APCERT
Asia Pacific Computer Emergency Response Team

TLP:CLEAR

ANNUAL REPORT 2024

Table of Contents

From the Chair

The Asia Pacific Computer Emergency Response Team (APCERT) has been in existence for 20 years since the APCERT agreement was accepted in 2003 in Taipei, and the inaugural Steering Committee (SC) was formed. Initially comprising 15 CSIRTs from 12 economies, APCERT has expanded to include 33 Operational Members from 24 economies, alongside 5 Liaison Partners, 4 Strategic Partners, and 6 Corporate Partners.

I believe that 2024 marked a significant milestone in APCERT's journey toward achieving its vision. Having moved past the challenges of COVID-19, we saw teams increasingly engage in in-person activities once again. The SC members had the valuable opportunity to convene face-to-face and visit our member organizations, strengthening collaboration and engagement. Additionally, APCERT members were able to take advantage of the FIRST Conference as an opportunity to meet and reconnect in person. Most notably, with the unwavering support of TWCERT/CC, we successfully hosted the APCERT Annual General Meeting (AGM) in a physical format for the first time in four years.

As cyber threats continue to challenge our constituencies, 2025 is expected to bring greater opportunities for face-to-face member engagement and the launch of new collaborative initiatives. As APCERT continues to grow, we aim to expand our membership base while strengthening participation from existing members & partners. Efforts will also focus on enhancing APCERT's visibility and fostering broader collaboration within the cybersecurity community. Additionally, we look forward to exploring new initiatives that facilitate and encourage greater in-person engagement among APCERT members, ensuring a more connected and resilient network.

This year marks KrCERT/CC's second term as chair, and I would like to express my heartfelt gratitude to all APCERT colleagues for their support in enabling us to fulfill this role effectively. Our collective efforts and trust-based engagement continue to strengthen APCERT as a leading incident response community in the Asia-Pacific region. I deeply appreciate the dedication and collaboration of our members & partners, which drive our shared success.

Eunju Pak
Chair, APCERT Steering Committee
KrCERT/CC of Korea Internet & Security Agency

About APCERT

Objectives and Scope of Activities

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

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

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

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

The formation of CERTs/CSIRTs at the organizational, national, and regional levels is essential for effective and efficient response against malicious cyber activities, widespread security vulnerabilities and incident coordination throughout the region. One important role of CERTs/CSIRTs is building cyber security capabilities and capacities in the region, including through education and training, to raise awareness and encourage best practices in cyber security. APCERT coordinates activities with other regional and global organisations.
The geographical boundary of the APCERT activities is the same as that of the APNIC. This covers the entire Asia Pacific, comprising 56 economies. The list of those economies is available at:
https://www.apnic.net/about-apnic/organization/apnic-region/

APCERT Members

The APCERT was formed in 2003 with 15 teams from 12 economies across the Asia Pacific region, and the membership has continued to increase since then. For further information on the APCERT membership structure and criteria, please refer to the APCERT Operational Framework:
https://www.apcert.org/documents/pdf/APCERT_Operational_Framework_18Oct2022.pdf
As of December 2024, APCERT consists of 33 Operational Members from 24 economies across the Asia Pacific region, 5 Liaison Partners, 4 Strategic Partners, and 6 Corporate Partners.

Operational Members

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

ID-SIRTII/CC	Indonesia Security Incident Response Team of Internet Infrastructure/Coordination Center	Indonesia
JPCERT/CC	Japan Computer Emergency Response Team / Coordination Center	Japan
KN-CERT	Korea National Computer Emergency Response Team	Republic of Korea
KrCERT/CC	Korea Internet Security Center	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
National CSIRT of Mongolia	National Computer Security Incident Response Team of Mongolia	Mongolia
NCSC NZ	National Cyber Security Centre New Zealand	New Zealand
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
TWCERT/CC	Taiwan Computer Emergency Response Team / Coordination Center	Chinese Taipei
VNCERT/CC	Viet Nam Cybersecurity Emergency Response Teams/Coordination Center	Vietnam

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

At the APCERT AGM 2024, KrCERT/CC was elected as the Chair of the APCERT, and CyberSecurity Malaysia as the Deputy Chair. The terms of each Steering Committee (SC) member are as follows:

Team	Term	Other positions
ACSC	2024 - 2026	Deputy Chair
CNCERT/CC	2024 – 2026	
CyberSecurity Malaysia	2023 – 2025	
JPCERT/CC	2023 – 2025	Secretariat
KrCERT/CC	2024 - 2026	Chair
Sri Lanka CERT|CC	2023 - 2025	
TWCERT/CC	2024 – 2026	

Working Groups (WGs)

There are 8 Working Groups (**WG**s) in APCERT.

5G Security WG (formed in 2024)

Objectives

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

Convener (1): Sri Lanka CERT|CC

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

Coordinated Vulnerability Disclosure WG (formed in 2023)

Objectives

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

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

Convener (1): JPCERT/CC

Members (5): AusCERT, CERT-In, CyberSecurity Malaysia, KrCERT/CC, TWCERT/CC

Drill WG (formed in 2017)

Objectives

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

Convener (1): KrCERT/CC

Members (12): ACSC, AusCERT, CERT-In, CyberSecurity Malaysia, ETDA, HKCERT, JPCERT/CC, SingCERT, Sri Lanka CERT|CC, TechCERT, TWCERT/CC

Information Sharing WG (formed in 2011)

Objectives

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

Convener (1): CNCERT/CC

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

IoT Security WG (formed in 2017)

*The WG concluded in January 2025.

Objectives

- Identification of the threat landscape and security challenges in the IoT ecosystem

- Suggesting steps to address the security issues including vulnerabilities tailored for IoT
- Recommendations for securing the IoT ecosystem
- Developing incident response mechanisms/measures for responding to cyber physical security incidents 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, HKCERT, IDSIRTII/CC, JPCERT/CC, NCSC NZ, Panasonic PSIRT, VNCERT/CC

Membership WG (formed in 2011)

Objectives

- Promote collaboration and participation by all APCERT members and partners
- Establish the organizational basis to enhance the partnership with cross-regional partners
- Guide activities such as checking and monitoring for sustaining the health of the membership and partnership structure

Convener (1): KrCERT/CC

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

Policy, Procedure and Governance WG (formed in 2013)

Objectives

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

Convener (1): ACSC

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

Training WG (formed in 2015)

Objectives

- Establish an overall training program to assist members to develop, operate, and improve their incident management capabilities
- Provide a channel for members to share and exchange valuable experiences with other member teams at regular intervals

- Nurture cooperation and collaboration among members, providing training activities such as conducting online and face to face technical workshops to enhance fellow members' cyber security capabilities and capacities in mitigating cyber incidents more efficiently and effectively

Convener (1): TWCERT/CC

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

APCERT Website

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

APCERT Activity Report

International Activities and Engagements

International Conferences and Events

APCERT has been dedicated to representing and promoting its activities at various international conferences and events. From January to December 2024, APCERT Teams hosted, participated and/or contributed to the following events:

National CSIRT Meeting (14-15 June – Fukuoka, Japan)

APCERT teams attended the 19th Annual Technical Meeting for CSIRTs with National Responsibility (NatCSIRT 2024) and exchanged various activity updates as well as recent projects and research.

36th FIRST Annual Conference (9-14 June – Fukuoka, Japan)

https://www.first.org/conference/2024/

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

APCERT Cyber Drill 2024 (29 August)

Press Release (29 August 2024)

The APCERT Cyber Drill 2024, the 19th APCERT cyber exercise drill, was successfully conducted to test the response capabilities of the participating APCERT Teams. 22 CSIRTs from 18 economies of APCERT Australia, Brunei Darussalam, Bhutan, People's Republic of China, Chinese Taipei, Hong Kong, India, Japan, Republic of Korea, Lao People's Democratic Republic, Malaysia, Myanmar, Mongolia, Philippines, Singapore, Sri Lanka, Thailand, and Vietnam) participated in the drill. From the external parties, 3 CSIRTs from 3 economies of OIC-CERT and AfricaCERT participated.

APCERT Annual General Meeting (AGM) and Conference 2024 (5-6 November – Chinese Taipei)

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

- 5 November APCERT Annual General Meeting
- 6 November APCERT Closed Conference

2024 APCERT & FIRST Regional Symposium for Asia Pacific (7-8 November – Chinese Taipei)

https://www.first.org/events/symposium/asia-pacific2024/

FIRST and APCERT co-hosted a symposium as a part of the open conference of APCERT Annual General Meeting (AGM)

and Conference 2024. The program overview is as follows:

- 7 November Plenary Sessions (Open Conference)
- 8 November Training

ASEAN CERT Incident Drill (ACID) 2024 (15-16 October – Online)

ACID 2024, led and coordinated by SingCERT, entered its 18th iteration with participation including ASEAN CERTs and APCERT Teams. The theme was "Navigating the Rise of AI-enabled Cyber Attacks," and the drill was completed successfully, providing an opportunity for teams to improve their knowledge and skills on investigation and response.

Other International Activities and Engagements

DotAsia

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

Forum of Incident Response and Security Teams (FIRST)

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

STOP. THINK. CONNECT (STC)

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

Asia Pacific Network Information Security Centre (APNIC)

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

Africa Computer Emergency Response Team (AfricaCERT)

The APCERT and AfricaCERT signed an MoU in 2019.

APCERT SC Meeting

From January to December 2024, the SC members held 5 teleconferences and 2 face-to-face meetings to discuss the APCERT operations and activities.

Date	Location
18 January	Teleconference
26 February	Face-to-face meeting (Bangkok)
8 May	Teleconference
1 July	Teleconference
16 August	Teleconference
25 October	Teleconference
5 November	Face-to-face meeting (Taipei)

APCERT Training

The APCERT held 6 training calls in 2024 to exchange technical expertise, information, and ideas.

Date	Title	Presenter
30 January	Incident Handling	CyberSecuirty Malaysia
26 March	Detecting malicious activities of APT groups	KZ-CERT
28 May	Cyber Security Incident Response	TWCERT/CC
16 July	Introduction to Threat Intelligence Tools	Huawei PSIRT
27 September	Incidents Handling and Ticketing	NCA-CERT
2 December	Experience sharing on Social Media Incident Handling	BtCIRT

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

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

Email: apcert-sec@apcert.org

Disclaimer on Publications

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

Activity Reports from Members

ACSC

Australian Cyber Security Centre

1. Highlights of 2024

1.1 Summary of major activities

In FY2023-24, the Australian Cyber Security Centre (ACSC) received over 36,700 calls to its Australian Cyber Security Hotline, an increase of 12% from the previous financial year. The ACSC also responded to over 1,100 cyber security incidents, highlighting the continued exploitation of Australian systems and ongoing threat to our critical networks.
The ACSC works broadly across government, industry and international partners to monitor, adapt and respond to this changing threat environment.

1.2 Achievements & milestones

ACSC is the Australian Government's technical authority on cyber security and below are some of our key achievements and milestones during Financial Year 2023–24.

What ACSC saw in Financial Year 2023-2024

- Average cost of cybercrime to businesses increased by 17%.
- Nearly **87,400 cybercrime reports**. On average a report every 6 minutes.
- Answered over **36,700 calls** to the Australian Cyber Security Hotline, up 12 per cent and on average 100 calls per day.

What ACSC did in Financial Year 2023–24

- Responded to over **1,100 cyber security incidents**.
- Notified **entities 930 times of potential malicious cyber activity**.
- **Australian Protective Domain Name System** blocked **over 82 million** malicious domain requests, **up 21 per cent**.
- **Domain Takedown Service** blocked **over 189,000** attacks against Australian servers, **up 49 per cent**.
- **Cyber Threat Intelligence Sharing partners** grew by **66 per cent** to over **400 partners**. **Shared over 1,372,400**

indicators of compromise.

- Published **29 PROTECT publications, updated the Information Security Manual quarterly, and updated the Essential Eight Maturity Model.**
- **Our Cyber Security Partnership Program** grew to around **119,300 partners**.
- Led **16 cyber security exercises** involving over **130 organisations** to strengthen Australia's cyber resilience.

2. CSIRT

2.1 Introduction

ACSC brings together capabilities to improve Australia's national cyber resilience including the following services:

- the Australian Cyber Security Hotline, which is contactable 24 hours a day, 7 days a week, via 1300 CYBER1 (1300 292 371)
- publishing alerts, technical advice, advisories and notifications on significant cyber security threats
- cyber threat monitoring and intelligence sharing with partners, including through the Cyber Threat Intelligence Sharing (CTIS) platform
- technical advice and assistance to help Australian entities respond to cyber security incidents
- national exercises and uplift activities to enhance the cyber security resilience of Australian entities
- collaborating with Australian organisations and individuals on cyber security issues through our Cyber Security Partnership Program.

2.2 Resources

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

2.3 Constituency

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

3. Activities & Operations

3.1 Incident handling reports

ACSC is able to build a national cyber threat picture, in part due to the timely and rich reporting of cyber security incidents by members of the public and Australian business. Cyber security incidents can be reported via the 'ReportCyber' tool on cyber.gov.au or via the Australian Cyber Security Hotline on 1300 CYBER1. Information reported to ACSC is anonymised prior to it being communicated to the community.

From 1 July 2023 to 30 June 2024 (FY2023–24) ACSC answered over 36,700 calls to the Australian Cyber Security Hotline, up 12%. This was an average of over 100 calls per day, an increase from 90 per day. ACSC also responded to over 1.100 cyber security incidents.

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

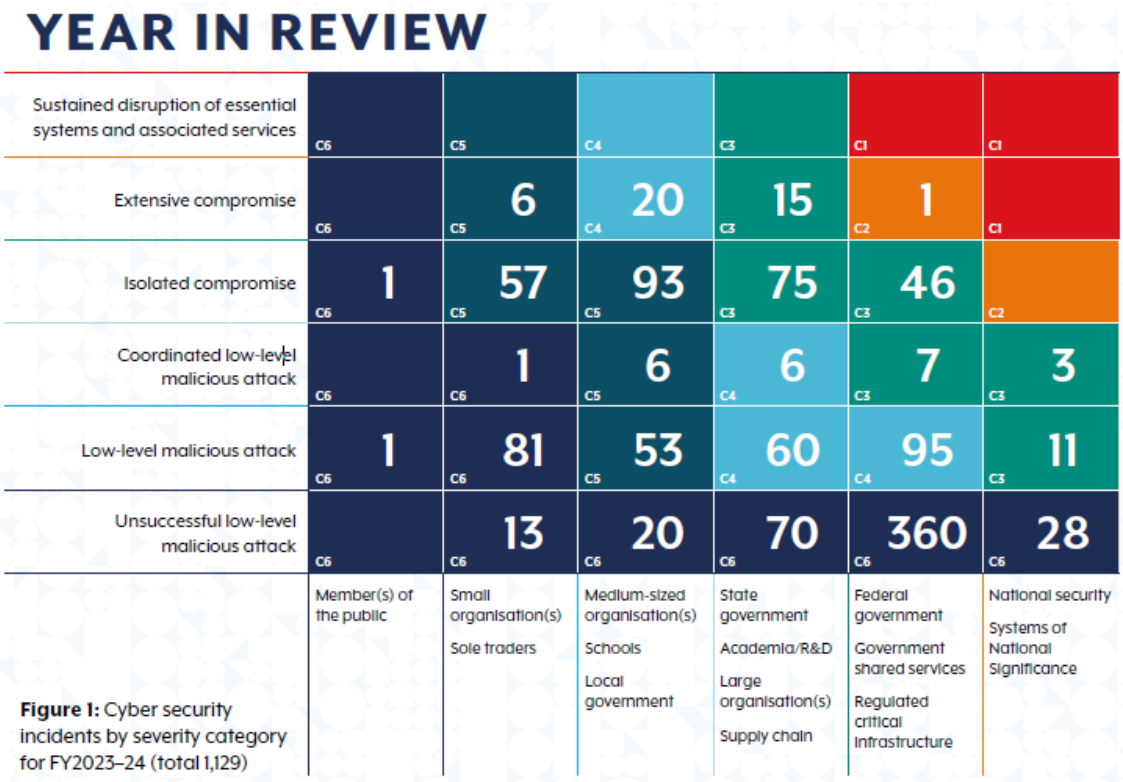


Figure 1: Cyber security incidents by severity category for FY2023–24 (total 1,129)

In FY2023–24, there was a slight decrease in the number of extensive compromises, while the number of unsuccessful low-level malicious attacks increased by 10% compared with FY2022–23. There was also a 39% increase in isolated compromises this financial year.

3.2 Publications and advisories

In 2023-24, ACSC published 118 alerts, advisories, incident and insight reports on cyber.gov.au and the Partnership Portal.

4. Events organized / hosted

4.1 Drills & exercises

ACSC's National Exercise Program helps critical infrastructure and government organisations validate and strengthen Australia's nationwide cyber security arrangements. The program uses exercises and other readiness activities that target strategic decision-making, and operational and technical capabilities.
In 2023, ACSC coordinated a national cyber security exercise series, known as DeliverEx, in partnership with Australian critical infrastructure owners and operators. The DeliverEx series strengthened industry and government's coordinated approach to cyber resilience, bringing together over 60 organisations from across Australia's transport and logistics sector, as well as government agencies responsible for transport and cyber security.

5. International Collaboration

5.1 International partnerships and agreements

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

5.2 Capacity building

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

5.2.1 Drills & exercises

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

In October, ACSC also participated in the ASEAN Cyber Incident Drill. Alongside 17 other regional CERTs, our organisation worked through a simulated incident under the theme 'Responding to Multi-Pronged Attacks Arising from Hacktivism'.

5.2.2 Seminars & presentations

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

6. Future Plans

6.1 Project REDSPICE

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

7. Conclusion

Through strong partnerships, ACSC works to defend Australians from cyber threats and make our country a harder target for malicious cyber actors.

Australia cannot face increasingly sophisticated cyber threats alone. Through networks like APCERT, we continue to partner with organisations to share information and expertise to collectively face shared cyber threats.

AusCERT

Australian Computer Emergency Response Team

1. Highlights of 2024

1.1 Summary of major activities

AUSCERT realises that continual improvement is the constant. That, in an ever changing threat landscape, this creates an ever changing operational landscape for a CERT or CSIRT. In 2024 AUSCERT has re-branded itself as "Allies in Cyber Security". Although this rebranding seems superficial, in fact the rebranding was made to highlight the service delivery methods have been modernised done to reflect the needs of our constituency. AUSCERT has also extended or deepened interactions with like minded entities. This action on the constant of change is the highlight of AUSCERT in 2024.

1.2 Achievements & milestones

1.2.1 Improvement of membership portal.

Easier access to the constituency of information from current notices as well as historic notices.

1.2.2 Machine Learning to detect Maliciously inclined Domains

Capability building in using various methods in detecting domains created with malicious intent. The use of machine learning is leveraged in capturing decision making experiences. This capability has not been kept to AUSCERT and the techniques has been shared to external CERTs as well as AUSCERT constituents in a tutorial.at the AUSCERT Conference 2024.

1.2.3 Improvement in creation of security Bulletins

AUSCERT has been in the process of changing core system and the last function of the core system was in the creation of security bulletins. Now, improvements in the data attached to bulletins can be made.

1.2.4 AUSCERT rebranding

AUSCERT has rebranded itself and is using the phrase "Allies in Cyber Security" to better reflect the position and stance of AUSCERT operations.

2. About CSIRT

2.1 Introduction

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

2.2 Establishment

AUSCERT was officially established on 8 March 1993 through the collaboration of three Brisbane based universities, including the University of Queensland.

Formed in 1993, AUSCERT is one of the oldest CERTs in the world and was the first CERT in Australia to operate as the national CERT, which it did until 2010.

Over time, as the Internet grew and government, business and ordinary users began to use the Internet for daily communications and business, AUSCERT's focus changed from being university centric to include the interests of all sectors.

2.3 Resources

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

2.4 Constituency

AUSCERT, due to its origins, continues to assist Australian private and public organisations and companies.

This is made possible by providing priority incident handling and additional services to our membership base of which

covers all industry definitions under the ANZ Standard Industry Classification.

AUSCERT works closely with Australian government agencies, industry and technology vendors and provides computer security and incident handling advice to a range of subscribers throughout Australia, New Zealand and the Asia-Pacific region. All Australian universities and the majority of New Zealand universities are members of AusCERT and there is a strong relationship with the Council of Australian University Directors of Information Technology (CAUDIT). AUSCERT participates in the Australian government's IT Security Experts' Advisory Group (ITSEAG).

3. Activities & Operations

3.1 Scope and definitions

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

Services provided are listed as:

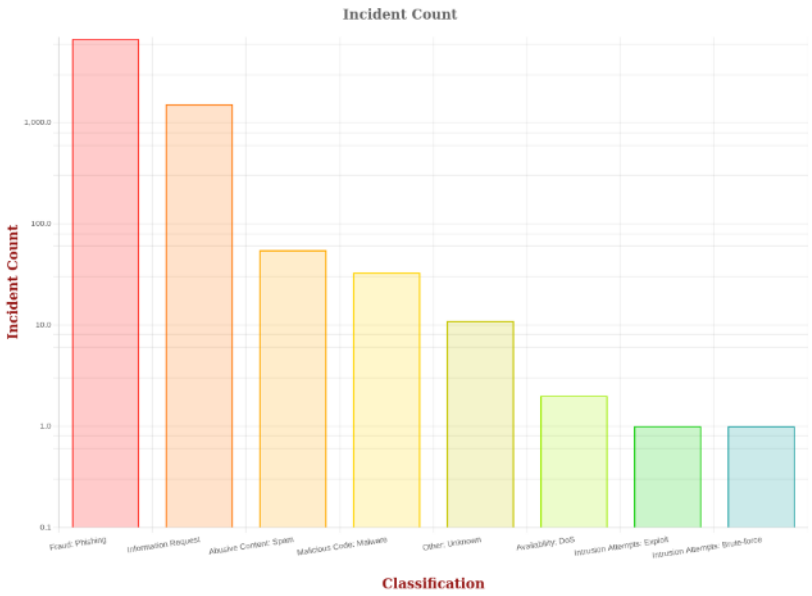
- Incident Management [3.2],
- https://www.auscert.org.au/services/incident-management-service/
- Early Warning Service
- https://www.auscert.org.au/services/early-warning-service/
- Malicious URL Feed
- https://www.auscert.org.au/services/malicious-url-feed/
- Security Bulletin Service [3.3]
- https://www.auscert.org.au/services/security-bulletins/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

3.2 Incident handling reports

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.

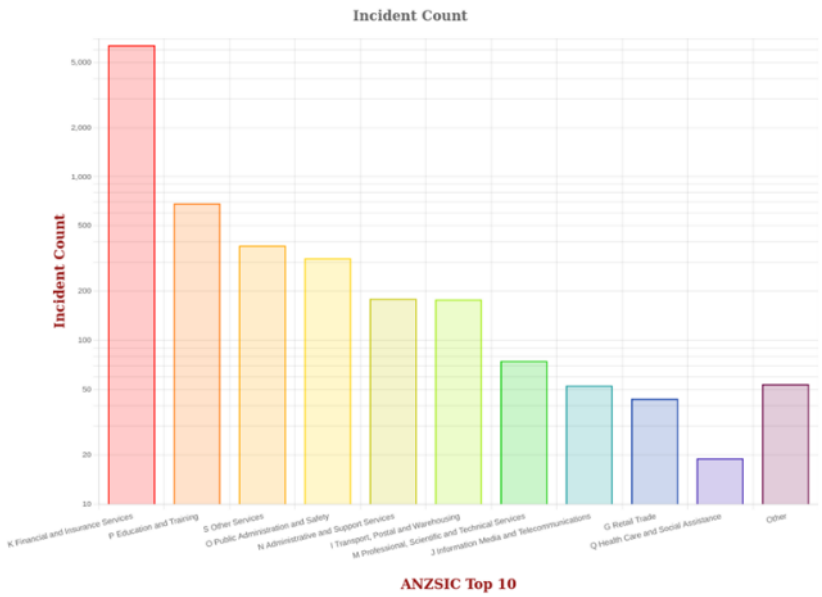
Incidents 2024 by Month

The diagram above shows the statistics of incidents that required handling for the calendar year of 2024. Overall, AUSCERT serviced 8365 tickets which resulted in just over 32 tickets per business day of operation.



Incidents 2024 by Classification

A vast majority of the work is around handling of phishing sites.



Incidents 2024 by Industry

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

The industry definition used is the Australian and New Zealand Standard Industrial Classification (ANZSIC) and further details can be found at:

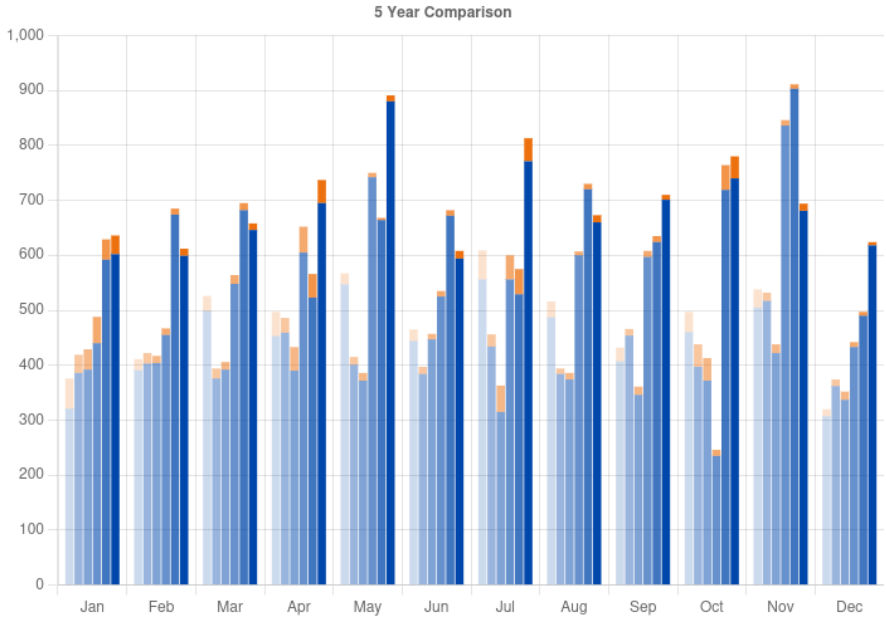
https://www.abs.gov.au/statistics/classifications/australian-and-new-zealand-standard-industrial-classification-anzsic/latest-release

3.3 Security Bulletins

AUSCERT distributes security advisories and bulletins to its members by email on each items as well as a summary of the day's volume.

Bulletins are published in a standardised format with a consistent approach to highlighting the maximum CVSS score, as well as the maximum EPSS that the patch release is addressing. Also notes are made about whether a CVE is in the Known Exploited Vulnerability (KEV), a list maintained by the United States of America's Cybersecurity Infrastructure Security Agency (CISA).

In 2024, 8147 External Security Bulletins (ESBs) and 249 AUSCERT Security Bulletins (ASBs) were published.



Bulletins by Month 5 Year Comparison

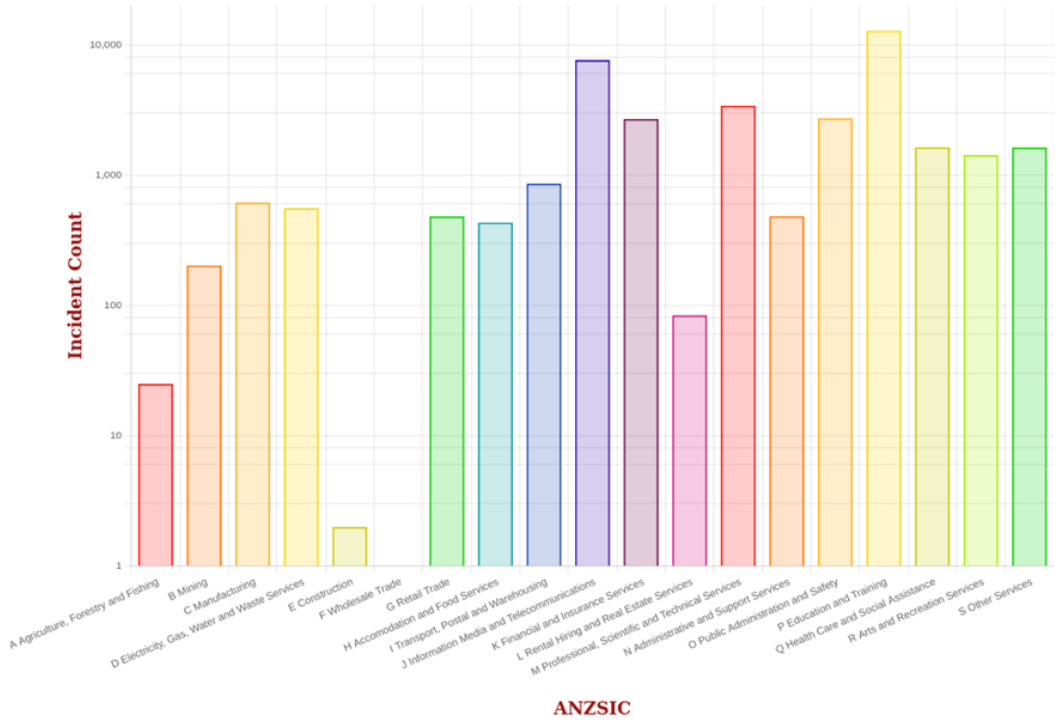
3.4 Member Security Incident Notification

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).

MSIN 2024 Mailout volume by Month

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



MSIN 2024 Mailout volume by Industry

3.5 Publications

3.5.1 ADIR

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

3.5.2 Week In Review

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

3.5.3 Social Media

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

3.5.4 Newsletter

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

3.5.5 Blog Post

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

3.5.6 Podcast

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

4. Events organized / hosted

4.1 Training

AUSCERT provides in the year of 2024 ten (10) cyber security training courses, suitable for cyber security, IT or risk management professionals, as well as cyber security awareness training that delivers important foundational knowledge in an engaging way that online, self-service training does not.
Training courses are available to everyone, membership is not required.
These training courses have been delivered throughout the year.

4.2 Tabletop exercises

AUSCERT's Tabletop Exercises help organisations enhance their cyber incident preparedness through customised, scenario-driven simulations that test decision-making and response strategies. Each includes tailored information gathering, an interactive simulation, a detailed post-exercise report, and a follow-up meeting to ensure continuous improvement in cyber resilience. Table top exercise were delivered throughout 2024 to organisations that have recognised that these activities assist in validating and verifying their approach to cyber security.

4.3 Conferences and seminars

4.3.1 AUSCERT Conference 2024

The AusCERT Conference 2024, took place from 21st May - 24th May 2024 at the Star, Gold Coast with the theme of "Pay it Forward". The conference included more than 50 presenters of ranging topics on cyber security. The conference has two format with the first two days with tutorial and the latter two days with speakers talking about contemporary topics on cyber security.

5. International Collaboration

5.1 International partnerships and agreements

AUSCERT maintains relationships with various like minded CERTs and CSIRTs around the world and carry these relationships with a mutual understanding on what are areas of collaboration. These relationships are active and are worked beyond written agreements. During 2024 AUSCERT has assisted another CERT in the Asia Pacific region on using machine learning in detection of suspicious domains, and embarked in assisting a CERT in Africa in using CERT centric tools.

AUSCERT also maintains membership with Asia Pacific Computer Emergency Response Team (APCERT) and the Forum of Incident Response and Security Teams (FIRST).

5.2 Capacity building

5.2.1 Drills & exercises

5.2.1.1 APCERT Drill 2024

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 "APT Group Attack Response: Where is Wally?". The drill fosters communication between the CERTs in the region and beyond. In all, 22 APCERT CERT/CSIRT teams from 18 economies participated.

5.2.1.2 ACID 2024

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

6. Future Plans

AUSCERT recognises that the landscape the CERTS and CSIRTS operates in has changed over time. There are vendors that have specialised in given CSIRT services and functions, whilst ISAC's has spawned with various efficacity as well as other non-governmental organisations have specialised in stolen identity in a cyber attack. These changes overtime need to be embraced as AUSCERT service are, at times overlapped with the services that are now available by complementary organisations. This necessitates a review of the strategy taken by AUSCERT in delivering cyber security service. This review will place AUSCERT in a better position to interact with the complementary services.

7. Conclusion

Operation of a CERT/CSIRT exists in a landscape that is ever changing. This is why AUSCERT connects with other like-minded entities in more than just agreements on the state of cybersecurity, but engages in enabling emergent and existing organisations in capacity and capability building. As the landscapes of operation change, to remain as an effective CERT, functions that enable services need to be reviewed improved and adapted and shared. AUSCERT will continue to engage with these like-minded entities to create a clean and safe internet.

BGD e-GOV CIRT

Bangladesh e-Government Computer Incident Response Team

1. Highlights of 2024

1.1 Summary of major activities

- BGD e-GOV CIRT has successfully organized "FINCII Cyber Drill 2024" for Financial Institution & Critical Information Infrastructure (CII) Cyber Drill 2024.
- Responding to five major cyber incidents reported to BGD e-GOV CIRT throughout the year.
- "Cyber Threat Intelligence" unit published 174 Cyber Threat Alerts and 7 Cyber Threat Advisories.
- Digital forensic services were provided to nine (9) organizations, involving the analysis of 61 artifacts across nine (9) cases.
- 20 cyber sensor analysis reports have been provided to multiple Critical Information Infrastructures.
- Vulnerability assessment and penetration testing (VAPT) have been carried out across various sectors in Bangladesh, including the financial sector, critical information infrastructures, and government sectors. VAPT was conducted for 15 organizations, assessing a total of 519 IT assets for vulnerabilities, which include web applications, APIs, servers, network devices, and mobile applications.
- IT audits Risk-based IT audits have been conducted across various sectors in Bangladesh, including Critical Information Infrastructures and government organizations.
- Provided Cyber security training to 183 Govt. officials in 2024.

1.2 Achievements & milestones

- The International Telecommunication Union (ITU) published the Global Cybersecurity Index 2024, where Bangladesh achieved Tier 1 – Role Modelling, with an impressive score ranging from 95 to 100.

2. About CSIRT

2.1 Introduction

Bangladesh Government's Computer Incident Response Team (BGD e-GOV CIRT) is acting as the National CERT of Bangladesh (N-CERT) currently with responsibilities including receiving, reviewing, and responding to computer security incidents and activities. Under the Government of People's republic of Bangladesh, BGD e-GOV CIRT reviews and takes necessary measures to resolve the issue with broad cybersecurity ramifications, conducts research & development and provides guidance on security vulnerabilities. BGD e-GOV CIRT also works with various government units, Critical Information Infrastructures, financial organizations, law enforcement agencies, academia & civil society to help to improve the cybersecurity defense of Bangladesh.

2.2 Establishment

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

2.3 Resources

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

2.4 Constituency

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

3. Activities & Operations

3.1 Scope and definitions

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

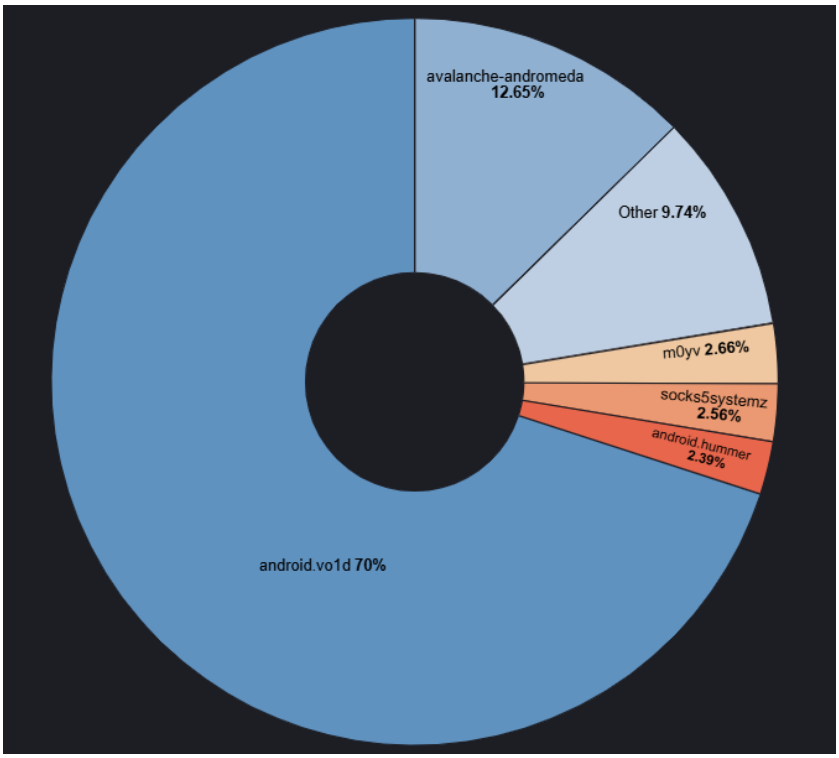
3.2 Incident handling reports

BGD e-GOV CIRT responded and investigated for 5 major cyber incident for different sectors of Bangladesh.

3.3 Abuse statistics

In 2024, the Cyber Threat Intelligence (CTI) unit of BGD e-GOV CIRT identified 194 unique malware strains from internet traffic specific to Bangladesh. The top five malware infections based on detected cases were:

- Android.Vo1d
- Avalanche-Andromeda
- M0yv
- Socks5Systemz
- Android.Hummer



3.4 Publications

- Total 7 cyber threat advisories are published.

4. Events organized / hosted

4.1 Training

- Conducted advanced cybersecurity training for 10 participants from The Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH.
- Conducted Cyber security training for 103 Govt. officials.

4.2 Drills & exercises

- BGD e-GOV CIRT has successfully organized "FINCII Cyber Drill 2024" for Financial Institution and Critical Information Infrastructure.

4.3 Conferences and seminars

- Organized a seminar on the "Cyber Security Strategy 2021-25".
- Organized a workshop on the "e-Sign".
- Organized a workshop on the "Cyber Resilience Workshop: Understanding Al Threats, Prevention, and Bangladesh Perspectives".

5. International Collaboration

5.1 Capacity building

5.1.1 Training

- Attend at "Japan -US Industrial Control Systems Cybersecurity Training" Tokyo, Japan from 12-15 November 2024.

5.1.2 Drills & exercises

- Participated Standoff 13 Cyberbattle which is a cyber exercise for information security researchers.
- Participated Standoff 14 Cyberbattle which is a cyber exercise for information security researchers.
- Participated "International Cyber Championship" organized by Economic Forum St Petersburg, Russia.

5.1.3 Seminars & presentations

- BGD e-GOV CIRT delivered an online presentation at the SANOG 41 event, organized by the South Asian Network Operators Group (SANOG) on 30th April 2024.

- Attend at "RSA Conference 2024".

6. Future Plans

6.1 Future Operation

- Arrange Cyber Drills for different sectors.
- Perform risk based IT audit in critical information infrastructure (CIIs).
- Provide training about Industrial Control System (ICS) in Public sector.
- Perform vulnerability assessment and penetration testing on multiple 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. Conclusion

As cyber threats continue to evolve in sophistication and scale, the need for vigilance, collaboration, and proactive defense has never been more urgent. Over the past year, BGD e-GOV CIRT has focused on strengthening critical systems, enhancing incident response capabilities, improving threat intelligence sharing and building human resource capacity. While significant progress has been made, the dynamic nature of cyber threats demands continuous adaptation and innovation. Moving forward BGD e-GOV CIRT remains committed to bolstering cybersecurity resilience, adopting in advanced technologies, enhancing workforce expertise and fostering collaboration across all sectors to safeguard sensitive information and ensure a more secure digital ecosystem.

8. Attachment (Photos)

Figure 1: FINCII Cyber Drill 2024 host team

Figure 2: Workshop on “Importance of the Cyber Security Act to Prevent Cyber Crime”

Figure 3: International Cyber Championship participation.

Figure 4: Advanced cyber security training for govt. officials

Figure 5: Cyber security strategy 2021-25 workshop

Figure 6: Cyber security training for govt. officials

Figure 7: Cyber security training for govt. officials

BruCERT

Brunei Computer Emergency Response Team

1. About BruCERT

1.1 Introduction

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

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

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

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

BruCERT Join Asia Pacific CERT (APCERT) in the year of 2005, join Organisation of Islamic Cooperation CERT in the year 2009 and join Forum for Incident Response Team (FIRST) in the year 2014.

BruCERT has been actively participating in local as well as international events, fostering more collaboration and establishing cooperation with other relevant organisations and CERT's.

1.1.1 BruCERT Services

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

1.2 BruCERT Establishment

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

1.3 BruCERT Workforce

BruCERT currently has a strength of 66staff (100% local) of which the majority are 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 relationships with Government agencies, 1 major ISPs and various numbers of vendors.

Government Ministries and Departments

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

E-Government National Centre (EGNC)

E-Government National Centre provides IT Services to all Government Departments and Ministries in Brunei Darussalam. Services such as IT Central procurement, Network Central Procurement, Co-location, ONEPASS (a PKI initiative), Co-

hosting are provided by EGNC. BruCERT works closely with EGNC in providing Incident Response and Security Monitoring since most of the government equipment resided at EGNC.

AITI

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

Royal Brunei Police Force (RBPF) and other Law-Enforcement Agencies (LEAs)

BruCERT has been collaborating with RBPF and other LEAs to resolve computer-related incidents through our Digital and Mobile Forensic services.

Unified National Network – UNN

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

Brunei Cyber Security Association – BCSA

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

1.5 BruCERT Contact

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

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

2. BruCERT Operation in 2024

2.1 Incidents response

For the year 2024, CSB's BruCERT, through the Cyber Watch Centre (CWC), has identified multiple instances of malicious behavior through the secure monitoring and intelligent sensors, located at the BruCERT constituent systems. Based on the information, most recorded incidents are related to Malicious Software (1,955 cases), making it the most significant cybersecurity concern. This is followed by Unsuccessful Hacking Attempts (320 cases) and Reconnaissance activities (202 cases), indicating persistent probing and attempted breaches. Additionally, Normal User Account (97 cases) and Privilege User Account (83 cases) events suggest potential security risks associated with user access. Denial of Service (2 cases) appears to be a minimal threat in comparison.

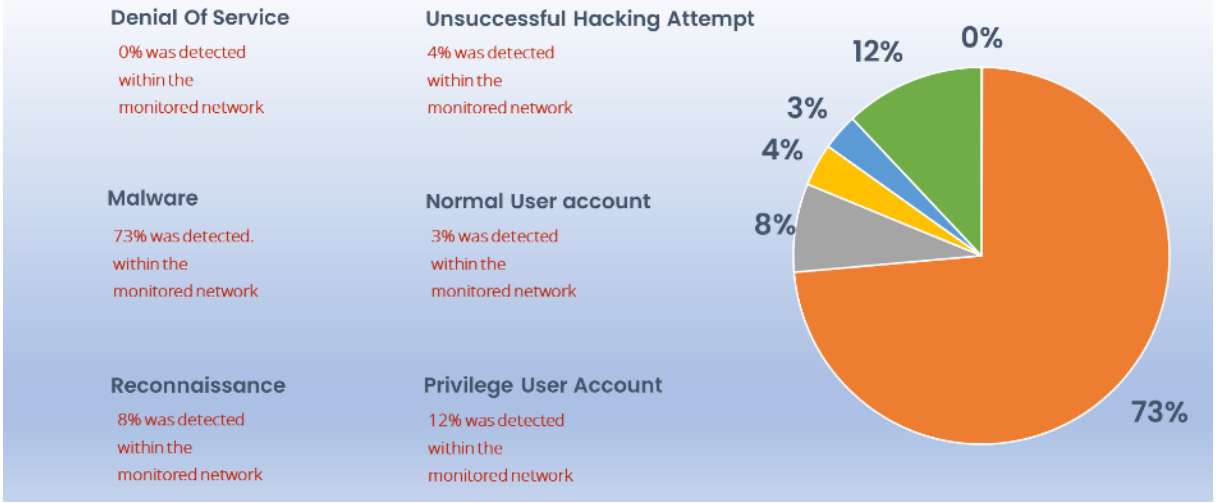


Figure 1

Types of Attacks	Count
Denial of Services	2
Malicious Software	1955
Reconnaissance	202
Unsuccessful Hacking Attempt	320
Normal User Account	97
Privilege User Account	83

Table 1

2.1 BruCERT Honey Pot

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

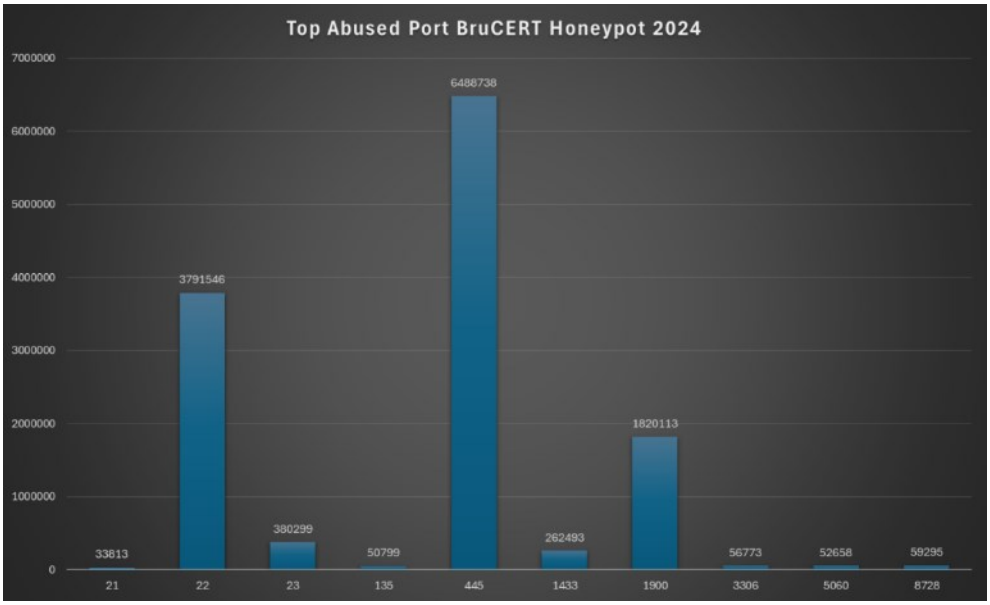


Figure 2

Port No	Count
21	33813
22	3791546
23	380299
135	50799
445	6488738
1433	262493
1900	1820113
3306	56773
5060	52658
8728	59295

Table 2

Reviewing the port abuse data reveals a targeted and nuanced landscape of cyber threats. You can see those certain ports, such as 445 (with over 6.4 million incidents) and 22 (nearly 3.8 million incidents), are not just numbers; they represent common gateways that attackers exploit to compromise SMB and SSH services, respectively. This suggests that if you're managing a network, placing extra emphasis on securing these endpoints with robust patching and multi-factor authentication is essential.

Looking deeper, the significant abuse of Port 1900 (over 1.8 million cases) raises a flag about vulnerabilities in UPnP, which could lead to DDoS reflection attacks. Meanwhile, ports like 23 (Telnet) and 1433 (Microsoft SQL Server) point toward lingering risks in legacy and database services—areas that might consider isolating or upgrading to mitigate potential breaches.

Additionally, the data for ports such as 135, 3306, 5060, and 8728 shows that even services that are perhaps less prominent in public discourse can be valuable targets. These ports are tied into critical areas like RPC communication, MySQL database access, and VoIP and network management vulnerabilities.

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

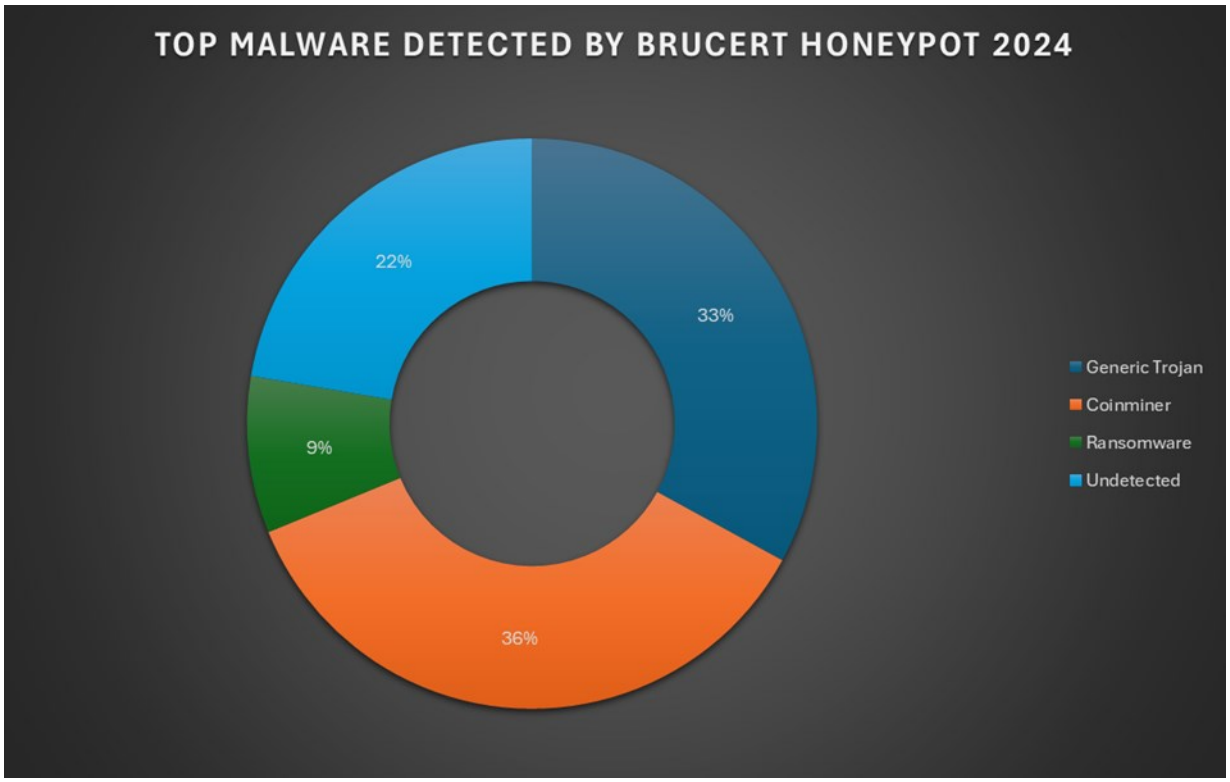


Figure 3

Malware Type	Total
COINMINER	378
GENERIC TROJAN	411
RANSOMWARE	102
UNKNOWN	256
Grand Total	1147

Table 3

The year 2024, BruCERT has been receiving incident reports from the public, including the private sector. Most of these reports pertained to "Scam" activities followed by "Social Media Issues". The former included instances of social media accounts such as Instagram, Facebook, WhatsApp, and Telegram being successfully compromised or taken over, with an increase in such incidents observed in Brunei Darussalam. Compromised social media accounts were often used as part of the "Scamming" activity. There has been a rise in scamming activity for the past three years specifically targeting Bruneians, utilizing local Brunei language and culture. Please refer to Figure 4.

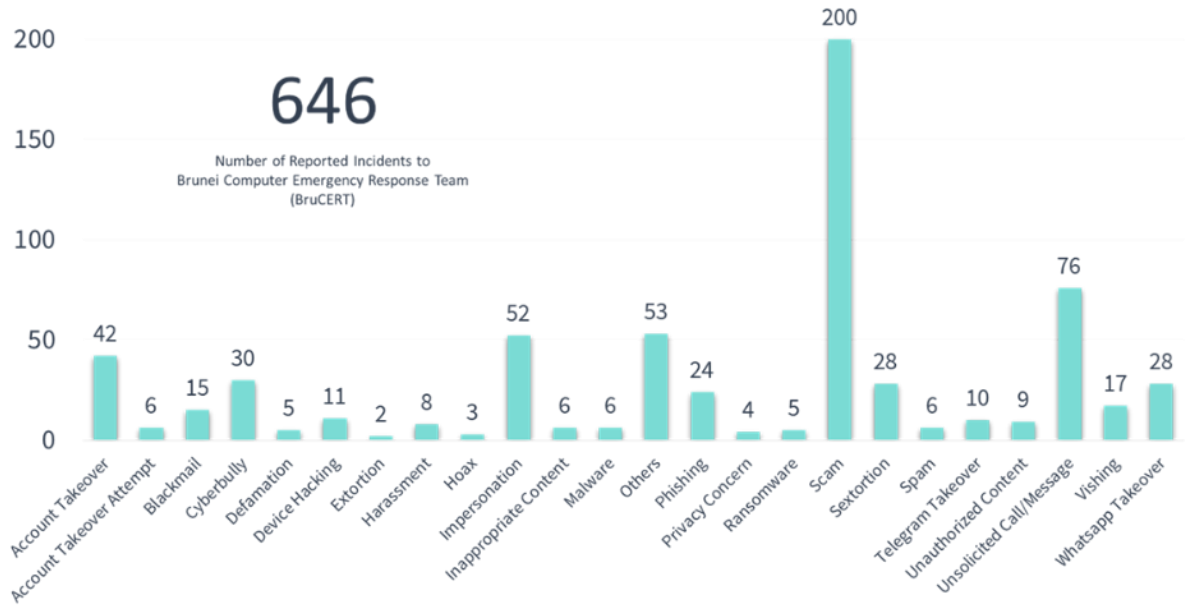


Figure 4

3. BruCERT Activities in 2024

3.1 Seminars/Conferences/Meetings/Visits

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

- From 5th November 2024 until 7th November 2024 – Three BruCERT delegates attended the APCERT AGM and Annual Conference 2024 which takes place at Taipei, Taiwan hosted by TWCERT/CC.
- From 27th October 2024 until 31st October 2024 - Four BruCERT delegates attended the OIC-CERT 11th General Meeting and 16th Annual Conference which takes place at Muscat, Oman. The event is also in conjunction with the 12th Regional Cybersecurity Summit & the FIRST & ITU-ARCC Regional Symposium for Africa and Arab Regions.

3.2 Awareness Activities

Throughout 2024, CSB via BruCERT conducted various awareness-raising activities aimed at educating both the public and public servants about the security threats present in the cyber world. BruCERT main awareness website for this program is www.secureverifyconnect.info, which received an average of 2,622 monthly website visits. Please refer to Figure 5 for BruCERT Awareness infographic activity for the year 2024.

Figure 5

"Rampai Pagi" is a live local interview segment on Friday morning where awareness personnel from BruCERT interviewed and provide insights on various security topics throughout the year 2024.

BruCERT awareness talk which was provided to schools, community as well as corporate/organization also took place almost every month in the year 2023. A total number of 5,048 students, 3,722 personnels from various organizations and 1,763 elderly attended BruCERT awareness talk for the year 2023.

Figure 6

BtCIRT

Bhutan Computer Incident Response Team

1. Highlights of 2024

1.1 Summary of major activities

In October 2024, a significant milestone was achieved in the national cyber security landscape with the launch of the country's first National Cybersecurity Strategy. This historic event coincided with the fourth edition of national cybersecurity week which was observed as part of international cybersecurity awareness month. The strategy marks a pivotal step in strengthening the national cybersecurity framework ensuring a safer and more resilient digital environment for both public and the private sector entities.

1.2 Achievements & milestones

Key activities in 2024 included:

- CIRT maturity assessment, malware analysis workshop and a tabletop exercise were conducted in collaboration with ITU.
- The fourth "Cybersecurity Week" was organized from October 25-27, featuring a range of programs, including a full-day conference, workshops on Application Security, Network Security, and Domain Abuse, as well as an Open Awareness Program. Additionally, awareness content promoting cyber hygiene best practices was shared through the BtCIRT Facebook page.
- Conducted Capture the Flag (CTF) challenge in three ICT colleges in Bhutan in partnership where 118 students participated from 3 technical colleges.
- Launched National Cybersecurity Strategy and drafted Critical Information Infrastructure (CII) Identification methodology.
- Published 83 Alerts and advisories on latest scams and threats.
- Handled a total of 262 incidents.

2. About BtCIRT

2.1 Introduction

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

2.2 Establishment

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

2.3 Resources

As of December 2024, BtCIRT operates with twelve working team members.

2.4 Constituency

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

3. Activities & Operations

3.1 Scope and definitions

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

The specific mandates of BtCIRT are as follows:

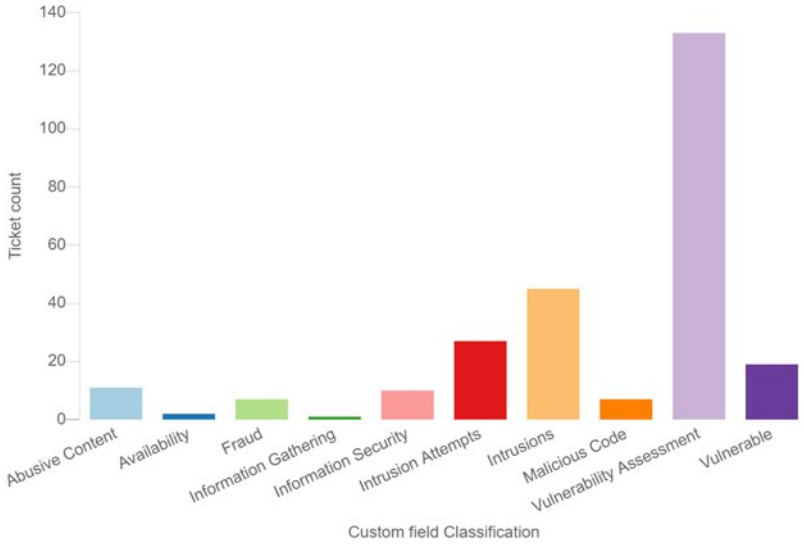
- Operate as a national contact in relation to coordinating and implementing all cyber security issues, plans and

programs.

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

3.2 Incident Handling Report

The incident trend indicates that Vulnerability Assessment (133) is the most recorded category, highlighting a major focus on identifying security weaknesses with proactive interventions. Intrusions (45) and Intrusion Attempts (27) collectively signal ongoing security breach attempts, while Vulnerable (19) cases suggest existing system weaknesses. Other categories like Information Security (10), Abusive Content (11), Malicious Code (7), and Fraud (7) contribute to security concerns but at a lower frequency. Availability (2) and Information Gathering (1) incidents are minimal. The following graph provides the overview of the types of incidents handled:



Custom field Classification	Ticket count
Abusive Content	11
Availability	2
Fraud	7
Information Gathering	1
Information Security	10
Intrusion Attempts	27
Intrusions	45
Malicious Code	7
Vulnerability Assessment	133
Vulnerable	19
Total	262

Figure 1: Incident handled by Incident Classification type in 2024

3.3 Awareness creation programs

Awareness and advocacy is a very important mandate of BtCIRT. A number of awareness programs were implemented in 2024, as described in the following:

3.3.1 Awareness Content Pamphlets

An awareness pamphlet covering cyber hygiene tips was published to be showcased and distributed during the cybersecurity awareness month in October. The topics covered were safeguarding against social engineering and phishing scams, safeguarding accounts and data through password security, updating systems and encrypting data.

3.3.2 Open Awareness Program

The Division had organized a Cybersecurity Open Awareness Program on the 29th of October. This year, the program was targeted at the Kaja Throm and financial institutions, as we had recently observed many people falling victim to OTP sharing and losing money through scams. This program was therefore designed to educate the general public on cyber hygiene and prevalent threats such as phishing and scams.

Figure 2: Desuups training the public on cyber hygiene

3.4 Security Advisory and Alerts

BtCIRT regularly shares the latest cybersecurity news and vulnerabilities to keep its constituents informed about recent developments in the field. In 2024, a total of 83 alerts and advisories on emerging scams and threats were published on its website and Facebook page.

4. Events organized / hosted

4.1 Workshops/ Training

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

4.1.1 Phishing Simulation on 1st October 2024

The phishing simulation was sent to 100 GovTech employees, including interns. Of those, 5 employees opened the email, 2 clicked on the malicious link, and 1 employee submitted sensitive data. Many employees did not open the email during the simulation period because Google flagged it as spam due to domain spoofing being detected.

4.1.2 Half-day cyber hygiene Workshop for new staffs in the GovTech Agency on 4th October 2024

BtCIRT conducted a Half-Day Cyber hygiene Workshop on October 4, 2024. This event marked the start of National Cybersecurity Month observation and was specifically tailored for staff members who joined GovTech in 2024 (including interns, new recruits, and those on lateral transfers from other agencies). The program was also opened to any other individuals interested in refreshing their cyber hygiene knowledge and skills to better protect their online presence.

Figure 3:Participants during the cyber hygiene Workshop

4.1.3 Seminar on cybersecurity by czechia experts (9th - 11th October)

Conducted three-day expert seminar on “National cybersecurity strategies, legal frameworks, and policy challenges”, in collaboration with the National Cyber and Information Security Agency of the Czech Republic (NUKIB), supported by the Embassy of the Czech Republic in New Delhi and the Honorary Consulate of the Czech Republic in Thimphu. The seminar aimed to create an interactive environment for participants to share experiences, discuss challenges, and exchange best practices to strengthen the preparedness and resilience of Bhutanese government institutions against cyber incidents.

Key focused areas were the foundation of NUKIB, Czechia's cybersecurity background, establishing cybersecurity legislation, and future policy challenges. Participants gained new perspectives on implementation of legal approaches and strategies, and attracted cybersecurity talents.

Figure 4:Participants during the seminar on cybersecurity

4.1.4 Technical workshops (22-24 October):

The Cybersecurity technical workshop was conducted on Network Security for more than 20 participants including Network Administrators, Information System Administrators, ICT officers and Data Protection related officers from Private, Corporations and Government agencies .

Figure 5:Participants during the workshop on Network security

4.1.5 Open awareness to public on (29th October):

Organized a Cybersecurity Open Awareness Program on the 29th of October. This year, the program was targeted at the Kaja Throm and financial institutions, as we had recently observed many people falling victim to OTP sharing and losing money through scams. This program was therefore designed to educate the general public on cyber hygiene and prevalent threats such as phishing and scams.

4.2 Drills/Exercises

The following drills were conducted:

4.2.1 Cybersecurity Capture The Flag Challenge (19-20 December)

The Cybersecurity Capture The Flag (CTF) challenge was conducted virtually, engaging participants from three colleges: College of Science and Technology (CST), Jigme Namgyel Engineering College (JNEC) and Gyalpozhing College of Information Technology (GCIT). The Cybersecurity CTF program was designed to cultivate the future cybersecurity workforce of Bhutan. It consisted of a workshop on introducing the basics of cybersecurity on Day 1 and Capture the Flag competition among the colleges on Day 2. The objective of the program was to develop the future cybersecurity workforce of Bhutan.

Figure 6:Participants during the Capture the Flag challenge

5. International Collaboration

5.1 International partnerships and agreements

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

5.2 Capacity building

BtCIRT members have participated in various skills development programs, including training sessions, workshops, and conferences, enhancing their knowledge and expertise. These engagements have also facilitated networking with national and international Cybersecurity/CIRT communities and experts. BtCIRT extends its gratitude to the organizers/sponsors for providing these valuable capacity-building opportunities.

5.2.1 Trainings

BtCIRT participated and benefited from the following international in-person events.

Event	Organizer/Trainer	Region
Global CyberDrill	United Arab Emirates Cyber Security Council (CSC) with ITU	UAE
Defense practice against cyber		
attacks	Knowledge Co-Creation program by JICA	Japan
APC-HUB event on		
Cybercrime Capacity Building	Asia-Pacific Cyber Crime Capacity Building	
Hub secretariat with the Supreme Prosecutors' Office of the Republic of Korea (KSPO)	South Korea	28-31 May, 2024
36th FIRST Conference	FIRST	Fukuoka, Japan
Meridian 16 Conference on CII Protection	National Critical Information Infrastructure Protection Centre (NCIIPC), Government of India	New Delhi, India
Dills and exercises	APCERT	Online
KrCERT APISC Basic Incident Handling Training	Ministry of Science and ICT	Seoul,
South Korea	23-27 September, 2024	

Integrated Cybersecurity for Safer Digital Worlds - Singapore	Singapore Cooperation Program, Govt. of Singapore Singapore

5.2.2 Contribution to Seminars, Conference & Presentations

- BtCIRT participated in the Bhutan Network Operator Group (btNOG) Conference on August 9, 2024, delivering a presentation titled "Updates on BtCIRT." btNOG, an annual event organized by volunteers comprising network, system, and ICT professionals, serves as a platform for knowledge sharing and collaboration.
- On December 2, 2024, BtCIRT conducted an online presentation titled "Experience Sharing on Incident Handling (Facebook)" at the APCERT event hosted by Taiwan CERT. During the session, a BtCIRT representative shared insights on responding to Facebook-related incidents, the challenges encountered in resolving issues, and the support and collaboration received from Meta Inc.

6. Future Plans

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

The future plans for BtCIRT include:

- CII identification and protection
- Finalise National cyber risk assessment(NCRA) methodology and conduct first NCRA
- Strengthening legal frameworks
- Enhancing the SOC and incident response services.
- Strengthen national and international collaboration.

7. Conclusion

In 2024, BtCIRT managed a total of 262 incidents and conducted various cybersecurity programs aligned with its mandates, including capacity development and awareness initiatives for diverse target groups. Moving forward, the implementation of the National Cybersecurity Strategy and the protection of Critical Information Infrastructure will remain key focus areas for 2025.

CCERT

CERNET Computer Emergency Response Team

1. Highlights of 2024

1.1 Introduction

The China Education and Research Computer Network Emergency Response Team (CCERT) is referred to CERNET network security emergency response architecture. The main tasks of CCERT include:

- Network security incidents co-ordination and handling (mainly for CERNET users)
- Network security situation monitoring and information publication
- Technical consultation and security service
- Network security training and activities
- Research in network security technologies

1.2 Establishment

China Education and Research Computer Network Emergency Response Team（CCERT）was founded in May 1999。

1.3 Resources

CCERT sends both security early-warning and notice to users via website(https://www.ccert.edu.cn) and mailing lists, and in the meanwhile, utilize instant messaging technology (such as Wechat and QQ) to communicate with users for fast handling of security events.

1.4 Constituency

CCERT provides quick response and technical support services for network security incidents to China Education and Research Computer Network and its members, as well as other network users.

2. Activities & Operations

2.1 Scope and definitions

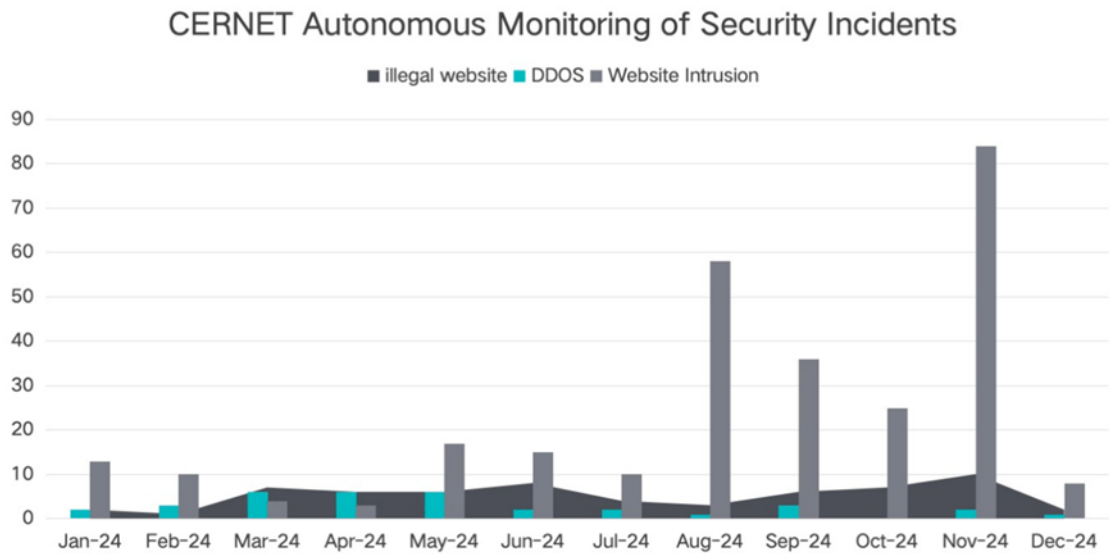
Currently, CCERT mainly deal with security events for CERNET users, which are mainly from:

- CERNET network security monitoring
- Complaint from other CERT organizations
- Information sharing from other security vendors

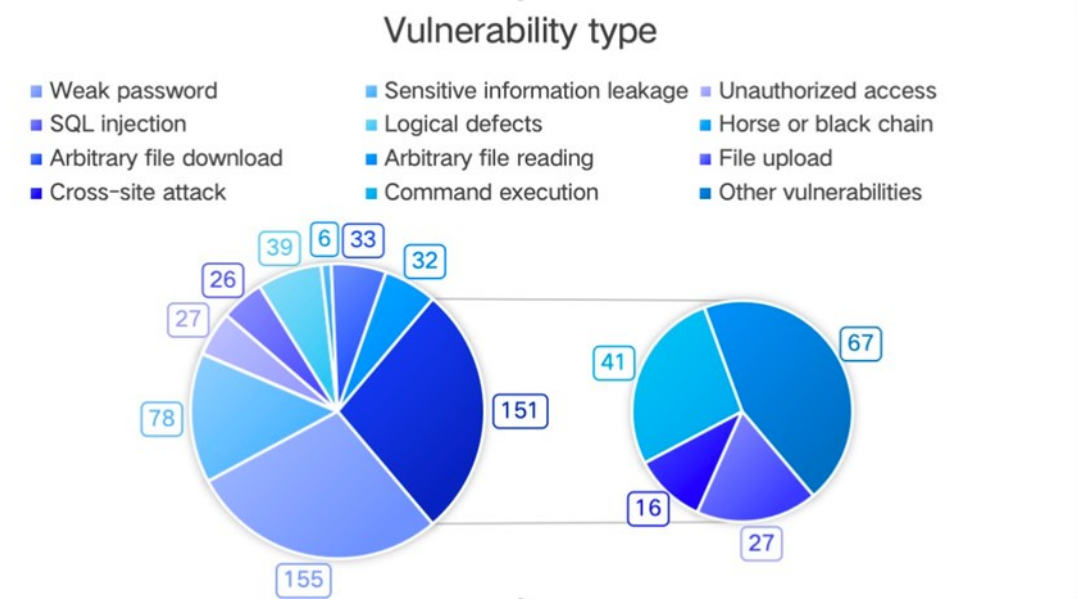
2.2 Incident handling reports

In 2024, CCERT handled a total of 2,573 security incidents related to CERNET users, including 379 incidents detected by CERNET Security Monitoring System, 700 security incidents forwarded from other domestic organization, and 1,493 international complaint incidents.

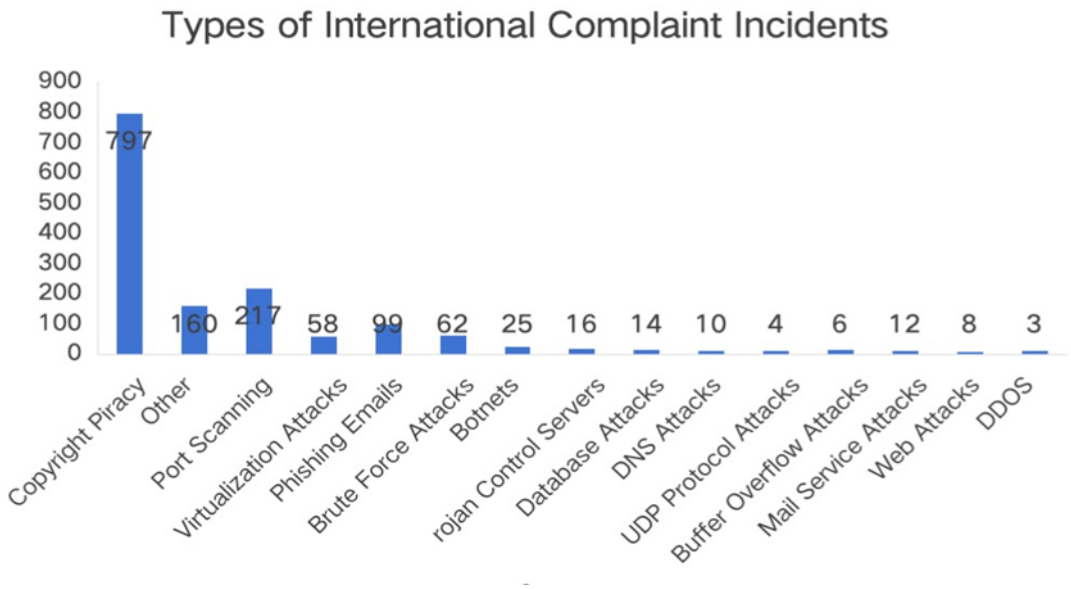
- The security incidents detected by CERNET Security Monitoring System are mainly composed of DDOS attacks, websites with illegal content, and website intrusion attacks.



- The distribution of website security issues is shown below.



- The graph below shows the type statistics of international complaint security incidents.



2.3 Publications

The CCERT regularly publishes weekly and monthly security reports. The weekly reports are sent via email to relevant units every week, while the monthly reports are published in a magazine and automatically pushed through the official WeChat account.

For security bulletins and vulnerability articles published by CCERT, please visit our website https://www.ccert.edu.cn

3. Events organized / hosted

3.1 Training

Organized 3 trainings, which includes:

- Supply Chain Security
- Prevention and Identification of Phishing Emails
- IPv6 Security Configuration

3.2 Drills & exercises

- Participated in two cybersecurity offense and defense drills in the education sector.
- Organized a self-assessment of cybersecurity risk for critical infrastructure.

4. Future Plans

4.1 Future projects

- Strengthen team building for CCERT
- Strengthen the CERNET Security System and Architecture in accordance with the Safety Requirements of Critical Infrastructure

4.2 Future Operation

In 2025, CCERT will continue to focus on cybersecurity emergency response efforts, strengthen cooperation with other security organizations, try to leverage AI technology to enhance security incident detection and response, and make more contribution to Internet security.

CERT-In

Indian Computer Emergency Response Team

1. Highlights of 2024

1.1 Summary of major activities

i. In the year 2024, Indian Computer Emergency Response Team (CERT-In) handled 20,41,360 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 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 959 security alerts, 72 advisories and 360 Vulnerability Notes were issued during the year 2024.

iii. CERT-In conducted 23 cyber security training and awareness programs for Government, Public, Critical Sector organisations to educate them in the area of Cyber Security with the latest security threats, needs and developments & deployment of techniques and tools in order to minimize security risk.

iv. CERT-In conducted 18 domestic cyber crisis exercises in 2024 for various organizations across Sectors and State Government Departments.

v. CERT-In has contributed in planning & scenario development in 2 exercise and participated as a player in 3 International cyber security drills in 2024.

vi. CERT-In contributed and participated in the APCERT Annual Cyber Drill 2024 held on 29th August 2024.

vii. CERT-In contributed & participated in the first BRICS Cyber Drill held in Kazan, Russia from 16th to 9th September 2024.

viii. CERT-In participated in the ACID Drill & TTX on 15th & 16th October 2024.

ix. CERT-In participated in the 4th edition of AFRICA CERT Cyber Drill on 29th November 2024.

1.2 Achievements & milestones

i. CERT-In contributed and participated in the APCERT Annual Cyber Drill 2024 held on 29th August 2024 and played three different roles namely as Exercise Controller (EXCON), as a Player and as an Observer for international CERTs in the Drill.

ii. CERT-In has published Technical Guidelines on Software Bill of Materials (SBOM). This technical SBOM guidelines has been issued for entities, particularly those in the public sector, government, essential services, organizations involved in software export and software services industry in order to improve security, compliance, risk management, supply chain transparency, quality assurance, interoperability, and vendor management in their software development and procurement processes.

iii. Cyber Forensic Lab of CERT-In became India's first Lab to get notified as Examiner of Electronic Evidence within India, with the following scope:
   - Computer (Media) Forensics including Drone Storage Media (excluding Floppy Disk Drive)
   - Mobile Devices Forensics
   - CCTV Forensics Media Recovery (excluding Video Authentication and Enhancement)
   - Cloud Forensics (from premises of Cyber Forensic Laboratory, CERT-In)

iv. CERT-In's initiative to strengthen cybersecurity resilience in Indian cooperative banks featured in the Global Cybersecurity Outlook 2025 report by the World Economic Forum (WEF).

2. About CERT-In

2.1 Introduction

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

ii. CERT-In has been designated to serve as national agency for incident response under Section 70B of the Information Technology Act, 2000 (Amendment 2008). CERT-In operates 24x7 incident response Help Desk for providing timely response to reported cyber security incidents. CERT-In performs the following functions in the area of cyber security:
   - Collection, analysis and dissemination of information on cyber incidents
   - Forecast and alerts of cyber security incidents
   - Emergency measures for handling cyber security incidents
   - Coordination of cyber incident response activities
   - Issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents
   - Such other functions relating to cyber security as may be prescribed.

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 from Government, Public & Private sectors and citizens. In addition, CERT-In provides services to the individuals and home users also.

3. Activities & Operations

3.1 Scope and definitions

CERT-In provides:

- Proactive services such as Advisories, Security Alerts, Vulnerability Notes, sharing of technical information such as Indicators of Compromises (IoCs), Situational awareness of existing & potential cyber security threats and Security Guidelines for helping organizations to secure their systems and networks.
- Reactive services when security incidents occur so as to minimize damage.
- Security Quality management services in the form of cyber security audits, promotion of best practices and cyber security exercises/drills.

3.2 Incident handling reports

The summary of activities carried out by CERT-In during the year 2024 is given in the following table:

Activities	Incidents in 2024
Security Incidents handled	2041360
Vulnerability Notes Published	360
Advisories Published	72
Security Alerts issued	959

Security Drills	21
Trainings Organized	21

Table 1: CERT-In Activities during year 2024

3.3 Abuse statistics

In the year 2024, CERT-In handled 2041360 incidents. The types of incidents handled were Website intrusion & Malware propagation, Malicious Code, Phishing, Distributed Denial of Service (DDoS) attacks, Website Defacements, Unauthorized Network Scanning/Probing activities, Ransomware attacks, Data Breaches/Leaks and Vulnerable Services. The summary of various types of incidents handled is given below:

Security Incidents	2024
Phishing	785
Unauthorized Network Scanning/Probing	1610608
Vulnerable Services	294908
Virus/ Malicious Code	119763
Website Defacements	5496
Website Intrusion & Malware Propagation	1246
Others	8554
Total	2041360

Table 2: Breakup of Security Incidents handled

3.4 Projects and initiatives of CERT-In

3.4.1. Botnet Cleaning Initiatives

Botnet Cleaning and Malware Analysis Centre (Cyber Swachhta Kendra – CSK) has been established by CERT-In for detection of compromised digital devices in India and to notify, enable cleaning and securing systems of end users to prevent further malware infections. The Centre is working in close coordination and collaboration with Internet Service Providers (ISPs), Antivirus companies, Academia and Industry.

Currently, CSK is covering ~98% of the subscriber base for notifications about botnet/malware infection. CSK also provides services for organizations from various sectors including Communications (Internet Service Providers), Finance, Healthcare, Transport, IT & ITeS, Government, Academia, 'Industries & Manufacturing', Energy, Commerce, Infrastructure, 'Information and Broadcasting' and Smart Cities are collaborating and being benefited by using CSK services.

CSK celebrated awareness campaign 'Cyber Swacchhta Pakhwada' from 01-15 February 2024 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. Over 3.18 Lakhs of Downloads were observed during the month of February 2024.

CSK has showcased the team's activities and accomplishments to a wide array of distinguished guests, including CISOs, dignitaries, and other technical and non-technical persons from various ministries/departments during the entire year.

CSK provides three Free Bot Removal Tools (FBRTs) developed in collaboration with "QuickHeal", "K7" and "eScan" with a cumulative of 69.83 lakh downloads recorded till December 2024. These FBRTs are available for Microsoft Windows and Google Android platforms. CSK also provide Mobile Security Application 'M-Kavach 2' for Android platform to users via web portal.

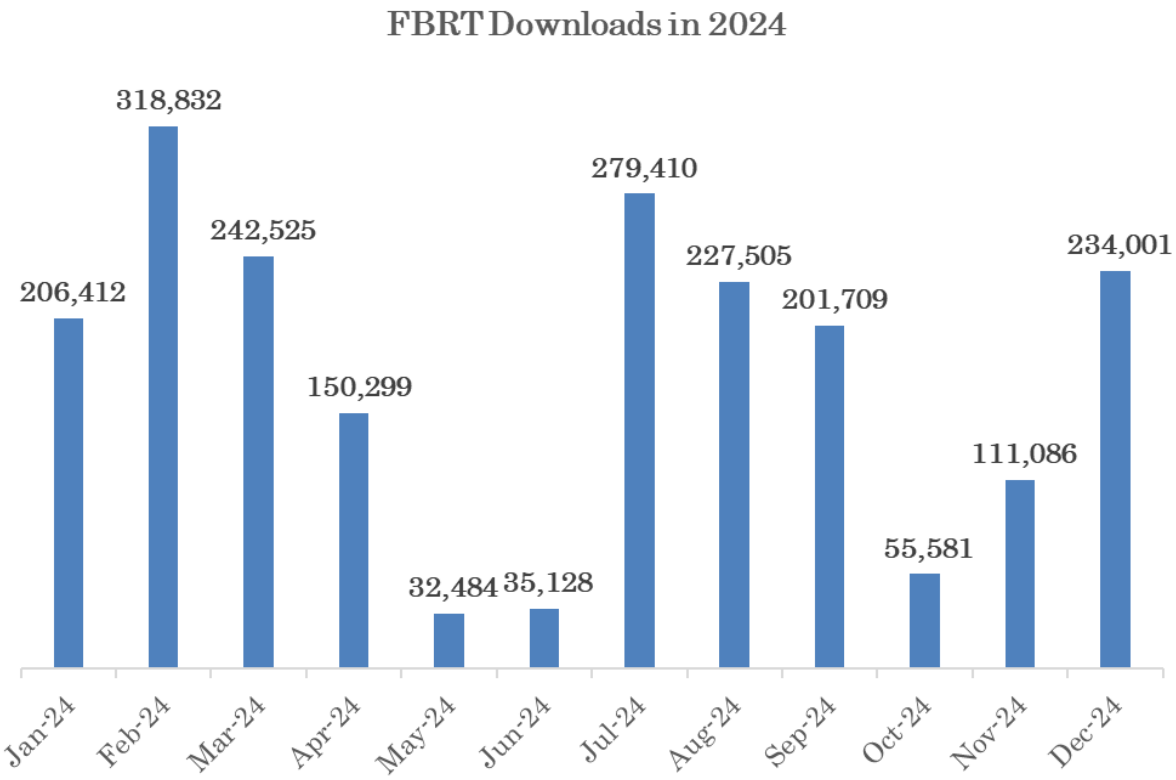


Figure 3: CSK Free botnet removal tools download statistics 2024

3.4.2 Security Profiling, Assurance framework and Audit Services

Under Security Assurance Framework, Indian Computer Emergency Response Team (CERT-In) has created a panel of 'IT security auditing organizations' for carrying out information security auditing, including vulnerability assessment and penetration testing of computer systems, networks & applications of various organizations of the Government, critical infrastructure organizations and those in other sectors of Indian economy.

CERT-In has empaneled 160 Information Security Auditing organizations, on the basis of stringent qualifying criteria, to carry out information security audit, including the vulnerability assessment and penetration testing of the networked infrastructure of government and critical sector organizations. This list of CERT-In empanelled information security auditing organizations is being consulted frequently by the entities in Government and critical sectors for their information security auditing requirements.

CERT-In has implemented data science platform for conducting periodic data analysis on audit findings from across country. The project enabled identification of areas for policy interventions. CERT-In has published Guidelines for Secure Application Design, Development, Implementation & Operations.

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

3.4.3 Cyber Threat Intelligence Sharing

A core part of CERT-In's mission as the first responder with respect to Incident Response and Security Teams is to provide a trusted community platform for sharing cyber threat intelligence and situational awareness. CERT-In releases Indicators of Compromises (IoC's) covering operational, tactical and strategic, alerts, advisories & vulnerability notes to update the Government and critical sector organizations about the existing and potential threats and suitable necessary actions to counter those threats.

CERT-In has operationalised its own Threat Intelligence eXchange platform based on STIX and TAXII standards. This automated platform facilitates bidirectional sharing of operational, strategic, enriched tactical threat intelligence to various counterparts and stakeholders in near real time in automatic fashion, thus helping to build a cyber-resilient ecosystem in the Indian cyber space.

The platform collects, correlates, enriches, contextualizes, analyses, integrates and pushes to the partners in near real time with Traffic Light Protocol (TLP) tags. The shared data can be consumed by the recipients into their automated workflows. This will help to streamline their threat detection, management, analysis and defensive process.

During the year 2024, CERT-In via its email mechanism and with its automatic threat Intel sharing platform- shared 954 Threat Intelligence alerts with the constituency. Chief Information Security Officers (CISOs) of various organizations are getting benefitted by the curated operational and tactical threat intelligence digest shared through an automated platform as well as email covering latest cyber threats targeting Indian Cyber space and enabling proactive mitigation actions.

3.4.4 National Cyber Coordination Centre (NCCC)

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

3.4.5. Cyber Forensics

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

3.4.6. 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 by organizations from around the world that have partnered with the CVE Program. Partners publish CVE Records to communicate consistent descriptions of vulnerabilities. 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.

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 catalogue enable program stakeholders to rapidly discover and correlate vulnerability information used to protect systems against attacks. In an effort towards responsible vulnerability disclosure and coordination process, CERT-In as a CNA has assigned and published a total of 77 CVE IDs during the year 2024.

CERT-In is also a member of APCERT Coordinated Vulnerability Disclosure (CVD) Working Group which is created with the aim to strengthen collaboration among APCERT members and facilitate information and knowledge sharing, enhance CVD cooperation, and promote the efficient adoption of CVD processes in the Asia-Pacific region.

3.5 Publications

3.5.1 Working group reports

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

3.5.2 Technical Guidelines

i. CERT-In has released the technical guidelines on Software Bill of Materials (SBOM) for entities, particularly those in the public sector, government, essential services, organizations involved in software export and software services industry. The guideline is available at https://www.cert-in.org.in/PDF/SBOM_Guidelines.pdf

3.5.3 Awareness Booklets

i. CERT-In released Internet Safety Awareness Booklet for Digital Nagriks and Digital Enterprises during the Safer Internet Day on 06th February 2024 to educate the users on the best practices that needs to be followed for using the internet in a safe and secure manner. The booklet is available online at https://www.cert-in.org.in/PDF/ISA_Booklet.pdf.

ii. CERT-In released a "Cyber security Awareness handbook for Digital Nagriks and Digital Enterprises" during the National Cyber security Awareness Month 2024 to create more awareness on the Cyber security best practices and reporting mechanisms. The booklet is available online at https://www.cert-in.org.in/PDF/CSH_Booklet.pdf

3.5.4 Research Publications

i. "Modern ransomware: Evolution, methodology, attack model, prevention and mitigation using multi-tiered approach" in Security and Privacy. (DOI: 10.1002/spy2.436)

ii. "Exploitation of SQL Common Language Runtime Assemblies: A Novel Attack Vector for Compromising Microsoft SQL Server Environments" published in IEEE Xplore Digital Library. (DOI: 10.1109/ICCCNT61001.2024.10725944)

iii. "AI Phishing Detection Framework for Businesses with Limited Resources" published in IEEE Xplore Digital Library (DOI: 10.1109/3ict64318.2024.10824248)

iv. "Proactive Mechanisms for Turning Smart Buildings to Cyber Smart Buildings in Artificial Intelligence Era" published in IEEE Xplore Digital Library (10.1109/ICAAIC60222.2024.10575761)

v. "Inclusion of Cyber Security Dimension for a Safe, Secure and Trusted E-waste Disposal" published in IEEE Xplore Digital Library (DOI: 10.1109/ISCS61804.2024.10581152)

4. Events organized / hosted

4.1 Training

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

In 2024, CERT-In has conducted 23 trainings on various specialized topics of cyber security. A total of 12014 participants including system/Network Administrators, Database Administrators, Application developers, IT Managers, Chief Information Security Officers (CISOs)/ Chief information officers (CIOs), and IT Security professional have been trained.

As part of services of CERT-In, for creation of awareness in the area of cyber security as well as training / upgrading the

technical knowhow of various stakeholders, CERT-In observed the National Cyber Security Awareness Month (NCSAM) during October 2024 by organizing various events and activities for citizens as well as the technical cyber community in India with a theme of "SatarkNagrik, Secure our World". CERT-In conducted several awareness activities such as Quiz, webinars, Capture the Flag event in collaboration with ISEA, C-DAC, Noida and other industrial partners. Total outreach during the NCSAM 2024 is 2,91,51,000+.

CERT-In also observes "Safer Internet Day" on 1st Tuesday of February Month every year, Swachhta Pakhwada from 1 to 15 February of every year and Cyber JagrooktaDiwas (CJD) on 1st Wednesday of every month for sensitizing internet users on cyber frauds, crimes and safety measures. In 2024, CERT-In has conducted 95 awareness sessions covering 23,724 participants (including NCSAM 2024).

4.2 Cyber Drills & Exercises

Cyber security exercises are being conducted by CERT-In to help the organizations to assess their preparedness to withstand cyber-attacks. These exercises have helped tremendously in improving the cyber security posture of the information infrastructure and training of manpower to handle cyber incidents, besides increasing the cyber security awareness among the key sector organizations. CERT-In has conducted 18 such cyber security exercises in 2024.

Till 31st December 2024, CERT-In has conducted 108 Cyber security exercises of different complexities, including table top exercises, with participation from around 1435 organizations covering various sectors of Indian economy from Government/Public/Private including Defense, Paramilitary forces, Space, Energy, Telecommunications(ISPs), Finance, Health, Oil & Natural Gas, Transportation (Railways & Civil Aviation), IT/ ITeS/ BPO sectors and State Data Centers.

5. International Collaboration

5.1 International partnerships and agreements

Strengthening International cooperation to effectively deal with cyber security issues has been one of the main focus areas of the Government. As such, this aspect is being dealt with by way of security cooperation arrangements in the form of Memorandum of Understandings (MoUs) between Indian Computer Emergency Response Team and its overseas counterpart agencies that are willing to work together and share information in a timely manner for preventing cyber incidents and cyber-attacks as well as collaborating for providing swift response to such incidents.

CERT-In is regularly coordinating with leading service providers and product vendors within and outside the country to obtain advance information on latest cyber threats and attack trends and devise appropriate proactive and preventive measures.

CERT-In is an operational member of Asia Pacific Computer Emergency Response Teams (APCERT). CERT-In is the convener of "IoT Security working group" across APCERT to address security threats and evolve best practices to secure IoT devices.

CERT-In is also member of various other working groups under APCERT such as Information sharing working group, Drill working group, Malware Mitigation working group, Tsubame working group and Training Working Group.
CERT-In is a member of global Forum of Incident Response and Security Teams (FIRST). The membership in FIRST enables incident response teams to more effectively respond to security incidents in a reactive as well as proactive manner
CERT-In is also an Accredited Member of Task Force for Computer Security Incident Response Teams / Trusted Introducer (TF-CSIRT/TI).

5.2 Capacity building

5.2.1 Training

i. CERT-In participated in the JP-US-EU Industrial Control Systems Cybersecurity Week for Indo-Pacific Region in Tokyo, Japan during 12- 15 November 2024.
ii. CERT-In participated in the 2024 APISC Security Training Course hosted by KrCERT/CC during 23-27 September 2024 at Seoul, Korea.
iii. CERT-In participated in the APCERT online training on "Incident Handling" on 30th January 2024.
iv. CERT-In participated in the APCERT online training on "Detecting malicious activities of APT groups in the organization's infrastructure through proactive threat hunting" on 26th March 2024.
v. CERT-In participated in the APCERT online training on "Cyber Security Incident Response - the regulation, statistics, and experience among TW government and CI" on 28th May 2024.
vi. CERT-In officials also participated in the training program on Industrial Control Systems (ICS) cybersecurity (301L) in Idaho Falls, Idaho, USA organized by Cybersecurity and Infrastructure Security Agency (CISA), USA during 12-15 February 2024.
vii. CERT-In officials also participated in the training program on Industrial Control Systems (ICS) cybersecurity (401L) in Idaho Falls, Idaho, USA organized by Cybersecurity and Infrastructure Security Agency (CISA), USA during 23 -25 April 2024
viii. CERT-In participated in the APCERT online training on "Introduction to Threat Intelligence Tools - OpenCTI introduction" on 16th July 2024.
ix. CERT-In participated in the APCERT online training on "Incidents Handling and Ticketing" on 27th September 2024.
x. CERT-In participated in the APCERT online training on "Experience sharing on Social Media Incident Handling by Bhutan Computer Incident Response Team" on 02nd December 2024.

5.2.2 International Drills & exercises

CERT-In has contributed in 2 international exercise planning & scenario development and participated as player in 3 International cyber security drills in 2024. Following are the brief of the exercises:

i. CERT-In contributed and participated in the APCERT Annual Cyber Drill 2024 held on 29th August 2024. The objective of the drill is to test the response capability of leading Computer Security Incident Response Teams (CSIRT) within the Asia Pacific economies.

ii. CERT-In contributed & participated in the first BRICS Cyber Drill held in Kazan, Russia from 16th to 9th September 2024. The theme of the drill was "Attacks on Suppliers (SupChain)". The primary agenda of the drill was to enhance communication and coordination.

iii. CERT-In participated in the ACID Drill & TTX on 15th & 16th October 2024. The theme of the drill was "Navigating the Rise of AI-Enabled Cyber Attacks". The primary objective of this drill was to test incident response processes, best practices to identify areas for further improvement and enhance operations planning capabilities.

iv. CERT-In participated in the 4th edition of AFRICA CERT Cyber Drill on 29th November 2024. The theme of the drill was "Enhance Your Readiness (Technical Exercise)" The drill included various threat simulations, including ransomware attacks, reverse engineering of malware, and strategic scenarios tailored to represent current cyber risks.

5.3 Other international activities

i. CERT-In participated and presented in the CVE/FIRST VulnCon 2024 & Annual CNA Summit during 25-27 March 2024 in Raleigh, USA.

ii. CERT-In officials attended the Forum of Incident Response and Security Teams (FIRST) Annual General Meeting (AGM) 2024 & 36th Annual FIRST Conference held during 10-14 June 2024 at Fukuoka, Japan.

iii. CERT-In participated in the seventh Substantive Session meeting of the UN Open-Ended Working Group (OEWG) on Security of and in the Use of Information and Communications technologies (ICTs) at UN HQ New York, USA during 4-8 March 2024.

iv. CERT-In participated and presented in the World Economic Forum Annual Meeting on Cybersecurity 2024 held during 11-13 November 2024 in Geneva, Switzerland.

v. CERT-In participated and presented in the Singapore International Cyber Week (SICW) 2024 held during 14-17 October 2024 at Singapore

vi. CERT-In participated in the 72nd Task Force for Computer Security Incident Response Teams (TF-CSIRT) Meeting during 25-27 September 2024 in Prague, Czech Republic.

6. Conclusion

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

Contact Information

Postal Address 1:

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

Postal Address 2:

CERT-In Office, Block – 1
Delhi IT Park, Shastri Park
Delhi – 110053, India

- Phone: +91-11-22902703, 22902704

Incident Response Help Desk:

Phone:

- +91-11-24368572
- +91-1800-11-4949 (Toll Free)

Fax:

- +91-11-22902657
- +91-1800-11-6969 (Toll Free)

Incident report to Incident Response Help Desk at:

Email: incident@cert-in.org.in

- User ID: incident@cert-in.org.in
- Key ID: 0xB620D0B4
- Key Type: RSA
- Expires: 2026-12-31
- Key Size: 4096/4096
- Finger Print: A768 083E 4475 5725 B81A A379 2156 C0C0 B620 D0B4

Phone:

- +91-11-22902657
- Toll Free Phone: +91-1800-11-4949
- Toll Free Fax: +91-1800-11-6969

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

Email: info@cert-in.org.in

PGP Key Details:

- User ID:
  - info@cert-in.org.in
  - advisory@cert-in.org.in
  - subscribe@cert-in.org.in
- Key ID: 0x275CCACF
- Key Type: RSA
- Expires: 2026-12-31
- Key Size: 4096/4096
- Finger Print: EABE 086A 6FC4 CB47 3F29 A90B DE30 A071 275C CACF

Email: csk@cert-in.org.in

PGP Key Details:

- User ID: csk@cert-in.org.in
- Key ID: 0x4EE11788
- Key Type: RSA
- Expires: 2025-05-31
- Key Size: 4096/4096
- Finger Print: E204 D43D 0296 40FB 8DB9 0290 706D EF4D 4EE1 1788

Security vulnerabilities can be reported at:

CERT-In Responsible Vulnerability Disclosure Coordination Team

Email ID: vdisclose@cert-in.org.in

- Key ID: 0x3B4E082C
- Key Type: RSA
- Expiry Date: 2026-12-31
- Key Size: 4096/4096
- Fingerprint: 6927 2217 D8D4 0208 6B1C 23E9 CE29 EA67 3B4E 082C
- Toll Free Phone: +91-1800-11-4949
- Toll Free Fax: +91-1800-11-6969

- PGP Key information available at https://www.cert-in.org.in/RVDCP.jsp

For International Liaison activities

Email: international@cert-in.org.in

PGP Key Details:

- User ID: international@cert-in.org.in
- Key ID: 0xECCB2102
- Key Type: RSA
- Expires: 2025-05-31
- Key Size: 4096/4096
- Finger Print: 0A71 3343 F7E2 A8D7 09FA A71E 9ED3 D110 ECCB 2102

CERT PH

Philippines National Computer Emergency Response Team

1. Introduction

The Philippine 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.

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

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

1.1 NCERT Core Functions

1.1.1 Incident Response

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

1.1.2 Vulnerability and Penetration Testing

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

1.1.3 Security Operations Center

- Provides technical details and analysis of discovered vulnerabilities and criticality to system owners.
- Ensures the continuous operation of the National SOC, its 24/7 monitoring and response, secure end-point access, protection against DNS-base attacks, and the reputation of connected agencies.

- serves as the centralized facility for detection, monitoring, and rapid response to security incidents in the connected agencies.
- Monitors the system for possible information security threats and injects countermeasures and remedies.

1.1.4 Cyber Threat Monitoring

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

2. CERT-PH Operations and Delivery of Frontline Services

2.1 Incident Response and Handling

From January 1 to December 31, 2024, NCERT managed a total of 2,855 cybersecurity incidents across various critical infrastructure sectors in the Philippines. Based on the data, Government and Emergency Services had the highest number of incidents recorded, making up 55.3% of the total, which is significantly more than any other sector. The academe, with 25.5%, recorded the second-highest number of incidents. Telecommunications followed with 7.3%. These three sectors combined account for the majority of incidents. Healthcare, transport and logistics, banking, and other sectors reported fewer incidents.

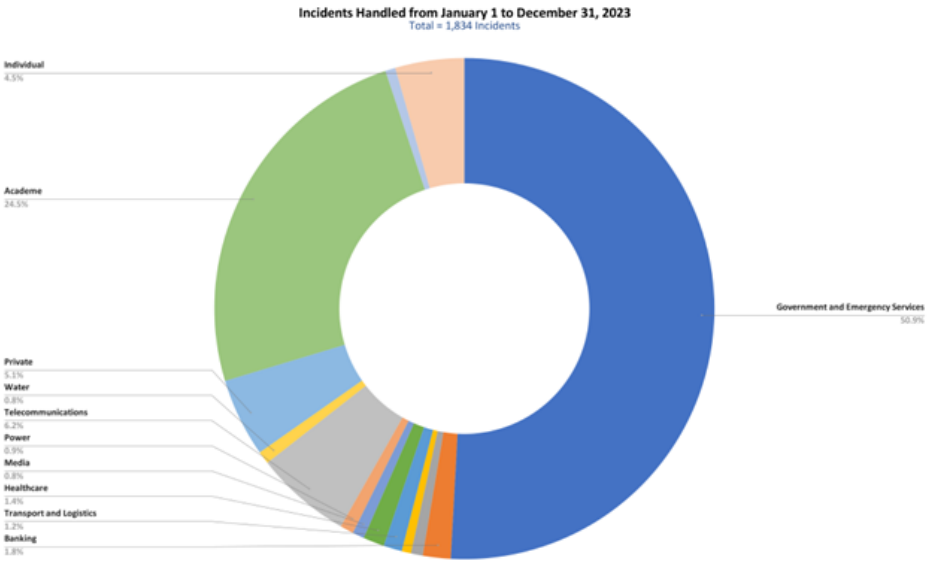


Figure 1. Incidents per Attack Category

The most significant incident type recorded was Data Exfiltration/Data Leaks, which accounted for 44.4% of the total incidents, with 1,266 cases. Following this, Compromised Websites and Systems represented 19.0% of the total, with 542 incidents, and Malware and Malicious Files made up 21.8%, totaling 621 incidents. Brute-force Attacks and APT Attacks were also notable, comprising 5.2% (148 incidents) and 2.1% (60 incidents) respectively.

Other types of incidents included Unauthorized Scanning with 0.4% (12 incidents), DDOS attacks at 2.1% (60 incidents), Email Attacks at 0.5% (14 incidents), and Server, Network, and Infrastructure Related Attacks at 1.6% (45 incidents). Technical Assistance requests made up 3.1%, with 87 incidents. These percentages highlight the diverse range of cyber threats, with data-related incidents being the most prevalent.

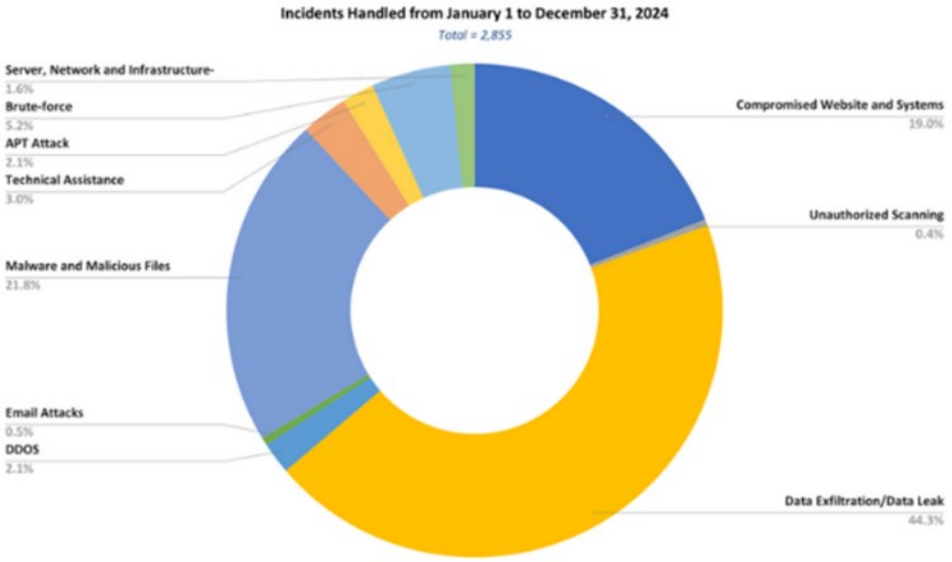


Figure 2. Types of Attacks

Meanwhile, the number of incidents handled each month varied significantly throughout the year. January recorded 375 incidents, the highest of the year, followed by a slight increase in February with 398 incidents. March saw a decrease to 282, and April had 325 incidents. May recorded 188 incidents, which was the lowest up to that point, and June followed with 146 incidents, continuing the downward trend. July had the lowest number of incidents for the year at 109. August experienced a rise to 251 incidents, and September saw a decrease to 133. October returned to a higher count with 376 incidents, while November dropped to 169. December ended the year with the fewest incidents at 103. This distribution shows fluctuations in the number of incidents handled each month without a consistent upward or downward trend.

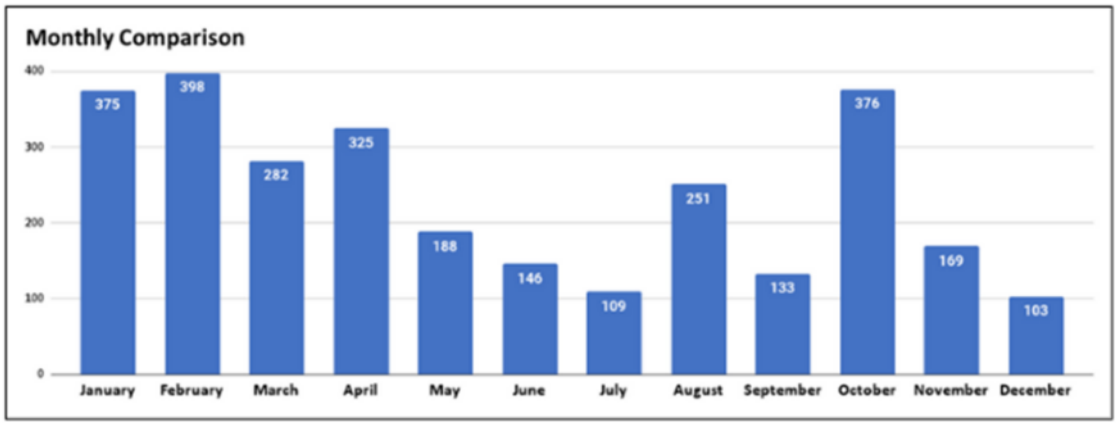


Figure 3. Monthly Comparison

Summary Of Achievements

- Responded to incidents with an average time of 7 minutes, exceeding the target of 90 minutes.
- Successfully conducted 20 cyber range exercise training sessions for various government agencies and regional offices nationwide.
- Expanded Points of Contact (POC) database, streamlining communication and response efforts.
- Facilitated numerous tabletop exercises to strengthen incident response management and coordination.
- Enhanced onsite response capabilities, ensuring faster mitigation and support.

2.2 Vulnerability Assessment and Penetration Testing

Number Of Accomodated Requests For Vapt

For the year 2024 (January-December), the NCERT has received and accommodated a total number of 94 requests from various Government Agencies and Instrumentalities.

Of these requests, vulnerability assessment and penetration testing services were conducted to a total of 1,034 web applications, network and source code to discover any existing attack vectors that could be used by adversaries for potentially compromising the overall security, privacy, and operations of the Government and other Cybersecurity Bureau stakeholders. This also includes proactive engagements with various stakeholders.

Additionally, NCERT conducted VAPT remotely and on-site on multiple platforms (Web App, Network, Mobile App, and Source Code) of various government agencies.

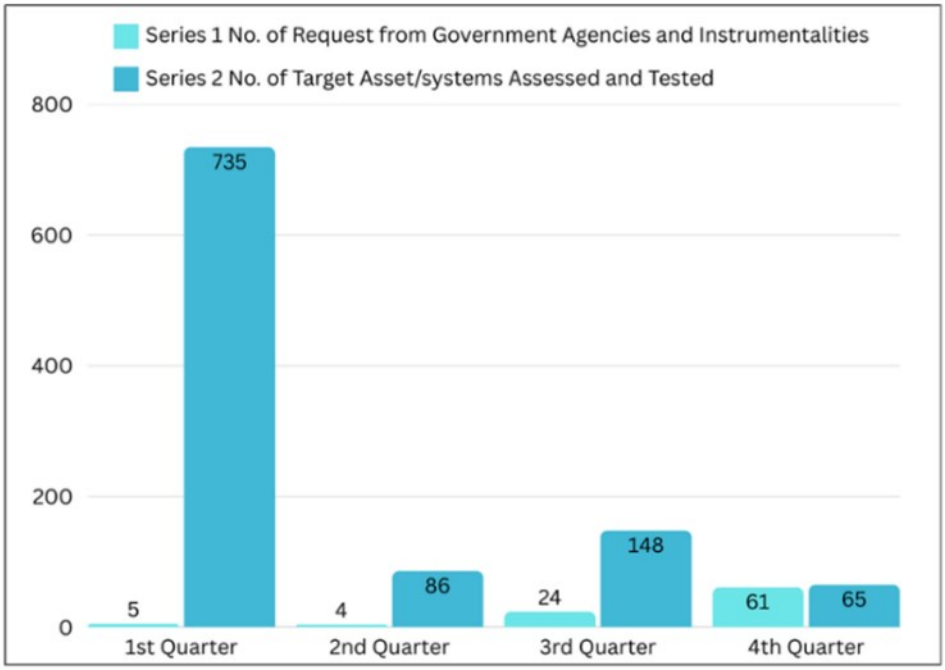


Figure 4. No. of Accommodated Request for VAPT

Project Secure Online Network Assessment And Response System (SONAR)

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

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

In 2024, NCERT has conducted automated vulnerability assessment to approaching 3000 website/web applications of 1,221 government agencies and instrumentalities, identifying more than 400,000 vulnerabilities.

2.3 National Security Operations Center

Deployment Overview

NSOC successfully achieved its goal of connecting to thirty (30) national government agencies in 2024.

Building on this success, NCERT aims to expand its coverage to 50 agencies in 2025 to strengthen further the government's defense against the ever-evolving cyber threat landscape.

Connected Agencies

The NSOC integration in 2024 encompassed additional ten (10) government agencies and institutions, each with critical information assets relative to national security, public safety, regulatory compliance, economic stability, and executive governance.

Security Metrics

Among the 30 agencies, 28 are seamlessly operational within the NSOC framework, demonstrating seamless coordination and collaboration across multiple sectors.

Furthermore, significant progress has been achieved in reinforcing the security posture of these agencies. Rigorous cybersecurity measures have been implemented to ensure protection of data and continuity of operations.

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

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

Ticket Status

In 2024, NSOC handled a total of 4,101 tickets, highlighting the system's comprehensive nature and the increasing volume of incidents managed.

The huge leap in the number of tickets from 2,076 in 2023 could be attributed to enhanced visibility brought by the expanding coverage of NSOC by deploying to more government agencies and institutions.

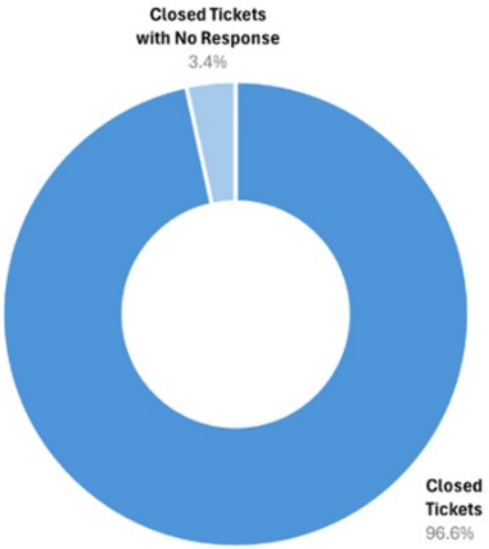


Figure 5. Percentage of Closed Tickets with No Response and Closed Tickets

With 3,837 tickets closed, NSOC demonstrated efficiency in monitoring and mitigating the incident. The 274 tickets closed with no response signify the incident cases that were closely monitored and reached the maximum follow-up threshold, highlighting the section's commitment to resolving the detected incidents.

Incident Case Severity

As for the severity classification of resolved incidents, NSOC handled a total of 1,750 low-risk cases, followed by 1,671 medium-risk, 639 high-risk, and 41 critical-risk cases.

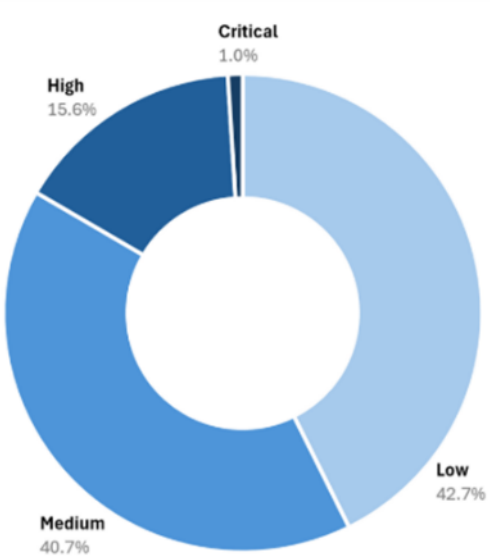


Figure 6. Severity Classification of Resolved Incidents

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

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

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

Protective Domain Name System (Pdns)

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

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

In 2024, PDNS processed an average of 210 million DNS queries per month and blocked an average of 450,000 malicious queries, resulting into the following:

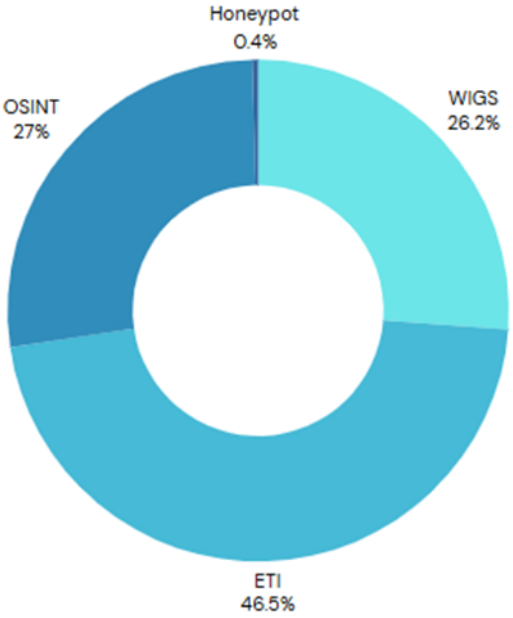
- **2.52B** DNS queries processed for the year
- **5.4M** Malicious queries blocked for the year

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

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

2.4 Cyber Threat Monitoring and Information Sharing

Throughout the period spanning January to December 2024, a comprehensive tally of
2,544 monitored threats was meticulously documented. The vigilant efforts of NCERT were channeled through multiple platforms, showcasing the organization's robust approach to threat intelligence.



Monitoring Sources

- Web Information Gathering System (WIGS): 663 Threats
- External Threat Intelligence System (ETI): 1175 Threats
- Open Sources: 682 Threats
- Honeypot and other Sources:

Type Of Threats Monitored

- Vulnerabilities
- Malware
- Alleged Data Leaks
- Website Defacement

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

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

Threats Feeds And Advisories

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

Summary Of Achievements

- Assisted the CII for immediate resolution of Monitored Vulnerabilities
- Provided 2544 monitoring reports for various CII sector

- Delivered 277 Cyber Threat and Intel Advisories and Feeds to CII
- 3,329 agency assets were monitored

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

3.1 HackforGov Capture the Flag Competition 2024

The program successfully launched in May 2024, bringing together 20 teams from state universities and colleges (SUCs) across the National Capital Region. Building on this momentum, regional qualifying rounds were held across 15 regions from June to September 2024, showcasing remarkable coordination and participation. The program achieved impressive engagement, with a total of 886 participants representing 142 SUCs nationwide.

On October 4, 2024, the nation's brightest students showcased their cybersecurity talents in the much-anticipated HackforGov: Cyber Challenge Competition. The event took place at the Sequoia Hotel Manila Bay in Parañaque, where a total of 20 elite teams from various regions across the Philippines competed for the prestigious title of National Champion.

This year's participants improved their problem-solving and technical skills compared to last year as reflected in their higher scores. Team Unit GG of the New Era University emerged as the national champion setting a record high of 3,560 points.

Following closely behind is the Wildcard Team shellShocked() won 1st runner-up with 3,411 points, while Team Cyb3rKn1ght$ of the Ateneo de Davao University placed 2nd runner-up with 3,220 points.

The winning team represented the country at prestigious international events such as the ASEAN - Japan Cybersecurity Capacity Building Centre (AJCCBC) Cyber Sea Games in Bangkok, Thailand.

This year's theme, "Today's Generation, Tomorrow's Champion: Shaping the Future of Cybersecurity through Shared Responsibility," underscored the government's commitment to fostering a secure digital environment.

It emphasized the importance of inclusivity and collaboration in addressing the complex challenges posed by cyber threats. By promoting shared responsibility, HackforGov aimed to empower participants to not only safeguard their own digital lives but also to contribute to the broader cybersecurity landscape.

Throughout the event, students demonstrated their cybersecurity skills within the Capture-the-Flag (CTF) platform, a competitive environment that simulated real-world cybersecurity scenarios. Participants engaged with a series of challenges designed to test their technical abilities, critical thinking, and problem-solving skills in various domains of cybersecurity.

3.2 Conduct of Cybersecurity Drills and Simulation Exercises

Philippine CERT Conference (CERTCON) 2024

Successfully conducted the 2nd Annual Philippine CERT/CSIRT Conference (CERTCON) 2024. CERTCON 2024 aims to address pressing cybersecurity challenges and foster collaboration across the nation. This year's theme, "Reinforcing RelationCERTS: Inclusivity and Resiliency in Cybersecurity," underscores the significance of partnership, diversity, and adaptability in responding to the ever-evolving cyber threat landscape.

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

As cybersecurity threats continue to evolve, CERTCON 2024 serves as a vital platform for knowledge sharing, skill enhancement, and the development of a unified response to cyber incidents. The DICT invited all media representatives to cover this important event and join in the efforts to create a safer, more inclusive, and resilient cybersecurity landscape for the Philippines.

This event brought together a diverse group of participants from various government agencies and the cybersecurity

community, to address pressing cybersecurity challenges and fostering collaboration across the nation. The conference featured a series of engaging workshops, presentations, and interactive sessions, all led by industry experts. These sessions focused on critical topics such as threat intelligence, digital forensics, and the development of effective security policies. The discussions provided participants with a deeper and more comprehensive understanding of contemporary cybersecurity issues, which is crucial in the face of an ever-evolving threat landscape.

3.3 Cyber Range Exercises

In a proactive effort to enhance cybersecurity readiness and collaboration among various government agencies, a series of Cyber Range exercises were conducted over the course of the year. These exercises, totaling 20 sessions, brought together a diverse group of **764 individuals from different government agencies**.

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

The collaborative nature of the exercises fostered knowledge sharing and cross-agency cooperation, ensuring that each participant gained valuable insights into the latest cybersecurity challenges. As a result of these Cyber Range exercises, the participants not only honed their technical skills but also established a network of contacts across government agencies, laying the groundwork for improved coordination in the event of a real-world cyber incident. The commitment to regular training and collaboration demonstrated a collective dedication to maintaining a robust and resilient cybersecurity posture across the government sector.

3.4 Tabletop Exercises Conducted by NCERT

From January to December 2024, the National Computer Emergency Response Team (NCERT) conducted six (6) tabletop exercises (TTXs), engaging 644 participants from government agencies, critical information infrastructure (CII) operators, and private sector organizations.

These exercises simulated real-world cyber incidents to enhance coordination, decision-making, and incident response capabilities. Through these sessions, NCERT strengthened collaboration, identified areas for improvement, and reinforced best practices to bolster national cybersecurity resilience.

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

3.5.1 APCERT (Asia Pacific Computer Emergency Response Team)

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

3.5.2 TWNCERT (Taiwan Computer Emergency Response Team)

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

3.5.3 CAMP (Cybersecurity Alliance for Mutual Progress)

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

3.5.4 SingCERT (Singapore Computer Emergency Response Team)

NCERT collaborates with SingCERT through the sharing of information on the evolving threat landscape. NCERT also participates in SingCERT's activities, including webinars and trainings, and cyber Drill contributing to mutual efforts aimed at addressing emerging cyber threats and improving cybersecurity resilience.

3.5.5 AJCCBC (ASEAN-Japan Cybersecurity Capacity Building Centre)

NCERT collaborates closely with AJCCBC in various capacity-building initiatives focused on enhancing cybersecurity skills and knowledge. These activities include specialized trainings, joint exercises, and participation in programs aimed at

developing cybersecurity professionals within ASEAN. NCERT also engages in information sharing with AJCCBC on current and emerging cyber threats, contributing to a broader regional effort to strengthen cybersecurity resilience across the ASEAN region.

3.5.6 Counter Ransomware Initiative

The Annual International Counter Ransomware Initiative (CRI) Gathering is a global forum that brings together representatives from various countries and sectors to collaborate on strategies to combat ransomware attacks. The gathering emphasizes information sharing about recent threats, discusses best practices for prevention and recovery, fosters international partnerships, and explores the role of emerging technologies such as Artificial Intelligence (AI) in strengthening cybersecurity. Over the coming year, the coalition plans to offer rapid assistance to CRI members affected by ransomware attacks targeting their governments or critical sectors, continue sharing actionable information with partners, and enhance cyber capacity building through mentorship for new members and tactical training.

3.5.7 UAE Cybersecurity Council

With the recent invitation from the UAE Cybersecurity Council, this marks the beginning of a collaborative effort to enhance cybersecurity measures and best practices, adapting key initiatives from Middle Eastern countries.

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

CERT Tonga

Tonga Computer Emergency Response Team

1. Highlights of 2024

1.1 Summary of major activities

2024 was a year of reviewing and mainly focused on Capacity Building with the implementation of the amended Cyber Security Workforce Development Program (CWDP). Other major events were the 53rd Pacific Islands Forum Leaders Meeting (PIFLM53) that was hosted in Tonga in August 2024. Which resulted in the collaboration with the Digital Transformation Department (DTD), CERT Tonga and the Australian Pacific Cyber RAPID (Ready to Assist Pacific Islands Disaster) Team (DFAT) consisting of Deloitte Cyber (Deloitte Technology and Transformation).

1.2 Achievements & milestones

On 14 December 2023, the Council of Europe (CoE) and European Union (EU) selected Tonga (Ministry of MEIDECC) to participate as one of the hub countries (one of eight hub countries) in the Global Action on Cybercrime Enhanced (GLACY-e), for enhancing regional capacity building on cybercrime and electronic evidence, duration until January 2026. CERT Tonga acts as the secretariat for the hub country national team (composed of Tonga Police, Attorney General's Office and Ministry of MEIDECC) in January 2024 to the Pacific Region.

On September 2024, CERT Tonga was selected and achieved the 2024 Information Society Innovation Fund (ISIF) Asia Award for outstanding Digital Development Contributions: Protecting Tongan Internet users online, during the APNIC58 Conference back-to-back with the Pacific Internet Governance Forum 2024 (PacIGF2024) in Wellington, New Zealand.

On October 2024, CERT Tonga completed the Outer Islands Outreach cyber awareness raising campaign that started in April 2023 to the main Island groups of Tonga, finishing with the Vava'u Island (Northern Is.) groups.

2. About CSIRT/CERT

2.1 Introduction

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

2.2 Establishment

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

Vision

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

Mission

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

2.3 Resources

CERT Tonga reviewed and amended its organizational structure to comprise of three divisions (governance, risk management and compliance (GRC) (amended from oversight with compliance); communication, awareness and engagements (CAE) (amended from coordination and communication), and Digital Forensics and Incident Response (DFIR) (amended from vulnerability detection with incident response and forensic analysis divisions (i.e. technical)), it is still with three established staff (Director, Senior Engagement Officer, and Security Analyst), five(5) contracted staff under the CERT Tonga Cyber Security Workforce Development Program (CWDP) funded by CERT NZ (Secondment and Internship). The volunteer program for young enthusiasts willing to gain working experience and apprenticeship with career in cybersecurity still stands, however there was no volunteer in 2024. The Information Department was no longer under CERT Tonga's caretaker. Hence the Media Division Staffs disbursed by either secondment, study leave or absorbed by CERT Tonga as a permanent staff.

2.4 Constituency

CERT Tonga's constituents are Government Ministries, the Private Sector, and the Public Enterprises as well as Non-Government Organizations (NGO).

3. Activities & Operations

3.1 Scope and definitions

As mandated in the TOR of HM CD 15th July 2016, CERT Tonga aims to:

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

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

Engagements

Engagements with Domestic, Regional, and international organizations and committees are managed and fit for purpose to assist CERT Tonga in carrying out its function.

Proactive Services

Maintaining proactive services (awareness raising, trainings, security bulletin and advisories) to ensure cyber threats are mitigated and cyber incidents prevented.

Reactive Services

Be prepared with reactive services (incident response SOPs and best practices) to ensure that the impact of cyber incidents is contained, investigated, mitigated, and restored back to normal services.

Digital Forensic Services

From time to time, providing digital forensic analysis services to the Tonga Police when requested to assist them. To enable their obtaining of digital evidence for investigation and battling cybercrime.

Administration and Management

Relevant administrative and support services are provided to ensure that the department can deliver its intended output, and with its collaboration with other departments of the Ministry of MEIDECC.

3.2 Incident handling reports

Throughout the year, occasional reports of malicious IP address activities from third parties scanning services. Phishing and fraud cases were also detected, several digital forensics assistance to the law enforcement (Tonga Police) throughout 2024. However, no major incidents reported or detected in Tonga, together with the assistance of Cyber RAPID Team (DFAT) to ensure the PIFLM53 went smoothly and securely.

3.3 Publications

As a result of the collaboration (Cyber Task Force) with the Cyber experts (Deloitte, Cyber RAPID Team) from Australia prior to and during the 53rd Pacific Islands Forum Leaders Meeting (PIFLM53), the Cyber Risk Assessment (July 2024) and Cyber Incident Response Plan (August 2024) was developed for this purpose. It was the playbook and guidance for the Command Post (CP) battle rhythm and routines during the significant event (PIFLM53), which the Government of Tonga gets to host once in every eighteen years.

4. Events organized / hosted

4.1 Training

4.1.1 USAID DCCP Cyber Hygiene Training – 20th June 2024

CERT Tonga was grateful for the support from USAID Pacific Islands through USAID Digital Connectivity and Cybersecurity Partnership Pacific Activity to equip participants with practical knowledge and best practices to safeguard against cyber threats.

Top: Opening of the USAID DCCP Workshop and Bottom: Cyber Hygiene Training on June 20 at Fe'ao Moe Ngalu, Customs Building at Ma'ufanaga, 2024.

4.1.2 Cybersecurity Awareness to the Ministry of Internal Affairs Social Protection & Disability Division, February 2024.

4.1.3 Tonga Women in ICT (TWICT) ICT Expo, March 21-22, 2024

4.1.4. Outer Island Outreach to Vava'u Islands: Cybersecurity Awareness Raising Campaign, October 8 – 14, 2024.

CERT Tonga completed the Outer Islands Outreach Program of Cybersecurity Awareness Raising during the Cyber month of October 2024. Covering seven (7) secondary schools, community and church youth, NGOs and Women's groups, and Government line of Ministries.

4.2 Drills & exercises

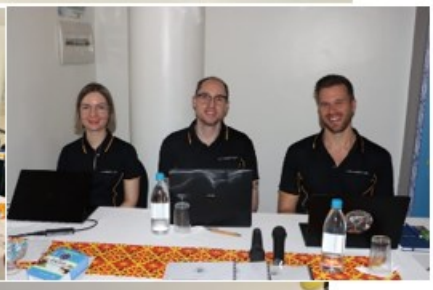
4.2.1 Cyber Task Force RAPID Team Risk Assessment and Incident Response Plan (drill) implementation prior (24 – 26 July 2024) to and during the PIFLM53 (19 – 31 August 2024).

4.2.2 Defensive Readiness and Cyber Security Exercise Program to strengthen Tonga's Emergency Response Capacity and Preparedness 16th – 20th September 2024

More than 50 participants from line ministries, Internet service providers and private sector will be attending the Defensive Readiness and Cyber Security Exercise Program, co-hosted by Tonga Computer Emergency Response Team (CERT Tonga) under the Ministry of MEIDECC and Retrospect Labs through the Australian Department of Foreign Affairs and Trade (DFAT). The program will focus on several fundamental principles and common protocols for responding to cyber security incidents. And an interactive cyber security exercise where participants are required to be a part of an

Incident Response team dealing with a ransomware case at a fictional company. A realistic scenario has been designed and crafted to simulate an actual incident response operation, providing offline files and live elements for the participants to interact with.

{retrospect_labs}



Top: Opening of the Defensive Readiness and Security Exercise with distinguished guests and Center: The Retrospect Labs facilitators on June 16 at Tanoa International Dateline Hotel (Tonga) at Fasi-Moe-Afi, 2024.

4.3 Conferences and seminars

- Cyber Awareness Challenge 2024 by the DoD Cyber Exchange Online Training on 26 January 2024.
- Train-the-Trainer Cybersecurity Workshop by the United States Department of State, Online Training (Virtual Classroom) from 24 -26 July 2024.

5. International Collaboration

5.1 International partnerships and agreements

Tonga was selected to be one of the hub countries (the regional hubs for capacity building in the Global Action on Cybercrime enhanced (GLACY-e) project (the other hubs are Chile, Dominican Republic, Ghana, Mauritius, Philippines, Senegal, Sri Lanka and Tonga).
The final implementation of the Cyber Security Workforce Development Program after review and amendment of the original agreement in 2021 between CERT Tonga and NCSC NZ.

5.2 Capacity building

5.2.1 Training

- Fostering the Digital Economy through AI and Data Governance (JSPP21) Course from 26 February to 1 March 2024 in Changi, SINGAPORE.
- Integrated Cybersecurity for Safer Digital Worlds (SCP) Course from 11 – 15 November 2024 in Changi, SINGAPORE.
- Basic Investigation of Computer & Electronic Crimes Program (BICEP) – ILEA from 9 – 13 December 2024 in Bangkok, THAILAND.

5.2.2 Drills & exercises

- Commonwealth Heads of Government Meeting (CHOGM), CERT Tonga was part of the 2024 Technical Team (with other members from the national CERTs in the South Pacific region)

5.2.3 Seminars & presentations

- **ICANN 79 Community Forum** from 2 – 7 March 2024 in San Juan, PUERTO RICO. CERT Tonga was an ICANN 79 Fellow.
- **2nd Japan Pacific Islands Defence Dialogue (JPIDD)** hosted by JMOD from 19 – 20 March 2024 in Tokyo, JAPAN. CERT Tonga was part of the delegation from Tonga.
- **UN ESCAP 80 Commission** from 22 – 26 April 2024 in Bangkok, THAILAND. CERT Tonga was part of delegations from Tonga.
- **USAID Digital Connectivity and Cybersecurity Partnership (DCCP) Pacific Sub-regional Workshop** from 21 – 24 May 2024 in Suva, FIJI. CERT Tonga was part of the delegation from Tonga.
- **ICANN 80 HLGM & Policy Forum** from 9 – 13 June 2024 in Kigali, RWANDA. CERT Tonga was the delegation from Tonga (Alternative GAC representative).
- **36th FIRST Annual Conference** from 9 – 15 June 2024 in Fukuoka, JAPAN. CERT Tonga attended.
- **3rd EU-Japan Strategic Communications Practitioners' Seminar on Countering Information Manipulation and Interference in Elections: Cross Regional Comparisons and Lessons Learned**, from 27 – 28 June 2024 at the University of Tokyo Strategic Communications Education and Research Unit (SCERU) Tokyo, JAPAN. CERT Tonga was one of the invited participants from the South Pacific region.
- **World Bank Group's (WBG) Cybersecurity Technical Deep Dive (TDD)** from 22 – 26 July 2024 in Tokyo, JAPAN. CERT Tonga was part of the delegation from Tonga.
- **Pacific Internet Governance Forum 2024 (PacIGF2024)**, Pacific Islands Chapter of Internet Society (PICISOC) and APNIC Conference #58, from 1 – 7 September 2024 in Wellington, NZ. CERT Tonga was invited to the events as well as to receive the ISIF 2024 Asia Award.
- **Pacific Cyber Security Operational Network (PaCSON) Annual General Meeting (AGM), back-to-back with the Pacific Cyber Capacity Building and Coordination Conference (P4C)**, from 9 – 13 September 2024 in Rarotonga, COOK IS. CERT Tonga members attended these events.
- **APCERT AGM** from 6 – 8 November 2024 in Taipei, TAIWAN. CERT Tonga joined the APCERT AGM.

6. Future Plans

6.1 Future projects

- CERT Tonga continues managing, collaborating, and implementing the projects with the Cyber Security Workforce Development Program with CERT NZ. CERT Tonga hopes to develop its own cybersecurity infrastructure to collect data and analyzed for first-hand information to detect vulnerabilities and threats to the critical infrastructure networks of the kingdom of Tonga.
- CERT Tonga also continues to collaborate with APNIC on a Project that looks into setting up a mini–Security Operation Center (SOC) for CERT Tonga which will help with CERT Tonga's Operation.

6.2 Future Operation

CERT Tonga hopes to work closely with the Internet Corporations for Assigned Names and Numbers (ICANN) mainly for the governance of the ".to" ccTLD and to become more active and engaging the APAC Space with the Asia-Pacific partners.

7. Conclusion

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

CERT-VU

Computer Emergency Response Team Vanuatu

1.Highlights of 2024

1.1 Summary of major activities

- In 2024, CERTVU responded to around 400 cybersecurity-reported incidents.
- Our cybersecurity awareness campaign covers Radio talkback shows
  - ICT Radio talkback shows
  - One-to-one awareness sessions with organizations
  - Regular rural communities' cybersecurity awareness initiatives
  - School's educational cyber awareness talks
- CERTVU, in collaboration with the Retrospect Lab team, conducted a Cyber Security Defensive Readiness Exercise Program for Vanuatu. This event brings together all critical infrastructure for a week-long cybersecurity capacity-building and tabletop exercises.
- CERTVU continues strengthening its international and regional collaboration through its efforts in PacSON, where it is a member of the Awareness Raising Working Group (ARWG), Capacity Building Working Group (CBWG), and Communications Working Group (CWG). These efforts continue to see the yearly implementation of Cyber Smart Pacific Week celebrated through the PaCSON community.

1.2 Achievements & milestones

- We continue to deliver Cyber Smart Pacific (https://cert.gov.vu/cybersmart/) activity within Vanuatu as we celebrate the Cyber Month in October
- This year, we completed the implementation of our SIEM, and our team now has insight into the different security events happening within the government digital environment.
- Vanuatu National Cyber Security Defensive Readiness Exercise Program – Bringing together all our critical infrastructure and partners for a week of cybersecurity exercises and tabletop exercises on Incident Response.
- Establishing a cybersecurity Incident Response Community (IR Community) comprises different voluntary

individuals from different organizations and sectors.

- Release our cybersecurity technical guide for train the trainers program

2. About CSIRT

2.1 Introduction

CERTVU, the Vanuatu National Computer Emergency Response Team, serves as the central entity for cybersecurity in Vanuatu. It collaborates with the Government, businesses, and civil society to address cybersecurity incidents. CERTVU offers reliable advisory information and is committed to enhancing cybersecurity in Vanuatu through awareness initiatives and capacity-building programs.

2.2 Establishment

CERTVU was established in 2018 within the Department of Communication and Digital Transformation (DCTD), formally known as the Office of the Government's Chief Information Officer (OGCIO) under the Ministry for the Prime Minister as the Minister for Information and Telecommunication.

2.3 Resources

CERTVU was established within the Department for Communication and Digital Transformation, with three dedicated staff members managing the overall operation, from awareness raising to capacity building to incident response.

2.4 Constituency

CERTVU is a national CERT for Vanuatu; therefore, it serves the entire country, including the government, private sectors, NGOs, civil society, and visitors who visit and live in Vanuatu while on holiday.

3. Activities & Operations

3.1 Scope and definitions

CERTVU is mandated to provide:

- Provide Incident Response to Vanuatu's constituents, including government, business houses, and citizens.

- Promote and provide Cyber Security Awareness to Vanuatu and all constituents.
- Collaborate with the regional and international CERTs.
- Vulnerability identifications.
- Issuance of security advisories and alerts.
- Provide cyber security awareness campaigns.
- Conduct incident report handling and incident response coordination.
- Continued support to the established cybersecurity collaboration framework.
- Identify and implement capacity-building programs nationally.
- Provide forensic services to the Vanuatu Police Force

3.2 Incident handling reports

CERT Vanuatu continues to see similar abuse trends compared to 2022, 2023, and 2024. Notably, Phishing is still common. However, we have seen an increase in Ransomware and Email-compromised activities over the last three years. Below is a summary of the threats identified.

Top five of the cybersecurity incidents reported to the CERTVU

- Phishing and credential harvesting
- Ransomware attack
- Malware attack
- Email-compromised
- DDOS

3.3 Publications

- Publish a press release on Vanuatu's participation in the Fourth International Counter Ransomware Initiative 2024 summit.
- Publish Press release on Vanuatu Agency Consultation Workshop
- Publish Press Release on CERTVU participation in the FIRST and NatCSIRT conference in Fukuoka, Japan
- Press release on A Day with CERTVU: Celebrates 6th Anniversary with successful public awareness.
- Publish security advisories on the different cyber threats and Vulnerabilities.
- Press release on CERT Vanuatu hosting ICT boot camp for high schoolers

3.4 New Initiatives

CERTVU is embarking on its train-the-trainer initiative to ensure meaningful educational awareness on cyber security and establish a focal point of contact in all local communities.

CERTVU team during Train-the-Trainers initiative at Nguna Island

CERTVU recently built a local community of cybersecurity responders called the "Vanuatu CyberIR Community." On 11-10-24 or 11th October 2024, the 1st "Community" meet-up (an informal get-together) took place at the "RoofTop" in Port Vila. We are designing and branding this community-based initiative as the "Vanuatu Cyber IR Community (VCIRC)." The Cyber Resilience initiative and operational model will innovate and capitalize on 'Cognitive Resilience' with a prime focus on building cyber experts and a robust "Incident Response" for our businesses, communities, and society. Cognitive resilience fosters an environment where individuals are better equipped to handle cyber threats, leading to a more resilient organizational structure. By understanding how cognitive factors influence behavior in cybersecurity contexts, organizations can develop training programs that enhance both individual and collective responses to cyber threats.

First Vanuatu CyberIR Community Team Meetup

4. Events organized/hosted

4.1 A Day with CERTVU

Spend a Day with CERTVU, a whole-day event organized on the 19th of June 2024 to celebrate CERTVU's 7 years of establishment. To provide cybersecurity awareness to the public and promote CERTVU operational activities to anybody on the street. The event is also planned to strategize future cyber initiatives. Gain insight into a proactive approach, empowering citizens and building a resilient digital landscape for Vanuatu.

4.2 Training

- CERTVU, in collaboration with the Retrospect Lab team, conducted a Cyber Security Defensive Readiness Exercise Program for Vanuatu. This event brings together all critical infrastructure for a week-long cybersecurity capacity-building and tabletop exercises.

Participant from the Vanuatu cybersecurity defensive readiness event

- Provide technical training for the Train the Trainers program in the local community. Our Train-the-Trainers "Cyber Security Bundle" program aims to build capacity within the local communities and schools. This will create capacity in communities and schools by establishing a focal point of contact within the community for citizens to get basic technical advice on cyber issues.

- Conducted ICT and Cybersecurity Training for the Vanuatu Youth Challenge, an NGO that focuses on the development of youth. CERT Vanuatu (CERTVU) continues to provide cybersecurity training on the WORK READY Program to help get youths ready for the place.

Vanuatu Youth Challenge Participant for the Cybersecurity workshop session

- Student boot camp—To celebrate this year's Information and Communications Technology (ICT) Day, CERT Vanuatu, in collaboration with the Office of the Government Chief Information Officer (OGCIO), hosted an ICT boot camp for high school students in Port Vila, particularly those in Years 12 and 13.

Students' participation on high school cybersecurity boot camps

CERTVU cyber hygiene awareness to secondary schools

- Joint Cyber Security training through the PaCSON Capacity Building Programs.

4.3 Conferences and seminars

In collaboration with USAID and the Young Pacific Leaders, CERT Vanuatu organized a day of ICT and Cyber workshops for young leaders in celebration of World Cyber Month. The workshop focuses on equipping young, interested leaders with the right tools to assist them in their respective organizations and communities.

5. International Collaboration

- Our continuous collaborations through the PaCSON community Platform continue to provide support to the Pacific community in terms of cybersecurity.
- The 36th FIRST Annual Conference is from 9 – 15 June 2024 in Fukuoka, Japan. CERT Tonga attended.
- CERT Vanuatu attended the 2024 APCERT AGM in Taiwan.
- Commonwealth Heads of Government Meeting (CHOGM), CERT Vanuatu was part of the 2024 Technical Team (with other members from the national CERTs in the South Pacific region)

6. Future Plans

6.1 Future projects

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

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

7. Conclusion

CERT Vanuatu, operating under the auspices of the Government of Vanuatu, persistently undertakes essential operations to guarantee a secure cyberspace and Internet environment for its constituents. This ensures that individuals can reside, exchange information, and conduct business, thereby enhancing economic advantages within Vanuatu

Cybersecurity and the function of a Computer Emergency Response Team (CERT) are of paramount importance in Vanuatu, thereby facilitating the nation's ongoing implementation and enforcement of its National Cyber Security Strategy for 2030. Guided by the priorities delineated in the Vanuatu National Cyber Security Strategy (NCSS) and supported by its NCSS Implementation Matrix, Vanuatu continues to address cybersecurity incidents, refine its Cybercrime Act No. 22 of 2021, and operate under a Cyber Security Memorandum of Understanding involving CERT Vanuatu, the Vanuatu Police Force (VPF), the Telecommunications Radiocommunications and Broadcasting Regulators' Office (TRBR), the Vanuatu Internet Governance Forum (VanIGF), and the Vanuatu Bureau of Standards (VBS). This collaboration empowers Vanuatu to adopt a multi-stakeholder approach in its cybersecurity endeavors

In conclusion, Vanuatu recognizes the necessity of establishing cyber resilience to safeguard its cyberspace and sovereignty. Consequently, the enhancement of Vanuatu's Cyber Security Posture is paramount, necessitating the

enforcement of stringent cybersecurity frameworks. This initiative enables Vanuatu to concentrate on improving various technical mechanisms, governance structures, and legal frameworks, specifically including efforts related to the Data Protection and Privacy Policy, as well as Act No. 13 of 2024, alongside its Harmful Digital Communications Policy and Act No. 14 of 2024.

CNCERT/CC

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

1. Highlights of 2024

1.1 Summary of major activities

As we traverse the annals of the past year, the field of cybersecurity stands as a testament to resilience and innovation in an era marked by unprecedented digital transformation. Each challenge encountered has illuminated a path for growth, fostering an environment where vigilance and exploration merge to confront the complexities of an ever-evolving threat landscape.

Amid new emergence of AI models and other new cyber trends, we continue to play our role in APCERT and the wider community underpinned by a host of events. We successfully hosted several international and domestic conferences, such as the Cybersecurity Forum for Technology Development and International Cooperation in 2024 World Internet Conference Wuzhen Summit, the 21st CNCERT Annual Conference and the Cyber Security Collaborative Governance Sub-Forum of China Cybersecurity Week, China-ASEAN Network Security Emergency Response Capacity Building Seminar. These conferences are increasingly well-received and supported by the international community. We also make active presence in cybersecurity drills, such as APCERT Drill 2024 and ASEAN CERT Incident Drill 2024. By participating in international and regional activities, we have facilitated information sharing, cross-border incident handling, technical training, capacity building, among other collaborative efforts. Overall, it was a year packed with fruitful outcomes and busy steps.

1.2 Achievements & milestones

Release of Action Plan for AI-powered Cybersecurity Cooperation Initiative

On 21st November 2024, CNCERT/CC has released the Action Plan for AI-powered Cybersecurity Cooperation Initiative during 2024 World Internet Conference Wuzhen Summit. The Initiative includes AI-powered cybersecurity capacity building, sharing AI threat information, formulating international standards for AI emergency response, and raising AI security awareness.

Building of AI-Based Phishing Detection System

CNCERT/CC has developed a web phishing monitoring and detection system based on AI and are making it available to CERT organizations who are interested. The phishing website detection technology will be made available free of charge to CERT organizations worldwide. By utilizing this AI-powered tool, CERT organizations can strengthen their capabilities to counter phishing attacks effectively.

2. About CNCERT/CC

2.1 Introduction

The National Computer Network Emergency Response Technical Team/Coordination Center of China (known as CNCERT/CC) is a non-profit cybersecurity technical center and the key coordination team for China's cybersecurity emergency response community.

2.2 Establishment

CNCERT/CC was founded in 2001, and became a member of FIRST and one of the founders of APCERT. As of 2024, CNCERT/CC has established "CNCERT/CC International Cooperation Partnership" with 292 teams in 86 countries and regions.

2.3 Constituency

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

3. Activities & Operations

3.1 Scope and definitions

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

Database (CNVD).

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

3.2 Incident Reports

CNCERT/CC found and handled two U.S. cyber attacks on China's large-scale tech firms

The National Computer Network Emergency Response Technical Team/ Coordination Center of China (CNCERT/CC) found and handled two incidents of cyber attacks originated from the United States on China's large-scale tech firms to steal trade secrets.

Since August 2024, an advanced materials design and research institution of China has been suspected of being attacked by a U.S. intelligence agency. Analysis showed that the attacker exploited vulnerabilities in an electronic document security management system to infiltrate the software upgrade management server deployed by the firm. The attacker then implanted Trojan in over 270 hosts of the firm via software upgrade service, stealing a large amount of trade secrets and intellectual property.

Since May 2023, a large-scale high-tech firm dedicated to intelligent energy and digital information of China has been suspected of being attacked a U.S. intelligence agency. Analysis showed that the attacker used multiple overseas hosts as springboards to exploit a Microsoft Exchange vulnerability, thus penetrating and controlling the firm's email server. By embedding backdoors in the server, the attacker managed to steal email data constantly. In the meantime, the attacker used the email server as a springboard to control over 30 hosts of the firm and its affiliates, stealing a large number of trade secrets.

A detailed report has been published by CNCERT/CC on the two incidents on January 17, 2025.

3.3 Publications

During the year of 2024, CNCERT/CC has published multiple weekly reports, as well as other released information, which were reprinted and cited by massive authoritative media and thesis at home and abroad.

Title	No. of Issues	Description
CNCERT Weekly Reports (Chinese)	52	Emailed to relevant organizations and individuals and published on CNCERT's Chinese website (https://www.cert.org.cn/)
CNCERT Weekly	52	Emailed to relevant organizations and individuals and published on CNCERT's

Reports (English)		English website (https://www.cert.org.cn/publish/english/115/index.html)
CNVD Vulnerability Weekly Reports (Chinese)	52	Published on CNCERT's Chinese website (https://www.cert.org.cn/)

Table 1: Lists of CNCERT's publications throughout 2024

4. Events organized / hosted

4.1 2024 World Internet Conference Wuzhen Summit: Cybersecurity Forum for Technology Development and International Cooperation

Hosted by CNCERT/CC, the Cybersecurity Forum for Technology Development and International Cooperation of 2024 World Internet Conference Wuzhen Summit was held in Wuzhen, Zhejiang Province on 21st November. With the theme of "AI for Good: Security Risks and Governance of Artificial Intelligence", the Forum aims to find solutions to current AI-related security and governance issues and promote the establishment of an open, fair, and effective governance mechanism.

During the Forum, CNCERT released the "Action Plan for AI-powered Cybersecurity Cooperation Initiative", with a focus to enhancing the capacity of AI-driven cybersecurity emergency response and foster the integration and innovation of AI and cybersecurity.

The forum was hosted by the National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT/CC) and the Zhongguancun Laboratory (ZGC LAB). Over 100 representatives from governments, international organizations, research institutions, industry associations, and enterprises attended the event.

4.2 The 21st CNCERT Annual Conference and the Cyber Security Collaborative Governance Sub-Forum of China Cybersecurity Week in Guangzhou

From 9th to 10th September 2024, the 21st CNCERT Annual Conference and the Cyber Security Collaborative Governance Sub-Forum of China Cybersecurity Week were successfully held in Guangzhou. With the theme of " Collaborative Construction of Cybersecurity Defense Systems", the Conference was hosted by the National Computer Network Emergency Response Technical Team/Coordination Center (CNCERT/CC). Since its inception in 2004, the Conference has been successfully held for 20 consecutive years, serving as an important bridge and link for in-depth exchanges among

national and local departments, critical information infrastructure operators, the cybersecurity industry, and academia. It has played a positive role in enhancing China's cybersecurity capabilities and strengthening the national cybersecurity barrier.

4.3 China-ASEAN Network Security Emergency Response Capacity Building Seminar

The China-ASEAN Network Security Emergency Response Capacity Building Seminar, hosted by the National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT/CC), was successfully held in Guangzhou from December 18th to 19th, 2024. Representatives from more than 10 organizations both domestic and international attended the meeting, with relevant representatives from CNCERT/CC participating and delivering speeches. Representatives from CNCERT/CC, as well as from the Information and Communication Security Bureau of the Ministry of Posts and Telecommunications of Cambodia, the Cybersecurity Bureau of the Ministry of Technology and Communications of Laos, the Ministry of Transport and Communications of Myanmar, the Singapore National Cybersecurity Agency, the Thailand National Cybersecurity Agency, and the Ministry of Information and Communications of Vietnam, exchanged views on their respective national cybersecurity policies, capacity situations, and work related to AI security.

5. International Collaboration

5.1 International partnerships and agreements

5.1.1 APCERT Drill 2024

On 29th August, CNCERT/CC participated in APCERT Drill 2024 and completed it successfully. The theme of this year's APCERT Drill is "APT Group Attack Response: Where is Wally?". This exercise reflects real world cyber security threats to our economies from Advanced Persistent Threat (APT) actors, the most sophisticated and well-resourced type of malicious cyber adversary. The participants handled a case by APT threat actors. 22 CSIRTs from 18 economies of APCERT, as well as 3 CSIRTs from 3 economies of OIC-CERT and AfricaCERT participated.

5.1.2 ASEAN CERT Incident Drill (ACID) 2024

On 15th October, CNCERT/CC participated in the ASEAN CERT Incident Drill (ACID) 2024. Themed "Navigating the Rise of AI-Enabled Cyber Attacks", this year's ACID was chosen against the backdrop of the multifaceted application of Artificial Intelligence (AI) technology for attack and defense. The participating teams investigated, analyzed, reported and recommended remediation and mitigation measures towards cyber incidents. ACID tests incident response procedures and strengthens cybersecurity preparedness and cooperation among CERTs in ASEAN Member States and

ASEAN Dialogue Partners.

6. Future Plans

i. Explore new needs of members, organize teleconferences to facilitate communication between members, motivate members to share information within APCERT and develop a new system for APCERT DataExchanger
ii. Plan to host Cybersecurity Forum for Technology Development and International Cooperation of 2025 World Internet Conference Wuzhen Summit
iii. Plan to host China-ASEAN Network Security Emergency Response Capacity Building Seminar of 2025 World Internet Conference Asia-Pacific Summit in Hong Kong on April, 2025

7. Conclusion

As we reflect upon this transformative year, it becomes evident that the journey of cybersecurity is one of perpetual evolution. With each stride forward, we are reminded of the imperative to remain steadfast, responsive, and proactive in the face of new challenges. The road ahead is illuminated by a shared commitment to APCERT community, ensuring a safe, clean and reliable cyber space in the Asia Pacific Region through global collaboration.

Guided by the lessons learned and the challenges overcome, CNCERT/CC, as a member of APCERT Steering Committee and the convener of Information Sharing Working Group, will remain committed to carrying on our missions and responsibilities, and fostering a better environment.

CyberSecurity Malaysia

CyberSecurity Malaysia

1. Highlights of 2024

1.1 Summary of major activities

26 Feb 2024	Participated in the APCERT Steering Committee Face to Face meeting, Bangkok Thailand
26 Feb – 2 Mar 2024	Participated in the OIC-CERT Face to Face meeting and OIC-CERT Activities in conjunction with MWC24 Barcelona
23 - 25 Apr 2024	Organised the OIC-CERT Team Expert Workshop in conjunction with the Gulf Information Security Exhibition & Conference (**GISEC**), United Arab Emirates
13 - 17 May 2024	Co-organized with UK High Commission and BAE UK on IPCP Training: Cyber Threat Intelligence, Incident Response and Security Operation Centre
25 Jun – 2 Jul 2024	Organised capacity building training under the Malaysian Technical Cooperation Program (MTCP) attended by selected APCERT members titled "Digital Security & Lifelong Learning Programme" (**DLSP**)
24 – 27 Jul 2024	Organised OIC-CERT Board & Leadership Meetings and Working Group Roundtable, Shenzhen China
18 Jul 2024	Organised the Webinar Serumpun **"A.I Dalam Kehidupan Seharian**". Malaysia Edition in cooperation with the Indonesian National Cyber and Crypto Agency (**BSSN**) and Cyber Security Brunei (**CSB**) (online)
6 – 8 Aug 2024	Organised the Cyber Digital Services, Defense and Security Asia (**CyberDSA**) 2024
29 Aug 2024	Participated in the APCERT Cyber Drill "APT Group Attack Response: Where is Wally" (online)
27 – 29 Oct 2024	Participated in the OIC-CERT 11th OIC-CERT General Meeting & 16th OIC-CERT Annual Conference, Muscat Oman
9 Nov 2023	Participated in the APCERT Annual General Meeting and Conference 2024 and The Regional Symposium for Asia Pacific, Taipei Taiwan

Table 1. Summary of major activities

2. About CSIRT

2.1 Introduction

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

i. Cybersecurity Responsive Services
   - Security Incident Handling
   - Digital Forensics

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

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

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

v. Industry and Research Development

vi. Cybersecurity Pre-emptive Services

2.2 Establishment

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

2.3 Resources

2.3.1 Cyber Security Incident Response

CyberSecurity Malaysia responds to and handles cyber security incidents through Cyber999 Cyber Incident Response Centre, a Unit within CyberSecurity Malaysia. This Unit is a leading technical reference point for Malaysian Internet users facing cyber security incidents. Cyber999 facilitates the handling and mitigating cyber security incidents for organisations and Malaysian Internet users. The types of incidents received and responded to are intrusion, fraud, malicious codes, vulnerability reports, intrusion attempts, spam, denial of service (**DOS**) and data breaches. Cyber999 Cyber Incident Response Centre receives incident reports from various parties in the constituency, such as the general public, private sectors, and SMEs. Additionally, we receive information about incidents involving Malaysia IPs or domains from trusted security teams from abroad (foreign CERTs) and Special Interest Groups such as Shadowserver Foundation and through CyberSecurity Malaysia's proactive monitoring. Cyber999 works closely with ISPs, CERTs, Special Interest Groups (**SIGs**) and Law Enforcement Agencies (**LEAs**), from local and international, to remediate and mitigate computer security incidents affecting Malaysia's organisations and the public.

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

Cyber999 responded to 6,209 incidents in 2024, with most reported incidents being fraud, data breach, malicious code, and intrusion.

2.4 Constituency

Cyber999 constituencies include SMEs, businesses, and Malaysian Internet users. Cyber security incidents reported to the Cyber999 Cyber Incident Response Centre will be resolved with technical assistance and guidance based on incident categories for users and organisations.

3. Activities & Operations

3.1 Scope and Definitions

3.1.1 Monthly Cyber Incidents Statistics

Cyber999 proactively produced 220 advisories and 5 alerts in 2024 to inform and warn the constituency about recent cyber threats. The security advisories, alerts, and summary reports produced by Cyber999 Cyber Incident Response Centre can be viewed at https://www.mycert.org.my/portal/advisories2024

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

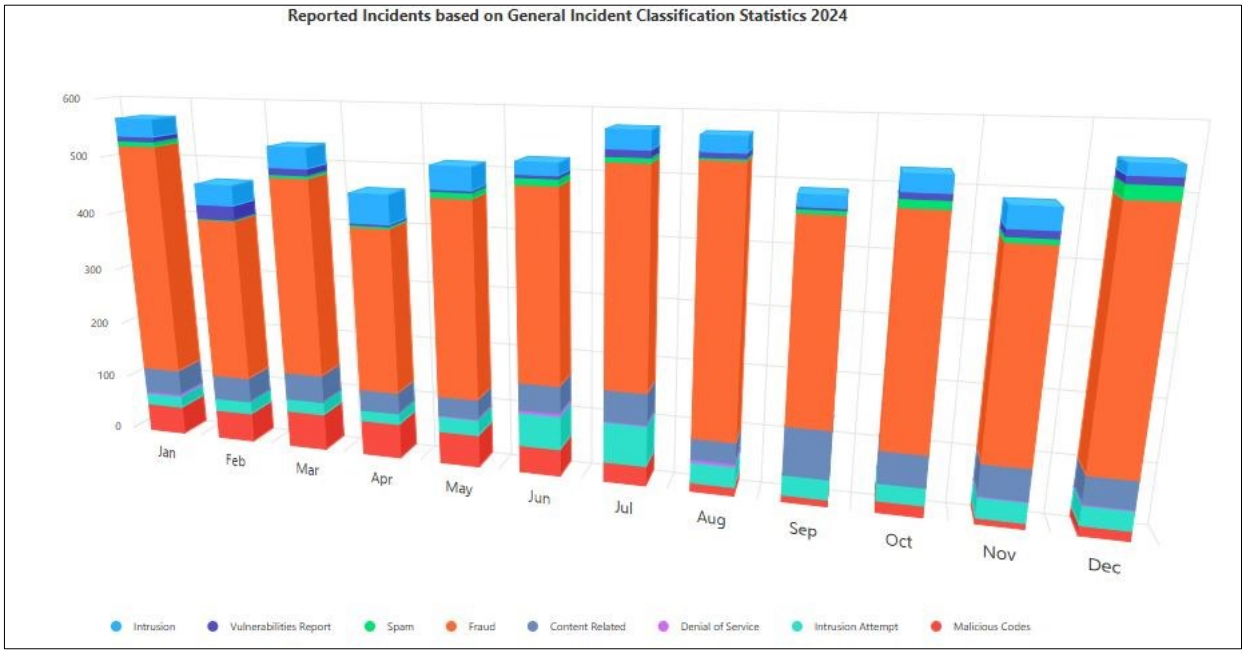


Figure 1: Incidents Reported to Cyber999 of CyberSecurity Malaysia in 2024

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

3.1.2 Security Alert and Advisory

In addition to assist in technical support for incident handling, Cyber999 will produce security alerts and advisories on the latest cyber threats targeting Malaysia and patch information for software vulnerabilities. It will mainly produce security alerts and advisories from the Cybersecurity & Infrastructure Security Agency (CISA), CSIRTs, and other trusted cyber security agencies.

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

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

3.1.3 Cyber Incident Quarterly Summary

The Cyber Incident Quarterly Summary Report 2024 provides an overview of computer security incidents handled by the Cyber999 Incident Response Centre of CyberSecurity Malaysia quarterly. Cyber Incident Report also highlights statistics of incidents dealt with by the Cyber999 Incident Response Centre in each quarter of 2024 according to their categories, security alerts and advisories released, and current security threats and trends. It should be noted that the statistics

provided in this report reflect only the total number of incidents reported and handled by the Cyber999 Incident Response Centre, excluding elements such as monetary value or aftermaths of the incidents. Computer security incidents dealt with Cyber999 Incident Response Centre involved IP addresses and domains from Malaysia.

3.2 CyberSOC

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

This facility managed 3 core services as below:

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

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/

4. Events organized / hosted

4.1 Training

4.1.1 Malaysian Technical cooperation Programme (MTCP)

Hands-on training entitled Digital Security Lifelong Learning Program (DSLP) under the Malaysian Technical cooperation Programme (MTCP) was conducted by CyberSecurity Malaysia from 25 Jun – 2 Jul 2024. There were 11 participants form Brunei, Cambodia, Indonesia, Morocco, Nigeria, Philippines, and Somalia.

4.1.2 Indo-Pacific Cyber Programme

The United Kingdom's Foreign, Commonwealth & Development Office, the British High Commission in Kuala Lumpur, and BAE Systems launched the Indo-Pacific Cyber Programme, co-organized by CyberSecurity Malaysia, from May 13 to 17, 2024. This five-day Cyber Technical Training program aims to equip professionals in the Indo-Pacific region with

practical cybersecurity skills

4.2 Drills & exercises

Organized the Capital Market Cyber Simulation (CMCS). A cyber-attack and defence simulation project under the Securities Commission and Cyber Security Malaysia. CMCS started in 2018 with only 38 participants and has been growing rapidly over the years, until today we have 110 participants joining CMCS. For CMCS2022, this project shifted from the role-playing method to the CTF method to cater for an increased number of participants. This is to ensure seamless accessibility for all participants and the readiness in handling simulation of real-life attack.

4.3 Conferences and seminars

CyberDSA (Cyber Digital Services, Defence and Security Asia) is a prestigious annual cybersecurity event held in Kuala Lumpur, Malaysia. The 2024 edition took place from August 6 to 8 at the Kuala Lumpur Convention Centre, under the theme "Navigating Tomorrow's Cyber and Digital Frontier." Organized by CyberSecurity Malaysia, the event is supported by a diverse range of partners from both the public and private sectors, including government agencies, industry leaders, and cybersecurity professionals.

5. International Collaboration

5.1 International partnerships and agreements

The Malaysia Cybersecurity Strategy 2024 identified international cooperation as one of the areas in enhancing cybersecurity. In line with this, CyberSecurity Malaysia is actively establishing collaborative relationships with foreign parties.

5.1.1 Working Visits

CyberSecurity Malaysia conducted working visits to relevant organisations overseas to further enhance the country's cybersecurity posture. The objective of the visits is to seek potential collaborations in cybersecurity.

This agency also received working visits from foreign organisations that have similar objectives. Among them are:

i. National Cyber Security Centre (**NCSC**), United Kingdom
ii. China Academy of Information and Communications Technology (**CAICT**)
iii. Embassy of the Kingdom of the Netherlands
iv. United Nations Institute for Disarmament Research (**UNIDIR**)
v. High Commission of Canada in Malaysia
vi. eWorldwide Group

vii. Cyber Security Agency of Singapore (**CSA**)
viii. National Information Security & Safety Authority (**NISSA**) – Libya-CERT
ix. Australia's eSafety Commissioner
x. InCyber Forum North America & International

5.1.2 International Roles

Amongst the international roles and contributions by CyberSecurity Malaysia

i. The Permanent Secretariat of the Organization of Islamic Cooperation – Computer Emergency Response Team (**OIC-CERT**), where a major role is to undertake daily operations and facilitate cooperation and interaction among the members countries
ii. The lead for the Capacity Building Initiatives in the OIC-CERT
iii. Co-Lead the OIC-CERT 5G Security Working Group with the objective of developing a security framework to be adopted by OIC member countries
iv. The Chair of the APCERT
v. Member of the Forum of Incident Response and Security Teams (**FIRST**)
vi. Member of the National CSIRT Committee
vii. Certificate authorising member of Common Criteria Recognition Arrangement (**CCRA**)
viii. Member of the ShadowServer Foundation
ix. Member of the ASEAN Forensic Science Network
x. Member of the Digital Forensics Working Group
xi. Member of the Traffic Accident Reconstruction Working Group
xii. Member of the INTERPOL Regional Expert Group for Cryptocurrency Investigation (**REG-CI**)
xiii. Member of the United Nations Office on Drugs and Crime (**UNODC**) Women in Cyber
xiv. Member of the Cybersecurity Alliance for Mutual Progress (**CAMP**)
xv. Member of the ASEAN CERT

5.2 Capacity building

5.2.1 Drills & exercises

CyberSecurity Malaysia, participated in three (3) international cyber drills in 2024 namely the APCERT Drill, ACID Drill, and the OIC-CERT Drill.

5.2.2 Seminars & presentations

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

i. 6 – 8 May 2024 - As a speaker at the cryptocurrency and digital evidence course program in ASEAN countries, United Nations Office on Drugs and Crime (**UNODC**)

ii. 26 – 30 Aug 2024 – As a speaker at the conference entitled "Enhancing first responders in digital forensic: best practice and advanced technologies" at Asian Forensic Science Network (**AFSN**)
iii. 16 – 19 Sep 2024 – As a speaker at the conference Science & Technology (ICST-2024) in Kyoto, Japan
iv. 18 -19 Sep 2024 – As a speaker at the Southeast Asia Cybersecurity Consortium (**SEACC**) Forum entitled "People Certification: The Need For Cyber Security Professionals" at Brunei Cybersecurity Conference (CYSEC) 2024
v. 31 Oct 2024 - As a speaker at OIC-CERT 16th Annual Conference, Oman
vi. 6 Nov 2024 – As a speaker at APCERT Closed Conference entitled "Targeted attack tactics & techniques trend in Malaysia" in Taiwan
vii. 5 Jun and 27 Nov 2024 – Presented on Country Updates of Local Cyber Threat Landscape in Bi-yearly ASEAN Partner CERTs Information Sharing, held virtual

5.3 Other international activities

5.3.1 Research Papers

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

i. Development of Cybersecurity Competency and Professional Talent for Cyber Ummah - Journal of Quranic Sciences and Research
ii. The Study of Randomness Properties Exhibited by LAO-3D Lightweight Block Cipher Algorithm - Springer Link
iii. Comprehensive Review on Data Preservation Models and Standards in Digital Forensic – IEEE
iv. A Systematic Review on Multi-Factor Authentication Framework - The Science and Information Organization (SAI)
v. A Proposed Framework of Vulnerability Assessment and Penetration Testing (VAPT) in Cloud Computing Environments from Penetration Tester Perspective - Semarak Ilmu Publishing
vi. A Framework for the Development of Risk-Based Guidelines for Cloud Service Subscribers - Semarak Ilmu Publishing
vii. LSTM-Based Analysis of De-Identification Techniques for Protecting Sensitive Data - Al-Noor
viii. A Comprehensive Study on Emerging Trends of Dark Web Marketplaces and Forums - IEEE

5.3.2 Social Media

In 2024, 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 X, which as of now the Facebook Page has about 62,000 followers and the CyberSecurity Malaysia X has 8,143 followers.

6. Future Plans

6.1 Future Operation

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

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

CyberSecurity Malaysia and Aerosea Exhibitions Sdn. Bhd will be organizing an international event known as the Cyber Digital Services, Defence and Security Asia (CyberDSA'25). This event is scheduled to take place from 30 September to 2 October 2025, at the MITEC, Kuala Lumpur. CyberDSA aspires to be a leading content-driven event, serving key stakeholders protecting national, public and business interests in cyberspace. It aims to connect decision makers in governments and private sectors to accelerate the digital drive with security on a regional scale. This event aims to impart latest knowledge and insights while showcasing cutting-edge technologies that would safeguard digital economies and foster global competitiveness. At the international arena, CyberSecurity Malaysia as the Permanent Secretariat of the OIC-CERT, continues to spearhead collaborations and organise international events such as the OIC-CERT Annual Conferences and Trainings.

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

6.2 ASEAN Events 2025 involving CyberSecurity Malaysia

In conjunction with Malaysia's ASEAN Chairmanship in 2025, several ASEAN-related events have been identified by the management of CyberSecurity Malaysia for implementation in 2025, as listed:

No	Programme	Date	Venue
1	Webinar ASEAN 2025	4 Sessions	Online webinar
2	ASEAN Digital Trust: Professional Development and Lifelong Learning Program	18th June 2025	TBC
3	ASEAN 5G & OT Security Summit	Brunei, Indonesia, Singapore dan Malaysia	MITEC, KL

4	CyberDSA	20th August 2025	MITEC, KL
5	https://www.cyberdsa.com/	Filipina, Laos, Cambodia dan Malaysia	MITEC, KL
6	Advancing Cryptocurrency Investigation: Empowering ASEAN Law Enforcement	22nd October 2025	MITEC, KL
7	Quantum Safe Migration Forum: Securing ASEAN's Digital Future	Thailand, Myanmar, Vietnam dan Malaysia	MITEC, KL
8	ASEAN Vehicle Forensic Investigation Forum: Driving Evidence & Exploring Techniques and Best Practices	9 July 2025	TBC
9	AI ASEAN - China: Shaping the Future in Digital Data Governance	Indonesia, Malaysia, Thailand	MITEC, KL

7. Conclusion

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

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

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

ETDA

Electronic Transactions Development Agency – Thailand

1. About CSIRT

1.1 Introduction and Establishment

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

Conversations have moved beyond face-to-face meetings to online chats or video calls. A person from one part of the world can communicate with another person from the other side of the world within a second. Work communications and documents no longer need to be printed and submitted to offices. Documents can now be sent via systems with various forms of authentication and sender identifications. Meetings can now be held as e-meetings without needing space for large numbers of people. Commerce has transitioned from walking into a store to buy things to buying things on a screen. Payments can now also be made online.

Changes in the structure of peoples' lives have created a need for agencies or organizations designed to support and govern services in the aforementioned topics in the digital world with reliable, secure and safe standards or "digital governance", in other words. This can help the economy and societies grow in step with the world's rapid changes.

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

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

- G2X, or Government-to-Government transactions, Government-to-Business transactions and Government-to-Citizen transactions.
- B2X, or Business-to-Business transactions, Business-to-Government transactions and Business-to-Citizen transactions.
- C2C, or Citizen-to-Citizen transactions such as transactions via social media platforms.

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

of electronic transactions.

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

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

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

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

- Data Analysis –If laws are to be enacted with a view toward the future, data is needed to see what will happen in order to prevent laws from becoming obsolete in new technological environments.
- Personnel Development – The ETDA develops personnel to be fully effective and useful in the electronic transactions ecosystem.
- Consultation – The ETDA provides consultation for government agencies, private organizations or citizens in order to understand what is legal, illegal, appropriate, reliable or inadvisable when conducting electronic transactions.
- Fraud Prevention – The ETDA emphasizes connections with platforms to provide education on self-defense and consultation, or accept complaints in order to coordinate with the agencies responsible and provide support for affected individuals.
- Innovation Promotion – Because electronic transactions and digital services come with new technologies, the ETDA's status as a governing agency over services may prevent newly fledged services from surviving. Therefore, the ETDA sees the significance of promoting innovation and sandboxes.

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

1.2 Constituency

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

2. Activities & Operations

2.1 Incident handling reports

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

2.2 Publications

- PGP/GnuPG Key Signing Party: Practical Guidance to Joining the Web of Trust, Jul 2024

3. Events organized / hosted / participated in

3.1 Training

Trainer:

- TRANSITS I for the NCSA, Sep 2024
- 2024 APISC Security Training Course. Sep 2024

3.2 Drills & exercises

Organized:

- Cyber Drill for the NCSA, Sep 2024
- Cyber Exercise for Certification Authorities (CA) TTX, Nov 2024

Participated:

- APCERT Annual Drill 2024, Aug 2024

3.3 Conferences and seminars

Participated:

- DEFCON Bangkok Community (DC2325) seminar, Oct 2024
- APCERT AGM & Conference 2024, Nov 2024
- FIRST Regional Symposium for Asia-Pacific, Nov 2024

GovCERT.HK

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

1.Highlights of 2024

1.1 Summary of Major Activities

The Government Computer Emergency Response Team Hong Kong (GovCERT.HK) persistently collaborated with different stakeholders to implement a wide range of activities and initiatives for strengthening cybersecurity resilience, promoting cybersecurity awareness, and enhancing defensive capabilities within the community, aiming at fortifying our defences and security posture as a whole.

1.2 Achievements and Milestones

Fortifying Cyber Security Resilience

To enhance the professional skills and incident response capabilities of cybersecurity personnel, we organised a series of attack and defence training and tournament with the Cyber Security and Technology Crime Bureau (CSTCB) of the Hong Kong Police Force (HKPF) and the Hong Kong Internet Registration Corporation Limited (HKIRC). We also launched Hong Kong's first Cybersecurity Attack and Defence Drill in collaboration with CSTCB, HKIRC and the Hong Kong Institute of Information Technology (HKIIT) with a view to strengthening the overall defensive capabilities of government departments and public organisations against cyberattacks. Furthermore, we conducted a comprehensive review of government information security regulations, policies, and guidelines to ensure their effectiveness and robustness and enhanced the monitoring systems and mechanisms for intelligence gathering, striving to strengthen our resilience for the evolving threats and challenges.

Awareness and Capability Building

To foster a comprehensive understanding of cybersecurity within the community, we collaborated with industry stakeholders to organise the Cybersecurity Awareness Campaign 2024, under the theme "Together, We Create a Safe Cyberworld". We launched a series of activities including contests, game booths, seminars and forums. The Cybersecurity Symposium 2024 was one of the major highlights, bringing together industry leaders to collectively share and address

cybersecurity challenges. To show our commitment and determination in strengthening the cybersecurity knowledge of IT practitioners, a wide spectrum of thematic seminars, technical workshops, certificate courses on information security and cyber security incident response were introduced and newly launched in 2024.

Liaison and Collaboration

We actively participated in Asia Pacific Computer Emergency Response Team (APCERT) training and drill exercises, collaborating closely with local organisations and global partners to exchange technical insights and enhance incident response and coordination. We signed a Memorandum of Understanding with the Cyberspace Administration of Guangdong Province and the Comissão para a Cibersegurança of Macao SAR to facilitate cybersecurity exchange and collaboration in the Guangdong-Hong Kong-Macao Greater Bay Area (GBA).

About GovCERT.HK

2.1 Introduction

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

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

2.2 Establishment

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

2.3 Resources

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

2.4 Mission and Constituency

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

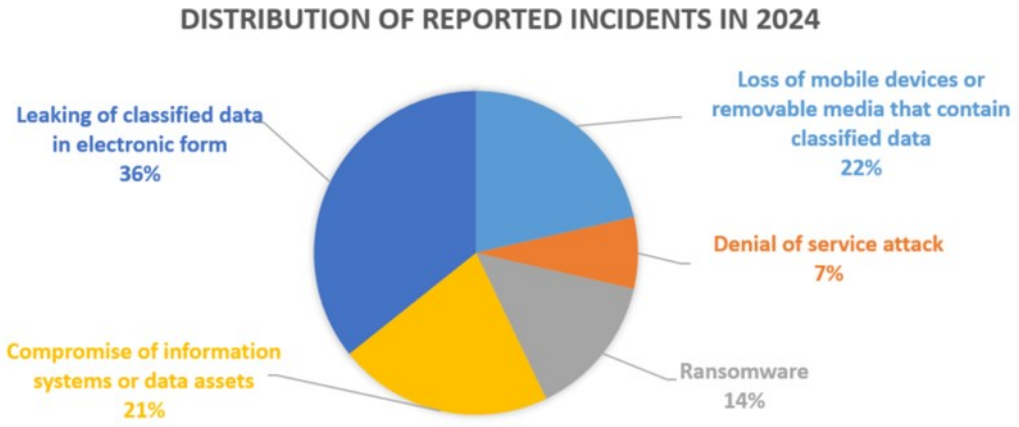
3. Activities and Operations

3.1 Alerts and Advisories

In 2024, GovCERT.HK issued 262 security alerts on known security vulnerabilities reported in common products. For those vulnerabilities with higher severity level, we proactively requested government departments to take prompt and appropriate preventive measures against potential information security risks.

3.2 Incident Handling Reports

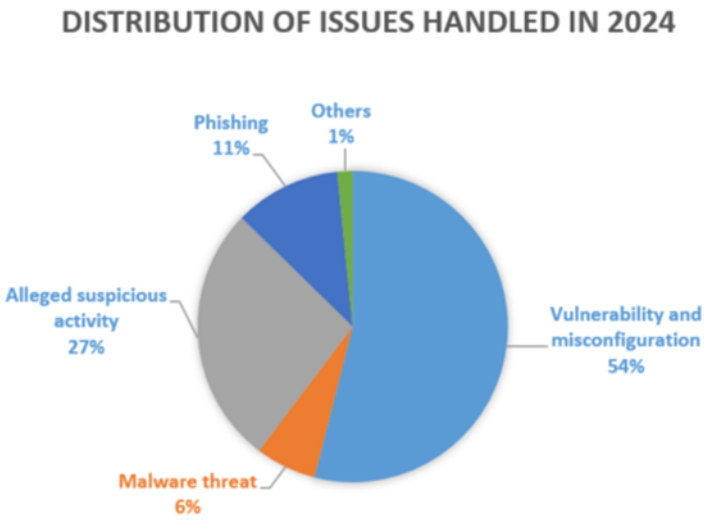
GovCERT.HK handled 14 reported incidents related to government installations, with the incident types shown below:



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

3.3 Abuse Statistics

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



3.4 Publications and Mass Media

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

- We partnered with Radio Television Hong Kong (RTHK) to broadcast radio episodes "e-World Smart Tips", covering a wide range of topics such as tips for sharenting tips, netiquette, Web 3.0, cloud services, smart travelling and safe use instant messaging and mobile devices, in a lively and interesting way. (www.cybersecurity.hk/en/media.php#Radio)
- We published practical leaflets and infographics with themes such as security tips for using QR codes and guide on using instant messaging to educate the public to protect themselves against cyberattacks. (www.cybersecurity.hk/en/resources.php)

- We organised "Together, We Create a Safe Cyberworld" Tram Body Design Contest. Many creative and impactful designs, interestingly raising public awareness of cybersecurity in an artistic way, were well-received, reminding the public from falling into online traps and strengthening the city-wide defence against cyberattacks.

Winning Entries

- We published a series of posts on the DPO Facebook page, with updates and tips on the latest cyber security news such as precautions for e-payment, privacy protection and data protection to enhance public awareness.

(http://www.facebook.com/digitalpolicyhk)

3.5 GovCERT.HK Technology Centre

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

4. Events Organised/Hosted

4.1 Training

Seminars/Webinars

In 2024, we organised various seminars, webinars and training featuring the latest IT security technologies and solutions, the latest cyber security threats and handling strategies. Over 7 000 government staff participated in the events with topics on security risk management, multi-factor authentication, Endpoint detection and response (EDR), Network detection and response (NDR) and protection against malicious web content.

In collaboration with the Civil Service College, we organised an Innovation and Technology (I&T) leadership series of thematic seminars to enhance the understanding and capabilities of government senior management in information system management, cybersecurity and data security.

Certificate in Cybersecurity for the Public Sector

With the aim to enhancing the skills of the staff of government departments and public organisations in IT management and applications, we worked closely with the HKIIT in 2024 to develop a wide range of IT-related training courses including the Certificate in Cybersecurity for the Public Sector which were recognised under the Hong Kong Qualifications Framework (HKQF).

4.2 Drills and Exercises

Inter-departmental Cyber Security Drill

GovCERT.HK joined hands with the CSTCB of HKPF to organise the annual inter-departmental cyber security drill (the Drill) to strengthen the preparedness and the overall incident response capability of bureaux and departments (B/Ds) to cyberattacks. Iin 2024, over 250 government officers from 70 B/Ds joined the Drill and online training workshop for sharing latest strategies and techniques in handling cyberattacks.

Cyber Health Check Exercise

A series of technical assessments was carried out to evaluate the effectiveness of existing security controls and identify potential weaknesses in government Internet-facing systems, critical infrastructure and mobile applications, with a view to building a stronger defence.

Hong Kong Cybersecurity Attack and Defence Drill 2024

We spearheaded to launch the first Hong Kong Cybersecurity Attack and Defence Drill in collaboration with the CSTCB of HKPF, HKIRC, and HKIIT in 2024, to enhance the technical skills, strategy, experience, and overall defence capabilities of participants in identifying and responding to cyberattacks. Blue Teams from government departments and public organisations participated in the drill, utilising their skills and knowledge to defence their information systems. Moreover, representatives from more than 50 organisations were invited as observers to gain insights and experience from the drill.

4.3 Conferences and Seminars

Build a Secure Cyberspace Promotional Campaign

A series of promotional activities under the theme “Together, We Create a Safe Cyberworld” were organised for businesses, organisations, schools and the public to raise their cyber security awareness and strengthen their cyber security postures. A set of interactive game booths were showcased for nine days at a shopping mall for fostering interest of the community in a fun environment while learning cybersecurity protection skills. Webinars and seminars were also organised under the campaign to further deepen cybersecurity knowledge of the participants.

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

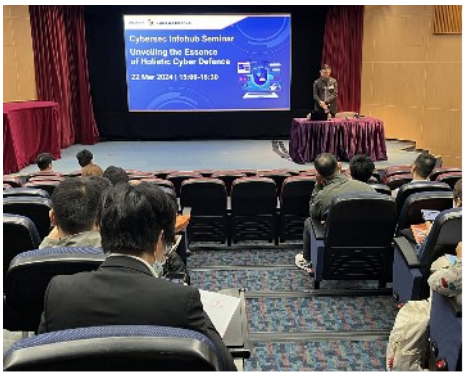
To promote cyber security awareness and cyber etiquette, we organised a total of 53 visits to primary and secondary schools, tertiary institutions, and NGOs to deliver information security talks to students, teachers, parents, service recipients and staff of NGOs.

InfoSec Tours with RTHK Radio 2

We continued to partner with the RTHK to conduct three InfoSec Tours with topics of "Cybersecurity and Information Literacy", "Safety Rules for the Cyberworld" and "Proctect yourself in the Cyberworld", which delivered information security messages in a relaxing way while promoting the importance of online safety and security.

Cybersec Infohub engagement activities

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



China Cybersecurity Week Hong Kong Sub-forum

We, along with the CSTCB of HKPF and the HKIRC, jointly organized the "China Cybersecurity Week Hong Kong Sub-forum 2024". A number of cybersecurity industry leaders and scholars from the Mainland and Hong Kong were invited as guest speakers to share and exchange views on the latest cybersecurity technologies and trends. The event attracted more than 200 public and private organisations with over 400 participants.

Cybersecurity Symposium 2024

We organised the Cybersecurity Symposium 2024 with the HKIRC and CSTCB of HKPF, aiming at fostering collaboration between public and private organisations and supporting Hong Kong's development as a leading digital economy, thereby strengthening Hong Kong's overall cybersecurity defence and resilience capabilities,. Several insightful keynote speeches and panel discussion sessions were held during the symposium. It brought together over 30 industry experts and business leaders from the Mainland and Hong Kong, as well as around 1 000 industry professionals from public and private organisations.

5. Local and International Collaboration

5.1 Local Collaboration

Promoting Cyber Security Information Sharing and Collaboration

We continued to promote and operate the Cybersec Infohub with HKIRC for establishing closer connections among local information security stakeholders. The programme attracted over 2 500 organisations and more than 3 700 representatives from various local sectors as of the end of 2024.

Nurturing Cyber Security Talents

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

- "CTF Challenge 2024" by HKCERT
- "Cyber Attack and Defence Elite Training cum Tournament" by HKIRC
- "Cyber Youth Programme 2024" including training courses, competition and a game-aided learning platform by HKIRC

Enhancing Overall Cyber Security Resilience

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

- "SME Cyber Security Connection Programme" including engagement with various SME associations by HKCERT
- "Healthy Web" with free web screening service by HKIRC
- "Cybersec Training Hub" with free training resources online by HKIRC
- "Cyber Security Staff Awareness Recognition Scheme 2024" by HKIRC

5.2 International Collaboration

To foster closer collaboration with international security experts for sharing experience in information security and for strengthening the knowledge base of emerging cyber threats, vulnerabilities and mitigation solutions, GovCERT.HK strived to learn from the CERT community on the global cyber security trends from different facets, including international standards development, global information security and data privacy policies and technological researches. GovCERT.HK participated in the following events in 2024:

- China Cybersecurity Week 2024
- 2024 China Cybersecurity Week' sub-forum in Macau
- APCERT Annual General Meeting and Conference
- APCERT Drill with the theme of "APT Group Attack Response: Where is Wally?"
- APCERT on-line training sessions
- CNCERT/CC Conference 2024
- NatCSIRT Meeting 2024 and 36th FIRST Annual Conference
- 2024 World Internet Conference Wuzhen Summit

Additionally, we signed a MoU with the Cyberspace Administration of Guangdong Province and the Comissão para a Cibersegurança of Macao SAR to facilitate cybersecurity exchange and collaboration in the Guangdong-Hong Kong-Macao Greater Bay Area (GBA). The MoU aims to a promote cybersecurity exchange and collaboration among the three regions, and provide robust cybersecurity support for building a digital GBA.

6. Future Plans

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

- Enhance the technical skills, strategy, experience, and overall defence capabilities of government departments and public sectors to effectively address emerging threats;
- Strengthen mechanisms for intelligence gathering and sharing within the government to improve responses to evolving threats;
- Foster connections and strengthen ties with local, regional, and international cybersecurity partners to ensure efficient communication during incident management;
- Collaborate closely with our partners to organise programs that nurture talents and promote cybersecurity awareness and resilience across different sectors; and
- Promote phishing awareness in the Government by launching a phishing drill campaign.

7. Conclusion

To maintain a secure and stable cyber environment that supports Hong Kong's development as a leading digital and smart city, GovCERT.HK will continue with its efforts to strengthen cybersecurity resilience and enhance security awareness throughout the community. By collaborating with various stakeholders, we will keep on to implement a wide range of programs aiming at empowering individuals and organisations to effectively navigate the complexities of the challenging environment, ensuring a sustainable growth and success in the digital landscape of Hong Kong.

HKCERT

Hong Kong Computer Emergency Response Team Coordination Centre

1. Highlights of 2024

1.1 Summary of Major Activities

- Rebranded the Chinese name of HKCERT to "香港網絡安全事故協調中心"
- Organised the "Build a Secure Cyberspace 2024 – Together, We Create a Safe Cyberworld" campaign with the Digital Policy Office and Hong Kong Police Force.
- Launched Tram Promotion to promote cyber security
- Organised the "2024 Cybersecurity Awareness Week Fun Day"
- Organised the "HKCERT Capture the Flag 2024"
- Released IoT research study on "Digital Signages"
- 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 emerging technology

1.2 Achievements & Milestones

- Organised the "Build a Secure Cyberspace 2024 – Together, We Create a Safe Cyberworld" campaign with the Digital Policy Office and Hong Kong Police Force. The campaign featured one webinar, one public seminar, a tram body design contest, and an award presentation ceremony. The contest attracted over 2,500 participants while more than 600 participants attended the webinar and seminar.
- Launched Tram Promotion. The promotion aimed to raise public awareness and adaptability regarding cyber security. Three trams featuring the winning designs from the "Together, We Create a Safe Cyberworld" tram body design contest toured along tram routes on Hong Kong Island, calling on all sectors of society to strengthen their awareness of cyber security.

- Organised the "2024 Cybersecurity Awareness Week Fun Day" to enhance public understanding of cyber security. The Fun Day was a nine-days exhibition and featured interactive game booths, offering a novel way to disseminate cyber security knowledge to the public.
- Organised "HKCERT Capture the Flag 2024". The HKCERT Capture the Flag 2024 event featured 3 workshops, a 48-hour online qualifying contest, a 1.5-day in-person competition for the finals and a public seminar with an award ceremony. This year marked the first time the competition included a physical component, with the top 5 teams from each category invited to compete on the same stage in the finals. The event drew a record-breaking 1,300 participants from renowned teams across Mainland China, other parts of Asia, Europe, and the United States.
- Released IoT research study on "Digital Signages". HKCERT researched eight different digital signage brands last year. The study identified 20 vulnerabilities, including 10 high-risk vulnerabilities requiring urgent remediation. HKCERT demonstrated common IoT attacks, showing how control could be gained in as little as three seconds.
- Published security advisories on latest risks on emerging technology and emerging cyber threats
- Continued the Healthcare Cyber Security Programme and Critical Infrastructure Cyber Security Programme.

2. About HKCERT

2.1 Establishment

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

2.2 Organisation and Workforce Power

The senior management of HKPC oversees the overall direction and operation of the centre. The daily operations are taken care 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 2024, HKCERT had handled 12,536 security incidents which was 62% increased of the previous year (see Figure 1).

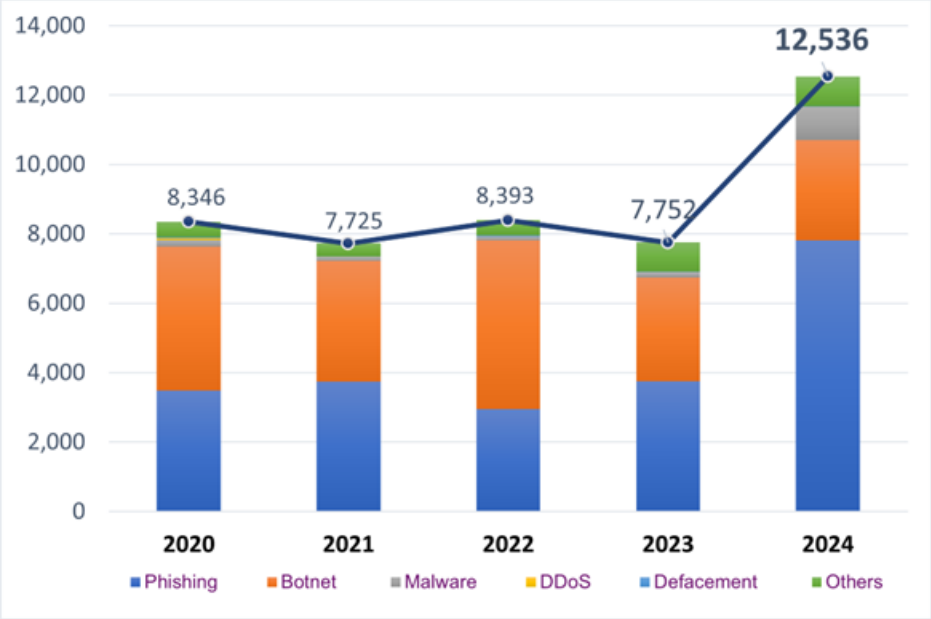


Figure 1. HKCERT Security Incident Reports

While the number of overall security incidents handled by HKCERT broke the record in 2024. It was the first time to hit over 10,000 cases. Phishing (7,811 cases or 62% of total cases) went up 108% and total phishing URLs was increased by 157%. Phishing primarily targeted the banking, finance and e-payment sectors, followed by social media, instant messaging, e-commerce, tech enterprises and public services respectively. Malware incidents also rose significantly in 2024, increasing 4.8-fold year-over-year, with most cases involving trojans targeting smart devices disguised as legitimate applications.

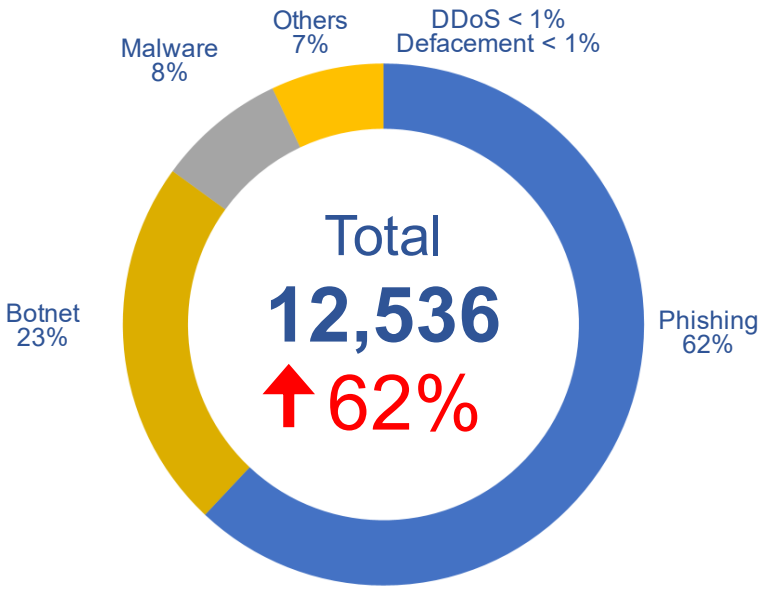


Figure 2. Distribution of Incident Reports

3.2 Watch and Warning

During the period from January to December of 2024, HKCERT published 428 security bulletins for the vulnerabilities of major software (see Figure 3) on the website. In addition, HKCERT have also published 26 security advisories, topics including 5 key risks in Hong Kong Cyber Security Outlook 2024 such as next-level phishing and topics covering emerging technology like deepfake and quantum computing.

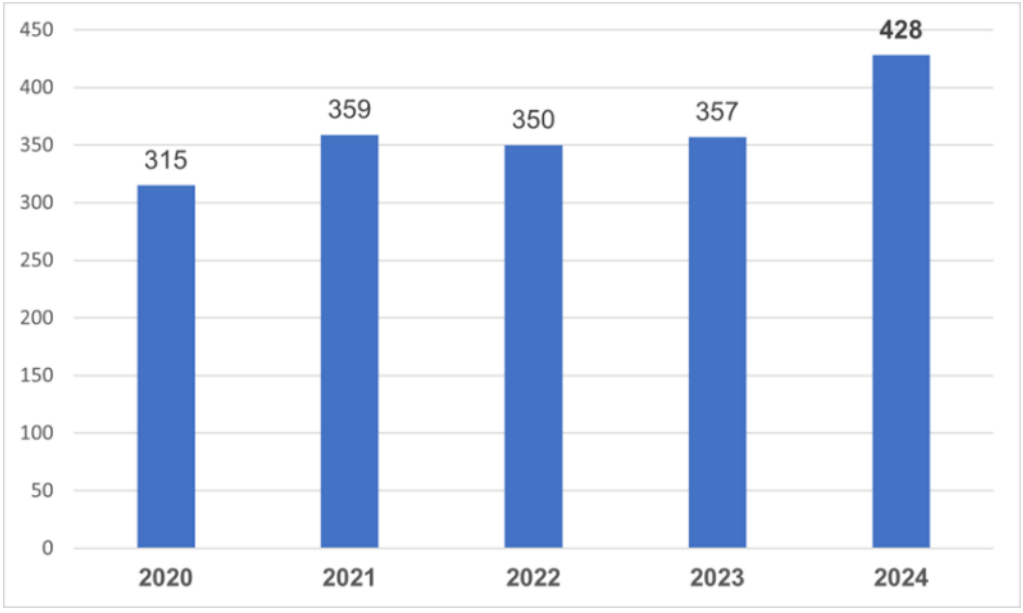


Figure 3. HKCERT Published Security Bulletins

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

3.2.1 Embrace Global Cyber Threat Intelligence

HKCERT used the Information Feed Analysis System (IFAS) to collect intelligence of compromised machines in Hong Kong from global security researchers. The system provided a better picture of security status of Hong Kong and a way to verify the effectiveness of the security incident response. For example, figure 4 showed the number of bot-related in Hong Kong network detected in IFAS reached a high count of 5,051 in 2024 Q3.

In May 2024, the U.S. Justice Department announced the successful dismantling of the "911 S5". Following the collapse of "911 S5", information about the infected devices was gradually released. In Hong Kong, HKCERT observed that over 2,000 IP addresses were infected by "911 S5" in the third quarter of 2024 from IFAS and HKCERT marked "911 S5" as the concerned botnet subsequently.

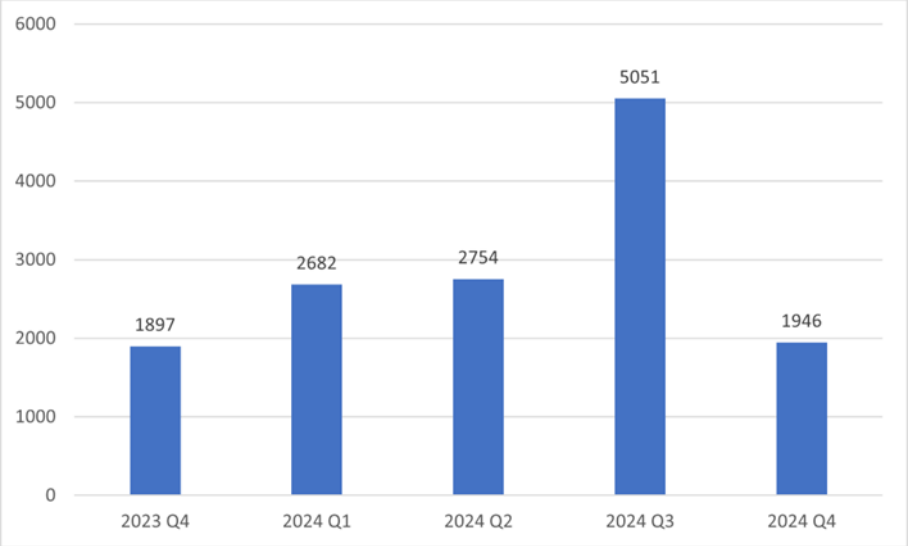


Figure 4. Trend of Bot related security events in the past year

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

3.3 Publications

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

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

4. Events organised and co-organised

4.1 Rebrand Chinese Name of HKCERT

HKCERT rebranded its new Chinese name to 香港網絡安全事故協調中心 and unveiled the launch of its cutting-edge technologies in the fight against cyber attacks. The rebranding better reflects the purpose and scope of HKCERT's services, enhancing the understanding of HKCERT in Hong Kong, especially small and medium-sized enterprises (SMEs) and the public.

Two new applications were introduced, leveraging artificial intelligence (AI) technology, to strengthen cyber attack detection and early alert capability, demonstrating HKCERT's commitment to enhancing overall cyber security protection in Hong Kong.

4.2 Build a Secure Cyberspace 2024 – Together, We Create a Safe Cyberworld

HKCERT jointly organised the "Build a Secure Cyberspace 2024" campaign with the Digital Policy Office and Hong Kong Police Force. The campaign involved 1 webinar, 1 public seminar and a tram body design contest. An award presentation ceremony was organised in Sep 2024.

For the tram body design contest, HKCERT received about more than 2,500 applications from Open Group, Secondary School and Primary School Group. A professional judge panel selected winners with most creative and meaningful. Winning entries: https://www.cybersecurity.hk/en/contest-2024.php)

4.3 Tram Promotion

The tram promotion aimed to raise public awareness and adaptability regarding cybersecurity. Three trams featuring the winning designs from the "Together, We Create a Safe Cyberworld" tram body design contest toured along tram routes on Hong Kong Island, calling on all sectors of society to strengthen their awareness of cybersecurity.

4.4 2024 Cybersecurity Awareness Week Fun Day

The cybersecurity exhibition ran from 7 September to 15 September 2024, at D·PARK in Tsuen Wan, with the 2024 Cybersecurity Awareness Week Fun Day taking place. HKCERT collaborated with renowned local illustrator DDED to create the brand new mascot（「網安小 C 虎」）

The Fun Day featured interactive game booths, offering a novel way to disseminate cybersecurity knowledge to the public.

4.5 HKCERT Capture the Flag 2024

The "HKCERT Capture the Flag 2024" partnered associations in information and education sectors. It was opened to all participants who were enthusiastic with Capture the Flag. This year, it was the first time for HKCERT CTF to have a qualifying and a final round. It was a success with more than 500 teams and 1,300 participants from universities, secondary schools, open categories and international. Following the final round, a public seminar with award ceremony was held in January 2025.

(Winners: https://www.hkcert.org/event/hkcert-capture-the-flag-challenge-2024-seminar-and-ceremony)

5. Collaboration

5.1 International Collaboration

HKCERT participated in a number of international coordination and collaboration events in year 2024:

- Participated in the AusCERT Conference 2024
- Participated in the FIRST Conference 2024
- Participated in the NatCSIRT Conference 2024
- Collaboration Meeting with CNCERT
- Participated in HITCON 2024
- Participated in 2024 APCERT Cyber Security Drill Exercise
- Participated in CNCERT Annual Conference
- Participated in CNCERT sub-forum in 2024 World Internet Conference Wuzhen Summit

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 1,400 companies, critical infrastructure organisations, banks and other enterprises in Hong Kong.
- HKCERT continued to work with police, ISPs and domain registries on closing down bulletproof hosting, phishing sites and botnet command and control centres in Hong Kong.
- HKCERT collaborated with Microsoft in the Healthcare Cyber Security Watch Programme to promote cyber security situational awareness in healthcare sector. The objective of this programme is to make use of global cyber threat intelligence to inform Hong Kong Healthcare sector of attacks targeting their IT infrastructure so that they can better mitigate security risks. The Programme was officially launched in December 2020 with 14 organisations including the Hospital Authority and most of the private hospitals in Hong Kong joining.
- HKCERT collaborated with Microsoft in the Critical Infrastructure Cyber Security Watch Programme to promote cyber security situational awareness in critical infrastructure sector. The objective of this programme is to make use of global cyber threat intelligence to inform Hong Kong critical infrastructure sector of attacks targeting their IT infrastructure so that they can better mitigate security risks. The Programme was officially launched in December 2021 with 7 organisations that provide essential public services to the citizens in Hong Kong joining.
- HKCERT collaborated with local regulators to deliver talks to related regulated organisations and members.
- HKCERT collaborated with local universities to conduct research on IoT and OT security.

6. Achievements & Milestones

6.1 Advisory Group Meeting

HKCERT had held two Advisory Group Meetings in September 2024. The meetings solicited inputs from the advisors and invited guests from SME associations on the development strategy of HKCERT.

6.2 Three Year Strategic Plan

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

6.3 Cyber Security Applications Leveraging AI

HKCERT had launched two cyber security applications leveraging AI technology. The first application aims to address the increasing severity of phishing attacks by using AI system that proactively detects and distinguishes phishing URLs. Upon detection, HKCERT will promptly take action to remove the phishing URLs, reducing the chances of individuals falling victims to phishing attacks. It is a collaboration work with AusCERT. Another application is cyber security risk alert system. This system utilises AI to analyse and access trends in phishing, malware, and botnet attacks specific to Hong Kong. It then disseminates alerts and defence measures to the public, enabling early prevention.

6.4 Security Guidelines and Advisories for Security Outlook 2024

HKCERT published different security guidelines and alerts in response to the cyber threats and incidents mentioned in "Year Ender Press Briefing 2024", such as attacks using artificial intelligence, next type of phishing attack and etc.

6.5 IoT Research on Digital Signage

HKCERT conducted the Cyber Security Awareness Survey on IoT Digital Signage from July to September last year. The survey involved telephone interviews with 624 companies across various industries, including retail and tourism, information and communication technology, public relations, financial services, professional services, non-profit organisations and schools. The aim was to understand and analyse the cyber security awareness of organisations regarding the use of digital signages and IoT.

HKCERT researched eight different digital signage brands. The study identified 20 vulnerabilities, including 10 high-risk vulnerabilities requiring urgent remediation. HKCERT demonstrated common IoT attacks, showing how control could be gained in as little as three seconds.

HKCERT has published a guideline for digital signage provide best practices and security measures for digital signage users, operators, advertisers and technology providers, in order to enhance the safety and privacy of the public, also ensure the long-term sustainable development of digital signage technology.

(IoT Security Guideline for Digital Signage https://www.hkcert.org/security-guideline/iot-security-guideline-for-digital-signage)

6.6 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.

6.7 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.

6.8 Year Ender Press Briefing

HKCERT organised a year ender press briefing to media in January 2025 to review cyber security landscape of 2024 and provided a cyber security forecast to 2025 to warn the public for better awareness and preparedness. It received very good press coverage.

7. Future Plans

7.1 Strategy

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

7.2 Funding

HKCERT had secured Government funding to provide the basic CERT services in 2025/2026. We shall work closely with the Government to plan for the future services of HKCERT and seek their support.

7.3 Enhancement Areas

HKCERT will launch a "Cyber Security Vendor List" theme page. This page will include trusted vendors who have passed the checklist created by HKCERT. Organisations can refer to the list to select vendors with good reputations.
HKCERT will continue to conduct IoT research as IoT networks become increasingly complex and are likely to be targeted

by attackers.

HKCERT will continue to organise the Capture the Flag (CTF) contest, HKCERT will continue to partner with different associations to organise another CTF in 2025 for the participants from universities, secondary schools and open categories.

8. Conclusion

In 2024, the number of overall security incidents reported to HKCERT increased by 62% and broke the record. The phishing cases and phishing URLs recorded a rise, increased by 62% and 157% respectively. It became the first major security incident in Hong Kong. Malware cases also recorded a rise, increased by 4.8-fold due to adding new sources of threat intelligence.

In 2025, HKCERT will continue to actively study the trends of cyber attacks and security technologies, and assist the community in meeting the ever-changing security challenges through various channels, such as issuing early warnings of cyber attacks, security recommendations, etc. HKCERT will also organise major international seminars and competitions such as Capture the Flag competition, to raise local cyber security awareness and nurture the next generation of cyber security talents.

There are five major information security risks that must be addressed in 2025:

1. Rising Risks from Third-Party

Risks from suppliers, contractors, or service providers can lead to serious consequences including legal proceedings and compensation claims. Security vulnerabilities in third-party software, applications and open-source code may result in cyber attacks and data breaches. Third-party risks can also lead to supply chain attacks, where hackers gain access to targeted enterprise systems through collaborating partners.

2. Risks of Leakage and Data Poisoning in LLMs

Large language models face data leakage and poisoning attacks: Prompt Hacking involves designing and manipulating input prompts to mislead models into outputting restricted information; Adversarial Attacks involve manipulating training data to influence future model judgments.

3. AI-Driven Cyber Attacks and Scams

Hackers actively discuss methods to jailbreak generative AI like ChatGPT to produce restricted content including generating malwares and phishing messages. GPTs designed for crimes reflect “weaponisation of AI” remains a security risk.

4. Increasing Cyber Attacks on Critical Infrastructure

Global critical infrastructure continues to face significant risks from cyber attacks. In 2024, there was a notable increase in attacks on critical infrastructure worldwide, including a ransomware attack on a Hong Kong hospital.

5. Cyber Security Challenges of IoT

IoT devices have already permeated various aspects of our daily lives such as digital signages, drones and smart home devices. However, if cyber security measures are inadequate, these devices can be easily compromised by hackers. HKCERT has found that digital signages available on the market possess common security vulnerabilities, making them susceptible to IoT attacks by hackers.

JPCERT/CC

Japan Computer Emergency Response Team / Coordination Center

1. Highlights of 2024

1.1 Summary of major activities

JPCERT/CC has been a member of FIRST, The Forum of Incident Response and Security Teams since 1998. FIRST holds annual conferences with the aim of sharing information about the latest trends in the prevention, handling, and technical analysis of cyber incidents, as well as strengthening collaboration in incident handling. The conference in 2024 was held in Fukuoka from June 9 to 14. JPCERT/CC served as the local host of the conference and supported FIRST by assisting visa applications for overseas participants and coordinating with domestic parties. In the exhibition area, we set up a local host booth and introduced the various activities of JPCERT/CC, including a demonstration of our incident investigation tools.
Through our support for this conference, we were able to highlight our contribution to FIRST over many years and reinforce our presence. Going forward, we intend to actively engage in various FIRST activities, such as events and Special Interest Groups (SIGs) and contribute to the promotion of international cooperation among CSIRTs.

Please refer to the following web page for details about the 36th Annual FIRST Conference.
36th Annual FIRST Conference
https://www.first.org/conference/2024/

1.2 Achievements & milestones

JPCERT/CC now oversees 10 CNAs as a Root
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 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 to work together in vulnerability coordination and information distribution. In 2024, 2 new organisations in Japan joined the CVE program as a CNA. Moving forward, JPCERT/CC is working on building even more effective distribution channels for vulnerability information through activities geared to the popularization of the CVE Program, such as establishing CVD working group in APCERT.

2. About CSIRT

2.1 Introduction

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

2.2 Constituency

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

3. Activities & Operations

3.1 Incident handling reports

In 2024, JPCERT/CC received 47,677 computer security incident reports from Japan and overseas.

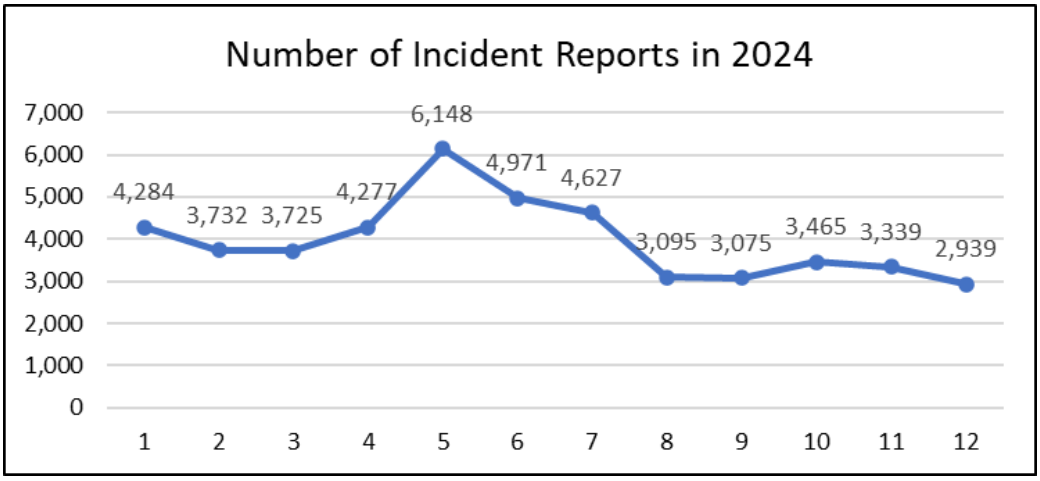


Figure 1. Number of Incident Reports (2024)

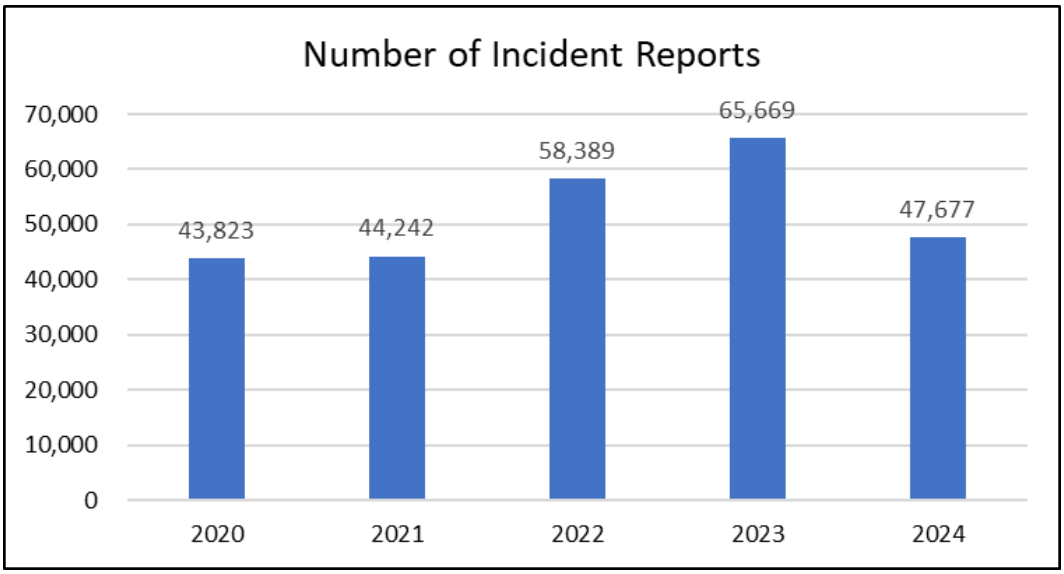


Figure 2. Incident reports to JPCERT/CC (2020-2024)

3.2 Abuse statistics

Incidents reported to JPCERT/CC during the last quarter of 2024 were categorized in Figure 3. More than 80% of the reports were on phishing sites, followed by scan.

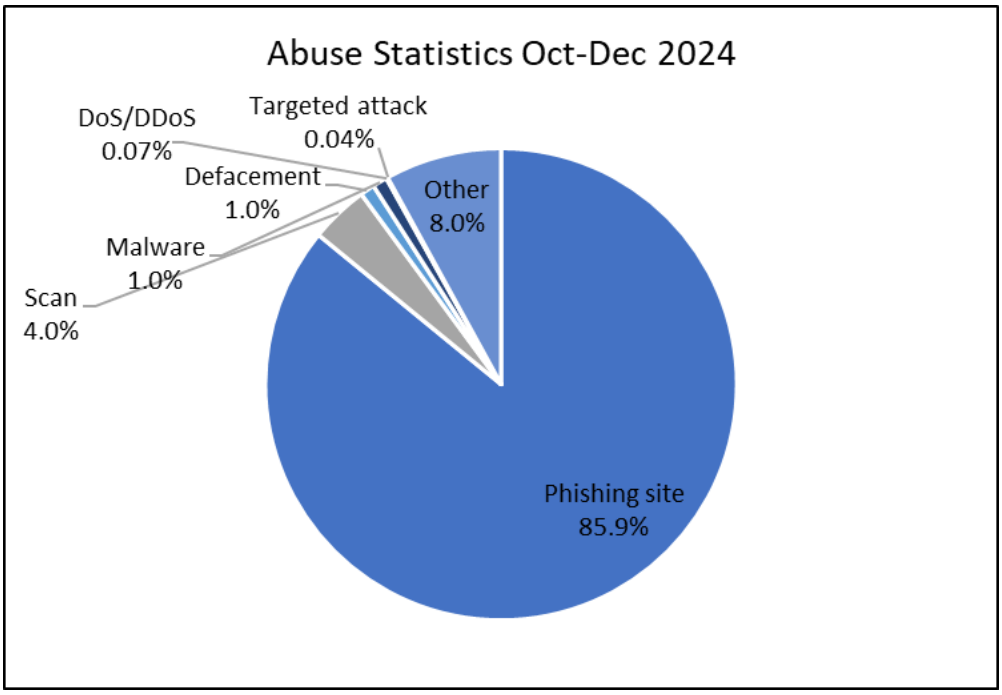


Figure 3. Abuse Statistics of Oct-Dec 2024

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 2024, 18 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)

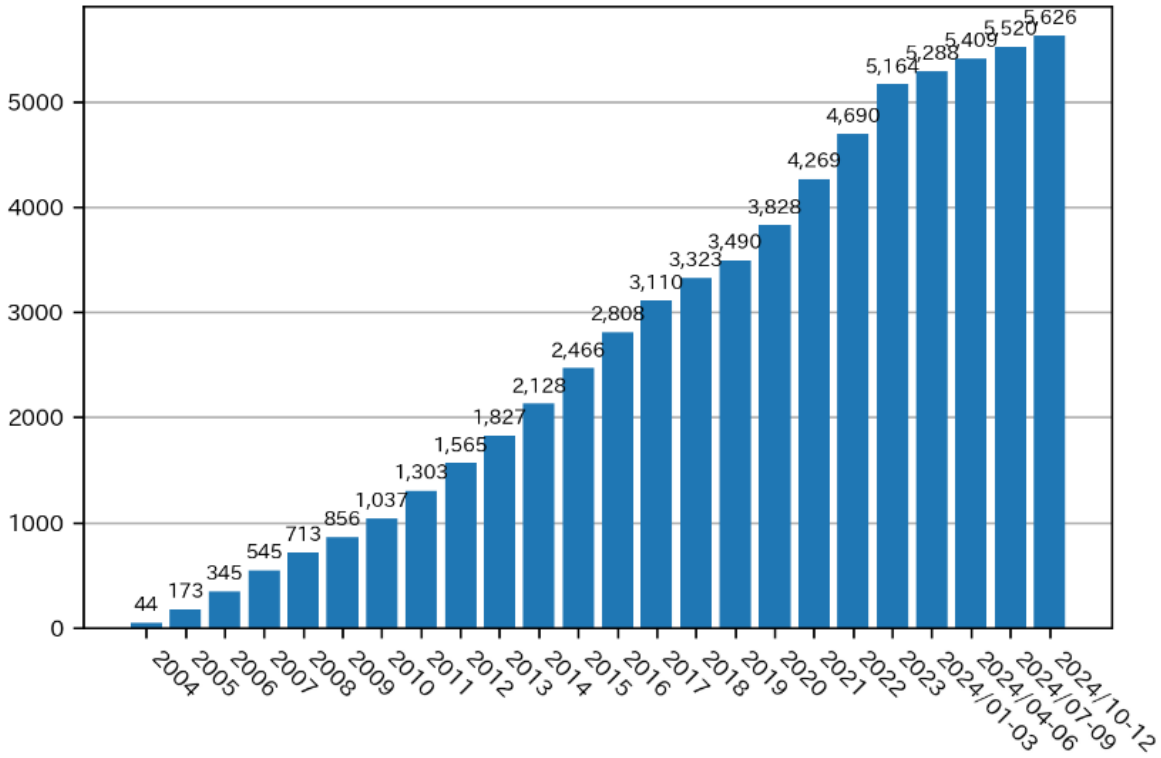
https://jvn.jp/en/ (English)

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).

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

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

Figure 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

Weekly Report

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

JPCERT/CC Eyes (Official Blog)

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

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

Quarterly Activity Reports

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

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

X (Twitter)

https://x.com/jpcert_en

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

GitHub

https://github.com/JPCERTCC

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

YouTube

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

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

3.4 Associations and Communities

Nippon CSIRT Association (NCA)

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

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

Council of Anti-Phishing Japan

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

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

4. Events organized / hosted

4.1 Training, Seminars and Workshops

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

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

5. International Collaboration

5.1 International partnerships and agreements

MoU

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

FIRST (Forum of Incident Response and Security Teams)

https://www.first.org

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

APCERT (Asia Pacific Computer Response Team)

https://www.apcert.org/

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

5.2 Capacity building

5.2.1 Drills & Exercises

JPCERT/CC participated in the following drills in 2024 to review our incident response capability:

- Locked Shields 2024 (23-26 April)
- APCERT Drill 2024 (29 August)
- ASEAN CERTs Incident Drill (ACID) 2024 (15 October)

5.2.2 Seminars & presentations

In 2024, JPCERT/CC delivered presentations at international cyber security events including:

- CVE/FIRST VulnCon (March, Raleigh)
- FIRST Annual Conference (June, Fukuoka)
- APAC DNS Forum (July, Indonesia)
- APISC Training Course (September, Seoul)
- Internet Governance Forum (December, Riyadh)
- FIRST & AfricaCERT Symposium (November, online)

5.2.3 Other international activities

In 2024, JPCERT/CC attended international cyber security events including;

- M3AAWG General Meeting
- NatCSIRT Meeting
- RECON
- BSidesLV
- BlackHat USA
- DEFCON
- Virus Bulletin
- RightsCon

6. Future Plans

6.1 Future projects/Operation

Enhance CVD-related activities both domestic and international context

JPCERT/CC has been a CVE Numbering Authority (CNA) since 2010 and actively participated in CVE program as a Root. With the aim to bolster the engagement in the area of Coordinated Vulnerability Disclosure in the Asia Pacific region, especially among the leading CSIRTs, JPCERT/CC launched APCERT CVD WG in 2023. The team is committed to increasing Asia and Pacific's regional representation in CVD activities through the WG. As a part of the activities, JPCERT/CC is actively involved in international discussions about a wide range of CVD-related topics such as SBOM.

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

1. Highlights of 2024

1.1 Summary of major activities

2024 was a memorable year in which Korea achieved level 1 in the ITU (International Telecommunication Union) Global Cyber Index (GCI). This accomplishment reflects the positive evaluation of the dedicated efforts made by KrCERT/CC and other related organizations in Korea to strengthen cybersecurity. Throughout 2024, the government took proactive steps to address cyber threats, particularly phishing attacks targeting citizens. A specialized unit was established to enhance the country's response to phishing incidents, and comprehensive countermeasures were developed and announced with the ultimate goal of eradicating such attacks. Accordingly, KrCERT/CC established the Digital User Damage Response Division to more effectively prevent and respond to phishing attacks that put citizens at risk. Furthermore, KrCERT/CC made significant improvements to its cyber exercise training platform, aimed at bolstering security capabilities of enterprises. KrCERT/CC also provided tailored prevention services, delivering customized datasets to help enterprises respond to the increasing threats posed by the misuse of AI technologies. Lastly, 2024 was a landmark year for KrCERT/CC as it assumed the chairmanship of the APCERT (Asia Pacific Computer Emergency Response Team) for the first time. In this role, KrCERT/CC made valuable contributions to the activities of APCERT by hosting APCERT annual cyber drill and organizing APCERT Membership Awards to further promote collaboration within the region.

1.2 Achievements & milestones

i. Improvement of National Cyber Security to the Global Top Level: In the fifth edition of the GCI, an initiative of ITU, Korea was included in the level 1 group. The Korea Internet & Security Agency (KISA), which is the parent organization of KrCERT/CC, oversees the GCI response and KrCERT/CC supports the KISA operations. KrCERT/CC, as one of the national pillars for cyber security, inspected and supplemented on the insufficiencies pointed out in the fourth edition, and significantly improved the GCI evaluation scores from 78 points for the second edition in 2017 to 100 points for the fifth edition in 2024.

ii. Development of Phishing Zero Strategies: In 2024, according to the phishing eradication measures announced by the government, KrCERT/CC installed the Digital User Damage Response Division. In addition, under the catchphrase of "Zero Phishing," it established zero exposure to crime (blocking phishing trick text messages and phone calls), zero attack diffusion (tracking and removing phishing crime infrastructure) and zero phishing damage (treating malicious app infections and protecting victims) strategies. As part of the effort, KrCERT/CC commenced the Qshing identification service, which is to identify if a QR code is used for phishing, in order to prevent citizens' damage caused by the QR code fraud that had surfaced as an issue. It also introduced the text message authentication mark to prevent damages resulting from phishing text messages sent by abusing overseas text messages sent through roaming, thereby raising awareness of people receiving text messages sent from abroad.

iii. Reinforcement of Corporate Autonomy for Cyber Exercise Training Platform: For hacking email response drills in the past, text-type emails were mostly sent to facilitate identification of training progresses. However, following this measure, enterprises could create images similar to the actual phishing emails and, accordingly, customized hacking emails with characteristics of each department reflected. In addition, while enterprises had to analyze the follow-up measures themselves in the past, the improved platform analyzed the results and also recommended information security services necessary for the enterprises.

iv. Datasets for Threats Customized to Companies Introducing AI Technologies: The enterprises that had introduced AI technologies in line with the diffusion of AI technologies were provided with the latest AI datasets (300 million datasets for security threats, such as generative AI abuse, malicious codes for IoT/mobile attack and vulnerabilities).

v. TTPs #11: Operation Octopus - While a focus was placed on tracking down ransomware hacking groups predicted to be backed by specific countries in 2023, in 2024, KrCERT/CC expanded information collection on the infrastructure of hacking groups through cooperation with overseas organizations and started applying threat hunting-based tracking technologies. In 2024, KrCERT/CC analyzed attack strategies aiming for centralized management solutions and announced the results.

*Refer to www.boho.or.kr (attach link)

vi. Following the chair election at the AGM in 2023, KrCERT/CC served as the chair of the APCERT in 2024. As the chair, a Steering Committee member and an APCERT Operational Member, KrCERT/CC has contributed continuously to the community. In 2024, it hosted the APCERT annual cyber drill under the subject to APT attack group response, and successfully held the APCERT Membership Awards, which began in 2022, as an in-person ceremony.

vii. KrCERT/CC organized the APISC training with invited instructors on incident response to share and exchange knowledge and experiences among global CSIRTs in addition to the APCERT members. It also hosted alumni workshops to discuss the importance of cooperation.

2. Activities & Operations

2.1 Incident handling reports

According to Article 48-3 (Report on Computer Security Incidents) of the Act on Promotion of Information and Communications Network Utilization and Information Protection, KrCERT/CC receives reports on security incidents from information and communications service providers in the private sector. The number of incident reports in each year increased by approximately 48% from 1,277 in 2023 to 1,887 in 2024. As for the half-yearly reports from 2022 to 2024, 473 and 669 incidents were reported in the first half and the second half of 2022 respectively, and 664 and 613 incidents were reported in the first half and the second half of 2023 respectively. In the first half of 2024, 899 incidents were reported, which increased by 35% from those in the first half of the previous year, and in the second half of 2024, 988 incidents were reported, which increased by 61% from those in the second half of the previous year. The increases are presumed to have resulted from a significant rise in the number of server hacking attacks (553) through the attackers' abusing of hacking bypass sites.

Category	2022		2023		2024	
	1st half	2nd half	1st half	2nd half	1st half	2nd half
Incidents Reported	473	669	664	613	899	988
Total	1,142		1,277		1,887	

As for the statistics on malware infection among the types of incidents reported, 85% or more of malware infections were reported as ransomware attacks. The number of ransomware reports had increased rapidly by 8.3 times over four years until 2022 (325 cases), and started decreasing to 259 in 2023 and 195 in 2024. The number of ransomware incidents reported in 2024 decreased by 24% year-on-year. The number decreased by 15% to 34 for middle-standing enterprises and by 25% to 150 for SMEs from the previous year. In addition, the percentage of incidents of middle-standing enterprises and SMEs represented 94% of all incidents.

Category		2023		2023		2024		2024	
		1st half	%	2nd half	%	1st half	%	2nd half	%
Incidents Reported	DDoS attacks	124	18.7	89	14.5	153	17.0	132	13.4
	Malicious codes	156	23.5	144	23.5	106	11.8	123	12.4
	(Ransomware)	(134)	(20.2)	(124)	(20.2)	(92)	(10.2)	(103)	(10.4)
	Server hackings	320	48.2	263	42.9	504	56.1	553	56.0
	Other	64	9.6	117	19.1	136	15.1	180	18.2
Total		664		613		899		988	

2.2 Publications

In 2024, KrCERT/CC distributed six technical reports including one cyber threat forecast report, eight rules and guidelines and two trend reports. The distributed data can be found on the KrCERT/CC website (www.boho.or.kr).

2.3 New services

Qshing identification service
Text message authentication mark introduced

3. Events Organized / Hosted

3.1 Training

KrCERT/CC holds training by inviting internal and external instructors with a goal of information sharing and knowledge exchange among the employees. In addition, it organizes separate sessions for insight sharing following attendance at conferences abroad.

3.2 Drills & exercises

Mock Training for Cyber Crisis Response in the Private Sector: First half and second half of the year

3.3 Conferences and seminars

KrCERT/CC directly hosts and sponsors various domestic conferences.

- The 28th Hacking Prevention Workshop (Dec.)
- AI Security Day (Sep.)
- The 3rd Ransomware Resilience Conference (Sep.)
- International Information Security Conference on the 13th Information Security Day (Jul.)

4. International Collaboration

4.1 Capacity building

4.1.1 Training

- APCERT – Incident Handling(Jan)
- APCERT – Experience sharing on Social Media Incident Handling by Bhutan Computer Incident Response Team(Dec)

4.1.2 Drills & exercises

- 2024 APCERT Cyber Drill(Aug)
- 2024 ASEAN Cyber Incident Drill(Oct)

4.1.3 Seminars & presentations

- JSAC 2024 Conference(Jan)
- GCTF 2025 Workshop(May)
- National CSIRT meeting(Jun)

5. Future Plans

5.1 Future projects

Looking ahead, KrCERT/CC is seeking to shift the approach from responding to smishing attacks after they occur to preventing citizens' damage right from the stage when smishing text messages are sent. KrCERT/CC will continue supporting APCERT in its role as chair, hosting the annual cyber drill, and engaging in other related activities.

6. Conclusion

2024 has been a year in which KrCERT/CC dedicated efforts to assisting citizens suffering direct damages caused by phishing attacks. With the newly established Digital User Damage Response Division, KrCERT/CC will strive to create a more convenient and safer cyber space for citizens by continuously improving its systems and services.

LaoCERT

Lao Computer Emergency Response Team

1. Highlights of 2024

1.1 Summary of Activities

- Organized Lao Digital Week event on 10–14 January 2024 at Km 6 Conference Hall, in Vientiane Capital, Lao PDR. Participants from all IT Private Company and Government sectors.
- Co-Organized workshop on Building a more inclusive and resilient cyberspace for the ASEAN women's community for ASEAN Member States on 26 to 27 September 2024 at Crowne Plaza Hotel, Vientiane Capital, Lao PDR. The workshop is designed to equip AMS women with the knowledge and tools to navigate cyberspace confidently, including digital literacy, online safety practices, and the capacity to formulate effective awareness campaigns on cyber threats. Participants have learned about methodologies and mechanisms to protect and prevent falling victim to online scams and cyberthreats.

1.2 Achievements & milestones

- Disseminated the use of social media security in Vientiane Capital and provincial
- Completed the National Cybersecurity Strategy issued by 14 August 2024.

2. About LaoCERT

2.1 Introduction

Lao Computer Emergency Response Team (LaoCERT) is the national CERT of Lao PDR, under, Ministry of Technology and Communications and it develop on capacity building for its staffs in the field of cyber security with other CERTs organizations in the region to against with cyber-attack. LaoCERT has been promoted to public and has been known among IT social, government agencies, private organizations in Laos PDR as well as international CERTs and LaoCERT

was a member of APCERT in 2014. This annual report will describe activities and operation of LaoCERT in 2024.

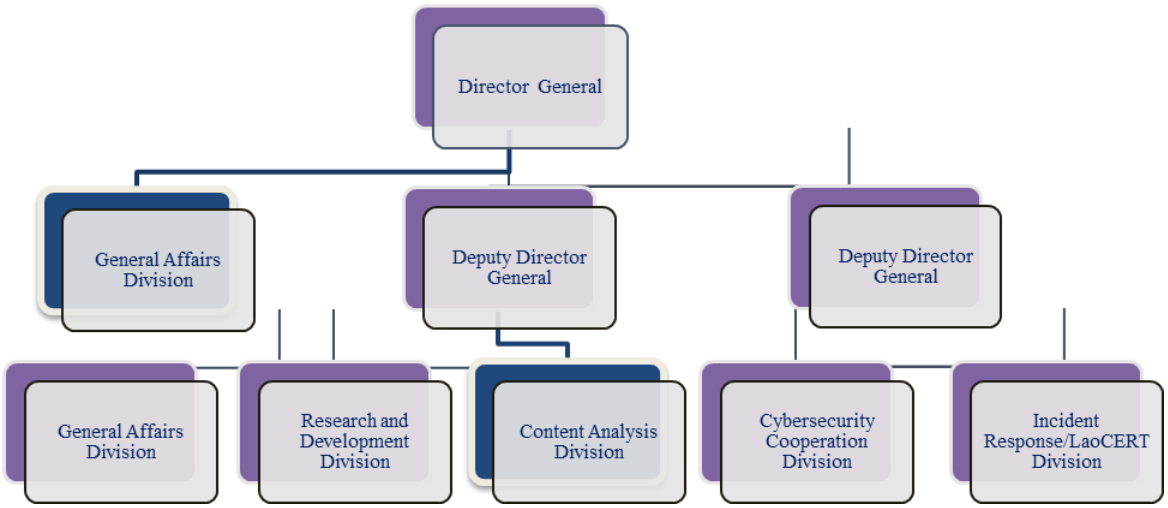
2.2 Establishment

LaoCERT was established in February 2012 by degree 220/MPT as a LaoCERT division under the Lao National Internet Center, Ministry of Post and Telecommunications (MPT), Government of Lao PDR. It was established by following up as ITU-IMPACT recommendations and it has been announcement to become the national CERT equivalent department in 2016, directly under to the Ministry of Post and Telecommunications.

Currently, the Ministry of Post and Telecommunications has been renamed the Ministry of Technology and Communications and also LaoCERT has been promoted to become the Department of Cyber Security under the Ministry of Technology and Communications (MTC).

2.3 Resource

Department of Cyber Security/LaoCERT currently consist of 5 divisions which control by 1 director general and 3 deputy director generals with the total number of staffs: 28 people, 7 are women.



Department/LaoCERT Organization Charts

2.4 Constituency

Department of Cyber Security/LaoCERT is a coordination center of cyber security within Laos and also cooperation with international CERT organizations in the field of cyber security. Department/LaoCERT is responsible for incident handling, cyber security protection, disseminating information security and awareness raising for ensuring the cyber safety to all citizens, government agency and private organizations include education institute, banks, internet service providers...etc. in Lao PDR.

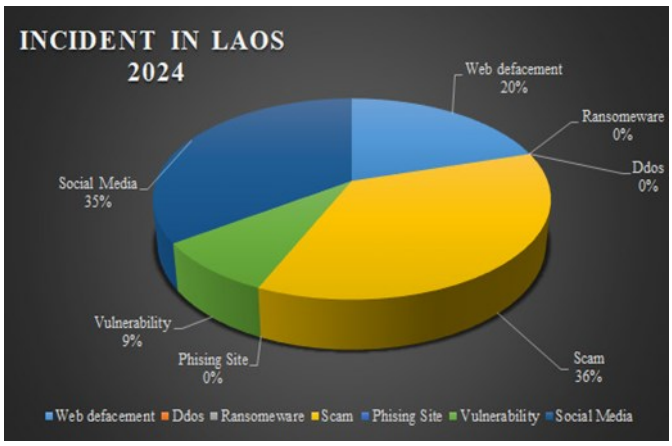
3. Activities & Operations

3.1 Scope and definition

Department of Cyber Security/LaoCERT aim to awareness raising on cyber security and solving issue on cyber security incident response as well as to collaboration with other CERT organizations to against with cyber-attack.

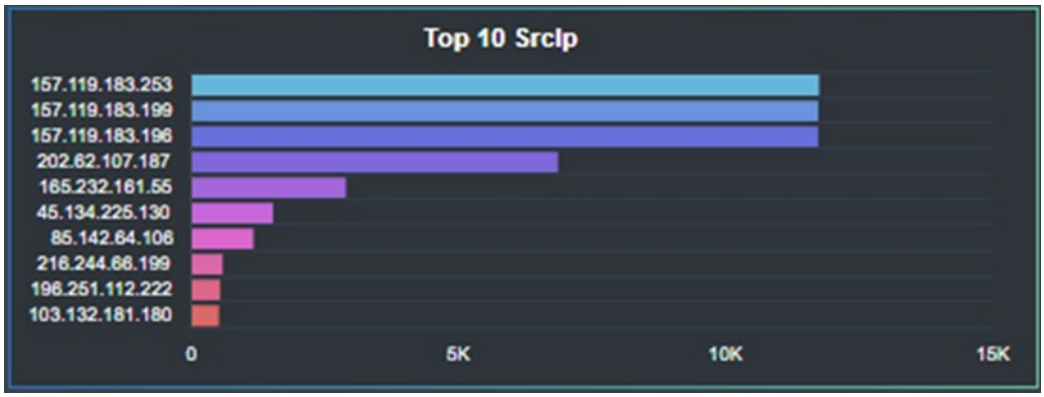
3.2 Incident handling report

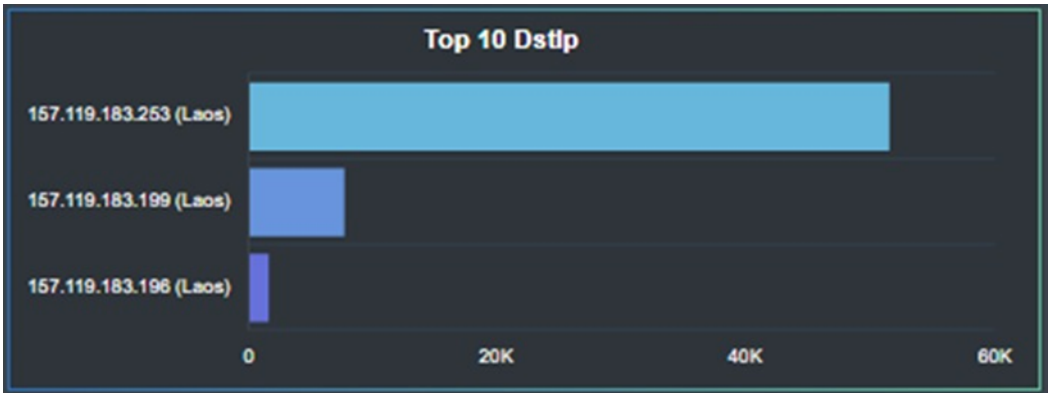
The following graph shows the statistic of incidents that happened in 2024.

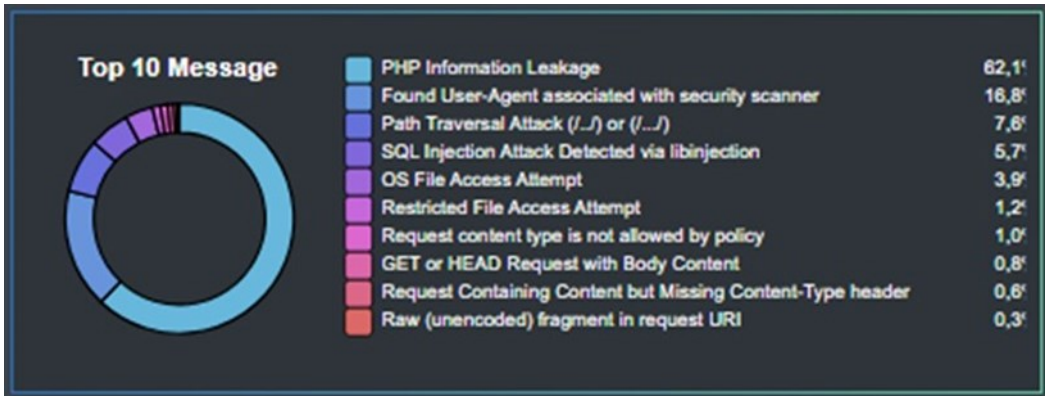


3.3 Abuse Statistics

The following graph shows Abuse Statistics in 2024:







3.4 Publication

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

3.5 New Services

- Website vulnerability scanning
- Advisory on the use of Social Media Security.
- Awareness raising on Cyber security to society.
- Provide training related cyber security.

4. Events organized / hosted

4.1 Training

- Organized Lao Cyber Security Hacking Challenge with Cyberus Company in Vientiane, Lao PDR.
- Organized Workshop on Cybercrime, Digital Forensic and Digital Evidence on 19-21 June 2024 with UNODC organization in Vientiane Capital, Lao PDR.
- Co-Organized Training with CyberCX Company (Australia) on Cyber Security Incident Response on 22-26 July 2024 in Vientiane Capital, Lao PDR.

4.2 Conferences and seminars

- Co- Host the workshop with Australia National University (ANU) on the Cyber Bootcamp Program Lao PDR from 26 February – 01 March 2024 at Crowne Plaza Hotel, Vientiane, Lao PDR.
- Co-Organized Workshop with CyberCX Company (Australia) on Cyber Security and Critical Information Infrastructure Service and Capabilities on 3-7 June 2024 in Vientiane Capital, Lao PDR.
- Co-Organized the workshop on Threat Hunting Workshop with Palo Alto Networks & Vintcom Technology company on 21 August 2024.
- Co-Organized workshop on Building a more inclusive and resilient cyberspace for the ASEAN women's community for ASEAN Member States on 26 to 27 September 2024 at Crowne Plaza Hotel, Vientiane Capital, Lao PDR.

5. International Collaboration

5.1 International partnership and agreement

In 2024, Department of Cyber security/LaoCERT has signed Memorandum of Cooperation (MOC) with Authority of Information Security (AIS), MIC of Vietnam, Signed on 10 September 2024.

5.2 Capacity Building

5.2.1 Training

The following has shown the statistic for attended the training in 2024:

- The UNODC Regional Ransomware investigate Training Exercise- Second Batch 16-20 January 2024 in Philippine.
- The APT Training Course on Cyber Security Technologies-Cyber threat from 17-26 January 2024.
- The 29th AJCCBC Cybersecurity Technical Training-J5 on penetration Test from 22-26 January 2024 in Bangkok, Thailand.
- The training course on Cybersecurity analysist from 22 January – 02 February 2024 in Indonesia.
- The training course on ICT core personnel Development (C) Information Security from 24 January – 25 February 2024.
- The Training course on Computer Ethical Hacking 19-23 February 2024 in Singapore.
- The training course on Defense Practice Against Cyber Attacks from 19 May – 01 June 2024 in Japan.
- The 30th AJCCBC Cybersecurity Technical Training J7 on Cyber Defense Exercise with Recurrence (CYDER) and Malware Analysis 27-31 May 2024 in Bangkok, Thailand.
- The training course on Investigating Criminal Use Cryptocurrencies Session 5 from 3-7 June 2024 in Bangkok, Thailand.
- The Capacity Building on Enhancement Scientific and Technological Indicators and Statistical system from 3-18 August 2024 in South Korea.
- The 31th AJCCBC Cybersecurity Technical Training-J8 Trainer Training in Network Forensics from 18-24 August 2024 in Bangkok, Thailand.
- The Asia-pacific Information Security Training Course 2024 from 22-28 September 2024 in South Korea.
- The 32th AJCCBC Cybersecurity Technical Training-J9 from 10-16 November 2024 in Bangkok, Thailand.
- The Workshop for Regional CERT Cooperation in ASEAN from 12-13 December 2024 in Japan.

5.2.2 Drills and Exercises

The following has shown the statistic for participated Drills and Exercises in 2024:

- APCERT Cyber Drill 2024.
- ASEAN CERT Incident Drill (ACID) 2024
- The ASEAN CyberKid Camp 2024 from 6-9 August 2024 in Hanoi, Vietnam.
- Attend the Cyber SEA Game on 24-25 October 2024 in Bangkok, Thailand.
- The 2024 Regional Cyberdrill for Asia and the Pacific Region from 19-21 November 2024 in Brunei.
- The 2nd ASEAN Cyber Shield (ACS) Hacking Contest from 19-23 November 2024 in Vietnam.

5.2.3 Seminar and presentation

The following has shown the statistic for participated the Seminar, Workshop and Meeting in 2024:

- The 1st ASEAN-Japan Cybersecurity Working Group Meeting on 6-7 February 2024 in Thailand.
- The Workshop for The 14th ASEAN-Japan Information Security Workshop for ISPs on 7-8 March 2024 in Tokyo,

Japan.

- The Cloud Security workshop on 20-25 April 2024 in Thailand.
- The 2nd ASEAN-Japan Cybersecurity Working Group Meeting on 21-21 May 2024 in Cambodia.
- The UNODC High-Level joint Policy Dialogue on cybercrime and E-evidence Strategies workshop on 28-29 May 2024 in Malaysia.
- The 15th ASEAN Network Security Action Council Meeting on 23-25 June 2024 in Brunei.
- The workshop on Executive course on International Law of Cyber Operations from 30 June-6 July 2024 in Singapore.
- The 6th Meridian Conference on Critical Information Infrastructure Protection (CIIP) workshops from 3-6 July 2024 in India.
- The Alumni Workshop on International Law of Cyber Operations from 8-10 July 2024 in Singapore.
- The 9th Annual Meeting of the Cyber Security Alliance for Mutual Progress (CAMP) on 10-11 July 2024 in South Korea.
- The 3rd ASEAN-Japan Cybersecurity Working Group Meeting on 29 July- 02 August 2024 in Japan.
- The Cyber Digital Services, Defence and Security Asia – CYBERDSA workshop from 4-8 August 2024 in Malaysia.
- The 3rd ASEAN Working Group on Anti-Online Scam (WG-AS) Meeting and The ASEAN Combatting Online Scam Workshop from 26-27 August 2024.
- The Seminar on Network Security and Information confrontation for Developing Countries from 11th - 24th September 2023, in China.
- The 2024 ASEAN ICT Forum from 26-27 September 2024 in Indonesia.
- The 9th Singapore International Cyber Week (SICW) and the 9th ASEAN Ministerial Conference on Cybersecurity (AMCC) from 14-18 October 2024 in Singapore.
- The Global Anti-Scam Alliance (GASA)'s Asia Summit 21-22 October 2024 in Singapore.
- The 17th ASEAN-Japan Cybersecurity Policy Meeting on 17-19 October 2024 in Singapore.
- The JP-US-EU Industrial Control Systems Cybersecurity Week for the Indo-Pacific Region from 12-15 November 2024 in Japan.
- The Workshop for Regional CERT Cooperation in ASEAN from 12-13 December 2024 in Japan.
- The China-ASEAN Network Security Emergency Response Capacity Building Seminar from 18-19 December 2024 in China.

6. Future Plans

- Continue to provide training and seminar on Cybersecurity to provincial both public and private sector throughout the country.
- Continue to collaboration to exchange the lessons and experiences on the development of legislation, laws and information on developing an online social media management system among National CERT, international organization and related sectors in the field of cybersecurity.
- Complete the drafting the Cybersecurity Law in 2025.

- Expanding the awareness raising on Cyber Crime Law and data protection Law.
- Establish a Cyber Security Operations Center (SOC) and now is under the coordination and set up the room and system.
- Planning for Establishing Government Threats Monitoring (GTM).
- Planning to set up the Network Monitoring System.

7. Conclusion

The Department of Cyber Security/Lao Computer Emergency Response Team (LaoCERT) continues to develop its team by enhancing both the quality and quantity of its technical capabilities. The focus remains on incident handling, network security, cybersecurity legislation development, and strengthening cooperation with domestic and international cybersecurity organizations. These efforts aim to promote and organize cybersecurity initiatives, including workshops, seminars, and training programs. Additionally, LaoCERT is dedicated to improving staff technical skills while raising awareness about cybersecurity laws, regulations, and best practices for using social media and computer networks securely to prevent cyber-attacks.

mmCERT

Myanmar Computer Emergency Response Team

1. Highlights of 2024

1.1 Summary of major activities

To ensure effective incident response services, mmCERT plays an active role in key cybersecurity initiatives, including the annual APCERT Drill and ACID Drill. In line with the commitment to capacity building, mmCERT promotes and facilitates international, regional, and local training programs for government officials and students alike. As part of awareness-raising efforts, the "Cybersecurity Awareness Video Competition" was successfully organized for university students. In terms of corporate engagement and collaboration, mmCERT contributes to organizations such as ASEAN Cyber-CC, ANSAC, BIMSTEC, ARF and APCERT. Additionally, mmCERT maintains strong relationships with cybersecurity organizations worldwide, fostering a global network of cooperation.

1.2 Achievements & milestones

- Myanmar supports co-chairmanship in "The 4th ASEAN-Russia Dialogue on ICT Security-related Issues" held on October 25, 2024 in Sochi (Russia).
- Cyber Security Law was completed in 2024 and enacted on 1st January, 2025.

2. About CSIRT

2.1 Introduction

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

2.2 Establishment

Myanmar Computer Emergency Response Team (mmCERT) was established by the e-National Task Force on 23rd July, 2004, in accordance with the Initiative of ASEAN Integration (IAI) agreement. Initially, mmCERT operated as a government-funded organization under the Information Technology Department, Ministry of Communications, Posts, and Telegraph (MCPT).

On 15th December, 2010, mmCERT expanded its services with the establishment of the service coordination center (cc). In 2011, mmCERT/cc became an operational member of APCERT.

In 2015, the Information Technology and Cyber Security Department (ITCSD) was formed under the Ministry of Communication and Information Technology (MCIT) to accelerate E-Government Services and enhance cybersecurity for government agencies and the private sector. As a result, mmCERT/cc was restructured under the National Cyber Security Center (NCSC), ITCSD.

In 2016, the Ministry of Communication and Information Technology (MCIT) was renamed the Ministry of Transport and Communications (MOTC). MOTC now leads activities related to Information Technology and Cyber Security Department in Myanmar. mmCERT/cc currently operates as a subdivision under NCSC.

2.3 Resources

All of mmCERT members are recruited by Ministry of Transport and Communications (MOTC). The operation of mmCERT was directly managed by the director of National Cyber Security Center under Information Technology and Cyber Security Department (ITCSD). As human resources of mmCERT is inadequate to handle cyber issues at present and thus it has been planned to extend the organization structure and to recruit more professionals.

2.4 Constituency

mmCERT initially handled computer incidents for government agencies and MPT, the state-owned telecom operator. Since its establishment, mmCERT/cc has been responsible for disseminating security information and advisories, as well as providing technical assistance to government agencies, telecom operators, internet service providers (ISPs), universities, and individual users in Myanmar. There have plans to expand the constituency to include financial institutions, banks, online services/ shopping platforms, research and development centers, and vendors.

3. Activities & Operations

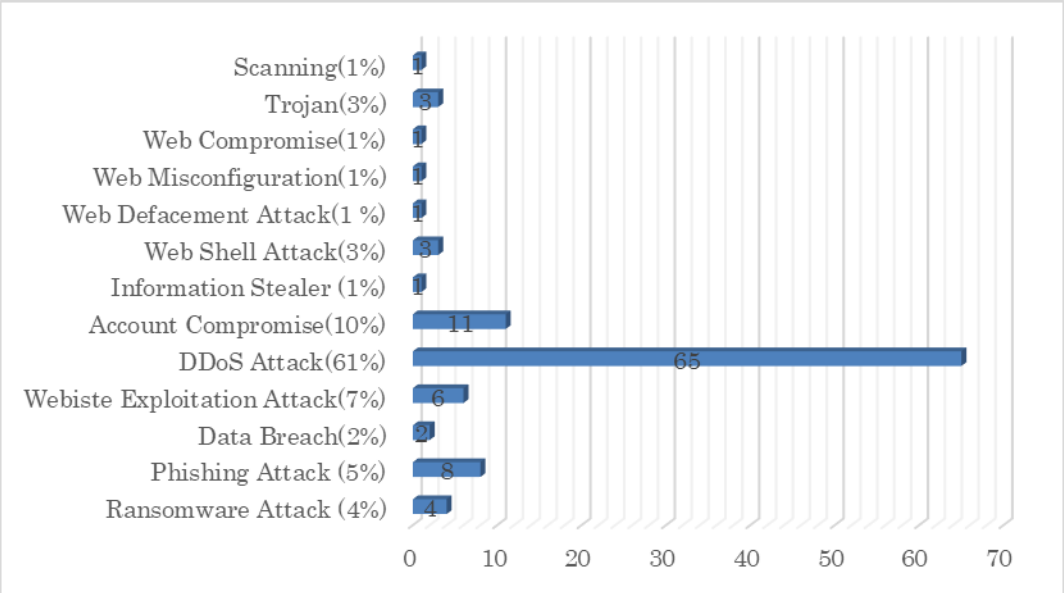
3.1 Scope and definitions

- Creates National IT image by collaborating with international CERT teams for cybersecurity and cybercrime.
- Disseminates security information and advisories.
- Provides technical assistance.
- Collaborates with law enforcement organizations for combating cybercrimes.

3.2 Incident handling reports

There has been a significant decrease in the number of incidents reported to mmCERT from individuals and private sectors. However, according to the incident analysis conducted by mmCERT, DDoS attack and Account Compromise incidents were prominent. mmCERT has closely coordinated with government organizations to respond to cyber incidents, mitigate their impact and implement preventive measures.

The following graph shows the incidents handled by mmCERT in 2024 :



3.3 Publications

"STOP Ransomware Guide" was released on its Facebook page and website from Version 1.1 to 1.4 according to timely changes in the encryption method by the developer.

https://www.mmcert.org.mm/mm/file-download/download/public/375

"PlugX Removal Guide (Version 1.2)" was also released to help victims of PlugX RAT understand the tactics of this RAT and the eradication method.
https://www.mmcert.org.mm/mm/file-download/download/public/374
"Guidebook for Suspicious Mails (Version 1.0)" was shared to provide knowledge about phishing mail attacks and preventive measures to a wide range of entities, from individuals to enterprises and government organizations.
https://www.mmcert.org.mm/mm/file-download/download/public/378
Current events and activities of mmCERT are found on the mmCERT website and NCSC website. Updated cyber trends, cyber incidents, and articles are also translated into the Myanmar language and appropriately published. CVEs for computer networks and systems can also be reviewed on the mmCERT website. Trending security and cyber threat news and articles can frequently be seen on the mmCERT Official Website, Facebook Page, and YouTube channel.

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

4. Events organized / hosted

4.1 Training

- Cyber Awareness and obtaining and maintaining of digital evidence" sessions were held at the detective training of Ministry of Home Affairs in April and August, 2024. Each training sessions included 120 detectives respectively.
- Provided awareness talk on "Email and Digital Account Security" for government organizations on 22nd March, 2024.
- Presented Cyber security awareness sessions in Ministry of Information in May and November, 2024.
- Shared insights on Cyber Security Awareness at Internal Revenue Department in August and December, 2024.

4.2 Conferences and seminars

- Held Email Security Awareness Conference for government CIOs and ACIOs on 20th June, 2024.
- To raise cyber security awareness through youth, and governmental personals, ITCSD provided Cyber Security Awareness Raising at the "Gathering of Outstanding Students for the 2023-2024 Academic Year" held at MICC-2, Nay Pyi Taw on 26th April, 2024. In this event NCSC also conducted Cyber Security Quiz.
  https://ncsc.gov.mm/2024/04

- In terms of Private-Public Partnership, MoTC held "Cyber Security in Digital Age" Workshop which was jointly organized with Telecom International Myanmar Co., Ltd on 12th December, 2024 in Nay Pyi Taw.
  https://www.mmcert.org.mm/index.php/mm/activity/2025-01-28t1627040630

4.3 Other Activities

- To encourage the young cyber security professionals and students for developing their skill in cyber security, telecommunication operators MPT, Atom, MyTel and other IT companies supported in organizing Myanmar Cyber Security Challenge (MCSC-2024) which was held by Ministry of Transport and Communications on 24th August, 2024.
  https://ncsc.gov.mm/2024/08/

- NCSC conducted Cyber Security Awareness Video Competition (University Level) in August, 2024 for selecting and submitting the representative video of Myanmar to join the ASEAN-JAPAN Cyber Security Awareness Video Competition-2024. There were 34 videos from the university students under 30 years old.

5. International Collaboration

5.1 International partnerships and agreements

- Myanmar contributes in ASEAN Working Group on Anti-online scam (WG-AS) and supports for the Report of the Online Scams Activities in ASEAN (2023–2024).
- NCSC also welcome the endorsement of the ASEAN Checklist for the Implementation of the Norms of Responsible State Behavior in Cyberspace at the 5th Cyber-CC.

5.2 Capacity building

5.2.1 Training

- A member of mmCERT virtually attended the "Regional Digital Financial Services Security Clinic for Asia Pacific Region" organized by ITU in Korea on 24th to 25th April, 2024.
- Members of mmCERT virtually attended the "Jupyter Notebooks in Incident Response" Course jointly provided by the AJCCBC and the Government of Switzerland, through FIRST, during 3rd to 4th June, 2024.
- A member of mmCERT attended "ARF Workshop on the Protection of ICT-Enabled Critical Infrastructures" provided by ASCCE, Singapore during 6th to 7th June 2024.
- Members of mmCERT virtually attended the Security Incident Management Maturity Model (SIM3) Course jointly provided by the AJCCBC and the Government of Switzerland, through FIRST, during 26th to 27th June, 2024.
- A member of NCSC attended "International Law of Cyber Operations" provided by ASCCE, Singapore during 8th to 10th July 2024.
- Members of NCSC virtually attended the "International Online Training for Raising Global Cyber Resilience" during 10th to 11th September, 2024.
- A member of NCSC attended the "Executive Course on International Law of Cyber Operations" during 11th to 15th November, 2024 in Singapore.
- Members of mmCERT virtually attended the "APT Online Training Course on Internet of Things and Cyber Security in the Era of Big Data" during 27th November to 3rd December, 2024.

5.2.2 Drills & exercises

- mmCERT participated in the APCERT Drill 2024 in August and the ACID Drill in October.
- mmCERT organized Myanmar students to participate in the ASEAN Students Contest on Information Security (ASCIS) 2024 in October.
- NCSC arranged the participants to join the 2nd ASEAN Cyber Shield Hacking Contest from 19th to 22nd November, 2024 in Vietnam.
  https://www.mmcert.org.mm/mm/activity/2024-11-26t1627190630

5.2.3 Seminars & presentations

- A member of mmCERT joined the "ASEAN-Australia Counter-Terrorism Workshop" during 30th to 31st January, 2024 in Indonesia.
- Members of mmCERT virtually attended Euro-Asia IT Forum "Digital Sovereignty as the Basis for Long-term International Cooperation on 20th to 21st February, 2024.
- Members of NCSC virtually attended the "2024 Beijing Cyber Security Conference" during 5th to 6th June, 2024 in Beijing.
- Members of NCSC virtually attended the "ASEAN Region Cyber Workshop; Protecting ASEAN Critical Infrastructure in the Age of AI" during 19th to 20th June, 2024.
- Members of NCSC attended the "ASEAN Norms Implementation Checklist Workshop" during 31st July to 1st August

2024 in Malaysia.

- A member of mmCERT joined the "Global Anti-Scam Alliance's Asia Summit" on 21st to 22nd October, 2024 in Singapore.
- A member of NCSC joined "ASEAN Cyber Shield Conference" on 22nd November, 2024 in Vietnam.
- Members of mmCERT participated in China-ASEAN Network Security Emergency Response Capacity Building Seminar on 18th to 19th December 2024 in Guangzhou, China.

5.3 Other international activities

- Attended ASEAN-Australia Counter-Terrorism Workshop in Indonesia on 30th to 31st January, 2024.
- Joined the 1st ASEAN-Japan Cybersecurity Working Group Meeting of 2024 in Thailand on 6th to 7th February, 2024.
- mmCERT joined the 1st Working Group on Anti-Online Scam (WG-AS) on 19th March, 2024 in Cambodia.

- Participated the 2nd ASEAN-Japan Cybersecurity Working Group Meeting of 2024 on 21st to 22nd May, 2024 in Cambodia.

- Attended in "The 15th Meeting of ASEAN Network Security Action Council (ANSAC)" held on 24th June, 2024 in Brunei.

- Myanmar support co-chairmanship in "The 4th ASEAN-Russia Dialogue on ICT Security-related Issues" held on 25th October, 2024 in Sochi (Russia).
- https://asean.mid.ru/en/news/4th_asean_russia_dialogue_on_ict_security_related_issues_/

- As an activity of ASEAN-JAPAN cybersecurity cooperation, NCSC contributed in ASEAN-Japan Cybersecurity Awareness Video Competition - 2024 and Myanmar contestant won the Second Prize in this competition.

6. Future Plans

6.1 Future projects

- It is planned to conduct Cyber Security Awareness Raising Workshops and Trainings for CIOs and ACIOs from government agencies.
- The Cyber Security Awareness Plan will be developed by mmCERT and distributed among government organizations for ensure secure endpoints.
- The Cyber Security Awareness Video Competition-2025 has been arranged to enhance cyber security knowledge among youth.

6.2 Future Operation

- As a developing team, mmCERT/cc is striving hard to become a developed and matured team by effectively handling incidents, conducting cyber security research, efficiently providing technical advisories, and organizing training, seminars, and workshops for its constituencies.
- Coordination with government ministries and agencies to establish CSIRT and ISAC in the future is planned.
- Incident Handling Courses will be extended to enhance capacity building across government agencies.
- Public Awareness Activities such as workshops, seminars and discussion will be organized to enhance ICT knowledge and raise awareness about the importance of cyber security.
- Web-Penetration Testing is carrying out for government agencies based on their requirements.
- Security Operation Center of NCSC monitors, detects, protects and responds to cyber incidents by utilizing the Security Operation Center Platform. It serves as 24/7 protection for government agencies as per their demands.
- Furthermore, mmCERT/cc will continue to engage in international and regional cooperation for CERT Activities as much as possible.

7. Conclusion

Throughout 2024, mmCERT successfully expanded the engagement with students and young professionals in the cybersecurity field. mmCERT also organized events that fostered Private-Public Partnerships, contributing to a stronger collaborative environment. mmCERT continued to strengthen its relationships with international and regional cybersecurity organizations and CERT teams. Our commitment to enhancing the nation’s cybersecurity capabilities remains steadfast, as we continue to promote public awareness about the importance of safeguarding personal information and effectively managing security risks.

MNCERT/CC

Mongolia Cyber Emergency Response Team/Coordination Center

1. Highlights of 2024

1.1 Summary of major activities

MNCERT/CC successfully fulfilled its commitment to strengthening cybersecurity by providing its constituencies with timely threat intelligence information, incident response support, and training and awareness programs. In addition, we actively engage with the public through the MNSEC information security annual conference, and the HaruulZangi ethical hacking competition, designed for both cybersecurity professionals and high school students.

This year, we continued our cooperation with APCERT, TEAM CYMRU, FIRST, APWG, MICROSOFT, NCFTA and ARCTIC, ensuring seamless collaboration and intelligence sharing. We also provided critical security insights on potential threats, suspected compromises, vulnerable services, and exposed services observed within our constituency's infrastructure.

To enhance public engagement, we expanded our annual cybersecurity conference by incorporating hands-on workshop sessions, increasing its reach and impact. As a result, we witnessed a growing number of participants, particularly from rural areas.

Beyond our core initiatives, we successfully organized a bug bounty program for professionals in the banking and finance sector, which also included a coordinated effort to identify and address security vulnerabilities within banking systems, further strengthening the sector's cybersecurity posture.

1.2 Achievements and milestones

One of the most significant milestones this year was our collaboration with the Public CERT which was established under the Ministry of Digital Development, Innovation and Communications of Mongolia as a consultant. Through this partnership, we have actively contributed to disseminating cybersecurity threat intelligence across all public and private sector organizations and the general public in Mongolia. Our efforts also included conducting cyber threat and vulnerability assessments, analyzing malicious code, studying the overall cybersecurity landscape of Mongolia and reporting the Public CERT.

This year, we successfully hosted MNSEC-2024 for the 12th consecutive year. The three-day event featured targeted

workshops, a main event open to the public, and exclusive closed-door networking sessions for select participants. With growing interest in the event, the number of attendees continues to increase each year.

Additionally, we successfully organized the Haruul Zangi CTF for the 13th year. This year's competition stood out as it was conducted on an international scale, allowing participants from any country to join. Furthermore, the Haruul Zangi U18 competition for high school students continues to spark greater interest in cybersecurity among young participants, encouraging them to pursue careers in the field. We believe this initiative is making a significant contribution to developing future cybersecurity professionals and strengthening the industry as a whole.

2. About MNCERT/CC

2.1 Introduction

The Mongolian Cyber Emergency Response Team / Coordination Center (MNCERT/CC) is a non-governmental organization established in 2014. MNCERT/CC is responsible for cyber incident response and monitoring, public awareness and education on cybersecurity, and developing methodologies to prevent cyber threats. The organization provides cybersecurity intelligence, training, and support to its constituencies while serving as a coordinator for national cybersecurity efforts. Through these initiatives, MNCERT/CC plays a pivotal role in strengthening Mongolia's cybersecurity resilience.

2.2 Establishment

The establishment of MNCERT/CC was driven by the Mongolian National Security Concept and the National Cybersecurity Program. In 2010, the State Great Khural (Parliament of Mongolia) approved Resolution No. 48, which laid the groundwork for the country's cybersecurity development. The resolution outlined key objectives, including:

- Objective 2.2: Establish a cyber incident response system, develop a national CERT, and expand cooperation with international organizations such as APCERT, FIRST, and CERT/CC.
- Objective 4.1: Strengthen the capacity of the organization responsible for securing the state's data and information infrastructure.

These foundational objectives provided the strategic direction for the establishment and operation of MNCERT/CC, ensuring that Mongolia aligns with international best practices in cybersecurity incident response, information sharing, and threat mitigation.

Through its continued efforts, MNCERT/CC remains committed to enhancing Mongolia's cybersecurity resilience, fostering international collaboration, and advancing national cyber defense strategies.

2.3 Resources

In accordance with the Non-Governmental Organizations Code of Mongolia, the founders of MNCERT/CC established a Steering Committee comprising nine members and a Advisory Team with three members. These teams consist of highly qualified professionals and researchers specializing in cybersecurity and information technology, along with a legal advisor.

The Executive Team, operating under the Steering Committee, is responsible for the center's day-to-day operations. This team includes a Chief Executive Officer (CEO), an Operational Manager, a Project Manager, an Incident Handlers, and a Cybersecurity Analysts. Together, they ensure the effective execution of MNCERT/CC's mission, focusing on cyber incident response, cybersecurity research, policy guidance, and legal compliance.

2.4 Constituency

MNCERT/CC serves a diverse range of constituencies, including:

- Internet Service Providers (ISPs)
- Banking and Financial Institutions
- Mobile Network Operators
- Mining companies
- Universities and Academic Institutions
- Other CERT Organizations
- The General Public

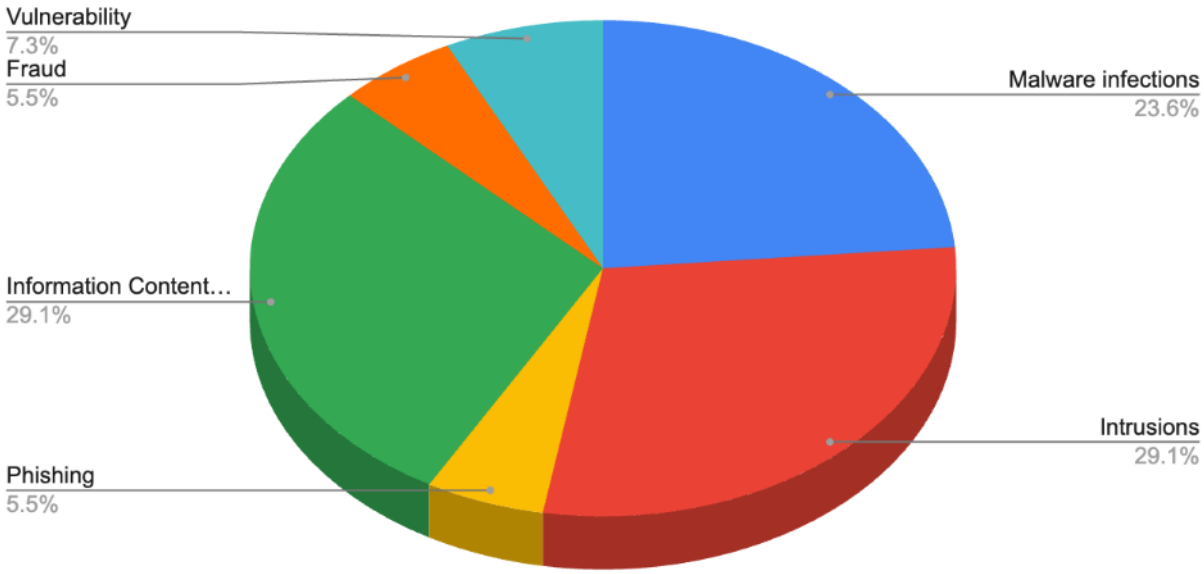
3. Activities & Operations

3.1 Scope and definitions

MNCERT/CC serves a diverse constituency, encompassing business enterprises, private sector organizations, financial institutions, universities, non-governmental organizations, and the general public. It delivers a wide range of cybersecurity services, including expert discussions, specialized training, security information and threat intelligence feeds, cybersecurity recommendations, consulting, and comprehensive research and analysis reports. Additionally, MNCERT/CC facilitates collaboration with both local and international CSIRTs to enhance the cybersecurity posture of its member organizations.

3.2 Incident handling reports

In 2024, we responded to a total of 55 cybersecurity incidents, providing assistance and advisory services. When categorized by type, the majority of incidents were related to intrusions and information content security. Additionally, the distribution of other incident categories is as follows: malware infections accounted for 23.6%, vulnerabilities for 7.3%, phishing for 5.5%, and fraud for 5.5%. The following pie chart visualizes the distribution of cybersecurity incidents in 2024.



Distribution of cybersecurity incidents handled

3.3 Abuse statistics

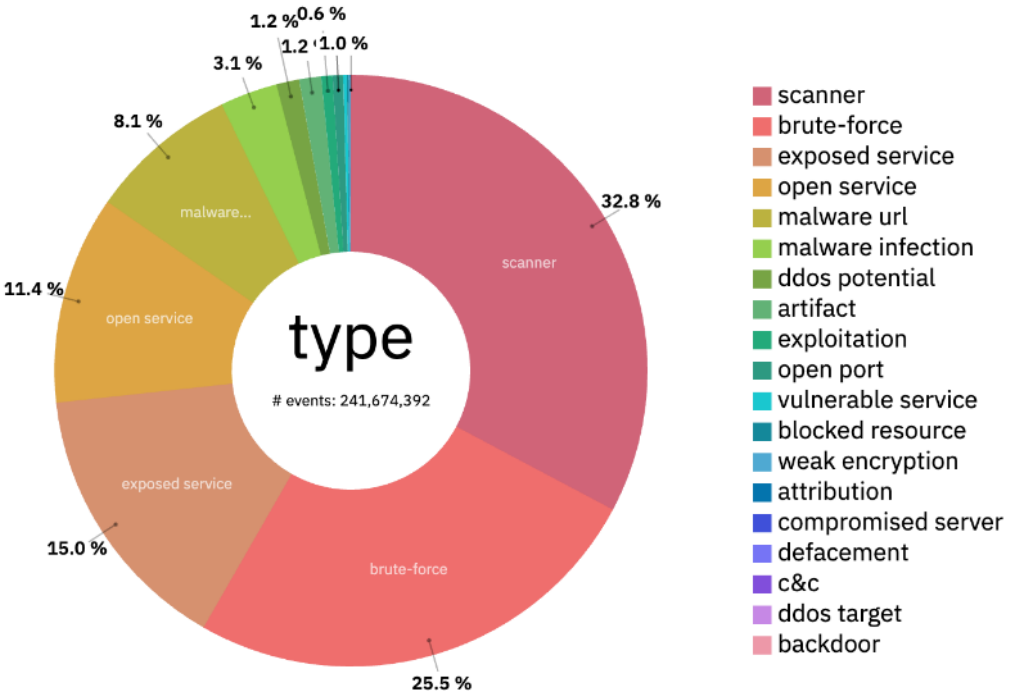
In 2024, a total of 241,674,392 cybersecurity suspicious events to Mongolian cyber environment were recorded, classified into various types of threats and vulnerabilities. The distribution of these events highlights key attack vectors, emphasizing the need for robust cybersecurity measures.

Among the recorded events, the most prevalent type was scanner attacks, accounting for 32.8% of the total incidents. These scanning activities indicate extensive reconnaissance attempts by threat actors to identify exploitable systems.

Brute-force attacks constituted 25.5% of the total, demonstrating a persistent effort by attackers to gain unauthorized access through credential-stuffing and password-guessing techniques. Following this, exposed services were responsible for 15.0% of incidents, further underscoring the risks associated with misconfigured or publicly accessible systems.

Additionally, open services represented 11.4% of the total cases, highlighting potential entry points for unauthorized access. Malware-related incidents, including malware URLs and infections, contributed to 8.1%, posing risks of system compromise and data exfiltration.

The remaining 7.2% of incidents were distributed across various categories, including DDoS potential (3.1%), exploitation attempts (1.2%), open ports (1.2%), vulnerable services (1.0%), and other security threats such as weak encryption, compromised servers, and backdoor access. Following pie chart visualizes the distribution of cybersecurity events towards Mongolia in 2024.



Distribution of cybersecurity events towards Mongolia in 2024

3.4 Publications

A total of nine advisories and warnings were developed and published on mncert.org website and social media platforms to inform organizations and the public about critical and potentially widespread cybersecurity incidents and vulnerabilities. These advisories aimed to enhance awareness and preparedness by providing timely guidance on emerging threats. The detailed information is presented in the following table.

Publications list

No.	Title	Date	Link
1	Mandatory Security Updates for GitLab Enterprise Edition (EE) and Community Edition (CE)	2024-01-29	https://mncert.org/#/mn/news/43
2	Critical Vulnerability in Jenkins Automation Server	2024-02-21	https://mncert.org/#/mn/news/44
3	LockBit Ransomware Group Disrupted	2024-02-22	https://mncert.org/#/mn/news/45
4	Critical Vulnerability in Microsoft Exchange Server	2024-02-23	https://mncert.org/#/mn/news/46
5	XZ Utils Backdoor	2024-03-28	https://mncert.org/#/mn/news/47
6	Critical Vulnerability in OpenSSH Server (regreSSHion)	2024-07-03	https://mncert.org/#/mn/news/49
7	Critical Vulnerability in VMware Systems (CVE-2024-22252)	2024-08-15	https://mncert.org/#/mn/news/50
8	Critical Vulnerability in Fortinet FortiOS and FortiProxy Systems	2024-09-18	https://mncert.org/#/mn/news/51
9	Critical Vulnerability in Zimbra Collaboration Systems	2024-10-16	https://mncert.org/#/mn/news/52

4. Events organized / hosted

4.1 Training

4.1.1 Members meeting and training

MNCERT/CC has been fostering a professional cybersecurity community, providing a platform where security experts from member organizations can discuss challenges, exchange knowledge and experiences, and engage in open discussions. The member meetings serve as an opportunity for professionals to share research findings, security measures implemented within their organizations, and best practices. Additionally, members can initiate discussions on topics of interest and learn from the experiences of other organizations.

In 2024, MNCERT/CC organized several member meetings and training covering a range of cybersecurity topics, as outlined in the following:

- Wild Exploit, Zero-day & N-day
- Threat Modeling, Incident Playbook
- Challenge Overcome Experience, Preparing Malware Analysis Environment
- Modern Malware Trends
- POS System Security
- Threat Modeling
- A Snapshot of Cyber Threats in Taiwan’s Financial Sector

4.2 Drills & Exercises

4.2.1 Cyber drill

MNCERT/CC Cyber Drill is an annual cybersecurity exercise conducted among MNCERT/CC member organizations. It aims to test the readiness of cybersecurity incident response plans and technical capabilities, assess the communication channels between MNCERT/CC and its member organizations, and evaluate the effectiveness of incident response coordination during cyberattacks.

This year, "MNCERT/CC Cyber Drill 2024" was successfully conducted on December 4, 2024, from 09:30 to 14:00. The exercise focused on achieving the following objectives:

- Verification of communication channels between MNCERT/CC and its member organizations.
- Evaluation of communication readiness in case of cybersecurity incidents.
- Assessment of response efficiency between MNCERT/CC and its member organizations.
- Technical preparedness assessment of member organizations for responding to cybersecurity incidents.
- Testing the implementation of incident response plans within member organizations.

The "MNCERT/CC Drill 2024" was designed in accordance with internationally recognized cybersecurity exercise methodologies, particularly aligning with best practices from cybersecurity drills in the Asia-Pacific region.

A total of 12 member organizations registered for participation, with 10 organizations actively taking part. The exercise simulated a real-world cyber incident involving an Advanced Persistent Threat (APT) group attack, providing participants with a hands-on scenario to improve their incident response strategies.

4.2.2 "Red Team 2024" bug bounty program

In collaboration with the Mongolian Banking Association, MNCERT/CC organized the "Red Team 2024 Bug Bounty Program" from March 28 to April 6, 2024, aiming to enhance banking sector security expertise and vulnerability assessment practices. This initiative provided a platform for cybersecurity professionals to exchange knowledge and experience, engage in discussions, and participate in a Capture the Flag (CTF) competition, which was structured around practical cybersecurity challenges.

As part of the program, a closed Bug Bounty Program was conducted to identify vulnerabilities in the systems of three participating banks. A total of 19 cybersecurity professionals participated, successfully identifying 13 vulnerabilities across the banking systems. The classification of the discovered vulnerabilities was as follows:

- 46% were classified as critical
- 15% were high severity
- The remaining were categorized as medium severity

The Bug Bounty Program played a crucial role in identifying real threats within banking systems, helping to prevent potential high-risk incidents in the future. By operating in a controlled and collaborative environment, the Mongolian Banking Association and its members successfully utilized this initiative to enhance security posture, mitigate risks, and foster a culture of ethical collaboration among banking sector cybersecurity professionals. The event was highly impactful, offering valuable learning experiences while significantly strengthening the cybersecurity resilience of the

participating financial institutions.

4.2.3 "HaruulZangi 2024" Cyber Security Competition

"Haruulzangi" Cybersecurity Competition has been held annually since 2013, providing an opportunity for all citizens of Mongolia to participate. The competition attracts numerous young professionals from the IT and Security sector, allowing them to test and showcase their cybersecurity skills.

The 2024 Haruulzangi Competition was structured into three stages:

i. First Stage (Online Round) – Conducted in an online format on September 13, 2024.
ii. Second Stage (Onsite Round) – Held on September 22, 2024, at Nest High School, where the top 32 teams from the first stage competed.
iii. Final Stage – The grand finale took place on September 26, 2024, at the Shangri-La Ulaanbaatar Hotel, where the champion of the ethical hacking competition was crowned.

For the first time in its history, "Haruulzangi 2024" was conducted at an international level, allowing foreign participants to compete. Additionally, the competition was officially recognized on ctftime.org, establishing itself as a globally ranked ethical hacking competition.

4.2.4 "HaruulZangi U18 2024" Cyber Security Competition

The "HaruulZangi U18" Cybersecurity Competition has been held annually since 2016 for high school students, providing a platform to enhance cybersecurity awareness and knowledge among young learners. The competition aims to:

- Raise awareness of information security and potential cyber threats among students.
- Improve understanding of online risks and cyberattacks in the digital space.
- Encourage students interested in information technology and cybersecurity to pursue further studies in the field.
- Challenge and inspire young talents, fostering early engagement in cybersecurity and IT disciplines.

In 2024, the 7th edition of the competition took place from May 18 to May 26, following a two-stage format. A total of 68 teams participated in the event, demonstrating their skills, problem-solving abilities, and knowledge of cybersecurity concepts.

4.3 Conferences and seminars

4.3.1 MNSEC 2024 Event

MNCERT/CC has been organizing the MNSEC Cybersecurity Conference annually since 2014. The MNSEC 2024 event took place over two days: on September 26th, 2024 – Main conference day, held in an open format for the public and on September 27th, 2024 – Exclusive networking day, conducted in a closed format for select participants.

The growing number of participants and their engagement demonstrates that MNSEC has established itself as a highly anticipated industry event for cybersecurity professionals. This year's event featured:

- 14 expert presentations
- Engaging networking activities
- Competitions and interactive challenges

- A total of 480 participants

Participants had the opportunity to attend specialized workshops, including web system penetration testing, hardware hacking and Cyber Threat Intelligence (CTI). Additionally, a hardware security village was set up, where attendees explored the security of automated machines such as massage chairs and vending machines, gaining insights into attack vectors and vulnerabilities.

The conference also featured insightful presentations covering a wide range of cybersecurity topics, including operating system security, artificial intelligence vulnerabilities and platform security risks. Participants had the opportunity to engage directly with speakers, ask questions on topics of interest, and gain valuable knowledge applicable to their roles and interests.

MNSEC 2024 successfully provided a dynamic and informative experience for cybersecurity professionals, IT specialists, and enthusiasts alike, offering valuable insights and networking opportunities within the field of information and cybersecurity.

5. International Collaboration

5.1 International partnerships and agreements

MNCERT/CC partners and collaborates with a broad spectrum of domestic and international organizations to strengthen cybersecurity capabilities and foster a unified approach to mitigating cyber threats.

Internationally, MNCERT/CC is an active member of FIRST (Forum of Incident Response and Security Teams) and APCERT (Asia Pacific Computer Emergency Response Team). Additionally, MNCERT/CC maintains contractual relationships with global cybersecurity leaders such as Team Cymru, NCFTA (National Cyber-Forensics and Training Alliance), APWG (Anti-Phishing Working Group), Arctic Security, Microsoft, and others. These collaborations provide access to near real-time threat intelligence, vulnerability feeds, and international cybersecurity expertise. By contextualizing this data to the local environment, MNCERT/CC ensures that not only its constituents but also any entities in Mongolia are well-informed and prepared to address evolving cybersecurity challenges.

5.2 Capacity building

5.2.1 Training

MNCERT/CC team attended the following trainings in 2024:

- 2024 APISC Security Training Course, conducted by KISA, Republic of Korea
- Critical Infrastructure Prioritization Part II, Capacity Building Workshop, by MITRE, in March 2024
- Effective Cyber Incident Response and Threat Information Sharing Techniques for Incident Responders, by FIRST and Africa CERT, in September 2024.
- Detecting Malicious Activities of APT Groups in the Organization’s Infrastructure Throu, by TWNCERT, in March

2024.

- Network Forensics, by APNIC, in April 2024.

5.2.2 Seminars & presentations

MNCERT/CC representatives delivered the following presentations in 2024:

- M. Otgonpurev, a Board Member, delivered a presentation on "Cyber Threat Intelligence" as part of the ITACTIC event, providing insights to participants on cyber threat analysis and intelligence gathering | January 13th, 2024
- V. Nyamsuren, Project Manager, conducted a theoretical and practical training session on "Digital Forensics", covering investigative techniques and methodologies | January 12th, 2024
- M. Otgonpurev participated as a speaker at the "FINSEC" Forum, presenting key insights on cybersecurity in the financial sector | March 6th, 2024
- L. Delgerbayar, Senior Security Analyst, presented on "The Role and Importance of CERT: Combating Cyber Incidents Together", emphasizing the significance of CERT in cybersecurity incident response and collaboration as part of the "Cyber Independence Conference" | November 25th, 2024
- T. Bilegdemberel, Security Analyst, delivered a presentation on "Automating Security Personnel Roles in Public and Private Sector Organizations", discussing automation strategies to enhance cybersecurity workforce efficiency as part of the "Cyber Independence Conference" | November 25th, 2024

MNCERT/CC representatives attended the following conferences in 2024:

- APCERT AGM 2024 | November 2024 | Taipei
- FIRST AGM 2024 | June 2024 | Fukuoka, Japan.

6. Future Plans

6.1 Future Operations

MNCERT/CC aims to expand its impact in Mongolia's cybersecurity landscape by continuously contributing to the community and enhancing the overall cybersecurity posture in the country. Our future goals include:

Expanding Membership and Collaboration

We plan to increase our membership base by engaging more public and private sector organizations, fostering greater collaboration across industries, and building stronger partnerships with international cybersecurity organizations.

Enhancing Cybersecurity Education and Awareness

We aim to develop new training programs, and awareness campaigns to further improve the skills of cybersecurity professionals and raise public awareness of online safety.

Developing Advanced Threat Intelligence Capabilities

MNCERT/CC will invest in enhancing its threat intelligence capabilities, ensuring more effective detection, analysis, and response to cybersecurity incidents. We will continue to share near real-time threat information with stakeholders, helping them stay ahead of emerging threats and vulnerabilities.

Strengthening National Cyber Resilience

We will continue to work closely with government agencies and critical infrastructure operators to fortify Mongolia's national cybersecurity posture through tailored programs, drills, and strategic frameworks.

Expanding Consultancy Services

MNCERT/CC plans to broaden its consultancy services, offering specialized support to domestic entities, and leveraging our expertise to shape effective cybersecurity strategies.

Research and Studies

MNCERT/CC aims to undertake comprehensive research initiatives focused on emerging cybersecurity trends, threats, and best practices. By collaborating with academic institutions and industry experts, we will develop studies that provide valuable insights and data-driven recommendations to strengthen cybersecurity practices in Mongolia. This research will also help inform policy decisions and foster a deeper understanding of the evolving threat landscape.

These future initiatives are part of MNCERT/CC's ongoing commitment to building a more secure and resilient digital environment in Mongolia.

7. Conclusion

In 2024, MNCERT/CC successfully strengthened its role in cybersecurity incident response, awareness, and collaboration both nationally and internationally. Through strategic partnerships with organizations such as APCERT, FIRST, and the Mongolian Banking Association, we enhanced cybersecurity intelligence sharing, improved incident response capabilities, and expanded our training and public awareness initiatives.

Key achievements include the successful execution of cybersecurity drills, including Red Team 2024 and MNCERT/CC Cyber Drill, as well as internationally recognized competitions such as HaruulZangi 2024. Additionally, our participation in global cybersecurity forums and trainings further reinforced our expertise and commitment to securing Mongolia's digital infrastructure.

Looking ahead to 2025, MNCERT/CC aims to expand its cybersecurity initiatives, enhance local and international partnerships, and continue advancing Mongolia's cyber resilience through proactive incident response, research, and capacity-building efforts. With a growing cybersecurity community and increased engagement from the board, MNCERT/CC remains committed to fostering a safer and more resilient digital ecosystem.

National CSIRT of Mongolia

National Computer Security Incident Response Team of Mongolia

1. Highlights of 2024

To strengthen and stabilize the operations of the National CSIRT, the center relocated to a new facility on January 15, 2024. The new facility is equipped with a dedicated monitoring room, meeting and conference rooms, and workspaces. Additionally, a call center and an official website were launched to ensure continuous and stable operations.
Preparations have been made for automating internal processes and integrating various systems. The National CSIRT has started using a cyber threat intelligence sharing platform.

2. About CSIRT

2.1 Introduction

The National CSIRT is dedicated to enhancing national capabilities in responding to cyber threats, establishing a robust cybersecurity system through both domestic and international cooperation. The center is responsible for safeguarding government and critical information infrastructure, detecting and preventing potential cyberattacks, responding to incidents, and ensuring recovery efforts.

2.2 Establishment

In accordance with Mongolia's "Vision-2050" Long-term development policy (Objective 7.5), the National Cybersecurity Strategy (Clause 3.5.1), and the Cybersecurity Law (Article 21), the National CSIRT was established in December 2022 under the Information Security Department. By September 2023, the legal framework, structure, staffing, and operational regulations of the National CSIRT were officially approved by a government decree.

2.3 Resources

The center consists of the following units:

- Security Operations Center
- Incident Response Unit
- Cyber Threat Intelligence Unit
- International Cooperation Unit

2.4 Constituency

Critical information infrastructure and government organizations connected to the State Information Consolidated Network.

3. Activities & Operations

3.1 Scope and definitions

The National CSIRT collects and analyzes cyber incidents, monitors internet traffic for organizations connected to the state information consolidated network and detects and verifies cyber threats. Relevant authorities are notified of detected threats, and appropriate mitigation measures are implemented. Additionally, expert guidance and recommendations are provided.

3.2 Incident handling reports & Abuse statistics

As of 2024, the National CSIRT has actively engaged in detecting, preventing, responding to, and recovering from cyber incidents, while also providing technical guidance. The types of recorded cyber incidents are illustrated in Figure 1.

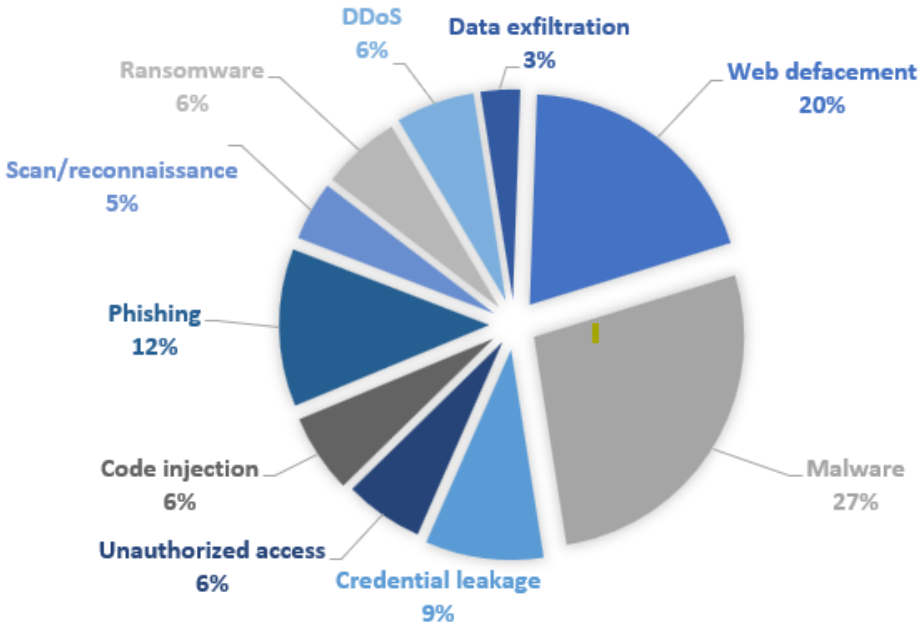


Figure. 1 Incident type

3.3 Publications

- The National CSIRT disseminates cybersecurity news, alerts, and information through its official website "ncsirt.gov.mn" to inform both the public and government agencies.
- A cybersecurity guide and recommendations for government officials have been distributed to relevant institutions.
- Actively participating in the activities of the Cybersecurity Young Researchers Club, initiated by the National Security Council's Strategic Research Institute, the National CSIRT has contributed research articles on cybersecurity and international cooperation.

4. International Collaboration

4.1 International partnerships and agreements

- On May 15, 2024, the National CSIRT became an official member of FIRST.
- On August 30, 2024, the National CSIRT joined the regional APCERT community.
- The National CSIRT also serves as the designated Technical Point of Contact for the Organization for Security and Co-operation in Europe's (OSCE) "Cyber/ICT security Confidence building measures" initiative.

4.2 Capacity building

4.2.1 Training

- APCERT "Experience Sharing on Social Media Incident Handling"
- APCERT "Incident Handling and Ticketing"
- JICA & TrendMicro "Incident Response"
- CySec Taimens "CISSP"
- OSCE "Cyber Incident Classification" workshop
- OSCE "International Cyber Diplomacy" workshop

4.2.2 Drills & exercises

- ITACTIC Cyber Drill
- Standoff
- CTFtime
- Kharuul Zangi

4.2.3 Seminars & presentations

- APCERT AGM & Conference
- MNSEC 2024
- 2024 APCERT & FIRST Regional Symposium for Asia Pacific
- KazHackStan 2024
- OSCE "Cyber/ICT security" CBM8 Point of Contacts Annual Meeting
- NatCSIRT 2024
- 36th Annual FIRST Conference
- OSCE "Cyber/ ICT security" Inter-Regional Conference
- OSCE, NCTC "Addressing the Prevailing Digital Information Disorder: Countering the Use of the Internet by Terrorists and Violent Extremists" Regional Conference

4.3 Other international activities

The National CSIRT contributed to the "Cyber Security Capacity Review" report, an assessment of Mongolia's cybersecurity landscape conducted by researchers from the University of Oxford.

5. Future Plans

5.1 Future projects

The National CSIRT is part of a task force for the "101 Project," an initiative in collaboration with the National Counter-Terrorism Council of Mongolia (NCTC), aimed at enhancing the protection and security of critical infrastructure. This project will focus on the adoption of international standards and the development of advanced security methodologies.

5.2 Future Operation

Aligned with the "Vision-2050" policy, the National CSIRT plans to integrate artificial intelligence into cybersecurity operations to strengthen the protection of critical information infrastructure. The National CSIRT will focus on automating internal processes, integrating systems, monitoring information flows, and enhancing incident response measures

6. Conclusion

In 2024, the National CSIRT has implemented a wide range of activities to enhance cybersecurity resilience and expand domestic and international cooperation. Through improved monitoring and oversight of information systems, the center has made significant progress in mitigating cyber threats and increasing the efficiency of incident response efforts.

NCSC NZ

National Cyber Security Centre New Zealand

1. Highlights of 2024

1.1 Summary of major activities

- In 2024, the integration of CERT NZ into the National Cyber Security Centre (NCSC) was completed. The CERT NZ functions will continue to be carried out by NCSC. The CERT NZ brand has started to be phased out, with NCSC and Own Your Online taking precedence.
- NCSC saw a decrease in reporting for most of 2024 with an average of 1,700 reports received through NCSC's general triage process.
- NCSC also received 343 incidents to the year 30 June 2024 that were triaged as being of potential national significance.

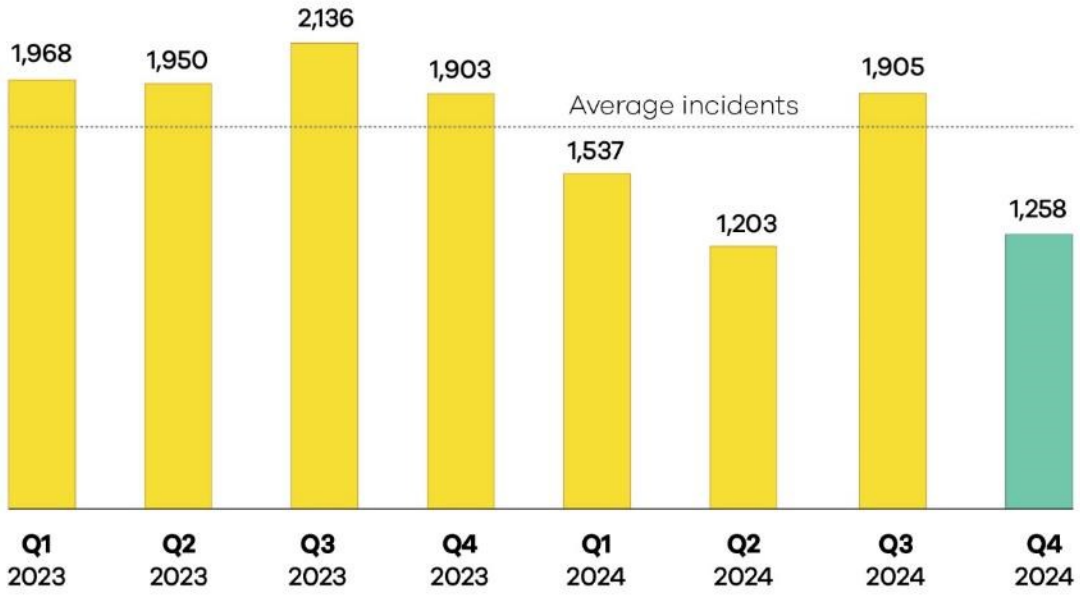


Figure 1. Incidents reported as part of NCSC's General triage process

2. About NCSC NZ

The National Cyber Security Centre (NCSC) was established in 2011, a part of the Government Communications Security Bureau (GCSB), is Aotearoa New Zealand's lead operational cyber security agency.
In July 2024, New Zealand's Computer Emergency Response Team (CERT NZ), formerly a part of the Ministry of Business, Innovation and Employment (MBIE), was integrated into the NCSC's organisational structure to form the New Zealand Government's lead operational cyber security agency.
https://www.ncsc.govt.nz/

3. Activities & Operations

3.1 Scope and definitions

The NCSC provides cyber security services to all New Zealanders - from individuals to small and medium businesses and organisations, large enterprises, government, and nationally significant organisations.
We work with government, critical infrastructure and other nationally significant organisations, as well as the digital supply chain, to offer technical protections, detection and disruption, including incident response for national-level harm.
We work to improve New Zealand's resilience to cyber security threats. The services we deliver include:

- providing cyber security information and educational resources;
- receiving reports of - and responding to - cyber security incidents;
- collating information about the cyber threat landscape to share with partners;
- disrupting cyber security attacks;
- hosting the Government Chief Information Security Officer (GCISO) function and providing system stewardship of public service information security;
- delivering cyber security uplift to Pacific Islands nations, and
- supporting government agencies and nationally significant organisations with tailored services and advice.

The NCSC makes use of its domestic and international networks to facilitate information exchanges within sectors, share information with trusted partners, and to support our cyber security work in New Zealand.

3.2 Incident handling reports

In quarter four 2024 a total of 1,358 incidents were reported to NCSC through its two distinct triage processes. Of these, 100 incidents were triaged for specialist support because of their potential national significance. This is a slight increase from 98 incidents of potential national significance in Q3.
1,258 reports were received through the CERT NZ online reporting tool and handled through the NCSC's general triage

process. This is a 34% decrease in the number of incidents from 1,905 in Q3. Financial loss in the same period went up by 24% from $5.5M to $6.6M.

We saw 17 incidents with losses over $100,000. This is the largest number of high-loss incidents we have seen in a quarter.

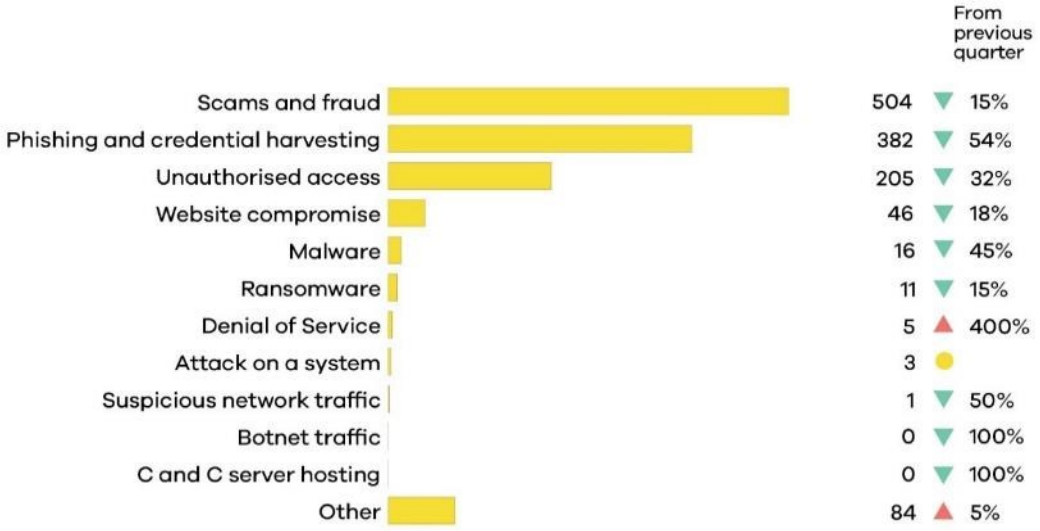


Figure 2. Incidents reported as part of NCSC's General triage process by incident category.

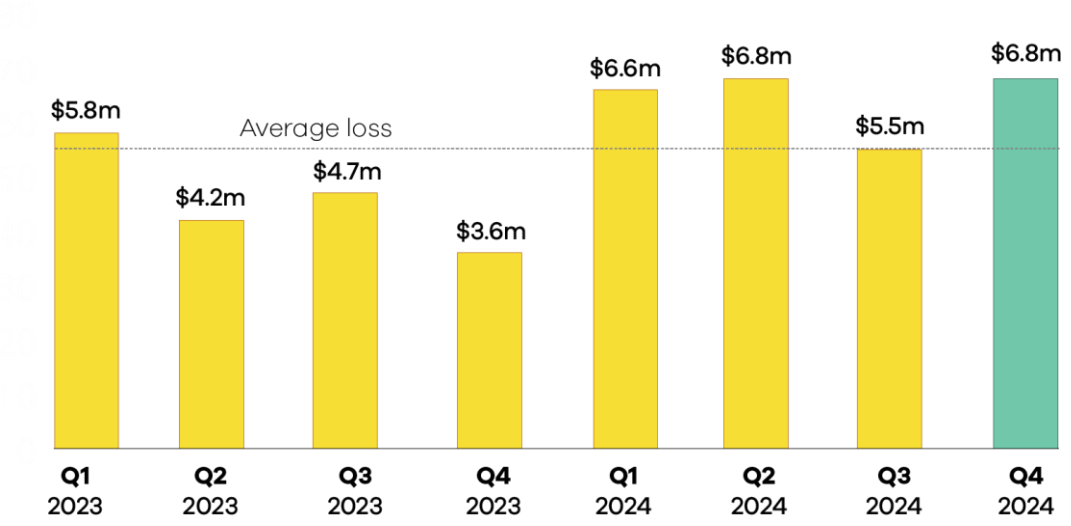


Figure 3. Financial loss reported as part of NCSC's General triage process by quarter.

3.3 Publications

NCSC continued to publish their quarterly reporting with the publication of the Cyber Security Insights Report. The report was moved to an online version from quarter three of 2024.

In 2024 NCSC published research tracking the cyber security behaviour of individuals and small to medium businesses in New Zealand. Highlights of the two research reports were:

- 95% of respondents know they need to take responsibility for themselves when it comes to cyber security.
- Almost half of New Zealanders had adopted a new cyber security behaviour in the last six months prior to the research.
- One in every three SMEs experienced at least one cyber-attack in the last six months.
- Of these, almost 60% took new actions to keep themselves more secure online. Compared to less than 30% of businesses that hadn't been targeted.

NCSC NZ joined several international partners in a number of joint publications. These pieces of cyber security advice and guidance ranged from engaging with artificial intelligence, to cyber security for operational technology and are an effective channel to get advice out to constituents.

4. Events organized / hosted

NCSC continued to run the annual cyber security awareness campaign, with Cyber Smart week running from 21 to 27 October 2024. This year's theme was 'Scamathon' calling for New Zealanders to stop 'donating' to The Scamathon and to protect themselves online. The Scamathon riffs off the idea of a Telethon, playing on all the different ways scammers appeal to us, to take advantage of us. The campaign features a host of scammers appealing to people to do all the wrong things because we're not as secure online as we could be. The campaign then encourages people to avoid giving to The Scamathon – by using long, strong and unique passwords and turning on two-factor authentication.

https://www.ownyouronline.govt.nz/our-campaigns/scamathon/

5. International Collaboration

5.1 International partnerships and agreements

Key International engagements:

- APCERT IoT Working group.
- APCERT annual conference
- PaCSON AGM
- APNIC 58
- FIRST Annual conference
- NatCSIRT annual meeting

5.2 Capacity building

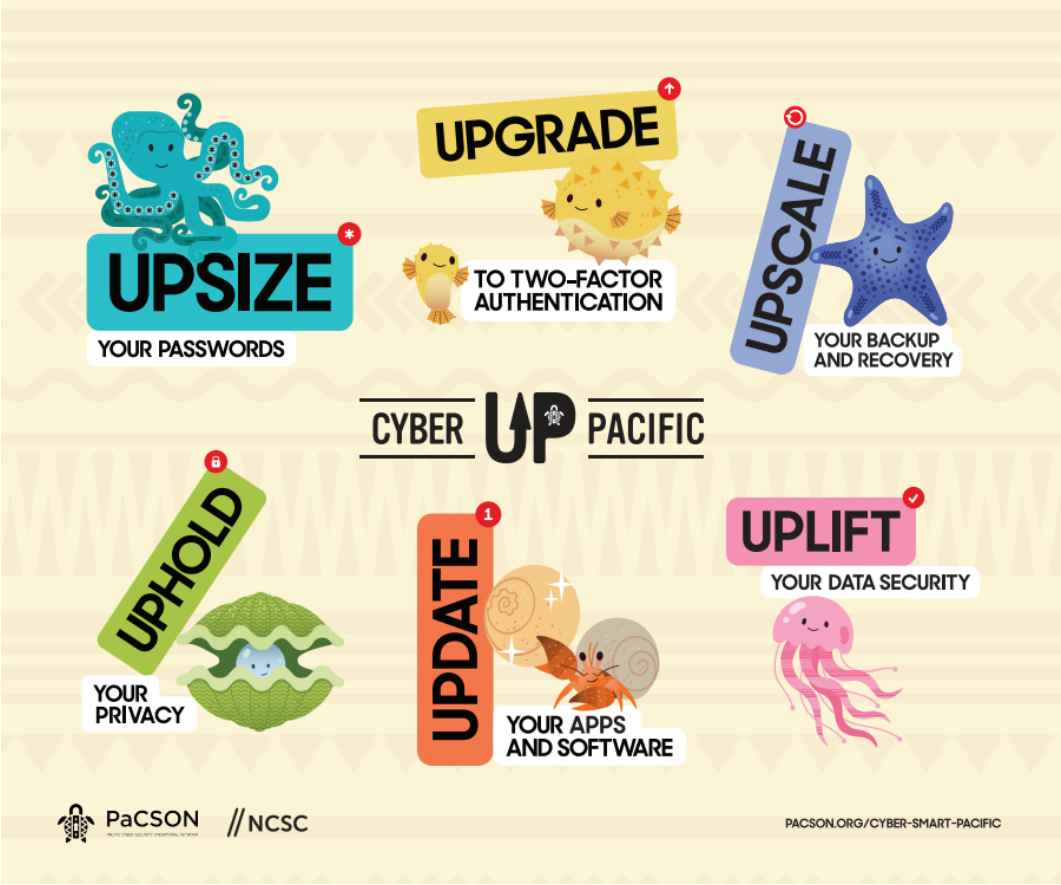
NCSC NZ has a dedicated Pacific Partnership team focused on capacity building. The team works closely with Pacific incident response counterparts and the wider regional cyber community. The Pacific programme delivers two primary lines of effort including business as usual (BAU) collaboration and standalone responsive programming.

BAU activities include:

- Information and good practice sharing and development;
- Community development and engagement;
- Formal and informal mentorship activities;
- 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 2024 has included:

- Chair of the Capacity Building Working Group.
- Support to the Awareness Raising Working Group – collaborating on developing and delivering the Cyber Smart Pacific (Cyber UP) annual regional awareness raising campaign
- in-country bilateral meetings and training with Solomon Islands, Fiji and Tuvalu
- partnering with SamCERT to for cyber security support for the Commonwealth Heads of Government Meeting.
- sharing CERT NZ reporting templates
- Continuing collaboration with CERT Tonga on a Cyber Security Workforce Development Program.



SingCERT

Singapore Computer Emergency Response Team

1. Highlights of 2024

The Singapore Cyber Emergency Response Team (SingCERT) is part of the Cyber Security Agency of Singapore (CSA). SingCERT serves as a trusted point of contact for cyber incident reporting for the members of the public, private businesses, and international CERTs around the world.

CSA launched four initiatives aimed at promoting cybersecurity awareness and fostering a more secure cyberspace in 2024:

i. Publication of Safe App Standards

Aims to strengthen the overall security posture of mobile apps deployed in Singapore and better safeguard app transactions and user data.

ii. Launch of Cybersecurity Labelling Scheme for Medical Devices

A voluntary scheme where medical devices are rated according to their levels of cybersecurity provisions.

iii. Cybersecurity Education and Learning Guidebook

Provides a comprehensive resource on cybersecurity education and talent programmes in Singapore.

iv. 8th Edition of Singapore Cyber Landscape

Highlights facts and figures on significant cyber threats and incidents in Singapore for 2023.

2. About SingCERT

2.1 Introduction

The Singapore Cyber Emergency Response Team (SingCERT) is Singapore's national CERT, serving as a trusted point of contact for cyber incident reporting to the members of the public, private businesses, and international CERTs around the world.

It was set up to facilitate the detection, resolution, and prevention of cyber security related incidents on the internet. Besides providing technical assistance and identifying trends in hacking activities, SingCERT also works closely with other security agencies and Internet Service Providers (ISPs) to resolve cybersecurity incidents.

SingCERT's Contact Information:

- Website: https://www.csa.gov.sg/resources/singcert
- Email: singcert@csa.gov.sg

2.2 Establishment

SingCERT was first set up in October 1997 by the then-Infocomm Development Authority of Singapore (IDA), in collaboration with the Centre for Internet Research, National University of Singapore (NUS). SingCERT transited to the Cyber Security Agency of Singapore (CSA) when it was established on 1 April 2015.

CSA is the national body overseeing cybersecurity strategy, operation, education and outreach, technology, and industry development for Singapore's critical information infrastructure. It is managed by the Ministry of Communications and Information and reports to the Prime Minister's Office.

In 2023, SingCERT rebranded from the 'Singapore Computer Emergency Response Team' to the 'Singapore Cyber Emergency Response Team'. The rationale was to modernise SingCERT's branding, as cyber has become a widely recognised and understood term in the context of security and technology, and in many cases, the term computer security has been phased out in favour of cybersecurity. It also better captured the modern interconnected digital landscape and is associated with a more comprehensive and strategic representation of the digital environment.

2.3 Resources

SingCERT publishes specific threat alerts and advisories on cyber threats and trends that affects its constituency on the SingCERT webpage (https://www.csa.gov.sg/resources/singcert). These are broadcasted through the SingCERT subscribers' mailing list, as well as via CSA's Facebook and Twitter platforms. SingCERT also maintains an incident reporting channel, supported by Cyber Aid (https://www.csa.gov.sg/resources/singcert/cyber-aid). Cyber Aid is a tool that helps users with their cybersecurity incidents, as users can get clarity on the cybersecurity issues that they are facing,

and advice on how to resolve them.

2.4 Constituency

SingCERT primarily serves the local constituency comprising members of the public and private businesses in Singapore.

3. Activities & Operations

3.1 Scope and definitions

SingCERT provides technical assistance, facilitates communications in response to cybersecurity related incidents, and collaborates with foreign CERT partners in handling cross border cyber threats.
SingCERT also monitors and evaluates global cyber threats and vulnerabilities. It publishes alerts and technical advisories with recommended preventive measures.

3.2 Incident handling reports

SingCERT receives incident reports via our incident reporting channels. Upon receipt of report, SingCERT will assess the incident and advise the victim and any other relevant entity on appropriate steps to take.
In 2024, SingCERT received reports of 7,493 incidents, an almost 50% increase from the 5,048 incidents reported to SingCERT in 2023. This resulted in an average of 29.85 incidents per each business day of operation. The table and graph below show the number of incidents that SingCERT handled over the course of the year.

	Jan – Mar	Apr – Jun	Jul – Sep	Oct – Dec	Total
Number of Incident Reports	1,413	1,594	1,597	2,889	7,493

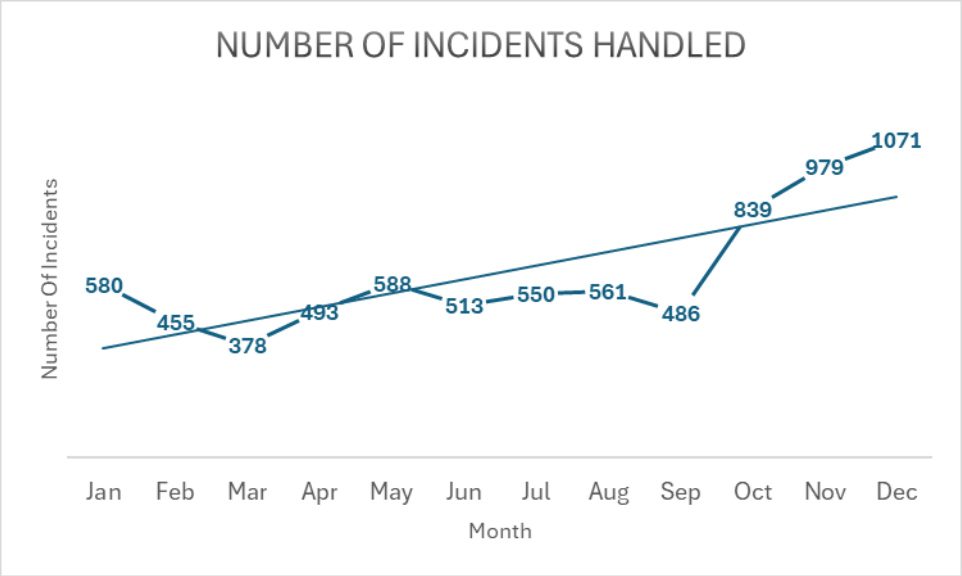


Figure 1: Number of Incidents Reported to SingCERT (2024)

3.3 Abuse statistics

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

In 2024, SingCERT handled a total of 7,493 cyber incidents, which was almost a 50% increase compared to 2023's figure. Phishing was, once again, the most prevalent cyber threat that was reported to SingCERT in Singapore, comprising over 70% of the incidents handled over the course of the year. This has been a trend that SingCERT has observed over the past few years. The phishing threats have also evolved to be more convincing in both the contents and the use of closely similar domain names to legitimate organisations operating in the country.

Cyber Incident Category	# Handled in 2023	# Handled in 2024
Phishing	3186	5443
Intrusion Attempt/Attack	703	891
Malware	734	475
Others	289	333
Vulnerability	136	351

Table 1: Breakup of Cyber Incidents handled (2023 vs 2024)

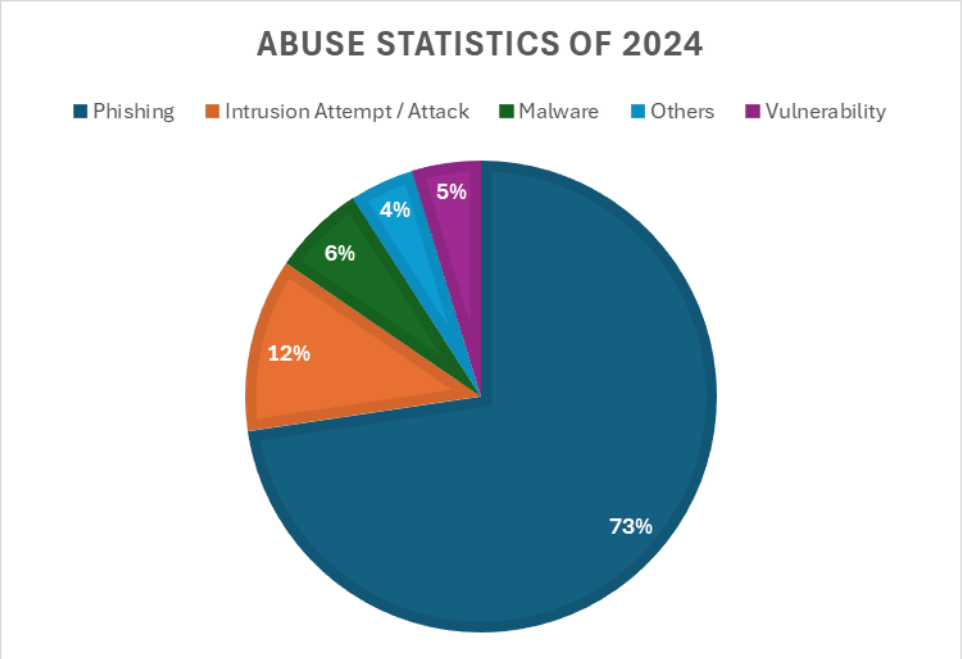


Figure 2: Abuse Statistics (2024)

3.4 Publications and Initiatives

3.4.1 Alerts and Advisories

SingCERT publishes alerts and advisories to raise the awareness and knowledge of our constituents to the current threats and trends, as well as to provide information on emerging threats and vulnerabilities and the recommended mitigation measures to adopt. SingCERT also publishes a weekly Security Bulletin on Wednesdays, which provides a summary of new vulnerabilities, their impacts and affected systems.

In 2024, SingCERT published a total of 168 alerts and advisories, in addition to 52 Security Bulletins, on SingCERT's website. This represented a 12% decrease from the 191 alerts and advisories published in 2023. The chart below shows the month-by-month comparison between 2023 and 2024.

	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Total
2023	13	16	18	19	16	16	17	11	14	22	12	17	191
2024	14	14	10	14	22	14	19	18	19	8	9	7	168

Table 2: Month-by-month comparison of Alerts and Advisories Published (2023 to 2024)

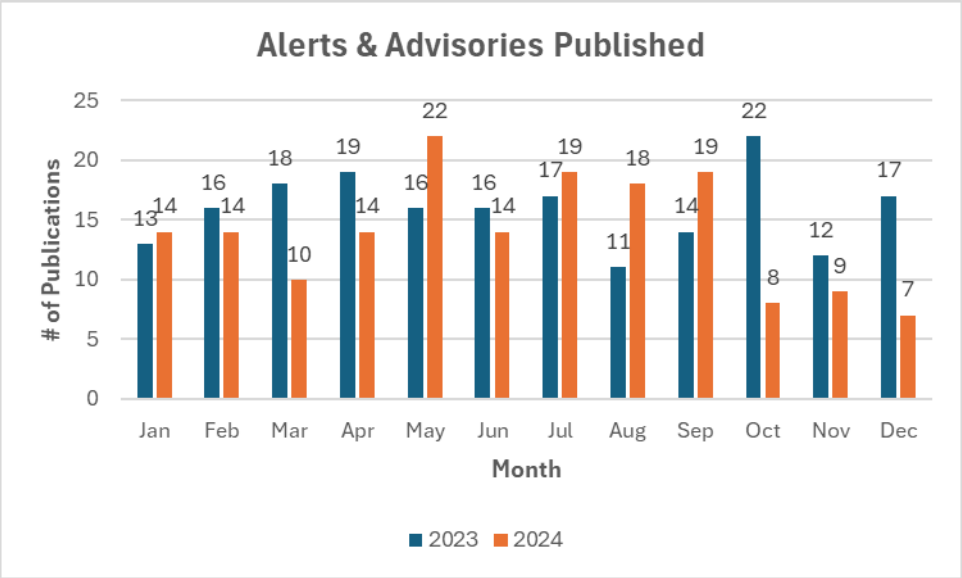


Figure 3: Comparing the Number of Alerts and Advisories Published (2023 to 2024)

Of the 168 alerts and advisories, 139 of them were published to address critical vulnerabilities discovered by software vendors, and the notification of patches released to fix the vulnerabilities. The list of alerts and advisories that were published by SingCERT in 2024 are tabulated below:

Date	Title
10 Jan	Jan 2024 Monthly Patch
11 Jan	Active Exploitation of Zero Day Vulnerabilities in Ivanti Connect Secure and Ivanti Policy Secure Gateways
14 Jan	Critical Vulnerabilities in GitLab Products
14 Jan	Critical Vulnerability in Juniper Networks Products
15 Jan	Active Exploitation of Critical Vulnerability in Microsoft SharePoint Server
17 Jan	Active Exploitation of Critical Vulnerability in VMware's Aria Automation
17 Jan	Active Exploitation of Zero-Day Vulnerability in Citrix's Netscaler ADC and Gateway Products
17 Jan	Active Exploitation of Zero-Day Vulnerability in Google Chrome
17 Jan	Critical Vulnerabilities in Siemens Products
19 Jan	Active Exploitation of Critical Vulnerability in Ivanti Products
23 Jan	Zero-Day Vulnerability in Apple Products
27 Jan	Critical Vulnerability in Cisco's Unified Communications Manager and Contact Center Solutions Products
30 Jan	Active Exploitation of Multiple Vulnerabilities in Jenkins Products
2 Feb	Active Exploitation of Vulnerability in Ivanti Products

2 Feb	Immediate Actions to Protect Against Multiple Zero-day Vulnerabilities in Ivanti Products
7 Feb	Importance of Cybersecurity Risk Management for Organisations
9 Feb	Active Exploitation of Critical Vulnerability in FortiOS
9 Feb	Authentication Bypass Vulnerability in Ivanti Products
15 Feb	Critical Vulnerability in Zoom Products for Windows
15 Feb	Feb 2024 Monthly Patch
16 Feb	Joint Advisory On Protecting Yourself From Compromised PayPal Accounts
17 Feb	Joint Advisory On Ransom Incidents Involving Network Attached Storage (NAS) Systems
19 Feb	Critical Vulnerabilities in SolarWinds ARM Product
22 Feb	Active Exploitation of Critical Vulnerability in WordPress Bricks Plug-in
22 Feb	Multiple Vulnerabilities in VMware Enhanced Authentication Plug-in
26 Feb	Active Exploitation of Multiple Vulnerabilities in ConnectWise ScreenConnect Software
29 Feb	High-Severity Vulnerability in Apple Products
6 Mar	Active Exploitation of Zero-Day Vulnerabilities in Apple Products
7 Mar	Critical Vulnerabilities in VMware Products
13 Mar	Mar 2024 Monthly Patch
14 Mar	Critical Vulnerabilities in Fortinet Products
15 Mar	Critical Vulnerability in QNAP Products
20 Mar	Critical Vulnerabilities in Unitronics Products
22 Mar	Active Exploitation of Critical Vulnerability in JetBrains TeamCity On-Premises
22 Mar	Advisory on Detecting and Responding to Deepfake Scams
27 Mar	Ongoing Malware Campaign Targeting WordPress Websites
28 Mar	Vulnerability Affecting User Datagram Protocol Implementations
1 Apr	Critical Vulnerability in XZ Utils
1 Apr	Multiple High Severity Vulnerabilities in Cisco IOS and IOS XE Software
4 Apr	Critical Vulnerability in WordPress LayerSlider Plugin
10 Apr	Multiple Vulnerabilities in HTTP/2 Protocol
11 Apr	Apr 2024 Monthly Patch
11 Apr	Critical Vulnerability in Rust Standard Library
12 Apr	Active Exploitation of Critical Vulnerability in Palo Alto Networks PAN-OS Software
12 Apr	Active Exploitation of Vulnerabilities in D-Link Products
12 Apr	How Organisations Can Secure Their Network Attached Storage (NAS) Systems

17 Apr	Critical Vulnerabilities in Ivanti Avalanche
19 Apr	Cryptographic Vulnerability in PuTTY
24 Apr	Protect Your Organisation Against Malware Threats Spread Through USB Devices
25 Apr	Active Exploitation of Vulnerabilities in Cisco Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD) Products
26 Apr	Critical Vulnerability in Progress Flowmon
3 May	High-Severity Vulnerability in R Programming Language
6 May	Active Exploitation of Critical Vulnerability in WordPress Automatic Plugin
8 May	Critical Vulnerability in Tinyproxy Instances
13 May	Active Exploitation of Zero-Day Vulnerability in Google Chrome
15 May	May 2024 Monthly Patch
17 May	Multiple Vulnerabilities in VMWare Workstation and Fusion
20 May	Defending Against Cyber Threats Leveraging Microsoft Graph API
24 May	Critical Vulnerabilities in Ivanti Endpoint Manager
24 May	Critical Vulnerability in Fluent Bit
24 May	Critical Vulnerability in Git
24 May	Critical Vulnerability in GitHub Enterprise Server
24 May	Critical Vulnerability in Veeam Backup Enterprise Manager
27 May	Active Exploitation of High-Severity Vulnerabilities in Google Chrome
27 May	Active Exploitation of Vulnerabilities in D-Link Routers
27 May	Critical Vulnerabilities in WordPress Plugins
28 May	Active Exploitation of Critical Vulnerability in NextGen Healthcare Mirth Connect
28 May	Active Exploitation of High-Severity Vulnerability in Apache Flink
28 May	Critical Vulnerabilities in Cacti
28 May	Critical Vulnerability in TP-Link Archer C5400X Gaming Router
28 May	High-Severity Vulnerability in Mozilla PDF.js
30 May	Critical Vulnerabilities in FortiSIEM
31 May	Active Exploitation of High-Severity Vulnerability in Check Point Virtual Private Network (VPN) Products
4 Jun	Using Personal VPN Services Safely
5 Jun	High-Severity Vulnerability in Atlassian Confluence Data Center and Server
5 Jun	Protecting Your IoT Devices
8 Jun	Critical Vulnerability in Hypertext Preprocessor (PHP) Software

8 Jun	Joint Technical Advisory on Akira
10 Jun	High-Severity Vulnerability in SolarWinds Serv-U File Servers
12 Jun	June 2024 Monthly Patch
13 Jun	Active Exploitation of High-Severity Zero-Day Vulnerability in Google Pixel
15 Jun	High-Severity Vulnerability in Windows Wi-Fi Driver
19 Jun	Critical Vulnerabilities in VMWare vCenter Server
20 Jun	Critical Vulnerabilities in ASUS' Router Products
24 Jun	Critical Vulnerability in Facebook PrestaShop Module
26 Jun	Ongoing Medusa Campaign Targeting Android Device Users
29 Jun	Active Exploitation of Critical Vulnerability in MOVEit Transfer
2 Jul	Active Exploitation of Vulnerability in Cisco NX-OS Software
2 Jul	Alert on Critical Vulnerability Affecting Juniper Devices
2 Jul	High-Severity Vulnerability Affecting OpenSSH
9 Jul	Critical Vulnerabilities in Gogs Open-Source Git Service
10 Jul	Critical Vulnerability in Apache HTTP Server
10 Jul	July 2024 Monthly Patch
11 Jul	High-Severity Vulnerability Affecting Microsoft Outlook
11 Jul	High-Severity Vulnerability in VMware Aria Automation Product
12 Jul	Critical Vulnerability in Palo Alto Networks Expedition Migration Tool
17 Jul	Critical Vulnerability in Exim Software
17 Jul	Critical Vulnerability in GitLab Products
19 Jul	Critical Vulnerabilities in SolarWinds Access Rights Manager (ARM) Product
19 Jul	Critical Vulnerability in Cisco Smart Software Manager (SSM) On-Prem
19 Jul	CrowdStrike System Outage
20 Jul	Ongoing Phishing Campaign Targeting CrowdStrike Users
24 Jul	Multiple Vulnerabilities Affecting LangChain Gen AI
30 Jul	Critical Vulnerability in Docker Engine
30 Jul	Vulnerability in VMware ESXi Hypervisor
31 Jul	Building Digital Resilience for Organisations
2 Aug	Multiple Vulnerabilities in Apple Products
5 Aug	How Individuals and Organisations Can Ensure Data Resilience
6 Aug	Ongoing "Panamorfi" Distributed Denial-of-Service (DDoS) Campaign Targeting Misconfigured Jupyter

	Notebooks
6 Aug	Ongoing SMS Stealer Campaign Targeting Android Device Users
7 Aug	Scammers Impersonating SingCERT Officers
8 Aug	Active Exploitation of Critical Progress WhatsUp Gold Vulnerability
12 Aug	Active Exploitation of Critical Apache OFBiz Vulnerabilities
12 Aug	Active Exploitation of Zero-Day Vulnerability in Android Devices
13 Aug	Critical Vulnerability in Sonos Smart Speakers
13 Aug	High-Severity Vulnerability in AMD Chips
14 Aug	August 2024 Monthly Patch
15 Aug	Critical Vulnerability in Ivanti Virtual Traffic Manager
15 Aug	Critical Vulnerability in SolarWinds Web Help Desk
16 Aug	Ongoing Malware Campaign Targeting Google Chrome and Microsoft Edge Browser Users
22 Aug	Critical Vulnerability in GitHub Enterprise Server
22 Aug	Best Practices for Event Logging and Threat Detection
23 Aug	Critical Vulnerability in SolarWinds Web Help Desk
28 Aug	Advisory on Extortion Emails
2 Sep	Critical Vulnerabilities in WhatsUp Gold
9 Sep	Joint Threat Advisory on GhostR
11 Sep	Active Exploitation of Critical Vulnerability in SonicWall SonicOS
11 Sep	September 2024 Monthly Patch
12 Sep	High Severity Vulnerability in Adobe Acrobat Reader
13 Sep	Critical Vulnerability in Ivanti's Endpoint Manager
13 Sep	Critical Vulnerability in Zyxel's NAS Devices
16 Sep	Critical Vulnerability in Gitlab Community and Enterprise Editions
16 Sep	Critical Vulnerability in SolarWinds Access Rights Manager
17 Sep	Multiple Vulnerabilities in D-Link Wireless Routers
18 Sep	Multiple Vulnerabilities in VMware vCenter Server Platform
20 Sep	Critical Vulnerabilities in Rockwell Automation Pavilion8
20 Sep	Critical Vulnerability in Apache Seata
20 Sep	Critical Vulnerability in Gitlab Community Edition and Enterprise Edition
20 Sep	Critical Vulnerability in NetIQ OpenText eDirectory
23 Sep	Active Exploitation of Critical Vulnerability in Apache HugeGraph-Server

23 Sep	Active Exploitation of Vulnerabilities in Ivanti Cloud Services Appliance
23 Sep	Critical Vulnerability in SPIP
27 Sep	Scammers Impersonating CSA and the SPF
3 Oct	High Severity Vulnerability in NVIDIA Container Toolkit
4 Oct	Critical Vulnerability in Zimbra Collaboration Suite (ZCS)
9 Oct	October 2024 Monthly Patch
10 Oct	Critical Zero-Day Vulnerability in Mozilla Firefox
15 Oct	Active Exploitation of Vulnerabilities in Ivanti's Cloud Services Appliance
17 Oct	Critical Vulnerability in Kubernetes Image Builder
24 Oct	Active Exploitation of a Critical Vulnerability in FortiManager
25 Oct	Active Exploitation of a Critical Vulnerability in Adobe Commerce Products
8 Nov	Critical Vulnerability in Cisco Unified Industrial Wireless Software
12 Nov	Multiple Vulnerabilities in Palo Alto Networks Expedition
13 Nov	November 2024 Monthly Patch
20 Nov	Active Exploitation of Critical Vulnerability in Palo Alto Networks PAN-OS Software
22 Nov	Defending Against Multi-Factor Authentication (MFA) Bypass Attacks
25 Nov	Critical Vulnerability in Wordpress Really Simple Security Plugin
27 Nov	Multiple Vulnerabilities in WordPress Plugin
28 Nov	How to Protect your Router from Hackers
29 Nov	Joint Advisory On The Safeguarding Of Cryptocurrency Assets Against Threat Actors
11 Dec	Critical Vulnerabilities in Ivanti Cloud Services Appliance
11 Dec	December 2024 Monthly Patch
12 Dec	Critical Vulnerability in OpenWrt Attended SysUpgrade
13 Dec	Critical Vulnerability in Apache Struts
30 Dec	Multiple Critical Vulnerabilities in Apache Products
30 Dec	Ongoing Campaign Targeting Chrome Browser Extensions
31 Dec	Vulnerabilities in Beyond Trust Products

3.4.2 Publication of Safe App Standards

CSA published the Safe App Standard 2.0 ("SAS 2.0") that aims to strengthen the overall security posture of mobile apps deployed in Singapore and better safeguard app transactions and user data.

SAS 2.0 continues to focus on high-risk apps with transactions that could result in significant financial losses. These high-risk transactions allow for modifications to financial functions, including the registration of third-party payee information

and increase of fund transfer limits. SAS 2.0 introduces four new key (on top of SAS 1.0), namely network communication, cryptography, code quality and exploit mitigations, as well as platform interactions. These enhancements are essential in providing app developers and owners with comprehensive guidelines to fortify the security of their mobile apps.

Overall, SAS 2.0 will cover security controls in eight key areas to improve mobile security. CSA strongly encourages developers of apps that are both developed and hosted in Singapore to adopt SAS 2.0 in their app development to fortify apps against common malware and phishing attacks. Consequently, this leads to a more secure environment for online financial transactions, instilling greater confidence in app transactions among members of the public.

More information is available at https://www.csa.gov.sg/news-events/press-releases/csa-publishes-safe-app-standard-version-20/.

3.4.3 Launch of Cybersecurity Labelling Scheme for Medical Devices

CSA, the Ministry of Health (MOH), Health Sciences Authority (HSA) and Synapxe jointly developed the Cybersecurity Labelling Scheme for Medical Devices, a voluntary scheme where medical devices are rated according to their levels of cybersecurity provisions.

As medical devices become increasingly connected to hospital and home networks, potentially elevating cyber risks, there is a need to take proactive measures to enhance the cybersecurity safeguards for medical devices. This scheme seeks to improve medical device security by incentivising manufacturers to adopt a security-by-design approach and enable consumers and healthcare providers to make more informed decisions about the security of such devices prior to purchase and usage.

More information about the playbooks is available via https://www.csa.gov.sg/news-events/press-releases/launch-of-cybersecurity-labelling-scheme-for-medical-devices/.

3.4.4 Cybersecurity Learning and Education Guidebook

CSA launched the "Cybersecurity Education and Learning Guidebook" which provides a comprehensive resource on cybersecurity education and talent programmes in Singapore.

In consultation with government agencies, industry, professional bodies, and academia, CSA has developed the guidebook to provide a comprehensive overview on industry trends, prospective pathways in cybersecurity and a structured learning roadmap for students, mid-career professionals, as well as employers, educators, and career counsellors.

More information about this guidebook is available via https://www.csa.gov.sg/news-events/press-releases/csa-launches-the-cybersecurity-edcation-and-learning-guidebook.

3.4.5 Singapore Cyber Landscape 2023

The 8th edition of the Singapore Cyber Landscape publication reviews Singapore's cybersecurity situation in 2023 against the backdrop of global trends and events, including (i) threats that leveraged vulnerabilities in supply chains and popular third-party services, (ii) the expanding operations of hacktivist groups, and (iii) the exploitation of generative artificial intelligence (AI) by malicious actors to enhance their attacks. It also highlights the nation's efforts in creating a safe and trustworthy cyberspace, such as initiatives to combat new and emerging cyber threats.

The publication provides an overview of the frequency and scope of cyber-attacks in Singapore, raising awareness of

cyber threats among stakeholders, including the public and businesses so that they can take appropriate actions to defend against such threats.

More information about the publication, including a downloadable copy, is available via https://www.csa.gov.sg/resources/publications/singapore-cyber-landscape-2023.

Figure 4: Singapore Cyber Landscape 2023

4. Events organised & hosted

4.1 Drills & Exercises

4.1.1 ASEAN CERT Incident Drill 2024

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 15 and 16 October 2024, SingCERT successfully conducted the 19th iteration of ACID. Nineteen CERTs from ASEAN Member States (AMS) and ASEAN Dialogue Partners participated in the drill. The theme "Navigating the Rise of AI-Enabled Cyber Attacks" was selected against the global backdrop of the multifaceted application of Artificial Intelligence (AI) technology for attack and defence, where the threat of AI-powered cyber-attacks is escalating. Participants were given a series of email injects that simulated similar tactics employed by threat actors, such as the use of AI to develop malware and AI-generated phishing messages.

This year's ACID also included a Tabletop Exercise (TTX) developed and moderated by SingCERT. In the TTX, scenario injects were provided for participants to discuss how they would respond to them, giving participating CERTs the opportunity to share information on their incident response processes, best practices to identify areas for further improvement and enhance their operations planning capabilities.

After the conclusion of the drill, participants feedbacked that the drill and TTX enhanced their capabilities and exposed their teams to new incident response scenarios and analysis techniques. They also highlighted the threats posed by emerging technologies such as AI, allowing the teams to practice responding to a diverse range of relevant scenarios.

More information about ACID can be found via https://www.csa.gov.sg/news-events/news-articles/19th-iteration-of-

asean-cert-incident-response-drill-tests-cert-s-preparedness-against-ai-enabled-cyber-attacks.

4.2 Conferences and seminars

4.2.1 Singapore International Cyber Week 2024

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 9th SICW was held from 14 to 17 October 2024, with the theme "Trust and Security in the Digital Era". SICW 2024 successfully concluded with more than 13,000 participants from over 90 countries and regions, as well as over 290 speakers and panelists who covered a myriad of topics ranging from election security, regulation of big technological companies and the possibility of establishing a meaningful interoperable framework for digital rules and standards to foster international operation even in the middle of geopolitical contestation, to the effects of newer digital technologies on matters of diplomacy, peace, and security.

More information about SICW can be found via https://www.csa.gov.sg/news-events/news-articles/sicw-2024-continues-to-drive-international-dialogue-and-cooperation-amid-climate-of-distrust.

4.2.2 Cybersecurity Awareness Alliance

One of the ways in which CSA drives cybersecurity awareness efforts, is through the Cybersecurity Awareness Alliance - a collaboration between public and private sector organisations as well as trade associations to raise awareness and adoption of cybersecurity measures. Alliance members actively give talks to schools, businesses, and the community at various platforms.

5. International Collaboration

5.1 Drills & Exercises

5.1.1 Asia Pacific Computer Response Team (APCERT) Cyber Security Drill 2024

The Asia Pacific Computer Response Team (APCERT) Cyber Security Drill tests the response capabilities of leading Computer Security Incident Response Team (CSIRT) within the regions.

The annual APCERT Cyber Security Drill was held on 29 August 2024 with the theme "APT Group Attack Response: Where is Wally?". The drill evaluates the response capabilities of member teams in responding to real incidents and issues that exist on the internet and allowed participating teams to review its procedures for responding to APT threat actors. As a member of the APCERT Drill Working Group, SingCERT was involved in the conducting of the drill as a part of the Exercise Controller Team.

5.2 Conferences, Seminars & Presentations

5.2.2 Forum of Incident Response and Security Teams (FIRST)

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

As a member of FIRST, SingCERT attended the FIRST Conference at Fukuoka, Japan from 9 June – 14 June 2024.

5.2.3 APCERT Annual General Meeting (AGM) and Conference 2024

The APCERT AGM and Conference is an annual event where CERTs from the Asia Pacific region gather to exchange information on the latest cybersecurity issues and incident response methodologies. SingCERT attended the APCERT Annual General Meeting (AGM) and Conference held in Taipei, Taiwan, from 5-6 November 2024. This was followed by the APCERT and FIRST Regional Symposium on 7-8 November 2024. Both the APCERT AGM and Conference events were held in-person for the first time since 2019, when it was hosted in Singapore.

6. Future Plans

SingCERT will continue with its work in facilitating detection, resolution, and prevention of cybersecurity related incidents. Planning and discussions are in progress for the following workstreams in the year 2025:

S/n	Description	Category
1	Singapore Cyber Landscape 2024	Publications
2	10th Singapore International Cyber Week (SICW)	Events Organising & Hosting
3	20th iteration of ASEAN CERT Incident Drill (ACID)	Events Organising & Hosting

Sri Lanka CERT|CC

Sri Lanka Computer Emergency Readiness Team | Coordination Centre

1. About Sri Lanka Cert

1.1 Introduction

The Sri Lanka Computer Emergency Readiness Team (Sri Lanka CERT) 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 acts as the central hub for the cyber security of the nation. It is the single trusted source of advice on the latest threats and vulnerabilities affecting computer systems and networks, and a source of expertise to assist the nation and member organizations, in responding to and recovering from Cyber-attacks. Sri Lanka CERT was established on the 1st of July 2006 as a subsidiary of the Information and Communication Technology Agency of Sri Lanka (ICTA). In 2018, Sri Lanka CERT was made independent of ICTA and was assigned to the Ministry of Digital Infrastructure and Information Technology. Currently, Sri Lanka CERT operates as a State-Owned Enterprise, and functions under the Ministry of Digital Economy. The constituency of Sri Lanka focuses on primarily the government, then citizens and business.

1.3 Constituency

Sri Lanka CERT's constituency encompasses the non-defence cyber community of Sri Lanka (private and public-sector organizations, and the general public). Sri Lanka CERT maintains a good rapport with the government and private sector establishments and extends assistance to the general public. Following its mandate, Sri Lanka CERT 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 activated in response to events that have the potential to adversely impact constituents' Cyber Systems. Examples include spam, virus infections, and anomalous activities identified by an Intrusion Detection System.
Sri Lanka CERT specializes in handling information security incidents. This service encompasses promptly responding to requests or notifications from constituents regarding unusual events that have been detected. Such events have the potential to disrupt the performance, availability, or stability of the services or cyber systems belonging to the concerned constituent.

3.2 Consultancy Services

This service is dedicated to empowering constituents with the means to evaluate the adequacy of their information security systems and to take necessary measures to strengthen their defences.

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's information security Team and certain predefined parameters. The 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 foremost authority on information security in Sri Lanka, Sri Lanka CERT assumes the key role of developing, introducing, and enforcing information security policy across its constituents. This advisory function ensures the establishment and adherence to robust national policies that safeguard digital assets and infrastructure effectively.

3.3 Managed Services

Sri Lanka CERT's managed security services offering is designed to strengthen the security posture of the organisation or business by providing the expertise and support that is needed to detect, prevent and remediate any cybersecurity-related threats to your IT infrastructure.

Vulnerability Assessments

Sri Lanka CERT's vulnerability assessment service plays a vital role in enhancing an organization's security posture by proactively identifying vulnerabilities before they escalate into security incidents. Leveraging a robust blend of industry tools, best practices, and proprietary techniques, our experts thoroughly examine networks and devices to uncover potential areas of risk. Through this comprehensive approach, we empower organizations to pre-emptively address vulnerabilities and fortify their defences against potential threats.

Penetration Testing

Sri Lanka CERT offers both internal and external penetration testing services, designed to replicate real-world cyberattacks and provide clients with a comprehensive understanding of vulnerabilities and threats to their network infrastructure.

These assessments commence with a discovery phase aimed at establishing a baseline profile of accessible services, ports, and systems, which serve as targets for subsequent internal or external penetration testing. Our process involves in-depth analysis, including manual probing, to:

- Assess identified components to gain access to the networks.
- Examine network devices such as firewalls, routers, and switches.
- Evaluate network services such as web, DNS, email, and FTP.
- Determine the potential impact or extent of access by attempting to exploit vulnerabilities.

Following the assessment, clients receive a detailed report outlining findings and recommendations to bolster their cybersecurity defences

System Hardening

System hardening serves the critical purpose of mitigating security risks by systematically assessing systems against established security best practices. Given the dynamic nature of organizational information systems, continuous changes

may inadvertently introduce new vulnerabilities such as misconfigurations or unnecessary software/services.
To address these evolving threats, Sri Lanka CERT conducts thorough assessments to identify potential weaknesses and recommends appropriate measures for remediation. A comprehensive report detailing findings and actionable recommendations is then provided to ensure effective risk mitigation and system protection.

On-site and off-site consultation

This service primarily revolves around incident response, aiming to alleviate the burden of day-to-day information security-related incidents for the client.
Key components of this service include:

- Over-the-phone consultancy to provide immediate guidance and support.
- On-site incident handling to address critical incidents promptly and effectively.
- Timely response and mitigation of incidents occurring at customer premises to minimize potential damage.
- Review of security policies and processes to identify areas for improvement and enhance overall incident response capabilities.

By offering comprehensive incident response support, Sri Lanka CERT ensures that clients receive timely assistance and guidance, enabling them to effectively manage and mitigate security incidents.

3.4 Digital Forensics Investigations

Since 2010, the Sri Lanka CERT has been providing exceptional digital forensic services, with a team of highly experienced digital forensics investigators. Equipped with globally accepted tools and adhering to internationally recognized procedures, Sri Lanka CERT ensures top-tier digital forensics capabilities. Sri Lanka CERT facilitates, law enforcement authorities with conducting forensic investigations under the Payment Devices Frauds Act No. 30 of 2006.
Moreover, Sri Lanka CERT conducts extensive digital forensics training programs and technical workshops tailored for both local and international audiences. These programs cater to the specific needs of public and private sector organizations, delivering customized training sessions to enhance their digital forensics proficiency.

3.5 Research & Policy Development

Sri Lanka CERT Research and Policy Development division was established with the intention of:

- Developing strategies and formulating policies related to information security and cyber security for the nation.
- Conducting national-level surveys on the various domains related to information and cyber security.
- Coordinating special national projects related to information security and cyber security.

3.6 Awareness Services

This suite of services is carefully designed to empower our constituents with knowledge and tools to reinforce their

information security posture:

Alerts & Advisory

This service delivers timely warning signals to constituents regarding computer viruses, hoaxes, security vulnerabilities, exploits, and other pertinent security concerns. It also furnishes short-term recommendations for mitigating the consequences of such attacks. Currently, alerts are disseminated through the Sri Lanka CERT website, and constituents have the option to subscribe to receive alerts via email.

Seminars & Conferences

This service aims to elevate awareness about the latest information security issues, security standards, and best practices. By equipping constituents with up-to-date knowledge, these events empower them to substantially reduce the likelihood of falling victim to cyber-attacks. Additionally, seminars can be tailored to address specific information security-related concerns upon request.

Workshops

Geared towards enhancing constituents' understanding of information security, workshops offer a more technical approach. Targeted primarily at IT professionals engaged in daily tasks related to information security, these sessions delve into specific topics with depth and detail. Workshops are organized regularly by Sri Lanka CERT, and constituents are encouraged to propose specific information security-related topics for tailored sessions that address their unique needs.

4. Operational Performance

4.1 Incident Handling Summary

Sri Lanka CERT being the national contact point for all cybersecurity-related matters receives numerous incident reports and complaints relating to the country's national cyber-space from both domestic and international partners.

In recent years, Sri Lanka has witnessed a significant rise in cyber security and social media related incidents, with Sri Lanka CERT receiving 21,743 social media and cybersecurity incidents in the year 2024. Social media-related cases (17,396) dominated, with hacked accounts (7,468) and fake accounts (4,011) being the most reported. Other concerns included online harassment, scams, and copyright violations.

Cybersecurity incidents totaled 4,347, with financial scams (2,241), phishing (79), ransomware (22), and data breaches (42) posing significant threats. Facebook accounted for 13,617 cases, highlighting social media as a key attack vector.

Category	Number of Incidents	Category	Number of Incidents
Social Media Incidents (Total)	17,396	Cybersecurity Incidents (Total)	4,347
Hacked Account	7,468	Financial Scams	2,241
Fake Account	4,011	General Scams	926
Hateful/Abusive Content	2,883	Phishing	79
Adults Sexual Harassment/Content	1,411	Ransomware	22
		Data Breach	42
Harmful & Dangerous Act	673	Website Compromise	11
Child Sexual Harassment	58	Database Compromise	4
Child Non-Sexual Harassment	60	Malware Infection	6
Suicide or Self-Harm	16	Malicious Software	4
False Information	767	Technical Issues	638
Copyright Violation/DMCA	49	Internal Inquiries	198
		System Failure	3
Total Incidents (Social Media + Cybersecurity)			21,743

Table 1: Incidents reported to Sri Lanka CERT

4.2 Services Provided By Sri Lanka Cert

Sri Lanka CERT continues to provide consultancy services, security-managed services, and web and mobile application security audits in response to requests made by both the public and private sectors.

Service Type	No. Services
Website security assessments – Government	76
Website security reassessments – Government	113
Web Security Assessments - Private Sector	25
Network security assessments and architecture reviews	12
Managed services	01
Mobile application assessments	12
Investigations	07

Table 2: Number of services in the year 2024

Further to the above services, Sri Lanka CERT has completed Twenty (20) digital forensic investigations during the year 2024. Sri Lanka CERT investigators have appeared in the courts to provide expert testimonies and provided expertise for law enforcement officers on identifying and seizing digital devices.

4.3 Training & Education Services

In order to fulfil its mandate to create awareness and build information security skills within the constituency; Sri Lanka CERT continued to organize awareness sessions and training programs targeting various audiences including Information Security Officers, Associate Information Security Officers, General Government Officers, System Administrators, Students, and the General Public.

4.3.1 Awareness Program and Training Sessions

Sri Lanka CERT conducted the following training and awareness programs:

- General Cyber Security Awareness sessions for following government organizations:
  - Sri Lanka College of Hematologists
  - Ministry of Public Administration, Home Affairs, Provincial Councils and Local Government
  - Ministry of Health – Health Informaticians
  - National Library and Documentation Services Board
  - ETF Board (Next Gen Gov Training Program)
  - Department of Registration of Persons
  - Registrar General's Department
  - District Secretariats including divisional secretaries – Kegalle, Gampaha, Anuradhapura, Polonnaruwa, Hambantota, Matara, Galle, Puttalam, Kandy, Ratnapura, Trincomalee, Batticaloa, Colombo
- General Cyber Security Awareness sessions for Industry bodies and private companies
  - Search for Common Grounds
  - Jetwing Group
  - Lanka Mineral Sands Limited
- Sessions conducted for law enforcement and judiciary.
  - Law Enforcement Officer Training- National Police Academy Katana
  - Government Analyst's Department
  - Sri Lanka Police – Designated police officials, Police IT department officials
  - Sri Lanka Police – Kurunegala division
  - Sri Lanka Police – Women and Child division's senior officials covering all island
- Sessions conducted for school community (Principles, Teachers, Students, Parents), universities and vocational training sector.
  - School Principals from the Northwestern Province
  - Education Sectoral Personnel- Western Province
  - Zonal Education Officers - Teacher Awareness Training

- Meepe Teacher Center - Zonal provincial English Subject Officers
- Youth Service Council - IT instructors
- Provincial and Zonal Education IT Officers - Awareness Program
- Vidyartha College - Galle

- Training Serious for CNII organization's ISO/AISO's
  - ISC2 CC Training for ISO/AISO
  - Continuous training program serious for CNII organizations ISO/AISOs
  - Continuous training program serious for Sri Lanka ICT service Class I officials

4.3.2 Awareness through Electronic/Print Media

Following are the details of awareness activities carried out by Sri Lanka CERT through electronic and printed media.

- Social Media Posts 147
- Monthly Newsletters 26
- Video Clips (Regular Awareness) 28
- TV & Radio Programs 18
- Press Release 15

4.3.3 Security Alerts

- 100+ compromised IPs were informed to ISPs during the year 2024.
- 18 critical security alerts were published.

4.4 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 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.

4.5 Infrastructure Development & Staff Capacity Building

4.5.1 Staff Capacity Building – International Initiatives

- Sri Lanka CERT staff members had the opportunity to participate in and represent Sri Lanka for the following training/ seminars/conferences as well.
  - The US International visitor Leadership program
  - Interpol Digital Security Challenge (DSC 2024)
  - The Asia Pacific Internet Conference on Operational Technologies (APRICOT) Summit 2024
  - APCERT Steering Committee Meeting on the margins of APRICOT Summit
  - World Internet Conference Digital Silk Road Development Forum
  - Global Cyber Drill GISEC
  - 16th Meridian Conference on Critical Information Infrastructure Protection
  - Personal Data Protection Week and Asia Privacy Forum
  - Asia Pacific Network Information Centre(APNIC) 58 Conference
  - The Elastic SIEM Training Program
  - The APNIC Program
  - 7th Annual JP-US-EU industrial control systems cyber security week for the Indo-Pacific region (FY 2024)
  - Substantive session of the open-ended working group on security of in the use of information and communication technologies

4.5.2 Staff Capacity Building – Local Initiatives

- Conducted a CISSP exam preparation Training program with the support of ISC2 Colombo Chapter

4.6 National Projects

Project Name	Project Status
National Cyber Security Operations Center (NCSOC) for real-time monitoring of cyber security incidents	• Hardware and software procured, Monitoring Centre is being prepared.
National Certification Authority (NCA) to issue certificates for Certificate Service Providers	• Hardware and software procured for NCA infrastructure upgrade.
Cyber Security Capacity Building Program for Government Officers	• A total of 48 ISOs and AISOs of CNII organizations were trained through a series of workshops. • A total of 64 Sri Lanka ICT Service Class I Officials were trained in basic cybersecurity. • A total of 3,620 government officials were given

	cybersecurity awareness trainings with the support of industry experts. • A total of 295 Police officials were given cybersecurity awareness trainings
Cyber Security Readiness of 10 Government Organizations	• Completed risk assessments of 10 government organizations.

Table 3: A Summary of National Projects

4.7 Information And Cyber Security Policy For Government Organizations

The Ministry of Technology issued a circular for all critical government organizations to implement the Cabinet approved Information and Cyber Security Policy. Sri Lanka CERT has prioritized 43 organizations that manage Critical Information Infrastructure to implement the policy. As a part of this process, IT General Control Reviews were completed for 19 organizations and risk assessments were completed in organizations.

4.8 Other Engagements

In addition to above services, Sri Lanka CERT 7 other security assessments including NIST completed Compliance reviews, BCP and DRP drill reviews etc.

5. Achievements

5.1 National Cyber Security Strategy Of Sri Lanka (2025 – 2029)

With the assistance of the World Bank, Sri Lanka CERT has undertaken the steps to develop the next version of the National Cyber Security Strategy, which will be implemented from 2025 to 2029. The drafting of the strategy was completed, and it will be submitted to the Cabinet of Ministers for necessary approval.

5.2 Other Achievements

- Winner of the prestigious ASOCIO 2024 DX Cybersecurity Award for the Public Sector, presented by the Asian-Oceanian Computing Industry Organization (ASOCIO) at the 2024 Digital Summit in Tokyo

- Recognized as Tier 2 – Advancing country in Global Cybersecurity Index (GCI) published by ITU (International Telecommunication Union) which demonstrates the effectiveness of the deployed National Cyber Security Strategy (2019:2023)
- Became a member state of the US-led Counter Ransomware (CRI) Initiative to foster cooperation between nations to combat ransomware.
- Became the Technical Point of Contact (PoC) in the UN global intergovernmental PoC directory established by the OEWG ICT security.
- Achieved the WebTrust Certification for NCA Operations, affirming that the Certification Authority meets the AICPA/CICA WebTrust Principles and Criteria, enhancing consumer confidence in e-commerce and the application of PKI technology.

5.3 Memberships

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

- Membership for Threat Intelligence from ShadowServer.
- Membership of FIRST
- Membership of APCERT
- Membership of CAMP, Korea
- Membership of TF-CSIRT
- Membership of CRI

6. International Collaboration

6.1 APCERT

04-01-2024	**Webinar for Registration Data Request Service (RDRS)**
18-01-2024	Steering Committee Meeting
30-01-2024	APCERT Training: Incident Handling
26-02-2024	APCERT Face-to Face SC Meeting - Bangkok, Thailand
15-03-2024	Team Report for APCERT Annual Report 2023
17-01-2024	Review Daft IoT Security WG 2nd Report (v3.0)
19-01-2024	Review APCERT Business Plan 2023-2024
21-02-2024	Proposal for 5G Security WG (convener Sri Lanka CERT) submitted
26-03-2024	APCERT Training: Detecting malicious activities of APT groups

18-03-2024	Invitations of members to 5G Security WG called by Sri Lanka CERT
25-03-2024	Review Information Sharing and Handling Policy of APCERT
08-05-2024	Steering Committee Meeting
18-04-2024	Review APCERT AccessLine Draft
18-04-2024	Membership Working Group Meeting
07-05-2024	APCERT Training: Cyber Security Incident Response
01-07-2024	Steering Committee Meeting
24-05-2024	APCERT Drill Working Group Meeting
16-07-2024	APCERT Training: Introduction to Threat Intelligence
03-07-2024	Sri Lanka CERT Official Registration for APCERT Drill 2024
26-08-2024	Steering Committee Meeting
24-07-2024	Review APCERT AccessLine (July 2024) f
10-09-2024	APCERT Training: Incidents Handling and Ticketing
05-11-2024	Annual General Meeting and Conference 2024 (Online)
29-08-2024	APCERT Drill 2024
29-08-2024	Review Mongolia National CSIRT's APCERT OM application
25-10-2024	Steering Committee Meeting
17-09-2024	Domain Trust Community Meeting / GCA
02-12-2024	APCERT Training: Experience sharing on social media

CAMP Table 4: APCERT Activities

6.2 CAMP

- CAMP Member Survey Participation
- CAMP Member Written-Interview
- 2025 Program of Work Review

7. Future Plans

7.1 Future Projects To Be Implemented

Following are key initiatives that will be implemented during the year 2024.

- Implementation of Information and Cyber Security Policy in the government organisations.
- Obtaining the Cabinet Approval for the National Cyber Security Strategy of Sri Lanka (2025 - 2029).
- Enactment of Cyber Security Act.
- Establishment of the Cyber Security Authority
- Complete the establishment of NCSOC
- Obtain ISO 27001 certification for IT operations of Sri Lanka CERT

8. Conclusion

In 2024, Sri Lanka CERT achieved remarkable success, effectively completing the majority of its tasks without encountering significant issues. A key milestone was the successful implementation of the Information and Cyber Security Strategy (2019-2024) and the commencement of the implementation of the Information and Cyber Security Policy for Government Organizations. Additionally, the initiation of the National Cyber Security Operations Centre and the drafting of the next version of the National Cyber Security Strategy (2025-2029) are noteworthy accomplishments. Sri Lanka CERT continues to provide its services to stakeholders to improve the country's cyber security resilience.

Sri Lanka CERT significantly enhanced national cyber security awareness through extensive awareness sessions and demonstrated a high-resolution rate in handling reported cases. Its active participation and representation in international forums underscored Sri Lanka CERT's commitment to global cyber security cooperation. Another important achievement was the onboarding of the first Sub-CA by the National Certification Authority, marking significant progress in digital certification efforts.

Reflecting on these accomplishments, Sri Lanka CERT is prepared to leverage its successes and further strengthen its impact in the coming year.

ThaiCERT

Thailand Computer Emergency Response Team

1. Highlights of 2024

1.1 Summary of major activities

- ThaiCERT actively monitored and responded to cyber threats. This involved both proactive and reactive measures. Total of 1,827 incidents reported in 2024.
- ThaiCERT conducted Vulnerability Assessments (VA) for 96 organizations and Penetration Testing (Pentest) for 15 organizations
- ThaiCERT focused on promoting cybersecurity awareness, conducting **78** knowledge sharing sessions. Total of 9,854 personal participated.
- ThaiCERT receiving and sharing cyber threat information through MISP, connecting **40** organizations. This platform processed **52,721,920** Indicators of Compromise (IoCs)
- ThaiCERT issued **90** cyber threat, risk, and vulnerability warnings, and **449** public information reports on cyber threats

1.2 Achievements & milestones

Global Cybersecurity Index (GCI) Ranking. Thailand scoring 99.22/100 in the GCI and classified in T1-Role Model Country.

2. About CSIRT

2.1 Introduction

ThaiCERT (Thailand Computer Emergency Response Team) is the national cybersecurity incident response team of Thailand, operating under the **National Cyber Security Agency (NCSA)**. ThaiCERT plays a crucial role in enhancing Thailand's cybersecurity resilience by coordinating incident response efforts, providing threat intelligence, and

supporting organizations in mitigating cyber threats.
As the central point of contact for cybersecurity incidents in Thailand, ThaiCERT works closely with government agencies, private sector, and critical information infrastructure organization to detect, prevent, and respond to cyber threats. It also collaborates with international cybersecurity communities to strengthen global cyber defense efforts.
Through proactive monitoring, security advisories, and capacity-building initiatives, ThaiCERT aims to improve the overall cybersecurity posture of the country and ensure a safer digital environment for all stakeholders.

2.2 Establishment

ThaiCERT (Thailand Computer Emergency Response Team) was established in 2000 as the national CERT of Thailand. It originally operated under the Electronic Transactions Development Agency (ETDA). However, in 2019, with the enactment of the Cybersecurity Act, ThaiCERT became part of the National Cyber Security Agency (NCSA), which is responsible for national cybersecurity policy, coordination, and incident response.
ThaiCERT's primary role is to coordinate cybersecurity incident response efforts, provide threat intelligence, and support government agencies, businesses, and critical information infrastructure organizations in handling cyber threats. It also collaborates with international cybersecurity organizations to enhance Thailand's cyber resilience.

2.3 Resources

ThaiCERT consists of a team of 20 professionals dedicated to cybersecurity operations, incident response, and national cyber resilience initiatives. The team is structured into the Cyber Operation Office and the Cyber Coordination Office, ensuring effective management of cybersecurity threats and collaborations.

2.4 Constituency

ThaiCERT's responsibilities encompass a diverse range of stakeholders, including critical information infrastructure (CII) organizations in sectors such as finance, energy, public health, and transportation, which are vital for national stability. The agency provides support to government entities at all levels in managing and responding to cyber incidents. Additionally, ThaiCERT promotes the establishment of Sectoral CERTs—specialized cybersecurity response teams within specific sectors—to enhance coordination and incident management efforts.
ThaiCERT also addresses the private sector's growing cybersecurity needs by offering guidance and resources to mitigate cyber threats. Furthermore, it collaborates with international partners to strengthen cyber threat intelligence and improve national cybersecurity capabilities.

3. Activities & Operations

3.1 Scope and definitions

ThaiCERT's scope includes cybersecurity incident monitoring, threat intelligence sharing, incident response, and capacity building to enhance Thailand's cyber resilience. It collaborates with government, private sectors, critical information infrastructure, and international partners. A cybersecurity incident threatens the confidentiality, integrity, or availability of systems, while incident response involves detecting and mitigating such threats. Critical Information Infrastructure (CII) refers to services that are important to national security, military security, economic security, and public order in the country. ThaiCERT aims to strengthen both national and global cybersecurity efforts.

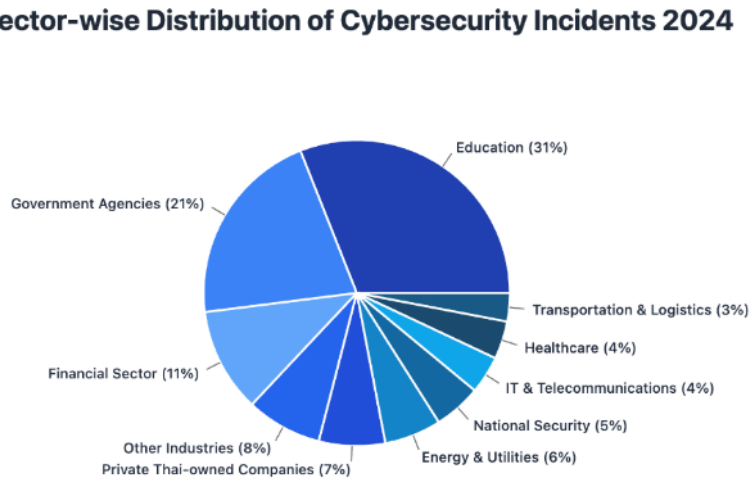
3.2 Incident handling reports

ThaiCERT has been proactive in monitoring and responding to cyber threats. From October 2023 to September 2024, 1,827 cybersecurity incidents were handled. Among these, 16% involved hacked websites due to defacement, while 15% were linked to illegal gambling sites. Additionally, 13% were related to fake websites, 12% accounted for other miscellaneous threats, and 10% involved privileged account compromises. Furthermore, there were 10% system vulnerabilities, 9% financial scams, 7% data breaches, 3% DDoS attacks, 3% security misconfigurations, and 2% data leaks.

In terms of proactive measures, ThaiCERT issued 90 notifications about cyber threat intelligence and 449 public releases of cybersecurity threats and useful information. To strengthen cybersecurity defenses, 96 vulnerability assessments (VA) and 15 penetration tests (Pentests) were conducted to identify weaknesses in system access, leveraging expert analysis.

3.3 Abuse statistics

ThaiCERT recorded a diverse range of cybersecurity incidents across multiple sectors. The education sector was the most affected, accounting for 31% of reported cases, followed by 21% in other government agencies and 11% in the financial sector. Additionally, 8% of incidents occurred in other industries, while 7% were reported by private Thai-owned companies. The energy and utilities sector experienced 6% of incidents, national security accounted for 5%, and both information technology & telecommunications and healthcare sectors reported 4% each. Lastly, the transportation and logistics sector encountered 3% of cybersecurity incidents.



3.4 Publications

3.4.1 ThaiCERT annual report

ThaiCERT releases annual reports summarizing its activities and findings every year.

3.4.2 Monthly report

3.4.2.1 IOC (Indicators of Compromise) monthly report

This report include details on specific IoCs identified, trends, and analysis of their potential impact.

3.4.2.2 Credential Leak monthly report

This report include the number of leaked accounts, affected sectors, and analysis of the sources and potential impact of these leaks. The information can be used for proactive protection.

3.4.2.3 Cyber Attack monthly report

This report provides an overview of cyber attacks that occurred during the month. It includes information on the types of attacks, targeted sectors, and the tactics and techniques used by attackers

3.5 New services

Cyber Threat Intelligence Sharing: The NCSA has established the Cyber Threat Intelligence Information Center and MISP platform to improve collaborative efforts in sharing cyber threat intelligence.

4. Events organized / hosted

4.1 Training

- Cybersecurity Leadership Programs: Hosted training sessions on leadership and incident response, including collaborations with international experts to enhance decision-making and response skills.
- Cloud Security Workshops: A series of hands-on workshops hosted in partnership with Fortinet Thailand, focusing on cloud security best practices.
- Web3.0 and Cybersecurity Seminar: Organized a seminar on Web3.0, attended by over 50 participants, discussing the intersection of blockchain and cybersecurity.

4.2 Drills & exercises

- Thailand National Cyber Exercise: A large-scale cybersecurity exercise with over 1,000 participants, simulating real-world cyber-attack scenarios and enhancing national cyber resilience.
- Cyber War Game Simulation: An event designed to simulate cyber-attacks, enabling participants to practice real-time decision-making and cybersecurity response strategies.
- ASEAN CyberSEA Game: Co-hosted by the NCSA and AJCCBC, this competition featured teams from 10 ASEAN countries, sharpening regional collaboration and defense strategies through simulated cyber-attacks.

4.3 Conferences and seminars

- Global Cybersecurity Summit: NCSA organized and participated in this summit, bringing together experts to discuss cutting-edge developments in cybersecurity.
- ASEAN Cybersecurity Awareness Forum: Organized forums that fostered cross-border communication and shared cybersecurity strategies between ASEAN nations.
- Women in Cybersecurity Initiatives: Held events like Women Thailand Cyber Top Talent to inspire and engage more women in cybersecurity, focusing on leadership and opportunities within the industry.

5. International Collaboration

5.1 International partnerships and agreements

MOU

To further strengthen cybersecurity cooperation, ThaiCERT exchanges a Memorandum of Understanding (MoU) with various cybersecurity organizations. This collaboration aims to enhance threat intelligence sharing, incident response coordination, capacity building, and joint cybersecurity initiatives. Through these partnerships, ThaiCERT works closely with both domestic and international entities to improve cyber resilience and mitigate emerging threats effectively.

FIRST (Forum of Incident Response and Security Teams) https://www.first.org

ThaiCERT actively contributes to the international CSIRT community FIRST, collaborating with global cybersecurity teams to enhance incident response capabilities. Additionally, ThaiCERT supports organizations in Thailand that seek FIRST membership by guiding them through the application process and fostering international cooperation.

APCERT (Asia Pacific Computer Emergency Response Team) https://www.apcert.org/

As a member of APCERT, ThaiCERT participates in regional cybersecurity initiatives, information sharing, and capacity-building efforts. ThaiCERT works closely with other national CSIRTs in the Asia-Pacific region to enhance collective cyber resilience and promote best practices in incident response.

5.2 Capacity building

5.2.1 Training

- Cybersecurity Foundation Course: This course, developed by the NCSA, has been delivered across ASEAN and serves as the foundation for building national cybersecurity frameworks.
- Cybersecurity Leadership Academy: The NCSA partnered with global cybersecurity experts like Google, Huawei, and EC-Council to offer leadership training to government officials and private-sector leaders in ASEAN countries.

5.2.2 Drills & exercises

- CyberSEA Game 2024: This regional event brought together cybersecurity teams from 10 ASEAN countries to simulate cyber threats and improve responses through collaborative exercises.
- Thailand National Cyber Exercise 2024: Engaged over 1,000 participants from government agencies, regulators, and critical information infrastructure organization to simulate responses to large-scale cyber threats in national cybersecurity drills.

5.2.3 Seminars & presentations

- ASEAN Cybersecurity Summit: The NCSA played a key role in co-hosting this summit, which attracted cybersecurity

experts from across ASEAN to share strategies, challenges, and innovations.

- Global Cybersecurity Awareness Forum: As part of its outreach, the NCSA organized this forum to discuss global cybersecurity trends and best practices, fostering international collaboration in securing the digital space.

5.3 Other international activities

- Cybersecurity Research Collaboration with NECTEC: NCSA collaborated with NECTEC (National Electronics and Computer Technology Center) to drive local research into cybersecurity technologies with global applications.
- Global Cybersecurity Capacity Building Project: In partnership with APEC and UNODC (United Nations Office on Drugs and Crime), NCSA helped to launch this initiative to enhance global cybersecurity training and capacity, especially in developing nations.
- Cybersecurity Standardization for ASEAN: The NCSA led efforts to establish cybersecurity standards across ASEAN through the ASEAN Cybersecurity Cooperation Strategy, aligning regional policies with international best practices.

6. Future Plans

6.1 Future projects

- Capacity Building and Training: The NCSA will work with international CERTs to offer training, develop educational materials, and build cybersecurity expertise globally.
- Public Awareness Campaigns: The NCSA will expand efforts to educate citizens about new fraud tactics, such as fake QR codes and phishing attacks, through international outreach programs.

6.2 Future Operation

- Strengthening Global Collaboration: The NCSA will maintain and deepen its collaboration with international law enforcement, CERTs, and cybersecurity bodies to stay ahead of emerging fraud tactics and ensure a coordinated global response.

7. Conclusion

Thailand's cybersecurity landscape has seen significant advancements in 2024, with enhanced public awareness programs, strengthened infrastructure, and successful collaborations both domestically and internationally. The expansion of training programs and the continued focus on capacity-building, policy development, and international cooperation ensure that Thailand is well-prepared to face future challenges in the ever-changing digital world.

TWCERT/CC

Taiwan Computer Emergency Response Team / Coordination Center

1. Highlights of 2024

1.1 Achievements & Milestones

TWCERT/CC is committed to strengthening Taiwan's capability to respond to and handle cybersecurity incidents. In 2024, TWCERT/CC merged with TWNCERT, expanding its services to government, industry and academia. Over the past year, TWCERT/CC has accomplished the following:

- Received and assisted in handling over 400 cybersecurity incident reports from the private sector.
- Published 12 e-newsletters, 4 awareness videos, and 4 cybersecurity awareness articles ("Cybersecurity Tips") to enhance cybersecurity awareness among enterprises and the public.
- Reviewed and assigned 157 CVE IDs issued on the Taiwan Vulnerability Note (TVN).
- Operated an online malicious file analysis service, scanning over 1,900 suspicious files.
- As the convener of the APCERT Training Working Group, organized six online training sessions, engaging 26 APCERT member teams.
- Hosted the APCERT AGM and Conference 2024, themed "Power of Together: More Than the Sum of APCERTs/CSIRTs" and co-hosted APCERT and FIRST Regional Symposium for Asia Pacific.

2. About TWCERT/CC

2.1 Introduction

TWCERT/CC provides services to government agencies, critical infrastructure (CI) providers, and local enterprises, including incident reporting and coordination, product vulnerability disclosure, Virus Check service, and cybersecurity awareness campaigns. It also fosters intelligence sharing with domestic and international CERTs/CSIRTs, cybersecurity organizations, academic institutions, civil communities, government agencies, and private enterprises. Through these efforts, TWCERT/CC strengthens national cybersecurity defenses and jointly safeguards Taiwan's digital environment.

2.2 Establishment

Established in 1998, TWCERT/CC merged with TWNCERT in 2024 and is now operated by the National Institute of Cyber Security (NICS) under the Ministry of Digital Affairs (MoDA). With an expanded scope of service covering government, industry, and academia, TWCERT/CC enhances its capabilities in cyber threat monitoring and incident coordination and response.

2.3 Constituency

TWCERT/CC is dedicated to enhancing the cybersecurity incident reporting and response capabilities of Taiwan's government agencies, critical infrastructure providers, and the private sector. It collaborates with various stakeholders, including CERTs and ISACs across sectors such as finance, telecommunications, energy, transportation, healthcare, high-tech parks, and academia, as well as MSSPs, law enforcement agencies, and both domestic and international cybersecurity vendors and organizations.

3. Activities & Operations

3.1 Scope and Definitions

Key responsibilities of TWCERT/CC:

Incident Response and Early Warnings

TWCERT/CC coordinates cybersecurity incident response for Taiwan's government agencies, CI providers, and private sector, analyzing and generating early warning intelligence to counter cyberattacks. It also provides the Virus Check service to assist the public in detecting the risk levels of suspicious files. Additionally, as a CVE Numbering Authority (CNA), TWCERT/CC reviews and assigns CVE IDs to vulnerabilities that meet the criteria.

Information Sharing

TWCERT/CC compiles cybersecurity intelligence from domestic organizations, establishing diverse channels for information sharing to foster cross-sector collaboration in cybersecurity.

Awareness Enhancement

TWCERT/CC strengthens the cybersecurity joint defense system by promoting the Taiwan CERT/CSIRT Alliance and raises public awareness through e-newsletters, articles, and awareness videos.

International Collaboration

TWCERT/CC establishes communication channels for domestic and international incident response organizations and

facilitates cooperation among global CSIRTs, vendors, and other cybersecurity entities.

3.2 Incident Handling Reports

In 2024, TWCERT/CC received over 400 cybersecurity incident reports from various sources, including private enterprises, private organizations (such as the HITCON community), and individuals. Reports from private organizations accounted for the majority, making up 53.06% of the total.

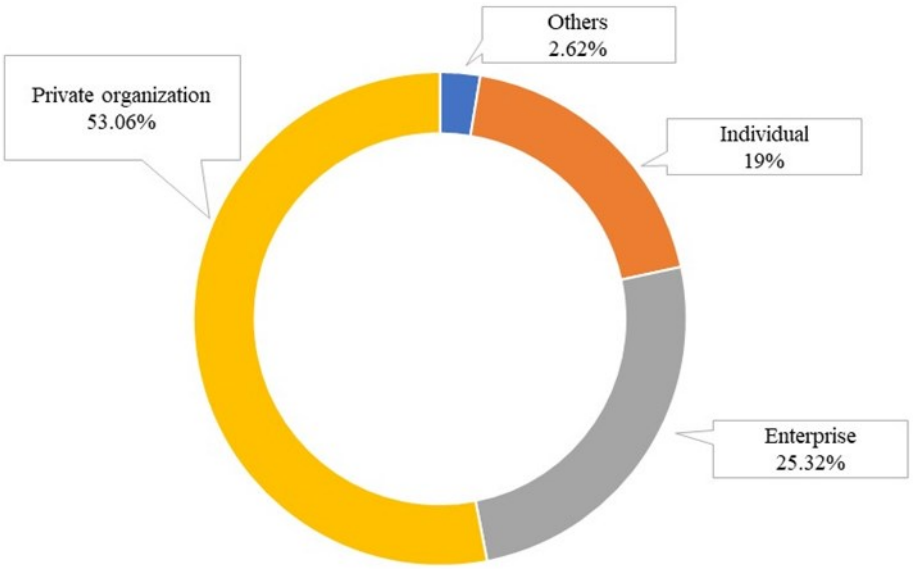


Figure 1. Incident Report Sources

3.3 Abuse Statistics

Incident Reports

In 2024, TWCERT/CC received over 400 incident reports from the private sector, with third-party vulnerabilities accounting for the largest share, approximately 54% of all reports.

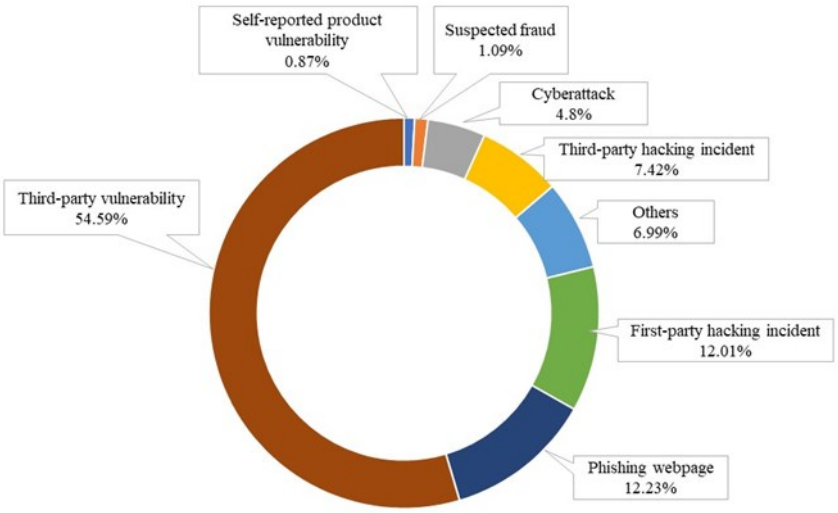


Figure 2. Incident Reports from the Private Sector

Domestic Cyber Information Sharing

TWCERT/CC integrates domestic resources and shares cybersecurity intelligence through its system with N-ISAC members, the Taiwan CERT/CSIRT Alliance, government agencies, and private enterprises.

In 2024, TWCERT/CC shared over 600 pieces of cyber information. Intrusion incidents accounted for the largest portion at 64.63%, followed by vulnerability intelligence at 32.73%. Indicators of compromise (IoC) and early warnings made up 2.15% and 0.49%, respectively.

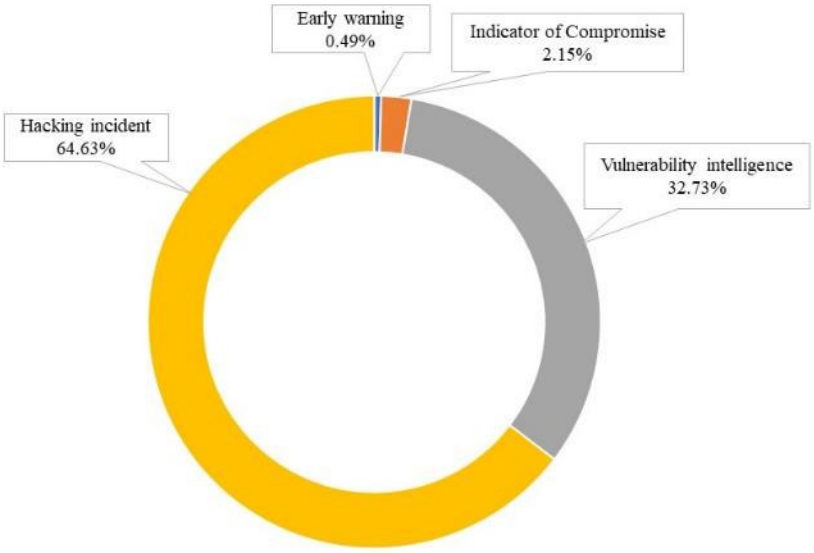


Figure 3. Domestic Cyber Information Sharing

CVE Assignment

In 2024, TWCERT/CC received vulnerability reports from various sources and assigned a total of 168 CVE IDs.

Virus Check

TWCERT/CC provides an online scanning service, allowing users to upload suspicious files for malware detection. The service first obtains the hash value of the submitted file and searches the threat intelligence to determine whether it is a known malware. It then conducts both static scanning and dynamic analysis to assess potential risks.

In 2024, we analyzed over 1,900 suspicious files. Among them, more than 700 were identified as risky through static scanning, while approximately 1,000 were determined to be risky following dynamic analysis.

3.4 Publications

E-newsletters

TWCERT/CC publishes a monthly e-newsletter featuring the latest cybersecurity updates, vulnerability alerts, and threat analyses. This helps the public stay informed and enables enterprises to monitor attack activities and implement defense strategies in a timely manner.

The newsletters also compile training resources and relevant information to facilitate public participation, aiming to enhance cybersecurity awareness and better prepare for potential risks.

Cybersecurity Awareness Videos

In 2024, TWCERT/CC produced four awareness videos highlighting cybersecurity threats that enterprises and the public should be aware of. The topics included:

- Social Engineering Attacks
- How Enterprises Can Defend Against Ransomware
- The Importance of Industrial Control System (ICS) Security
- Supply Chain Cybersecurity 2.0

Awareness Articles

TWCERT/CC published four awareness articles (“Cybersecurity Tips”) in 2024 on topics including:

- Preventing Cryptocurrency Address Poisoning Attacks
- How to Identify Fake News in the Digital Age
- The New PassKey Authentication Method
- Common OTP Authentication Practices

These articles aim to improve the public’s and enterprises’ basic understanding of cybersecurity and its practical principles, preventing data breaches, unauthorized access, and cyber threats while ensuring the security and stability of the digital environment.

4. Events organized/hosted

In 2024, TWCERT/CC organized two cybersecurity incident reporting training sessions and hosted its annual conference to expand the exchange of cybersecurity incident response and threat intelligence among local enterprises. These efforts aimed to promote incident reporting within local businesses and enhance cybersecurity awareness.

Taiwan CERT/CSIRT Alliance Training

In August, TWCERT/CC held a half-day training session in Taichung, and another in Taipei in October. The training combined two topics: "Preparing for and Handling Cybersecurity Incidents" and "Cybersecurity Incident Reporting and Response Guidelines", along with emerging cybersecurity issues and trends. Academic and industry experts were invited to share insights on incident reporting and protection measures. Additionally, discussion sessions were arranged after the training to encourage attendees to share and exchange their thoughts.

2024 TWCERT/CC Annual Conference

On November 22, 2024, TWCERT/CC hosted the 2024 Taiwan Cybersecurity Incident Response Annual Conference. The conference focused on topics such as incident management, generative AI, zero trust architecture, and supply chain management. Experts from both the public and private sectors were invited to share their valuable insights and experiences.

5. International Collaboration

5.1 International Partnerships and Agreements

TWCERT/CC actively participates in the member activities of international organizations, including regular meetings, working group activities, annual conferences, and other collaborative initiatives. Currently, TWCERT/CC is involved with the following international organizations:

- APCERT
- FIRST

5.2 Capacity Building

5.2.1 Training

As the convener of the APCERT Training Working Group, TWCERT/CC coordinated member teams and organized 6 online training sessions in 2024:

Date	Topic	Trainer
Jan 31	Incident Handling	Cybersecurity Malaysia
Mar 26	Detecting Malicious Activities of APT Groups	KZ-CERT
May 28	Cyber Security Incident Response: The Regulation, Statistics, and Experience Among Taiwan Government and Critical Infrastructure	TWCERT/CC
Jul 16	Introduction to Threat Intelligence Tools: OpenCTI Introduction	HUAWEI PSIRT
Sep 27	Incidents Handling and Ticketing	NCA-CERT
Dec 2	Experience Sharing on Social Media Incident Handling by Bhutan Computer Incident Response Team	BtCERT

5.2.2 Drills & Exercises

On August 22, 2024, the APCERT Drill, titled "**APT Group Attack Response: Where is Wally?**", was held. TWCERT/CC successfully completed the exercise scenario within the allocated time.

5.2.3 Seminars & Presentations

TWCERT/CC hosted the APCERT AGM and Conference 2024 on November 5-6, themed "Power of Together: More Than the Sum of AP CERTs/CSIRTs." Additionally, in collaboration with FIRST, TWCERT/CC co-hosted the 2024 APCERT and FIRST Regional Symposium for Asia Pacific, which featured an Open Conference on November 7 and Training on November 8. The event attracted cybersecurity experts from 25 Asia-Pacific region and global economies, where they discussed global cybersecurity threat trends, the impact and opportunities of emerging AI technologies, cybersecurity governance strengthening, cross-border collaboration, and talent development.

In addition, TWCERT/CC also participated in the following international events:

- APEC TEL Conference
- 36th Annual FIRST Conference
- 2024 National CSIRT Meeting

6. Future Plans and Conclusion

TWCERT/CC remains committed to expanding private sector participation in the Taiwan CERT/CSIRT Alliance, and enhancing information sharing through collaborative projects. By integrating existing government defense mechanisms, we aim to build a more robust public-private cybersecurity defense system. At the same time, we are exploring partnerships with competent authorities, industry associations, and corporate alliances to develop initiatives such as cybersecurity assessments, data protection measures, and training programs—gradually strengthening cybersecurity resilience across industries.

For the APCERT online training program, TWCERT/CC will continue coordinating speakers and participants, delivering

bi-monthly training sessions, and deepening collaboration with other APCERT working groups. Additionally, we will stay actively engaged in APCERT activities, including the APCERT Drill, while exploring new partnerships with international organizations. These efforts will further expand and enhance training programs, strengthening cybersecurity awareness and incident response capabilities on a global scale.

Activity Reports from APCERT Partners

CERT-GIB

Computer Emergency Response Team Group-IB

1. About the Organization

CERT-GIB (https://group-ib.com/) is the Computer Emergency Response Team created by the global cybersecurity company Group-IB. It is launched with the mission to immediately contain cyber threats, regardless of when, where they take place, and who is involved. CERT-GIB combines the power of human intelligence with technological prowess to offer the most effective response and remediation actions.

Group-IB adopted a decentralized operational strategy enabling collective action against cybercrime and comprehensive coverage of threat actors across all geographies for information exchange as the only effective long-term solution. Group-IB's GLOCAL strategy ensures the most robust response to cybercrime worldwide through its Digital Crime Resistance Centers (DCRCs), which deliver immediate, comprehensive, localized expertise and intelligence support. DCRC network spans multiple strategic locations, including Singapore, the Netherlands, UAE, Saudi Arabia, Vietnam, Malaysia, Thailand, Italy, Uzbekistan, Chile, and Egypt.

Aside from being an APCERT member, CERT-GIB is a member of Trusted Introducer, Anti-Phishing Working Group (APWG), FIRST, OIC-CERT, Europol European Cybercrime Centre's (EC3) Advisory Group on Internet Security, and a strategic partner of Afripol and the International Multilateral Partnership Against Cyber Threats (IMPACT).

2. Activities & Operations in 2024

2.1 Operations

Group-IB contributed mission critical data and investigative research that supported eight local and international law enforcement operations, including two operations covering the APAC region.

In June 2024, Group-IB supported **Operation DISTANTHILL**, a joint effort by Singapore, Hong Kong, and Malaysian police to dismantle cyber fraud syndicates behind a 2023 Android Remote Access Trojan (RAT) campaign. Group-IB's analysis revealed over 250 phishing pages, C2 servers linked to 100+ malware samples, and insights into the syndicate's network. The campaign defrauded 4,000+ victims across Southeast Asia, including 1,899 cases in Singapore, with losses exceeding US$25 million.

In November 2024, Group-IB supported **Operation Synergia II**, an INTERPOL-led initiative involving 95 countries to combat phishing, ransomware, and malware attacks. The operation dismantled 22,000 malicious servers, seized 59 servers and 43 electronic devices, and led to 41 arrests, with 65 suspects under investigation. Group-IB analysts identified over 2,500 IPs linked to 5,000 phishing sites and 1,300 IPs tied to malware activities across 84 countries. In total, approximately 30,000 suspicious IPs were uncovered, significantly disrupting global cybercrime infrastructure.

2.2 Anti-Phishing and Anti-Scam Activities

In 2024, CERT-GIB detected more than 80,000 phishing websites, marking a 22% increase over the previous year.
In APAC, the most targeted industries were financial services, commerce and shopping, and transportation, accounting for 51.6%, 20.4%, and 15% of phishing websites, respectively.
CERT-GIB also detected more than 200,000 scam resources, marking a 22% increase year-on-year, with nearly 79% of observed scams in APAC targeting the financial institutions.
One of the key responsibilities of CERT-GIB is not only to detect violations, but also to take down violating resources. CERT-GIB actively interacts with domain name registrars, TLD administrators, ISPs, as well as with other CERT and CSIRT teams to eliminate the violations.
In 2024, CERT-GIB responded to more than 69,000 phishing resources and 104,000 scam resources, achieving successful takedowns of 99% and 96% of these, respectively.

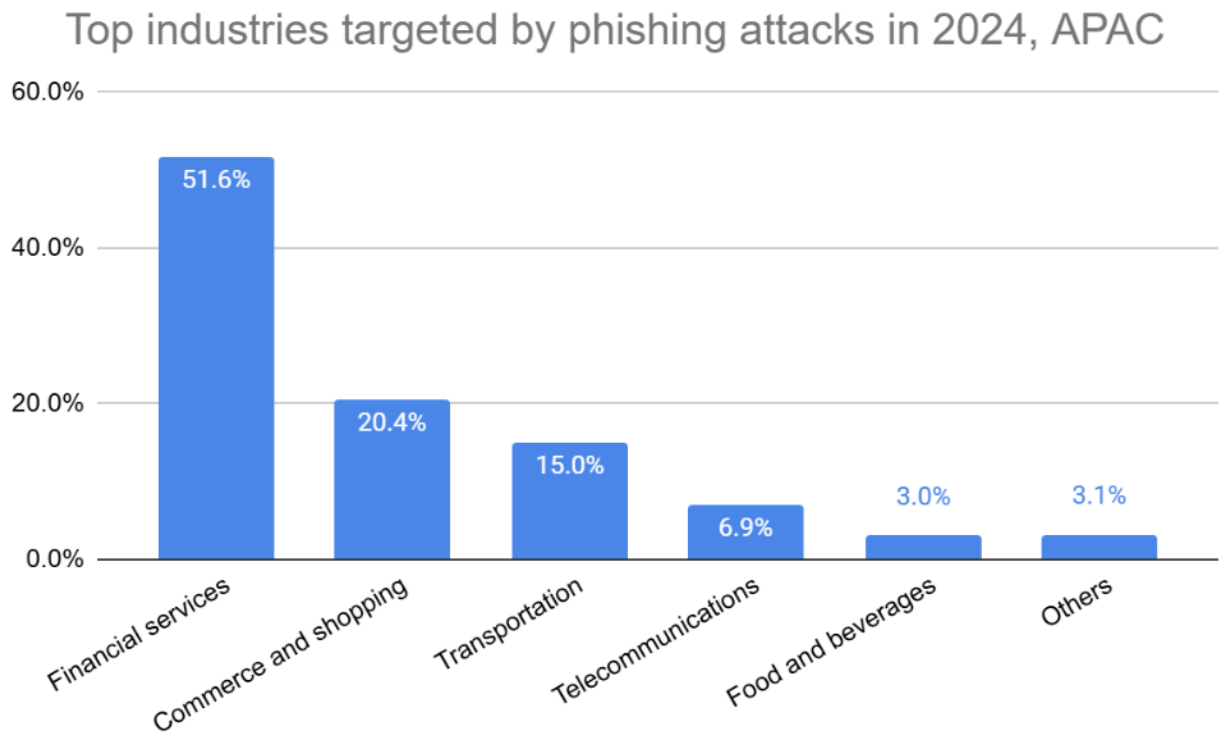


Figure 1. Top industries in APAC targeted by phishing attacks in 2024

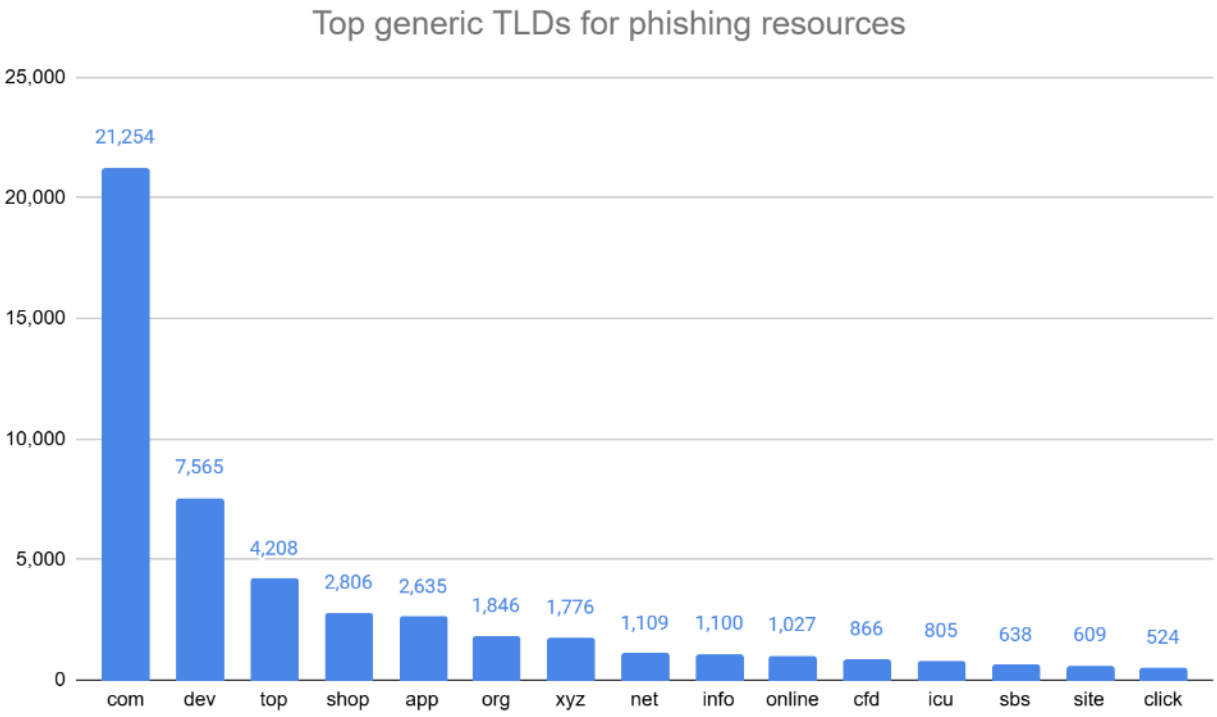


Figure 2. Top generic TLDs for phishing resources

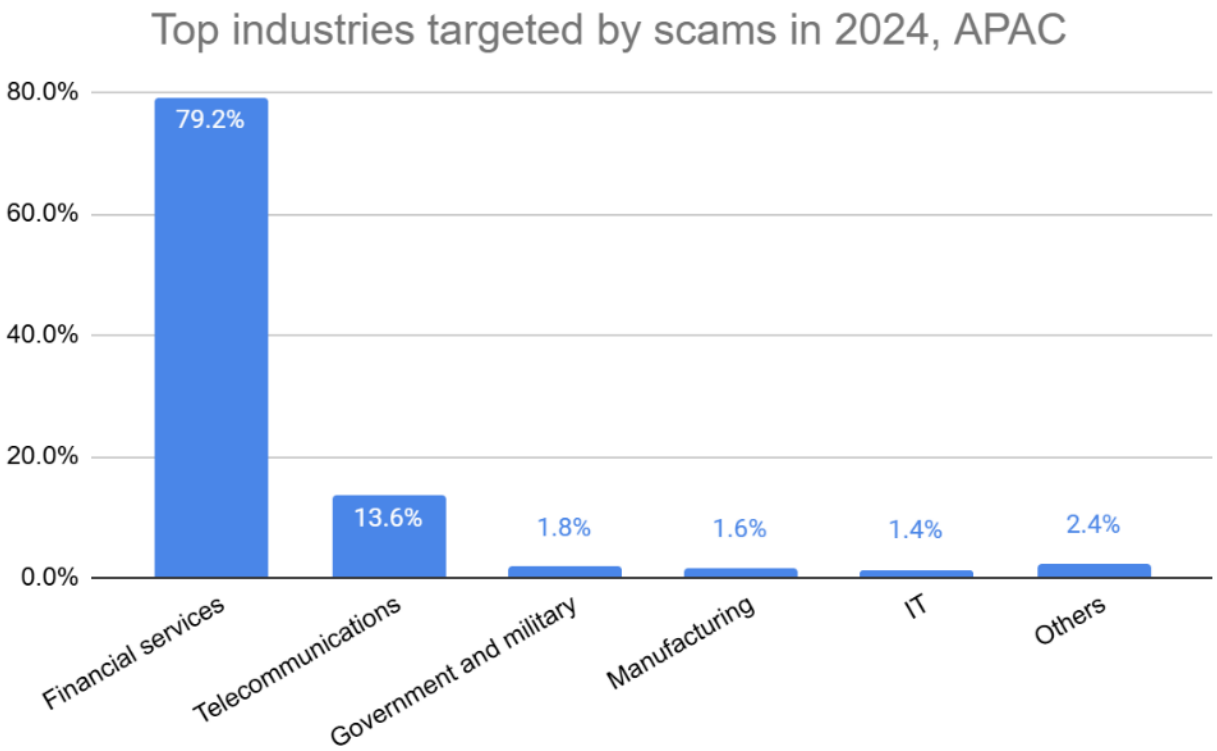


Figure 3. Top industries in APAC targeted by scams in 2024

2.3 Activities

№	Activity	Description	Date
1	Training	National Cyber Security Agency of Thailand (NCSA)	25 January 2024
2	Training	Hong Kong Police Force (HKPF) Annual Cyber Command Course	29 January 2024
3	Event	Fraud Protection Roundtable (Hong Kong)	30 January 2024
7	Event	Seamless Asia	20 February 2024
8	Achievement	Group-IB uncovers new VietCredCare information stealer targeting Facebook advertisers	21 February 2024
11	Event	Group-IB launches in Cambodia	6 March 2024
13	Training	Hong Kong Police Force: AI Fueled Efficiency Race Between Cybercriminals and Defenders	24 April 2024
14	Event	Panel Discussion at HELP University Annual Strategy Seminar	4 May 2024
15	Event	Panel Discussion at Sigma Asia (Held in the Philippines)	5 May 2024
16	Event	Fraud Protection Roundtable in Singapore	14 May 2024
17	Event	India Fraud Risk Summit	16 May 2024
18	Event	Panel Discussion at General Membership Meeting of the Philippine Finance Association (PFA)	20 May 2024
19	Event	Panel Discussion at Regulation Asia Fraud & Financial Crime Asia Summit	21 May 2024
20	Achievement	Group-IB becomes the first SOC-CMM Network Silver Support Partner in Asia	10 June 2024
22	Event	Participation and Demonstration of National SOC Concept at CyberDSA (Malaysia)	6 August 2024
24	Event	TB-CERT Annual Conference (Thailand)	28 August 2024
25	Event	ISS World Asia Conference + Demonstration of Graph 2.0	3 September 2024
26	Achievement	Top Women in Security ASEAN Awards 2024: Anastasia Tikhonova and Ha Hai Phan win Country Awards, with Vesta Matveeva and Sharmine Low among top 30 finalists	13 September 2024

29	Event	GovWare 2024: 1) Cyber Insights Live podcast 2) Panel Discussion for Singapore International Cyber Week (SICW) 3) Tech Talk Panel Discussion	15 October 2024
30	Achievement	Outstanding Security Performance Award (OSPA) Southeast Asia - Jennifer Soh for Outstanding Female Security Professional	4 November 2024
31	Event	Panel Discussion at the 14th Cybercrime Directors Workshop jointly hosted by INTERPOL and Hong Kong Police Force (HKPF)	8 November 2024
32	Event	Presentation at ASEAN Cybercrime Conference jointly organised by Singapore Police Force (SPF) and Ministry of Home Affairs Singapore (MFA)	13 November 2024
33	Training	Guest Lectures at Ngee Ann Polytechnic for Cybersecurity & Digital Forensics Diploma Course	13 November 2024
34	Event	Participation at Malaysia Institute of Accountants (MIA) Cyber Security Conference	19 November 2024
35	Achievement	Group-IB identifies a phishing campaign targeting Singapore residents disguised as SupportGoWhere government website.	13 December 2024
36	Event	Annual GSEC (Group-IB Security) Day & Capture-The-Flag (CTF) Battle Royale in Hanoi, Vietnam	18 December 2024

2.4 Publications

№	Publication	Link
1	Inferno Drainer: A Deep Dive into Crypto Wallet-Draining Malware	https://www.group-ib.com/blog/inferno-drainer/
2	Dead-end job: ResumeLooters infect websites in APAC through SQL injection and XSS attacks	https://www.group-ib.com/blog/resumelooters/
3	Face Off: Group-IB identifies first iOS trojan stealing facial recognition data	https://www.group-ib.com/blog/goldfactory-ios-trojan/
4	Extra credit: VietCredCare information stealer takes aim at Vietnamese businesses	https://www.group-ib.com/blog/vietcredcare-stealer/
5	In-depth analysis of Pegasus spyware and how to detect it on your mobile devices	https://www.group-ib.com/blog/pegasus-spyware/
6	Hunting Rituals #4: Threat hunting for execution via Windows Management Instrumentation	https://www.group-ib.com/blog/hunting-rituals-4/

7	Phishy Business: Unraveling LabHost's scam ecosystem	https://www.group-ib.com/blog/labhost-operation/
8	GoldPickaxe exposed: How Group-IB analyzed the face-stealing iOS Trojan and how to do it yourself	https://www.group-ib.com/blog/goldpickaxe-ios-trojan/
9	Boolka Unveiled: From web attacks to modular malware	https://www.group-ib.com/blog/boolka/
10	Craxs Rat, the master tool behind fake app scams and banking fraud	https://www.group-ib.com/blog/craxs-rat-malware/
11	Eldorado Ransomware: The New Golden Empire of Cybercrime?	https://www.group-ib.com/blog/eldorado-ransomware/
12	Patch or Peril: A Veeam vulnerability incident	https://www.group-ib.com/blog/estate-ransomware/
13	Qilin Revisited: Diving into the techniques and procedures of the recent Qilin Ransomware Attacks	https://www.group-ib.com/blog/qilin-revisited/
14	GXC Team Unmasked: The cybercriminal group targeting Spanish bank users with AI-powered phishing tools and Android malware	https://www.group-ib.com/blog/gxc-team-unmasked/
15	Beware CraxsRAT: Android Remote Access malware strikes in Malaysia	https://www.group-ib.com/blog/craxs-rat-malaysia/
16	Under Siege: The threat of compromised Mobile Device Management credentials and its implications for organizational security	https://www.group-ib.com/blog/compromised-mdm-credentials/
17	Deciphering the Brain Cipher Ransomware	https://www.group-ib.com/blog/brain-cipher-ransomware/
18	Hiding in plain sight: Techniques and defenses against `/proc` filesystem manipulation in Linux	https://www.group-ib.com/blog/linux-pro-manipulation/
19	RansomHub ransomware-as-a-service	https://www.group-ib.com/blog/ransomhub-raas/
20	APT Lazarus: Eager Crypto Beavers, Video calls and Games	https://www.group-ib.com/blog/apt-lazarus-python-scripts/
21	The Duality of the Pluggable Authentication Module (PAM)	https://www.group-ib.com/blog/pluggable-authentication-module/
22	Ajina attacks Central Asia: Story of an Uzbek Android Pandemic	https://www.group-ib.com/blog/ajina-malware/
23	Storm clouds on the horizon: Resurgence of TeamTNT?	https://www.group-ib.com/blog/teamtnt/

24	Inside the Dragon: DragonForce Ransomware Group	https://www.group-ib.com/blog/dragonforce-ransomware/
25	Pig Butchering Alert: Fraudulent Trading App targeted iOS and Android users	https://www.group-ib.com/blog/pig-butchering/
26	Unveiling USB Artifacts: A Comparative Analysis	https://www.group-ib.com/blog/unveiling-usb-artifacts/
27	Encrypted Symphony: Infiltrating the Cicada3301 Ransomware-as-a-Service Group	https://www.group-ib.com/blog/cicada3301/
28	Woodn't You Believe It? The Rise of Fake Wood Scams	https://www.group-ib.com/blog/fake-wood-scams/
29	Delivery Deception: Escalating cybercriminal tactics in the Balkan region	https://www.group-ib.com/blog/cybercriminal-tactics-in-the-balkan-region/
30	Stealthy Attributes of Lazarus APT Group: Evading Detection with Extended Attributes	https://www.group-ib.com/blog/stealthy-attributes-of-apt-lazarus/
31	Tracing the Path of VietCredCare and DuckTail: Vietnamese dark market of infostealers' data	https://www.group-ib.com/blog/tracing-the-path-of-vietcredcare-and-ducktail/
32	Shady Bets: How to Protect Yourself from Gambling Fraud Online	https://www.group-ib.com/blog/shady-bets/
33	Deepfake Fraud: How AI is Bypassing Biometric Security in Financial Institutions	https://www.group-ib.com/blog/deepfake-fraud/
34	Trust Hijacked: The Subtle Art of Phishing Through Familiar Facades	https://www.group-ib.com/blog/trust-hijacked/

3. Collaboration with APCERT members/partners

№	Activity	Description	Date
1	Partnership	Group-IB enhances partnership with INTERPOL with Signing Ceremony in Singapore	23 February 2024
2	Partnership	Group-IB joins the Cyber Security Action Task Force (CSATF) led by the Hong Kong Police Force (HKPF)	29 February 2024
3	Partnership	Memorandum of Understanding (MOU) Signing Ceremony with HELP University at Singapore HQ	19 March 2024
4	Partnership	Memorandum of Understanding (MOU) with CyberSecurity Malaysia (CSM)	7 August 2024

5	Partnership	Memorandum of Understanding (MOU) with I.T. Protective Security Services, the commercial arm and information technology subsidiary of Cybersecurity Brunei (CSB)	26 September 2024
6	Collaboration	Participation at Philippine CERT-CSIRT Conference	4 November 2024
7	Partnership	Group-IB partners HELP University, BIMP-EAGA Business Council (BEBC) and BIMP-EAGA ICT CEO Forum (BEICF)	14 November 2024

FIRST

Forum of Incident Response and Security Teams

1. About the Organization

FIRST brings together Internet security teams and experts from across the world, to share knowledge and insights, ensuring a safer Internet for all. Founded in 1990, FIRST consists of security practitioners from over 700 corporations, government bodies, universities and other institutions, representing over 100 countries in the Americas, Asia, Europe, Africa, and Oceania.

FIRST gives the global incident response community a place to build trust and work together. It also provides valuable opportunities to build capability, such as:

- technical colloquia for security experts,
- hands-on classes,
- annual incident response conference,
- publications and web services,
- special interest groups, and
- community and capacity building.

2. Activities and Operations in 2024

- The FIRST Annual Conference 2024 was hosted in Fukuoka, Japan from 9 to 14 June.
- FIRST also hosted the FIRST Cyber Threat Intelligence Conference, CVE/FIRST VulnCon 2024, four Regional Symposium, six Technical Colloquim, and numerous training workshops in 2024
- FIRST membership has grown to 773 teams across 111 economies and 183 liaison members

3. Collaboration with APCERT members/partners

FIRST has been an APCERT Strategic Partner since 2021 and the two organizations have a strong shared membership leading to mutual engagement across our events and activities.

The following are some select recent collaborations with APCERT members and partners.

- In November 2024, **TWCERT/CC** graciously hosted the APCERT-FIRST Asia-Pacific Regional Symposium alongside the APCERT Annual General Meeting.
- As part of the Asia-Pacific Regional Symposium, FIRST organized the APAC Incident Response Fellowship Program. The program welcomed nine participants from Kiribati, Indonesia, Thailand, Solomon Islands, Philippines, Malaysia, Bhutan, Mongolia, and Papua New Guinea. This program included introductions to community mentors, with volunteers from **TWCERT/CC**, **KrCERT/CC**, **JPCERT/CC**, and **APNIC** working with the fellows. The fellowship was generously supported by the APNIC Foundation.
- In September 2024, **APNIC** hosted a FIRST Technical Colloquium (TC) as part of the APNIC 58 Conference in Wellington, New Zealand. The event was also co-located with the Pacific Internet Governance Forum (PacIGF) and various other events.
- The June 2024 FIRST Annual Conference was organized in close collaboration with **JPCERT/CC** and other partners in the region. More information on the conference is available at: https://www.first.org/conference/2024/
- FIRST has engaged with **CERT-PH**, **CERT Tonga**, and **CERT VU**, as participants in the FIRST Suguru Yamaguchi Fellowship Program in 2024.

FSI-CERT

Financial Security Institute – Computer Emergency Response Team - Korea

1. About FSI-CERT

1.1 Introduction

FSI-CERT is an organization dedicated to cyber security in the financial sector. The institute is a non-profit corporation funded by member financial companies.
FSI-CERT operates a cybersecurity incident response system in the financial sector including building an information-sharing system for cybersecurity incidents, notifying intrusion attempts, analyzing the cause of incidents, and providing prompt response and prevention measures.
When security incidents occur, FSI-CERT deploys digital forensics and malware analysis to identify the cause of the incident, and provides initial measures to limit damage and avoid any recurrences of such incidents.

1.2 History

FSI-CERT was founded on April 2015 to specialize as a cyber security organization for the financial sector. Its mission is to create a safe and reliable environment to enhance the convenience of customers and the development of the financial industry.

1.3 Organization

FSI-CERT has more than 300 employees working in 4 groups(13 departments), conducting cyber security monitoring in the financial sector, cyber attack response, and vulnerability analysis/assessment.

1.4 Contact Information

Tel: +82-2-3495-9410
Fax: +82-2-3495-9399
Email: cert@fsec.or.kr
Website: https://www.fsec.or.kr/en

2. Activities & Operations

2.1 Summary of major activities

2.1.1 Operate a financial threat response intelligence platform

FSI-CERT has completed the development of a financial sector cyber incident response intelligence platform, which compiles and analyzes cases of cyber incidents that occurred in the financial sector in October 2024. The platform systematically stores and manages cyber incident and malware reports analyzed by FSI-CERT itself, and visually presents the relationships between the indicators of compromise.

2.1.2 Monitoring and Response to dark web threats

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

2.1.3 Bug-bounty program for the financial sector

FSI-CERT launched a continuous bug bounty program to discover unprecedented security vulnerabilities and strengthen preemptive prevention activities against cyber infringement threats. The bug bounty program was broadened to include widely used software in the financial sector, as well as IT and information security solutions.

2.1.4 Operation of a next-generation financial ISAC system

FSI-CERT has established and operated a next-generation financial security monitoring system that leads security monitoring technology by expanding the use of artificial intelligence (AI), producing and providing threat intelligence for security monitoring, and introducing a new security monitoring model (ASM*).

* A process and technology that continuously monitors and responds to all potential attack pathways targeting the organization.

2.1.5 Information sharing of voice phishing threats

FSI-CERT has established and operated a financial sector-wide voice phishing fraud information sharing system to support the prevention and response to the growing threat of voice phishing. This system enables the rapid sharing and dissemination of related information within the financial sector through MoUs and API integration with relevant law

enforcement, communication, and security agencies.

2.1.6 Autonomous Incident Response Training Platform

FSI-CERT has established a practical incident response training platform (CATS) to strengthen the incident response capabilities of financial companies and ensure the stable establishment of autonomous security systems. Using the platform, financial companies can conduct their own training for server hacking attacks and malicious email attacks, with official services starting in 2025.

2.2 Incident Response

2.2.1 Incident analysis and response

When cyber attacks occur in financial companies, FSI-CERT gathers digital evidence and utilizes digital forensics on scene to analyze the cause of the incident. FSI-CERT also establishes measures to prevent damage propagation and enhance financial companies' cyber threat response capabilities by conducting incident prevention digital forensic analysis on PCs that are likely to be targeted.

Figure 1. Incident Response Process

2.2.2 Malware Response and Sharing

FSI-CERT shared information on cyber threats including IoCs(Indicator of Compromise) such as distribution sites, hash values, and C&C servers by analyzing cyber attack attempts on financial companies and also malicious codes that are spread for financial purposes.

Furthermore, FSI-CERT provided correlation analysis information by systematically managing a multitude of collected/analyzed results of malicious codes.

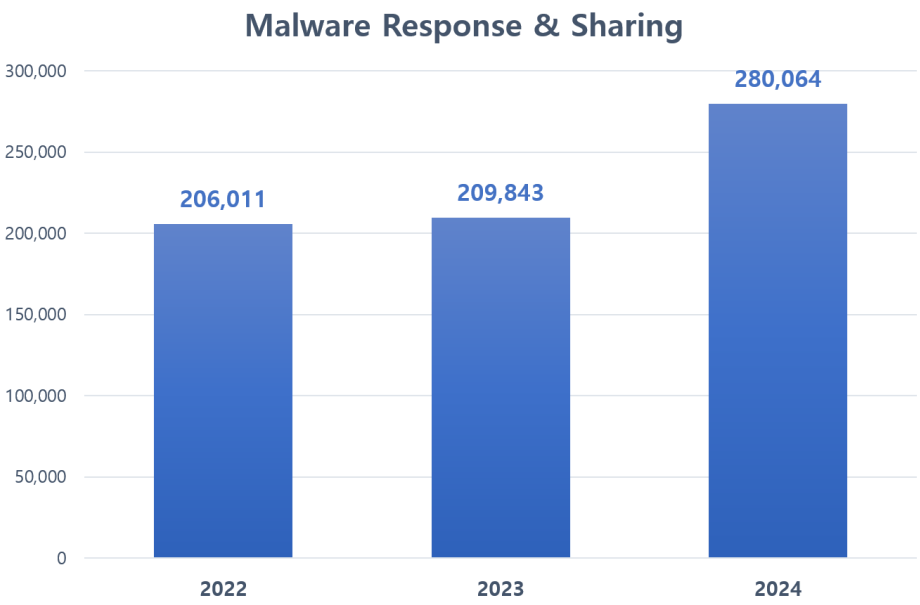


Figure 2. Total Malware Response and Sharing Cases

2.2.3 Simulation training on cyber security incidents

FSI-CERT conducted response training for various electronic cyber incidents, such as DDoS attacks, server hacking, and malicious email attacks, to assess the incident response systems of financial companies and contribute to improving security awareness.

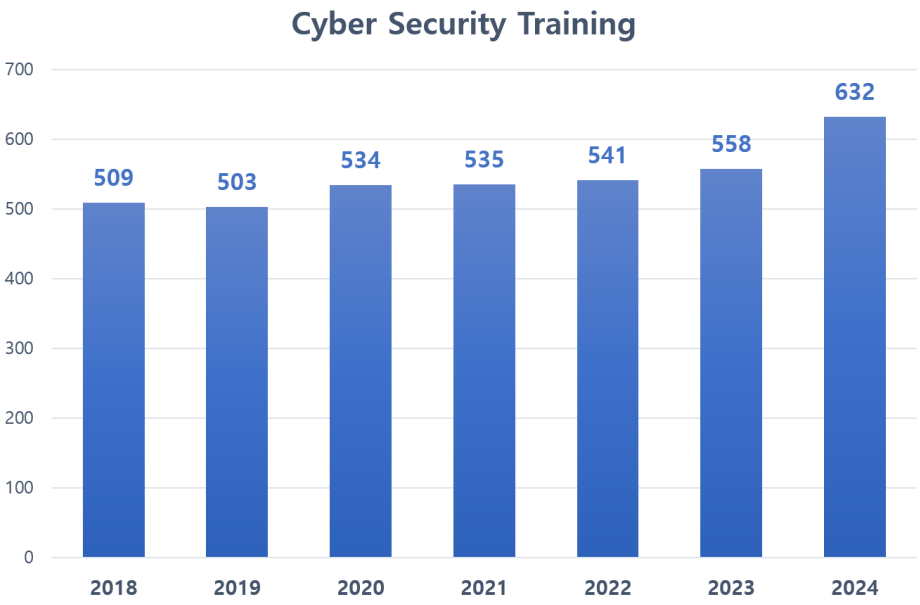


Figure 3. Total Cyber Security Training Sessions

2.2.4 Operation of DDoS Attack Emergency Response Center

When large-scale DDoS attacks to which financial companies cannot respond on their own occur, FSI-CERT operates the DDoS attack emergency response center which filters DDoS attacks and sends back only valid network traffic to financial companies. It is achieved by utilizing FSI CERT's own shelter and cloud-based DDoS cyber shelters built domestically and abroad.

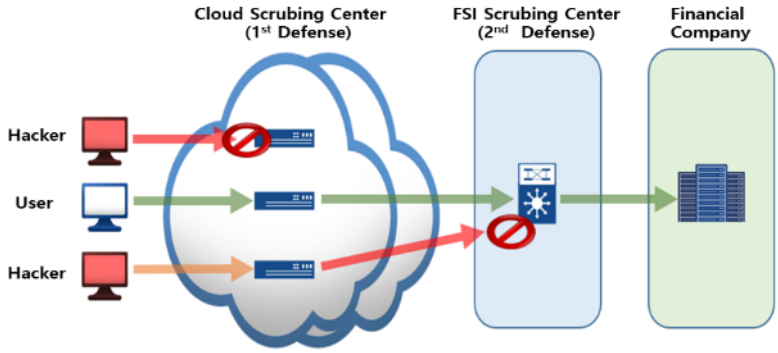


Figure 4. DDoS Attack Response Process

2.3 Operation of an integrated security monitoring system

FSI-CERT operates a next-generation integrated security monitoring system based on AI, big data, and cloud technology. Using the information accumulated through the threat intelligence-based system completed in 2023, it plans to enhance monitoring technologies such as ASM (Attack Surface Management) and CTI (Cyber Threat Intelligence) by 2025.

**Increased number of responses compared to 2022, due to introduction of next-generation financial security control system*

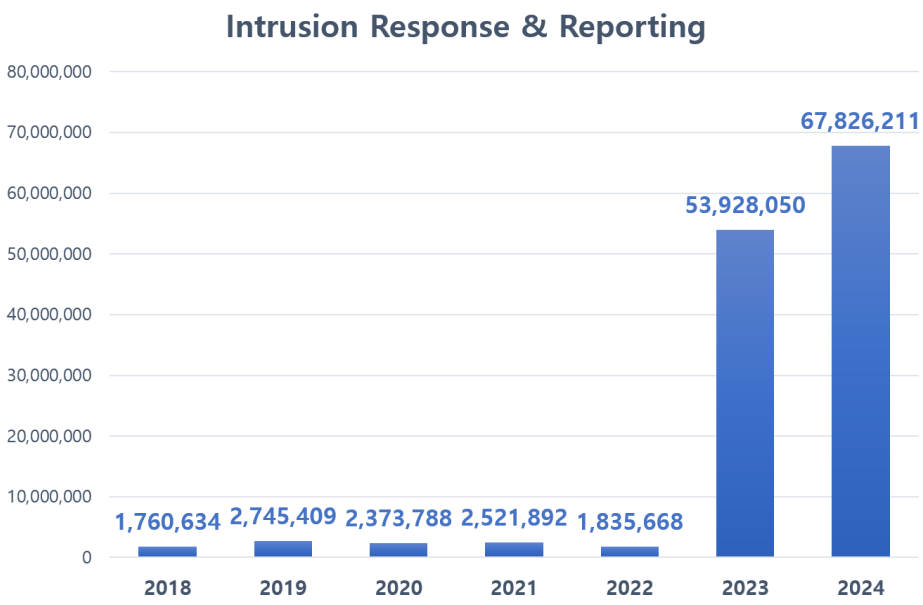


Figure 5. Total Intrusion Response and Reporting Cases

FSI-CERT protects financial assets from voice phishing by detecting phishing or pharming sites through a self-developed system and by blocking the spread of malicious applications through an information sharing system across the financial sector.

In addition, by signing MOU with major specialized organizations (police, telecommunication companies, security companies) on voice phishing response, we strengthened our cooperation system to eradicate electronic financial fraud such as voice phishing.

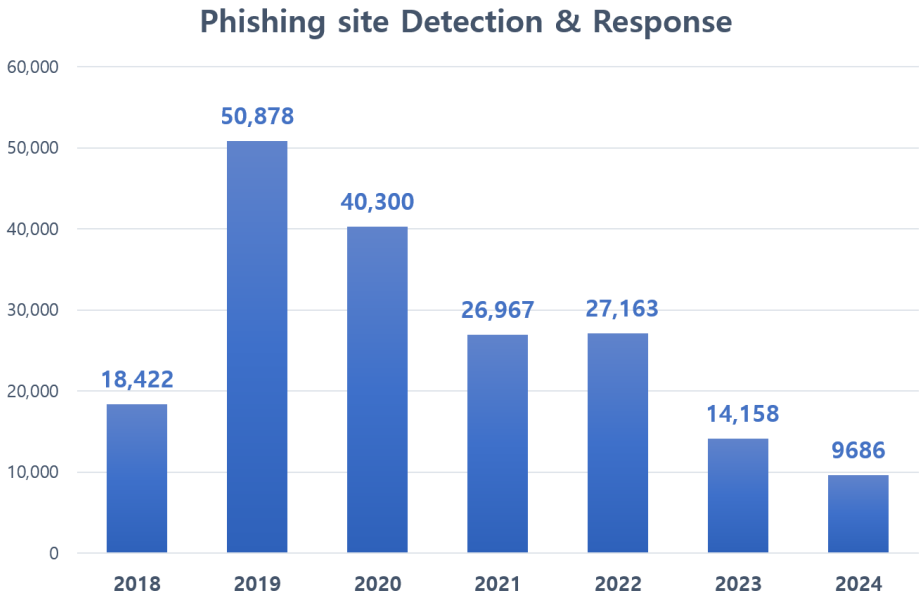


Figure 6. Total Phishing Site Detection and Response

2.4 Vulnerability analysis and assessment

FSI-CERT provides comprehensive inspections and vulnerability checks on digital financial infrastructure (ex. public webpages) of financial companies to find potential vulnerabilities and take necessary measures.
In order to support the autonomous security system so that financial companies can self-inspect their vulnerabilities, technical support and training such as upgrading evaluation methods and inspection tools are provided.

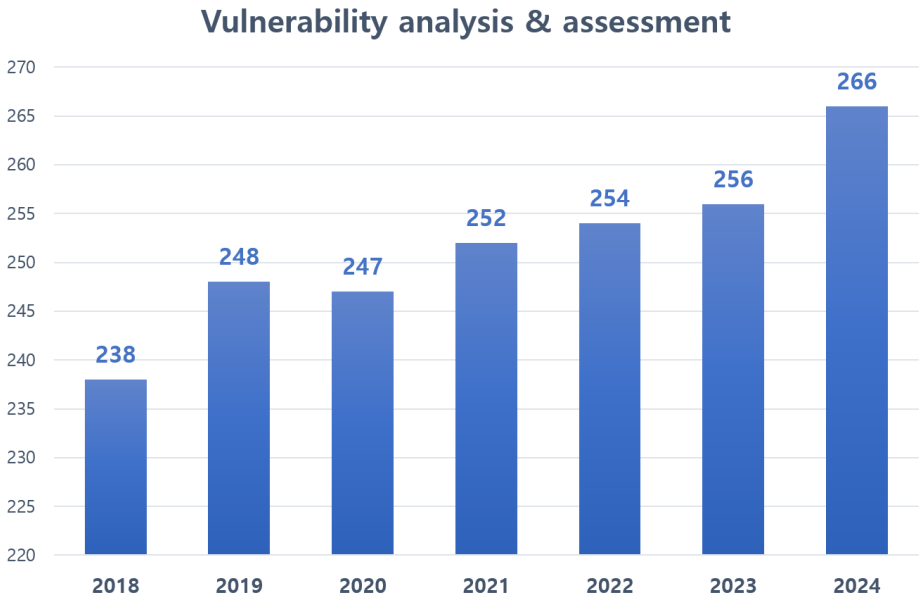
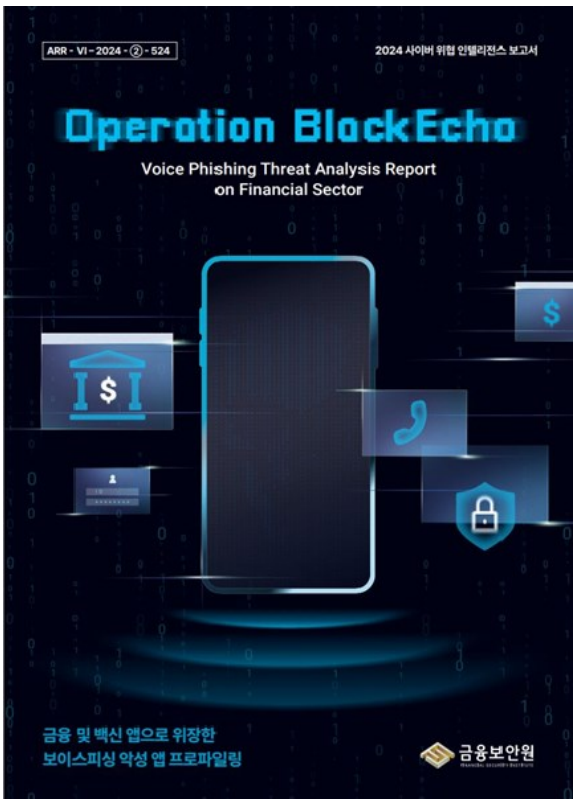


Figure 7. Total Vulnerability Analyses and Assessments

Areas of Inspection: information security management systems, servers, database, network, network equipment, information security system equipment, web applications, mobile applications, HTS(Home Trading System) applications, penetration testing etc.

3. Publications

FSI-CERT analyzes various cyber threat and uploads monthly financial security trend reports on the website. Also, FSI-CERT selects research topics and publishes cyber threat intelligence reports every year.



Operation BlackEcho : Vocie Phising Threat Analysis Report on Financial Sector (2024.12.)

A new criminal organization distributing malicious apps under the pretext of low-interest loan applications and checking card issuance details has been identified. The organization directly distributes the first-stage malicious app to victims via social media and other platforms. This malicious app then installs a second-stage malicious app disguised as a mobile antivirus, which carries out voice phishing, remote control, and data theft attacks. The Financial Security Institute conducted an in-depth analysis of the entire attack process and named the operation “BlackEcho.”

4. Organized/Hosted Events

- Voice Phishing Response Meeting
- New Technology in Financial Security Seminar
- FISCON 2023 (Financial Information Security Conference)
- Financial Security Academy 2023
- Financial Sector Bug Bounty program

- FIESTA 2023 (Financial Institutes' Event on Security Threat Analysis)
- Financial Sector Threat Identification Working Group Meeting
- Financial Sector Malware Working-level Meeting
- Financial Sector Software Supply Chain Security Enhancement Strategy Seminar

5. Conferences and Presentations

BlactHat Asia 2024 (Singapore, April)

- Operation PoisonedApple: Tracing Credit Card Information Theft to Payment Fraud

BlactHat Europe 2024 (London, December)

- Operation Midas – Tracking Fraudulent Financial Program Organizaions

6. Collaboration with APCERT

At the 2020 APCERT online training session, FSI-CERT presented on the topic "ATM Cyber Attack." FSI-CERT looks forward to participating continuously in various seminars of APCERT to share research and information of the financial security sector.

7. Conclusion

Cyber security threats such as the dark web, cloud security threats, COVID-19, and cyber warfare are increasing day by day. Accordingly, FSI-CERT will continue to enhance cyber security systems—such as the financial ISAC(Information Sharing and Analysis Center), digital forensics, malware analysis, etc.—to combat such increasingly developing security threats. In addition, FSI-CERT will follow by its mission of providing a safe environment for the financial industry by incorporating new technologies (ex. big data, AI, etc.) into cyber security.

OIC-CERT

Organisation of The Islamic Cooperation – Computer Emergency Response Teams

1. About the Organization

1.1 Introduction

The Organisation of the Islamic Cooperation - Computer Emergency Response Team (OIC-CERT) was established through the Organization of the Islamic Cooperation (OIC) Resolution No 3/35-INF Collaboration of Computer Emergency Response Team (CERT) Among the OIC Member Countries. It was passed during the 35th Session of the Council of Foreign Ministers of the OIC in Kampala Uganda on 18-20 June 2008.

In 2009 through the Resolution No 2/36-INF Granting the Organization of the Islamic Cooperation –Computer Emergency Response Team an Affiliated Institution Status, the OIC-CERT became an affiliate institution of the OIC during the 36th Session of the Council of Foreign Ministers of the OIC Meeting in Damascus, Syrian Arab Republic on 23-25 May 2009.

Vision

Envisioning the OIC-CERT to be a leading cybersecurity platform to make global cyber space safe.

Mission

A platform to develop cybersecurity capabilities to mitigate cyber threats by leveraging global collaboration.

1.2 Membership

As of Dec 2024, the OIC-CERT has a network and strategic collaboration with 67 members from 30 OIC countries. This comprised of 27 Full Members & 22 General Members as well as in support from 6 Commercial Members, 4 Professional Members, 3 Fellow Member, 1 Affiliate Member, and 1 Honorary Member.

The membership categories are as follows:

1.2.1 Full Members

These are CERTs, Computer Security Incident Response Teams (CSIRTs) or similar entities that are located and/ or have

the primary function within the jurisdiction of the OIC CERT member countries. They are wholly or partly owned by the government with the authority to represent the country's interest.

1.2.2 General Members

These are other related government organizations, non-governmental organizations or academia that deal with cybersecurity matters. However, these parties do not have the authority to represent the country's interest.

1.2.3 Affiliate Members

These are not-for-profit organizations that deal with cybersecurity matters from non-OIC-CERT member countries.

1.2.4 Commercial Members

These are industrial or business organizations that deal with cybersecurity matters from the OIC and non-OIC member countries.

1.2.5 Professional Members

Individual professionals, mainly in the cybersecurity domain, and not restricted to the OIC community.

1.2.6 Fellow Members

These are individuals who are considered as co-founders of the OIC-CERT and have actively represented their organization as an OIC-CERT member for a minimum period of 5 years.

1.2.7 Honorary Members

Individuals or organizations who have demonstrated extraordinary contribution, support, and exemplary leadership to the OIC-CERT.

Details of the members can be found at www.oic-cert.org

2. Activities & Operations in 2024

2.1 OIC-CERT 11th General Meeting & 16th Annual Conference, Muscat, Oman

The OIC-CERT 11th General Meeting & 16th Annual Conference was held in Muscat, Oman from 27-31 October 2024 in conjunction of 12th Regional Cybersecurity Summit & the FIRST & ITU-ARCC Regional Symposium for Africa and Arab Regions with theme "Cybersecurity as an Enabler for Digital Economy".

2.2 Online Training

To raise awareness on cybersecurity within the OIC-CERT member states, 11 sessions of online training were conducted in 2024 as follows:

Date	Topic	Host
27 May	Webinar "Introducing A New Cybersecurity Awareness Training and Phishing Simulation Platform" (AZ)	AeCERT/ TDRA, UAE
28 May	OIC-CERT Technical Activity (Part 1): Development Of OIC-CERT Cyber Security Standard Operating Policies, Procedures and Best Practices (BN)	UAE
18 Jul	Webinar Serumpun ASEAN 2024 | AI Dalam Kehidupan Seharian (MY)	NCCA, Indonesia
28 Aug	OIC-CERT Technical Activity (Part 2): Production of ISMS Documentation L1 Workshop (ISMS Policy and Framework) (BN)	ICANN
25 Sept	OIC-CERT Technical Activity (Episode 3): Production of ISMS Documentation L2 (Management Systems Procedures) (BN)	AeCERT/ TDRA, UAE
23 Oct	Awareness Program: Webinar on Threat Information Sharing and Future Prediction on Critical Infrastructure Sector	CyberSecurity Malaysia
20 Nov	Security Evaluation Of IoT/Ot Devices	EG|CERT, Egypt
24 Dec	Cross-border CSIRT Collaboration on Critical Infrastructure Threat Information Sharing Simulation	AeCERT/ TDRA, UAE

2.3 Cyber Drills

As in previous years, the OIC-CERT organizes an international cyber drill for the members and partners (including APCERT members). In 2024, Oman National CERT and ITU-ARCC organized the drill with the theme "The Impact of Cybersecurity Threats on the Digital Economy" on 30-31 Oct 2024. The event was held in conjunction with the 12th Regional Cybersecurity Summit & the FIRST & ITU-ARCC Regional Symposium for Africa and Arab Regions. The objective of this drill is to measure the readiness of the participants in facing cyber-attacks. 35 countries participated in the drill.
The OIC-CERT members also participated in the APCERT Drill that was held on 29 Aug 2024.

2.4 OIC-CERT Journal of Cyber Security

The growth in cybersecurity research has encouraged the collaboration between the public sectors, academia, and industry practitioners. The OIC-CERT has a substantial pool of resources and expertise both from the academia and industry practitioners that can produce quality research papers in the field of cybersecurity and can be published as a journal contributing to the body of knowledge in cybersecurity. The OIC-CERT Journal of Cyber Security (JCS) is an

initiative under the OIC-CERT led by CyberSecurity Malaysia and the Technical University of Malaysia Melaka, Malaysia (UTeM). The OIC-CERT welcomed contributions from all parties, especially the APCERT members for this journal. More details at https://www.oic-cert.org/en/call-for-paper.html

2.5 Cyber Security Guidelines/Procedures

The OIC-CERT has published several cybersecurity guidelines in 2024. The guidelines are as follows:

- Cyber-Security Governance Framework
- The Essential Cybersecurity Controls
- Cyber Security Laws for OIC Members
- Malware Protection & Threat Intelligence Policy
- Cybersecurity Service providers Licensing Guidelines
- Cyber Crisis Management Playbook
- Cyber Resilience Assessment Tool

2.6 Awareness posters and presentations

UAE as Awareness pillar lead has published awareness posters as following topics:

- Cloud security
- Data privacy
- Data protection
- Generative AI
- Insider treat
- Internet of things
- Mobile security
- Multi-factor authentication
- social engineering
- Social media

2.7 OIC-CERT Working Group (WG) & Study Group (SG)

OIC-CERT has established a few working groups (WG) & study groups (SG) as follows:

WG/SG	Lead	Objective
5G Security	Huawei & Malaysia	Develop, update, and release OIC-CERT 5G Security Framework and iteratively adopt this framework to support OIC member states' telecom development of best practices, standards, and research
Cloud security	UAE, Egypt & Huawei	Develop, update, and release OIC-CERT Cloud Security Framework and adopt this framework to support OIC member states' telecom development of best practices, standards, and research
Blockchain	UAE & Brunei	Explore good practices of blockchain security based on national application practices
Supply Chain	Egypt, Oman & Huawei	Adopt a supply chain security standard and best practices to guide the members to return supply chain security issues to the essence of technology and management
AI	Egypt & Oman	To gain insights into and discuss the hot topic of AI security and effectively transfer knowledge
Anti Ransomware SG	Bangladesh & UAE	Develop anti-ransomware and anti-fraud capabilities and build related management requirements with best practices
Post Quantum Computing SG	Bangladesh & Egypt	Gain insights into and discuss the hot topic of Post Quantum Computing security and effectively transfer knowledge

3. Future plans

- OIC-CERT 17th Annual Conference, in conjunction with Arab Regional Summit in Morocco from 15-19 Sep 2025
- OIC-CERT Cyber Drill

Disclaimer on Publications

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

APCERT ANNUAL REPORT 2024

TLP:CLEAR

APCERT
Asia Pacific Computer Emergency Response Team