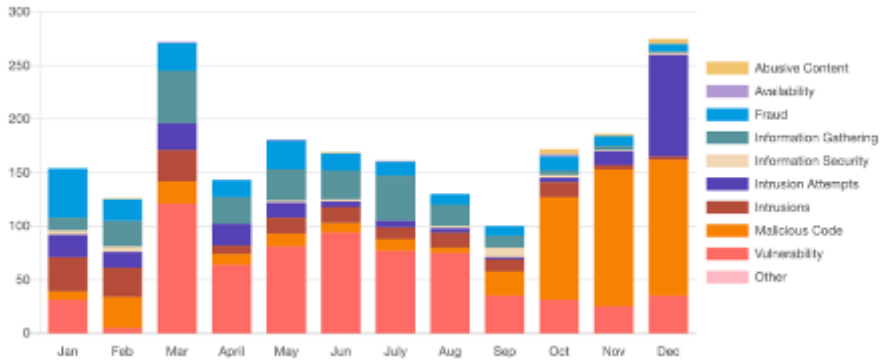


Figure 1. The number of reported incidents in 2021

Via triage, ThaiCERT handled a total of 2,069 reported incident cases (tickets) in 2021, which is a 8% decrease from those of 2019 (2,250 cases). The received reports per month are around 172 cases.

According to the reported incidents in 2021, classified by the eCSIRT incident classification, Vulnerabilities dominated with 33% followed by Malicious Code at 23%, where all cases were mostly botnet or hacked websites that redirect victims to other malicious website, and Information Gathering at 12%. All such information was handled and notified to the relevant parties through e-mail channels.

4. International Collaboration

4.1 Capacity building

4.1.1 Training

- 2021 APISC Security Training Course
- AJCCBC Cybersecurity Capacity Building Workshop 2021

4.1.2 Drills & exercises

- APCERT Annual Drill 2021
- ASEAN-Japan Table Top Exercise 2021
- ASEAN Cyber Incident Drill (ACID) 2021

4.1.3 Seminars & presentations

- PaCSON Remote Session
- Cyber Threat Intelligence Network of KR
- APT Web Dialogue on COVID-19 and Cybersecurity
- APCERT AGM & Conference 2021
- TWCERT 2021
- CyberAttack Bangkok 2021

4.2 Other international activities

- Cyber SEA Game 2021
- 2021 FIRST CTI SIG Summit
- 20th Annual AusCERT Information Security Conference
- 16th NatCSIRT Annual Conference
- 33rd Annual FIRST Conference
- 2021 Global Conference on CNCERT International Partnership
- NCSC ONE Conference 2021
- Global Forum on Cyber Expertise (GFCE) Southeast Asia Regional Meeting

5. Future Plans

- Cyber SEA Game 2022 Event
- AJCCBC Cybersecurity Capacity Building Workshop 2022

TWCERT/CC

Taiwan Computer Emergency Response Team / Coordination Center – Chinese Taipei

1. Highlights of 2021

1.1 Summary of Major Activities

In 2021, Taiwan Computer Emergency Response Team / Coordination Center (TWCERT/CC) has shared nearly 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 2021 including 12 cybersecurity intelligence newsletters and 343 domestic and global cybersecurity news articles. In addition, 57 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 167 CVE IDs in 2021. 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 both CWE and CVSS3.1 by MITRE in May and June of 2021.

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 2021 Conference of Taiwan Cyber Security Notification and Response, working group meetings and security trainings for Taiwan CERT/CSIRT Alliance, and 5 cybersecurity conferences for Taiwan's small-medium enterprises (SMEs). 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 million cyber events and IoCs in 16 categories, where outbound attack, system intrusion and botnet were the three most common types of cybersecurity attacks in 2021.
- TWCERT/CC has Issued 12 monthly e-newsletters, 343 domestic and global cyber security news articles. In addition, 57 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 167 CVE IDs in 2021.
- TWCERT/CC has participated in 5 international and 13 domestic cybersecurity conferences and seminars, hosted the 2021 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 2021, 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.
- Established the Anti-Ransom site containing ransomware preventive measures and response as well as post-incident recovery information to assist individuals and

enterprises respond to ransomware attacks.

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 2021, TWCERT/CC shared about 1 million cyber events and IoCs. The monthly statistics and the types of cyber intelligence are shown respectively in Figure 1 and Figure 2.

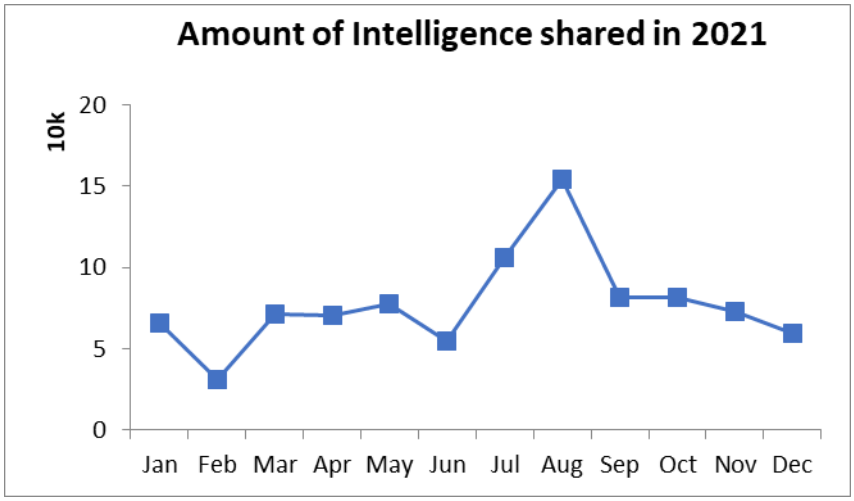


Figure1. Cyber intelligence shared by TWCERT/CC in 2021

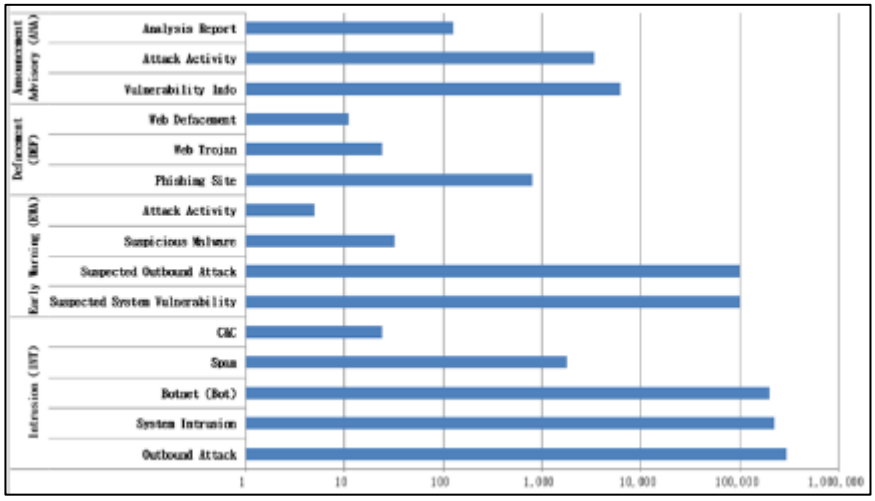


Figure2. Types of cyber intelligence shared by TWCERT/CC in 2021

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, 343 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 2021, 167 vulnerabilities were assigned. The list of assigned CVE IDs as shown in Table 1.

Category	Amount	CVE ID
IOT devices	54	CVE-2021-30165、CVE-2021-30166、CVE-2021-30167、CVE-2021-30168、CVE-2021-30169、CVE-2021-32506、CVE-2021-32507、CVE-2021-32508、CVE-2021-32509、CVE-2021-32510、CVE-2021-32511、CVE-2021-32512、CVE-2021-32513、CVE-2021-32514、CVE-2021-32515、CVE-2021-32516、CVE-2021-32517、CVE-2021-32518、CVE-2021-32519、CVE-2021-32520、CVE-2021-32521、CVE-2021-32522、CVE-2021-32523、CVE-2021-32524、CVE-2021-32525、CVE-2021-32526、CVE-2021-32527、CVE-2021-32528、CVE-2021-32529、CVE-2021-32530、CVE-2021-32531、CVE-2021-32532、CVE-2021-32533、CVE-2021-32534、CVE-2021-32535、CVE-2021-37216、CVE-2021-32536、CVE-2021-32537、CVE-2021-37911、CVE-2021-41290、CVE-2021-41291、CVE-2021-41292、CVE-2021-41293、CVE-2021-41294、CVE-2021-41295、CVE-2021-41296、CVE-2021-41297、CVE-2021-41298、CVE-2021-41299、CVE-2021-41300、CVE-2021-41301、CVE-2021-41302、CVE-2021-37910、CVE-2021-41289
Software and Service	78	CVE-2021-22850、CVE-2021-22851、CVE-2021-22852、CVE-2021-22847、CVE-2021-22849、CVE-2021-22853、CVE-2021-22854、CVE-2021-22855、CVE-2021-22856、CVE-2021-22857、CVE-2021-22858、CVE-2021-22859、CVE-2021-22860、CVE-2021-22848、CVE-2021-28171、CVE-2021-28172、

		CVE-2021-28173、CVE-2021-28174、CVE-2021-30170、CVE-2021-30171、CVE-2021-30172、CVE-2021-30173、CVE-2021-30174、CVE-2021-32544、CVE-2021-32539、CVE-2021-32540、CVE-2021-32541、CVE-2021-32542、CVE-2021-32543、CVE-2021-32538、CVE-2021-35961、CVE-2021-35962、CVE-2021-35963、CVE-2021-35964、CVE-2021-35965、CVE-2021-35966、CVE-2021-35967、CVE-2021-35968、CVE-2021-37211、CVE-2021-37212、CVE-2021-37213、CVE-2021-37214、CVE-2021-37215、CVE-2021-37909、CVE-2021-37912、CVE-2021-37913、CVE-2021-41563、CVE-2021-41564、CVE-2021-41565、CVE-2021-41566、CVE-2021-41567、CVE-2021-41568、CVE-2021-41974、CVE-2021-41975、CVE-2021-41976、CVE-2021-42329、CVE-2021-42330、CVE-2021-42331、CVE-2021-42332、CVE-2021-42333、CVE-2021-42334、CVE-2021-42335、CVE-2021-42336、CVE-2021-42337、CVE-2021-42338、CVE-2021-42838、CVE-2021-42839、CVE-2021-43358、CVE-2021-43359、CVE-2021-43360、CVE-2021-44159、CVE-2021-44160、CVE-2021-44161、CVE-2021-44162、CVE-2021-44163、CVE-2021-44164、CVE-2021-45916、CVE-2021-45917
Server	35	CVE-2021-28175、CVE-2021-28176、CVE-2021-28177、CVE-2021-28178、CVE-2021-28179、CVE-2021-28180、CVE-2021-28181、CVE-2021-28182、CVE-2021-28183、CVE-2021-28184、CVE-2021-28185、CVE-2021-28186、CVE-2021-28187、CVE-2021-28188、CVE-2021-28189、CVE-2021-28190、CVE-2021-28191、CVE-2021-28192、CVE-2021-28193、CVE-2021-28194、CVE-2021-28195、CVE-2021-28196、CVE-2021-28197、CVE-2021-28198、CVE-2021-28199、CVE-2021-28200、CVE-2021-28201、CVE-2021-28202、CVE-2021-28203、CVE-2021-28204、CVE-2021-28205、CVE-2021-28206、CVE-2021-28207、CVE-2021-28208、CVE-2021-28209

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 2021 IPv6 Cybersecurity Seminar (figure 3), co-organizing CyberSec 2021 and HITCON Conference 2021, participated in Cryptology and Information Security Association (CISC) 2021 and HICON Pacific 2021. TWCERT/CC has also presented at seven domestic cyber forums for SMEs regarding cyber defense, case study and promoting cyber awareness.

Figure 3. 2021 TWNIC IPV6 Cybersecurity Seminar

TWCERT/CC has organized a Taiwan CERT/CSIRT Alliance Conference and two cybersecurity trainings for private enterprises in Taiwan (figure 4), where topics such as emerging cyber threats, vulnerability report, incident response were explored.

Figure 4. Cybersecurity Training

4.2 International Cybersecurity Events

TWCERT/CC has been actively engaged with its international partners and cyber security events. In 2021, TWCERT/CC participated in eight international conventions as shown in Table 2. TWCERT/CC will continue to interact with its global partners and strengthening its capability as a CERT organization.

Date	Conference/Seminar
2021/3/2~4	APEC TELWG and SPSG
2021/3/3	APNIC 51-APRICOT 2021
2021/6/6~9	FIRST 2021 Annual Conference
2021/5/24~25	NatCSIRT 2021 Annual Conference
2021/9/13~16	APNIC 52

Table 2. international conferences and seminars participated in 2021

TWCERTCC has organized the TWCERT 2021 Annual Conference (figure 5). The theme was 'Taking Joint Defense System for Cyber security across Public and Private Sectors', 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. A broad cybersecurity topics are discussed, such as supply chain management under 5G era, joint defense across public and private sectors, and cybersecurity application in high-tech industry. Several honorable guests were invited

to share their expertise and experience from National Communications Commission, Department of Cybersecurity of Executive Yuan, American Institute in Taiwan, Cycraft, Hong Hai Research Institute, ASUS, QNAP and ASE Technology.

The Panel Discussion regarding 'joint defense system of cyber security across public and private sector' was hosted by Kenny Huang, the CEO of TWNIC. Several international experts from JPCERT/CC, CERT-In, ThaiCERT were invited to share their experiences in coordinating cyber joint-defense in their constituency.

Figure 5. TWCERT 2021 Annual Conference

TWCERT/CC has participated in APCERT Cyber Drill 2021. The theme was 'Supply Chain Attack Through Spear-Phishing – Beware of Working from Home', where TWCERT/CC handled a case of supply chain attack triggered by spear phishing. 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 19 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 51 and presented 'A Case Study of ProxyLogon Exploit in Taiwan' at APNIC 52 (figure 6). ProxyLogon was considered one of the most severe Microsoft Exchange vulnerabilities in recent years and has been exploited by threat actors in numerous hacking incidents in 2021. ProxyLogon affected more than 400,000 servers across 224 countries. At APNIC 52, TWCERT/CC shared its experience on incident response and the attack chain that was used in a recent incident that happened in Taiwan.

Figure 6. TWCERT/CC's presentation on ProxyLogon at APNIC 52

5. Future Work

TWCERT/CC is dedicated to optimizing its services and raise awareness of cybersecurity with the following items:

i. Disseminate vulnerability information and cybersecurity incidents, monthly cybersecurity e-newsletter, and annual cybersecurity report.
ii. Notify emerging cyber threats, policies to its constituency regularly.
iii. Collect, analyze and release the latest information regarding cybersecurity conferences, seminars, and trainings.
iv. 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 – Chinese Taipei

1. Highlights of 2021

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 2021, TWNCERT issued more than three thousand notice 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 2021 (CODE 2021), including Red vs Blue confrontation live action exercise in energy-field.

Besides, TWNCERT launched a series of cyber security competitions in 2021 to nurture cyber security talents and promote cyber security awareness. There are more than thirty thousand students, and the general public participated.

1.2 Achievements & milestones

TWNCERT developed three online courses to improve cyber security protection and awareness among government agencies in 2021. More than twenty thousand government staff attended the online and onsite training and took course exams.

As the convener of APCERT Training Working Group, TWNCERT convened seven online training sessions. A total of twenty-three APCERT member teams had 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, 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 Department of Cyber Security of the Executive Yuan, 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 under cyber attacks or facing threat situations.
- 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 sector.
- 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 2021, TWNCERT received nearly nine hundred reports on cyber security incidents from Taiwan government agencies. We also received about one thousand and two hundred cyber security incident reports from international CERTs/CSIRTS and cyber security organizations.

Moreover, more than one million 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

3.3.1 Government agencies

In 2021, TWNCERT received reports on cyber security incidents from government agencies. About 64% of the reported security incidents are in the category of Intrusion, as shown in Figure 1.

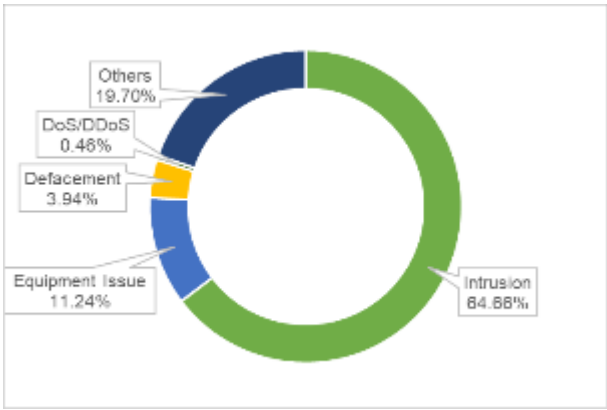


Figure 1. Security Incidents from Government Agencies

3.3.2 International incident report

In 2021, TWNCERT received about one thousand and two hundred cyber security incident reports from international CERTs/CSIRTS and cyber security organizations. The incident reports were categorized as shown in Figure 2. About 67% of the incident reports were Malware Infected System, followed by Attack, Spam, and Phishing.

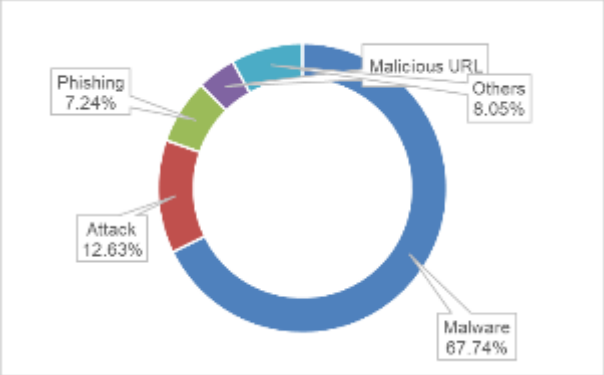


Figure 2. Category of International Incident Reports

3.3.3 N-ISAC information sharing

N-ISAC members shared more than one million cyber security incidents and critical information. The Early Warning is the most shared cyber security information in 2021, as shown in Figure 3.

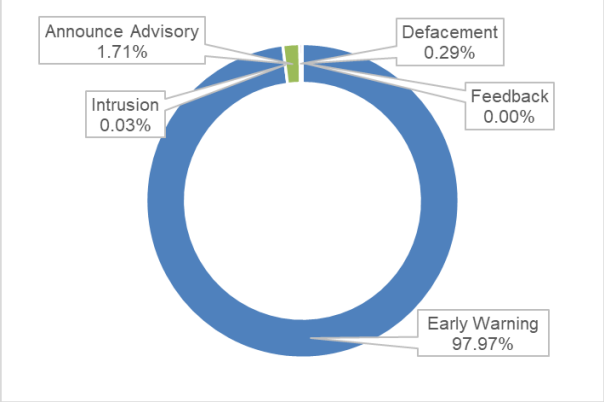


Figure 3. Distribution of N-ISAC Information Sharing

3.4 Publications

3.4.1 Website publication

TWNCERT collects and publishes cyber security advisories, news, and guidelines on the website. In 2021, TWNCERT published more than one hundred articles, including cyber security news and security alerts.

3.4.2 Advisory and Alert

In 2021, TWNCERT issued more than three thousand advisories to government agencies. The categories were distributed as in Figure 4.

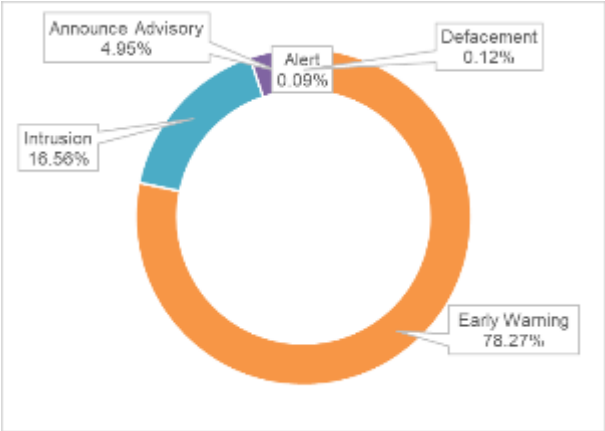


Figure 4. Distribution of Government Notice Advisories

3.4.3 International incident report

In 2021, TWNCERT shared more than seventeen thousand incident reports to other national CERTs/CSIRTS, as shown in Figure 5.

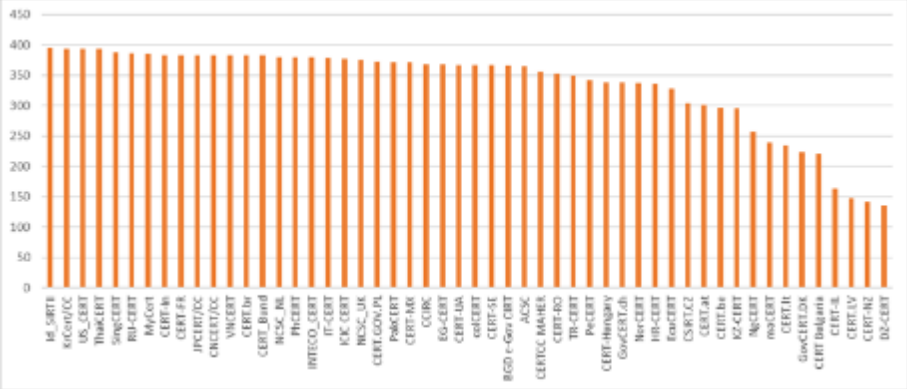


Figure 5. International Incident Report Sharing

4. Events organized/hosted

4.1 Training

TWNCERT developed three online courses to improve cyber security protection and awareness among government agencies in 2021. About twenty thousand government staff attended the online and onsite training and took course exams.

4.2 Drills & exercises

4.2.1 Drill

To strengthen the preparedness against cybercrimes, technology failures, and Critical Information Infrastructure (CII) incidents, TWNCERT conducted Cyber Offensive and Defensive Exercise 2021 (CODE 2021). There are twenty countries, and thirty-one public and private organizations attended the event in CODE 2021. CODE 2021 included Red vs Blue confrontation live action exercise in the energy CI sector, as shown in Figure 6. Beside that, TWNCERT also conducted a national cyber security exercise including social engineering exercise, information system penetration exercise to help promote the preparedness of Taiwan government agencies.

Figure 6. CODE 2021

4.2.2 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 2021. More than twenty thousand students and the general public participated.

Figure 7. Cyber Security Competition

4.3 Conferences and seminars

In 2021, TWNCERT held N-ISAC meetings in July and December. We discussed the recent cyber security issues and improved information sharing efficiency and effectiveness through the meetings. During the N-ISAC annual meeting in December, the experts from the public and private sector 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 covered supply chain management, zero-trust security, and information sharing. Members learn how to process and share cyber security information 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 seven online training sessions in 2021.

Date	Topic	Presenter
2021/2/23	Implementing IoT Security Testing	HKCERT
2021/4/6	ncident Management and Digital Forensics Investigation	CERT-PH
2021/6/8	The OWASP API Security Top 10	TWNCERT
2021/7/13	Training for APCERT Operational Member on the APCERT DRILL	AusCERT
2021/6/8	Zero Trust (Sun Tze's way)	SingCERT/CSA
2021/11/2	How to automate advisories – CSAF Overview and Examples	CERT-Bund
2021/12/7	Stop using Wi-Fi! It's DANGEROUS	IDSIRTII

Figure 10. APCERT Training Programs

5.2.2 Drills & exercises

TWNCERT participated in APCERT Drill under the theme "Supply Chain Attack Through Spear-Phishing - Beware of Working from Home" on August 25th and solved a set of drill scenarios within the given time limit.

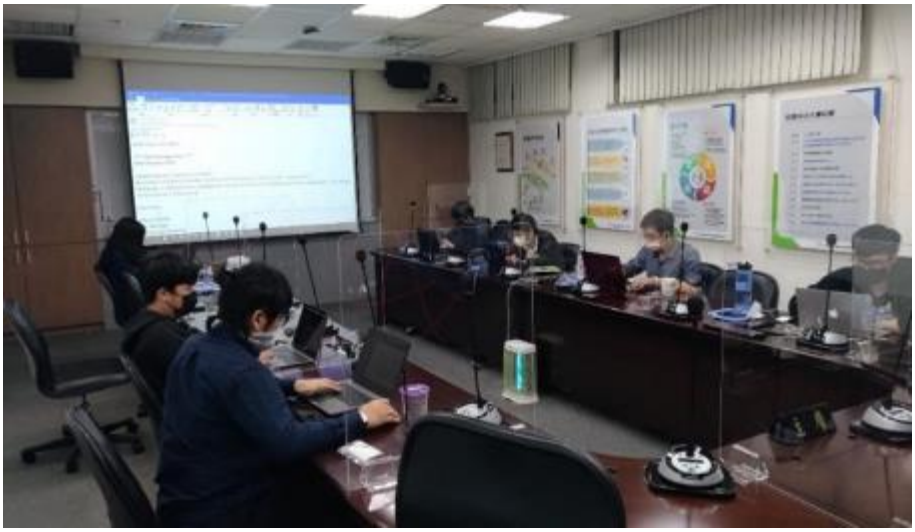


Figure 11. APCERT Drill 2021

5.2.3 Seminars & presentations

Below is the list of international events that TWNCERT participated in.

- APEC TEL Conference (online)
- FIRST 2021AGM (online)
- APCERT AGM 2021(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 the 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 partnership and introduce quality services
- Defense-in-depth deployment and toward 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 cyber security

Within the region, TWNCERT dedicates 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 2021

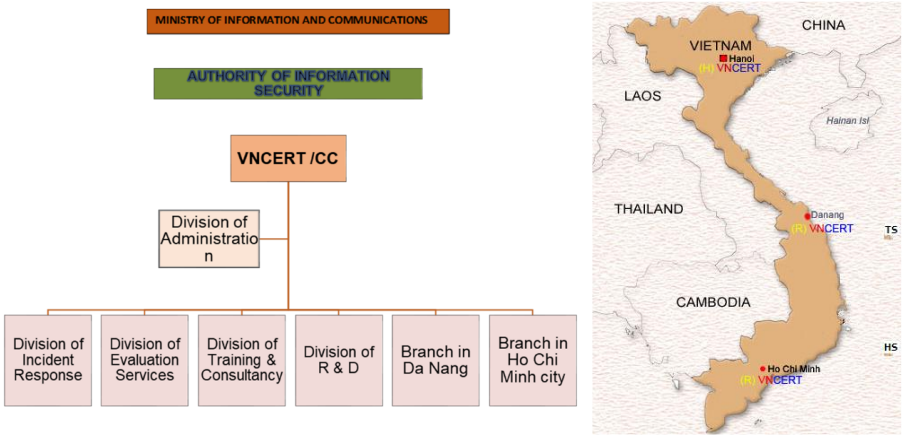
In 2021, VNCERT/CC has focused on anti-spam, assess information security products. Besides, VNCERT/CC Vietnam has begun implementing a program for children protection in the cyber environment in the period of 2021-2025.

- Developed Basic Technical Requirements for WAF, SIEM, TIP, Network IDPS, VPN, SOAR products.
- Inspect and evaluate information security for domestic products.
- Developed a portal and Platform to look up and report spam messages and calls.
- Worked as a permanent member of the executive board of the Viet Nam's Network for Child Online Protection (VN-COP), established 2021 with 24 members.
- Developed the Child Online Protection Portal Site - https://vn-cop.vn/ with purpose to: share information awareness on Child Online Protection; receive the reports about child abuse cases in the Internet environment, and enhance quality, efficient connectivity of all the resources in society in Viet Nam.

2. About CSIRT

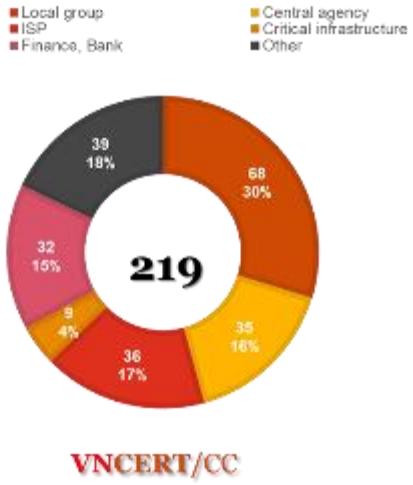
2.1 Introduction

- 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 of 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 in Hanoi, Da Nang branch for the middle region, and Ho Chi Minh city branch for the southern region.



The organizational structure of VNCERT/CC

- VNCERT/CC is the leader and the coordination center of the national CSIRTs Network (Vietnam CSIRTs Network) that consists of 219 members with more than 4,000 staffs from members.
- VNCERT/CC is a full member of the Forum of Incident Response and Security Teams (FIRST).



2.2 Contact Information

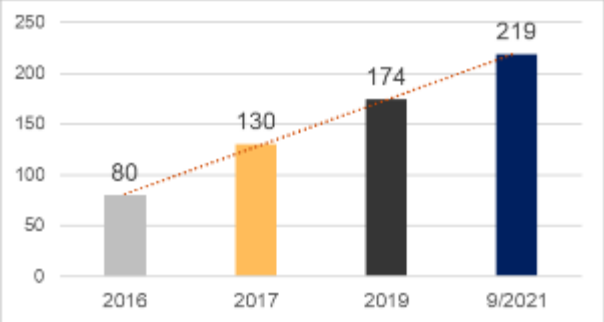
- Website: http://www.vncert.gov.vn/
- E-mail: international@vncert.vn
- Tel: +84-24-36404421 (08:00-17:00) Working hour
- Incident report: ir@vncert.vn / ucsc@vncert.vn
- (+ 84-868100317) 24 x 7

3. Activities & Operations

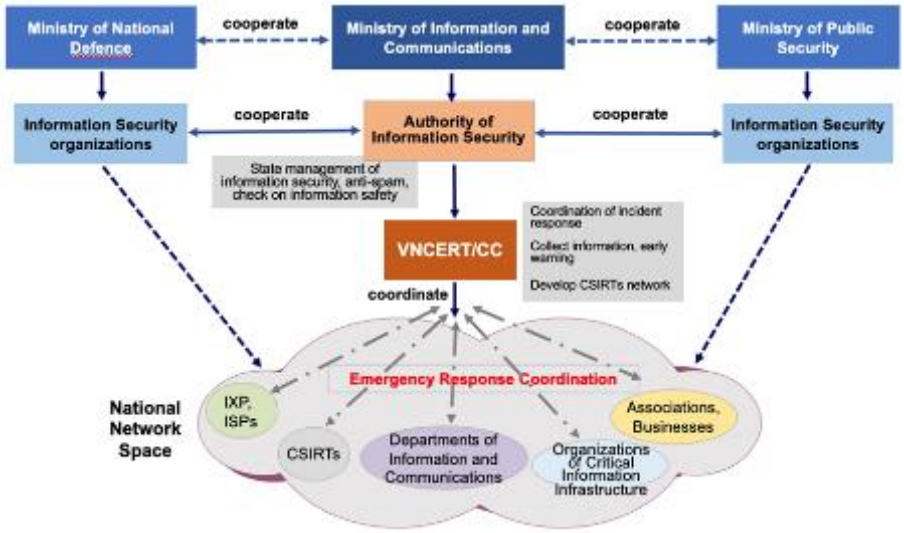
3.1 Scope and definitions

VNCERT/CC has the roles of:

- Operating activities of Vietnam CSIRTs (VNCSIRTs) Network with 219 members (including incident response center, information security center or information technology centers of Ministries, ministerial agencies, governmental agencies, telecommunication enterprise, Internet service providers, Finance Organizations, Banks, the organizations in charge of information systems of national importance).

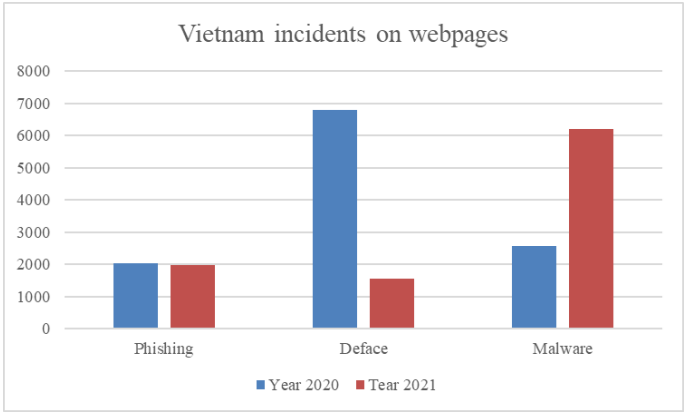


- Receiving reports of security incidents and warning
- Coordinating national computer incident response activities.
- Promoting to build CERTs/CSIRTs in Vietnam's organizations, enterprises, and agencies.
- Being the point of contact of Vietnam with the other CERTs in the world.
- Implementing and deploying the anti-spam activities.
- Receiving reports of incidents, harmful content, child abuse in the cyber as a being an operation member of VN-COP (Viet Nam's Network for Child Online Protection) established 2021 with 24 members.



3.2 Incident handling reports

In 2021, Vietnam has 9,729 incidents on webpages (1,980 phishings, 1,549 defaces, 6,200 malwares), 4,445,547 IP addresses infected by bots from botnets, and 7,718 incidents on information systems.



3.3 New services

- Platform to receive feedback and coordinate the handling of spam messages, spam calls.
- Platform to receive feedback on child protection support online.
- Platform to support information security inspection and assessment.

4. Events organized/hosted

4.1 Training

Participated and/or organized:

- Over 50 times of VNCERT/CC's staffs joined skills training courses as CEH, CompTIA+ Security, OSCP, OSWE, CHFI, ECSS; Malware Analysis, ISACA CISM / CISA, CISSP, …
- More than 5 training courses for technicians in provinces
- More than 12 training courses for members of VNCSIRTs Network.

4.2 Drills & exercises:

Participated:

- ASEAN - JAPAN Cyber Remote Exercise, June 2021.
- APCERT Incident Handling Drill 2021, August 2021.
- ASEAN CERT Incident Drill (ACID) 2021, Oct 2021.

Organized:

- 2 drills for members of the Nation Cybersecurity Emergency Response Team.
- 1 drill of real attack to information system for the transportation sector

4.3 Conferences and seminars

VNCERT/CC cooperated with other organizations to organize annual events such as "Security World 2021", "National Information Security Day 2021" and organized other conferences for CSIRTs Network members and information security departments from all over the country.

5. International Collaboration

5.1 International partnerships and agreements

- Completed a connection with India's national CERT organization and is discussing the signing of a Memorandum of Understanding.
- Contributed ideas to the plan to establish ASEAN-CERT.
- Exchanged information, connect with CNCERT to launch the China-ASEAN Network Security On-Site Training.

5.2 Capacity building

5.2.1 Training

Attended online courses of foreign organizations, international organizations such as distance training conducted by JICA, Kaspersky, Korean companies, AJCCBC Cyber Security Training, GCCD Cybersecurity Webinar.

5.2.2 Drills & exercises

Attended 3 drills of APCERT 2021, ASEAN-Japan, and ACID.

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

Contact and discuss with international organizations and businesses for security protection, mitigation, resilience, etc.

6. Future Plans

6.1 Future projects

Security Evaluation Lab.

6.2 Future Operation

- Develop technical human resources of VNCERT/CC;
- Continue to deploy the project of development VNCSIRTs Network according to improve the cybersecurity service quality and quantity for community
- Develop cooperation with other CERTs in the world

- Project of Children Protection on Cyberspace.
- Improve Anti-spam.
- Continue to collaborate 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 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.

IV. Activity Reports from APCERT Partners

AfricaCERT

The African forum of Computer Incident Response Teams

1. International Collaboration

1.1 Capacity building

1.1.1 Drills & exercises

1st African Cybersecurity Drill

The AfricaCERT organised the 1st Africa Cybersecurity Drill for the National CERTs/CSIRTs/CIRTs, IXPs & RENs in Africa from 30 June to 1 July 2021. The member countries of the OIC-CERT OIC and APCERT Member Teams were also invited to participate in the cyber drill exercise.

The primary purpose of the online cybersecurity drill was to enhance the communication and incident response capabilities of the participating teams and to ensure a continued collective effort in mitigating cyber threats among the region's CERTs/CSIRTs.

A steering committee comprising the National CSIRT of Benin Republic (BJCSIRT), the national Computer Emergency Response Team for Egypt (EG-CERT), the National Kenya Computer Incident Response Team Coordination Center (KE-CIRT/CC), the Computer Emergency Response Team of Mauritius (CERT-MU), the Tunisian Computer Emergency Response Team (tunCERT) and AfricaCERT organized the event. CERT-MU led the drill's organisation and chaired the steering committee meetings.

The fully automated drill comprises various scenarios such as Phishing, Website Defacement, Malware Analysis, and Ransomware. Thirty-two (32) teams from twenty-four (24) countries across Africa, the Arab region, and the Asia Pacific region participated in the two-day drill exercise.
The conducted simulations were beneficial to the participants as they could get acquainted with the different types of cyber-attacks. The exercise provided participating team with the technical know-how of responding to such attacks if they occur.

Mr. Chris Gibson, the Executive Director of the Forum of Incident Response and Security Teams, delivered a keynote reminding participants of the importance of exercises, stressing lessons learned such as “working and exercising together builds confidence and trust”. External observers from the UK Home Office and the Cyber4Dev team of Estonia attended the cyber drill.

From:
Dr. Kaleem Ahmed USMANI
Head, CERT Mauritius

FINCSIRT

Financial Sector Computer Security Incident Response Team – Sri Lanka

1. About the Organization

1.1 Introduction

FinCSIRT is a financial sector security specialized organization in Sri Lanka, and a non-profit cooperation founded by Central Bank & Financial sector of Sri Lanka.

Through information sharing of threat intelligences via advisory, informational, vulnerability and FSOC alerts, and promptly attending to discovered or incidents which were notified by the members, FinCSIRT offers reactive responses while working together with its 40+ member base, regulator, and the related stakeholders to implement proactive controls, which ultimately sums to the stability of the Sri Lankan Financial Sector.

1.2 Establishment and Constituency

Sri Lanka Financial Sector Computer Security Incident Response Team (FinCSIRT), formally known as "BankCSIRT" established in 2014 as a project initiated by the Central Bank of Sri Lanka (CBSL), Sri Lanka Bankers Association (SLBA) and Sri Lanka Computer Emergency Response Team Coordination Centre (Sri Lanka CERT | CC). LankaClear Pvt Ltd, who operates the Sri Lankan Payment Network, was invited to host FinCSIRT as independent unit.

FINCSIRT is established as a centralized body (Not-for-Profit Organization) to coordinate security efforts within the banking and financial sector and operated as an entity steered and funded by the Banks.

1.3 Resources

As of Dec. 2021, around 8 employees including manager, assistant manager, senior security engineer, two security engineers and three security analysts with following qualifications:

- MSC in Information Security
- BSc in Cyber Security/Information Systems/Information Technology
- CDPSE - Certified Data Privacy Solutions Engineer
- CISA - Certified Information Systems Auditor

- CISM - Certified Information Security Manager
- CRISC - Certified in Risk and Information Systems Control
- eJPT- eLearnSecurity Junior Penetration Tester
- CEH - Certified Ethical Hacker
- CSA - Certified SOC Analyst
- ISMS- Information Security Management System

1.4 Contact Information

- Tel: +94 112039777
- Email: info@fincsirt.lk
- Website: http://fincsirt.lk/index.html

2. Activities & Operations

2.1 Summary of key activities conducted by the FinCSIRT in year 2021

2.1.1 Incident handling for members

Assisted members in resolving reported incidents including ATM skimming incident (1), Malware infection (1), Banking apps scam (1), Phishing (1), Social media scams (10) during the year.

2.1.2 Monthly Follow up calls for members

FinCSIRT always stay alerted on the information security status of the financial sector in Sri Lanka and do continuous follow ups with the members to keep the information up to date.

2.1.3 Disseminating Alerts to the members

In order to keep our members up to date on the information security aspect we have sent

- Advisory Alerts (134)
- FSOC Alerts (11)
- ISOC Alerts(897)
- Informational Alerts (7)
- Vulnerability Alerts (4)

2.1.4 Online Monitoring System by FinCSIRT to members

FinCSIRT conducted the Online monitoring system which helps the financial sector banks and finance companies to monitor availability of their internet facing banking systems, applications, and websites.

2.1.5 Conducted external security reviews for members on 42 web applications.

FinCSIRT assists members with external security reviews to determine the likelihood of breaking into an information system via the Internet network. The review is intended for public services, which are the most frequently targeted.

2.1.6 Conducting financial sector cyber security readiness assessment with members.

Conducted financial sector cyber security readiness assessment covering the capabilities of handling rapidly advancing threats under the control environments under the areas including IT Security Policy (ISP), Physical Access to Server Room and DR, User Access Management, Password and Account Lockout, User Monitoring, Firewall, Change Management, BCP and DRP, Backup and Restoration, Incident Management, Secure Vendor Access, Audit Logs, Wi-Fi, Software Development, Patch Management, Vulnerability Management, for all banking members whose IT operations are in Sri Lanka.

2.1.7 Digital poster campaign to raise Cybersecurity awareness with ISACA and NSBM university student group

Digital poster campaign was carried out joining the University students in order to increase the information security awareness among Sri Lanka using creative artwork to convey the idea effectively.

3. Events Organized / Hosted

3.1 Conducting national cyber drill with British high commission, Sri Lanka CERT and TechCERT.

In collaboration with the British High Commission, Sri Lanka CERT (APCERT member) and TechCERT (APCERT member) a cyber drill was conducted in order to understand the actual versus perceived capabilities of people and technology improving the moral and team building, as well as to determine where to allocate budgets for

training or new technology, checking compliance with regulatory requirements, stress reduction for security teams/ management and so on. This was participated by members of the banking community LankaClear Pvt Ltd and the regulator who are the key stakeholders of Sri Lanka financial sector.

4. Training Activities

4.1 Conducted webinar for members on Information Security Standards introduction.

Topic Summary : FinCSIRT conducted an information security standards awareness program to provide an introductory overview of most common internationally recognized information security standards and frameworks, including the areas that each cover. First part of the session focused on ISO standards and NIST that help to manage Information security and risks. Second part of the session focused on frameworks that help to set up incident handling organizations, units, departments and their services.

- Date : 22th March 2021
- By : Cyber4Dev team
- Audience: FinCSIRT members

4.2 Conducted webinar on establishing organizational information security structure session

Topic Summary : Managing information security systematically is the key to protect organization and its assets. The establishment of an Information Security Management System (ISMS) is essential, will help provide focus to information security policy and will mitigate risk. This training session helped provide the ability and knowledge, to enable the participants to establish ISMS and its structure.

- Date:19th & 20th May 2021
- By: Cyber4Dev team
- Audience:
  Information Security Managers and Officers
  Data Protection Officers
  Risk Managers

Business Continuity Managers

Internal Auditors

Security Leadership

CTO, CIO

FSI-CERT

Financial Security Institute – Computer Emergency Response Team - Republic of Korea

1. About the Organization

1.1 Introduction

FSI-CERT is a financial security-specialized organization Korea, and a non-profit cooperation founded by financial companies.

Through information sharing of incidents, notification of intrusion attempts, analysis of the incidents' cause, prompt response and prevention measures, FSI-CERT has established and is operating cyber security incident response systems in the financial sector.

In case of incidents resulting from cyber-attacks, FSI-CERT analyzes the cause of the incident through digital forensics and provides initial response along with prevention measures to hold back further damage or incidents.

FSI-CERT protects the financial industry from various cyber threats through threat monitoring, computer emergency response, vulnerability analysis and assessment for digital financial infrastructures.

1.2 Establishment

FSI-CERT is a Korean financial security specialized organization founded on April 2015 to create a safe and reliable financial environment and to contribute to the establishment of a convenient financial environment for financial services consumers and financial institutions.

1.3 Resources

As of Dec. 2021, FSI-CERT has more than 250 employees working in 7 divisions and 3 centers, in charge of financial security monitoring, cyber attack response, and vulnerability analysis & assessment, etc.

1.4 Contact Information

Tel: +82-2-3495-9431

Fax: +82-2-3495-9399

Email: cert@fsec.or.kr

Website: http://www.fsec.or.kr/fseceng/index.do

2. Activities & Operations

2.1 Summary of major activities

2.1.1 Log4j Zero-day vulnerability attack detection & response

FSI-CERT has quickly and successfully responded to Log4j Zero-day vulnerability attacks targeting financial companies in Korea.

2.1.2 Dark-web threat monitoring & response

FSI-CERT successfully responded to cyber threats and security incidents related to the dark web by monitoring financial information and the latest hacking traded on the dark web.

2.1.3 AI-based malware analysis model development

FSI-CERT developed and applied a next-generation malware analysis system model using artificial intelligence (AI) analysis. As a result, the detection and response efficiency of unknown and variant malware has increased.

2.1.4 Bug-bounty program for the financial sector

FSI-CERT held a Bug-bounty program to discover unknown vulnerabilities in the financial sector that could pose a threat to cyber-security in the future

2.1.5 Next-generation financial ISAC system operation

FSI-CERT operated a next-generation Financial Information Sharing and Analysis Center(ISAC) system by applying artificial intelligence (AI) technology, threat intelligence, and private cloud technology.

2.1.6 Voice Phishing threat sharing

FSI-CERT established a voice phishing fraud sharing system between financial, communication, security, and public sectors using information sharing APIs to cope with advanced voice phishing threats.

2.1.7 Financial mobile apps Integrated analysis system operation

For cyber-security and safe use of financial apps, 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 gets on the scene immediately to gather digital evidence and analyze the cause of the accident through digital-forensics. FSI-CERT also establishes measures to prevent damage propagation and enhance cyber threat response capabilities of related financial companies 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 information

FSI-CERT collects and analyzes malware related to financial companies, shares recent cyber security trends, and performs the leading role in establishing and implementing the corresponding actions. FSI-CERT systematically analyzes a large amount of malware by using AI-based malware analysis system and provide information from the correlation analysis.

In 2021, the number of malware threat information sharing increased significantly due to improved analysis efficiency such as improving methods of collecting malware threat information and applying AI detection models.

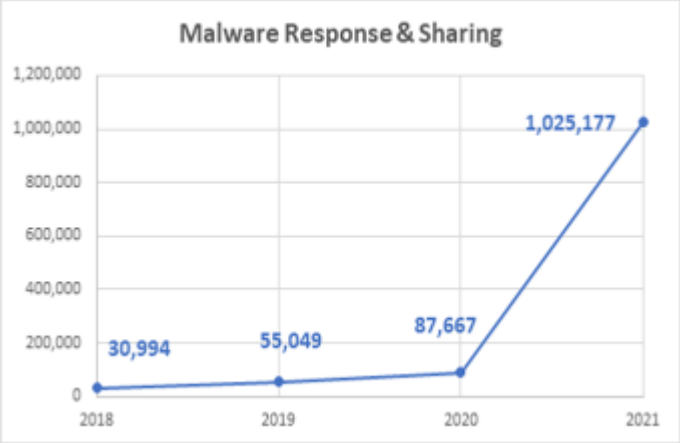


Figure 2. The Number of Malware response & Sharing

2.2.3 Cyber Security Incident Simulation Training

FSI-CERT performs cyber security incident simulation training for financial companies. The training simulates the conditions of real cyber-attacks. During the training, the testers from FSI-CERT attack the servers and web pages in operation, using attack techniques that real-world hackers commonly exploit. Through the training, FSI-CERT has contributed to improving the security awareness and response capabilities of the financial sector against real cyber-attacks and intrusion.

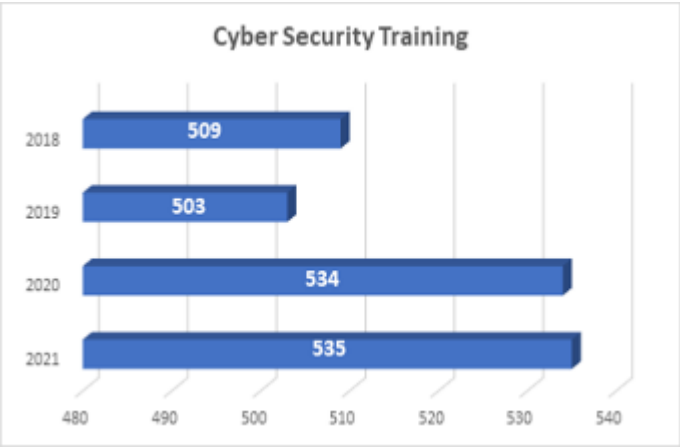


Figure 3. The Number of Cyber Security Training

2.2.4 Operation of DDOS Attack Emergency Response Center

In the event of large-scale DDoS Attacks that cannot respond to financial companies, FSI-CERT supports them by filtering DDoS attacks and sending back valid network traffic to the financial companies. The cloud-based DDoS cyber shelters block large-scale bandwidth attacks in advance. Then FSI-CERT's DDoS attack emergency response center blocks application-layer attacks on critical services.

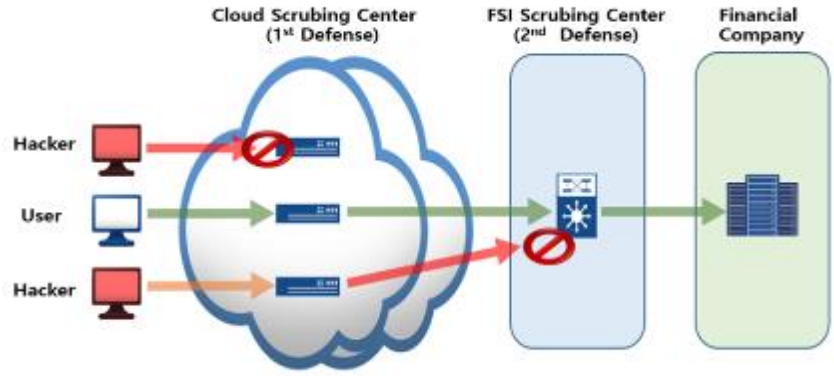


Figure 4. DDoS Attack Response Process

2.3 Integrated Security Monitoring

FSI-CERT operates a financial sector ISAC and uses AI and big data-based security monitoring system to detect cyber threats against the entire financial industry 24/7. In 2021, FSI-CERT has quickly and successfully responded to Log4j vulnerability Zero-day attacks targeting Korea financial companies.

Figure 5. The Number of Intrusion Response & Reporting

FSI-CERT protects the financial assets by detecting phishing & pharming websites and blocking the spread of malicious apps used for voice phishing crimes.

Figure 6. The number of Phishing Site Detection & Response

2.4 Vulnerability Analysis and Assessment

FSI-CERT have provided comprehensive inspections and vulnerability checks on electronic financial infrastructure such as public webpage to find and mitigate potential vulnerabilities in financial company systems.

In order to support the autonomous security system, technical support and education such as improving evaluation methods and inspection tools were provided so that financial companies could inspect their own vulnerabilities.

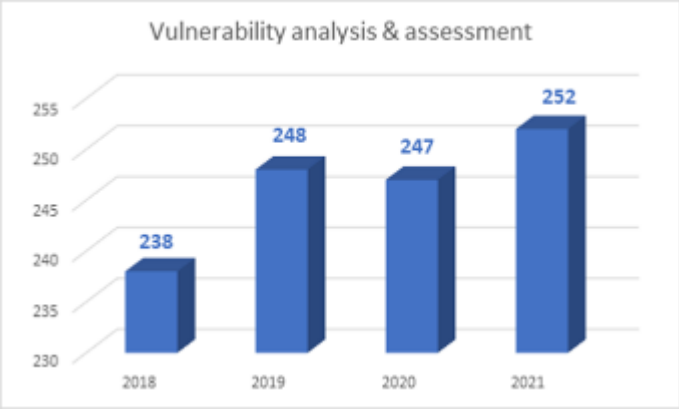


Figure 7. The Number of Vulnerability analysis & assessment

Areas: Information security management systems, Servers, Network, Information security systems, 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.

3.1.1 Cyber threat analysis targeting credit card information

This report presents comprehensive analysis results of threat groups targeting credit card information, malware profiling, illegal transactions on the dark web, leaked credit card data profiling

Download: www.fsec.or.kr/common/proc/fsec/bbs/163/fileDownLoad/3286.do

3.1.2 Analysis of major Encryption algorithms used by ransomware

This report classified and analyzed major encryption algorithms used by ransomware, which is recently being distributed. Through this, a ransomware encryption operation process and an analysis method of core algorithms were presented.

Download: www.fsec.or.kr/common/proc/fsec/bbs/163/fileDownLoad/3091.do

4. Events Organized / Hosted

- Korea Financial Security Forum 2021
- Voice Phishing Response Meeting
- New Technology for financial security Seminar
- Financial ISAC Research Exchange Meeting (Financial ISAC JAPAN)
- FISCON 2021 (Financial Information Security Conference)
- ASIA-Economy (Korea media company) financial IT Forum
- Financial Data Exposition
- FIESTA 2021 (Financial Institutes' Event on Security Threat Analysis)
- Financial Sector Threat Identification Working Group Meeting
- Malware Working-level Meeting

5. Conferences and Presentation

- DEFCON 29 CTF, hosted by Order of the Overflow(Las Vegas, August)
- HDCON 2021, hosted by CONCERT(Korea, October)

6. Collaboration With AP-CERT

At 2020 APCERT online training, FSI-CERT held an education program related to ATM Cyber Attack. FSI-CERT hopes to continue participating in seminars of APCERT to share our research results of the financial security sector.

7. Conclusion

Cybersecurity 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 upgrade cybersecurity systems such as financial sector Information Sharing and Analysis Center (ISAC), digital forensics, and malware analysis to cope with increasingly intelligent security threats. In addition, it will provide a safer foundation for the financial industry by incorporating new technologies such as big data and artificial intelligence into security.

KZ-CERT

Kazakhstan Computer Emergency Response Team - Kazakhstan

1. About the Organization

Computer Emergency Response Team (KZ-CERT) is a single centre for national information systems users and kazakhstani Internet segment providing collection and analysis of security incidents reports 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 the republican state enterprise with the right of economic management “Center for technical support and analysis in telecommunications”.

On January 28, 2013, the republican state enterprise with the right of economic management was renamed to the republican state enterprise with the right of economic management “State Technical Service” by the government decision. Ministry of Transport and Communications was designated as an administrative body for enterprise governance (“On some state technical service issues”, Decree of the Government of the Republic of Kazakhstan dated August 28, 2013 №49).
Apart from that, there was also an establishment of the National Coordination Center for Information Security which unified KZ-CERT, e-government information security monitoring and telecommunications network management services.

1.2 Resources

Currently, KZ-CERT Team employs more than 20 people of various profiles.

2. Activities and operations over 2021

KZ-CERT Team is responsible for handling the following computer incidents in order to detect and neutralize them

- Bruteforcing of passwords or other authentication data;
- Hacking security systems;
- Hostile scanning of national information networks and hosts;
- Unauthorized access to information resources;

- Spreading the malware and unsolicited mail (spam);
- Attacks on network infrastructure and server resources.

2.1 Incident handling report

In 2021, KZ-CERT has handled a total of 23,358 cybersecurity incidents. The largest number of cybersecurity incidents managed is associated with the creation and distribution of malware. Figure 1 shows a more detailed information on their types.

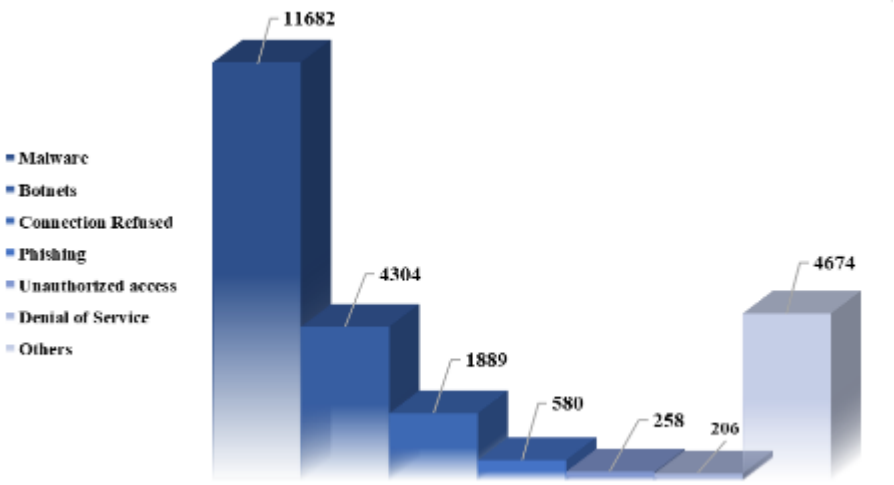


Figure 1. Types of the handled incidents by KZ-CERT over 2021

For example, in the 1st half of 2021, KZ-CERT received information about workstations infected by malware. In the course of the investigation of this case, KZ-CERT identified a suspicious file named DOC001.exe. While studying the DOC001.exe object, it was discovered that it creates files such as NsCpuCNMiner32.exe and NsCpuCNMiner64.exe in the With:¥Users¥* username¥AppData¥Roaming¥Temps folder.

In such scenario, an explorer.lnk file is created in the startup folder. Restarting the workstation would trigger the download of the VID001.exe malicious file which helps to establish a connection with malicious servers.

Malware runs a bash script that copies the DOC001.exe file to open network directories, which allows it to spread across the entire network.

Malicious file DOC001.exe starts running either NsCpuCNMiner32.exe file or NsCpuCNMiner64.exe file (depending on the system bit set), which in turn performs mining tasks using the computing power of the victim's hosts. File NsCpuCNMiner32.exe can be found located by the C:¥Users¥admin¥AppData¥Roaming¥Temps¥NsCpuCNMiner32.exe path.

KZ-CERT collected indicators of compromise and provided step-by-step recommendations for detecting and eliminating malicious activity.

In 2021, based on the results of handling cybersecurity events and incidents, KZ-CERT has sent 2503 notifications to foreign organizations of 80 countries and received 2278 notifications from the foreign organizations of 75 states.

The top 10 countries for notifying and getting notified by KZ-CERT are shown in Figure 2 and Figure 3, respectively.

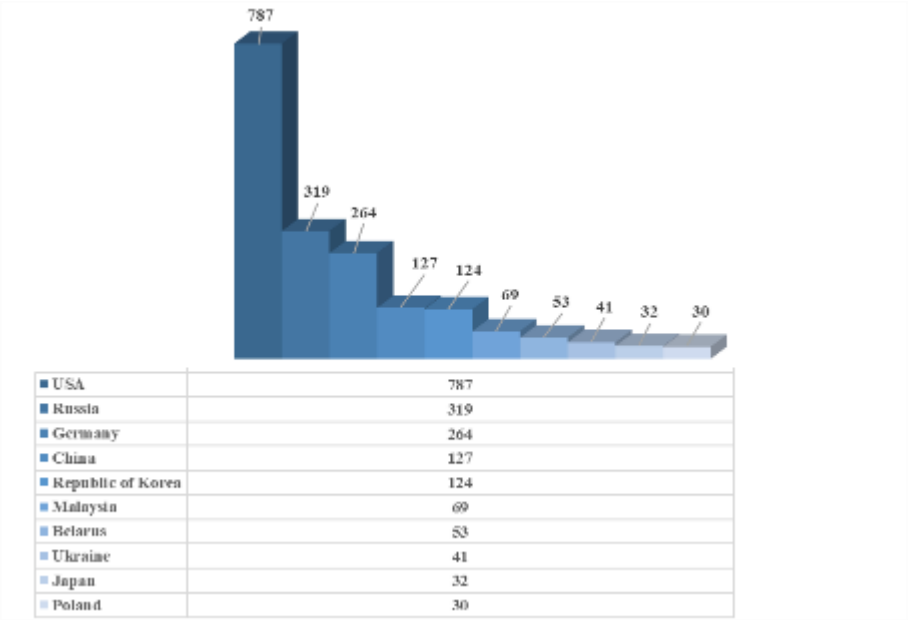


Figure 2. Incoming foreign notifications statistics

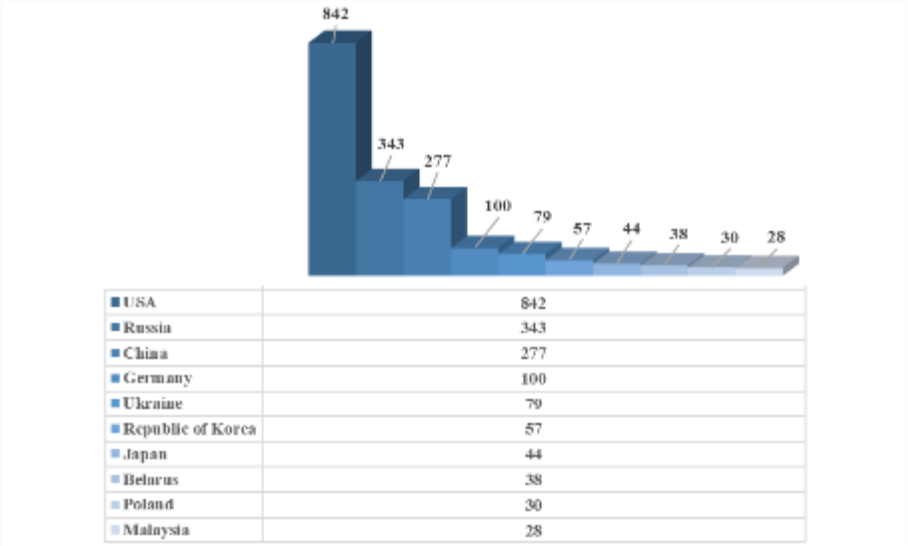


Figure 3. Outcoming foreign notifications statistics

2.2 Publications

Official website of KZ-CERT (cert.gov.kz), along with the newsfeed, features regularly published articles containing recommendations on the topics of cyberhygiene and cybersecurity. All the material is provided in three languages - Kazakh, Russian and English. Among the published articles for 2021, you can find the following:

- what to do if your money was debited from your bank card? (cert.gov.kz/news/13/1382)
- how can your stories help attackers? (cert.gov.kz/news/13/1385)
- how to avoid giving your account to fraudsters? (cert.gov.kz/news/13/1395)
- updating passwords on iPhone iOS 14 (cert.gov.kz/news/13/1430)
- do you know what interests virtual fraudsters the most? (cert.gov.kz/news/13/1429)
- how to set up a secure DNS? (cert.gov.kz/news/13/1428)
- how to use the wireless network safely? (cert.gov.kz/news/13/1439)
- how mobile apps steal money from your smartphones (cert.gov.kz/news/13/1449)
- Apple hides passwords in screenshots (cert.gov.kz/news/13/1461)
- how to remove a computer from the botnet? (cert.gov.kz/news/13/1474)
- tips for safe online shopping (cert.gov.kz/news/13/1488)
- how to protect Chrome and YouTube history with a password or fingerprint? (cert.gov.kz/news/13/1515)
- recommendations for kazakhstani mobile app developers (cert.gov.kz/news/13/1518)
- recommendations for technical specialists on proactive threat search

(cert.gov.kz/news/13/1559)

- recommendations for preventing incidents related to the cryptographer (cert.gov.kz/news/13/1558)
- Big data, how to be friends with it? (cert.gov.kz/news/13/1612)

2.3 Awareness-raising

In 2021, KZ-CERT Team staff organized visits to a number of educational institutions in order to give lectures on cybersecurity. The program involved middle school and high school students to whom our lectures on the following topics were presented:

- Phishing;
- Cyberbullying;
- Personal data protection;
- Malware;
- Antivirus;
- Dangerous content;
- Public networks.

During the lectures, KZ-CERT Team staff also demonstrated cybersecurity incidents. Students showed great interest and actively participated in discussions and quizzes to consolidate the acquired knowledge.

3. Collaborations with APCERT members/partners

KZ-CERT, as any other, recognizes the importance of cooperation with similar services and organizations; therefore, it is always open to invitations and opportunities to participate in various events dedicated to the information security field.

International cooperation plays a big role in establishing communications with the global IT and IS 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 at different international information security conferences and other events.

3.1 Trainings

- On August 25, 2021, KZ-CERT participated in the "Supply Chain Attack Through

Spear-Phishing - Beware of Working from Home" APCERT Drill 2021. At each stage, all the necessary recommendations were developed to find the source and eliminate malicious activity, and notifications were sent to other CERTs to stop the malicious activity of detected C&C servers and phishing websites depending on the country in whose jurisdiction they are located.

- On October 28, 2021, KZ-CERT participated in OIC-CERT CyberDrill 2021 organized by the International Organization of Islamic Cooperation of Computer Incident Response Services (OIC-CERT). 2 KZ-CERT Team members as main participants were engaged in solving practical tasks, while the other 2 specialists acted as observers, whose task was to monitor the process.
- In October 2021, KZ-CERT participated in GCCD Cybersecurity Hands-on Exercise program organized by the Korean Internet and Security Agency (KISA). It is worth noting that through participation in the above-mentioned cybersecurity events useful experience was gained by interacting with foreign partners in responding to cybersecurity incidents. These events contributed to the development of the processes and procedures for managing cybersecurity incidents, as well as the growth of the technical competence.

3.2 Events

In 2021 KZ-CERT has signed a Memorandum of Cooperation with JPCERT/CC. Apart from that, KZ-CERT actively participated in various international events, including those organized or hosted by organizations our team shares APCERT membership with. Of these, the following can be mentioned:

- Annual CNCERT Conference (online, as a speaker);
- 6th CAMP Annual Meeting (our team prepared a special video);
- CAMP Regional Forum (our team presented a video themed “Digital transformation of the Republic of Kazakhstan over 30 years of Independence”;
- 16th NatCSIRT Annual Technical Meeting (online, as a speaker)
- Philippine International Cybersecurity Conference 2021 organized by DICT.

Disclaimer on Publications

The contents of the Activity Report on Chapter III and IV 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 2021

TLP: WHITE

APCERT
Asia Pacific Computer Emergency Response Team