APCERT
Asia Pacific Computer Emergency Response Team

TLP:CLEAR

ANNUAL REPORT 2023

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 2023 was a time to emerge from the seemingly never-ending COVID-19 pandemic and start working freely within APCERT once again to achieve our vision - help to create a safe, clean, and reliable cyberspace. The SC members were finally able to convene for a face-to-face meeting. For the past four years in a row, we have successfully conducted our Annual General Meetings online to such an extent that we hardly even realized our meetings were exclusively virtual. Our prideful tradition, the APCERT annual Cyber Drill, was executed seamlessly, involving 24 CSIRTs from 21 economies, OIC-CERT, and Africa CERT. Additionally, we delivered a total of 4 training sessions, sharing our expertise in Honeynet analysis, 5G vulnerability case analysis, search engines, and machine learning pertaining to phishing domains. Apart from these, APCERT also participated in the Asia-Pacific Economic Cooperation Telecommunications and Information Working Group (APEC TEL WG) meeting, and the ASEAN CERT Incident Drill.

With cyber threats persisting in our constituencies, 2024 will witness an increase in face-to-face member engagement and the introduction of new collaborative tasks. The Coordinated Vulnerability Disclosure Working Group, established in 2023, along with upcoming working groups, will facilitate in-depth discussions on the challenges encountered by CSIRTs. Furthermore, we eagerly anticipate our in-person Annual General Meeting and Conference for the first time in five years, viewing it as an opportunity to rebuild trust with partners beyond our Operational Members. In addition, the Membership Working Group anticipates increased member engagement within APCERT, with outcomes acknowledged through Awards at the Annual General Meeting.

This year marks KrCERT/CC's first chairmanship period, and I would like to thank all of our members for providing KrCERT/CC with the opportunity to serve as chair and for their ongoing support. APCERT is not exclusive to any single nation. I firmly believe that it is only through our trust-based engagement that we can become the leading incident response community in the Asia Pacific region, fostering greater productivity and benefits for all.

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 cybersecurity experts in the Asia Pacific region to improve the region's awareness on malicious cyber activities and the collective abilities to detect, prevent and mitigate such activities through:

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

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

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

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 2023, 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 NZ	Computer Emergency Response Team New Zealand	New Zealand
CERT-PH	Philippines National Computer Emergency Response Team	Philippines
CERT Tonga	Tonga Computer Emergency Response Team	Tonga
CERT VU	Computer Emergency Response Team Vanuatu	Vanuatu
CNCERT/CC	National Computer network Emergency Response technical Team / Coordination Center of China	People's Republic of China
CyberSecurity Malaysia	CyberSecurity Malaysia	Malaysia
ETDA	Electronic Transactions Development Agency	Thailand
GovCERT.HK	Government Computer Emergency Response Team	Hong Kong, China

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

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

At the APCERT AGM 2023, 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	2022 - 2024	
CNCERT/CC	2022 - 2024	
CyberSecurity Malaysia	2023 - 2025	Deputy Chair
JPCERT/CC	2023 - 2025	Secretariat
KrCERT/CC	2022 - 2024	Chair
Sri Lanka CERT|CC	2023 - 2025	
TWNCERT	2022 - 2024	

Working Groups (WG)

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

Information Sharing WG (formed in 2011)

Objectives

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

Convener (1): CNCERT/CC

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

Membership WG (formed in 2011)

Objectives

- Promote collaboration and participation by all APCERT members and partners

- Establish the organizational basis to enhance the partnership with cross-regional partners
- Guide activities such as checking and monitoring for sustaining the health of the membership and partnership structure

Convener (1): KrCERT/CC

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

Policy, Procedure and Governance WG (formed in 2013)

Objectives

- Develop and maintain policies, procedures and governance structures that together makes up the APCERT Operational Framework. The WG will periodically review and advise the Steering Committee if changes are required ensuring APCERT remains fit-for-purpose to 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): TWNCERT

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

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): CyberSecurity Malaysia (until August 2023)

Members (12): ACSC, AusCERT, CERT-In, HKCERT, JPCERT/CC, KrCERT/CC, SingCERT, Sri Lanka CERT|CC, TechCERT, ThaiCERT, TWCERT/CC, TWNCERT

IoT Security WG (formed in 2017)

Objectives

- Identification of the threat landscape and security challenges in the IoT ecosystem
- Suggesting steps to address the security issues including vulnerabilities tailored for IoT
- Recommendations for securing the IoT ecosystem
- Developing incident response mechanisms/measures for responding to cyber physical security incidents impacting human life
- Discussions on existing security standards and gaps for IoT ecosystem and considerations for adoption
- Development of threat sharing platform and threat sharing mechanism

Convener (1): CERT-In

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

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

APCERT Website

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

APCERT Activity Report

International Activities and Engagements

International Conferences and Events

The APCERT has been dedicated to representing and promoting its activities in various international conferences and events. From January to December 2023, APCERT Teams have hosted, participated and/or contributed to the following events:

National CSIRT Meeting (2-3 June – Montreal, Canada)
APCERT teams attended the 18th Annual Technical Meeting for CSIRTs with National Responsibility (NatCSIRT 2023) and exchanged various activity updates as well as recent projects and research.

35th FIRST Annual Conference (4-9 June – Montreal, Canada)
https://www.first.org/conference/2023/
APCERT Teams attended the Annual FIRST Conference in Montreal, Canada, and shared valuable experience and expertise through various presentations.

APCERT Cyber Drill 2023 (16 August)
https://www.apcert.org/documents/pdf/APCERTDrill2023PressRelease.pdf
The APCERT Cyber Drill 2023, the 18th APCERT cyber exercise drill, was successfully conducted to test the response capabilities of the participating APCERT Teams. 24 CSIRTs from 21 economies of APCERT (Australia, Bangladesh, Brunei Darussalam, Bhutan, People's Republic of China, Chinese Taipei, Hong Kong, India, Indonesia, Japan, Republic of Korea, Malaysia, Myanmar, Mongolia, New Zealand, Philippines, Singapore, Sri Lanka, Thailand, Vanuatu, and Vietnam) participated in the drill. From the external parties, 11 CSIRTs from 11 economies of OIC-CERT and AfricaCERT participated.

APNIC 56 (7-14 September)
APCERT co-hosted sessions with APNIC and FIRST to enhance information sharing in various topics among the

conference attendees. One of the APCERT Operational Member teams present at the session. APCERT SC meeting was held on the margins of APNIC 56.

AP* Retreat (11 September)

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

APCERT Annual General Meeting (AGM) and Conference 2023 (8-9 November – Online)

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

- 8 November APCERT Annual General Meeting
- 9 November APCERT Closed Conference

ASEAN CERT Incident Drill (ACID) 2023 (19 October – Online)

ACID 2023, led and coordinated by SingCERT, entered its 17th iteration with participation including ASEAN CERTs and APCERT Teams. The drill was completed successfully, providing an opportunity for teams to improve their knowledge and skills on investigating and responding to a ransomware incident, which also involves a DDoS attack.

Other International Activities and Engagements

DotAsia

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

Forum of Incident Response and Security Teams (FIRST)

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

STOP. THINK. CONNECT (STC)

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

Asia Pacific Network Information Security Centre (APNIC)

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

Africa Computer Emergency Response Team (AfricaCERT)

The APCERT and AfricaCERT signed an MoU in 2019.

APCERT SC Meeting

From January to December 2023, the SC members held 5 teleconferences and 1 face-to-face meeting to discuss the APCERT operations and activities.

Date	Location
18 January	Teleconference
27 March	Teleconference
25 May	Teleconference
27 July	Teleconference
11 September	Face to face meeting
30 October	Teleconference

APCERT Training

The APCERT held five (5) training calls in 2023 to exchange technical expertise, information, and ideas.

Date	Title	Presenter
28 March	DNS Security and Threats for Incident Responders	ICANN
9 May	5G Vulnerability Analysis	KrCERT/CC
14 July	Cyberspace Search Engine – Overview and Applications	TWNCERT
11 October	Exploring Machine Learning on Phishy Domains	AusCERT

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 2023

1.1 Achievements & milestones

Throughout Financial Year 2022–23 (1 July 2022 – 30 June 2023), Australia was targeted by a range of actors who conducted persistent cyber operations that posed significant threats to Australia and continued to observe an increase in the speed with which malicious actors have researched and then pivoted to exploit publicly released vulnerabilities. The Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) is the Australian Government's technical authority on cyber security and below are some of our key achievements and milestones during Financial Year 2022–23.

What ASD's ACSC saw in Financial Year 2022–23

- Average cost of cybercrime per report up **14 per cent**.
- Nearly **94,000 cybercrime reports**. on average a report every 6 minutes.
- Answered over **33,000 calls** to the Australian Cyber Security Hotline, up 32 per cent and on average 90 calls per day

What ASD's ACSC did in Financial Year 2022–23

- Responded to over **1,100 cyber security incidents**.
- Notified **158 entities** of **ransomware activity** on their networks, compared to **148** last year, roughly a **7 per cent** increase.
- **Australian Protective Domain Name System** blocked **over 67 million** malicious domain requests, **up 176 per cent**.
- **Domain Takedown Service** blocked **over 127,000** attacks against Australian servers, **up 336 per cent**.
- **Cyber Threat Intelligence Sharing partners** grew by **688 per cent** to over **250 partners**.
- Published **64 alerts, advisories, incident and insight reports** on **cyber.gov.au** and the **Partnership Portal**.
- **ASD's Cyber Security Partnership Program** grew to around **110,000 partners**
- Led **20 cyber security exercises** involving over **75 organisations** to strengthen Australia's cyber resilience.

2. About CSIRT

2.1 Introduction

The Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) is the Australian Government's technical authority on cyber security. ASD brings together capabilities to improve Australia's national cyber resilience and its ACSC services include:

- 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 ASD's Cyber Security Partnership Program.

2.2 Resources

ASD's 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

The 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

3.2 Incident handling reports

ASD's 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 ACSC's 24/7 hotline 1300 CYBER1. This aggregation of cyber security incident data enables ASD to inform threat mitigation advice with the latest trends and threats posed by malicious cyber actors. Any degradation in the quantity or quality of information reported to ASD harms cyber security outcomes. Information reported to ASD is anonymised prior to it being communicated to the community.

ASD categorises each incident it responds to on a scale of Category 1 (C1), the most severe, to Category 6 (C6), the least severe. Incidents are categorised on severity of effect, extent of compromise, and significance of the organisation.

	Member(s) of the public	Small organisation(s) Sole traders	Medium-sized organisation(s) Schools Local government	State government Academia/R&D Large organisation(s) Supply chain	Federal government Government shared services Regulated critical infrastructure	National security Systems of National Significance
Sustained disruption of essential systems and associated services	C6	C5	C4	C3	C1	C1
Extensive compromise	C6	C6 15	C4 23	C3 17	C2 3	C1
Isolated compromise	C6	C5 38	C5 57	C3 63	C3 35	C2 2
Coordinated low-level malicious attack	C6	C6 7	C5 14	C4 32	C3 46	C3 1
Low-level malicious attack	C6 1	C6 73	C5 72	C4 88	C4 90	C3 9
Unsuccessful low-level malicious attack	C6	C6 19	C6 21	C6 73	C6 292	C6 43

Table 1: Cyber security incidents by severity category for FY 2022–23 (total 1,134)

3.1 Publications

In Financial Year 2022–23, 64 alerts, advisories, incident and insight reports were released to cyber.gov.au and the Partnership Portal to support government, large organisations, small and medium businesses, individuals, and families to improve their cyber security posture.

3.2 New services

The ASD's ACSC continues to provide new high-quality cyber security services and advice to all Australians to make Australia the most secure place to connect online. Over the reporting period this included:

- Guidance to avoid risks related to social media and messaging applications;
- An online tool (Have you been Hacked?) to help people who may be a victim of a cyber attack;
- A self-assessment tool for critical infrastructure operators to assess their level of cyber security maturity and

preparedness;

- An Exercise in a Box to help small to medium enterprises understand the cyber risks they are currently exposes to and what they can to mitigate them;
- A series of guides to help business secure their cloud environment;
- Supporting, with the Office of the Australian Information Commission, Privacy Awareness Week; and
- A revamped Small Business Cyber Security Guide.

4. Events organized / hosted

4.1 Drills & exercises

ASD's ACSC continued to facilitate exercises through our National Exercise Program (NEP). This program helps critical infrastructure and government organisations validate and strengthen Australia's nationwide cyber security arrangements. The NEP delivered 20 exercises for government and critical infrastructure organisations during 2022-23.

4.2 Conferences and seminars

Through ASD's Cyber Security Partnership Program, Australian entities can engage with the ASD to develop collective understanding, experience, skills, and capability to lift cyber resilience. Over 250 events with at least 3,100 participants were held at ASD state offices located throughout Australia.

5. International Collaboration

5.1 International partnerships and agreements

ASD's 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.
ASD's 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

ASD's ACSC supported the delivery of 'Cyber Bootcamps' to Association of Southeast Asian Nations (ASEAN) countries, in collaboration with the Australian National University. As part of each Cyber Bootcamp, the ACSC boosted regional

cyber resilience by sharing insights into Australia's cyber security threat landscape and whole-of-government arrangements.

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

5.2.1 Drills & exercises

ASD's 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, ASD's 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

ASD's 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 Future projects

Implementation of the Australian Government's $9.9 billion REDSPICE (**R**esilience, **E**ffects, **D**efence, **Sp**ace, **I**ntelligence, **C**yber, **E**nablers) investment over the next decade will be used to enhance the capabilities of ASD's ACSC to further protect Australians from cyber adversaries.

Commencing on 1 July 2022, ASD scaled existing services and introduced new intelligence and cyber capabilities to enhance Australia's cyber defences.

To help achieve this, in Financial Year 2022-23, ASD opened new facilities in Brisbane and Melbourne, and received over 26,000 job applications across Canberra, Melbourne, Brisbane and Perth.

7. Conclusion

In Financial Year 2022-23, ASD's ACSC saw cyber threats continue to grow as Australia became more interconnected and malicious cyber actors become more sophisticated. Globally, cyber actors increasingly targeted critical infrastructure networks.

Australia's region, our region, the Indo-Pacific, is also now seeing growing competition on multiple levels – economic, military, strategic and diplomatic – framed by competing values and narratives.

In this context, Australian governments, critical infrastructure, businesses, and households continue to be the target of malicious cyber actors.

ASD's ACSC offers advice on actions individuals and organisations can take to improve cyber resilience. This advice is informed by a global network of international partners, including APCERT. Ultimately cyber security is a team sport where collaboration and cooperation is the norm rather than the exception.

AusCERT

Australian Computer Emergency Response Team

1. Highlights of 2023

AUSCERT has always found it paramount to contribute back to the cybersecurity community in one form or another. Human assets are a pinnacle resource in operations and development.

1.1 Achievements & milestones

1.1.1 Domain Phishing Construct detection through Machine Learning.

AUSCERT has in the year of 2023 designed, created, tested, and implemented a Machine Learning model to be able to assist in determining if a domain name is constructed in a manner that is probably be used for phishing. This effort has been a culmination of a year's work in proving that the model placed in production is performing in a manner that is expected. This accomplishment and retainment of skills in design and rollout of models for a given task has been the basis of ongoing collaboration projects in the late part of 2023 and is envisaged to continue throughout 2024.

1.1.2 Contribution to APCERT

Every year AUSCERT contributes back to the APCERT community in being part of several working groups. The 2023 saw AUSCRET contribute to effort in the following working groups. APCERT Drill WG, APCERT Membership WG, the APCERT PPG-WG……

1.1.3 Tertiary Education Capstone Projects

In 2023, AUSCERT has enabled two more final year Cyber Security Masters student in their capstone projects. As always, the great results from the projects of the capstone students are then assimilated in provided service that to increase AUSCERT's capacity and capability in early warning notifications.

2. About CSIRT

2.1 Introduction

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

2.2 Establishment

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

2.3 Resources

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

2.4 Constituency

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

region. All Australian universities and the majority of New Zealand universities are members of AusCERT and there is a strong relationship with the Council of Australian University Directors of Information Technology (CAUDIT). AUSCERT participates in the Australian government's IT Security Experts' Advisory Group (ITSEAG).

3. Activities & Operations

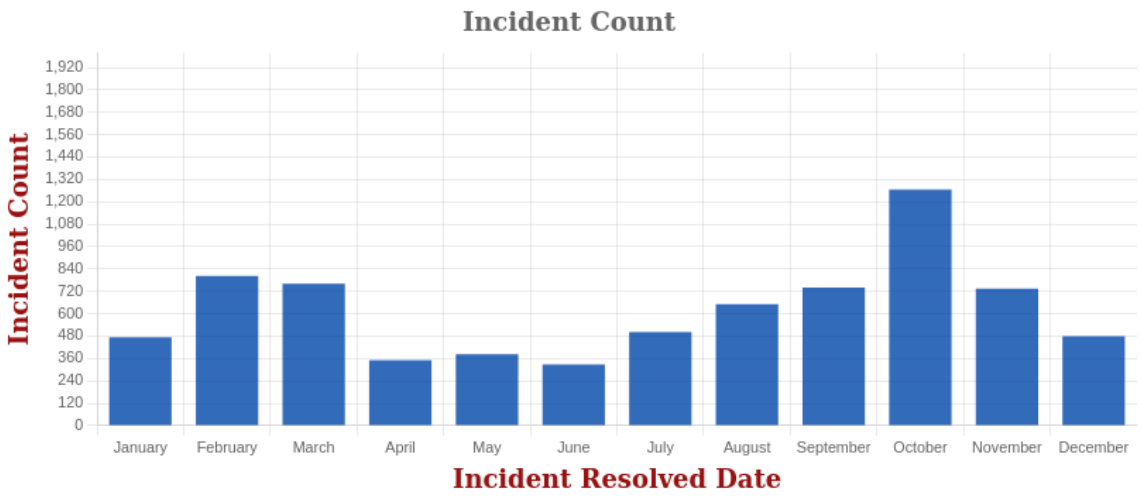
3.1 Scope and definitions

AUSCERT monitors and evaluates global cyber network threats and vulnerabilities and remains on-call for members after hours. 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:

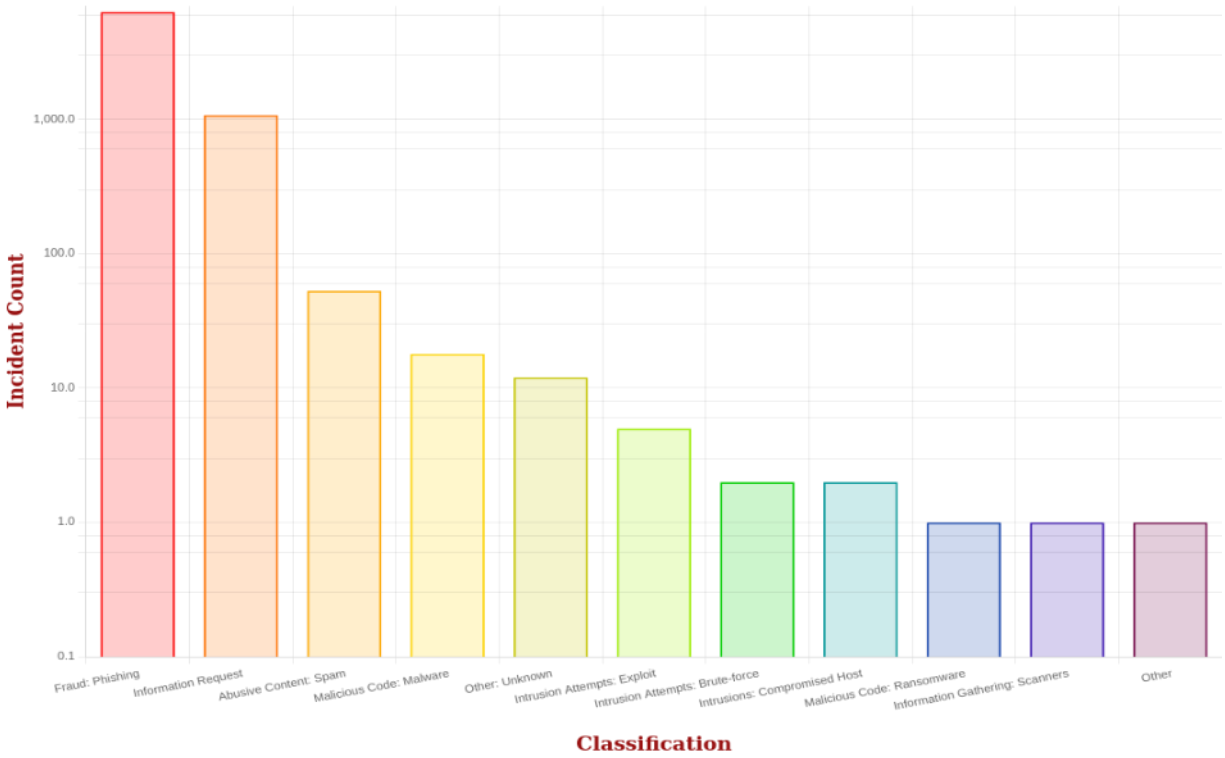
- Incident Management [3.2], https://www.auscert.org.au/services/incident-management-service/
- Early Warning Service https://www.auscert.org.au/services/early-warning-service/
- Malicious URL Feed https://www.auscert.org.au/services/malicious-url-feed/
- Security Bulletin Service [3.3] https://www.auscert.org.au/services/security-bulletins/
- 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 Management

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

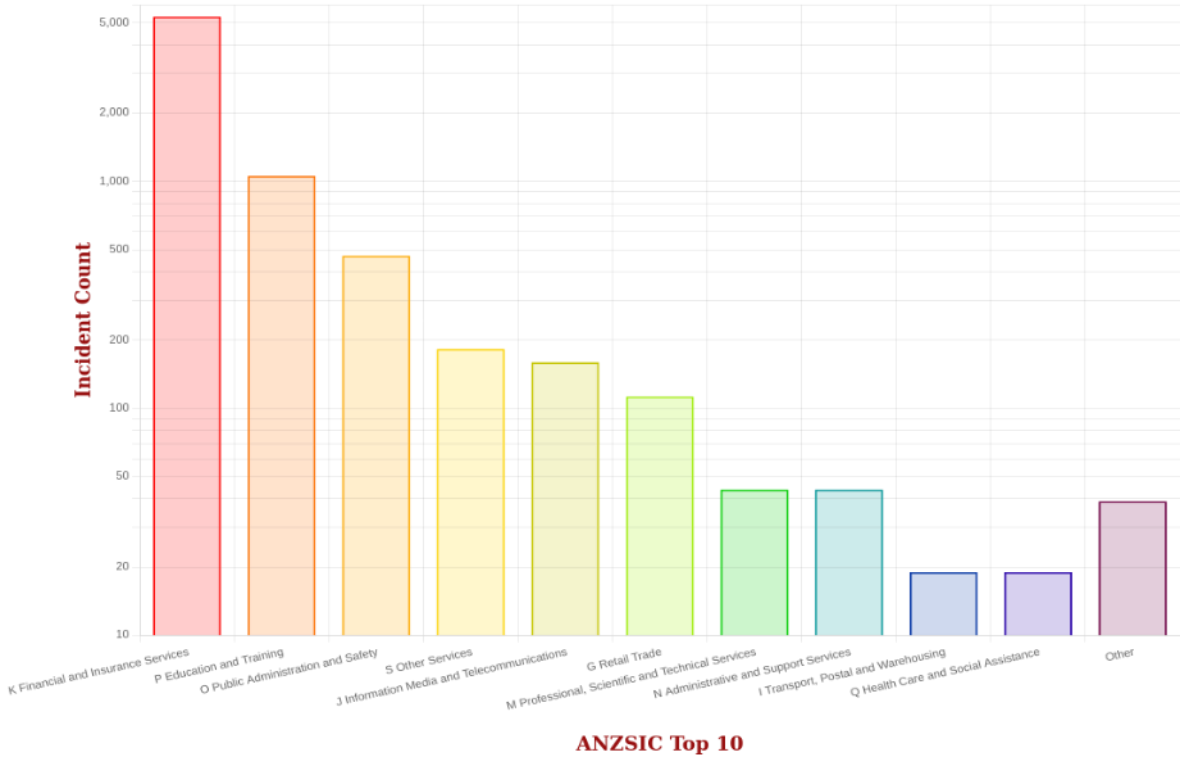


The diagram above shows the statistics of incidents that required handling for the calendar year of 2023. Overall, AUSCERT serviced seven thousand, four hundred and seventy-four (7474) tickets which resulted in just under 30 tickets per business day of operation.



Incidents 2023 by Classification

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

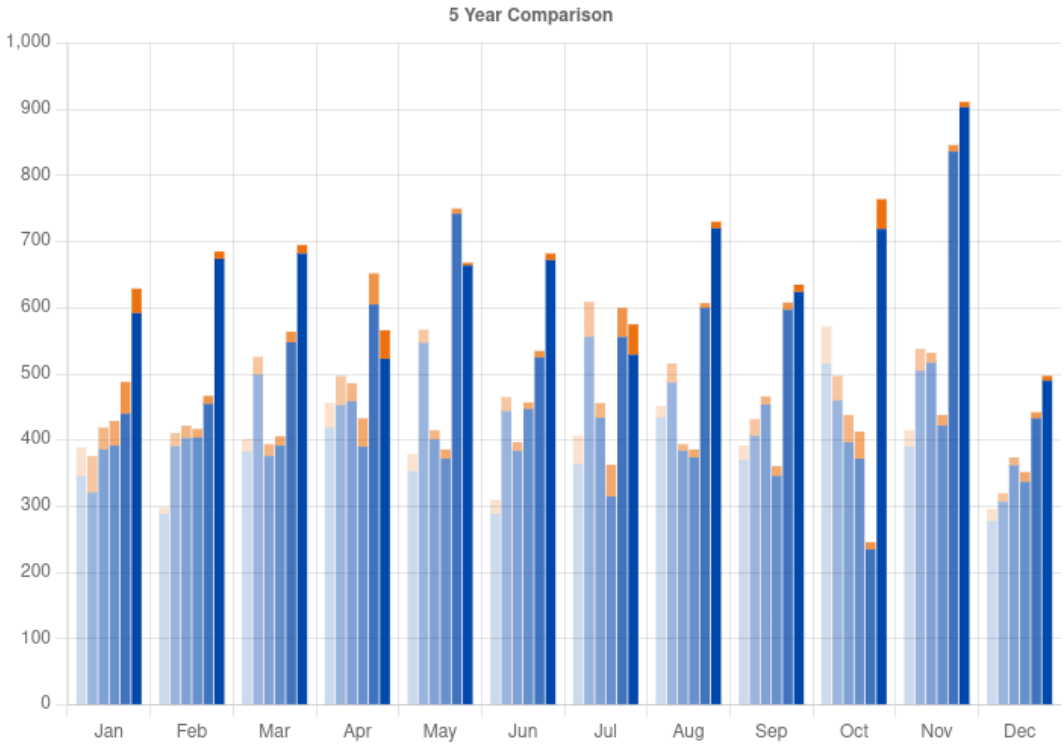


Incidents 2023 by Industry

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 and publishes a portion of them to its public website.
Bulletins are published in a standardised format with a consistent approach to classifications of vulnerabilities, impacts and affected operating systems.
In 2023, 7154 External Security Bulletins (ESBs) and 245 AusCERT Security Bulletins (ASBs) were published.



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

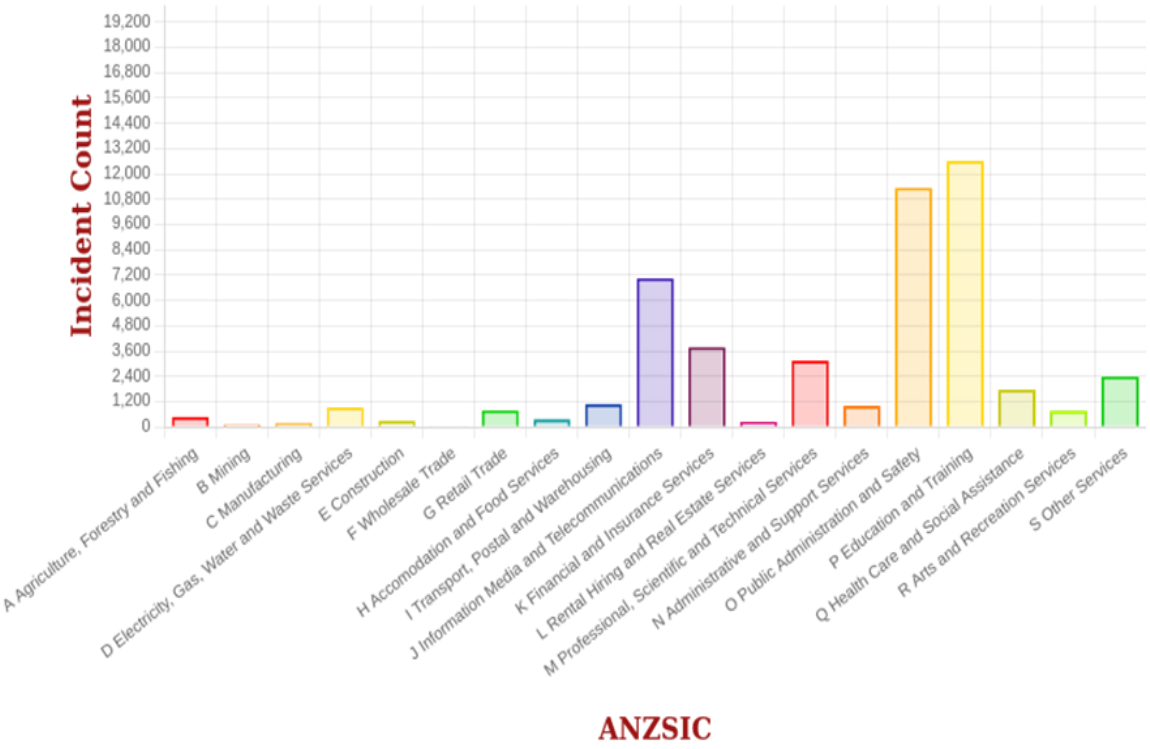
3.4 Member Security Incident Notifications

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

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

MSIN 2023 Mailout by Month

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



MSIN 2023 Mailout by Industry

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

Critical MSIN 2023 Mailout

3.5 Publications

3.5.1 ADIR

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

3.5.2 Week in Review

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

3.5.3 Social Media

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

3.5.4 Newsletter

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

3.5.5 Blog Post

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

3.5.6 Podcast

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

4. Events organized / hosted

4.1 Conferences and seminars

4.1.1 AusCERT Conference

The AusCERT Conference 2023, took place from 9th May -12th May 2023 at the Star hotel Gold Coast with the theme of "Back to The Future" that was also broadcasted online. The conference included more than 50 presenters of ranging topics on cyber security.

5. International Collaboration

5.1 International partnerships and agreements

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

5.2 Drills and Exercises

5.2.1 APCERT Drill 2023

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 “Digital Supply Chain Redemption”. The drill fosters communication between the CERTs in the region and beyond. In all, 24 APCERT CERT/CSIRT teams from 21 economies participated.

5.2.2 ACID 2023

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

6. Conclusion

AUSCERT continues to look for further improvement in the way it provides assistance to its constituency. During this improvement techniques are being shade with other CERT/CSIRT in APCERT. With the use and retainment of machine learning knowledge and its application, more analyst detection skill set is being mechanized to make more efficient use of our valued human resources. Although AUSCERT has started to share the skills in making machine learning models work for CERT and CSIRT, further collaboration in 2024 is expected with other CERTs and CSIRTs in sharing experience in using this technology to make a safer and cleaner internet.

BGD e-GOV CIRT

Bangladesh e-Government Computer Incident Response Team

1. Highlights of 2023

1.1 Summary of major activities

- BGD e-GOV CIRT has successfully organized Financial Institution & Critical Information Infrastructure (CII) Cyber Drill 2023.
- BGD e-GOV CIRT has successfully organized Cyber-Maitree 2023, Cyber security training and exercise in association with CERT-In.
- A total of 98 meticulously crafted cyber threat alert reports were distributed to diverse organizations across Bangladesh.
- Responding to three major ransomware incidents reported to BGD e-GOV CIRT throughout the year.
- "Cyber Threat Intelligence Report" provided to 71 government and non-government organizations.
- 12 cyber sensor analysis reports have been provided to multiple Critical Information Infrastructures
- Vulnerability assessment and penetration testing (VAPT) have been performed on different sectors in Bangladesh including financial sectors, Critical Information Infrastructures and Govt. sectors.

1.2 Achievements & milestones

- Published "Ransomware Landscape: A Data-driven Threat Analysis of Bangladesh, Year 2023."
- Participated in the 11th Regional Arab, OIC-CERT & CIS Cyber Drill in Abu Dhabi, United Arab Emirates.
- Participated in the APCERT Cyber Drill 2023 "digital supply chain redemption".

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

In recent years, there has been a significant increase in ransomware attacks in Bangladesh, impacting various industries. Cybersecurity experts argue that most of these attacks are not the result of highly sophisticated methods but rather a lack of proper cybersecurity practices. Nevertheless, the consequences for the affected industries are quite severe. BGD e-GOV CIRT has taken a leading role in advocating for the adoption of enhanced cybersecurity practices.

The organization consistently encourages entities across Bangladesh to promptly report any incidents or suspicious activities identified within their networks. This willingness to report ransomware incidents to BGD e-GOV CIRT marks a significant stride in the ongoing battle against the ransomware.

Identified Ransomware incidents of Bangladesh 2023

1. LOCKBIT 3.0

- INCIDENT TIME
  December 2022
- TARGET
  Leading Pharmaceutical company in Bangladesh.
- DATA BREACH
  750GB of data, including personal folders, infrastructure, and accounting data.
- MODEL
  Ransomware-as-a Service (RaaS)

2. Money Message

- INCIDENT TIME

  March 2023
- TARGET

  Leading transportation organization in Bangladesh.
- NOTABLE

  Newcomer to the ransomware landscape.
- IMPACT

  Critical server and computer systems affected; operations disruption.

3. ALPHV/BlackCat

- INCIDENT TIME

  June 2023
- TARGET

  Financial organization in Bangladesh.
- INITIAL ACCESS METHOD

  Stolen credentials obtained through initial access brokers
- DATA BREACH

  170 GB of sensitive data, including SQL backups, financial data, and employee information.
- NOTABLE

  Ransomware family written in Rust.
- MODEL

  Ransomware-as-a Service (RaaS)

4. Akira Ransomware Group

- INCIDENT TIME

  June 2023
- TARGET

  Conglomerate company in Bangladesh.
- INITIAL ACCESS METHOD

  Infiltration through compromised VPN services and exploiting unsecured credentials.
- NOTABLE

  Emerging group, ¬first discovered in March 2023.
- TOTAL VICTIMS

  Compromised more than 63 victims
- TARGET PROFILE

  Actively targeting small and medium-sized businesses worldwide

4. Events organized / hosted

4.1 Training

- BGD e-GOV CIRT has successfully organized Financial Institution & Critical Information Infrastructure (CII) Cyber Drill 2023.
- BGD e-GOV CIRT has successfully organized Cyber-Maitree 2023, Cyber security training and exercise in association with CERT-In.
- Organized a 5 days long training session for officials of PKSF.
- Organized MIST LeetCon 2023, "Hack Me If You Can".
- Organized "Safe CII" workshop for all the CII organizations of Bangladesh.
- Supported partner in Cyber Security conference renasCON 2023.
- Organized daylong seminar, titled "Secure Our World", at the event of Cyber Security Awareness Month 2023 for women entrepreneurs.
- Organized training for officials of ICT division on cyber security awareness and social engineering aspects.

4.2 Drills & exercises

- BGD e-GOV CIRT has successfully organized Financial Institution & Critical Information Infrastructure (CII) Cyber Drill 2023.
- BGD e-GOV CIRT has successfully organized Cyber-Maitree 2023, Cyber security training and exercise in association with CERT-In.
- Organized MIST LeetCon 2023, "Hack Me If You Can".

5. International Collaboration

5.1 Capacity building

5.1.1 Training

- Participated in Cyber Defense Conference 2023.
- Conducted training session at APBn Head Quarter.
- Conducted session on "Capacity Building on Cyber Security for RAJUK Officials"
- Conducted training session at Cyber Training Center, CID.
- Attended "Black Hat Asia 2023", Singapore.
- Attended "RSA Conference 2023", USA.

- Conducted training on CIRT operation and Digital Forensics at the Office of the CCA.
- Conducted a 5 days long training session for officials of Department of ICT in cooperation with the EDGE project.
- Conducted a day long training session on "Cyber security challenges in 4IR revolution" at the Security Services Division under the Ministry of Home Affairs of Bangladesh.
- Conducted a session on "Case study on Spear Phishing" at System Administrator's Day 2023, organized by Bangladesh System Administrators Forum (BDSAF).
- Conducted 5 days long training session for officials of CII organizations, organized by EDGE project.
- Conducted 2 days long training session on Cyber Security Awareness for Female Member of Parliament, organized by EDGE project.
- Conducted 2 days long training session on Cyber Security Act 2023, Digital Forensics and Social Engineering for the officials of Corps of Military Police Center and School.
- Conducted training on Cyber Security for officials of Police Telecom and Information Management, Bangladesh Police.
- Conducted training session on cyber security awareness and Cyber Security Act 2023 at Department of Women Affairs.

5.1.2 Drills & exercises

- Participated in the Cyber Championship, organized by National Cyber Range of Russia.
- Participated in "Financial Sector Tech Camp #1" conducted by Carnegie Mellon University, organized by the State Department of the USA.
- Participated the following events in the Regional Cybersecurity Week 2023 in Abu Dhabi, United Arab Emirates
    - The 11th Regional Arab, OIC-CERT & CIS Cyber Drill
    - The 11th Regional Cybersecurity Summit
    - The 15th Annual OIC-CERT Conference and FIRST Symposium for Arab and Africa Regions

6. Future Plans

6.1 Future Operation

- Arrange Cyber Drills for different sectors.
- Perform risk assessment to critical infrastructure (CIIs).
- Provide training about Industrial Control System (ICS) in public sector.
- Perform vulnerability assessment and penetration testing on 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. Attachment (Photos)

Figure: Financial Institution & Critical Information Infrastructure (CII) Cyber Drill 2023

Figure: Cyber-Maitree 2023, Cyber security training and exercise

Figure: Cyber security training for Critical Information Infrastructure organizations.

Figure: 5 days long training session for officials of PKSF, Bangladesh.

Figure: Training session at Armed Police Battalion Head Quarter, Bangladesh.

Figure: Training session at Cyber Training Center, Criminal Investigation Department Bangladesh Police.

Figure: "Safe CII" workshop for all the CII organizations of Bangladesh

Figure: World Bank high officials visiting the cyber security training for CII organizations.

Figure: Participated in the Cyber Championship, organized by National Cyber Range of Russia.

Figure: A day long seminar, titled "Secure Our World", at the event of Cyber Security Awareness Month 2023 for women entrepreneurs.

Figure: Cyber security training for Government officers'

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 2023

2.1 Incidents response

For the year 2023, CSB's BruCERT, through the Cyber Watch Centre (CWC), has identified multiple instances of malicious behavior through the secure monitoring and intelligent sensors, located at the BruCERT constituent systems. Based on these findings, malware infections, are the most prevalent form of cyber threat in Brunei Darussalam which some instances involve "Ransomware" attacks. The second most common type of incident detected involved attacks on user accounts, including both normal user and privilege accounts. Figure 1 and Table 1 depict the statistics of these security incidents.

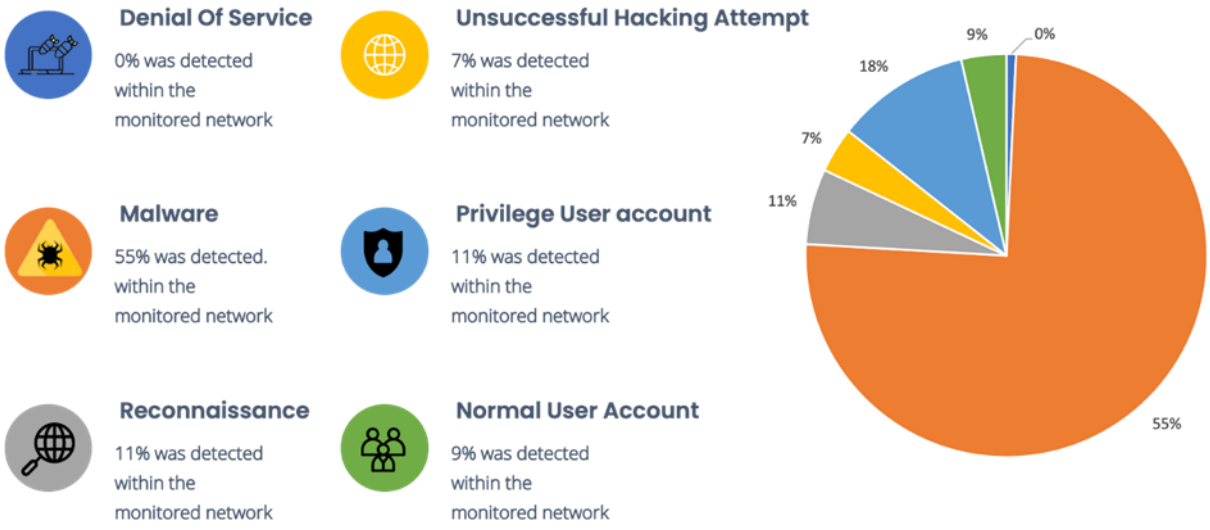


Figure 1

Types of Attacks	Count
Denial of Services	4
Malicious Software	1746
Reconnaissance	345
Unsuccessful Hacking Attempt	221
Normal User Account	300
Privilege User Account	555

Table 1

Malware outbreak within BruCERT constituents had decreased from the previous year 2022 due to successful deployment of Cyber Security Brunei (CSB) end point detection Response (EDR) system. However, with the deployment of EDR CWC had detected an increased amount of reconnaissance upon its constituents which were suspected perform by malicious software.

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.

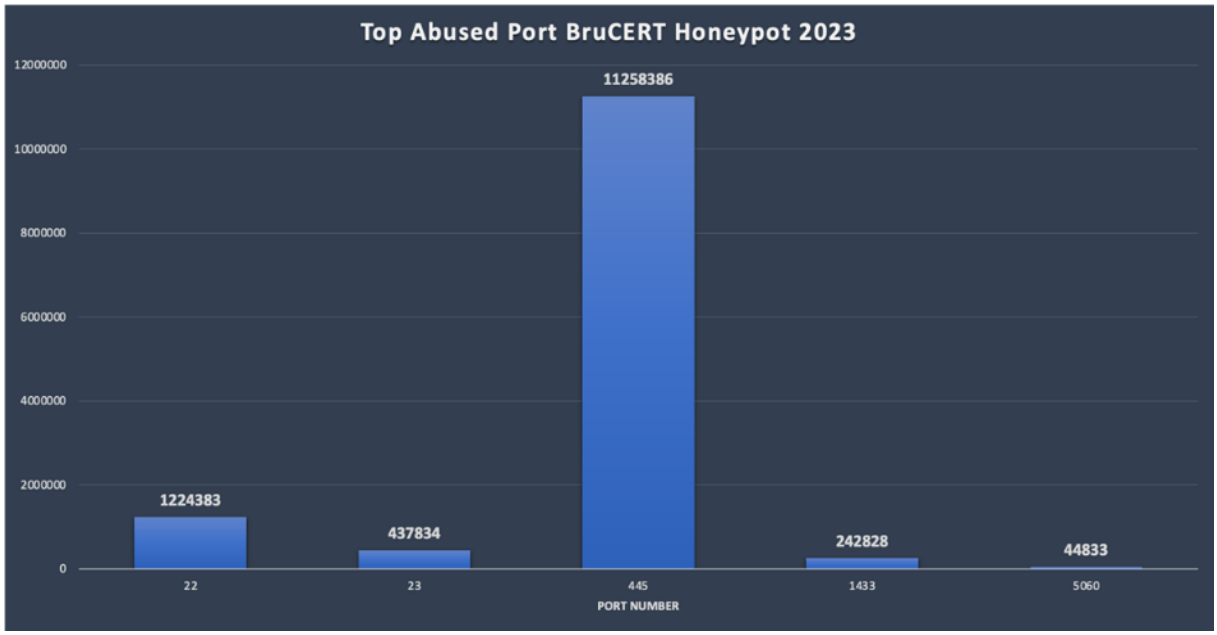


Figure 2

Port No	Count
22	1224383
23	437834
445	11258386
1433	242828
5060	44833

Table 2

From BruCERT honey pot, it seems new variants of malware had been targeting the organizations using port 22 as well as port 445. This can be further 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 the Honeypot.

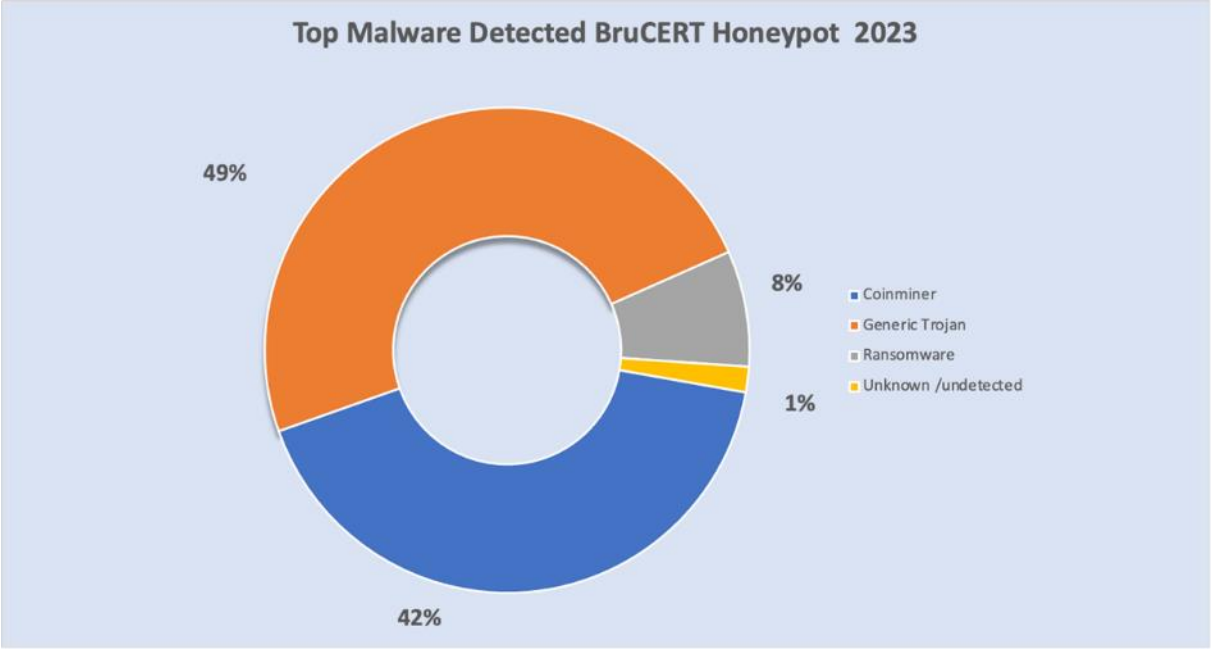


Figure 3

Malware Type	Total
COINMINER	7081
GENERIC TROJAN	8261
RANSOMWARE	1307
UNKNOWN	287
Grand Total	16936

Table 3

The year 2023, 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.

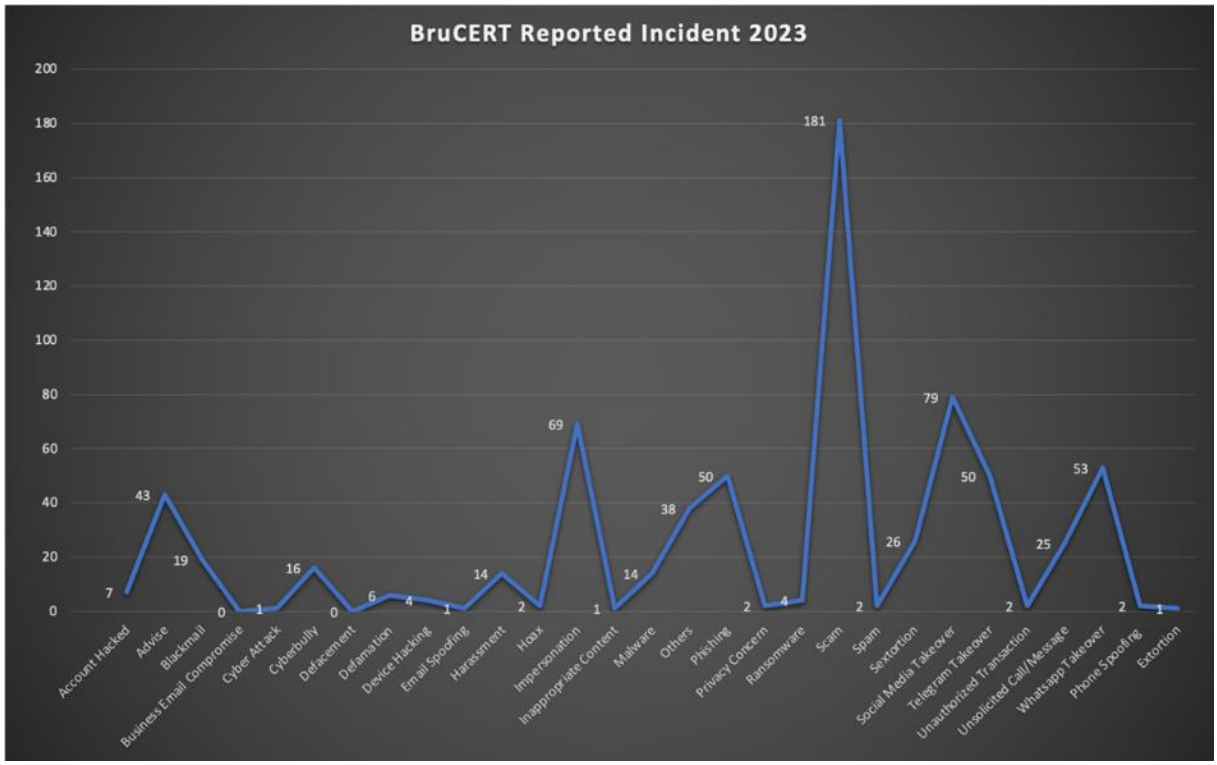


Figure 4

3. BruCERT Activities in 2023

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 8th November 2023 until 9th November 2023 - BruCERT delegates attended the APCERT AGM and Annual Conference 2022 which takes place online.
- From 16th October 2023 until 20th October 2023 - Three BruCERT delegates attended the OIC-CERT 15th ANNUAL CONFERENCE which takes place at Abu Dhabi, UAE, hosted by Cyber Security Council.

3.2 Awareness Activities

Throughout 2023, 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 1,841 monthly website visits. Please refer to Figure 5 for BruCERT Awareness infographic activity for the year 2023.

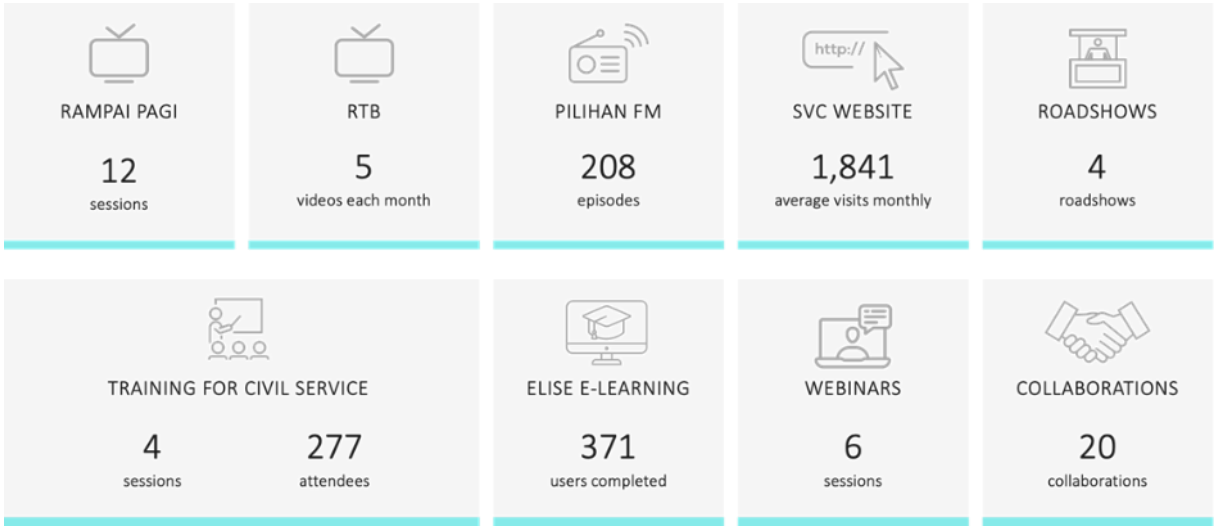
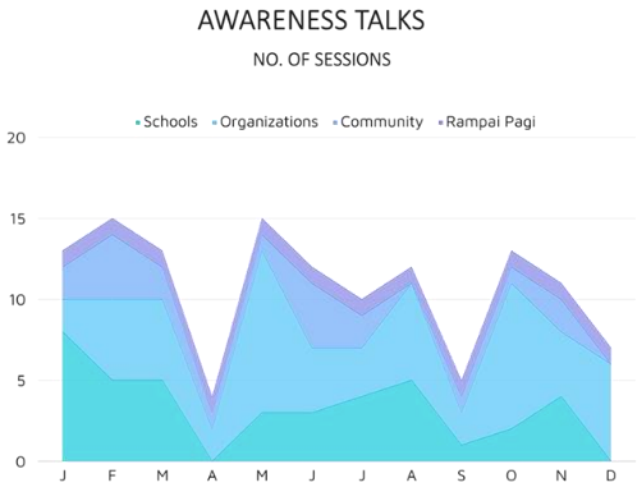


Figure 5

"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 2023.

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 had attended BruCERT awareness talk for the year 2023.



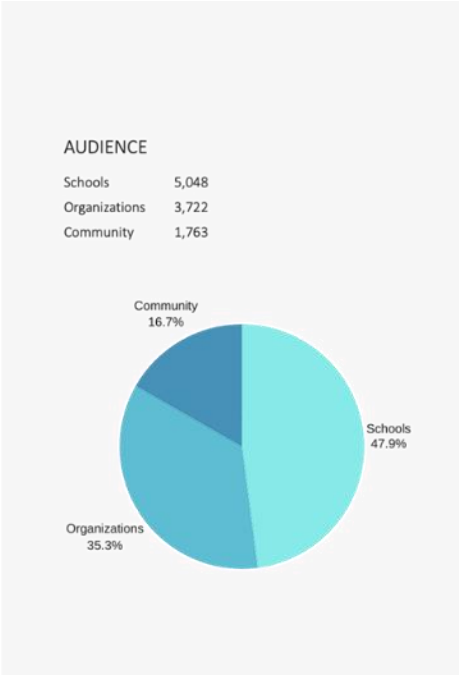


Figure 6

BtCIRT

Bhutan Computer Incident Response Team

1. Highlights of 2023

1.1 Summary of major activities

In 2023, the third edition of the "National Cybersecurity Week" was also conducted successfully in October 2023 as a part of the Cybersecurity Awareness Month in October. In addition, BtCIRT participated in the GFCE conference in Ghana, November 2023, CAMP meeting in South Korea in July 2023, ITU CyberDrill Inter-Region in Cyprus December 2023 and APCERT Drill virtually in August 2023. A few workshops and training were also conducted. A CIRT maturity assessment was also conducted.

1.2 Achievements & milestones

Key activities in 2023 included:

- ITU conducted CIRT maturity assessment and also conducted a malware analysis workshop and a tabletop exercise.
- Organized the third "Cybersecurity Week" from 25-27 October, covering various programs; a full day Conference, Application Security, Network security and Domain abuse workshops and an Open Awareness program with awareness content published in BtCIRT Facebook page promoting cyber hygiene best practices.
- Conducted Capture the Flag (CTF) challenge in three ICT colleges in Bhutan in partnership with Asia Pacific Telecommunity (APT) where 138 students participated from 3 technical colleges.
- Published Child Online Protection (COP) related posters and drafted COP Guidelines.
- Drafted the National Cybersecurity Strategy and Critical Information Infrastructure (CII) Identification methodology
- Published 83 Alerts and advisories on latest scams and threats
- Handled a total of 171 incidents in the past year

2. About BtCIRT

2.1 Introduction

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

2.2 Establishment

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

2.3 Resources

Currently, BtCIRT consists of thirteen 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, 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

A total of 178 incidents were handled in 2023, majority of which were vulnerabilities (66.9%), followed by fraud related incidents like phishing and scams (11.8%). The following graph provides the overview of the types of incidents handled:

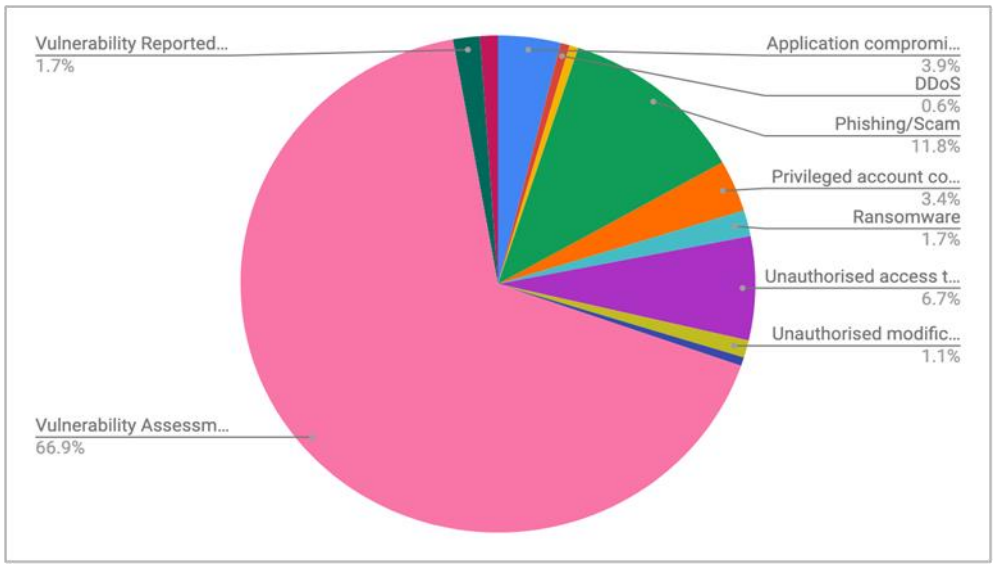


Figure 1: Percentage of Incident handled by Incident Classification type

3.3 Awareness creation programs

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

3.3.1 Drafting Child Online Protection (COP) Guidelines

In collaboration with ITU and UNICEF a localized version of the COP guidelines 2020 by ITU were drafted taking into consideration the existing COP measures and the lack thereof. The guidelines are very prescriptive and outline the

necessary steps that the respective COP targets; Parents & Educators, Policy Makers, and Industry should take to help children to be safe online and to ensure that they are adequately protected. Online safety related Posters for children and young individuals were also published to be distributed to schools around the country.

3.3.2 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.

3.3.3 Open Awareness Program

As a part of Cybersecurity Awareness month and Cybersecurity Week programs, an open cybersecurity awareness program was conducted targeting the general public to help with their understanding of prevalent cybersecurity threats and cybersecurity best practices in the online world. Awareness content was also published in the BtCIRT Facebook page throughout the week promoting cyber hygiene best practices.

3.4 Security Advisory and Alerts

BtCIRT publishes latest cyber security news and vulnerabilities to keep the constituents well informed about the latest development in the area of cybersecurity on its website and Facebook page. A total of 60 alerts and advisories were published in 2023. Of these alerts and advisories, a significant proportion were released to address critical patches released by software vendors to fix the vulnerabilities.

4. Events organized / hosted

4.1 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 Cybersecurity GRC workshop (23-25 May, 2023)

The cybersecurity experts from Welchman Keen provided a three-day workshop consisting of six modules including National Cybersecurity Strategy Lifecycle, Critical National Information Infrastructure Protection, Risk Management Strategy, Cybersecurity Governance and Risk, Cybersecurity for e-Gov Services, GDPR Implementation and Compliance, and Data protection and privacy. There were 130 attendees, comprising key decision-makers, managerial staff, and data protection related officers from diverse government, corporate, and private sectors, all holding crucial roles in implementing Governance Risk & Compliance practices.

4.1.2 Workshop on Incident Handling and Malware Analysis

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

4.1.3 National Cybersecurity Week (25-27 October)

The 3rd edition of the National Cybersecurity Week was observed from 25-27 October, whereby several training programs and a conference were conducted.

4.1.4 Technical workshops (25-26 October):

The Cybersecurity technical workshop was conducted on Domain Name Abuse and Network Security for more than 50 participants including Network Engineers, System Administrators, ICT officers and Data Protection related officers from Private, Corporations and Government agencies.

4.1.5 Cybersecurity conference (27th October):

Panel of experts from various agencies and institutions within the country were engaged in discussions on critical cybersecurity issues, including data privacy, ransomware attacks, National Digital Identity, and the role of artificial intelligence in cybersecurity. The interactive session covered a diverse range of perspectives surrounding the theme 'Trust in the Digital Age'.

Figure 2:Participants during the Cybersecurity Conference

4.2 Drills/Exercises

The following drills and tabletop exercises were conducted:

4.2.1 Cybersecurity Capture the Flag Challenge (16 - 17 October)

The Cybersecurity CTF 'Capture the Flag' challenge took place at three colleges: College of Science and Technology, Jigme Namgyel Engineering College, and Gyalpozhing College of Information Technology. It consisted of a hands-on workshop on introducing the basics of cybersecurity on Day 1 and Capture the Flag competition among the students on Day 2. The objective of the program was to develop the future cybersecurity workforce of Bhutan.

4.2.2 Tabletop Exercise (15th August 2023)

As a part of the CIRT assessment and training session, a tabletop exercise on Cybersecurity Crisis management was conducted by the ITU experts for the critical agencies. The exercise helped the participants understand the role of different team members in responding to incidents.

5. International Collaboration

5.1 International partnerships and agreements

BtCIRT has been a member of FIRST and APCERT since 2017. The newest memberships were established with CAMP and GFCE in 2023.

5.2 Capacity building

The BtCIRT members have availed a number of skills development opportunities through training, workshops, conferences which have helped the members to upskill their knowledge and skills. These have also provided opportunities to network with a number of international and national Cybersecurity/CIRT communities and experts. BtCIRT is grateful to all the organizers for providing these various capacity building opportunities.

5.2.1 Trainings

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

Event	Organizer/Trainer	Region	Date
Cybersecurity Bootcamp Program	National Security College	Australia	5-9 June, 2023
8th Annual CAMP Meeting	CAMP	South Korea	11-13 July, 2023
Training on Cybersecurity Ecosystem in Indonesia	JICA	Indonesia	21-25 August, 2023
APT Training Course on Empowerment of Blockchain, Cyber Security & Cyber Forensic	Asia Pacific Telecommunity	India	1-6 September, 2023
GFCE Annual Meeting, GC3B Conference	GFCE	Ghana	26th December, 2023 27 - 28 December, 2023
ITU Interregional CyberDrill for Europe and Asia-Pacific	International Telecommunication Union	Cyprus	28th Nov to 1st Dec, 2023

5.2.2 Drills and exercises

BtCIRT had the opportunity to attend and participate in the following cyber exercises:

- Annual APCERT Drill themed "Digital Supply Chain Redemption" on 16th August.
- Participated in ITU Interregional CyberDrill

5.2.3 Seminars, Conference & Presentations

BtCIRT had the opportunity to participate in the following seminars, meetings, and conferences:

- A BtCIRT member participated in the first day of the four-day ITU Interregional CyberDrill for Europe and Asia-Pacific on 28th November and shared the national cyber crisis response plans and insights on experience with intersectoral coordination in Bhutan.
- A BtCIRT member presented best practices of Network Security during btNOG-10 in Paro in June 2023, which is the annual Bhutan Network Operators Group (btNOG) program.

6. Future Plans

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

The future plans for BtCIRT include:

- Implementation of National Cybersecurity Strategy
- Building relevant cybersecurity capabilities to defend and protect critical information infrastructure
- Cybersecurity awareness for leaders, Critical operators, Small and Medium Businesses, and general public
- Strengthening cooperation and collaboration with more organizations internally and internationally

7. Conclusion

In 2023, BtCIRT handled a total of 178 incidents and carried out various cybersecurity programs in line with the various cybersecurity mandates of BtCIRT which included various capacity development and awareness programs covering a broad range of target groups. In future, BtCIRT will continue to focus on improving its visibility in the country and to create awareness on the importance of cybersecurity. In addition, the implementation of National Cybersecurity Strategy and the protection of Critical Information Infrastructure protection will be a priority.

CERT-In

Indian Computer Emergency Response Team

1. Highlights of 2023

1.1 Summary of major activities

i. In the year 2023, Indian Computer Emergency Response Team (CERT-In) handled **15,92,917** incidents. The type of incidents handled were Website Intrusion & Malware Propagation, Malicious Code, Phishing, Distributed Denial of Service attacks, Website Defacements, Unauthorized Network Scanning/Probing activities, Ransomware attacks, Data Breach and Vulnerable Services. Remedial measures for handling incidents were suggested and implemented in coordination with relevant stakeholders.

ii. CERT-In tracks latest cyber threats and vulnerabilities. A total of **657** security alerts, **52** advisories and **397** Vulnerability Notes were issued during the year 2023.

iii. CERT-In conducted **26** 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 **14** domestic cyber crisis exercises in 2023 for various organizations across Sectors and State Government Departments.

v. CERT-In has conducted 3 international exercise, contributed in planning & scenario development in 1 exercise and participated as a player in 4 International cyber security drills in 2023.

vi. CERT-In conducted G20 Cyber Security Exercise and Drill on 31st January 2023 for 400 Participants including international participants from more than 12 countries who joined through online mode while domestic participants from diverse sectors such as Finance, Education, Telecom, Ports & Shipping, Energy, IT/ITeS and others attended in-person for the Strategic Table Top Exercise and for the Operational Drill.

vii. "Cyber Security Exercise for Banking Sector" under India's G20 Presidency was jointly conducted by CERT-In and Reserve Bank of India (RBI) on 5th June 2023, for more than 200 participants from International Monetary Fund, Bank for International Settlements, Central Banks and Computer Emergency Response Teams of G20 Member Countries, MD & CEOs of select Commercial and Urban Cooperative Banks, Chief Information Security Officers (CISOs) and Chief Technology Officers (CTOs) of Indian and Foreign Banks.

viii. CERT-In successfully conducted cybersecurity exercise & training program **"Cyber-Maitree 2023"** for organizations of Government of Bangladesh from 02nd-04th October 2023 in Dhaka, Bangladesh.

ix. CERT-In has trained & enabled sectoral entities to conduct sector specific exercise and drills.

x. CERT-In is the convener of APCERT Internet of Things (IoT) Security technical working group. As a member of APCERT Drill WG, CERT-In has also contributed in APCERT drill 2023 design & execution.

xi. CERT-In has become an associate partner in Charter of Trust (CoT) global forum. The Associated Partner Forum (APF) of CoT brings together regulators, research institutes, universities, and think tanks with the CoT's industry partners to build a trusted network committed to creating a strong digital security environment across the global economy

1.2 Achievements & milestones

i. CERT-In conducted G20 Cyber Security Exercises and Drills on 31st January 2023 and 5th June 2023 for 600 Participants including international participants from more than 12 countries.

ii. CERT-In conducted cybersecurity exercise & training program "Cyber-Maitree 2023" for critical sector organizations of Government of Bangladesh from 02nd-04th October 2023 in Dhaka, Bangladesh.

iii. CERT-In has trained and enabled sectoral entities to conduct sector specific exercise and drills.

iv. In 2023, CERT-In Signed bilateral agreements in the area of cyber security with The Egyptian Computer Emergency Readiness Team (EG-CERT) and renewed the agreements with The Information System Authority of The Republic of Estonia and National Cyber Security Centre (NCSC)-UK to enable information sharing and collaboration for incident resolution.

v. CERT-In has become an associate partner in Charter of Trust (CoT) global forum. The Associated Partner Forum (APF) of CoT brings together regulators, research institutes, universities, and think tanks with the CoT's industry partners to build a trusted network committed to creating a strong digital security environment across the global economy

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

3. Activities & Operations

3.1 Scope and definitions

CERT-In provides:

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

3.2 Incident handling reports

The summary of activities carried out by CERT-In during the year 2023 is given in the following table:

Activities	Incidents in 2023
Security Incidents handled	1592917
Vulnerability Notes Published	397
Advisories Published	52
Security Alerts issued	657
Security Drills	22
Trainings Organized	26

Table 1: CERT-In Activities during year 2023

3.3 Abuse statistics

In the year 2023, CERT-In handled 1592917 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	2023
Phishing	869
Unauthorized Network Scanning/Probing	447720
Vulnerable Services	941592
Virus/ Malicious Code	184131
Website Defacements	10665
Website Intrusion & Malware Propagation	1045
Others	6895
Total	1592917

Table 2: Breakup of Security Incidents handled

3.3.1. Tracking of Indian Website Defacements

CERT-In has been tracking the defacements of Indian websites and suggesting suitable measures for hardening the web servers to concerned organizations. A total of **10,665** numbers of defacements have been tracked.

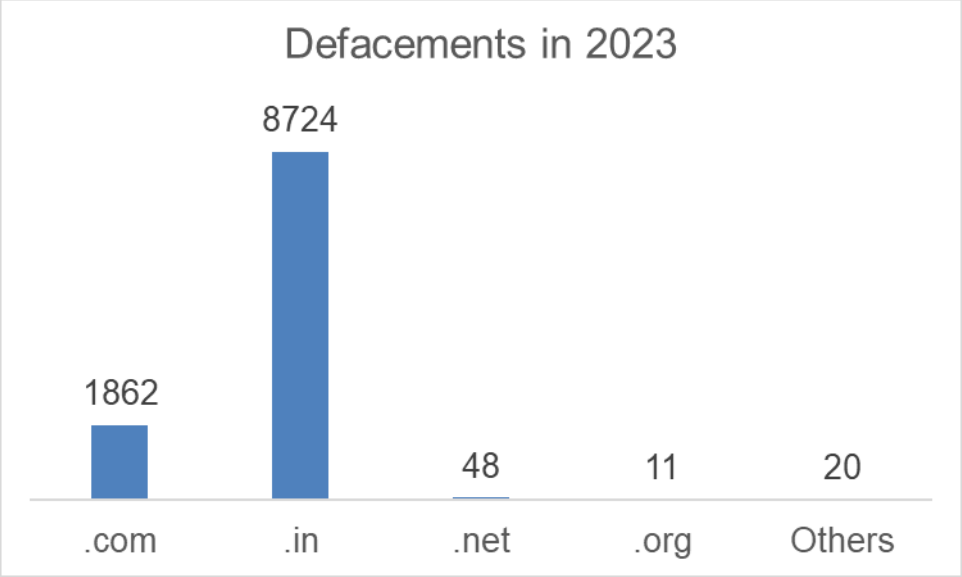


Figure 2: Indian Website Defacements tracked by CERT-In during 2023

3.3.2. Botnet Cleaning Initiatives

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

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

CSK celebrated awareness campaign 'Cyber Swacchhta Pakhwada' from 1-15 February 2023 and 'Swachhta Campaign 3.0' in October 2023, in coordination with Internet Service Providers (ISP) and Antivirus Companies for spreading awareness and information regarding cyber security threats, challenges and safeguarding citizens against them.

CSK provides three Free Bot Removal Tools (FBRTs) developed in collaboration with "QuickHeal", "K7" and "eScan" with a cumulative of 48.88 lakh downloads recorded till December 2023. These FBRTs are available for Microsoft Windows and Google Android platforms.

CSK also provide Mobile Security Application for Android platform to users via web portal.

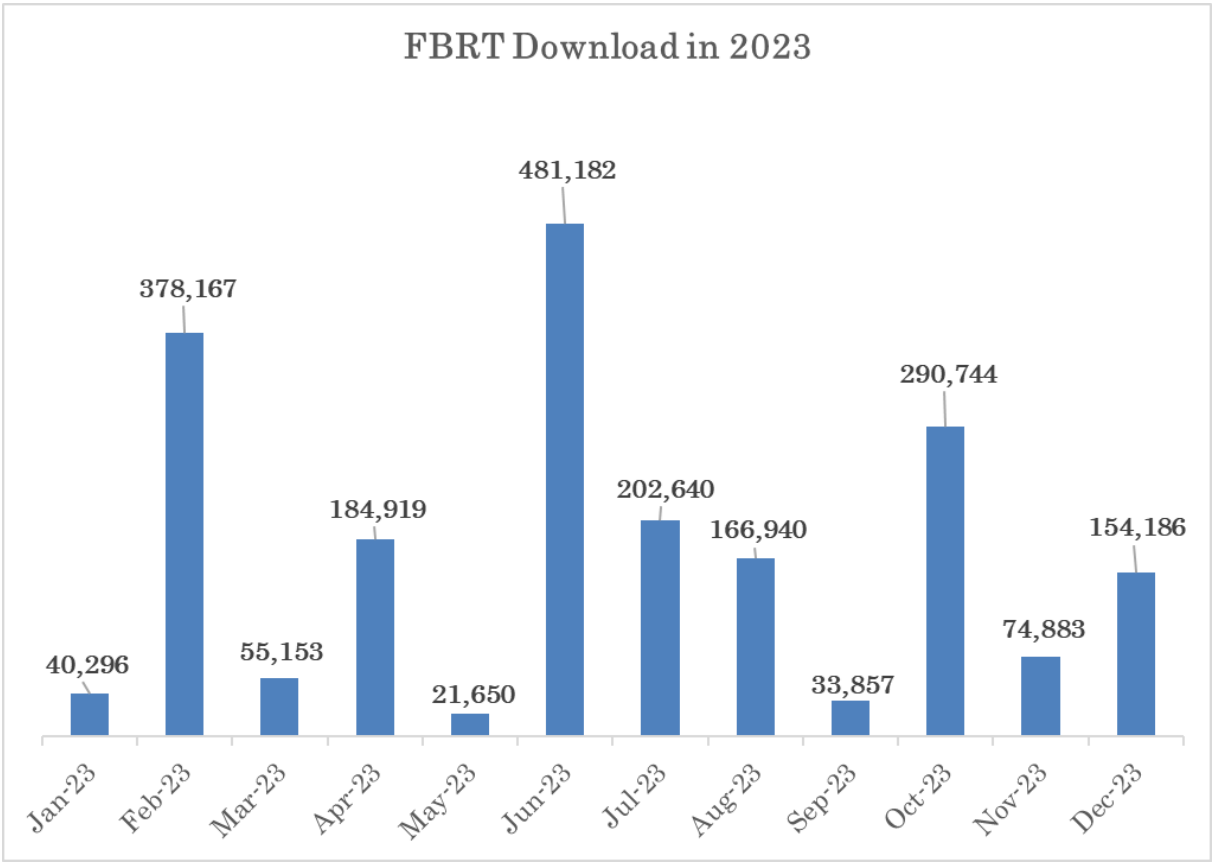


Figure 3: CSK Free botnet removal tools download statistics 2023

3.3.3. Security Profiling, Assurance framework and Audit Services

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

CERT-In has empaneled **176** 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.

3.3.4. Cyber threat Intelligence Sharing

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

CERT-In has opearationalised 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 2023, CERT-In via its email mechanism and with its automatic threat Intel sharing platform- shared 634 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.

3.3.5. National Cyber Coordination Centre (NCCC)

Continuously evolving cyber threat landscape and its impact on well-being of information technology, National Economy, and Cyber Security necessitates the need for near-real time situational awareness and rapid response to cyber security incidents. 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.

3.3.6. Cyber Forensics

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

3.3.7. CVE Numbering Authority (CNA)

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

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

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

4. Events organized / hosted

4.1 Training

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

In 2023, CERT-In has conducted **26** trainings on various specialized topics of cyber security. A total of **10074** 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 2023 by organizing various events and activities for citizens as well as the technical cyber community in India with a theme of " Secure our world". The total outreach of National Cyber Security Awareness Month October 2023 is 86,13,62,533. 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 2023, CERT-In conducted 48 awareness sessions

for different sectors in collaboration with different organizations covering 20,139 participants

4.2 Drills & exercises

Cyber security exercises are being conducted by CERT-In to help the organizations to assess their preparedness to withstand cyber-attacks. These exercises have helped tremendously in improving the cyber security posture of the information infrastructure and training of manpower to handle cyber incidents, besides increasing the cyber security awareness among the key sector organizations. CERT-In has conducted 14 such cyber security exercises in 2023.
Till 2023, CERT-In has conducted 87 Cyber security exercises of different complexities, including table top exercises, with participation from around 1200 organizations covering various sectors of Indian economy from Government/Public/Private including Defense, Paramilitary forces, Space, Energy, Telecommunications(ISPs), Finance, Health, Oil & Natural Gas, Transportation (Railways & Civil Aviation), IT/ ITeS/ BPO sectors and State Data Centers.

5. International Collaboration

5.1 International partnerships and agreements

Strengthening International cooperation to effectively deal with cyber security issues has been one of the main focus areas of the Government. As such, this aspect is being dealt with by way of security cooperation arrangements in the form of Memorandum of Understandings (MoUs) between Indian Computer Emergency Response Team and its overseas counterpart agencies that are willing to work together and share information in a timely manner for preventing cyber incidents and cyber-attacks as well as collaborating for providing swift response to such incidents.
In 2023, CERT-In Signed bilateral agreements in the area of cyber security with The Egyptian Computer Emergency Readiness Team (EG-CERT) and renewed the agreements with The Information System Authority of The Republic of Estonia and National Cyber Security Centre (NCSC)-UK to enable information sharing and collaboration for incident resolution. CERT-In is regularly coordinating with leading service providers and product vendors within and outside the country to obtain advance information on latest cyber threats and attack trends and devise appropriate proactive and preventive measures.
CERT-In is an operational member of Asia Pacific Computer Emergency Response Teams (APCERT). CERT-In is the convener of “IoT Security working group” across APCERT to address security threats and evolve best practices to secure IoT devices.
CERT-In is also member of various other working groups under APCERT such as Information sharing working group, Drill working group, Malware Mitigation working group, Tsubame working group and Training Working Group. As a member of APCERT Drill WG, CERT-In has also contributed in APCERT drill 2023 design & execution.
CERT-In is a member of global Forum of Incident Response and Security Teams (FIRST). The membership in FIRST enables incident response teams to more effectively respond to security incidents in a reactive as well as proactive manner

CERT-In 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 ICS Cybersecurity Week for Indo-Pacific Region organized by METI, Japan from 09th to 13th October in Tokyo, Japan.
ii. CERT-In participated in the APISC security training course hosted by KrCERT/CC, KISA during Oct 23-27 at Seoul, South Korea.
iii. CERT-In participated in the APCERT online training on "DNS Security and Threats for Incident Responders" on 28th March 2023.
iv. CERT-In participated in the APCERT online training on "5G Vulnerability Analysis" on 09th May 2023.
v. CERT-In participated in the APCERT online training on "Exploring Machine Learning on Phishy Domains" on 11th October 2023.
vi. CERT-In officials also participated in the 301L ICS Cybersecurity Training provided by CISA in Idaho falls USA in 2023.
vii. CERT-In participated in the APCERT conference held on 09th November 2023 in Virtual mode.

5.2.2 International Drills & exercises

CERT-In has conducted 3, contributed in 1 international exercise planning & scenario development and participated as player in 4 International cyber security drills in 2023. Following are the brief of the exercises:

i. CERT-In conducted G20 Cyber Security Exercise and Drill on 31 January 2023 for 400 Participants including international participants from more than 12 countries.
ii. "Cyber Security Exercise for Banking Sector" under India's G20 Presidency was jointly conducted by CERT-In and RBI on 5 June 2023, for more than 200 participants.
iii. CERT-In conducted cybersecurity exercise & training program "Cyber-Maitree 2023" for Government organizations of Bangladesh from 02-04th October 2023 in Dhaka, Bangladesh.
iv. CERT-In participated in the APCERT Annual drill 2023 in August 2023 which was conducted with the objective to test the response capability of leading Computer Security Incident Response Teams (CSIRT) within the Asia Pacific economies. The theme of APCERT Drill 2023 was "Digital Supply Chain Redemption". CERT-In also acted as exercise coordinator (EXCON) for international CERTs in the Drill.
v. CERT-In participated in the 3rd Edition Africa CERT Cyber Drill 2023 and played in multiple scenarios on 09th & 10th November 2023. The exercise was on challenge based scenarios like phishing, incident-response, malware analysis, reverse engineering and forensic analysis.
vi. CERT-In participated in Quantum Dawn VII from 14th to 16th November 2023. The exercise engaged over 1000 participants from more than 150 public and private sector institutions in over 20 countries around the globe including financial firms. Central banks, regulators and law enforcement entities.

vii. CERT-In participated in ASEAN CERT Incident Drill (ACID) – 2023 in October 2023. The theme of ACID Drill 2023 was 'Responding to Multi-Pronged Attacks Arising from Hacktivism'. 18 CERTs from various countries have participated in the drill.

viii. CERT-In participated in National Cybersecurity Authority (NCA)- International Telecommunication Union (ITU) Technical CyberDrill 2023.

5.3 Other international activities

i. CERT-In participated in the CVE Global Summit-Spring 2023 held during 22 - 23 March 2023 in Mclean, Virginia, USA.

ii. CERT-In officials attended the 35th Annual FIRST Conference and AGM held in Montreal, Canada from 04th to 09th June 2023.

iii. CERT-In participated in the APCERT AGM held in Virtual Mode on 08th November 2023.

iv. CERT-In participated virtually in the Community Town Hall Meeting, held on 11th November in Paris.

v. CERT-In participated virtually in the UN Ad-Hoc committee meetings on countering the use of ICTs for criminal purposes.

vi. CERT-In participated in 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

vii. CERT-In participated in the 70th Task Force for Computer Security Incident Response Teams (TF-CSIRT) Meeting at Stockholm, Sweden held during 25 to 27 September 2023.

6. Conclusion

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

Contact Information

Postal Address 1:

Indian Computer Emergency Response Team (CERT-In)

Ministry of Electronics & Information Technology (MeitY)

Government of India

Electronic Niketan

6, CGO Complex, Lodhi Road

New Delhi – 110003, India

Postal Address 2:

CERT-In Office, Block – 1

Delhi IT Park, Shastri Park

Delhi – 110053, India

Phone: +91-11-22902703, 22902704

Incident Response Help Desk:

Phone: +91-11-24368572

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

Fax: +91-11-24368546

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

Incident report to Incident Response Help Desk at:

Email: incident@cert-in.org.in

User ID: incident@cert-in.org.in

Key ID: 0xB620D0B4

Key Type: RSA

Expires: 2024-12-31

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: 2024-12-31 Key Size: 4096/4096

Finger Print: EABE 086A 6FC4 CB47 3F29 A90B DE30 A071 275C CACF

Phone: +91-11-22902657

Toll Free Phone: +91-1800-11-4949

Toll Free Fax: +91-1800-11-6969

Email: csk@cert-in.org.in

PGP Key Details:

User ID: csk@cert-in.org.in

Key ID: 0x4EE11788

Key Type: RSA

Expires: 2025-05-31

Key Size: 4096/4096

Finger Print: E204 D43D 0296 40FB 8DB9 0290 706D EF4D 4EE1 1788

For International Liaison activities

Email: international@cert-in.org.in

PGP Key Details:

User ID: international@cert-in.org.in

Key ID: 0xECCB2102

Key Type: RSA

Expires: 2025-05-31

Key Size: 4096/4096

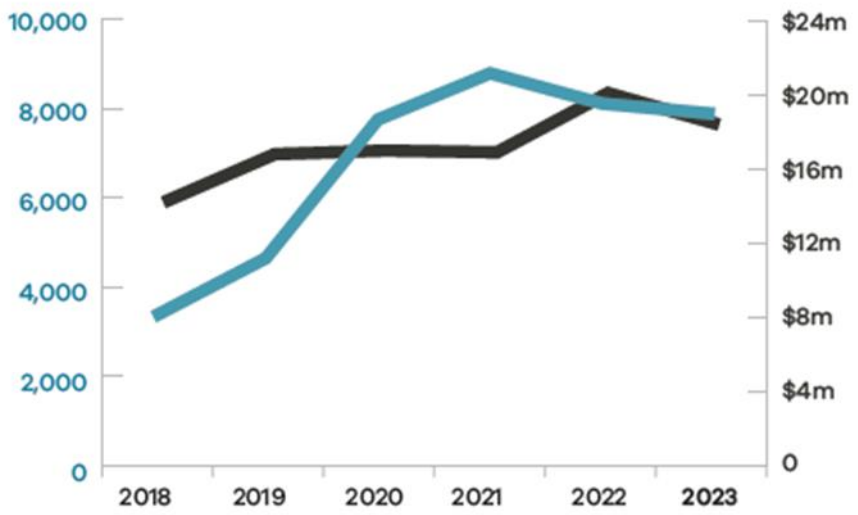
Finger Print: 0A71 3343 F7E2 A8D7 09FA A71E 9ED3 D110 ECCB 2102

CERT NZ

Computer Emergency Response Team New Zealand

1. Highlights of 2023

- In 2023, a total of 7,935 incidents were reported to CERT NZ, a 3% decrease in 2022. There was a total of $18.3million in financial loss reported to CERT NZ in 2023.



- CERT NZ launched a new Cyber Security Awareness Programme, Own your Online. Own Your Online is a new website that helps individuals and businesses understand the online world by explaining common cyber threats and providing practical cyber security advice.
- CERT NZ's key annual awareness-raising activity, Cyber Smart Week, was held for the seventh year running, on 30 October to 5 November 2023.
- CERT NZ was integrated into the National Cyber Security Centre in August 2023, with the view to create a new lead operational cyber security agency for New Zealand.

2. About CERT NZ

2.1 Introduction

CERT NZ is New Zealand's Computer Emergency Response Team, and works to support businesses, organisations and individuals who are affected (or may be affected) by cyber security incidents. CERT NZ provides trusted and authoritative information and advice, while also collating a profile of the threat landscape in New Zealand. See www.cert.govt.nz for more information.

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

2.2 Resources

In 2023 CERT NZ was integrated into the National Cyber Security Centre (NCSC) in New Zealand. CERT NZ has 36 FTEs, including operations, communications & engagement, governance & analytical reporting staff. CERT NZ also has a contact centre to receive incident reports.

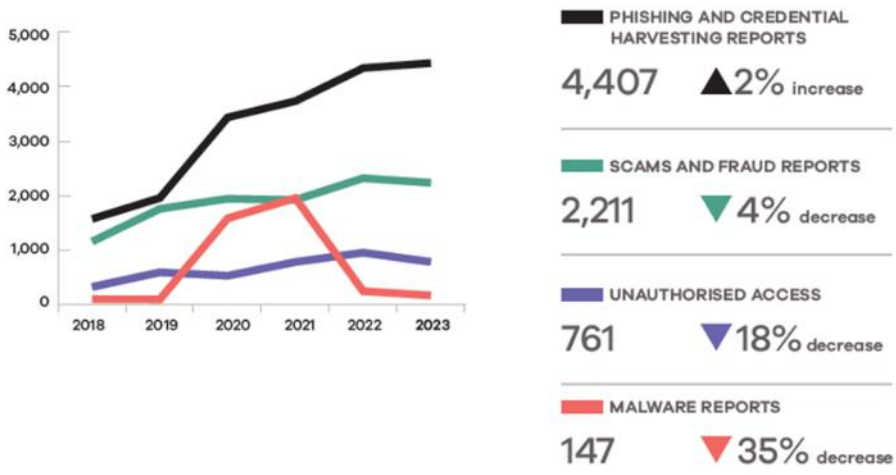
3. Activities & Operations

3.1 CERT NZ's key services are:

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

3.2 Top incident categories

Phishing and Credential Harvesting remains the top reported incident category with a slight increase in report in 2023. The three other top incident categories are "Scams and Fraud", "Unauthorised Access" and "Malware reports" which all saw a decrease in 2023 compared to 2022.



Of the reports received by CERT NZ in 2023 24% included a direct financial loss, with a combined total of $18.3 million.

3.3 Publications

CERT NZ continued their quarterly reporting, with the publication of the Cyber Security Insights report:

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

CERT NZ joined a number of international partners in publishing a comprehensive guidance on LockBit Ransomware.
https://www.cert.govt.nz/it-specialists/news-and-events/u-s-and-international-partners-release-comprehensive-cyber-advisory-on-lockbit-ransomware/
CERT NZ joined the National Cyber Security Alliance and international partners in taking part in the annual Oh Behave Research report, allowing us to understand how the New Zealand public rate internationally in their cyber security behaviours.

CERT NZ also joined international partners in publishing a new guidance for software manufactures on memory safety roadmaps.
With the emergence of AI CERT NZ published a Threat Report on the use of AI to target regional and culturally significant language groups.
https://www.cert.govt.nz/assets/Threat-Reports/CERT-NZ-Threat-Report-AI-and-RCS-Languages-TLP-CLEAR.pdf
2023 saw CERT NZ continue to review their critical controls, designed to help businesses and security professionals decide where best to spend their time and money.

https://www.cert.govt.nz/assets/Uploads/documents/cert-nz-critical-controls-2023.pdf

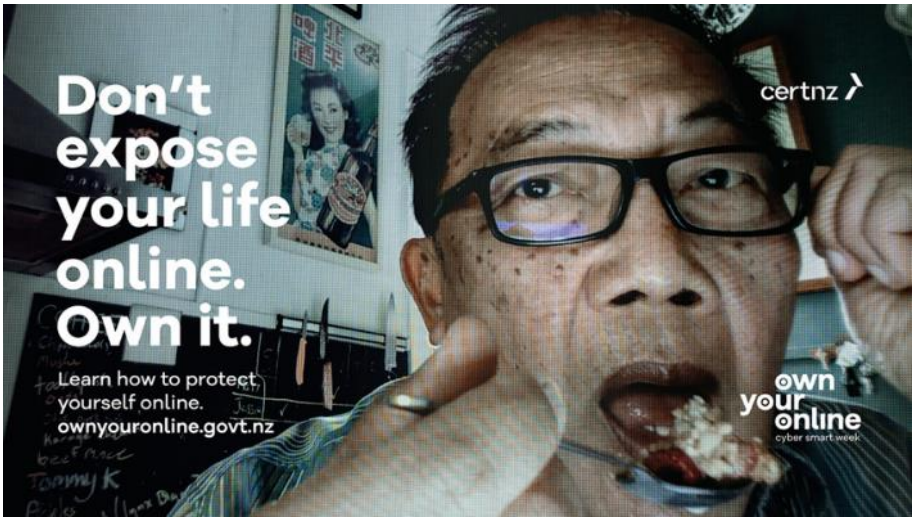
3.4 Social Media

CERT NZ launched new Instagram and Facebook accounts for Own Your Online.
https://www.instagram.com/ownyouronline/
https://www.facebook.com/ownyouronline
CERT NZ has continued to build on their use of social media in 2023 as a way to reach our audience. We continue to run on our existing use of Twitter (@CERTNZ) and Facebook page https://www.facebook.com/certnzgovt and CERT NZ LinkedIn page https://www.linkedin.com/company/certnz/

4. Events organized / hosted

4.1 Campaigns

CERT NZ ran its seventh cyber security awareness campaign, Cyber Smart Week, in October/November 2023, which saw the launch of Own your Online. CERT NZ ran a Campaign during cyber smart week titled "Exposed" that tells the stories of 10 New Zealanders who have been targeted by cyber criminals.



https://www.ownyouronline.govt.nz/

The "Exposed" campaign was launched with a photo exhibition where we hosted partners and key media personnel. CERT NZ engaged with 1,200 supporters from across the government and private sectors to share the message around being secure online. The campaign was successful with 19 media stories, 2000 webinar attendees and over 5 million impressions.

5. International Collaboration

5.1 Capacity building

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

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

The menu of BAU activities includes:

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

Responsive programming since January 2023 has included:

- The PaCSON Remote Session Series including guest speakers from international partners.
- Spearheading the development and delivery of the Cyber Smart Pacific annual regional awareness raising campaign.
- In-country training to continue to build the cyber security capacity of our Pacific partners.

5.2 Other international activities

Key International engagements:

- APCERT IoT Working group.
- APCERT annual conference
- PaCSON AGM
- GFCE Annual Meeting
- APNIC 56
- FIRST Annual conference

6. Contact information

Website:

www.cert.govt.nz

Twitter:

@CERTNZ

Facebook:

https://www.facebook.com/certnzgovt

https://www.facebook.com/ownyouronline

LinkedIn

https://www.linkedin.com/company/certnz/

Instagram

https://www.instagram.com/ownyouronline/

By post:

CERT NZ

PO Box 1473

Wellington 6140

By phone (to report an incident):

- In New Zealand, call us on 0800 CERT NZ (0800 2378 69).
- From overseas, call +64 3 966 6295

CERT-PH

Philippines National Computer Emergency Response Team

1.Highlights of 2023

1.1 Summary of major activities

HackforGov: CERT-PH Cyber Challenge 2023

Following its initial conduct in 2019, this year's main goal is to increase the pace of developing cyber-proficient students in the Philippines and engage them to take a path in cybersecurity. The HackForGov is also a great avenue to identify qualified students as Philippine representatives for international capture-the-flag competitions.

1.2 Achievements & milestones

Inauguration of the Annual Philippine CERT Conference (CERTCON)

A dynamic and comprehensive event that simultaneously hosted four (4) activities, each contributing significantly to enhancing cybersecurity awareness, preparedness, and resilience in the Philippines. These activities encompass the Philippine National CERT Forum, the Setting-up CERT Workshop, the CERT-PH Cyber Incident Drill (CCID) 2023, and the National Cyber Drill (NCD) 2023.

2. About CSIRT

2.1 Introduction

The National Computer Emergency Response Team (NCERT) is a division under the Cybersecurity Bureau of the Department of Information and Communications Technology (DICT). Under Section 15 of the Republic Act 10844, NCERT was established simultaneously with the other programs and projects of DICT. Section 1 of the DICT Department Circular 003 series of 2020 established NCERT as the National CERT of the Philippines and shall be known as the Philippine National Computer Emergency Response Team (CERT-PH).

CERT-PH is responsible for receiving, reviewing, and responding to computer security incident reports and activities. This division also ensures that a systematic information gathering/dissemination, coordination, and collaboration among stakeholders, especially computer emergency response teams, are maintained to mitigate information security threats and cybersecurity risks.

By conducting seminars and events to organizations, CERT-PH provides knowledge and awareness about the threats of cyber-related incidents and the importance of establishing CERTs by replicating the established processes, procedures, and protocols of CERT-PH, as well as making the necessary improvements and configurations to conform to the needs and requirements of their organization as far as applicable.

2.2 Establishment

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

2.3 Resources

CERT-PH, as of this writing, has 45 full-time staff. The operational funding comes from the Department of Information and Communications Technology – Philippines.

2.4 Constituency

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

3. Activities & Operations

3.1 Scope and definitions

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

3.1.1 Cyber Incident Response Section

- Respond to Cybersecurity incidents reported to the Bureau (internal and external to the Department).
- Monitor the implementation of the information security incident response plan to ensure that detected and

reported incidents are given appropriate immediate action.

- Develop well-structured processes for handling and managing information security events and enabling tools, methodologies, and practices.
- Provide ongoing training to incident response teams, ensuring they are well-equipped to handle diverse cybersecurity challenges.
- Foster collaboration and knowledge-sharing among different departments to enhance the overall incident response capability.
- Maintain transparent and effective communication with internal and external stakeholders during incident response efforts.
- Develop standardized reporting mechanisms for incidents, ensuring accurate and timely communication to relevant parties.

3.1.2 Cybersecurity Assessment and Testing Section

- Conducts vulnerability assessment, penetration testing, and source code assessment to ensure the system's security, and integrity of government agencies and instrumentalities.
- Evaluation and identification of cyber security loopholes and system deficiencies that can lead to major cyber attacks.
- Provide government agencies with solutions and provide recommendations on the assessed systems.
- Provide timely reports based on the provided services.
- Develop vulnerability assessment, penetration testing, and source code assessment plan for a systematic approach to conducting the VAPT services.

3.1.3 Cyber Threat Intel and Monitoring Section

- Develop and implement policies and procedures that improve the accuracy and effectiveness of threat monitoring.
- Ensure that all data collection and analysis processes comply with relevant laws, regulations, and best practices for data privacy and security.
- Establish and maintain relationships with external partners or stakeholders to stay up to date on emerging threats and best practices.
- Usage of various cybersecurity platform for the proactive monitoring of possible cyber-attacks internally and externally
- Collaborate with other departments to implement new security measures or enhancements.
- Preparation and issuance of cyber threat feeds and cyber security advisories
- Provide timely reports based on the provided services.

3.1.4 National Security Operations Center Section

- Manage and operate the National Security Operations Center (NSOC). Responsible for monitoring, detecting, analyzing, responding, remediating and information sharing of computer security incidents connected to the NSOC.
- Conducts regular network monitoring security testing, source code analysis, vulnerability and risk management, and escalation and resolution of cybersecurity related incidents; and

- Monitors the system for possible information security threats and injects countermeasures and remedies.[

3.2 Incident handling reports

From January 1 to December 31, 2023 CERT-PH responded and handled 100% of all the 1,834 reported and monitored cybersecurity incidents within the desired response timeframe.
Figure 1 displays the breakdown of incidents based on category.

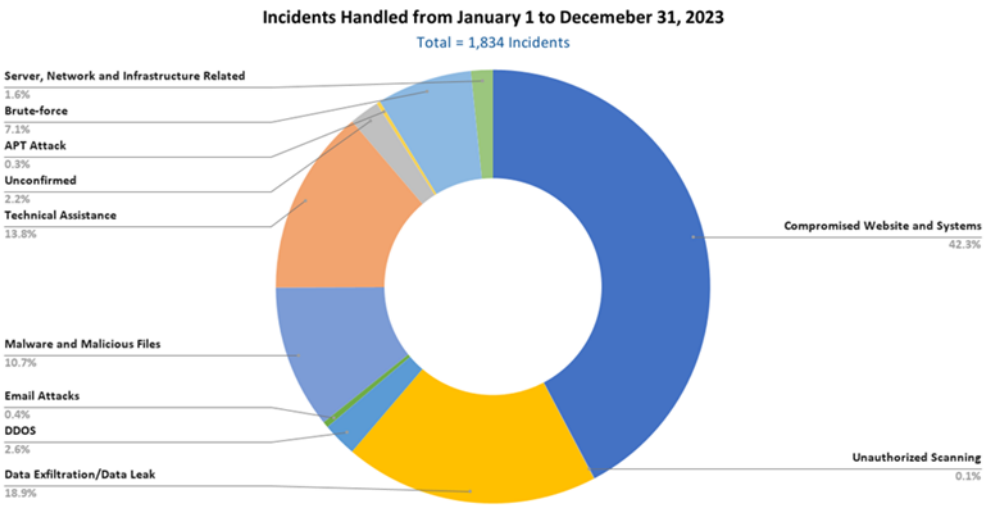


Figure 1

The figure below, on the other hand, displays the sectoral distribution of all attacks monitored and handled by the CERT-PH. As shown in the figure, agencies under the Government and Emergency Services sector have been the most popular target of cyberattacks.

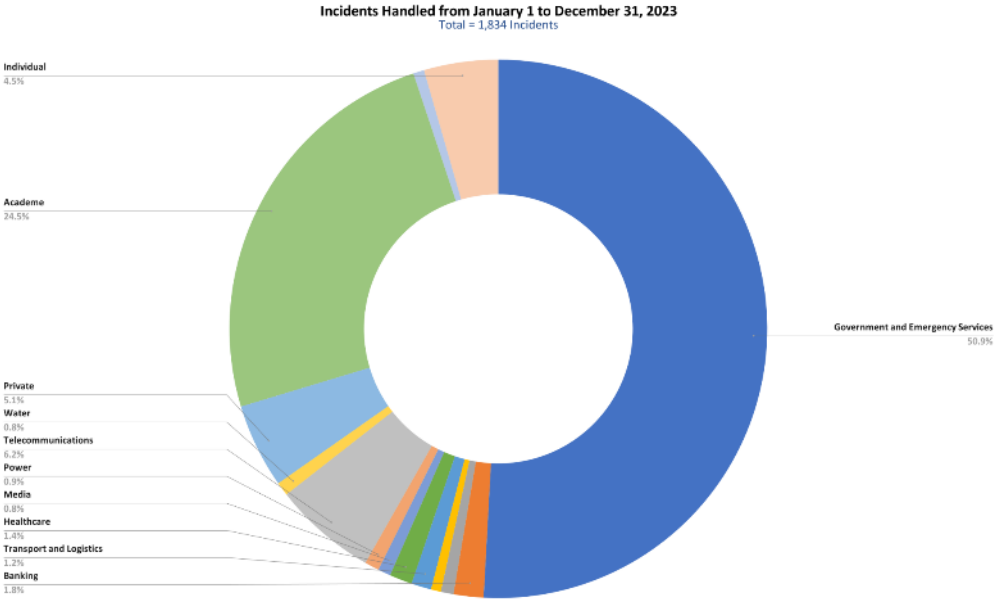
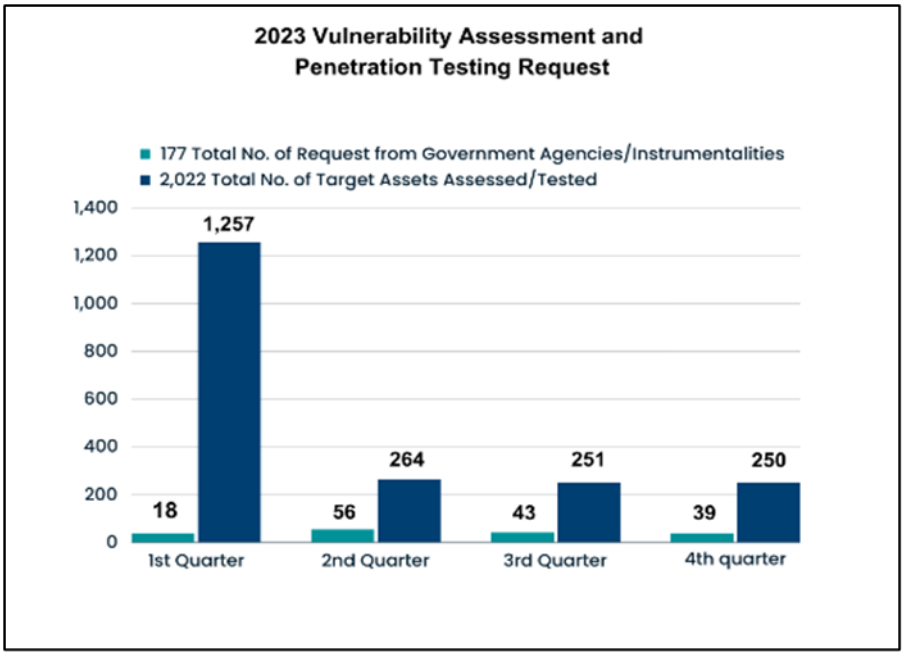


Figure 2

3.3 Vulnerability Assessment and Penetration Testing

	1st Qtr	2nd Qtr	3rd Qtr	4th Qtr	Total
No. of Requests from Government Agencies/Instrumentalities	39	56	43	39	177
No. of Target Asset/Systems Assessed/Tested	1,257	264	251	250	2,022

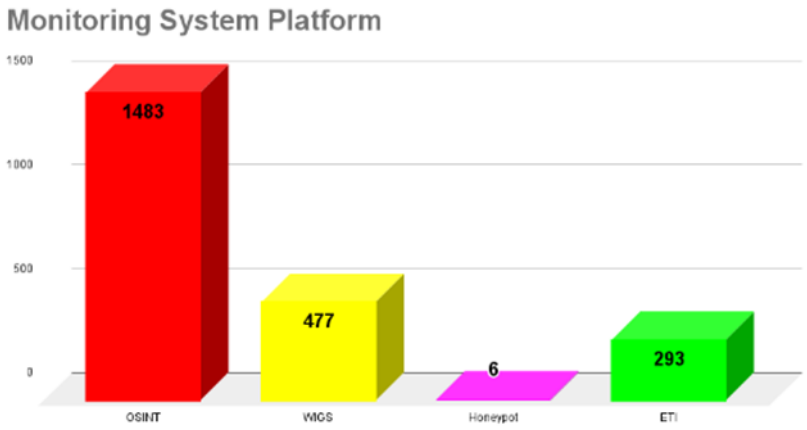


For the year 2023 (January-December), the CERT-PH has received and accommodated a total number of 177 requests from various Government Agencies and Instrumentalities.

Of these requests, vulnerability assessment and penetration testing services were conducted to a total of 2,022 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.

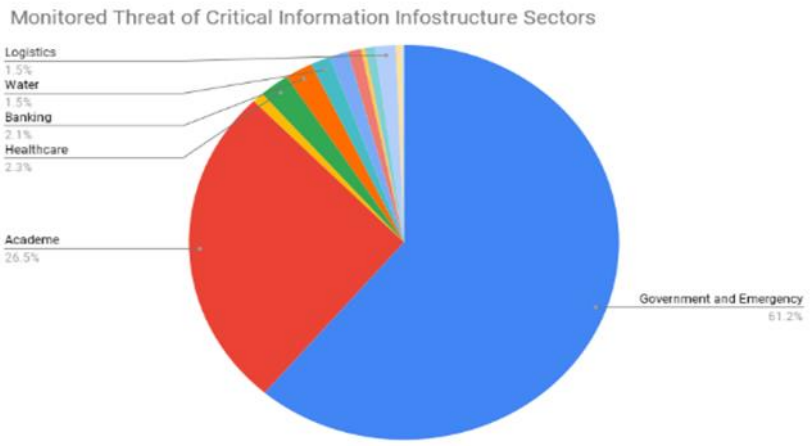
3.4 Cyber Threat Monitoring and Information Sharing

From January to December 2023, a total of 2,259 Monitored Threats were created. CERT-PH through the Web Information Gathering System (WIGS) has monitored 477 threats, while the External Threat Intelligence System (ETI) has 293 monitored threats. Those monitored through Open Sources account for 1483 monitored threats. Lastly, the CERT-PH monitoring team, through the use of Honeypot, a tool that shows how attackers work and examines different types of threats, has monitored 6 threats.



Number of Monitored Reports using Various Platforms

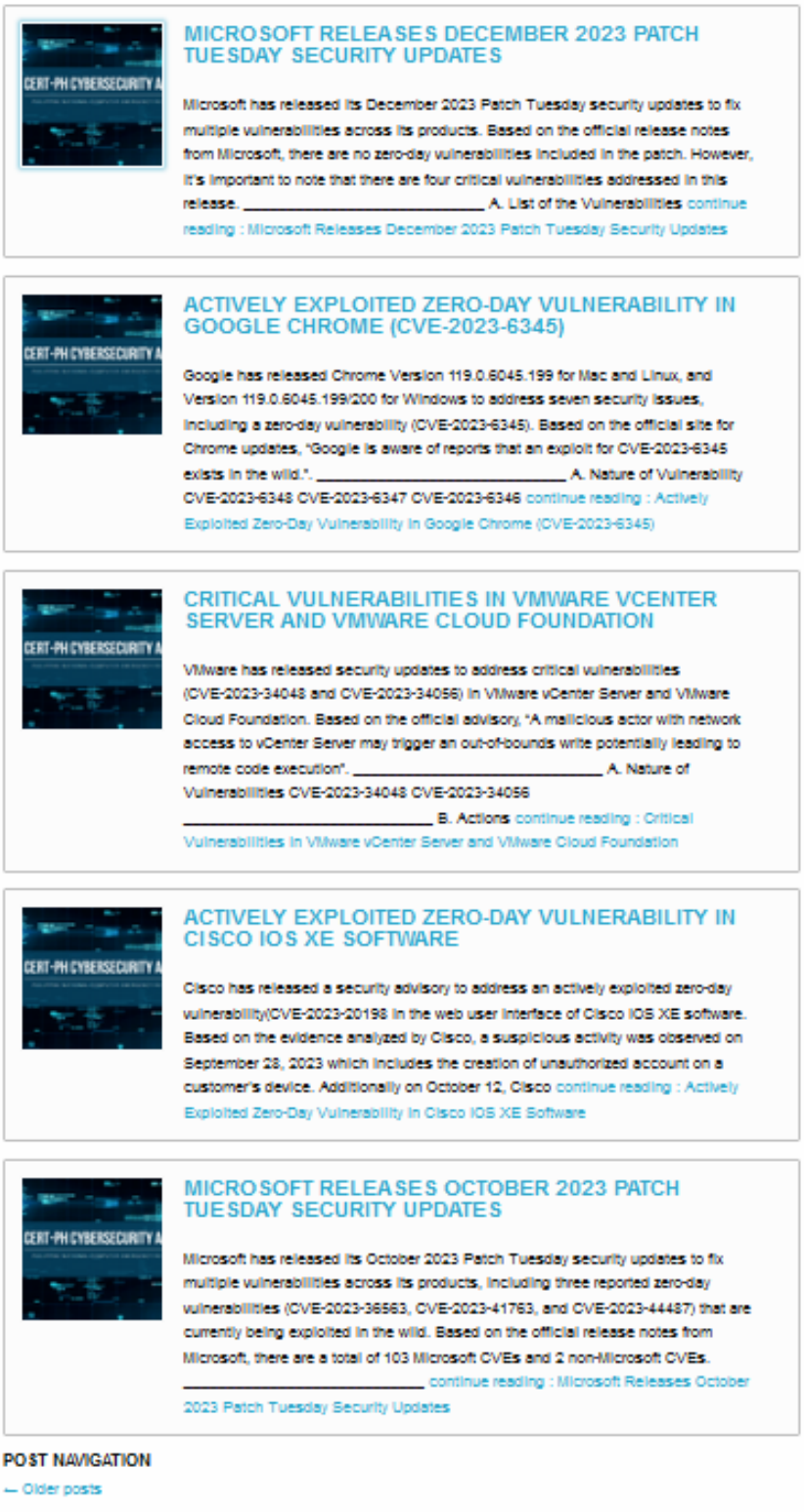
Based on CERT-PH Monitoring Systems, the Government and Emergency Services which includes NGAs, LGUs GOCCs, and instrumentalities have a large number of monitored threats which accounted for 61.2% of the total monitored threats. Various monitored threats reported such as vulnerabilities, malware, alleged data leaks, and website defacement were either reported or escalated to the Incident Response Section.



Monitored Threats of CII (January to December 2023)

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. From January to December 2023, CERT-PH issued:

- 239 Cyber Threat Feeds
- 20 Security Advisories for Public



MICROSOFT RELEASES DECEMBER 2023 PATCH TUESDAY SECURITY UPDATES

Microsoft has released its December 2023 Patch Tuesday security updates to fix multiple vulnerabilities across its products. Based on the official release notes from Microsoft, there are no zero-day vulnerabilities included in the patch. However, it's important to note that there are four critical vulnerabilities addressed in this release. _____ A. List of the Vulnerabilities continue reading : Microsoft Releases December 2023 Patch Tuesday Security Updates

ACTIVELY EXPLOITED ZERO-DAY VULNERABILITY IN GOOGLE CHROME (CVE-2023-6345)

Google has released Chrome Version 119.0.6045.199 for Mac and Linux, and Version 119.0.6045.199/200 for Windows to address seven security issues, including a zero-day vulnerability (CVE-2023-6345). Based on the official site for Chrome updates, "Google is aware of reports that an exploit for CVE-2023-6345 exists in the wild.". _____ A. Nature of Vulnerability CVE-2023-6348 CVE-2023-6347 CVE-2023-6346 continue reading : Actively Exploited Zero-Day Vulnerability in Google Chrome (CVE-2023-6345)

CRITICAL VULNERABILITIES IN VMWARE VCENTER SERVER AND VMWARE CLOUD FOUNDATION

VMware has released security updates to address critical vulnerabilities (CVE-2023-34048 and CVE-2023-34056) in VMware vCenter Server and VMware Cloud Foundation. Based on the official advisory, "A malicious actor with network access to vCenter Server may trigger an out-of-bounds write potentially leading to remote code execution". _____ A. Nature of Vulnerabilities CVE-2023-34048 CVE-2023-34056 _____ B. Actions continue reading : Critical Vulnerabilities in VMware vCenter Server and VMware Cloud Foundation

ACTIVELY EXPLOITED ZERO-DAY VULNERABILITY IN CISCO IOS XE SOFTWARE

Cisco has released a security advisory to address an actively exploited zero-day vulnerability(CVE-2023-20198 in the web user interface of Cisco IOS XE software. Based on the evidence analyzed by Cisco, a suspicious activity was observed on September 28, 2023 which includes the creation of unauthorized account on a customer's device. Additionally on October 12, Cisco continue reading : Actively Exploited Zero-Day Vulnerability in Cisco IOS XE Software

MICROSOFT RELEASES OCTOBER 2023 PATCH TUESDAY SECURITY UPDATES

Microsoft has released its October 2023 Patch Tuesday security updates to fix multiple vulnerabilities across its products, including three reported zero-day vulnerabilities (CVE-2023-36563, CVE-2023-41763, and CVE-2023-44487) that are currently being exploited in the wild. Based on the official release notes from Microsoft, there are a total of 103 Microsoft CVEs and 2 non-Microsoft CVEs. _____ continue reading : Microsoft Releases October 2023 Patch Tuesday Security Updates

POST NAVIGATION

← Older posts

Some of the Issued CERT-PH Security Advisories in 2023

4. Events organized / hosted

4.1 HackforGov: CERT-PH Cyber Challenge 2023

MANILA – As part of the global celebration of Cybersecurity Awareness Month, the Department of Information and Communications Technology through its Cybersecurity Bureau – Philippine National Computer Emergency Response Team (CSB CERT-PH) successfully pulled off the Finals of the HackforGov 2023 Capture-the-Flag Competition on October 16, 2023 at the Manila Grand Opera Hotel and Casino, Sta. Cruz Manila.

Eyes were on the prize as twenty (20) teams from different academic institutions all over the country engaged in a battle of cyber prowess and vied for the most sought-after and prestige title of HackforGov 2023 National Champion. The competition came about with the participation of four-person teams who emerged as front-runners during the series of regional qualifying rounds carried out from August to October 2023 throughout the country.

With the theme "Building Cyber Champions: Stronger Nation through Cyber Awareness and Action", the cyber challenge is primarily designed to raise the level of awareness among students on the importance of cybersecurity and provide them with hands-on experience in various techniques used in the virtual world. The competition format is capture-the-flag (CTF) where participants diligently showcased their exceptional skills in solving a series of cybersecurity-related challenges in areas such as cryptography, web security, and network security, among others.

Team AdDU from the Ateneo de Davao University bagged the hard-earned National Championship after garnering a total of 1600 points and besting nineteen (19) teams during the one-day laborious battle.

Team AdDU has recently raised the Philippine Flag in the international CTF stage by representing the country in the recently concluded ASEAN - Japan Cybersecurity Capacity Building Centre (AJCCBC) Cyber Sea Games in Bangkok, Thailand; and 1st ASEAN CyberShield (ACS) Hacking Contest (ACS CON) in Jakarta, Indonesia, both held on November 2023. Moreover, top performing individuals from various schools and regions consist of Saint Columban College, University of San Jose Recoletos, CARAGA State University and Cebu Institute of Technology University were also recognized and conferred with Performance Excellence Award thereby producing a new team who had taken their talents overseas as they were also the country's flag bearer at the 1st ACS CON alongside Team AdDU.

HackforGov serves as a way for the DICT CERT-PH to engage with the future generation of cybersecurity professionals and encourage them to consider careers in the field. It similarly provides a unique opportunity for students to learn from experts, network with peers and develop critical thinking and problem-solving skills. DICT understands the dire need to elevate the status of cybersecurity in the country and look forward to more activities in the future encouraging more participation and involvement among its stakeholders. By the same token, exposure to competitions like the HackforGov not only sparks interest among the students in various areas of cybersecurity but also enhances understanding, leading to the discovery of new approaches in many areas of the digital landscape.

4.2 CERT Security Essentials Training

Back-to-back with the conduct of the HackforGov, the CERT-PH also conducted the CERT Security Essentials Training from August to October 2023 in all regions across the country to provide individuals and organizations currently working for a CERT and those with interest in establishing a CERT with the information, skill requirements, capabilities, and resources necessary to effectively respond to cybersecurity occurrences. It is a continual process that aids organizations in enhancing their cyber security posture and CERT's effectiveness thereby making them more prepared and equipped for future security.

The training enables participants to understand how CERT undertakes processes of investigations, containment and mitigation of cyber incidents, and application of preventative measures to avoid future accidents. In addition, it facilitates the alignment of the CERT's operations with the organization's broader security strategy where the following module were used depending on the region's need and request:

MODULE/ TITLE	SCOPE	MODE OF INSTRUCTIONS
Introduction to CERT-PH Services and training programs	Objectives CERT-PH services CERT-PH yearly Events Ladderized training Programs	Lecture / discussions
Latest Cyber Threat Landscape of the Philippines	Incident detected, reported, and handled Common Cyber threats and its definition	Lecture / discussions
Review of Setting up CERT	Definition of CERTs Setting UP CERT requirements	Lecture / discussions
Incident Response Concepts	IR Lifecycle Basic IR Tools	Lecture / discussions

Securing the CERT Environment	Establishment of Security Zone for CERT Cybersecurity Awareness for CERT Workforce	Lecture / discussions
Deep Dive to CERT operations	SOC Operations Vulnerability Management Incident Response Handling & Reporting Procedures Handling of Incident types recorded by CERT-PH Cyber-Attack Countermeasures Threat Monitoring and Information Sharing	Lecture / discussions
Security / CERT Tabletop	1-3 cyber-Scenarios	Lecture / discussions & group participation
Q&A	Question and Answer Portion	

4.3 Seminars/ Presentations

Country / Region	Event	Date
Tesda Office, Taguig	Cybersecurity Awareness and Orientation Program, TESDA (Resource Speaker)	September 11, 2023
Camp Crame	Cybersecurity Seminar (Resource Speaker)	September 27, 2023
PNP - ITMS	Cybersecurity Seminar	October 05, 2023
Online (Zoom)	Coordination Meeting with PNP and DICT Region 2 (Resource Speaker)	October 11, 2023
Hive Hotel, QC	CICC's Peer Review Digital Forensics Manual Draft (Reviewer)	October 12-13, 2023
Pampanga	DILG Cybersecurity CERT Training & Workshop (Resource Speaker)	October 11-12, 2023
Online (Zoom)	Cybersecurity Awareness Month DICT Region 12 & Mainland BARMM (Resource Speaker)	October 19, 2023
Online (Zoom)	6th Cyber Defense Exercise (Resource Speaker)	October 23, 2023
Manila Police District Headquarters	Sub-Committee on Counterintelligence, RIC-NCR (Resource Speaker)	October 25, 2023
Online (Zoom)	DTI Webinar on NCSP 2023 - 2028, NCERT and PNPKI	October 20, 2023

	(Resource Speaker)	
	DOJ Cybersecurity CERT Training (Resource Speaker)	October 25, 2023
	DENR Cybersecurity Campaign Program (Resource Speaker)	October 19-20, 2023
Online	Webinar on the Implementation of the NCSP 2023-2028 and the NCERT (DTI)	October 20, 2023
Crown Plaza	Stepping Ahead of Ransomware: Preventing Imminent Attacks (Trend Micro)	October 24, 2023
Online	Foundation on CERT Operations Training (Resource Speaker)	October 25-26, 2023
Online	Mariano Marcos Memorial Hospital and Medical Center (MMMHC)	November 9, 2023
DHSUD Hall	DHSUD Cyber Security Awareness Month 2023	November 15, 2023
Online	Sandiganbayan Cybersecurity Awareness Webinar	November 29, 2023
Eastwood Richmonde Hotel, Quezon City	Philippine CERT Conference (CCID 2023, NCD 2024, Setting-up CERT Workshop, Philippine National CERT Forum, Plenary Talk)	December 6, 2023
Intramuros	Bureau of Immigration's Cybersecurity Awareness Seminar & Personal Cybersecurity	December 7, 2023
Pasig City	NSOC Product Training with Philcox and Comclark	December 11, 2023
PNP Headquarters Camp Crame	Cybersecurity : Incident Response Training	December 14, 2023

4.4 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 12 sessions, brought together a diverse group of 61 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.

4.5 Philippine CERT Conference (CERTCON) 2023

The DICT through its Cybersecurity Bureau - CERT-PH, springboarded a significant milestone with the grand launching of the Philippine CERT Conference (CERTCON) on December 4-6, 2023. Regarded as the first-ever CERTCON, the three-day conference underscores a decisive leap toward fostering collaboration, knowledge sharing, and the advancement of best practices within the dynamic realm of cybersecurity and the significance of Computer Emergency Response Teams (CERTs) in the country.

On its opening day, the conference welcomed more or less 200 attendees emanating from 67 government agencies and relevant stakeholders including representatives from the Critical Information Infrastructures (CIIs). These comprise the sectors of Government and Emergency services, Banking, Business Process Outsourcing, Financial, Healthcare, Energy, Transport and Logistics, Telecommunications, Water & Power. The event's primary objective was to provide a dynamic platform for the cybersecurity industry, both public & private, to connect, exchange ideas, network & build stronger relationships with their colleagues, & representatives from diverse entities.

Filled with exciting and multifaceted sessions, the second day was partaken by a total of 139 attendees from 64 agencies while the third and concluding day recorded around 135 participants from 55 various organizations. As a dynamic and comprehensive event, the CERTCON 2023 encompasses four key activities carried out concurrently, each contributing significantly to enhancing cybersecurity awareness, preparedness, and resilience in the Philippines. Breakout sessions stirred up the participants' skills and knowledge as they take on several drills and exercises tailored fit to heighten their cybersecurity awareness, to wit:

Philippine National CERT Forum

A vital forum for established and operational CERTs/CSIRTs from various organizations in the Philippines. Representatives from various organizations with established and operational CERTs/CSIRTs were convened for the first time to discuss and exchange pressing issues and concerns they come across and have been encountering during the process of establishing their CERTs up until now that they already have an existing one. Mitigating measures and recommendations were also raised and will be taken into consideration by the DICT for the future conduct of similar activities.

Setting-up CERT Workshop

An activity focused on the concepts, establishment, and operation of a CERT. It entails providing individuals currently working for a CERT and those with interest in establishing a CERT with the information, skill, requirements, capabilities, and resources necessary to effectively respond to cybersecurity occurrences.

CERT-PH Cyber Incident Drill (CCID) 2023

Around 67 agencies actively played their part as they delved to this drill aimed at strengthening the Critical Information Infrastructures (CIIs) cybersecurity awareness and principles. CCID primarily aims to solidify the CII's knowledge and principles in keeping their organization secure; simulate a real-life cyber incident; and evaluate their cyber response capabilities and preparedness. The sessions were conducted and divided into sectoral groups as follows:

> Day 2

- AM session - Government and Emergency Services
- PM session - Healthcare and BPO

> Day 3

- AM session - Financial, Banking and Transport and Logistics
- PM session – Water, Power, and Telecommunications

National Cyber Drill (NCD) 2023

An activity geared towards raising awareness and understanding of fundamental cybersecurity principles among the general public. Through a creative and multilayered approach, the NCD allowed the participants to strategically engage themselves in an interactive story-based learning path centered on the existing and emerging cyber incidents in the country.

With the initiative of carrying out an event to convene cybersecurity professionals and enthusiasts across the country in a series of activities combined in one setting, distinguished experts and speakers were likewise invited in the conference to share their expertise, experiences and know-how on various topics related to cybersecurity operations, policies, legalities, technologies, and other relevant matters. Moreover, event partners from different industries were also present in the conference taking advantage of the opportunity to network with potential clients as they showcase their products and services to the conference's audience.

Taking cognizance of the need to regularly gather the cybersecurity professionals and enthusiasts especially the CERTs in the country, the CERT-PH fully understands the necessity to hear the industry and look into the long-term and emerging issues, innovations, and possible partnerships in the near future. This is a one vital step towards the CERT-PH's commitment of promoting the relevance of CERTs nowadays as an instrumental initiative in bolstering the relationship with other CERTs globally.

Ultimately, the DICT looks forward to the involvement of the general public to more similar activities in the ensuing years to ensure the continuity and annual conduct of CERTCON while strengthening the collaboration with both the public and private sector in so doing driving into the notion of providing the stakeholders with not what the government wants but more on what they really need.

5. International Collaboration

5.1 Capacity building

5.1.1 Conferences & Trainings

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

Country / Region	Organization	Event	Date
Tokyo, Japan	ASEAN-Japan	13th ASEAN-Japan Information Security Workshop for ISPs	25-28 January 2023
Kuala Lumpur, Malaysia	U.S. Department of State, Office of Weapons of Mass Destruction Terrorism	Technical Training under Phase Two of Building Technical Capacity of Law Enforcement to Conduct Cyber-Enabled Investigations	13-17 February 2023
Osaka, Japan Tokyo, Japan	Japan International Cooperation Agency	JICA KCCP GRF Strengthening of Cooperation Among Organizations Against Cyberattacks	14-22 February 2023

	(JICA)		
Sofitel Manila	APRICOT	Asia Pacific Regional Internet Conference on Operational Technologies (APRICOT) 2023	February 27-March 2, 2023
Online	FIRST / AfricaCERT	2023 FIRST & AfricaCERT Symposium: Africa and Arab Regions	February 28-March 3, 2023
Tagaytay City	ASEAN-Japan	2023 1st ASEAN-Japan Cybersecurity Policy/ Working Group Meeting	14-15 February 2023
Diamond Hotel Manila		Australia National University Philippines Cyber Resilience Workshop 2023	March 29-30, 2023
Online	Cisco	Cisco Cyber Range Training - Host Triage Forensics	April 26-28
Shangri-La the Fort, Philippines		Energy Sector Cybersecurity Workshop - Enhancing Energy Resilience through a Cybersecurity Assessment Framework	April 24 - 26 2023
Quezon City		Cybersecurity Workforce Workshop	April 18-20, 2023
Online	Interpol	Intermediate Malware Analysis Training (Interpol)	April 17-21, 2023
Online		APO: Cybersecurity Management System	May 16-19, 2023
Pasig, Manila	Interpol	Interpol Advanced Malware Analysis	June 26 - June 30 2023
Online		STCOM CYBER OSINT/SOCMINT TRAINING	June 22-23, 2023
Online		ICVR "Non - Fungible Tokens (NFT) - Implications for Law Enforcement	June 21, 2023
Online	ASEAN	ASEAN Regional Forum Workshop on Terminology in the Field of Security of and in the Use of ICTs in the Context of Confidence Building	June 21, 2023
Online		Data Visualization using Tableau: Tableau Challenge	June 19-20, 2023
Online		INVITATION: SOP-EWBS Public Consultation	June 15, 2023

Online		Cyber Bitrange - Stockholm	June 5, 2023
Online		Cyber Bitrange - Stockholm	June 9, 2023
Montreal, Canada	FIRST	35th Annual FIRST Conference and 18th National CSIRT Meeting	May 31-June 13 2023
Bangkok, Thailand		Cybersecurity Evaluation Tool	July 10-13, 2023
Seoul, South Korea	Cybersecurity Alliance for Mutual Progress (CAMP)	8th Annual Meeting of the CAMP	July 11-13, 2023
National Intelligence Coordinating Agency		Cybersecurity Offensive Training	July 6, 19, 27
Bali, Indonesia		Regional Capstone Forum on Building Law Enforcement Capacity to Conduct Cyber-Enabled Investigations to Counter WMD Terrorism	August 9-10, 2023
Kuala Lumpur, Malaysia		8th Digital Forensic Expert Group	August 15-17, 2023
Manila		ThreatSpace Workshop: Cyber Capacity Building for Highly Trafficked Ports by CRDF	August 22-25, 2023
Penang Malaysia / Online		Launch Meeting of the Regional Expert group for Malware Analysis REG-MA - Interpol	August 29-30
Taguig City	Cybercrime Investigation and Coordinating Center (CICC)	Cybersphere Philippines 2023	September 5-6, 2023
Manila		Digital Forensics Training	September 8, 2023
Online		2023 APT Landscape Unveiled: Trends, Challenges, Solutions	September 12, 2023
Makati City		Philippine Anti-Terrorism Council Tabletop Exercise	September 15, 2023
Pasay City		Map, Analyze, and Develop a Modernization Plan for the Philippines' Bio Enterprise Information Infrastructure	October 3 - 5, 2023

Taguig City	ISOG	ISOG I AM SECURE 2023 CONFERENCE	October 26, 2023
DICT CO	DICT Cybersecurity Bureau- CERT-PH	CyberRange Exercises of DICT and AFP	October 27, 2023
Online	CSA Singapore	ASEAN CERT Incident Drill (ACID)	October 18-19, 2023
Thailand	ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC)	27th AJCCBC Cybersecurity Technical Training	October 16-20, 2023
Brussels, Belgium	EU	The Role of the EU Ecosystem in Global Cybersecurity Stability - European Security and Defence College	November 5-11, 2023
Dusit Thani, Makati	Intelligence-Sec	Cyber Intelligence Asia 2023	November 29-30, 2023
Red Hotel, Quezon City		Basic Customer Service Skills	November 7-8, 2023
Novotel hotel, Cubao	Institute of Electronics Engineers of the Philippines (IECEP)	IECEP 73rd Annual General Membership Meeting and Convention	November 23-25, 2023
Eastwood Richmonde Hotel, Quezon City	DICT Cybersecurity Bureau- CERT-PH	1st Philippine CERT Conference (CERTCON)	December 04-06, 2023
Pasig City	Trend Micro	Product Training with Philcox and Comclark	December 11, 2023
Online	DICT	MEETING/TRAINING Designated focals for answering phone calls and addressing public feedback and complaints	December 18, 2023
Bangkok, Thailand	ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC)	28th AJCCBC Cybersecurity Technical Training – J4 Trainer Training on Network Forensics	December 18-22, 2023

5.1.2 Drills & exercises

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

Country / Region	Organization	Event	Date
Online	NCA-ITU	WSIS 2023: NCA-ITU CyberDrill	May 3, 2023
26-27 - Online 28 - at the PAF Multi-Purpose Gymnasium, CJVAB, Pasay City	Philippine Air Force	Philippine Air Force's Cybersecurity Exercise "Castle Siege 2"	July 26-28, 2023
Online	Asia Pacific CERT	APCERT 2023 Cybersecurity Drill	August 16, 2023
Bali, Indonesia	ASEAN-Korea Cooperation Fund - Korea Internet & Security Agency (KISA)	ASEAN Cyber Shield Hacking Contest (ACS CON) Participation	November 21-24, 2023

6. Future Plans

6.1 Future projects

- HackforGov: CERT-PH Cyber Challenge 2024 - April to October 2024
- 2nd Philippine CERT Conference - October 2024

6.2 Future Operation

Implementation of CERT-PH 24/7 Operation

With the upsurging cases of ever-evolving cyber threats and cyber-attacks in the country that can potentially happen to anyone, anytime and anywhere, it is imperative for the DICT to provide continuous and uninterrupted services to address such concerns to be able to improve its incident response capabilities, fulfill its mandate of safeguarding the Philippines' cyberspace and ensure the integrity and security of critical information infrastructure (CIIs). Thus, to effectively and efficiently carry out this function, it is crucial that a 24/7 operation be implemented at the division.

CERT Tonga

Tonga's Computer Emergency Response Team

1. Highlights of 2023

1.1 Summary of major activities

Early last year, the Government of Tonga through its National Critical Infrastructure encountered a major ransomware attack where Cyber Experts from Australia, CERT NZ, CERT Tonga staff and the affected party collaborated to contain and restore the infrastructure services. Another fraud case on ccTLD (".to" DNS) alerted key government ministries and Tonga diplomatic missions abroad were reported to CERT Tonga including several IP abuses, brute force attacks and exploitations of DNS inactive.

1.2 Achievements & milestones

In commemoration of CERT Tonga's establishment under the Ministry of Meteorology, Energy, Information, Disaster Management, Environment, Communications and Climate Change (MEIDECC) on July 15, 2016, CERT Tonga celebrated its 7th Anniversary last year with a Cyber Resilience Week, July 09 – 14, 2023.

CERT Tonga had the opportunity to conduct seventeen (17) cyber awareness and outreach programs to government ministries, departments, and to the outer islands of Tonga. The cooperation with bilateral partners on cybersecurity trainings led CERT Tonga to engage with CERT NZ, ACSC, Trustwave (a cybersecurity detection and response provider under DFAT initiative Cyber Security Services in the Pacific (CSSP)), Table Topic Exercise (TTX) with the United States Institute for Security Governance (ISG) and cybersecurity training with APNIC.

On behalf of the Tongan Government, MEIDECC and the New Zealand Department of Internal Affairs (NZDIA) signed a Partnership Arrangement for the extension of the Digital Child Exploitation Filtering System (DCEFS) for Tonga, August 2023. CERT Tonga is the primary contact in the Ministry of MEIDECC for this initiative.

2. About CSIRT

2.1 Introduction

CERT Tonga is the national body and the main point of coordination for cyber security issues in the Kingdom of Tonga. Operated under MEIDECC, CERT Tonga engaged with domestic – both public and private sectors, regional and international stakeholders within its statutory scope in gathering information, knowledge, and expertise to raise awareness, mitigate threats, while allowing safe developments and usage of digital technologies within Tonga cyberspace.

2.2 Establishment

The establishment of CERT Tonga was based on the Term of References (TOR) endorsed by His Majesty's Cabinet Decision (HM CD, Tonga) on July 15, 2016 with its Board to provide oversight and strategic direction.
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 amended its organizational structure comprising of three divisions. They are as follows:

- Oversight and compliance.
- Coordination and communication
- Vulnerability detection with incident response and forensic analysis

Under this government organization, a Cyber Security Workforce Development Program (CWDP) was also developed with the ongoing support from CERT NZ, allowing CERT Tonga to recruit two staff (Secondment and Internship) to assist in operation. From the usual three established staff (Director, Senior Engagement Officer, and Security Analyst) of CERT Tonga, to five employees now. CERT Tonga also has a volunteer program for young enthusiasts who are willing to gain working experience, apprenticeship, and career in cybersecurity.

2.4 Constituency

CERT Tonga's constituents are Government Ministries, Private Sector, Public Enterprises and Non-government Organizations (NGOs).

3. Activities & Operations

3.1 Scope and definitions

Mandated in the TOR of HM CD, Tonga – July 2016, CERT Tonga aims to:

- Serve as 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 programs for staff
- Conduct incident handling
- Perform vulnerability handling
- Digital evidence handling
- Conducting risk analysis
- Provide security consultant and advice
- Research development
- Provide forensic services

Current operations within the Ministry of MEIDECC:

- **Engagements** – engage with domestic, regional, and international organizations and established committees.
- **Proactive Services** – maintaining proactive services by providing awareness, trainings, security bulletin and advisories to ensure cyber threats and incidents are mitigated.
- **Reactive Services** – provide 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, CERT Tonga also provides digital forensic analysis services to Tonga Police with regards to 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 outputs, and collaboration with the MEIDECC's other departments.

3.2 Incident handling reports

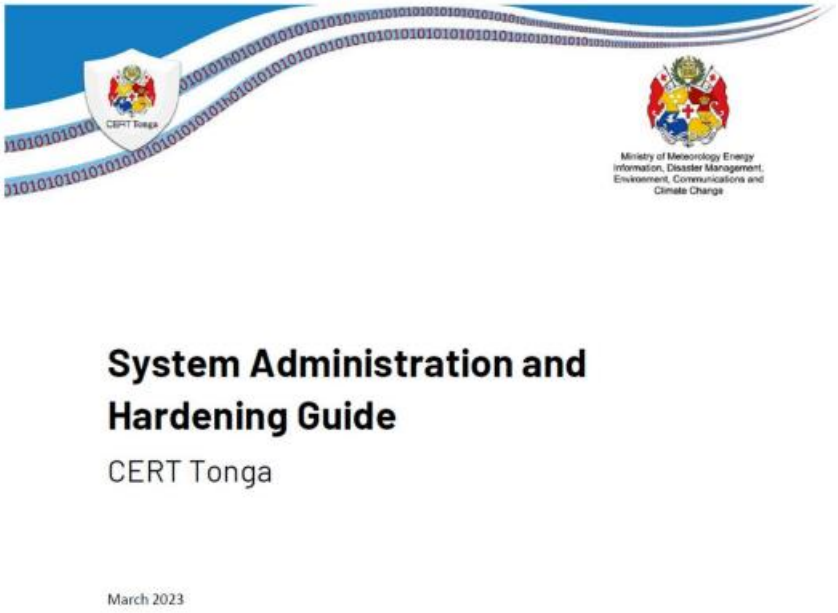
Since 2022 with the reports of the International Revenue Fraud Services on several occasions to the National Critical Infrastructure (ISP), followed by the malicious activities reports with IP addresses for websites and email servers concerning this ISP leads to the early incident of the 2023 Medusa Locker ransomware attack to Tonga's National Critical in February 2023. This was a critical matter for the government with regards to the connection via the infrastructure fiber

optic cables. The Tongan Government then requested assistance to the Australian Government. An emergency response relief team from Australia was dispatched and CERT Tonga led the coordination. In collaboration with the team from Australia (Cyber Experts) concurrently with the scheduled bilateral meeting and training with CERT NZ, generated the first Tonga CSIRT.

Throughout the year, CERT Tonga received occasional reports of malicious IP address activities from third parties scanning services. This includes three IP addresses reported by the FBI (Australia) that were linked to Iranian government-sponsored Iranian malicious cyber activity targeting US big tech companies. Other cases are phishing and fraud from international actors impersonating international CERT with fraud court law orders to takedown ".to" website, while causing a chain of emails between the Tongan diplomatic mission and the government ministries, law enforcement and legal prosecutors. Additionally, scam emails appeared to also increase last year. The DCEFS reports of positive hits for attempts to child exploitations sites is still very minimal.

3.3 Publications

As a result, from the collaboration with the Australian Cyber Experts during the investigation and recovery of the National Critical Infrastructure (ISP), the System Administrators Hardening Guide was composed to assist ISPs and critical infrastructure networks to strengthen their network security.



The partnership with Trustwave initiated a workshop to develop the Information Security Policy with other standard guides' documents to accompany the procedure.

CERT Tonga continued publishing Advisories to assist constituents in resolving common threats and vulnerabilities observed to be exploited in the wild with Monthly Security Bulletins. The circulation of email advisory to constituents is ongoing through mailing list to notify them of any possible attacks or threats detected.

CERT Tonga also utilized the social media platforms (Facebook and X) to spread the word with news events and tips for the public on how to remain safe and secure online. CERT Tonga's website encountered a few technical issues during the second half of last year, which it was reported by the host organization that their webserver was corrupted and most of the data was lost. Hence, CERT Tonga's website was down for a while and the data had to be repopulated to start up the website again.

4. Events organized / hosted

4.1 Trainings

CERT NZ Bilateral Meeting and Cybersecurity Training, February 2023

A successful two-day bilateral meeting was held between CERT Tonga and CERT NZ during the cooperation with the Australian Cyber Experts in assisting one of Tonga's Critical Infrastructure as a victim of a ransomware attack. Following this ongoing collaboration, CERT Tonga and CERT NZ also conducted a three-day in country face-to-face training for system administrators from government ministries, public enterprises, and ISPs.





Trustwave SIEM and MISP Training, March 2023

After almost two years of virtual collaboration with Trustwave under the Cybersecurity services project in the Pacific and Australia's Department of Foreign Affairs and Trade (DFAT), CERT Tonga finally met with Trustwave to configure and install the Security Information and Event Management (SIEM), and Malware Information Sharing Platform (MISP) systems shipped near the end of 2022.

A three-day training was also conducted and was facilitated by Trustwave's Manager Consultant and Specialist Technician on SIEM and MISP systems with the involvement of CERT and Security Operation Center (SOC) in sharing information

and resources to proactively monitor indicators of compromise (IOCs) and mitigate Cyber incidents and Cyber-attacks. The systems were introduced to ISPs, law enforcement and cybersecurity agencies as a platform and next level of cybersecurity measures.

Australian Cyber Security Center (ACSC) Bilateral Pacific Training Package – Tonga, June 2023

The bilateral training offered by the ACSC to the Pacific CERTs was focused on several key areas including Threat Intelligence and Incident Response. The outcomes of this training enhanced CERT Tonga's ability to allocate the incident response resources, comprehend how to appropriately prioritize resources during a cyber-event, map escalation process and mechanism as well as support the comprehensive development of the existing CERT Tonga's incident response and risk management plans. The training was held for five-day, June 26 – 30, 2023 and was facilitated by members from ACSC and CERT Tonga staff.


Commemorating CERT Tonga's 7th Anniversary of establishment with a Cyber Resilience Week, July 09 – 14, 2023

The six-day of activities and trainings this week was to mark CERT Tonga's 7th Anniversary since its establishment. The event commenced with a church service on Sunday, July 09, Cyber training for Tonga Women in ICT (TWICT) on Monday, July 10, followed by a cybersecurity training session for key community leaders on Tuesday, July 11, and Cyber readiness training for system administrators on Wednesday, July 12.

On Thursday, July 13, CERT Tonga hosted a singing and poem competitions for students from Government Middle Schools and High schools on cybersecurity and internet safety with a Capture the Flag (CTF) event hosted by Retrospect Labs from Australia for Tertiary institutes and Tonga Women in ICT (TWICT) and an awareness training to the Legislative Assembly of Tonga. The trainings were facilitated by CERT Tonga and CERT NZ. Final day of the week-event, Friday, July 14 concluded with an exhibition from CERT Tonga's local key partners and prize giving awards to the participating students.

APNIC Cybersecurity Training

APNIC and CERT Tonga facilitated Security Management:

Comprehending Cyber Threats & Defense Training to IT Operators and System Administrators from government ministries, private and public sectors.

4.2 Drills & exercises

Representatives from His Majesty's Armed Forces, Tonga Police, PMO's Digital Transformation Department, Communications Department and CERT Tonga participated in a Cybersecurity Tabletop Exercise (TTX) hosted by the United States Institute for Security Governance (ISG) and Nevada's National Guard State Partnership Program in Nuku'alofa, October 30 – November 01, 2023.


4.3 Conferences and seminars

CERT Tonga attended in the Cyber Safety Pasifika (CSP) Tier 2 Cybercrime Investigation training, facilitated by the Australian Federal Police (AFP), Pacific Asia Command and Tonga Police at Tanoa International Dateline Hotel, October 27 – November 03, 2023.

CERT Tonga also participated in the Pacific Network Operators Group (PacNOG) 32nd Conference, which was also held in Nuku'alofa, November 27 – December 01, 2023. Hosted by Tonga Communications Corporation, CERT Tonga had the opportunity to join the other members from the Pacific Islands Telecommunication Association (PITA) in the event.

5. International Collaboration

5.1 Drills & exercises

5.1.1 Training

Candidate from CERT Tonga completed the Asia-Pacific Telecommunity (APT) Training Course on Cyber Security Technologies – Trend of Risks in the latest and its Countermeasures, hybrid, and face to face attendance in Tokyo, Japan, February 13 – 17, 2023, and was conducted by KDDIF. CERT Tonga's Security Analyst also participated in the E-Evidence First Responder National Trainers Workshop organized by the Council of Europe (CoE) in cooperation with Interpol and the Department of Justice of the Philippines in Cebu, Philippines, November 13 – 24, 2023.

5.1.2 Drills & exercises

CERT Tonga attempted to participate in a drill hosted by APCERT but due to technical difficulties, CERT Tonga was unable to complete the drill. CERT Tonga was also invited to a Fellowship Opportunities for the ITU Europe & Asia-Pacific Interregional CyberDrill in Limassol, Cyprus, November 28 – December 01, 2023 but similar reason to the abovementioned, CERT Tonga did not make it to Limassol, Cyprus.

5.1.3 Seminars & presentations

Representatives from CERT Tonga participated at the 35th Annual Forum of Incident Response Security Teams (FIRST) in Montreal, Canada, June 04 – 09, 2023. CERT Tonga also took part in the session of the "Stories from the Pacific – the human side of cyber incidents" at the Asia Pacific Regional Internet Governance Forum (APrIGF) in Brisbane, Australia, August 29 – 31, 2023.

This includes attended three events in Port Vila, Vanuatu at the same time.

- The Development Cybersecurity Workforce to Enhance National Security Workshop hosted by CISA, September 13 – 15
- Annual General Meeting (AGM) for Pacific Cyber Security Operational Network (PaCSON), September 18 – 20
- FIRST Symposium, September 21 – 22, 2023.

In addition, CERT Tonga also partook in the Pacific Cyber Capacity Coordination Conference (P4C) in Denarau Island in Nadi, Fiji, October 02 – 04, 2023 and the First Global Conference on Cyber Capacity Building (FGC3B) in Accra, Ghana, November 28 – 30.

6. Future Plans

6.1 Future projects

CERT Tonga continues to manage, collaborate, and implement the Cyber Security Workforce Development Program (CWDP) with the intention to develop its own cybersecurity infrastructure to collect data and analyzed for first-hand information in detecting vulnerabilities and threats for the critical infrastructure networks of the Kingdom of Tonga. And because Tonga was also elected to be one of the Hub Countries responsible for the Pacific Region, CERT Tonga and the Cybercrime Working Group formed a National Committee for the GLACY-E project.

6.2 Future Operation

CERT Tonga anticipates working closely with the Internet Corporations for the Assigned Names and Numbers (ICANN) mainly for the governance of the ".to" ccTLD and to be more involved and engaged in the APAC Space and the Asia-Pacific partners.

7. Conclusion

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

CNCERT/CC

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

1. Highlights of 2023

1.1 Summary of major activities

As we reflect on 2023, it's clear that it has been a year marked by meaningful events, where we made our presence in APCERT and the wider community by a series of work done. We successfully hosted several international and domestic conferences, such as the Cybersecurity Forum for Technology Development and International Cooperation, and the 20th CNCERT Annual Conference. Besides, we actively participated in cybersecurity drills, such as APCERT Drill 2023 and ACID 2023. We have made further collaboration with both global and regional partners. Spanning across emergency response, cross-border incident handling and other fields, these are the moments and issues that defined the past 12 months.

1.2 Achievements & milestones

In the past year, CNCERT/CC has fulfilled its responsibility as the Deputy Chair, SC member and convener of Information Sharing Working Group. CNCERT/CC has maintained and promoted the APCERT Data Exchanger platform, with 31 APCERT members having registered and 23 members uploaded their PGP keys. Over 400 reports were shared via this platform in 2023. Meanwhile, CNCERT/CC has continued to improve the "Chatroom" and "Feedback" functions in the platform. Now platform users are able to review the content, type, time, etc. of the information shared by APCERT members through ADE and APCERT mailing lists. And the new functions can provide statistical support for APCERT Membership Awards calculation.

2. About CSIRT

2.1 Introduction

The National Computer Network Emergency Response Technical Team/Coordination Center of China (known as CNCERT/CC) is a non-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 2023, CNCERT/CC has established "CNCERT/CC International Cooperation Partnership" with 289 teams in 83 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 actively carries out international cooperation in cybersecurity and is committed to establishing the mechanism of prompt response to and coordinative handling of cross-border cybersecurity incidents. CNCERT/CC is a full member of the Forum of Incident Response and Security Teams (FIRST) and one of the founders of the Asia Pacific Computer Emergency Response Team (APCERT). CNCERT/CC has also actively engaged in activities of APEC, ITU, SCO, ASEAN, BRICS, and other international and regional organizations.

3.2 Publications

During the year of 2023, CNCERT/CC has published weekly, monthly, and annual reports, as well as other released information, which were reprinted and cited by massive authoritative media and thesis at home and abroad.

Title	No. of Issues	Description
CNCERT Weekly Reports (Chinese)	52	Emailed to over 400 organizations and individuals and published on CNCERT's Chinese website (https://www.cert.org.cn/)
CNCERT Weekly Reports (English)	52	Emailed to relevant organizations and individuals and published on CNCERT's English website (https://www.cert.org.cn/publish/english/115/index.html)
CNVD Vulnerability Weekly Reports (Chinese)	52	Published on CNCERT's Chinese website (https://www.cert.org.cn/)
Articles Analyzing Cybersecurity Threats	8	Published on journals and magazines

Table 1: Lists of CNCERT's publications throughout 2023

4. Events organized / hosted

4.1 2023 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 2023 World Internet Conference Wuzhen Summit was held in Wuzhen, Zhejiang Province on 9th November. With the theme of "Pursue Mutual Benefit with One Heart and One Mind", the Forum calls on the international community to work together for stronger dialogue and cooperation towards a peaceful, secure, open, cooperative, and orderly cyberspace. Nearly 100 representatives from government, international organizations, research institutes, civil society, and enterprises attended the Forum. World-renowned Internet pioneers, heads of international organizations, senior officials from cyber administrations of China and other countries, founders, and executives of well-known enterprises at home and abroad delivered keynote speeches in three sessions: "Co-building Rules and Policies", "Co-ordinating Ways of Cooperation" and "Co-sharing Emerging Technologies". The Forum also held a panel discussion on "Cybersecurity Technology and Cooperation" to share and exchange practical results of cooperation, the latest development trends, policies and strategies, technological opportunities and challenges, and the status quo and prospects of international cooperation in cybersecurity.

4.2 The 20th CNCERT Annual Conference and the Cyber Security Collaborative Governance Sub-Forum of China Cybersecurity Week in Fuzhou

On 12th September, 2023, with the theme of "Deepening Collaborative Governance to Jointly Forge a Strong Cyber Security Barrier", the 20th CNCERT Annual Conference and the Cyber Security Collaborative Governance Sub-Forum of China Cybersecurity Week were successfully held in Fuzhou. The Conference invited representatives from government, research institutes and cybersecurity companies to discuss and exchange new trends, hot topics, and ideas in cybersecurity. The Conference also initiated the 2023 China Cyber Security Technology Competition and the Crowdsourced Cyber Security Testing Competition.

5. International Collaboration

5.1 Drills & exercises

5.1.1 APCERT Drill 2023

On 16th August, CNCERT/CC participated in APCERT Drill 2023 and completed it successfully. The theme of this year's APCERT Drill is "Digital Supply Chain Redemption". This exercise reflects real incidents and issues that exist on the Internet today. The participants handled a case of server incident triggered by a vulnerability. 24 CSIRTs from 21 economies of APCERT, as well as 11 CSIRTs from 11 economies of OIC-CERT and AfricaCERT participated.

5.1.2 ASEAN CERT Incident Drill (ACID) 2023

On 18th October, CNCERT/CC participated in the ASEAN CERT Incident Drill (ACID) 2023. The theme of this drill is "Responding to Multi-Pronged Attacks Arising from Hacktivism". The participating teams investigated, analyzed, reported, and recommended remediation and mitigation measures towards cyber incidents. 18 CSIRTs from 10 AMS and 5 key Dialogue Partners participated in the drill.

6. Conclusion

This year, we have actively participated in various activities organized by APCERT and kept close collaboration with APCERT members, and there have been concrete achievements within APCERT community.

By reflecting on the year of 2023, we have always cherished what the past year brought us, be it challenge or opportunity. Looking ahead, we will hold on with our mission and responsibilities, making further contributions as an SC member and the convener of Information Sharing Working Group. Together, we will help to build a safe, clean, and reliable cyber space.

CyberSecurity Malaysia

CyberSecurity Malaysia

1. Highlights of 2023

1.1 Summary of major activities

12-16 Mar 2023	Participated in the OIC-CERT 5G Security WG Meeting and Activity Roll Out Event in conjunction with the Gulf Information Security Exhibition & Conference (**GISEC**), United Arab Emirates
16-18 May 2023	Participated in the OIC-CERT Promotion Programme and the "Egyptian Cybersecurity & Data Intelligence System – CDIS" Conference & Expo, Egypt
31 Jul 2023	Organised the Webinar Serumpun "**Susah-Susah Cari Rezeki, Senang-Senang Scammer Curi**". Malaysia Edition in cooperation with the Indonesian National Cyber and Crypto Agency (**BSSN**), Cyber Security Brunei (**CSB**), and the Cyber Security Agency of Singapore (**CSA**) (online)
16 Aug 2023	Organised the APCERT Cyber Drill "Digital Supply Chain Redemption" (online)
11-13 Sep 2023	Chaired the APCERT Steering Committee Physical, Kyoto Japan
8 Oct 2023	Organised OIC-CERT Board Meeting 05/2023, Abu Dhabi, United Arab Emirates
9 – 10 Oct 2023	Participated in the 11th Arab Regional Security Summit, OIC-CERT & CIS Cyber Drill, Abu Dhabi, United Arab Emirates
11 – 12 Oct 2023	Participated in the 15th annual OIC-CERT Conference & FIRST Symposium for Arab and Africa with the theme "Cybersecurity Innovation and Industry Development", Abu Dhabi, United Arab Emirates
8 Nov 2023	Chaired the APCERT Annual General Meeting (**AGM**) (online)
9 Nov 2023	Participated in the APCERT Annual Conference 2023 (Online)

2. About Cybersecurity Malaysia

2.1 Introduction

CyberSecurity Malaysia is the national cybersecurity specialist agency under the purview of the Ministry of Communications and Digital having the vision of being a globally 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 January 1997 under the Ministry of Science, Technology, and Innovation Malaysia. In 2018, with the restructuring of the government administration, CyberSecurity Malaysia was transferred to the Ministry of Communications and Multimedia Malaysia which later became the Ministry of Communications and Digital. CyberSecurity Malaysia is committed in providing a broad range of cybersecurity innovation-led services, programmes, and initiatives to help reduce the vulnerability of digital systems, and at the same time strengthen Malaysia's self-reliance in the cyberspace

2.3 Cybersecurity Incident Management

CyberSecurity Malaysia managed security incidents through MyCERT, a department within CyberSecurity Malaysia. The agency is a leading point of reference for the Malaysian Internet community when faced with cybersecurity incidents.

MyCERT facilitates the mitigation of cyber threats for Malaysia's Internet users particularly on cyber intrusion, identity theft, malware infection, and cyber harassment, among others

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

2.3.1 Cyber999 Cyber Incident Reference Centre

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

MyCERT's Cyber999 cyber incident reference centre, has responded to 5,917 incidents in 2023 and most being malicious codes and online fraud

2.3.2 Cyber Threat Research Centre

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

2.3.3 Constituency

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

3. Activities & Operations

3.1 Incident Handling Reports and Abuse Statistics

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

CyberSecurity Malaysia through MyCERT had proactively produced 87 advisories and 17 alerts to inform the constituency on issues relating to cybersecurity. The specific list of the advisories, alerts and summary reports can be viewed at https://www.mycert.org.my/portal/advisories

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

managed by MyCERT.

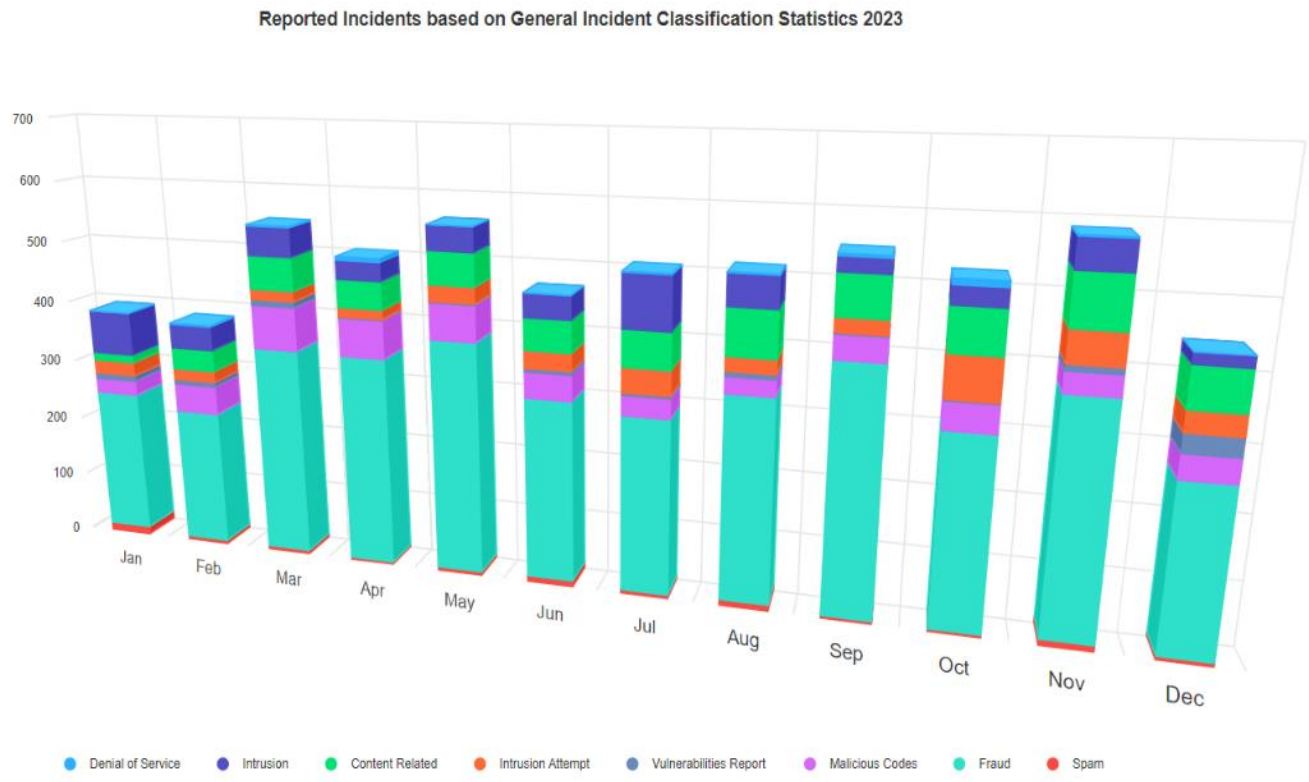


Figure 1 2023 Reported Incident

More information on incidents reported to CyberSecurity Malaysia can be viewed at: https://www.mycert.org.my/portal/statistics-2023.

3.2 Cyber Threat Research Centre

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

Other activities by the centre includes

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

3.3 The LebahNET Project

LebahNET is a Honeypot Distributed System where a collection of honeypots is used to study the exploits functioned as well as to collect malware binaries. Honeypots are computer software mechanism set up to mimic a legitimate site to

ensnare malicious software into believing that it is a legitimate site which is in a weak position for attacks. Honeypot allows researchers to detect, monitor, and counter malicious activities by understanding the activities done during the intrusion phase and attacks' payload. It can be viewed at https://dashboard.honeynet.org.my/

The URLs of the LebahNET project are:

- LebahNET portal at https://dashboard.honeynet.org.my/dashboard/12/2023
- Kibana portal at https://es.honeynet.org.my/ by using guest authentication
  Username: guest
  Password: guest2021!

4. Events Involvement and Achievements

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

4.1 Cyber Drills

CyberSecurity Malaysia was successful organised the APCERT Cyber Drill 2023 theme "Digital Supply Chain Redemption". The objective of the drill is to test on the procedures and incident handling practices of participating organisations. There were 28 CSIRT from 24 economies of APCERT and non APCERT members, 15 CSIRTs from 14 economies of OIC-CERT and AfricaCERT

Apart from the APCERT Cyber Drill, CyberSecurity Malaysia had also participated in two cross-national Cyber Drills namely the OIC-CERT and Arab Regional Cyber Drill 2023 and ASEAN CERT Incident Drill (**ACID**) 2023

4.2 Trainings

Hands-on training entitled Digital Security Lifelong Learning Program (**DSLP**) under the Malaysian Technical cooperation Programme (**MTCP**) was conducted by CyberSecurity Malaysia from 13-16 &19-20 June 2023. There were 11 participants form Algeria, Bhutan, Eswatini, Indonesia, Jordan, Maldives, Nigeria, Philippines, Oman, Sri Lanka, and Uzbekistan.

4.3 Presentations

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

i. 14 – 16 March 2023 - As a speaker at the Gulf Information Security Exhibition & Conference (**GISEC**) at the Dubai World Trade Centre, UAE
ii. 16 -18 May 2023 - As a speaker at Egypt Cybersecurity & Data Intelligence System (CDIS), Cairo

iii. 5 – 7 October 2023 - As a speaker at the conference entitled "Collaboration for a Cyber-Safe ASEAN-Japan Community" at International Conference on ASEAN Japan Cybersecurity Community, Tokyo, Japan
iv. 9 November 2023 – As a speaker at the APCERT closed conference entitled "Threat Analysis on Emerging Data Leakage in Malaysia from MyCERT Perspective" (online)
v. 5 – 6 December 2023 - As a speaker at the conference entitled "Empowering Global Cooperation in Cybersecurity" at the Arab International Cybersecurity Summit 2023, Bahrain

4.4 Research Papers

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

i. RENTAKA: Identifying Windows Cryptographic Ransomware based on Pre-Attack API Calls Features and Machine Learning Classifiers - Semarak Ilmu Publishing
ii. M-health digital evidence taxonomy system (MDETS): Enabling digital forensics readiness with knowledge sharing approach - AIP Publishing
iii. Systematic literature review: Trend analysis on the design of lightweight block cipher - Elsevier
iv. Modified Generalized Feistel Network Block Cipher for the Internet of Things – MDPI
v. The Systematic Literature Review on Information Security Culture (ISC) Research - Institute of INFORMATICS
vi. Understanding How National CSIRTs Evaluate Tools and Data: Findings from Focus Group Discussions - Association for Computing Machinery (ACM)
vii. Ransomware Behavior on Windows Endpoint: An Analysis - IPN Education Group Conference
viii. Cryptographic Ransomware Early Detection using Machine Learning Approach and Pre-Encryption Boundary Identification - WAWM Academy, Semarak Ilmu
ix. The National Cyber Ethics Modules: An Approach for Teaching Cyber Safety to K12 Students - International Academy of Technology, Education and Development (IATED)

4.5 Social Media

In 2023, CyberSecurity Malaysia received continuous invitations to speak in cybersecurity events at the local radio and television stations. CyberSecurity Malaysia also actively disseminates cybersecurity concerns through social media such as the Facebook and Twitter, which as of now the Facebook Page has about 59,000 followers and the CyberSecurity Malaysia Twitter has 7,873 followers

5. International Collaboration

The Malaysia Cybersecurity Strategy 2023 identified international cooperation as one of the areas in enhancing

cybersecurity. In line with this, CyberSecurity Malaysia is actively establishing collaborative relationships with foreign parties

5.1 Working Visits

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

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

i. Bangladesh e-Government Computer Incident Response Team (BGD e-GOV CIRT)
ii. Badan Siber dan Sandi Negara, Indonesia
iii. British High Commission Singapore
iv. National Revenue Authority (NRA) Republic of South Sudan
v. Minister of Security, Republic of Uganda
vi. Tanzania Bank, Tanzania

5.2 International Roles

Amongst the international roles and contributions by CyberSecurity Malaysia

i. The Permanent Secretariat of the Organization of Islamic Cooperation – Computer Emergency Response Team (**OIC-CERT**), where a major role is to undertake daily operations and facilitate cooperation and interaction among the members countries
ii. The lead for the Capacity Building Initiatives in the OIC-CERT
iii. Co-Lead the OIC-CERT 5G Security Working Group with the objective of developing a security framework to be adopted by OIC member countries
iv. The Chair of the APCERT
v. Member of the Forum of Incident Response and Security Teams (**FIRST**)

6. Future Plans

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

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

CyberSecurity Malaysia and Aerosea Exhibitions Sdn. Bhd will be organizing an international event known as the Cyber

Digital Services, Defence and Security Asia (**CyberDSA'24**). This event is scheduled to take place from 6 August to 8 August 2024, at the Kuala Lumpur Convention Centre. Held concurrently with this prestigious show are The Cybersecurity Malaysia ACE Awards (**CSM-ACE**) and Sibersiaga. The CSM-ACE which is an annual event providing awareness, trainings, and awards to information security professionals, and the National ICT Security Discourse to boost the cybersecurity awareness among the youth. At the international arena, CyberSecurity Malaysia as the Permanent Secretariat of the OIC-CERT, continues to spearhead collaborations and organise international events such as the OIC-CERT Annual Conferences and Trainings.

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

7. Conclusion

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

In line with the Malaysia Cybersecurity Strategy 2020 that emphasized on capacity and capability building, mitigation of cyber threats, and international collaboration, CyberSecurity Malaysia will continue to enhance existing and develop new cybersecurity processes, capabilities, and technologies. CyberSecurity Malaysia will also continue with the commitment to seek new edges in cybersecurity and to be a catalyst in developing the industry.

International cooperation and collaboration are an important facet in mitigating other cybersecurity issues. As the cyber environment does not conform to the physical boundary of the countries, international relations will remain an important initiative. With the rapid development of the internet, the economies are now dependent on public network applications such as online banking, online stock trading, e-business, e-governments, and the protection of the various national information infrastructures. CyberSecurity Malaysia will continue to establish and support cross border collaboration 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

2023 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

- Establishing a Certification Authority (CA), Feb 2023
- Certification Authority (CA) Maturity Model, Sep 2023
- An Introduction to PGP/GnuPG, Oct 2023

3. Events organized / hosted / participated in

3.1 Training

Trainer:

- TRANSITS I for the NCSA, Apr 2023
- 2023 APISC Security Training Course. Oct 2023

3.2 Drills & exercises

Organized:

- Cyber Drill for the NCSA, Apr 2023
- Cyber Exercise for Certification Authorities (CA) TTX, Nov 2023

Participated:

- APCERT Annual Drill 2023, Aug 2023

3.3 Conferences and seminars

Participated:

- APCERT AGM & Conference 2023 (speaker), Nov 2023

GovCERT.HK

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

1.Highlights of 2023

1.1 Summary of Major Activities

The Government Computer Emergency Response Team Hong Kong (GovCERT.HK) continued to collaborate with different stakeholders, pressing ahead with various activities to strengthen the cyber security measures and awareness of the community.

1.2 Achievements and Milestones

Building Cyber Security Capabilities and Resilience

We co-organised the Inter-Departmental Cyber Security Drill with the Cyber Security and Technology Crime Bureau (CSTCB) of the Hong Kong Police Force (HKPF) to enhance capabilities and resilience of government bureau/departments (B/Ds) in tackling the evolving cyber security threats. Furthermore, we proactively and adaptively reviewed the Government Information Security Related Regulations, Policies and Guidelines with a view to strengthening the cyber security governance and safeguarding national security.

Raising Awareness and Knowledge

We held the "Build a Secure Cyberspace Promotional Campaign 2023" with Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) and HKPF, to raise the public awareness of digital identity protection. We also co-organised the Cybersecurity Symposium 2023 with the Hong Kong Internet Registration Corporation Limited (HKIRC), uniting the industry to address the cyber security challenge together.

Fostering Cross-boundary Collaboration

We actively engaged in training activities and drill exercises, and closely worked with global partners to exchange technical views and to cooperate in incident response and coordination. Invited by CNCERT/CC, we joined World Internet Conference (WIC) as a non-profit institution member to expand our presence and to share experience with leading international organisations for addressing common global cyber security challenges.

2. About GovCERT.HK

2.1 Introduction

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

GovCERT.HK works closely with HKCERT, local industries and critical Internet infrastructure stakeholders on cyber threat intelligence sharing, capability development, public education, and continuous promotion on cyber security. GovCERT.HK also actively collaborates with other governmental and regional CERTs, and international organisations in sharing cyber threat intelligence and incident information; participating in training events, workshops, forums, and drills; and 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 Office of the Government Chief Information Officer (OGCIO) of the Government.

2.3 Resources

GovCERT.HK is an establishment under OGCIO and funded by the Government.

2.4 Mission and Constituency

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

3. Activities and Operations

3.1 Security News Bulletins

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

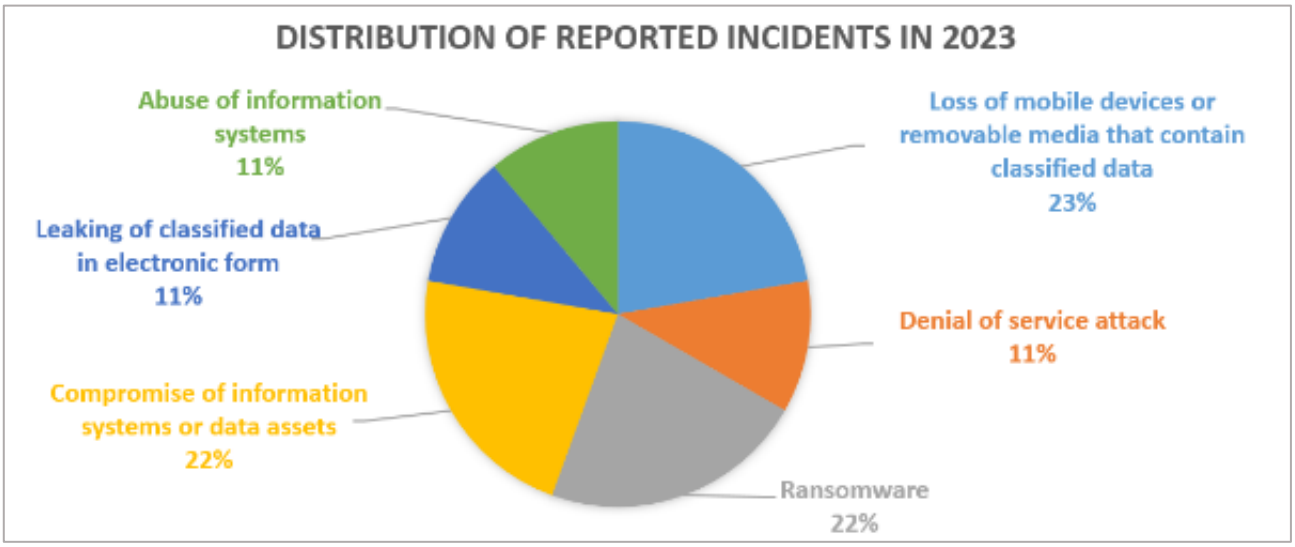
- "Security Vulnerabilities and Patches" and "Security Industry News" to registered subscribers through emails on every working day; and
- "Weekly IT Security News Bulletins" with summary of security news and product vulnerabilities to registered government subscribers through emails and posted to the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

3.2 Alerts and Advisories

In 2023, GovCERT.HK issued over 245 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.

3.3 Incident Handling Reports

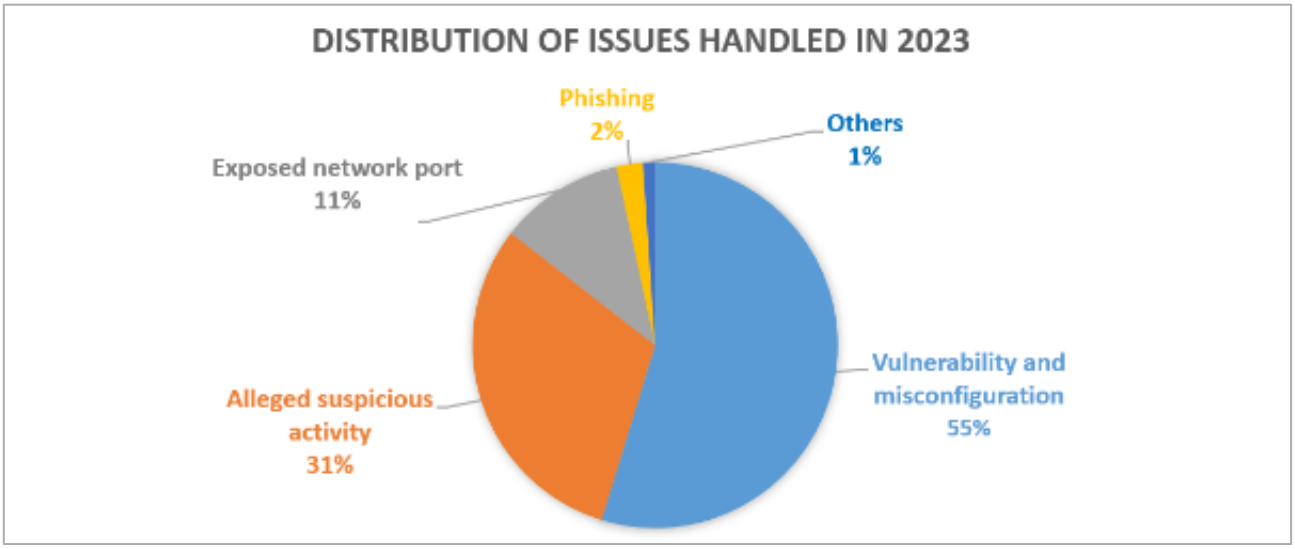
GovCERT.HK handled 9 reported incidents related to government installations, with the incident types shown below:



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

3.4 Abuse Statistics

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



3.5 Publications and Mass Media

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

- We partnered with Radio Television Hong Kong (RTHK) to broadcast radio episodes "e-World Smart Tips" every week, covering a wide range of topics such as phishing attacks, online shopping, devices disposal, smart travelling and safe use of social media and instant messaging, in a lively and interesting way.
  (www.cybersecurity.hk/en/media.php#Radio)
- We published practical guidelines and infographics with themes such as artificial intelligence (AI) chatbot challenges & best practices, cyber safe travel and guide on using instant messaging to educate the public to protect themselves against cyber attacks.
  (www.cybersecurity.hk/en/resources.php)

- We organised "Protect Your Online Identity" Speech Contest. Many creative videos with witty speeches reminding the public to safeguard their digital identities and protect personal information were received.

Winning Entries

- We published a series of posts on the OGCIO Facebook page, with updates and tips on the latest cyber security topics such as phishing, Web 3.0, artificial intelligence, and incident response, to enhance communications with the public.
  (www.facebook.com/OGCIOHK)

3.6 GovCERT.HK Technology Centre

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

4. Events Organised/Hosted

4.1 Training

In 2023, we organised various seminars, webinars and training featuring the latest IT security technologies and solutions, as well as the latest cyber security threats and how to deal with them. Some 3240 government staffs participated in the events with topics on security risk management, Web 3.0, AI, quantum computing, ransomware protections and application security testing. A Catalogue of IT Security Solutions (CoSS) is also maintained to facilitate B/Ds to reference and explore the potential of various IT security solutions.

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 drills to strengthen the preparedness and the overall incident response capability of B/Ds to cyber attacks. In 2023, it was held in a hybrid online-offline format featuring a practical exercise system, with participation of 232 information technology officers from 68 B/Ds.

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 and mobile applications, with a view to building a stronger defence.

4.3 Conferences and Seminars

Build a Secure Cyberspace Promotional Campaign

Varies promotional activities under the theme "Protect Your Online Identity" were organised for businesses, organisations, schools and the public to raise their cyber security awareness and strengthen their cyber security postures. Two seminars were organised in May and September 2023 under the campaign.

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

To promote cyber security awareness and cyber etiquette, we organised a total of 44 visits to primary and secondary schools, tertiary institutions, and NGOs to deliver information security talks to students, teachers, parents, service recipients and staff of NGOs.

InfoSec Tours with RTHK Radio 2

GovCERT.HK continued to partner with the RTHK to conduct three InfoSec Tours with topics of "Protect Your Online Identity", "Protect Personal Information and Privacy" and "Beware of Phishing Attacks", which delivered information security message in a relaxing way and equipped the public to be a smart Internet user. A short video clip with the theme of fact-checking has also been produced to raise awareness about the importance of verifying information before sharing it.

Cybersec Infohub engagement activities

To promote cyber security information sharing among public and private organisations, various activities such as sector-specific meeting and networking, technical professional workshops and seminars were arranged under the Cybersec Infohub partnership programme with affirmative feedback.

Cybersecurity Symposium 2023

The event aimed to bring together quangos, enterprises, and other local organisations to explore industry collaboration in addressing cyber security challenges in the digital era. Over 10 industry experts and business leaders from the Mainland of China and Hong Kong, together with over 450 industry professionals representing about 200 public and private organisations, exchanged views on different topics including protection of critical data and the latest technologies and trends in cyber defence matters. The event also featured a showcase of cyber security solutions, allowing participants to gain insights and to engage with industry experts regarding the latest cyber security technologies and solutions.

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 has attracted over 2 000 organisations and more than 3 100 representatives from various local sectors as of the end of 2023.

Enhancing Overall Cyber Security Resilience

We continued to support our working partners to organise various programmes and campaigns to educate the public to cope with the latest cyber attacks and to acquire fundamental knowledge with a view to nurturing cyber security talents in a long run. GovCERT.HK supported the following events and initiatives:

- CTF Challenge 2023 and Phishing Public Awareness Campaign by HKCERT
- Free online training resources at "Cybersec Training Hub" and "Cyber Youth Programme 2023", including certified training courses, game-aided learning platform and competitions, 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, cyber crime initiatives and technological research.

GovCERT.HK participated in the following events in 2023:

- China Cybersecurity Week 2023
- APCERT Annual General Meeting and Conference
- APCERT Drill with the theme of "Digital Supply Chain Redemption"
- APCERT on-line training sessions
- CNCERT/CC Conference 2023
- NatCSIRT Meeting 2023 and 35th FIRST Annual Conference

6. Future Plans

It is GovCERT.HK's ongoing effort to strengthen the cyber security resilience and promote security awareness through various activities:

- Enhance the intelligence gathering and sharing mechanism within the government to cope with the emerging threats;
- Bolster the connections with local, regional, and international cyber security partners to foster efficient communications on incident management; and
- Continue to work closely with our partners to organise various programmes for nurturing talents and enhancing awareness and resilience within the government departments and the public.

7. Conclusion

To maintain cyber security readiness, response capabilities and resilience of the public and organisations, GovCERT.HK will continue to raise cyber security awareness in the community by proactively working with B/Ds, various stakeholders in the industry in a holistic approach with a view to strengthening the capability in combating the ever-changing cyber security trends.

HKCERT

Hong Kong Computer Emergency Response Team Coordination Centre

1. Highlights of 2023

1.1 Summary of Major Activities

- Organised the "Build a Secure Cyberspace 2023" campaign with the Government and Hong Kong Police Force.
- Organised the "Hong Kong Cyber Security New Generation Capture the Flag Challenge 2023".
- Held "All-Out Anti-Phishing" moving showroom campaign.
- Participated in smart city roving exhibition organised by the Government.
- Participated in Innocarnival 2023 organised by Innovation and Technology Commission.
- Presented in different international conferences and local press briefing.
- "Year Ender" in local media briefing to call on public to raise awareness of information security
- Media interviews in local media, radio, and TV programme to raise general public awareness on cyber security risks.
- Published timely security guidelines and advisories in response to the digital transformation.

1.2 Achievements & Milestones

- Organised the "Build a Secure Cyberspace 2023" campaign with the Government and Hong Kong Police Force. The campaign involved 2 public seminars , a Speech Contest, and an award presentation ceremony. Over 150 participants joined the contest and over 400 participants joined the seminars.
- Organised "Hong Kong Cyber Security New Generation Capture the Flag Challenge 2023". It involved 2 workshops, a 48-hours online contest and a public seminar with award ceremony. The international category was the first time to open for registration and attracted over 100 teams to participate. HKCERT also collaborated with SECCON and could assign 1 winning team in tertiary or open categories to participate in SECCON CTF 2023 final.
- Held "All-Out Anti-Phishing" moving showroom campaign. It involved 3 phases and over 10 different locations in Hong Kong. HKCERT crossed over DinDong designer to design an anti-phishing themed moving showroom. The campaign visited Hong Kong, Kowloon, and the New Territories to teach citizens how to identify and prevent

phishing attacks.

- Participated in smart city roving exhibition organised by the Government. It involved how various smart city initiatives in Hong Kong can bring convenience to their daily life through the adoption of technology. HKCERT held a booth in the exhibition to raise the awareness of cyber security among the public.
- Participated in Innocarnival 2023 organised by Innovation and Technology Commission. HKCERT held a booth in the activity and interacted with the public via deepfake technology.
- Published security advisories on latest phishing and ransomware attacks patterns and emerging cyber threats
- Continued the Healthcare Cyber Security Programme and Critical Infrastructure Cyber Security Programme. The which covered almost all public and private hospitals of Hong Kong.

2. About HKCERT

2.1 Establishment

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

2.2 Organisation and Workforce Power

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

2.3 Mission and Constituency

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

3. Activities and Operations

3.1 Incident Handling

During the period from January to December of 2023, HKCERT had handled 7,752 security incidents which was 8% decreased of the previous year (see Figure 1).

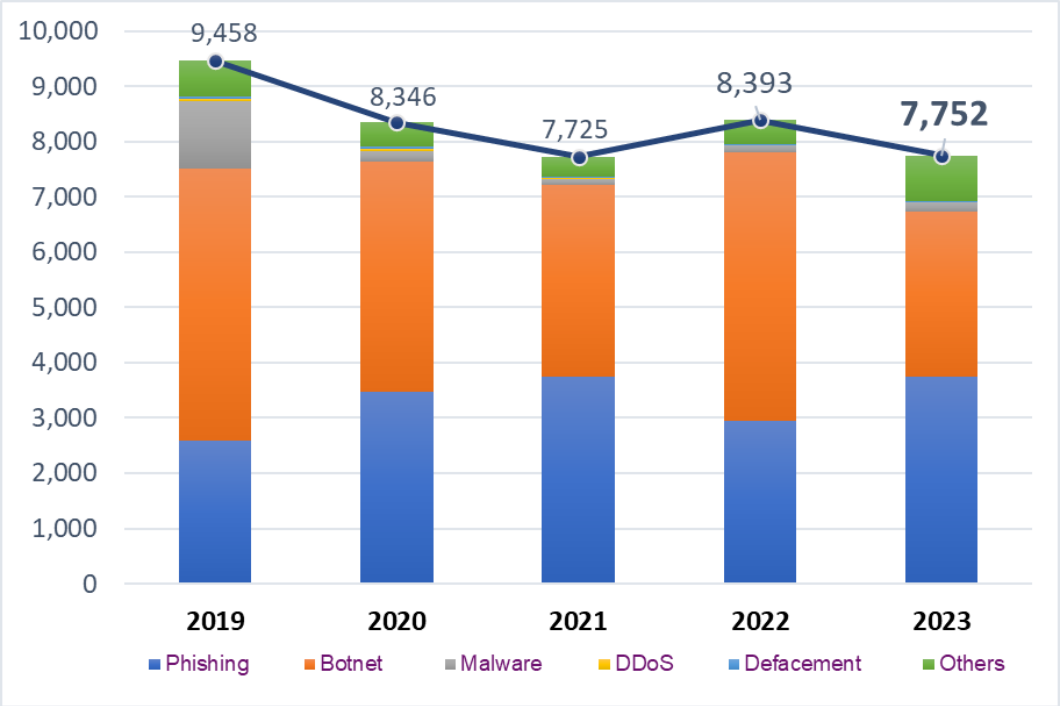


Figure 1. HKCERT Security Incident Reports

While the number of overall security incidents handled by HKCERT kept fluctuating since 2020. The amplitude ranged from -9% to +9%. Phishing (3,752 cases or 48% of total cases) went up 27% and total phishing URLs was increased by 22%. During the period from March to April of 2023, Hong Kong seriously suffered from phishing attacks targeting reward programs of some Hong Kong organisations. On the other hand, botnets (2,982 cases or 38% of total cases) dropped significantly and went down 39%.

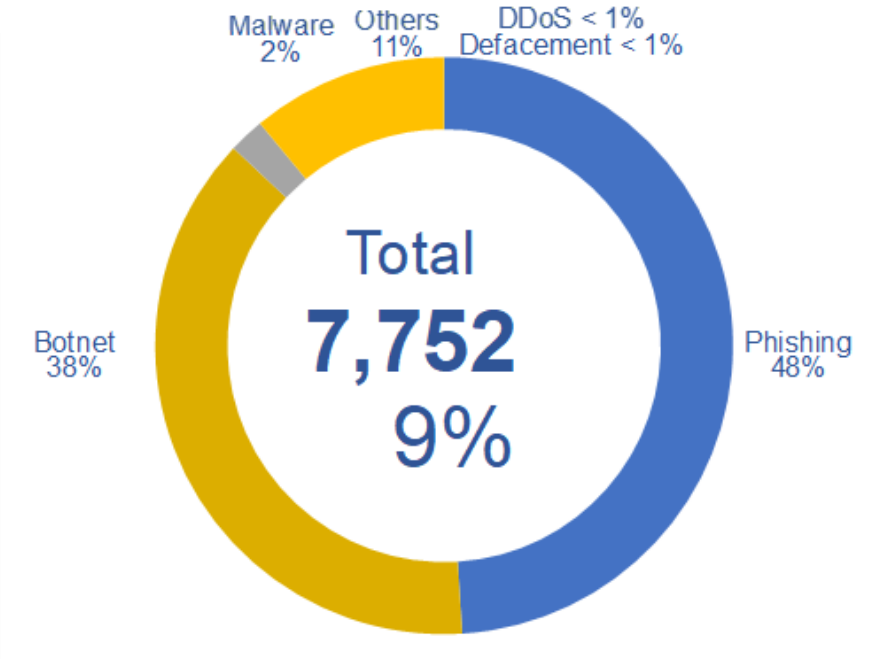


Figure 2. Distribution of Incident Reports

3.2 Watch and Warning

During the period from January to December of 2023, HKCERT published 357 security bulletins for the vulnerabilities of major software (see Figure 3) on the website. In addition, HKCERT have also published 31 security advisories, topics include 5 key risks in Hong Kong Information Security Outlook 2023 such as artificial intelligence, IoT, Crime-as-a-service, Web 3.0 and identity theft, analysis of ransomware trend across Asia-Pacific, guideline for using artificial intelligence and instant message application.

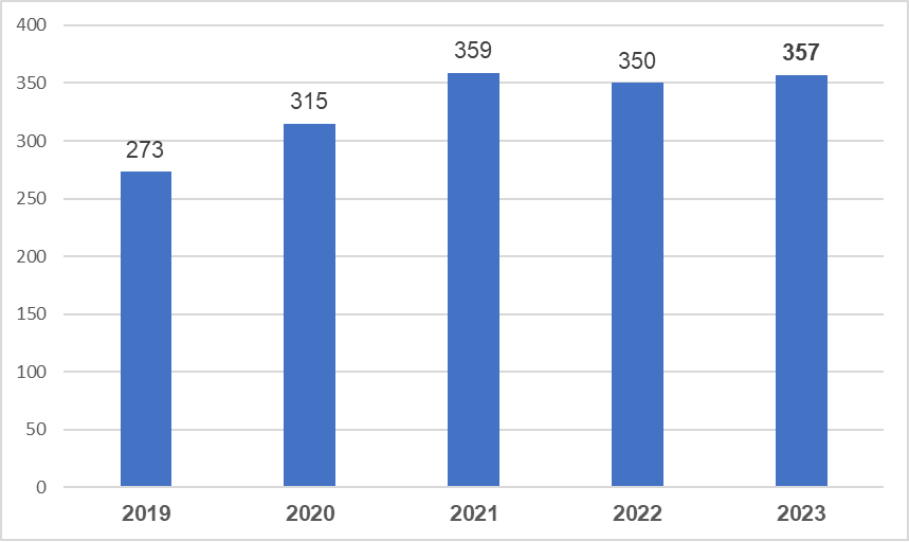


Figure 3. HKCERT Published Security Bulletins

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

3.2.1 Embrace Global Cyber Threat Intelligence

HKCERT used the Information Feed Analysis System (IFAS) to collect intelligence of compromised machines in Hong Kong from global security researchers. The system provided a better picture of security status of Hong Kong and a way to verify the effectiveness of the security incident response. For example, figure 4 showed the number of bot-related in Hong Kong network reached a high count of 2,583 in 2023 Q1 and kept up and down in subsequent quarters. The major botnet remained as Mirai.

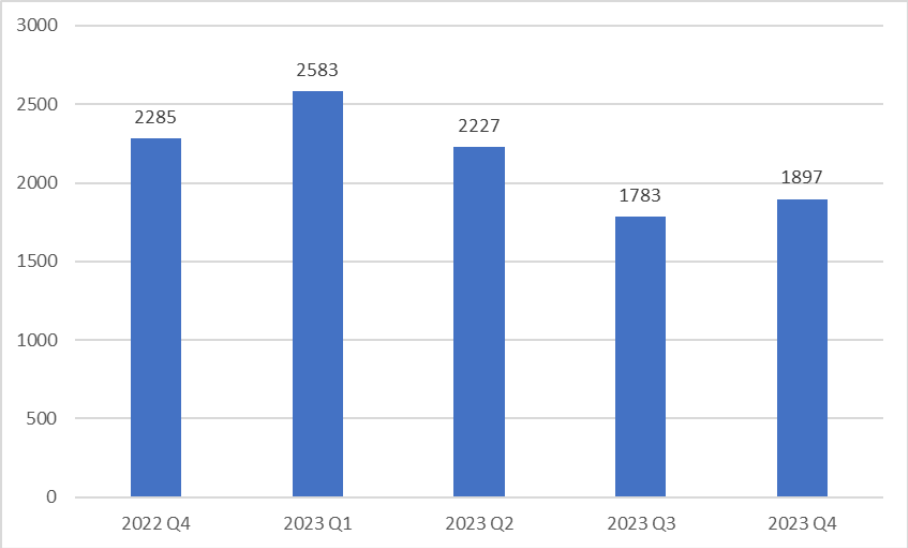


Figure 4. Trend of Bot related security events in the past year
(Source: data feeds from overseas security researchers, not from incident reports)

3.3 Publications

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

- HKCERT had published 12 issues of monthly e-Newsletter in the period (see https://www.hkcert.org/newsletters).
- HKCERT had published the statistics of incident reports every quarter (see Figure 5) (see https://www.hkcert.org/statistics).

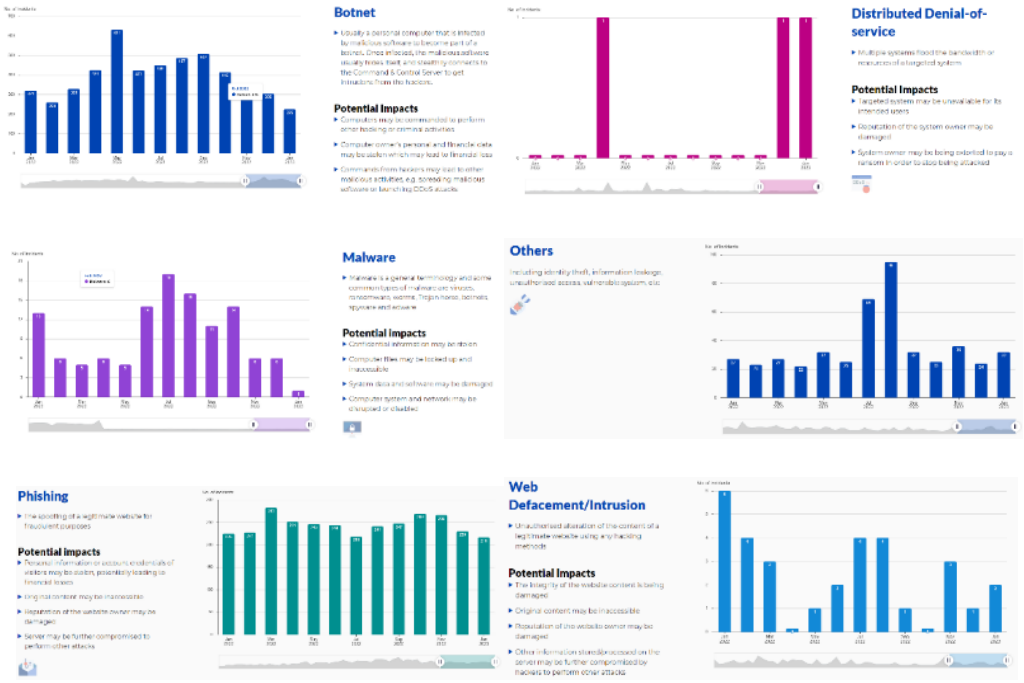


Figure 5. Charts in HKCERT website showing the statistics of different types of incident reports.

4. Events organised and co-organised

4.1 Build a Secure Cyberspace 2023

HKCERT jointly organised the "Build a Secure Cyberspace 2023" campaign with the Government and Hong Kong Police Force. The campaign involved 2 public seminars, and a speech contest. An award presentation ceremony was organised in Sep 2023.

For the Folder Design Contest, HKCERT received about more than 150 applications from Open Group, Secondary School, and Primary School Group. A professional judge panel selected winners with most creative and meaningful. Figure 6 shows the photos of winners receiving the rewards.

Primary Group

Secondary Group

Open Group

Figure 6. Winners of Primary School, Secondary School, Open Categories received the rewards.

Use this link to access the winning entries online:

- https://www.cybersecurity.hk/en/contest-2023.php

4.2 Capture the Flag Contest

HKCERT jointly organised the "Hong Kong Cyber Security New Generation Capture the Flag Challenge 2023" (HKCERT CTF 2023) with partner associations in information and education sectors. The 48-hours contest was opened to all participants who were enthusiastic with Capture the Flag. This year, HKCERT CTF 2023 was firstly opened to international to register. It was a success with more than 500 teams and close to 1,100 participants from universities, secondary schools, and open categories, also from international. A public seminar with award ceremony was organised in December 2023. Furthermore, it received prestigious acclaim from SECCON CTF 2023, a flagship CTF competition in Japan. The winning team of HKCERT CTF 2023 received a special privilege of bypassing the qualifying round and participated directly in the international finals taking place in Tokyo during Christmas of 2023.

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

- https://www.hkcert.org/event/hong-kong-cyber-security-new-generation-capture-the-flag-challenge-2023-seminar-and-award-presentation-ceremony

4.3 "All-Out Anti-Phishing" Moving Showroom Campaign

Moving showroom campaign involved 3 phases and over 10 different locations in Hong Kong. HKCERT crossed over DinDong designer to design an anti-phishing themed moving showroom. The campaign visited Hong Kong, Kowloon,

and the New Territories to teach citizens how to identify and prevent phishing attacks. Thousands of residents visited the showroom with positive feedback.

4.4 Smart City Roving Exhibition

Smart city roving exhibition was organized by Hong Kong government. HKCERT was one of the participant. It involved how various smart city initiatives in Hong Kong can bring convenience to their daily life through the adoption of technology. In the exhibition, HKCERT held a booth to raise the awareness of cyber security among the public.

4.5 Innocarnival 2023

Innocarnival 2023 was organised by Innovation and Technology Commission. HKCERT held a booth in the activity and interacted with the public via deepfake technology.

5. Collaboration

5.1 International Collaboration

HKCERT participated in a number of international coordination and collaboration events in year 2023:

- Participated in the NatCSIRT Conference 2023
- Participated in the AusCERT Conference 2023
- Participated in the HITCON 2023
- Participated in the 2023 APCERT Cyber Security Drill Exercise
- Participated in the APISC Security Training Course 2023
- Participated in the APCERT AGM and Conference 2023
  - Presented "Raising Cyber Security Awareness – A Localised Approach"
- CNCERT Annual Conference
  - Presented "Hong Kong SME Cyber Security Connection Programme "
- Participated in the SECCON 2023
- Participated in the JSAC 2024

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

5.2 Local Collaboration

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

- HKCERT continued to work closely with the government (GovCERT.HK) and law enforcement agency and held meetings to exchange information and to organise joint events regularly.
- HKCERT continued to actively participate in the Cyber Security Information Sharing platform 'Cybersec Infohub" which comprised of over 300 companies, critical infrastructure organisations, banks, and other enterprises in Hong Kong.
- HKCERT continued to work with police, ISPs, and domain registries on closing down bulletproof hosting, phishing sites and botnet command and control centres in Hong Kong.
- HKCERT collaborated with Microsoft in the Healthcare Cyber Security Watch Programme to promote cyber security situational awareness in healthcare sector. The objective of this programme is to make use of global cyber threat intelligence to inform Hong Kong Healthcare sector of attacks targeting their IT infrastructure so that they can better mitigate security risks. The Programme was officially launched in December 2020 with 14 organisations including the Hospital Authority and most of the private hospitals in Hong Kong joining.
- HKCERT collaborated with Microsoft in the Critical Infrastructure Cyber Security Watch Programme to promote cyber security situational awareness in critical infrastructure sector. The objective of this programme is to make use

of global cyber threat intelligence to inform Hong Kong critical infrastructure sector of attacks targeting their IT infrastructure so that they can better mitigate security risks. The Programme was officially launched in December 2021 with 7 organisations that provide essential public services to the citizens in Hong Kong joining.

- HKCERT collaborated with local regulators to deliver talks to related regulated organisations and members.
- HKCERT collaborated with local universities to conduct research on IoT and OT security.

6. Achievements & Milestones

6.1 Advisory Group Meeting

HKCERT had held the Advisory Group Meeting in October 2023. The meeting solicited inputs from the advisors and invited guests from SME associations on the development strategy of HKCERT.

6.2 Three Year Strategic Plan

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

6.3 HKCERT Comprehensive Guide to Social Media Scams

HKCERT had launched the "Comprehensive Guide to Social Media Scams: Setting up Defense to Safeguard Your Personal Information" (https://www.hkcert.org/security-guideline/comprehensive-guide-to-social-media-scams-setting-up-defense-to-safeguard-your-personal-information) in Aug 2023. The guideline covered information of 2 areas to aid user to handle social media scams. These 2 areas include (1) Phenomenon of social media scams, and (2) Preventative measures to social media scams, also how to report the scams on social media platforms.

6.4 HKCERT Open Threat Intelligence Campaign

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

6.5 Analysis of Ransomware Trend

HKCERT studied and analysed the ransomware trend across Asia-pacific. Advisories were published to raise situational awareness of users for the prevention and detection measures. (https://www.hkcert.org/blog/ransomware-trends-q2-2023-surge-in-attacks-across-asia-pacific-persistent-multiple-extortion-and-evolving-threat-landscape)

6.6 Security Guidelines and Advisories for Security Outlook 2023

HKCERT published different security guidelines and alerts in response to the cyber threats and incidents mentioned in "Year Ender Press Briefing 2023", such as identity or credential theft, attacks using artificial intelligence, crime-as-a-service, attacks targeting Web 3.0 and attacks targeting IoT.

6.7 HKCERT "All-Out Anti-Phishing" Thematic Page

HKCERT would like to reinforce our target of preventing phishing through educating the public. Therefore, HKCERT introduced a new thematic page "All-Out Anti-Phishing" (https://www.hkcert.org/publications/all-out-anti-phishing). The thematic page consolidates all essential information about phishing, including attack techniques, prevention, identification, and handling procedures for suspicious messages.

6.8 Research on IoT and OT security

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

6.9 Embrace Global Intelligence and Build Security Health Metrics

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

6.10 Open Data

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

6.11 Year Ender Press Briefing

HKCERT organised a year ender press briefing to media in February 2024 to review cyber security landscape of 2023 and provided an outlook to 2024 to warn the public for better awareness and preparedness. It received very good press coverage.

Figure 7. HKCERT at the Year Ender press briefing.

7. Future Plans

7.1 Strategy

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

7.2 Funding

HKCERT had secured Government funding to provide the basic CERT services in 2024/2025. 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 “Cyber security on the Trams”. HKCERT will invite participants from open group, secondary school, and primary school groups to design the outlook of the tram, following the theme of cyber security. The designs of the winners will be displayed on the physical trams.
HKCERT will launch a cyber security public awareness campaign called “Cyber Security Week”. A big exhibition will be held in a shopping mall with different display booths and interactive games.
HKCERT will hold a large cyber security drill exercise with critical infrastructure shareholders.
HKCERT will continue to work on IoT research. Electronic billboards will be our target.
HKCERT will continue to organise the Capture the Flag (CTF) contest, HKCERT will continue to partner with different associations to organise another CTF in 2024 for the participants from universities, secondary schools, and open categories.

8. Conclusion

In 2023, the number of overall security incidents reported to HKCERT dropped by 8% and went back to level of 2021. The phishing cases and phishing URLs recorded a rise, increased by 27% and 22% respectively. It became the first major security incident in Hong Kong. It was believed that the rise came from phishing campaigns targeting reward programs owned by Hong Kong organisations. Botnet just recorded a decrease. The reason was complicated and under investigation.
In 2024, 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, including the Information Security Summit and the Hong Kong Cyber Security New Generation Capture the Flag Challenge, to raise local cyber security awareness and nurture the next generation of cyber security talents.
There are five major information security risks that must be addressed in 2024:

1. "Weaponisation" of AI:
Hackers use generative AI to issue instructions for generating malicious code, dominating cyber attacks. Additionally, hackers can use AI to generate disinformation that affects the output of other AI, bypassing cyber security measures. Hackers also use AI to create fake videos to deceive for personal gain.

2. Next-Level Phishing Attacks:
In addition to using traditional methods such as emails and text messages to conduct phishing attacks, hackers also use fake videos to impersonate someone’s identity. Phishing attacks also extend to social media platforms, impersonating some brand pages. At the same time, hackers use search engine optimisation (SEO) techniques to make phishing websites appear at the top of search results, deceiving more victims.

3. Trend towards Organised Cybercrime:

In 2023, Hong Kong experienced several ransomware attacks targeting local organisations, resulting in large amounts of ransom being extorted and sensitive data being exposed. Citizens also faced threats from malicious apps and phishing. Globally, the number of ransomware attacks and vulnerabilities reached a new high in 2023, indicating an increasingly serious trend of organised and systematic cybercrimes.

4. Attacks Arisen from Smart Devices:

Electronic products nowadays are most equipped with network connectivity, allowing them to connect to other devices or the internet. These products have varying cyber security standards and are susceptible to intrusion and malicious manipulation. Some products cannot patch security vulnerabilities, making them difficult to block cyber attacks.

5. Third-party Risk:

Most companies use IT services provided by third-party, such as software and IT personnel, but this gives rise to IT supply chain attacks and insider threats, leading to data breaches, ransomware attacks, and other consequences. Additionally, research suggests that generative AI may produce incorrect information, such as code with security vulnerabilities or false information. If organisations adopt such information without verification, it brings risks to their operations.

JPCERT/CC

Japan Computer Emergency Response Team / Coordination Center

1. Highlights of 2023

1.1 Summary of major activities

JPCERT/CC leads CVD Working Group in APCERT

The number of CNAs in the Asia Pacific region is growing, however at the same time, there are significant gaps in experience and knowledge among APCERT members, and there are still CVD/CNA adoption spaces left in the region. To address this issue, CVD Working group (WG) has been established in APCERT to build a network in the Asia Pacific region for information/knowledge sharing, CVD/CVE cooperation, and efficient CVD/CVE adoption. There are 6 teams in the WG, and JPCERT/CC is leading its activity.

YAMA customizable malware detection tool released

JPCERT/CC developed and released a tool called YAMA (Yet Another Memory Analyzer for malware detection), which is designed to support malware detection. YAMA uses YARA rules created by the user to conduct memory scans. As such, even fileless malware can be detected if it is deployed on memory. In addition, even if the malware is obfuscated, it may be detected by scanning the deobfuscated malware running on memory. YAMA is available in the following GitHub repository.

- GitHub JPCERT/CC YAMA

https://github.com/JPCERTCC/YAMA

1.2 Achievements & milestones

JPCERT/CC now oversees 8 CNAs as a Root CNA

JPCERT/CC has been working to streamline the global distribution of vulnerability information as a Common Vulnerability and Exposure (CVE) Numbering Authority (CNA). Following the establishment of a policy to authorize key product developers as CNAs and assign CVE IDs in a more decentralized manner, JPCERT/CC has been supporting the stable

operation of the CVE Program as a Root CNA through efforts such as inviting product developers in Japan to become a CNA. The CVE Program welcomes the recent addition of new CNAs from Japan, and JPCERT/CC is pleased to have more partners with which it can address vulnerability information and share values on vulnerability coordination and information distribution. In addition, 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.

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

FIRST is the world's largest community boasting a membership of 679 CSIRTs from 105 countries and economies as of June 2023. Yukako Uchida, Manager of the Global Coordination Division, ran for the Board of the Forum of Incident Response and Security Teams (FIRST) from JPCERT/CC and was elected for another 2-year term.

2. About JPCERT/CC

2.1 Introduction & Establishment

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

2.2 Constituency

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

3. Activities & Operations

3.1 Incident Handling Reports

In 2023, JPCERT/CC received 65,669 computer security incident reports from Japan and overseas.

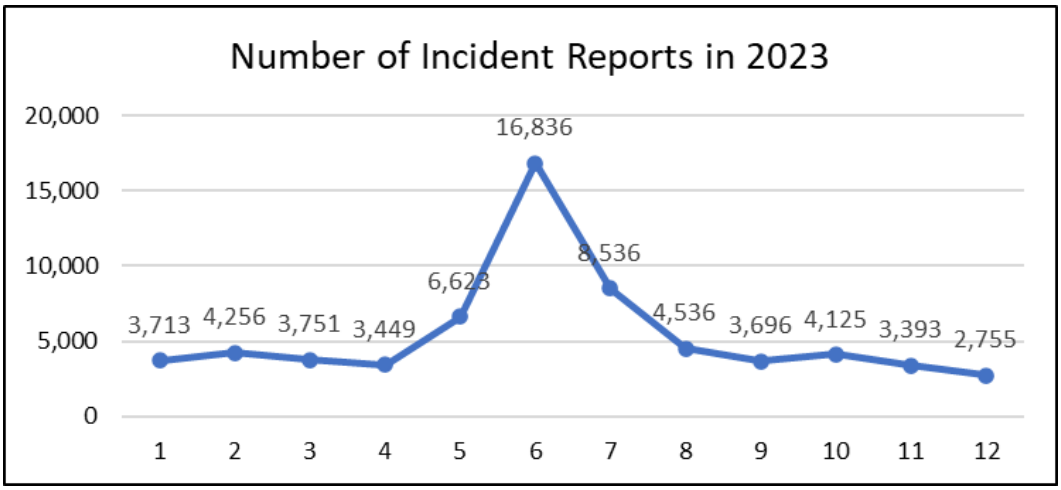


Figure 1. Number of Incident Reports (2023)

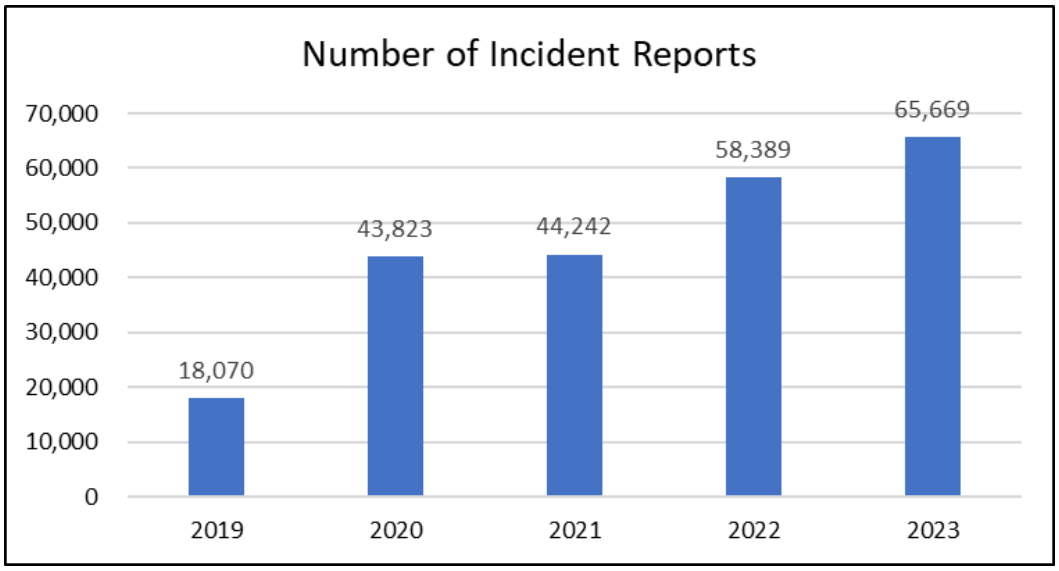


Figure 2. Incident reports to JPCERT/CC (2019-2023)

3.2 Abuse statistics

Incidents reported to JPCERT/CC during the last quarter of 2023 were categorized as in Figure 3. Roughly 70% of the reports were on phishing site, followed by scan and website defacement.

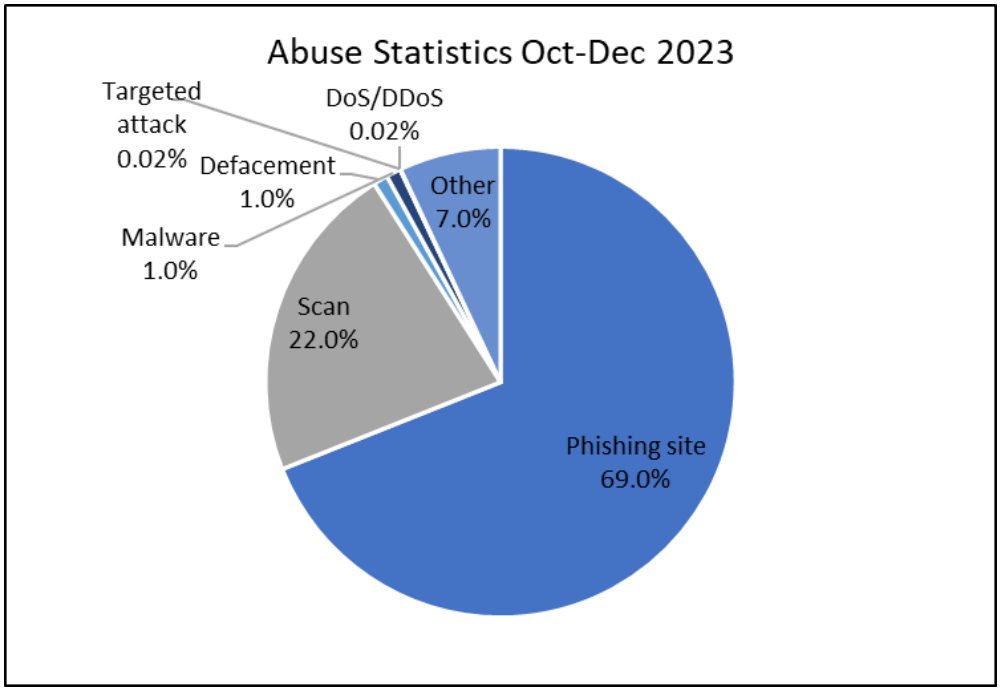


Figure 3. Abuse Statistics of Oct-Dec 2023

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 2023, 26 security alerts were published.

Early Warning Information

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

Japan Vulnerability Notes (JVN)

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

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

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

JPCERT/CC also directly receives vulnerability reports from overseas researchers and coordinates with the researchers and developers with vulnerable products. Once solutions become publicly available, JPCERT/CC publishes advisories for the reported issues on JVN.

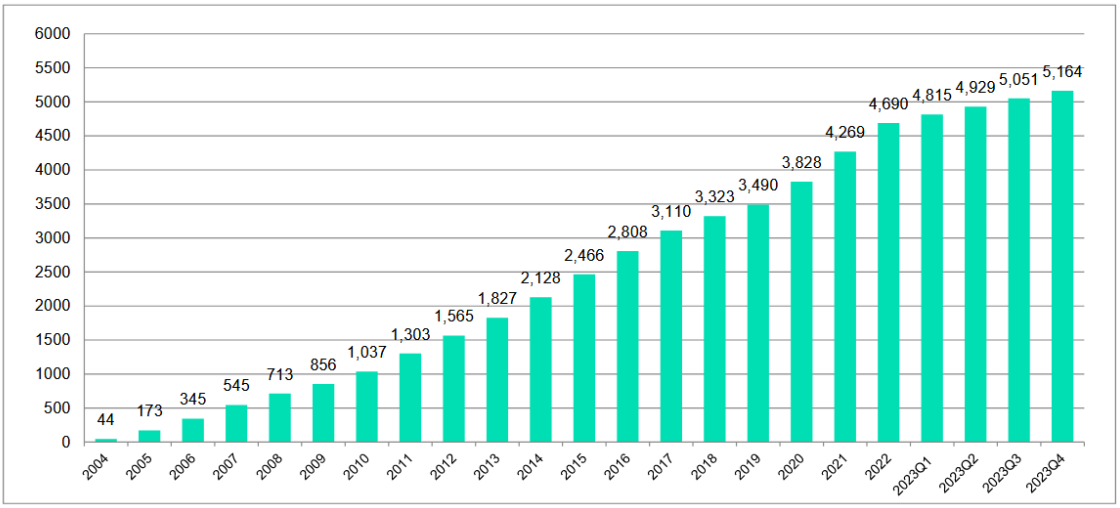


Figure 4. Number of vulnerabilities published on JVN by year

In 2023, 19,959 vulnerabilities coordinated by JPCERT/CC were published on JVN.

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

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

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

JPCERT/CC Weekly Report

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

JPCERT/CC Official Blog

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

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

Quarterly Activity Reports

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

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

JPCERT/CC on X (Twitter)

https://twitter.com/jpcert_en

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

JPCERT/CC GitHub

https://github.com/JPCERTCC

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

3.4 Services

Industrial Control System Security

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

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

3.5 Associations and Communities

Nippon CSIRT Association

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

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

Council of Anti-Phishing Japan

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

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

4. Events

4.1 Trainings, Seminars and Workshops

JPCERT/CC offers trainings, seminars and workshops for technical staff, system administrators, network managers, etc.

JPCERT/CC hosts the JSAC in January (held annually since 2018) and the Control System Security Conference in February (held annually since 2009).

5. International Collaboration

5.1 International partnerships and agreements

MoU

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

FIRST (Forum of Incident Response and Security Teams)

https://www.first.org

JPCERT/CC contributes to the international CSIRT community FIRST. JPCERT/CC also supports CSIRTs who wish to become a member of FIRST. 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. JPCERT/CC 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 2023 to test our incident response capability:

- APCERT Drill 2023 (16 August)
- ASEAN CERTs Incident Drill (ACID) 2022 (27 October)

5.2.2 Seminars & presentations

In 2023, JPCERT/CC delivered presentations at the following international cyber security events:

- JSAC2023 (January, Tokyo)
- 2023 FIRST Annual Conference and NatCSIRT Meeting (June, Montreal)
- Black Hat USA 2023 (August, Las Vegas)
- APNIC (September, Kyoto)
- Cyber Security Summit - Central Eurasia 2023 (September, Tashkent)
- Internet Governance Forum (October, Kyoto)
- Global Conference on Cyber Capacity Building (November, Accra)

...and more

5.2.3 Other international activities

Below are some of the international events that JPCERT/CC attended in 2023:

- ICANN APAC-TWNIC Engagement Forum
- NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) Locked Shields 2023
- 34th Annual FIRST Conference
- NatCSIRT Meeting
- RECON 2023
- BSidesLV
- BlackHat USA
- DEFCON
- M3AAWG General Meetings
- Virus Bulletin 2023

⋯and many more

6. Future Plans

6.1 Future projects/operation

Resume capacity building activities

JPCERT/CC aims to resume its capacity building project for national CERTs in and out of the region, which had to be suspended for several years, primarily due to travel restrictions. The team will also work with external organisations to offer training abroad, as well as to develop materials and conduct field research.

Broaden engagement in multiple areas

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

7. JPCERT/CC Contact Information

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

KN-CERT

Korea National Computer Emergency Response Team

1. Highlights of 2023

1.1 Summary of major activities

- Official Launch of the NCRMU
- A Memorandum of Understanding Signed between the ROK's KN-CERT and the US CISA to Strengthen Cooperation on Cybersecurity.
- Hosted 2023 International Conference on Building Global Cyberspace Peace Regime(GCPR)
- Held 2023 Cyber Conflict Exercise(CCE)
- On-site Exercises in Response to National Cyber Crises
- Held the 1st ICT Supply Chain Security Conference

2. About KN-CERT

2.1 Introduction

The Korea National Computer Incident Response Team(KN-CERT) of the National Intelligence Service of the Republic of Korea has been serving the mission of safeguarding national cyber security for the past 20 years since its establishment in 2004.

2.2 Establishment

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

3. Key Functions

Policy establishment and consulting

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

Threat detection and response

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

Education and training

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

Information sharing and cooperation

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

Incident investigation and damage control

- Attribution of cyber campaigns
- Providing solutions for recovery and measures to prevent recurrence

4. Education and Training

4.1 Cyber Security training

- The KN-CERT offers a professional cyber security training program through the cyber security training center in order to improve professional skills and cyber crisis response of the cyber security officers working for national public institutions.
- In 2023, The KN-CERT held training sessions for 1,491 cyber security officers with 32 courses including cyber security policy, cyber security management, security control, and malicious code analysis.

4.2 Cyber Incident Response Training

- The KN-CERT conducts drills to improve the capabilities of national and public organizations in responding to cyber

incidents and attacks against the industrial control system(ICS)

- For cyber incident response training(Cyber Guard), from August 17th to September 21st 2023, three types of cybersecurity drills – virtual network-based real-time defense; response against spearphishing email; and alert-level situation message response – were conducted for employees of 193 public institutes as part of cyber crisis response exercise.

5. Partnership

5.1 Participation in "Locked Shields 2023"

- The NCSC attended international cyber defense exercise "Locked Shields" – hosted by the North Atlantic Organization(NATO)'s Cyber Defense Center (CCDCOE) – as a joint team with Türkiye, along with about 60 personnels from ten public, private and military organizations, including the MND, Korea Electric Power Corporation, and NSR from April 18th to 21st, 2023.
- "Locked Shields" in 2023 focused on the detection of cyber incidents, real-life incident response exercises and technologies currently in operation. The ROK competed with teams from over 30 countries, including the US, the UK, and Estonia, and it was an opportunity to further our response and technical capabilities as well as to strengthen partnerships with NATO member countries.

5.2 International Cybersecurity Conference

- The KN-CERT has been holding International Conference Building Global Cyberspace Peace Regime (GCPR) in collaboration with the NSR since 2017 to discuss international norms, legal systems, and global partnership against malicious actors posing national security threats.
- In this year, "GCPR" held from September 12th to 13th, 2023. In the keynote session, The KN-CERT gave a keynote speech on "Korea's strategy for order and security" in cyberspace, and Anne Neuberger, Deputy National Security Advisor for Cyber & Emerging Technologies for the White House and Jen Easterly, CISA Director, gave a keynote lecture on the topic of order in cyberspace through a video link, and emphasized the importance of global partnership on cybersecurity.

KrCERT/CC

Korea Internet Security Center

1. Highlights of 2023

1.1 Summary of major activities

In 2023, KrCERT/CC began the year with a flurry of activity, responding to incidents at academic and research institutions as well as telecommunications companies in Korea. Two of these incidents prompted KrCERT/CC to convene a specialized public-private inspection team to investigate and announce preventive measures and victim compensation. To combat smishing, which delves into our citizens' daily lives and causes financial harm, KrCERT/CC launched a smishing risk warning service and implemented an integrated detection system to swiftly identify cyber threats, consolidating previously separate detection systems for DDoS and phishing. Furthermore, particularly in 2023, KrCERT/CC engaged in attacker group profiling, notably contributing to disrupting the revenue streams of a specific attacker group by analyzing and tracking ransomware attacks targeting enterprises. Alongside operational enhancements, efforts were made to prevent future incidents through revised systems, including enforcing incident mitigation measures by affected companies and defining incident reporting timelines.

1.2 Achievements & milestones

In 2023, KrCERT/CC remained dedicated to preventing cyber threats against citizens and businesses, while also responding to incidents. Notably, we sustained our focus on combating smishing, a persistent concern for our citizens, and mitigating the relentless ransomware attacks occurring worldwide.
Key activities in 2023 were as follows:

Preventing Direct Smishing Victimization and Empowering Citizen Response through Perceptible Risk Alerts
KrCERT/CC provided a perceptible risk warning service to assist citizens in promptly identifying and assessing smishing risks, thereby averting potential victimization. Through this service, we mitigated the risk of smishing damage resulting from past instances of inadequate feedback. Additionally, we enhanced our preventive measures by introducing a warning screen for citizens to conduct self-checks. Consequently, we successfully prevented 2,279 cases of smishing in

2023, thereby averting direct harm to the public. These efforts garnered recognition from the National Police Agency, a collaborative partner, which awarded KrCERT/CC a certificate of appreciation for its service.

Preemptive Detection and Response to Large-scale Attacks by Expanding the Integration of Detection Systems

The frequency of sophisticated attacks by international hacking organizations and state-sponsored entities, posing threats to countries, economies, and individuals, is stead. The complexity of these advanced attacks often hinders early detection. Building upon a 169% increase in detection efficiency achieved by consolidating four detection systems in 2022, KrCERT/CC embarked on validating an "integrated detection system" in 2023, integrating eight types of attack detection systems across network, service, and infrastructure domains. This initiative resulted in eliminating over 95% of cyber threats through proactive measures against national information and communication network and daily life.

Analyzing and Tracking Ransomware Attacks to Minimize Damage Inflicted by Specific Attacker Groups

KrCERT/CC preemptively thwarted ransomware attacks conducted by hacker groups Lazarus and Andariel, safeguarding approximately 78 targeted companies from extortion.[1] These attacks, which typically incurred an average loss of KRW 1.38 billion per incident, amounted to a total of $107.6 billion. By integrating generative AI technology into the existing FENS[2] profiling analysis system, we improved the accuracy of identifying correlations between incidents and revealed the attack strategies, techniques, and methodologies employed by specific attacker groups in profiling reports. The service and activities garnered recognition from partner organizations, earning both the Director's Award from National Intelligence Service and the Certificate of Appreciation from National Police Agency.

Strengthening Security Checks for Major Victim Companies of Hacking

KrCERT/CC has implemented a customized security check service for companies to prevent damage from increasingly sophisticated cybersecurity threats and hacking attacks. Specifically tailored for manufacturing companies dealing with critical technologies, vital for national competitiveness, KrCERT/CC supports mock hacking checks to prevent technology theft and production interruptions. Additionally, it facilitates security checks to enhance the stability of services offered to the public (websites, mobile apps) and fortify server security, by preemptively addressing numerous vulnerabilities susceptible to exploitation. Through these comprehensive incident prevention activities, we successfully averted KRW 61.3 billion in hacking damages. Notably, we encouraged manufacturing firms to make ongoing security investments by hiring security personnel and deploying security equipment.

---

[1] KISA. (2021, December). A Study Estimating the Economic and Social Costs of Cyber Incidents.

[2] FENS(Feature Engineering Normalization System): An analysis management that utilizes automatically extracted feature information from malware, malicious apps, victim system logs, and more to identify and correlate high-risk incidents

Integrated Response to Malicious Apps through a Collaborative Effort by Public and Prive Sectors in Support of Cybercrime Victims

KrCERT/CC partnered with telecommunications companies, antivirus developers, manufacturers, law enforcement agencies, and financial institutions to establish a unified public-private system for combating malicious apps, aiming to eradicate cyberfraud crimes. Through this collaboration, we have pioneered the eradication of cyberfraud crimes by orchestrating a unified response to malicious apps and by effectively blocking access to and preventing the installation of malicious app distribution sites. In contrast to the previous process for detecting and blocking malicious apps, which took three hours and left the public vulnerable to frequent harm, in 2023, we reduced response time to just 10 minutes through emergency blocking, significantly mitigating damages. As a result of these efforts, we successfully decreased voice phishing damage by KRW 120 billion won ,from KRW 543.8 to 421.7 billion, compared to the previous year. Furthermore, we increased our effectiveness in blocking access to malicious app distribution sites by approximately 125% ,from 762 to 1,711, compared to the previous year. Additionally, we prevented 1,171 malicious app installations, introducing a new service. These achievements were recognized by the National Police Agency for our collaboration in apprehending a cyberfraud crime organization.

Improving the Legal Framework for Reporting and Preventing Recurrence

In 2023, incidents involving personal information leaks, webpage defacement, and other incidents underscored the necessity of enhancing the legal framework for reporting and preventing the recurrence of such incidents by information and communication service providers. Consequently, the Ministry of Science and ICT and KrCERT/CC advocated for amendments to the Information and Communications Network Act to bolster the reporting system and countermeasures for infringement incidents amended in February 2024. The Enhancement of the Incident Reporting System provides clear guidelines for reporting incidents, including specified timing for 'immediate reporting' and delineated reporting methods and procedures. Additionally, the penalty for non-compliance to report such incidents has been increased threefold, from KRW 10 million to KRW 30 million. Regarding the enhancement of measures against incidents, the amendment empowers the Ministry of Science and ICT to take stronger actions against incidents. Previously limited to 'recommendations,' the authority now includes 'implementation orders,' 'implementation inspections,' and 'corrective orders.' This strengthening was necessary because compliance with these measures, such as responding to, recovering from, and preventing recurrence of incidents, was previously optional, leading to a decrease in effectiveness. Furthermore, regulations have been established to delegate the enforcement of implementation inspection methods and procedures. Failure to comply with an order to take measures against incidents now carries a penalty of 'not more than 30 million won'.

2. About CSIRT

2.1 Introduction

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

2.2 Establishment

KrCERT/CC was established in 1996 as a small team responsible for hacking incidents under the Korea Information Security Agency (a former KISA). Since its foundation, it has responded to and handled numerous security issues and tasks. The first major incident was the Internet Crisis caused by so-called 'slammer worm' in 2003. At that time, KrCERT/CC had difficulties in communicating efficiently with a telecommunication carrier, which marked the turning point for the Korean Government to recognize the importance of cooperation with security incident response teams and businesses such as ISP. As a result, the Security Incident Response Team was established under the former KISA in December 2003, and has evolved into its current form by responding to major national security incidents that occurred in 2007, 2009 and 2013. Domestically it is usually called KISC, or the Korea Internet Security Center.

2.3 Resources

As of December 2023, about 130 employees from 3 divisions work for KrCERT/CC.

2.4 Constituency

KrCERT/CC serves as the focal point to coordinate security incidents in the Korean cyberspace. According to the national cyber security framework and related legislation, mainly in Information and Communications Network Act, KrCERT/CC is responsible for handling incidents and ensuring the security of information systems and networks in the private sector, such as the telecommunication sector and home users. At the international level, KrCERT/CC cooperates with many leading and national CERTs/CSIRTs, international organizations, and security vendors.

3. Activities & Operations

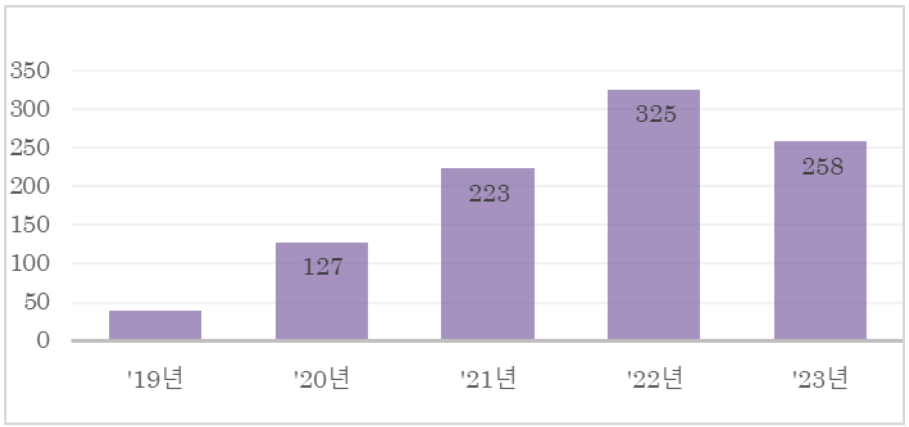
3.1 Scope and definitions

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

3.2 Incident handling reports & Abuse statistics

KrCERT/CC's incident response scope encompasses all cybersecurity incidents involving Korean citizens and businesses. While not all statistics are publicly disclosed, below are some of the incident figures available:

- Ransomware: Despite a significant surge since 2019 and ongoing harm to companies caused by ransomware, the number of ransomware reports in 2023 went down, compared to the previous year.



- As HTTP-based malware distribution has been increased since 2006, KrCERT/CC has maintained a detection and response system against web-based malware. Furthermore, it has strengthened to monitor the spread of malware through file-sharing and free software distribution. In 2022, there was a significant increase in IoT malware distribution site detected, nearly doubling the number of waypoints. In 2023, we observed a further rise in distribution site detections, attributed to the enhanced performance of our website monitoring systems.

Year	2019	2020	2021	2022	2023
Distribution site	566	738	2,584	4,354	7,307
Landing site	7,733	5,296	4,459	9,307	5,424
Total number	8,299	6,034	7,043	13,661	12,731

Table 1. The Number of Detection of Malware Distribution

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

- KrCERT/CC initiated its service in 2011 to alert infected PC users about malware infections via pop-up windows, aiming to mitigate the spread of incident damage, including DDoS attacks and spamming. As mobile malware distribution intensified in the latter half of 2012 and surged in 2013, the service expanded its scope to include mobile devices, notifying users of infected devices such as PC and mobile and guiding them to implement security measures through general antivirus treatment and inspection. In 2023, a total of 110,947 malware-infected devices were detected and notified, enabling users to take necessary security precautions. The analysis of the decreased in infection notifications suggest that security enhancements such as generalization of HTTPS ad other security measures, coupled with a decrease of PC users, have had an impact.

Year	2019	2020	2021	2022	2023
Number of Cases	297,208	436,025	179,544	212,953	110,947

Table 2. The Number of Malicious Infection Notification

3.3 Publications

In 2023, KrCERT/CC released six reports, including two secure coding guides (for JavaScript and Python), two technical reports covering the Black Cat and Xiaoqiying incidents, and two reports on attacker strategy analysis and vulnerability analysis. Additionally, KrCERT/CC distributed the 2023 Cyber Threat Trends Report (First half of the year) and the 2024 Cybersecurity Threat Outlook Report. These reports are accessible on the KrCERT/CC website at www.boho.or.kr.

3.4 New services

New services introduced in 2023 include the following:

- Establishment of a joint public-private malicious app response system to swiftly block the distribution and installation of malicious apps on devices
- Identification of victim companies undergoing ransomware attacks and removal of malicious code through analysis of incident data
- Preemptive detection and response to signs of large-scale cyberattacks by integrating information from individual

detection systems

- Focused identification of high-risk vulnerabilities with significant impact and implementation of an automatic responsive system
- Development and deployment of hacking diagnostic tools enabling companies to independently identify being detected

4. Events organized / hosted

4.1 Training

KrCERT/CC has conducted trainings, inviting both internal and external experts to facilitate information sharing and knowledge exchange among employees. The internal trainings held in 2023 were as follows:
Legal system and safety measures for personal information leakage incidents (Feb)
Protected Country Homepage Administrator User Manual (Feb)
DNS Security and Threats for Incident Responders (March)
Phishing and Bitracker Incident Case Sharing (June)
Utilizing Super-sized AI Models for Natural Language Processing (NLP), Transformer Models, and ChatGPT (June)
SME Incident Support Service in 2023(June)
AI Era, Technology Trends, and Utilization (July)
APCERT Cyber Drill (Aug)
Generative AI Analysis/Response Utilization and Analysis System (Sept)
Metaverse Security: Checklist and Countermeasures for DDoS Attacks in the Enterprise Infrastructure Environment (Sept)
Sharing RF hacking and incident response using SDR (Sept)
Practical cyberattack defense drill(ELECCON) methodology and development plan (Oct)
Understanding and utilizing malicious app analysis solutions (Nov)
Customized anti-malware technology with XAI technology (Dec)
Trends in code signing certificate-related incidents (Dec)
In addition, KrCERT/CC conducted both online and offline APISC incident response training sessions for external organizations in October, 2023.

4.2 Drills & exercises

Private Sector Cyber Crisis Response Drills: First and Second Half

4.3 Conference

2023 Blockchain Meetup Conference (2023 BCMC)(April, KISA)
The 29th Information Communication Network Information Protection Conference
(NetSec-KR 2023)(April, KISA)
The 12th International Information Protection Conference on the day of Information Protection (July, KISA)
The 2nd Ransomware Resilience Conference (Sept, KISA)
The 15th CODEGATE (Nov, KISA)
2023 AI Security Global Festa (Nov, KISA)
MyData Conference 2023 (Nov, KISA)
The 13th Software Development Conference (Nov, KrCERT/CC)
The 28th Hacking Prevention Workshop (Dec, KrCERT/CC)

5. International Collaboration

5.1 International partnerships and agreements

KrCERT/CC exchanges MoU(Memorandum of Understanding) with CSIRTs among APCERT members.

5.2 Capacity building

5.2.1 Training

- APCERT – 5G vulnerability Analysis(May)
- APCERT – DNS Security and Threats for Incident Responders(Jul)

5.2.2 Drills & exercises

- 2023 APCERT Cyber Drill(Aug)
- 2023 ASEAN Cyber Incident Drill(Oct)

5.2.3 Seminars & presentations

- 2023 GCCD (Nov)

6. Future Plans

6.1 Future projects

Moving forward, KrCERT/CC aims to enhance security diagnosis support for small and medium-sized enterprises, address challenges in implementing software development security, boost analysis capabilities through AI, and broaden profiling research to reinforce preemptive measures. Additionally, we will advocate for mandatory development of patches for high-risk vulnerabilities to mitigate their spread at an early stage.

7. Conclusion

As highlighted in the summary ahead, a year of 2023 proved to be a demanding for KrCERT/CC, marked by significant incident responses early on. Despite several challenges stemming from lack of resources, KrCERT/CC successfully launched a few of new prevention, response, and recovery initiatives for both the public and businesses, earning recognition through numerous certificates of appreciation and awards from external organizations. KrCERT/CC will continue to endeavor to establish relevant regulations and improve support services in order to create a secure cyberspace of South Korea.

LaoCERT

Lao Computer Emergency Response Team

1. Highlights of 2023

1.1 Summary of Activities

- Co-host The Seminar on Cybersecurity for Critical Information Infrastructure in Pursuance of Digitalization on 1 March 2023 at Crowne Plaza Hotel, Vientiane Capital, Lao PDR
- Co-Organized Workshop on Cyber Security and Cyber Incident Response "CSIRT Essentials on 12-13 September 2023 in Vientiane Capital, Lao PDR,
- Co-host Workshop on Cybersecurity Capacity Building for Policymakers and Cyber Diplomats on 20-21 September 2023 in Vientiane Capital, Lao PDR, Participants from Banks, ISPs, Private sectors, and related Ministries

1.2 Achievements & milestones

- To establish Security Operation Center (SOC)
- To be full operation

2. About LaoCERT

2.1 Introduction

Lao Computer Emergency Response Team (LaoCERT) is the national CERT of Lao PDR, under, Ministry of Post and Telecommunications and it develop on capacity building for its staffs in the field of cyber security with other CERTs organizations in the region to against with cyber-attack. LaoCERT has been promoted to public and has been known among IT social, government agencies, private organizations in Laos PDR as well as international CERTs and LaoCERT was a member of APCERT in 2014. This annual report will describe activities and operation of LaoCERT in 2023.

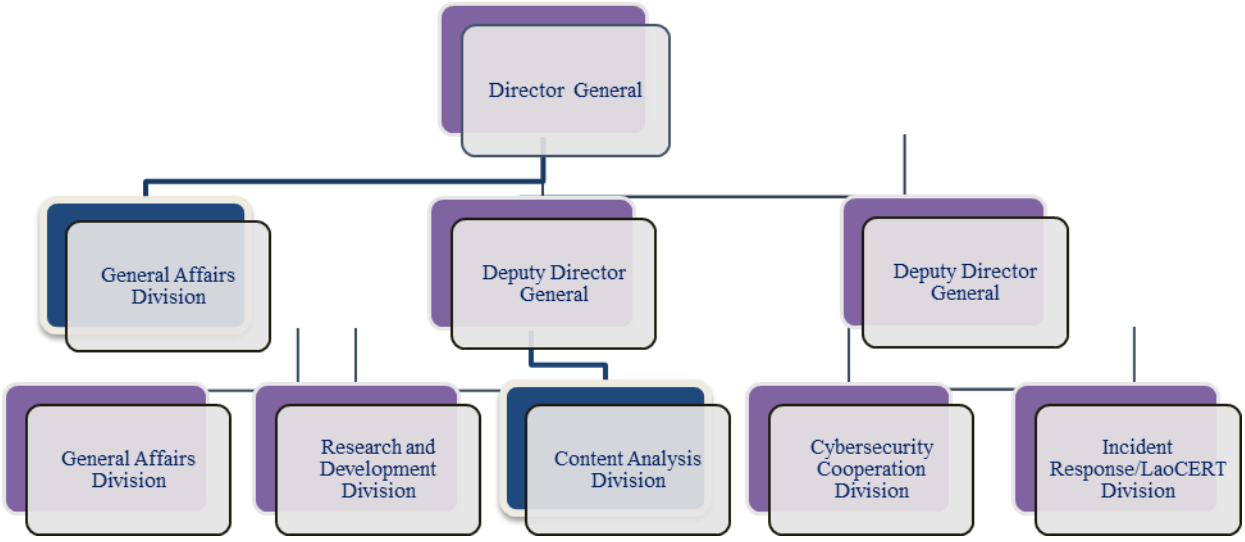
2.2 Establishment

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/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 Laos PDR.

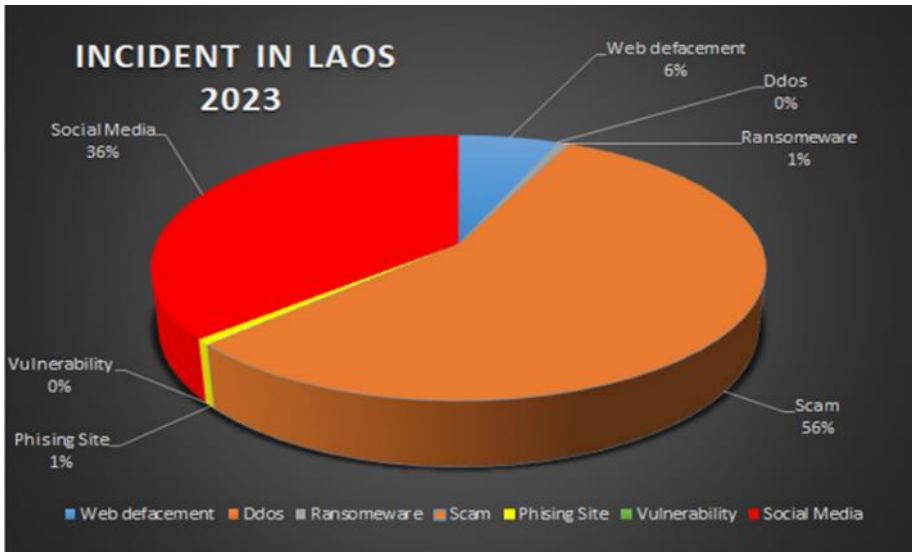
3. Activities & Operations

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.

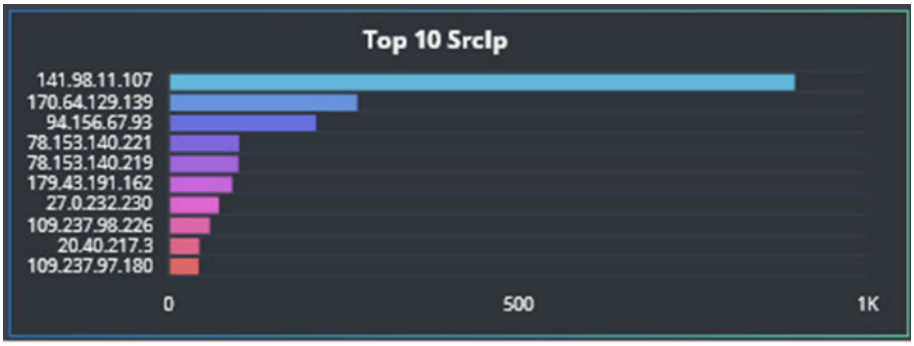
3.2 Incident handling report

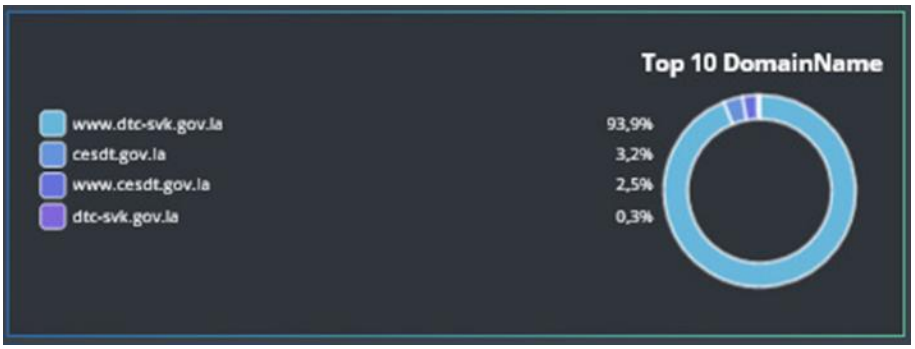
The following graph shows the statistic of incidents that happened in 2023.

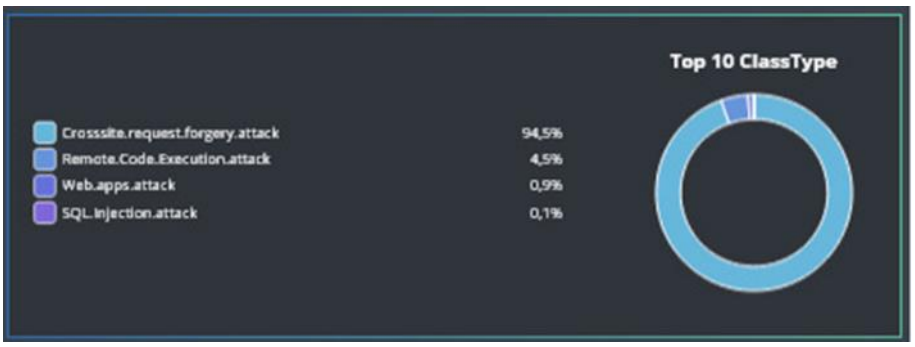


3.3 Abuse Statistics

The following graph shows Abuse Statistics in 2023:







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

- 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

- Training on Enhancing Information Security and Social Media Security Practices for Provincial Authorities in Lao PDR

4.2 Conferences and seminars

- Co-host The Seminar on Cybersecurity for Critical Information Infrastructure in Pursuance of Digitalization on 1 March 2023 in Vientiane Capital, Lao PDR
- Co-Organized Workshop on Cyber Security and Cyber Incident Response "CSIRT Essentials on 12-13 September 2023 in Vientiane Capital, Lao PDR.
- Co-host Workshop on Cybersecurity Capacity Building for Policymakers and Cyber Diplomats on 20-21 September 2023 in Vientiane Capital, Lao PDR

5. International Collaboration

5.1 International partnership and agreement

In 2023, LaoCERT did not sign any agreement on cooperation plan yet, however, we are now planning to prepare the contract for joint activities in cybersecurity field with ASEAN countries, international organizations, and the national CERT.

5.2 Capacity Building

5.2.1 Training

The following has shown the statistic for attended the training in 2023:

- The 25th ASEAN-Japan Cybersecurity Building Centre Training (AJCCBC) on 19-23 June 2023 in Bangkok, Thailand.
- Training on Malware Analysis (Advanced Level) from 26-30 June 2023 in Manila, Philippines.
- The Regional Ransomware Training Course from 26–28 July 2023 in Manila, Philippines.
- Training on Capacity Building in International Law and Policy Formation for Enhancement of Measures to Ensure Cyber Security from 21-25 August 2023 in Tokyo, Japan.
- The Enhancing Capabilities of Public and Private Sector to Implement Regional Digital Agenda for CLMV Countries training from 29-31 August, 2023 Danang, Viet Nam.

- The 26th ASEAN-Japan Cybersecurity Building Centre Training (AJCCBC) on 28 August-01 September 2023 in Bangkok, Thailand.
- The 27th ASEAN-Japan Cybersecurity Building Centre Training (AJCCBC) on 16-20 October 2023 in Bangkok, Thailand.
- The 28th ASEAN-Japan Cybersecurity Building Centre Training (AJCCBC) on 18-22 December 2023 in Bangkok, Thailand.

5.2.2 Drills and Exercises

The following has shown the statistic for participated Drills and Exercises in 2023:

- APCERT Cyber Drill 2023.
- ASEAN CERT Incident Drill (ACID) 2023
- The 5th ASEAN Students Contest on Information Security 2023 (ASCIS 2023) host by Vietnam via online.
- Attend the Cyber SEA Game 2023 on 9-10 November 2023 at the AJCCBC' in Bangkok, Thailand.
- The ACS Cybersecurity Defense Competition on 20-24 November 2023 in Jakarta, Indonesia.

5.2.3 Seminar and presentation

The following has shown the statistic for participated the Seminar, Workshop and Meeting in 2023:

- The Workshop for the 13th ASEAN-Japan Information Security Workshop for ISPs on 26-27 January 2023 in Tokyo, Japan.
- The Workshop on Cyber Security from 6-10 February 2023 in Singapore.
- The 1st ASEAN-Japan Cybersecurity Working Group Meeting on 14-15 February 2023 in Philippine.
- The Workshop Cyber Security and Cyber Incident Response Essentials "CSIRT Essentials" on 17th – 19th May 2023 in Cambodia.
- The Course on International Law of Cyber Operations from 22–26 May 2023 in Singapore.
- The 2nd ASEAN-Japan Cybersecurity Working Group Meeting on 23-24 May 2023 in Brunei Darussalam.
- The Comprehensive Security Cooperation (CSC) workshop from 24 May-29 June 2023 in U.S.A
- The Global Cyber Policy Dialogues: Southeast Asia from 3 - 4 July 2023 in Singapore
- The workshop on International Law of Cyber Operations from 3–7 July 2023, at the ASEAN- Singapore Cybersecurity Centre of Excellence (ASCCE), Singapore.
- The 8th Annual Meeting of the Cyber Security Alliance for Mutual Progress (CAMP) on 11-13 July 2023 in Seoul, South Korea.
- The 3rd ASEAN-Japan Cybersecurity Working Group Meeting on 01-04 August 2023 in Hanoi, Vietnam.
- The Seminar on Network Security and Information confrontation for Developing Countries from 11th - 24th September 2023, in China.
- The Workshop on Cybersecurity Capacity Building for Policymakers and Cyber-diplomats on 25-26 September 2023 in Siem Reap, Cambodia.
- The 16th ASEAN-Japan Cybersecurity Policy Meeting on 03-04 October 2022 in Japan.
- The JP-US-EU Industrial Control Systems Cybersecurity Week for the Indo-Pacific Region from 9-13 October 2023

in Japan.

- The 08th Singapore International Cyber Week (SICW) and ASEAN Ministerial Conference on Cybersecurity (AMCC) on 16-19 October 2023.
- The Seminar on Building Cyber Capabilities with the Global South on 23-24 October 2023 in Florence, Italy.
- The Workshop on the International Law of Cyber Operations from 15 – 17 November 2023 in Singapore.

6. Future Plans

- Continue to provide training and seminar on Cybersecurity to provincial both public and private sector throughout the country.
- Continue to collaboration to exchange the lessons and experiences on the development of legislation, laws, and information on developing an online social media management system among National CERT, international organization, and related sectors in the field of cybersecurity.
- Complete the drafting and issue the Cybersecurity Law on or before the end of 2024.
- Finalize the drafting and release the National Cybersecurity Strategy by mid-2024.
- Expanding the awareness raising on Cyber Crime Law and data protection Law.
- Planning to establish a Cyber Security Operations Center (SOC) and now is under the coordination and set up the room.
- Planning for Establishing Government Threats Monitoring (GTM).
- Planning to set up the Network Monitoring System.

7. Conclusion

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

mmCERT

Myanmar Computer Emergency Response Team

1. Highlights of 2023

1.1 Summary of major activities

For the purpose of effective incident response services, mmCERT contributed to the APCERT Drill, ACID Drill, and Tabletop Exercise yearly. In terms of capacity building, mmCERT encourages international, regional, and local trainings for government officials and students. As part of the awareness-raising campaign, the "Cybersecurity Awareness Video Competition - 2023" was successfully organized for university students.

1.2 Achievements & milestones

- Myanmar served as the Chair at the 14th ANSAC Meeting in Bali, Indonesia.
- Myanmar presented as a speaker at "the ASEAN Workshop on the Implementation of Artificial Intelligence on Energy Security, Agriculture, Cyber Security, and Creative Industry" held virtually from 7th to 8th September 2023.
- Organized the "Myanmar Cyber Security Challenge - 2023" on 5th August, 2023.
- Virtually hosted Cyber Security Awareness Video Competition - 2023 for university students under 30 years old. Following this local competition, the winning video was submitted to "the ASEAN-Japan Cyber Security Awareness Video Competition-2023" organized as a coordination activity in the cyber security awareness raising domain.
- NCSC conducted Cyber Security Awareness Trainings for government officials in August, September, October, and November.
- "Cyber Security Policy Workshop" was held on 1st November 2023 in Nay Pyi Taw. In this event, Cyber Security Policy, approved by the meeting of the Government of the Union of Myanmar No. (9/2022), was discussed among representatives from the Information Technology and Cyber Security Department, as well as CIOs, ACIOs from ministries and government organizations.

2. About CERT

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 of MOTC.

2.3 Resources

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

2.4 Constituency

mmCERT 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 are 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

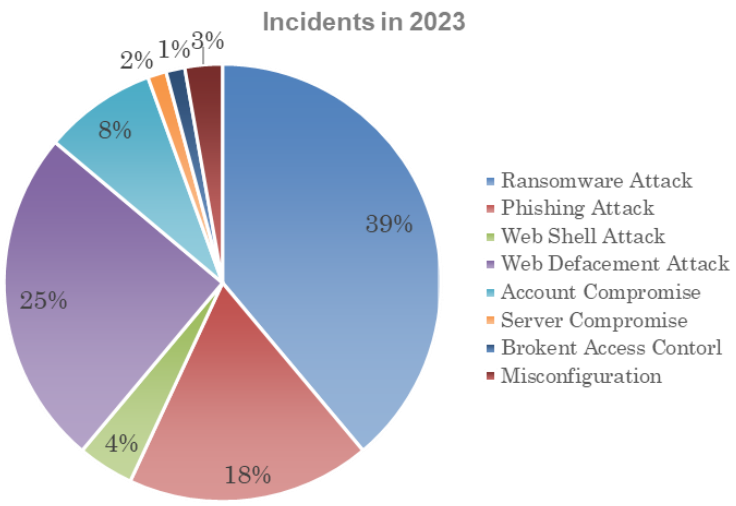
- Creates National IT image by collaborating with international CERT teams for cybersecurity and cybercrime.
- Disseminates security information and advisories.
- Provides technical assistance.
- Collaborates with law enforcement organizations for combating cybercrime

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, ransomware attacks remain a prominent type of incident. mmCERT has closely coordinated with government organizations to respond to cyber incidents, mitigate their impact and implement preventive measures.

3.3 Abuse statistics

The following graph shows the incidents statistics handled by mmCERT in 2023.



3.4 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://ncsc.gov.mm/wp-content/uploads/2022/06/STOPRansomwareGuide1.4.pdf
- "PlugX Removal Guide (Version 1.1)" was also released to help victims of PlugX RAT understand the tactics of this RAT and the eradication method.
  https://ncsc.gov.mm/wp-content/uploads/2022/06/PlugXRemovalGuideVersion1.1.pdf
- "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://ncsc.gov.mm/wp-content/uploads/2022/12/Guidebook-for-Suspicious-Mails-Version-1.0_with-cover.pdf

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

3.5 New services

To provide prompt assistance for incidents, mmCERT/cc offers the following contact points:

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

4. Events organized / hosted

4.1 Training

- In collaboration with the Ministry of Home Affairs, NCSC provided training for police officers in June and November 2023.
  https://www.mmcert.org.mm/index.php/en/activity/2023-08-22t2325560630
- NCSC conducted a Cyber Security Awareness Program at the Central Bank of Myanmar from 16th October to 10th

November , 2023.
https://www.mmcert.org.mm/en/activity/2023-11-08t1811220630

- Training for "Capacity Building Training (1/2023)" was offered at the Information & Public Relation Department (Nay Pyi Taw), Ministry of Information in November 2023. There were a total of 22 attendees from district and division branch offices in this training.
https://www.mmcert.org.mm/mm/activity/2023-11-30t1930220630
- NCSC provided Cyber Security Awareness to mid-level officers at the Internal Revenue Department during August, September, October, and November 2023.
https://www.mmcert.org.mm/en/activity/2023-10-27t1441460630

4.2 Drills & exercises

- Myanmar Cyber Security Challenge-2023 was held at Nay Pyi Taw on 5th August, 2023. The total 25 teams of university students and young professionals participated in this event.
https://ncsc.gov.mm/en/myanmar-cyber-security-challenge-2023-open-level2/

4.3 Conferences and seminars

- MOTC organized the "Safe ICT Service" Dialogues and Workshop on 17th February, 2023. CIOs and ACIOs from government agencies attended and participated in discussions at this event.
https://www.mmcert.org.mm/en/videos/2023-08-31t2132170630

- In July 2023, mmCERT provided knowledge sharing workshops at the universities to promote the participation of students in MCSC Challenge and to understand the cyber security challenges.

4.4 Other activities

- NCSC arranged for participants to join the 1st ASEAN Cyber Shield Hacking Contest from 21st to 24th November, 2023, in Indonesia.
  https://www.mmcert.org.mm/mm/news/2023-11-20t1011040630
- mmCERT arranged and supervised Myanmar students to participate in the 5th ASEAN Students Contest on Information Security (ASCIS) 2023 in October.
  https://www.mmcert.org.mm/en/events/2023-09-02t1006510630
- To raise cybersecurity awareness among young people, parents, government personnel, and citizens, ITCSD participated in the "Youth, Literature, and Art Show" from 20th to 22nd December, 2023, at Wunna Theikdi Stadium, Nay Pyi Taw. Cyber Security Awareness Booklets were distributed, and a Cyber Security Quiz was conducted during these days. Remarkable participants were presented with gifts, and the six participants who achieved the highest marks in Basic Education High School and University Level were awarded prizes.

- Cybersecurity Awareness Video Competition-2023 was held virtually and the top 5 videos were rewarded on 1st November 2023. There were 47 videos from the university students under 30 years old. The 1st winning video of Myanmar was submitted to the ASEAN-Japan Cybersecurity Awareness Video Competition 2023 and took the 6th position among ASEAN-Japan contestant videos.

5. International Collaboration

5.1 International partnerships and agreements

Myanmar and Russian Federation signed "Agreement between the Government of the Russian Federation and the Government of the Republic of the Union of Myanmar on Cooperation in the field of International Information Security" on 5th December, 2023.

5.2 Capacity building

5.2.1 Training

- A member of mmCERT virtually attended the APT Online Training Course on the Utilization of ICT Services to Achieve Future Digital Community from 31st January to 14th February, 2023.
- A member of mmCERT virtually attended the Training Course on Cyber Forensics provided by India in February 2023.
- A member of NCSC attended the "Executive Course on International Law of Cyber Operation" provided by ASCCE, Singapore in May 2023.
- Two members of mmCERT attended the Cybersecurity Evaluation Tool (CSET) Training provided by AJCCBC and USA from 10th to 13th July, 2023, in Thailand.
- Members of NCSC virtually attended technical skill training related to incident response using a CTF format in October 2023.
- A member of mmCERT attended the APT Online Training Course on Internet of Things and Cyber Security in the Era of Big Data during 8th to 14th October, 2023.
- A member of mmCERT attended the 2023 APISC Security Training Course hosted by KrCERT/cc from 23rd to 28th October, 2023 in Seoul, Korea.

5.2.2 Drills & exercises

- Also joined APCERT Drill in July 2023.
- Participated in the "Tabletop Exercise" during the 3rd ASEAN-JAPAN Cybersecurity Working Group Meeting of 2023 held in Vietnam.
- mmCERT/cc participated in ACID Drill in October 2023.

5.2.3 Seminars & presentations

- Participated in the "Sharing Sessions" hosted by SingCERT twice a year among ASEAN Member States. mmCERT/cc also shared "Local Threat Landscape of Myanmar" in these sessions.
- One of NCSC member performed as a speaker at "the ASEAN Workshop on the Implementation of Artificial Intelligence on Energy Security, Agriculture, Cyber Security, and Creative Industry" held virtually during 7th to 8th September, 2023.
- Discussed in the "3rd ASEAN-U.S. Cyber Policy Dialogue" held virtually on 1st February, 2023.
- Joined virtually in the INTERPOL Global Cybercrime Conference on 15th-16th February, 2023.
- Participated virtually in Cybersecurity Standards and Conformance to Support Digital Trade in ASEAN on 24th May, 2023.
- Joined virtually in APT Web Dialogue "Challenges and Opportunities in addressing Online Scams" on 31st May, 2023.
- The two attendees joined virtually the "ASEAN Regional Forum Workshop on Terminology in the Field of Security of and in the Use of ICTs in the Context of Confidence Building" on 21st June, 2023.
- Attended the Discussion on ASEAN Cyber Shield on 16th August, 2023.
- Joined virtually the "Operational Technology Cybersecurity Expert Panel (OTCEP) on 22nd-23rd August, 2023.
- Joined the event "Racing Against the Clock: Pushing Forward with Child Online Protection in the ASEAN Region - Consolidation of Regional Cooperation under the Indonesia ASEAN Chairmanship in 2023" held online on 27th September, 2023.
- Joined virtually "the 18th Internet Governance Forum (IGF)" during 8th-12th October, 2023.
- Virtually attended the "3rd ASEAN-Russia Dialogue on ICT Security-related Issues" on 18th December, 2023.

5.3 Other international activities

- The two attendees participated in the Personal Data Protection (PDP) Week 2023 in Singapore during 18th-21st July, 2023.
- Attended the 6th ASEAN Data Protection and Privacy Forum held on 21st-22nd August, 2023, in Bali, Indonesia.
- Myanmar served as the chair at the 14th ASEAN Network Security Action Council (ANSAC) Meeting held in Bali, Indonesia, in August.

- Closely coordinated with ASEAN-JAPAN Cybersecurity Working Group. Attended 1st AJCWG Meeting in Philippine, 2nd AJCWG Meeting in Brunei and 3rd AJCWG Meeting in Vietnam. Myanmar continues to join and participate in the following Coordination Activities of ASEAN-JAPAN Cybersecurity Working Group:

i. Cybersecurity Policy Reference
ii. Voluntary Mutual Notification Program
iii. Cyber Exercises
iv. Joint Awareness Raising
v. Capacity Building and
vi. CIIP Workshop

- mmCERT arranged and supervised students to participate in the 5th ASEAN Students Contest on Information Security (ASCIS) 2023 in Vietnam during October 2023.
- mmCERT arranged the participants to join the 1st ASEAN Cyber Shield Hacking Contest from 21st to 24th November, 2023 in Jakarta, Indonesia.

- NCSC arranged the participants to join the Cyber SEA GAME 2023 - ASEAN Cybersecurity Competition by AJCCBC in November 2023.

6. Future Plans

6.1 Future projects

- Public Key Infrastructure Project is being implementing.
- It is planned to conduct Cyber Security Awareness Raising Workshops and Trainings for CIOs and ACIOs from government agencies.
- Cyber Security Awareness Video Competition-2024 has been planned to enhance the cyber security knowledge among younger ages.
- A Cyber Security Awareness Survey will be conducted as a collaborative activity with the ASEAN Member States.

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.
- Cyber Security Awareness Movies will be produced for broadcast media and other social media platforms.

- 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

During the year 2023, we had established more engagement with the students and young professionals in the cybersecurity field. mmCERT remains committed to enhancing the nation's cybersecurity capabilities and promoting public awareness about the importance of safeguarding personal information by managing security risks effectively.

MNCERT/CC

Mongolia Cyber Emergency Response Team/Coordination Center

1. Highlights of 2023

1.1 Summary of major activities

MNCERT/CC has successfully organized its annual event and cyber security competition on-site. The biggest cyber security event of Mongolia MNSEC2023 has covered larger scope of participants than the last few years and continued for two days for the public.

“Haruulzangi U18” CTF among high school senior grade students and “Haruulzangi 2023” CTF among security specialists had been held successfully by MNCERT/CC.

One of the key achievements was that MNCERT/CC is cooperating as a consultant with Public CERT which was established in 2023.

1.2 Achievements and milestones

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

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

We continued providing our member organizations with threat intelligence, indicators, threat actor information using MISP open-source threat intelligence and sharing platform. We had a new collaboration with Arctic security hub which provided us with a daily observation report including artifact, backdoor, blocked resources, breached data, C&C connection, compromised account, potential DDOS and much more information related to our constituency assets.

One of the key achievements of this year was the continuation of “HaruulZangi” and “HaruulZangi U18” cyber security competitions which were held on-site. Winners of the contest expressed their impression that the missions were more exciting and challenging than the past years.

MNSEC 2023 event included an offsite networking day beside the official event and covered over 400 participants which

are a relatively large percentage of the security sector of Mongolia.

2. About MNCERT/CC

2.1 Introduction

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

2.2 Establishment

"MNCERT/CC" was established on March 15th, 2014 and founded on following grounds:
Based on the component of information security of the Mongolian National Security Concept and National program for Cyber security, the 48th resolution was approved by Mongolian State Great Hural (State Great Assembly) in 2010:

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

2.3 Resources

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

2.4 Constituency

Our constituencies are:

- Internet Service Provider Companies
- Banks
- Mobile Operator Companies
- Universities
- other CERT organizations and
- General public

3. Activities & Operations

3.1 Scope and definitions

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

4. Events organized / hosted

4.1 Training

4.1.1 Members meeting and training

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

4.2 Drills & Exercises

4.2.1 Cyber drill

MNCERT/CC has organized the local cyber drill among the member and non-member organizations under the scenario of digital supply chain. The goal of the drill was to practice incident response capability of local organizations. The scenario simulated that the cloud service provider was infected with malware and the attackers compromised the constituency's virtual server and they caused unauthorized data modification and data leakage using a backdoor. The drill was held with 21 tasks of 5 stages. Throughout the exercise, the participating organizations activated and tested their incident handling arrangements. This drill included the need for participants to interact locally with MNCERT/CC.

4.2.2 "HaruulZangi 2023" National Cyber Security Competition

Haruulzangi CTF competition was organized by MNCERT/CC in collaboration with volunteers consisting of cybersecurity specialists and students and the support of our sponsors. The competition of 2023 consisted of three rounds: an online Round-1 held on 23th September, onsite Round-2 held on 1st of October at Nest Education High School and an onsite final Round held at Shangri-La Ulaanbaatar hotel on 5th October.

The primary objectives of the CTF competition were to enhance security enthusiasts', specialists' and public's understanding of the risks associated with cybersecurity and cyber attacks in the internet environment. The competition aimed to push the cybersecurity specialists' skill, challenge their limit and motivate them to do everything they do with cybersecurity in mind.

By actively participating in the CTF competition, specialists were exposed to real-world cybersecurity challenges and problem-solving scenarios. The competition fostered critical thinking skills, analytical reasoning, and technical knowledge related to cybersecurity concepts. In addition to that, the final round has been organized in an Attack and Defense style, thus, players are challenged to not only attack or find holes in the system, but also to defend their given system, services.

The goals of the competition were as follows:

- To raise awareness among the IT industry specialists and public about the importance of cybersecurity in today's interconnected world.
- To demonstrate the potential risks and vulnerabilities present in various online platforms and services.
- To encourage players to challenge their limit and, keep the cybersecurity in mind, whenever they take an action.
- To provide a platform for every player to showcase their skills, creativity, and innovative approaches to solving cybersecurity challenges.
- To facilitate networking opportunities with industry professionals and cybersecurity experts, enabling everyone to gain insights into potential knowledge sharing and lifelong friendship.

Through these objectives and goals, the CTF competition aimed to make a lasting impact on Mongolian cybersecurity specialists. As the community matures, Haruulzangi aims to become the National level Cybersecurity Challenger in Mongolia.

The first round of the Haruulzangi 2023 CTF competition was conducted online and lasted for a duration of 4 hours.

Participants were presented with a total of 20 challenges across various categories, including AWS, Crypto, Forensic, MISC, PWN, Reverse and Web.

The prequalified round-2 of Haruulzangi 2023 CTF took place on-site. The top 30 + 2 (high school teams) from the first round gathered on-site to compete for the final round of Haruulzangi 2023. The Second Round followed a Jeopardy-style capture-the-flag format, where teams raced against the clock and each other to solve a series of hands-on cybersecurity challenges. These challenges required participants to apply their technical skills, critical thinking abilities, and teamwork in order to overcome the obstacles and accumulate points.

The highly anticipated final round of the Haruulzangi 2023 CTF competition, themed around milestones of Haruulzangi since first it has been organized, took place at Shangri La Ulaanbaatar Hotel along with the MNSEC 2023 Cybersecurity event. The top 10 teams from the second round gathered on-site.

4.2.3 "HaruulZangi U18 2023" National Cyber Security Competition

Haruulzangi U18 CTF competition was organized by MNCERT/CC in collaboration with volunteers consisting of cybersecurity specialists and students and the support of our sponsors. The competition of 2023 consisted of two rounds: an online round held on 20th May and an onsite round held at Nest Education High School on 27th May.

The primary objectives of the CTF competition were to enhance high school pupils' understanding of the risks associated with cybersecurity and cyber attacks in the internet environment. The competition aimed to introduce them to the field of cybersecurity at an early age, sparking their interest and potential career choices in this domain.

By actively participating in the CTF competition, high school pupils were exposed to rthreal-world cybersecurity challenges and problem-solving scenarios. The competition fostered critical thinking skills, analytical reasoning, and technical knowledge related to cybersecurity concepts

4.3 Conferences and seminars

4.3.1 MNSEC 2023 Virtual Event

MNCERT/CC has been organizing the MNSEC cybersecurity conference since 2014. MNSEC2023 was held on 5th and 6th of October at the Shangri-La Ulaanbaatar Hotel Ballroom. The main goals of the conference are to share information, gain knowledge and experience, and learn from others, for amateurs and professionals in the cybersecurity field, and build professional connections with one another. The MNSEC has been extended over the years and has become the biggest cybersecurity conference and meeting in Mongolia.

By attending the conference, the cybersecurity professionals, students, and researchers are sharing their knowledge and experience and building professional networks with fellow professionals, and for the organizations, MNSEC is offering sponsor options with the benefit of promoting their products, increasing their market share and headhunting opportunity for the young talents. The conference program consisted of 2 days of full schedule that had 16 speeches and other fun & team building activities. The total number of attendees was 400.

The speeches were about Implications and Effects of Large Language Models for Cybersecurity, Mongolian IP address's reputation, Threat landscape through VirusTotal, Mongolian's hacked data through the darkweb, Infrastructure Tracking and Visualization of Modern Threat Actors, Mining Bots, Mitigating Digital Fraud: The Role of Technological Solutions,

Cyber Threat Landscape for Mongolia (2022-2023), Using a Kill Chain to Kill Everything, Full Circle: Role of CERT/CSIRT after 35 years and Security of Cloud Technology – How to Secure Cloud Email Senders from Impersonation. In other words, regardless of their knowledge base and position, everyone who attended the conference could learn something new within their interested areas.

5. International Collaboration

5.1 International partnerships and agreements

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

5.2 Capacity building

5.2.1 Training

- MNCERT/CC attended KrCERT/CC training held by KrCERT/CC and KISA on October 2023.

5.2.2 Seminars & presentations

- MNCERT/CC attended to APCERT VIRTUAL AGM 2023.
- MNCERT/CC attended Annual FIRST conference 2023, at Montreal, Canada, on June 4–June 9, 2023.

6. Future Plans

6.1 Future Operations

MNCERT/CC planned the following activities in 2024.

Events, conferences and drill to participate are as follows:

- APCERT Annual General Meeting 2024.
- APCERT Drill 2024.
- FIRST CON 2024.

Local activities to organize are as follows:

- MNSEC 2024 Cyber Security Event
- “Haruulzangi 2024” CTF Contest among security specialists
- “Haruulzangi U18 2024” CTF Contest among high school pupils
- Local cyber drill among member organizations
- “Red team” drill among bank and financial sectors
- Local training for our constituency.

7. Conclusion

We are looking forward the year 2024 to be a more progressive year in both local and international stage and greater collaboration with APCERT and other international organizations.

SingCERT

Singapore Computer Emergency Response Team

1. Highlights of 2023

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 2023:

i. One-stop Ransomware Portal
   Provides aid to ransomware victims seeking recovery support while providing organisations with access to ransomware related resources.

ii. Exercise Cyber Star (XCS23)
   Improves Singapore's crisis response capabilities and readiness to respond promptly and effectively to a cyber-attack.

iii. Cloud Security Companion Guides for Organisations
   Helps small-medium enterprises (SMEs) understand what they and their providers each need to take care of to secure the cloud environment.

iv. 7th Edition of Singapore Cyber Landscape
   Highlights facts and figures on significant cyber threats and incidents in Singapore for 2022.

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/Explore/who-we-are/our-identity/about-singcert
- Email: singcert@csa.gov.sg

2.2 Establishment

SingCERT was first set up in October 1997 by the then-Infocomm Development Authority of Singapore (IDA), in collaboration with the Centre for Internet Research, National University of Singapore (NUS). SingCERT transited to the Cyber Security Agency of Singapore (CSA) when it was established on 1 April 2015.
CSA is the national body overseeing cybersecurity strategy, operation, education and outreach, technology, and industry development for Singapore's critical information infrastructure. It is managed by the Ministry of Communications and Information and reports to the Prime Minister's Office.
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/Explore/who-we-are/our-identity/about-singcert). These are broadcasted through the SingCERT subscribers' mailing list, as well as via CSA's Facebook and Twitter platforms. SingCERT also maintains an incident reporting channel, supported by Cyber Aid (https://www.csa.gov.sg/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 2023, SingCERT received reports of 5,048 incidents, an 8.58% increase from the 4,649 incidents reported to SingCERT in 2022. This resulted in an average of 13.8 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	1,128	1,373	1,160	1,387	5,048

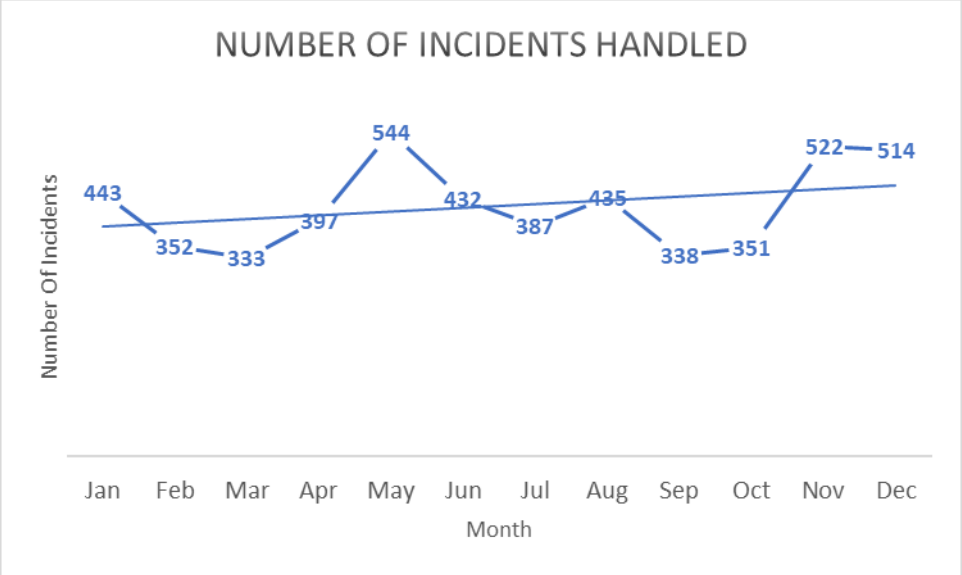


Figure 1: Number of Incidents Reported to SingCERT (2023)

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 2023, phishing was, once again, the most prevalent cyber threat that was reported to SingCERT in Singapore, comprising over 60% of the incidents handled over the course of the year. This has been a trend that SingCERT has observed over the past few years. The phishing threats have also evolved to be more convincing in both the contents and the use of closely similar domain names to legitimate organisations operating in the country.

Cyber Incident Category	# Handled in 2022	# Handled in 2023
Phishing	3060	3186
Intrusion Attempt/Attack	576	703
Malware	641	734
Others	287	289
Vulnerability	85	136

Table 1: Breakup of Cyber Incidents handled (2022 vs 2023)

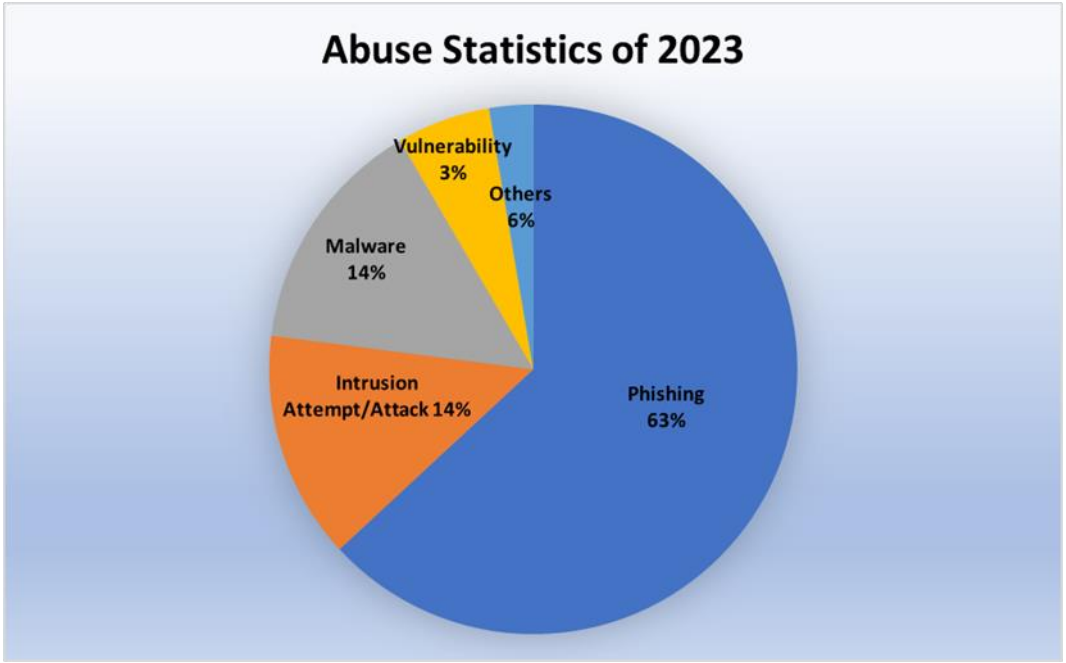


Figure 2: Abuse Statistics (2023)

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 2023, SingCERT published a total of 191 alerts and advisories, in addition to 52 Security Bulletins, on SingCERT's website. This represented a 95% increase from the 81 alerts and advisories published in 2021. The chart below shows the month-by-month comparison between 2022 and 2023.

	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Total
2022	2	7	11	4	6	5	6	13	12	13	9	10	98
2023	13	16	18	19	16	16	17	11	14	22	12	17	191

Table 2: Month-by-month comparison of Alerts and Advisories Published (2022 to 2023)

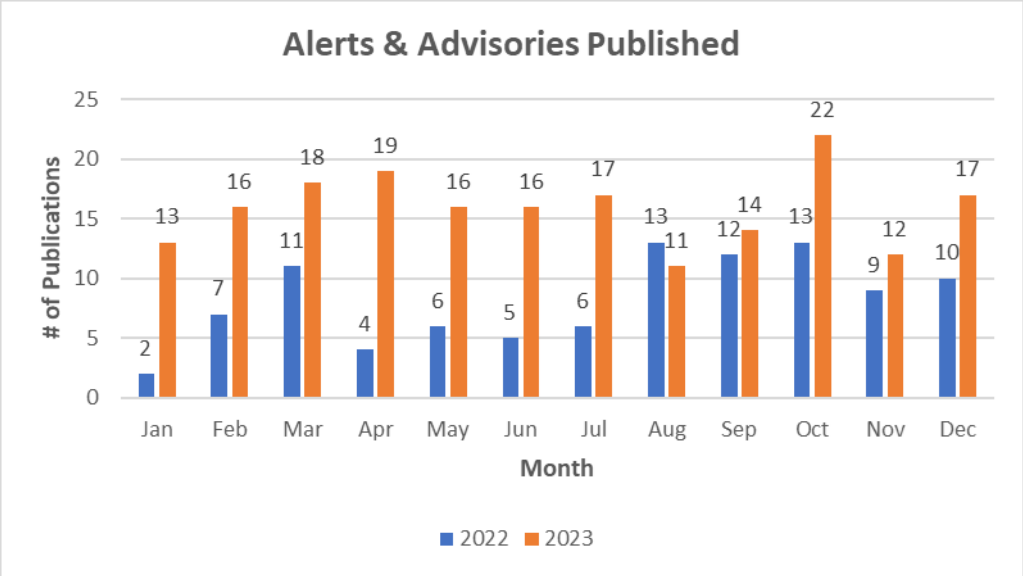


Figure 3: Comparing the Number of Alerts and Advisories Published (2022 to 2023)

Of the 191 alerts and advisories, 156 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 2023 are tabulated below:

Date	Title
4 Jan	Critical Vulnerability in Synology Virtual Private Network (VPN) Plus Servers
5 Jan	Critical Vulnerability in Multiple ManageEngine Products
5 Jan	Critical Vulnerability in FortiADC
6 Jan	Protecting Yourself and Your Organisation from Data Breaches
10 Jan	Critical Vulnerability in Cacti Product
11 Jan	January 2023 Monthly Patch
11 Jan	Protecting Your Software from Malicious Third-party Dependencies
12 Jan	Multiple Vulnerabilities Affecting Cisco Virtual Private Network (VPN) Routers
17 Jan	Critical Vulnerability Affecting InHand Networks InRouters
18 Jan	Critical Vulnerabilities Affecting Git
19 Jan	Vulnerability Affecting Sudoedit
25 Jan	Multiple Critical Vulnerabilities in WordPress Plugin LearnPress
25 Jan	Multiple Vulnerabilities Affecting VMware vRealize Log Analysis Tool
2 Feb	Critical Vulnerability in Realtek Jungle Software Development Kit (SDK)
2 Feb	Critical Vulnerability in Dompdf PHP Library
3 Feb	Multiple Vulnerabilities Affecting F5 Networking Products
4 Feb	Massive Ransomware Campaign Targeting Unpatched VMware ESXi Servers
6 Feb	Critical Vulnerability in Atlassian's Jira Service Management Server
14 Feb	Active Exploitation of Zero-Day Vulnerability in Apple Products
15 Feb	February 2023 Monthly Patch
16 Feb	Multiple Vulnerabilities Affecting Citrix Systems Products
18 Feb	High-Severity Vulnerability in Joomla Content Management System
19 Feb	Multiple Critical Vulnerabilities in FortiNAC and FortiWeb
19 Feb	Critical Vulnerability in Cisco's ClamAV Products
21 Feb	New Ongoing Magecart Campaign
23 Feb	Joint Advisory on The Dangers of Downloading Applications from Third Party or Dubious Sites
24 Feb	Technical Advisory on Secure API Development
26 Feb	Joint Advisory on Tech Support Scams
28 Feb	Active Exploitation of Critical Vulnerabilities in WordPress Plugin Houzez
2 Mar	Critical Vulnerabilities in ArubaOS
2 Mar	Critical Vulnerability in Cisco IP Phones

8 Mar	Critical Vulnerabilities in Android Operating System
9 Mar	Critical Vulnerability in Fortinet's FortiOS and FortiProxy Products
9 Mar	Critical Vulnerability in IBM Instana's Products
10 Mar	Multiple Vulnerabilities in Jenkins Server and Update Centre
13 Mar	High-Severity Vulnerability in Cisco IOS XR Software
15 Mar	March 2023 Monthly Patch
15 Mar	Critical Vulnerabilities in SAP Products
15 Mar	Critical Vulnerabilities in Adobe ColdFusion
16 Mar	Critical Vulnerability in Microsoft Outlook for Windows
23 Mar	Importance of Using Secure Multi-Factor Authentication Methods
24 Mar	Critical Vulnerability in WooCommerce Payments
25 Mar	Ongoing Ransomware Campaign Actively Exploiting a Vulnerability in Fortra's GoAnywhere
30 Mar	Active Exploitation of Critical Vulnerability in IBM Aspera Faspex
30 Mar	High-Severity Vulnerability in QNAP NAS
31 Mar	Malware Discovered in 3CX DesktopApp
31 Mar	Cybersecurity Advisory for Online Content Creators
1 Apr	Active Exploitation of High-Severity Vulnerability in Elementor Pro
3 Apr	New Indicators of Compromise (IOCs) Discovered for Windows and Linux-based Backdoor Malware KEYPLUG
8 Apr	Active Exploitation of Zero-Day Vulnerabilities in Apple Products
10 Apr	Critical Vulnerability in vm2 Library
12 Apr	April 2023 Monthly Patch
12 Apr	Critical Vulnerabilities in Adobe Acrobat and Reader
14 Apr	Critical Vulnerability in Hikvision Products
15 Apr	Multiple Vulnerabilities in Microsoft Products
15 Apr	Active Exploitation of Zero-Day Vulnerability in Google Chrome
17 Apr	Joint Advisory on Protecting Mobile Devices from Malicious Wireless and Wired Connections
20 Apr	Critical Vulnerabilities in vm2 Library
20 Apr	Active Exploitation of Zero-Day Vulnerability in Google Chrome
21 Apr	Critical Vulnerability in VMware Aria Operations for Logs
21 Apr	Active Exploitation of SNMP Vulnerabilities in Cisco IOS and IOS XE Software
27 Apr	High-Severity Vulnerability in Service Location Protocol

27 Apr	Multiple Vulnerabilities in VMware Workstation and Fusion Products
27 Apr	Critical Vulnerability in PrestaShop SQL Manager
28 Apr	Ongoing Ransomware Campaign Targeting VMware ESXi Servers
28 Apr	Joint Technical Advisory on LockBit 3.0
10 May	May 2023 Monthly Patch
12 May	Critical Vulnerabilities in Aruba Access Points
12 May	Use-After-Free Vulnerability in Linux Kernel
15 May	Critical Vulnerability in WordPress Elementor Plugin
15 May	Active Exploitation of Critical Vulnerability in PaperCut MF (Multifunction) and NG (Next Generation)
18 May	Critical Vulnerabilities in Cisco Small Business Series Switches
19 May	Critical Vulnerability in vm2 Sandbox Library
19 May	Active Exploitation of Zero-Day Vulnerabilities in Apple WebKit
22 May	Joint Advisory on Protecting Yourself from Malicious QR Codes
23 May	Critical Vulnerability in Zyxel Firewalls
25 May	Critical Vulnerability in GitLab
26 May	New Ongoing Malware Campaign Targeting Android Devices
26 May	Ongoing Ransomware Campaign exploiting Malicious Windows Kernel Drivers
26 May	Critical Vulnerabilities in Zyxel Firewall and VPN Products
26 May	Critical Vulnerabilities in D-Link Products
31 May	Critical Vulnerability in Barracuda Networks' Email Security Gateway
2 Jun	Active Exploitation of Zero-Day Vulnerability in MOVEit Transfer
7 Jun	Active Exploitation of Zero-Day Vulnerability in Google Chrome
8 Jun	Critical Vulnerabilities in Android Operating System
8 Jun	Ongoing Campaign Abusing Small Office and Home Office Devices
12 Jun	Critical Vulnerability in MOVEit Transfer Web Application
13 Jun	Critical Vulnerability in Fortinet's FortiOS and FortiProxy Products
14 Jun	June 2023 Monthly Patch
15 Jun	Joint Advisory on the Importance of Reviewing Permissions for Applications in Android Devices
16 Jun	Critical Vulnerability in MOVEit Transfer
21 Jun	Critical Vulnerabilities in ASUS's Router Products
21 Jun	Critical Vulnerability in Zyxel Network Attached Storage (NAS) Products
22 Jun	Active Exploitation of Zero-day Vulnerabilities in Apple Products

23 Jun	Critical Vulnerabilities in WordPress Plugins
23 Jun	High-Severity Vulnerability in Cisco Secure Client Software
26 Jun	Critical Vulnerability in Fortinet's FortiNAC Products
26 Jun	High-Severity Vulnerabilities in VMware vCenter Server and Cloud Foundation Products
6 Jul	Active Exploitation of Zero-day Vulnerability in Ultimate Member Plugin
7 Jul	High-Severity Vulnerability in Cisco Nexus 9000 Series Fabric Switches
11 Jul	Active Exploitation of Zero-day Vulnerability in Apple Products
12 Jul	Critical Vulnerability in Citrix ShareFile Storage Zones Controller
12 Jul	Critical Vulnerability in FortiOS & FortiProxy
12 Jul	Critical Vulnerabilities in Android Operating System
12 Jul	July 2023 Monthly Patch
13 Jul	Critical Vulnerability in Ghostscript
14 Jul	Critical Vulnerabilities in SonicWall Products
19 Jul	Critical Vulnerabilities in Citrix Netscaler ADC and Netscaler Gateway
24 Jul	Critical Vulnerabilities in Adobe ColdFusion
24 Jul	Critical Vulnerabilities in AMI MegaRAC Baseboard Management Controller (BMC) Firmware
24 Jul	Active Exploitation of Unpatched Vulnerabilities in Fortinet Products
25 Jul	Active Exploitation of Zero-day Vulnerability in Apple Products
25 Jul	Active Exploitation of Zero-Day Vulnerability in Ivanti Endpoint Manager Mobile (EPMM)
28 Jul	High-Severity Vulnerability in Ubuntu OverlayFS Module
31 Jul	Active Exploitation of High-Severity Vulnerability in Ivanti Endpoint Manager Mobile (EPMM)
9 Aug	Aug 2023 Monthly Patch
14 Aug	High-Severity Vulnerability in Python URL Parsing Function
14 Aug	Active Exploitation of Zero-Day Vulnerability Affecting Microsoft Office & Windows
15 Aug	Joint Advisory on Malware Scams Affecting Android Users
16 Aug	Critical Vulnerabilities in Ivanti Avalanche
21 Aug	How Organisations and Their Employees Can Stay Ahead of Cybersecurity Threats
22 Aug	Critical Zero-Day Vulnerability in Ivanti Sentry Products
22 Aug	High-Severity Vulnerability in WinRAR
22 Aug	Advisory on Cybersecurity during Elections for Voters
31 Aug	Critical Vulnerability Affecting VMware Aria Operations for Networks
31 Aug	Joint Advisory on Social Media Impersonation Scams Involving Telegram

6 Sep	Critical Vulnerabilities in ASUS' Router Products
8 Sep	Active Exploitation of Zero-Day Vulnerabilities in Apple Products
8 Sep	Critical Vulnerability in Cisco BroadWorks
13 Sep	Critical Zero-day Vulnerability in Mozilla Firefox & Thunderbird
13 Sep	Critical Zero-day Vulnerability Affecting Adobe Acrobat and Reader
13 Sep	Active Exploitation of Zero-day Vulnerability in Google Chrome
13 Sep	Sept 2023 Monthly Patch
19 Sep	Critical Vulnerability Affecting Juniper Devices
20 Sep	Critical Vulnerability in GitLab's Products
22 Sep	Active Exploitation of Zero-Day Vulnerabilities in Apple Products
27 Sep	Critical Zero-day Vulnerability Affecting libwebp Library
29 Sep	Active Exploitation of Zero-Day Vulnerability in Google Chrome
29 Sep	Critical Vulnerability Affecting Cisco Catalyst SD-WAN Manager
30 Sep	Critical Vulnerabilities Affecting Progress WS_FTP Server software
2 Oct	Critical Zero-Day Vulnerability Affecting Exim Mail Transfer Agent
2 Oct	Advisory On Securing Your Routers
4 Oct	Multiple Critical Vulnerabilities in Python TorchServe Library
5 Oct	Active Exploitation of Critical Vulnerability in Confluence Data Center and Server
5 Oct	Active Exploitation of Zero-Day Vulnerability in Apple Products
6 Oct	Critical Vulnerability Affecting Cisco Emergency Responder
6 Oct	Active Exploitation of High-Severity Vulnerability in Android Devices
9 Oct	Ongoing Attacks Against Microsoft Azure Cloud Virtual Machines
11 Oct	Oct 2023 Monthly Patch
11 Oct	Double-Free Vulnerability in CC-Link IE TSN Industrial Managed Switch
13 Oct	Critical Vulnerabilities in Citrix NetScaler ADC and NetScaler Gateway
13 Oct	Active Exploitation of High Severity Vulnerability in Adobe Acrobat Products
13 Oct	Defending Against Lumma Information Stealer Malware
16 Oct	Active Exploitation of Zero-Day HTTP/2 Vulnerability
17 Oct	Active Exploitation of Zero-Day Vulnerabilities in Cisco IOS XE Software
17 Oct	Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software
21 Oct	Critical Vulnerabilities in SolarWinds ARM Product
22 Oct	Enhancing Your Cybersecurity Posture Amidst Developments in Israel-Hamas Conflict

25 Oct	How Organisations and Their Employees can Ensure Data and Device Security
25 Oct	SQL Injection Attacks Affecting Singapore Websites
26 Oct	Critical Vulnerability in VMware vCenter Server
26 Oct	Common Cybersecurity Misconfigurations in Networks
1 Nov	Critical Vulnerability in Atlassian Confluence Data Center and Server
2 Nov	Critical Vulnerability in F5's BIG-IP Traffic Management User Interface (TMUI)
7 Nov	Critical Vulnerabilities in Veeam ONE
7 Nov	Critical Vulnerabilities in QNAP QTS Operating System and Applications
8 Nov	Active Exploitation of High Severity Vulnerability in GNU C Library
10 Nov	Joint Advisory on Protecting Yourself against Malware Scams during the Festive Season
15 Nov	Nov 2023 Monthly Patch
15 Nov	Critical Vulnerability in VMWare Cloud Director Appliance
17 Nov	Critical Vulnerability in Fortinet's FortiSIEM Product
23 Nov	Active Exploitation of Critical Vulnerability in Apache ActiveMQ
27 Nov	Critical Vulnerabilities in ownCloud File Sharing Application
29 Nov	Active Exploitation of Zero-Day Vulnerability in Google Chrome and Chromium-based Browsers
1 Dec	Active Exploitation of Zero-Day Vulnerabilities in Apple WebKit
5 Dec	Ongoing Fake CVE Phishing Campaign Targeting WordPress
6 Dec	Critical Vulnerabilities in Android Devices
6 Dec	Ongoing Attacks Against Exposed Unitronics Devices
7 Dec	Critical Vulnerability in Open Network Demarcation Service (OpenNDS)
8 Dec	Multiple Critical Vulnerabilities in Atlassian Products
13 Dec	Dec 2023 Monthly Patch
13 Dec	Active Exploitation of Zero-Day Vulnerabilities in Apple Products
13 Dec	Active Exploitation of Critical Vulnerability in Apache Struts 2
14 Dec	Multiple High Severity Vulnerabilities in Qualcomm and MediaTek Products
15 Dec	Active Exploitation of Critical Vulnerability in JetBrains TeamCity On-Premises
16 Dec	Multiple High Severity Vulnerabilities in Samsung Products
18 Dec	Critical Vulnerability in WordPress Backup Migration Plugin
18 Dec	Active Exploitation of Zero-Day Vulnerability in QNAP VioStor Network Video Recorder (NVR)
21 Dec	Active Exploitation of Zero-Day Vulnerability in Google Chrome
28 Dec	Active Exploitation of Critical Vulnerability in Barracuda Networks' Email Security Gateway

3.4.2 One-stop Ransomware Portal

CSA, in collaboration with the Singapore Police Force (SPF), launched a one-stop ransomware portal on 6 Sep 2023 to provide aid to ransomware victims seeking recovery support while providing organisations with access to ransomware-related resources. The portal allows victims to easily report ransomware cases, and it also offers recovery support in the form of decryption tools, incident response checklists and Frequently Asked Questions (FAQs). In addition, the portal includes ransomware advisories, trends and prevention measures that organisations can adopt to avoid falling victim to ransomware attacks.

The ransomware portal can be accessed via https://go.gov.sg/rwportal.

3.4.3 Exercise Cyber Star (XCS23)

CSA held its fifth edition of XCS on 22 Sep 2023. XCS is a nationwide cyber crisis management exercise to improve Singapore's crisis response capabilities and readiness to respond promptly and effectively to a cyber-attack. More than 450 participants from CSA and the 11 Critical Information Infrastructure (CII) sector leads and owners took part in XCS23.

To ensure that all sectors remain responsive and coordinated in the event of a national cyber crisis, the sectors were exercised under XCS23 on a wider number of complex scenarios which included distributed denial-of-service attacks, ransomware attacks, widespread phishing campaigns as well as malicious exploits targeting Internet-based resources, corporate networks, and industrial control systems (ICS). Sectors were tested on their responses to attacks resulting in water supply disruption, large-scale power outages, data leaks and communications network failure.

A new technical component, "Grid NetWars", was incorporated this year, and required participants to use their technical skills to tackle a series of hands-on cybersecurity challenges involving ICS technologies commonly found in sectors such as Energy and Water.

More information about the XCS23 is available via https://www.csa.gov.sg/News-Events/Press-Releases/2023/nationwide-cyber-crisis-management-exercise-to-test-11-critical-sector-s-response-to-complex-cyber-attack-scenarios.

3.4.4 Cloud Security Companion Guides for Organisations

Two Cloud Security Companion Guides to support Cyber Essentials and Cyber Trust were launched by CSA and the Cloud Security Alliance.

The companion guide for Cyber Essentials, targeted at SMEs, uses a shared responsibility model to help organisations understand what they and their providers each need to take care of the cloud environment. The companion guide for Cyber Trust, targeted at larger or more digitalised organisations, maps each of the cybersecurity preparedness domain in the Cyber Trust mark, such as cyber governance and oversight and cyber education, to the framework published by the Cloud Security Alliance. This mapping provides a useful and convenient reference for organisations, making it easier for them to implement the measures necessary to attain the Cyber Trust mark.

More information about the companion guides, including downloadable copies, is available via https://www.csa.gov.sg/News-Events/Press-Releases/2023/launch-of-cloud-security-companion-guides-for-organisations.

3.4.5 Singapore Cyber Landscape 2022

The 7th edition of the Singapore Cyber Landscape publication reviews Singapore's cybersecurity situation in 2022 against the backdrop of global trends and events, such as the ongoing Russia-Ukraine conflict, and highlights the nation's efforts in creating a safe and trustworthy cyberspace, such as initiatives to combat new and emerging cyber threats.

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

More information about the publication, including a downloadable copy, is available via https://www.csa.gov.sg/Tips-Resource/publications/2023/singapore-cyber-landscape-2022.

Figure 4: Singapore Cyber Landscape 2022

4. Events organized & hosted

4.1 Drills & Exercises

4.1.1 ASEAN CERT Incident Drill 2023

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 18 and 19 October 2023, SingCERT successfully conducted the 18th iteration of ACID. Eighteen CERT teams from ASEAN Member States (AMS) and ASEAN Dialogue Partners participated in the drill. The theme "Responding to Multi-Pronged Attacks Arising from Hacktivism" was selected against the global backdrop of increasing cyber-attacks motivated by hacktivism, where hacktivist groups typically perform cyber-attacks on organisations to further their ideological beliefs. Participants were given a series of email injects that simulated similar tactics employed by hacktivists, such as the deployment of wiperware to disrupt the operations of target organisations.

This year's ACID was also expanded to include a Tabletop Exercise (TTX) component developed and moderated by SingCERT. In the TTX, realistic 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, as well as identify areas for further improvement and enhance their operations planning capabilities.

After the conclusion of the drill, participating CERTs feedbacked that the cyber drill and TTX were well organised and enhanced participants' incident response capabilities, as well as broadening their horizons by exposing their teams to new drill scenarios and incident response techniques, which allowed them to practice responding to a variety of realistic scenarios.

More information about ACID can be found via https://www.csa.gov.sg/News-Events/News-Articles/2023/18th-iteration-of-asean-cert-incident-response-drill-tests-cert-s-preparedness-against-multi-pronged-attacks-arising-from-hacktivism.

4.2 Conferences and seminars

4.2.1 Singapore International Cyber Week 2023

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 8th SICW was held from 16 to 19 October 2023, with the theme "Building Trust and Security in the Emerging Digital Order". SICW 2023 successfully concluded with more than 12,000 participants from the region and beyond, as well as over 270 speakers who covered a myriad of topics ranging from reshaping cybersecurity in the era of

generative artificial intelligence, public-private sectors roles and partnership in the cyberspace and combating advanced cybersecurity threats.

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 Training

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

Date	Title	Presented by
28 Mar	DNS Security and Threats for Incident Responders	ICANN
9 May	5G Vulnerability Analysis	KrCERT/CC
11 Jul	Cyberspace Search Engine – Overview and Applications	TWNCERT

5.2 Drills & Exercises

5.2.1 Asia Pacific Computer Response Team (APCERT) Cyber Security Drill 2023

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 16 August 2023 with the theme "Digital Supply Chain Redemption". The drill evaluates the response capabilities of member teams in responding to real incidents and issues that exist on the internet. As a member of the APCERT Drill Working Group, SingCERT was involved in the conducting of the drill as a part of the Exercise Controller Team.

5.3 Conferences, Seminars & Presentations

5.3.1 Forum of Incident Response and Security Teams (FIRST)

The Forum of Incident Response and Security Teams (FIRST) is an organisation and recognised global leader in incident response. FIRST brings together a wide variety of security and incident response teams including product security teams from the government, commercial, and academic sectors. The Forum is also beneficial to both newly established

and matured National CSIRTs as it serves as a platform for networking and collaboration. More details about the organisation can be found at https://www.first.org.
As a member of FIRST, SingCERT attended the FIRST Conference at Montreal, Canada from 4 June – 9 June 2023.

5.3.2 APCERT Annual General Meeting (AGM) and Conference 2023

The APCERT AGM and Conference is an annual event where CERTs from the Asia Pacific region gather to exchange information on the latest cybersecurity issues and incident response methodologies. SingCERT attended the APCERT Annual General Meeting (AGM) held on 8 November 2023 and the conference held on 9 November 2023. Both events continued to be held virtually.

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 work plan in the year 2024:

S/n	Description	Category
1	Singapore Cyber Landscape 2023	Publications
2	9th Singapore International Cyber Week (SICW)	Events Organising & Hosting
3	19th 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). ICTA is the Government Agency responsible for the development of IT Infrastructure and Policy in Sri Lanka. Thereafter, Sri Lanka CERT was made independent of ICTA in 2018 and was assigned to the Ministry of Digital Infrastructure and Information Technology. In the year 2019, Sri Lanka CERT was assigned to the Ministry of Defence and later reassigned to the Presidential Secretariat in October 2020. Currently, Sri Lanka CERT serves the Ministry of Technology under the purview of his excellency the President of Sri Lanka from 2021 onwards.

At the end of December 2023, the headcount comprised thirty (30) staff members. This included the Chief Executive Officer(Actg.), Head of Human Resources and Administration, two Chief Information Security Officers, one Information Security Manager, two Lead Information Security Engineers, three Senior Information Security Engineers, one Information Security Engineer, eight Associate Information Security Engineers, one Program Manager, one Project Manager, one Finance Manager, one Legal Manager, three Associate SOC Engineers, one Finance Assistant, three Call Centre officers. Twelve undergraduate interns were assisting the operations.

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

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

1.3 Constituency

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

Sri Lanka CERT handles information security incidents. This service involves responding to a request or notification by a

constituent on an unusual event that has been detected, which may affect the performance, availability or stability of the services or cyber systems belonging to that constituent.

3.2 Awareness Services

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

Alerts & Advisory

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

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

Seminars & Conferences

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

Workshops

This service is aimed at increasing the constituents' awareness of information security. However, unlike seminars, these are more technically oriented and targeted at IT professionals, who perform daily tasks related to information security. Workshops will be arranged regularly, or on request, by Sri Lanka CERT for its constituents addressing general topics. If desired, constituents may submit specific information security-related topics, so that the workshops are tailored to their needs.

3.3 Consultancy Services

This service is aimed at providing constituents with means of determining the adequacy of their information security systems and taking necessary steps to strengthen their 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 primary authority on information security in Sri Lanka, Sri Lanka CERT is responsible for developing, introducing, and enforcing information security standards to its constituents.

3.4 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 helps an organization improve its security posture by identifying vulnerabilities before they become security incidents. Our experts use a proven combination of industry tools, best practices, and in-house techniques to probe the network/ devices for vulnerabilities and hence identify potential areas of risk.

Penetration Testing

Sri Lanka CERT provides an internal and/or external penetration testing service that involves simulating real-world attacks to provide a current view of vulnerabilities and threats to the client's network infrastructure.

These assessments begin with a discovery process to develop a baseline profile of accessible services, ports, and systems as targets for further internal or external penetration testing.

The process involves an in-depth analysis including manual probing to:

- Test identified components to gain access to the networks
- Network devices such as firewalls, routers, and switches
- Network services such as web, DNS, email, FTP, etc.
- Determine possible impact or extent of access by attempting to exploit vulnerabilities

A detailed report is provided with findings and recommendations

System Hardening

The purpose of system hardening is to eliminate as many security risks as possible. This is typically done by assessing the systems against the security best practices. There may be continuous changes to the information systems of the organization. As a result, it may introduce new vulnerabilities due to misconfiguration, and/or unnecessary software/services etc. A detailed report will be provided with findings and recommendations.

On-site and off-site consultation

This service mainly focuses on incident response. The main purpose of this service is to ensure that the client is not unduly burdened with day-to-day information security-related incidents.

- Over-the-phone consultancy
- On-site incident handling

- Timely response and mitigation to incidents occurring at customer premises
- Review of security policies and processes

3.5 Digital Forensics Investigations

Sri Lanka CERT digital forensics team has been offering the service since the year 2010 and has well-experienced digital forensics investigators. Sri Lanka CERT is equipped with globally acceptable tools and adheres to globally recognized digital forensics procedures.

Furthermore, Sri Lanka CERT conducts digital forensics training programs and technical workshops for both local and international audiences. Sri Lanka CERT has successfully conducted tailor-made digital forensics training programs for public and private sector organizations based on client requirements.

3.6 Research & Policy Development

Sri Lanka CERT Research and Policy Development division was established with the intention of:

- Developing strategies and formulating policies related to information security and cyber security for the nation
- Conducting national-level surveys on the various domains related to information and cyber security
- Coordinating special national projects related to information security and cyber security.

4. Operational Performance (Routine Responsibilities & Projects)

4.1 Incident Handling Summary

Sri Lanka CERT being the national contact point for all cybersecurity-related matters receives numerous incident reports/complaints relating to the country's national cyber-space from both domestic and international partners.

The types of incidents received by Sri Lanka CERT include incidents related to social networks, email compromise, phishing, website compromise, scams, malicious software issues and ransomware, privacy violations, financial frauds, compromised unique IPs extracted from the information collected by automated systems operated by international organizations. The largest incidents reported involve social media, with an average of over 1650 cases per month. Comparing 2022 to 2023, there was a notable increase in social media-related incidents. Additionally, there has been a noticeable rise in reported email-related incidents compared to the previous year.

Table 1 depicts the distribution of various types of incidents reported to Sri Lanka CERT in the year 2023. All the incidents reported to Sri Lanka CERT have been resolved satisfactorily.

Incident Type	Number of Incidents in 2023
File Recovery	0
DDOS	44
Ransomware	31
Abuse/Hate/Privacy violations	186
Malicious Software issues	2
Phone Hacking	9
Scams	98
Phishing	61
Website Compromise	37
Financial Fraud	58
Intellectual property violation	1
Server Compromised	11
Cloud Related	1
Email Incidents	7998
Social media	20033
Total Number of Incidents	28570

Table 1: Number of reported incidents in the year 2023

4.2 Consultancy Services

Sri Lanka CERT continues to provide consultancy services in response to requests made by both the public and private sectors.

- Network Security / Architecture Review Assignments - 04
- Email Incidents - 8241
- Malware Analysis - 2

4.3 Information Security Managed Services

1. Sri Lanka CERT was able to deliver the following security-managed services;

- External penetration testing
- Internal penetration testing
- Device configuration reviews

- Network architecture reviews
- Application security assessments
- Server OS configuration reviews

Two managed services were received in the year 2023 and one was already completed. The other activity is in progress.

4.4 Application Security Audits

Sri Lanka CERT performed Web and Mobile Application Security Audits was performed throughout the year. Continuous monitoring of web applications was conducted in order to identify potential cyber-attacks. The statistics of the activities are as follows.

- Government Web assessments – 109
- Private Web Assessments - 9
- Mobile App Assessments – 5
- Web assessments received from ICTA – 100
- Investigations - 6
- Reassessments - 177

4.5 Digital Forensics

Sri Lanka CERT has completed seven (7) digital forensic investigations during the year 2023. 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.

Sri Lanka CERT has received six (6) digital forensic cases in 2023. Provided one (1) Consultation digital forensic service. There are 5 digital forensic cases pending at the end of the year 2023.

4.6 Training / Education Services

In order to fulfil its mandate to create awareness and build Information Security skills within the constituency; Sri Lanka CERT continued to organize training programs and education sessions targeting various audiences including CIOs, Engineers, System Administrators, Banking and Telecom Sector Staff, Students, and the General Public.

4.6.1 Awareness Program and Training Sessions

Sri Lanka CERT conducted the following training and awareness programs:

- General Cyber Security Awareness sessions for government officials/organizations:
- Telecommunications Regulatory Commission of Sri Lanka
- Institute of National Security Studies (INSS)
- National Institute of Education

- Ministry of Health
- Finance Commission
- Sri Lanka Administrative Service (SLAS) Officers - SLIDA
- Sri Lanka Accountancy Service Officers - SLIDA
- ICT Agency of Sri Lanka (for government officials, private sector, and startups)
- Ministry of Education (Teacher training programs)

- General Cyber Security Awareness sessions for Industry bodies and private companies
  - The Institute of Charted Professional Managers of Sri Lanka (CPM Sri Lanka)
  - Sri Lanka Sumithrayo
  - Pership House (One)
  - CCG Mt.Lavinia
  - Sithara Limited
- Sessions conducted for law enforcement and judiciary
  - Session on "Digital Evidence Handling" for Katana Police Academy
  - Maradana Police In-service Training Center - Leveraging Cutting-edge Technology for Crime Prevention and Resolution | Workshop
- Sessions conducted for university students

i. ISACA Student Group - NSBM Green University
ii. University of Colombo School of Computing – Support with MITRE
iii. SLIIT

- Training Serious for CNII organization's ISO/AISO's

i. 8 Workshops conducted with the support of SLIDA
ii. 2 Workshops conducted with the support of MITRE

4.6.2 Awareness through Electronic/Print Media

Following are the details of awareness activities carried out by Sri Lanka CERT through electronic and printed media.

- Number of newspaper articles 09
- Number of TV Programs/YouTube 10
- Number of radio Programs 07
- Number of Voice cuts 05
- Number of Social Media posts 110
- Number of newsletters 6x3 =18 (Sets)

Further to the above activities, a short TV program about Sri Lanka CERT was completed in all three languages.

4.6.3 Security Alerts

- 10,000+ compromised IPs were informed to ISPs during the year 2023.
- 54 critical security alerts were published and sent to subscribers.

4.7 Publications

Website

The Sri Lanka CERT website publishes security-related awareness bulletins for the public via News Alerts and a Knowledge Base. Glossaries, case studies and FAQs are among some of the other published items.

E-mails

Disseminating security-related information via e-mail alerts to Sri Lanka CERT website subscribers.

Newsletters

Sri Lanka CERT publishes and circulates the Cyber Guardian e-newsletter to a large number of students, through the 'SchoolNet' - the network connecting secondary schools in Sri Lanka.

Newspapers/media

Sri Lanka CERT continues to educate the general public through the electronic and print media about emerging cyber security threats and vulnerabilities with recommendations on how to safeguard against these attacks.

4.8 Infrastructure Development & Staff Capacity Building

4.8.1 Staff Capacity Building – International Initiatives

Sri Lanka CERT staff members had the opportunity to participate in and represent Sri Lanka for the following training/ seminars/conferences as well.

i. Cyber Bootcamp Program - Australia
ii. 8th Annual Meeting of the Cyber Security Alliance for Mutual Progress (CAMP) – South Korea
iii. APNIC56 Conference - Japan
iv. Global Workshop on Digital Public Infrastructure (DPI) - USA
v. UN Internet Governance Forum (IGF) - Japan
vi. ASPIC Security training course and 2023 RISE – South Korea
vii. JP-US-EU Industrial control system Cyber security week for the Indo-Pacific Region - Japan
viii. Global Action Cybercrime Convention, Octopus Conference 2023 & Closing of the GLACY+ project - Romania
ix. The International Visitor Leadership Programme - Advancing an Open, Reliable, and Secure Digital Economy – USA
x. Instructor development program on electronic evidence first responder training and national level electronic evidence first responder training program – Philippines

4.9 National Projects

Project Name	Project Status (Simple Description)
National Cyber Security Operations Center for real-time monitoring of cyber security incidents	Delivery of threat intelligence report to ISPs weekly Real-time monitoring of websites (availability of websites) - 500+ Website Security monitoring of selected websites through Open Source SIEM tools
Implementation of the National Certification Authority of Sri Lanka to issue certificates for Certificate Service Providers	Certificate Revocation List (CRL) was generated. The CSR was signed with LankaPay.
Development of a Web Portal to increase citizens' awareness of cyber security (www.onlinesafety.lk)	The tri-lingual web portal is in operation.
Development of National Vocational Qualification (NVQ) Standard for Information and Cyber Security	NVQ Level 5 and 6 (National Diploma) Curriculum developments completed.
Cyber Security Capacity Building Program for Government Officers	A total of 56 ISO and AISO members from CNII organizations were trained through a series of workshops and training sessions with the support of SLIDA. A total of 403 Sri Lanka ICT Service Officials were trained on basic cybersecurity. A total of 1,682 government officials were trained and aware on basic cybersecurity and cyber hygiene with the support of industry experts.
Improve the Cyber Security Readiness of 10 Government Organizations	Project Initiated with 7 organizations and in progress for 2 organizations
Development of Online Modules on e-Learning for Government Officers	Project Completed.
Cyber security skills framework for government officials	The document has been drafted and is scheduled for publication in 2024 as part of the new strategy.

Table 2: National Projects

4.10 Information and Cyber Security Policy for Government Organizations

The implementation of the Information and Cyber Security Policy for government organizations, which received Cabinet approval in August 2022, has commenced. Sri Lanka CERT has prioritized 43 organizations that operate Critical Information Infrastructure within the country for the implementation process. Below are the details of the assessments conducted.

- Number of ITGC Initiated/completed – 6/1
- Number of Risk assessments Initiated/completed – 5/0

4.11 Other Engagements

- CBSL Compliance Review 1
- BCP Drill review 1
- IT policy Development 1
- Feasibility study & Risk Assessment for Cloud Migration 1
- NIST Compliance Review 1
- Cyber Security Training 1
- ICAO Security Assessment 1

5. Achievements

5.1 National Cyber Security Strategy of Sri Lanka (2024 – 2027)

With the assistance of the World Bank, Sri Lanka CERT has undertaken the essential measures to develop the forthcoming version of the National Cyber Security Strategy, slated for implementation from 2024 to 2027. The initial draft of the strategy has been finalized and is currently undergoing presentation for stakeholder and public consultations.

5.2 Memberships

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

- (ISC)2 Colombo Sri Lanka Chapter is the local representative organization of the International Information Systems Security Certification Consortium.
- Membership for Threat Intelligence from ShadowServer.

- Membership of FIRST
- Membership of APCERT
- Membership of CAMP, Korea
- Membership of TF-CSIRT

6. International Collaboration

6.1 CAMP

- Actively Participated in CAMP Operations Committee(OC) meetings
- Leading processes and procedures relevant to the membership component in CAMP OC
- Participated in many online and offline discussions on CAMP AGM 2023
- Participated in 8th Annual Meeting of the Cybersecurity Alliance for Mutual Progress (CAMP) – Seoul, South Kora July 2023
- Participated in CAMP Operations Committee 31st Meeting 2023 (online)
- Participated in cyber security webinars in 31st OC Meeting 2023 (online)
- Cooperation in preparing the content for the CAMP Newsletter November 2023

6.2 APCERT

- Participated in APCERT steering committee meetings
- Participated in a Call with Global Cyber Alliance (GCA)
- APCERT cyber drill 2023 working group discussions and its activities
- Participated in APCERT cyber drill 2023
- Participated for APCERT Conference 2023
- Represented Sri Lanka CERT in the APCERT AGM Panel discussion
- Participated in APCERT Policy Procedure and Governance Working Group (PPGWG)

7. Future Plans

7.1 Future Projects to Be Implemented

- Implementation of Information and Cyber Security Policy in the government organisations
- Obtaining the Cabinet Approval for the National Cyber Security Strategy of Sri Lanka (2024 - 2027)
- Obtaining the Cabinet Approval for the Cyber Security Bill

- Establishment of Cyber Security Regulatory Authority

8. Conclusion

In 2023, Sri Lanka CERT demonstrated notable success, effectively accomplishing the majority of its tasks without encountering significant issues. The successful implementation of the Information and Cyber Security Policy across government organizations signifies a crucial milestone. Especially, Sri Lanka CERT successfully executed the activities outlined in the Cabinet Approved Information and Cyber Security Strategy (2019-2023), paving the way for the seamless transition to the next version spanning from 2024 to 2027. The drafted National Cyber Security Strategy will soon undergo submission for cabinet approval, marking a crucial step forward in fortifying our nation's cyber security landscape.

Through extensive awareness sessions, Sri Lanka CERT played a crucial role in enhancing the nation's cyber security awareness, while also demonstrating a high-resolution rate in handling reported cases. Active participation and representation in international forums highlighted 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.

As we reflect on these accomplishments, Sri Lanka CERT is self-confident to leverage its successes and further strengthen its impact in the year ahead.

TechCERT

TechCERT

1. About TechCERT

TechCERT, Sri Lanka's first and largest Computer Emergency Readiness Team (CERT) helps the public and Sri Lankan organizations keep their computer systems and networks secure. TechCERT celebrated 17 years of excellence on the 1st of September 2023. Originating as a pioneering project of the LK Domain Registry - it's now academic partner, TechCERT's goal is to provide a safety net for external entities, from the general public to large corporations against cyber-attacks and cyber emergency situations.

TechCERT has collaborative partnerships with several national and global information security organizations, such as APCERT that provide the latest data on computer and network security threats and vulnerabilities. TechCERT also works closely with these organizations on handling cyber security incidents that require multinational support. Issuing security advisories to the public, conducting security/cyber-crime related workshops and public awareness programs on the safe use of computers and the internet, and providing engineering consultancy services are a few more items in its repertoire of services.

TechCERT, as a leader in providing Cyber Security Services, works with its members to develop and implement customized and fully integrated IT security technologies and services across a wide range of IT infrastructures. We provide a high quality of service by using not just industry standard systems and software, but even more importantly, our qualified and experienced staff of full-time security experts who are active in the security community.

1.1 Establishment

TechCERT was originally founded in 2006 and has its origins as a pioneering project of the LK Domain Registry and its academic partners, it seeks to provide a way of providing a safety net for large and small organizations against cyber-attacks and emergency situations. To improve its operations and to further develop TechCERT, it was incorporated as an independent not-for-profit organization, affiliated with LK Domain Registry, on 05th September 2016 (Company registration no. GA 3238)

1.2 Resources

TechCERT currently has an expansive technical team of qualified and experienced professionals. The details of the academic/professional qualifications held by all members of the technical team are given below (the majority of the team members have multiple qualifications in different areas of information security, computer systems security, network security etc.):

Name	Designation	Qualification
Prof. Gihan Dias	Chairman	PhD, MSc, BSc Eng (Hons), MIE(SL), CEng
Prof. Shantha Fernando	Director	PhD (TU Delft), MPhil (Moratuwa), MCS (SL), BSc Eng (Hons) (Moratuwa), IET (UK), MIE (SL), CEng
Dileepa Lathsara	Chief Executive Officer	MSc, BSc Eng (Hons), CISSP, C|EH, CEng, MIE(SL), BCS(UK), ACS(Aus), Certified ISMS Auditor (ISO27001), CPISI (PCI DSS V3)
Kushan Sharma	Chief Operating Officer	MBA (Colombo), MSc in Computer & Network Security (Moratuwa), BSc Eng. (Hons)(Moratuwa), C|EH, Certified ISMS Auditor (ISO27001), AMIE(SL), MCS(SL), CPISI (PCI DSS V3.2.1)
Kasun Chathuranga	Principal Engineer	MSc in Information Systems Security (Moratuwa), BSc Eng. (Hons) in Electrical Engineering, MIEEE, AMIE (SL)
Kalana Guniyangoda	Principal Engineer	MSc in Computer & Network Security (Moratuwa), BSc IT (Hons), GCFA
Geethika Wijerathne	Senior Manager - HR & Administration	MSc in Information Systems Management (UOC), PMP, PGDip in ISM (UOC), Chartered Qualification in HRM (CIPM)
Mishra De Silva	Head of Enterprise Business	MBA (Colombo), BBA (U.S.A), AS (U.S.A), MSLIM, CIMA Adv. Dip. MA
Vijan Herath	Project Manager	BSc in Computer Science, HND in Computing (UK), ORACLE HCM (Cert), Project Management & SCRUM Immersion (Cert), CPISI (PCI DSS V3.2.1)
Chathuranga Gunatillake	Lead Security Engineer	Msc Information Security (UCSC), BEng (Hons) Computer Networks & Security, MBCS, E|NSA, C|EH, CPISI (PCI DSS V3.2), ISO/IEC 27001 Lead Auditor, C|HFI
Sahan Nanayakkara	Lead Security Engineer	BICT UCSC, MISM UoC, CPISI (PCI DSS v4.0), ISO 27001 : 2013 Lead Auditor
Chalana Madusanka	Associate Lead Security Engineer	BSc Eng. (Hons) in Computer Engineering, AMIE (SL)

Hirushan Thilanka	Associate Lead Security Engineer	Master of Information Security (UCSC), BSc in Information Systems (UCSC)
Pubudu Ranasinghe	Senior Information Security Engineer	Bsc (Hons) Information Technology (Sp. Cyber Security) - SLIIT, RHCSA(Red Hat 8.0)
Nisal Priyanka	Senior Information Security Engineer	Bsc (Hons) Information Technology (Sp. Cyber Security) - SLIIT, PGD in Cyber Security, Msc in Cyber Security
Akalanka Perera	Information Security Engineer	BSc (Hons) in IT Specialized in Cyber Security
Chamitha Gunawardena	Information Security Engineer	Bsc (Hons) Information Technology (Sp. Cyber Security) - SLIIT, CPISI (PCI DSS V3.2)
Lalindra Perera	Information Security Engineer	BSc (Hons) Computer Security, MSc Cyber Security and Forensics - Reading
Udeshika N. Alupotha	Information Security Engineer	Bsc (Hons) Information Technology (Sp. Cyber Security) - SLIIT, Msc Information Security (UoC) - Reading, CPISI (PCI DSS V4.0)
Kavindu Viraj Rathnayake	Information Security Engineer	Bsc (Hons) Information Technology (Sp. Cyber Security) - SLIIT
Shanuka Ashen Karunadasa	Information Security Engineer	Undergraduate - Bsc (Hons) Information Technology (Sp. Cyber Security) - SLIIT
Amal Hewagama	Information Security Engineer	BCS PGD, PGD in networking (NSBM), MBA sp. project management (Cardiff Metropolitan), MSc in cybersecurity (SLIIT) -reading
Umesh Erangana	Information Security Engineer	MSc in Computer Forensics (USW), BSc (Hons) Computer Security (Plymouth), CHFI, C|EH Masters
Bhathiya Pulasthi Wickramasinghe Madanayaka	Information Security Engineer	Bsc (Hons) Information Technology (Sp. Cyber Security) - SLIIT
Sudeepa Shiranthaka	Information Security Engineer	Bsc (Hons) Information Technology (Sp. Cyber Security) - SLIIT, AMIEEE
Arun Viraj Poobalan	Information Security Analyst	BSc (Hons) Information Technology (Sp. Cyber Security) - SLIIT, CPISI (PCI DSS v4.0), ISO 27001 : 2013 Lead Auditor
Lasitha Bandara	Associate Information Security Engineer	Undergraduate - Bsc (Hons) Information Technology (Sp. Cyber Security) - SLIIT
Kawya Nayanathara	Associate Information Security Engineer	Undergraduate - Bsc (Hons) Information Technology (Sp. Cyber Security) - SLIIT

Priyasuthan Pushparajah	Associate Information Security Engineer	Undergraduate - Bsc (Hons) Information Technology (Sp. Cyber Security) - SLIIT
Ravindu Pabasara Illeperuma	Associate Information Security Engineer	BSc (Hons) in IT Specialized in Cyber Security

1.3 Constituency

TechCERT's constituency comprises its member organizations, private sector organizations, selected government organizations and the general public of Sri Lanka. In accordance with its mandate, TechCERT provides effective incident response to malicious cyber threats, widespread security vulnerabilities, identifies and responds to cyber security incidents, conducts training and awareness to encourage best practices in information security and disseminates cyber threat information among Sri Lankan organizations and the public.

2. Highlights of Year 2023

TechCERT celebrated its 17th anniversary on the 1st of September 2023. TechCERT continued providing its arsenal of services through the year 2023, with a number of new additions. Following the gradual recovery of the Sri Lankan economy, TechCERT was able to meet the increasing requirements of local businesses and industries. TechCERT continued to conduct its activities in a hybrid mode of work to enhance team efficiency. TechCERT continued to secure major cyber security projects of leading conglomerates and industry giants while competing with global brands. Listed below are a few of the major activities that were successfully completed in 2023.

TechCERT Cyber Security Drill

Conducted 03 Cyber Security Drills for Banking, Financial, Telecommunication, Manufacturing sector organizations and Large Conglomerates.

- TechCERT Cyber Security Drill for Financial Sector organizations was conducted on 25th August 2023.
- TechCERT Cyber Security Drill for Banking Sector organizations was conducted on 20th September 2023.
- TechCERT Cyber Security Drill for Telecommunications Sector and Other Sectorial organizations was conducted on 25th October 2023.

TechCERT Annual Cyber Security Training and Awareness Sessions

The TechCERT annual training was conducted through a series of in-person seminars for a set number of participants from each of TechCERT's Managed Security Services clients.

- TechCERT annual training 2023:
- Pen Testing Sieges in Cyber Battle Grounds.
- Securing Payment Mobile Apps.
- Windows Artifact Analysis in Incident Response.

- Regular information security awareness sessions for employees of leading banks, financial institutions, insurance companies, telcos, and other corporations.

SWIFT Customer Security Program Independent Reviews

For the 3rd consecutive year, TechCERT continued the independent security reviews aligning with the SWIFT CSP (customer security program). This project saw definite improvements and refinements over the past two years. Four major banks in Sri Lanka engaged with TechCERT to conduct independent reviews during the year 2023.

Payment Card Industry – Data Security Standard (PCI DSS) Version Upgrade

2022 marked the proliferation of version 4.0 of the PCI DSS Standard. TechCERT ever shifting with the dynamic landscape of the industry, upgraded all PCI DSS related services to be in line with the latest version of the standard during the year 2023. Consulting services were offered to clients who were in the process of upgrading to version 4.0.

Security Assessments & Incident Responses

Conducted nearly 9500 Security Assessments on various IT infrastructures and responded to more than 650 Cyber Security incidents.

TechCERT ISO 27001:2022 Certification

TechCERT commenced the process for ISO 27001 Certification and will be implementing measures through 2024 and plans to achieve certification by end of 2024.

3. Activities & Operations

3.1 Scope and definitions

Customers can choose from a large, and constantly expanding repertoire of services ranging from Digital Forensics Investigations to Penetration tests to Web and Server Security Assessments and more. TechCERT's Managed Security Services include a range of engineering and consultancy services listed below:

- API Security Assessment
- Assumed Breach Assessment
- ATM / POS Security Assessment
- Board Level Awareness Sessions
- Cloud Architecture Security Review
- Compromise Assessment
- Cyber Security Drill
- Cyber Security Posture Assessment
- Cyber Security Strategy Development
- Digital Attack Surface Review Assessment

- Digital Forensic Readiness Review
- Digital Forensic Investigation
- Firewall Security Assessment
- Managed Security Services
- Microsoft Active Directory Security Assessment
- Microsoft O365 Security Assessment
- Mobile Application Security Assessment
- Network & Security Architecture Review
- Operation Security Assessment
- PCI DSS Certification & Consultancy
- Penetration Testing
- Physical And Environment Security Checks
- Ransomware Readiness Assessment
- Red Team Exercise
- Review Of Cyber Security Incident Management
- Risk Based Vulnerability Assessment
- Router / Switch Security Configuration Assessment
- Security Code Review
- Security Incident Response
- Security Policy Gap Assessment
- Security Risk Assessment
- Security Posture Assessment
- Server Security Configuration Evaluation
- SWIFT Security Audit
- Threat Hunting
- Thick Client Penetration Testing Assessment
- Training And Awareness
- Vulnerability Assessment
- Web Application Security Assessment
- Wireless Security Assessment

3.2 Security Assessment

Statistics related to the security assessments conducted by TechCERT during the year 2023 are given below:

Assessment Type	Count
Internal Vulnerability Assessments	4051
External Vulnerability Assessments	3100
Web-based Security Vulnerability Assessments	1467
Firewall Rule Review and Security Assessments	151
Other Assessments (DF investigations, Wireless, Network, etc.)	721

Table 3 Number of Conducted Security Assessments

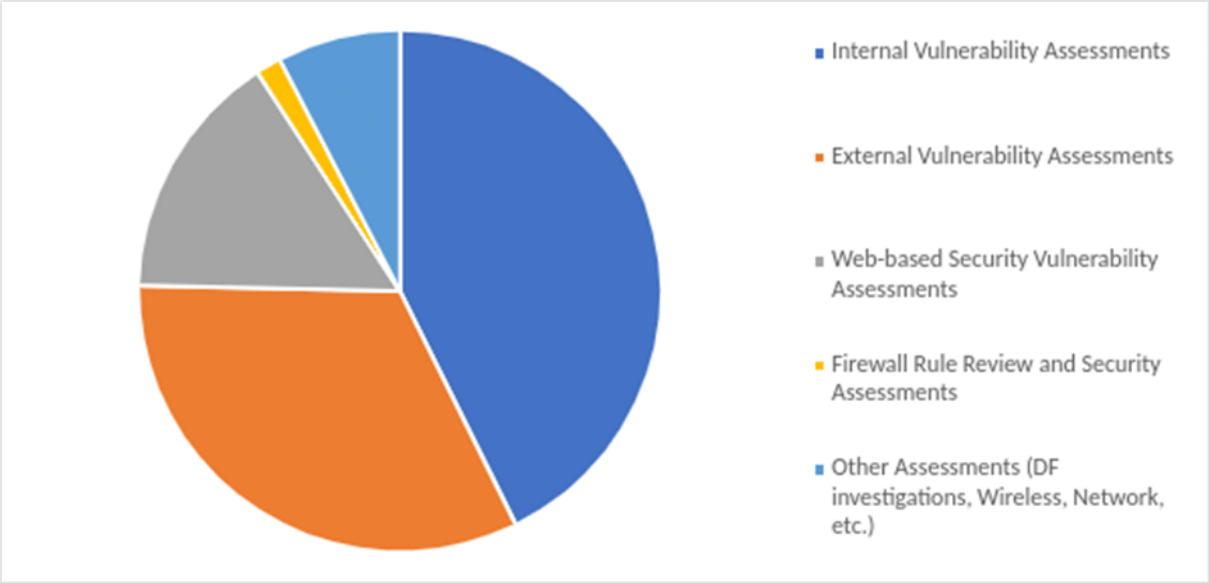


Figure 1 Number of Conducted Security Assessments

3.3 Incident handling

A broad range of entities reported Cyber Security incidents to TechCERT during the year 2023, including clients from the Banking sector, Telecommunications sector, Finance sector, General Public and Corporations. The following are statistics pertaining to the Cyber Security Incidents that were received by TechCERT in the year 2023:

Activity Type	Count
Server Security Compromises	182
Malware Infections	145
Ransomware Related Incidents	132
Social Network Related Incidents	50
Phishing Incidents	21
Website Defacement	15
Other Incident Responses	119

Table 4 Number of Responded Incidents

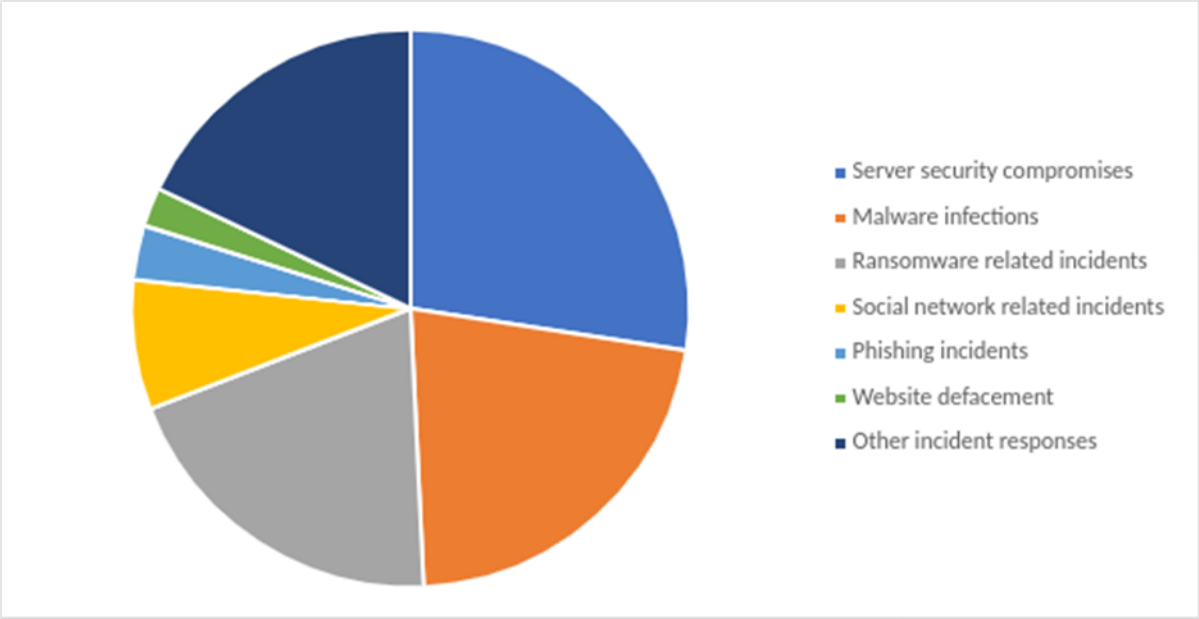


Figure 2 Number of Responded Incidents

3.4 Abuse statistics

Server compromise, Malware infections and Ransomware related incidents are some of the most serious and abundant cyber threats in Sri Lanka. The most consistent and common type of Cyber Security incident observed in 2023 was Server Security Compromises. An increase in the amount of Ransomware Related incidents was noted in 2023.

3.5 TechCERT's New services

Listed below are services commenced by TechCERT in 2023:

- Thick Client Penetration Testing Assessment
- Microsoft O365 security assessment
- Active Directory security configuration review
- Security Posture Assessment
- Board level awareness sessions

4. Events organized / hosted

4.1 Training

In 2023, TechCERT conducted a number of training sessions for its member organizations and other entities. The trainings were conducted in-person. Given below is a list of training sessions conducted:

- TechCERT annual training 2023:
  - Pen Testing Sieges in Cyber Battle Grounds.
  - Securing Payment Mobile Apps.
  - Windows Artifact Analysis in Incident Response.
- Regular information security awareness sessions for employees of leading banks, financial institutions, insurance companies, telcos, and other corporations.
- Ransomware Readiness training for customers;
  - Focused on the developing threat of AI based Ransomware.

4.2 Cyber Security Drills

In addition to being a proven method of spreading knowledge among customers and members of TechCERT, it also serves the important purpose of creating an effective means of grading each candidate on their pre-existing experience and expertise. Listed below are the drills that were hosted by TechCERT in 2023:

- TechCERT Cyber Security Drill 2023– Finance Sector.
- TechCERT Cyber Security Drill 2023– Telecommunications Sector and Other Sectors.
- TechCERT Cyber Security Drill 2023– Banking Sector.

4.3 Conferences and seminars

TechCERT upholds an active position in the local and international arena by partaking in various Conferences and/or Seminars. On occasion, team members of TechCERT who are experts in certain fields will speak at/coordinate these events. In 2023, TechCERT conducted multiple in-person seminars as given below:

- Seminar on career opportunities in Information Security:
- Seminar for the University of Kelaniya.
- Seminar for the University of Moratuwa.
- Seminar for NSBM Green University.

TechCERT participated in the following local conferences:

- The CIO Confluence – February 2024.
- 41st National IT Conference hosted by Computer Society of Sri Lanka (CSSL) - October 2023.

TechCERT nominated an employee to partake in the Asia Pacific Next Generation (APNG) Camp 16 held in Bangkok, Thailand on the 23rd to the 25th of February 2024.

5. International Collaboration

Collaboration with the Internet Assigned Numbers Authority (IANA) during 2023:

- Mr. Dileepa Lathsara participated in the Root Zone KSK Ceremony of April 2023 held in Virginia, USA. He continues to fulfill his role as an IANA Crypto Officer. His duty involves key aspects of managing the Root Zone Key Signing Key of DNSSEC.

6. Capacity building

TechCERT greatly values the contribution its employees provide, and as such seeks to enhance their knowledge both for the betterment of TechCERT and for their own professional development. Mentioned in the following sections are the efforts taken by TechCERT towards advancing this goal in the year 2023.

6.1 Training

TechCERT enlisted its workforce in a number of external and internal training sessions to enhance their skillset. TechCERT also launched its new internal training program titled “Vanguard”, focused at expanding the technical knowledge of all employees. Mentioned below is the list of training sessions undergone by TechCERT employees:

- TechCERT - SISA - 417th CPISI- PCI DSS v4.0 Implementation e-Workshop – January (2024).
- Internal Training workshops covered under the Vanguard training program so far:
- Wireless Network Security Configuration Review Assessment

- Firewall Security Configuration Review and Rule Evaluation
- Other internal staff skill development training workshops:
  - Security Vulnerability Assessment
  - Mobile Security Assessment
  - Network Vulnerability Assessment and Penetration Test
  - API Security Assessment
  - Web Vulnerability Assessment and Penetration Test
  - Incident Response Capability Development
- Information Security Awareness sessions were conducted for internal employees in line with ISO 27002 requirements.
- Workshop conducted by an external legal professional for entire staff: Overview of Legal Aspects Within Information Security.

6.2 Drills & exercises

To fortify its own employee's collective knowledge, TechCERT participated in the annual APCERT Cyber Drill as follows:

- APCERT Cyber Drill 2023: Digital Supply Chain Redemption.

7. Future Plans

7.1 Future projects and operation

The past year contained several challenges brought on by an increase in workload and the economic crisis which is now gradually receding. With Sri Lanka now on the path to economic recovery, TechCERT plans for a bright and prosperous future. As such, it has set forth several ambitious goals it hopes to achieve in the future.

- Achieving new levels of sustainable business growth and ensuring an efficient delivery of services to customers
- Continue providing assistance and awareness to the citizens of the country on the ever-rising stream of cyber security threats.
- Work towards the enhancement and maintenance of the information security posture of all our member organizations.
- Expanding the TechCERT Annual Cyber Security Drill in order to encompass broader topics.
- Conducting more Cyber Security Drills to accommodate a diverse and larger number of participants.
- Focus on providing information security awareness seminars to university students and the general public to enhance information security posture.
- Grow and strengthen the TechCERT team and provide them with the opportunity to garner new skills and talents.

8. Conclusion

In 2023, TechCERT met and exceeded the needs of all its patrons, by promptly and effectively responding to the evolving threat landscape within Sri Lanka. Key among which included a high number of compromised servers and malware infections. Observing a spike in the number of Ransomware Related Incidents, TechCERT recognizes the importance for its clientele to be well informed prior to incidents, that way ensuring a minimum impact on operations. TechCERT also expanded its skilled workforce by adding new skilled individuals and complementing existing ones with the sharing of skills. Maintaining its commitment to consistency and quality, TechCERT strives to provide a superior service to all.

In conclusion, 2023 saw the slow stabilization and then gentle recovery of the Sri Lankan economy. TechCERT has overcome a multitude of challenges in the past and is once again looking forward to a thriving future. TechCERT remains committed to the wellbeing of its employees by offering flexible work arrangements and much needed support. As Sri Lanka's leading Cyber Security Service provider, TechCERT is committed to continue growing and meeting the future headfirst.

TWCERT/CC

Taiwan Computer Emergency Response Team / Coordination Center

1. Highlights of 2023

1.1 Summary of Major Activities

In 2023, the Taiwan Computer Emergency Response Team / Coordination Center (TWCERT/CC) shared over 530,000 cyber events and Indicators of Compromise (IoC), 12 cybersecurity intelligence newsletters, and 228 cybersecurity news articles globally. As a CVE Numbering Authority (CNA) for the Common Vulnerabilities and Exposures (CVE) system, TWCERT/CC reviewed and assigned 109 CVE IDs in 2023. TWCERT/CC participated in seven international cybersecurity conferences, seminars, and drills. It also hosted the 2023 Conference of Taiwan Cyber Security Notification and Response and other nine cybersecurity events for Taiwan's enterprises, including working group meetings and security training for the Taiwan CERT/CSIRT Alliance. TWCERT/CC actively seeks opportunities to collaborate with multilateral partners to raise the visibility of the Taiwan CERT/CSIRT Alliance and participate in international events to contribute to the global community.

1.2 Achievements & Milestones

- TWCERT/CC shared more than 530,000 cyber events and IoCs across 16 categories. Outbound attacks, suspected system vulnerabilities, and system intrusions were the three most common types of attacks in 2023.
- TWCERT/CC issued 12 monthly e-newsletters and 228 articles covering domestic and global cybersecurity news.
- As a CVE Number Authority, TWCERT/CC reviewed and assigned 109 CVE IDs in 2023.
- TWCERT/CC participated in seven international cybersecurity conferences. We also held ten domestic cybersecurity events, including the 2023 Conference of Taiwan Cyber Security Notification and Response, regular meetings, and training events for the Taiwan CERT/CSIRT Alliance.

2. About TWCERT/CC

2.1 Introduction

Taiwan Computer Emergency Response Team / Coordination Center (TWCERT/CC) responds to major cybersecurity incidents, analyzes cyber threats, publishes vulnerability information, and exchanges cyber intelligence with trusted global partners. In 2023, TWCERT/CC:

- Strengthened international cooperation with cybersecurity partner teams and enhanced intelligence gathering and sharing.
- Issued monthly e-newsletters regarding cybersecurity trends, cybersecurity tips, and security advisories.
- Participated actively in international and domestic conferences and seminars.
- Established the Taiwan CERT/CSIRT Alliance.
- Assisted enterprises with cybersecurity incident response and coordination and raised cybersecurity awareness.
- Offered Virus Check, CVE reporting, Phishing Check services, and cybersecurity incident reporting channels.

TWCERT/CC is a member of FIRST, APCERT, and is a Numbering Authority of the Common Vulnerabilities and Exposures (CVE®) system. TWCERT/CC also collaborates with other CERT organizations in the world to handle cybersecurity incidents and exchange cyber intelligence.

2.2 Constituency and Scope of Work

TWCERT/CC is dedicated to increasing the overall cybersecurity capabilities of Taiwan. The result of our work is a national collaborative defense mechanism, so that the cybersecurity industry has advanced capabilities, our nation has ample cybersecurity human resources, and a strong public-private partnerships on cybersecurity matters.

TWCERT/CC provides cybersecurity services to enterprises and individuals in Taiwan, and serves as a pillar for cybersecurity awareness in Taiwan's public/private sectors, working closely with cybersecurity organizations, academic institutions, civil communities, governmental institutions, private enterprises, and the global CERT/CSIRT community.

Our services include intelligence collection and dissemination, incident reporting, handling, coordination, and cybersecurity consulting. To raise awareness of incident reporting, we also actively disseminate educational resources on incident handling and organize enterprise cybersecurity trainings and events.

3. Activities & Operations

3.1 Incident Handling & Cyber Intelligence Sharing

TWCERT/CC regularly analyzes and disseminates cybersecurity incident reports and intelligence received from CERT partners, the public and private sectors in Taiwan, cybersecurity companies, and individual researchers, to help foster Taiwanese and international defense capacity, as well as strengthen the synergy of TWCERT/CC with its partners.
Using these reports, we coordinate incident handling and help individuals and enterprises mitigate cyber threats. In 2023, TWCERT/CC shared more than 530,000 cyber events and IoCs with CERT and cybersecurity organizations, private enterprises, and cybersecurity communities globally. Monthly breakdowns of the cyber intelligence shared are shown in Figure 1.

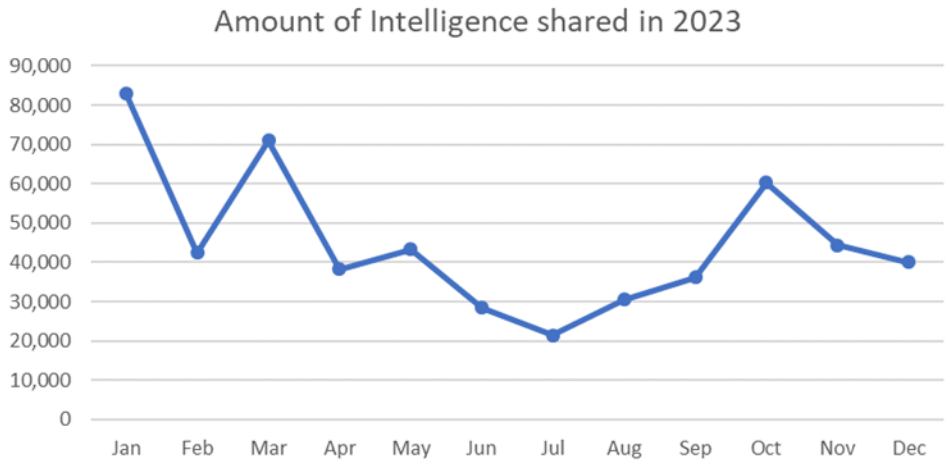


Figure 1 Cyber Intelligence shared by TWCERT/CC in 2023

TWCERT/CC consistently seeks progress on:

- Prevention: Provide advisories and early warnings to our constituency so that they can take preventative measures to lower the risk of cybersecurity breaches.
- Reporting: Issue timely warnings for cybersecurity incidents so that remedial measures can be taken immediately.
- Handling: Provide technical support, consultation, and coordination for threat mitigation and recovery.

3.2 Publications

As part of our continuous effort to raise public awareness of cybersecurity, TWCERT/CC releases a monthly e-newsletter regarding important cyber intelligence through email, TWCERT/CC's official website, Facebook fan page, and a popular domestic blog platform (Pixnet). The e-newsletter contains information on TWCERT/CC's recent contributions,

cybersecurity policies, emerging threats, cyberattacks, vulnerabilities, events, and the statistics of cybersecurity incident reports. In 2023, TWCERT/CC issued a total of 12 monthly e-newsletters and 228 domestic and global cybersecurity news articles.

3.3 Services

Common Vulnerability Disclosure

TWCERT/CC receives vulnerability reports from global researchers and maintains a Taiwan Vulnerability Note (TVN) database to disclose vulnerability information. As a CVE Numbering Authority, TWCERT/CC reviews and assigns CVE IDs to vulnerabilities that meet the criteria. By assisting with vulnerability mitigation and remediation coordination, TWCERT/CC helps Taiwanese enterprises reduce the risk and impact of potential cybersecurity incidents. In 2023, we assigned IDs to 109 vulnerabilities.

Virus Check

We offer an online file analysis service that conducts both static and dynamic analysis to determine the risk level of a file. When a file has high-risk behavior but a low anti-virus detection rate, it will be passed to TWCERT/CC's collaboration partners: Trend Micro, CyCraft Technology, and TeamT5, for manual analysis. If a new type of malware is recognized, the partners will create a corresponding virus signature to improve future detection of this malware.

Phishing Check

Phishing Check is an online phishing site reporting service for the general public. The service includes analysis and validation of the reported phishing web pages as well as reporting to relevant parties for takedown requests. Phishing Check is dedicated to mitigating the impact of phishing websites and improving the overall cybersecurity capabilities in Taiwan.

Anti-Ransom

TWCERT/CC has established a dedicated Anti-Ransom site containing critical information on ransomware preventive measures and response, as well as post-incident recovery. Anti-Ransom is aimed at assisting individuals and enterprises to improve their cybersecurity capability in response to the fast-growing threat of ransomware today.

4. Cybersecurity Events

4.1 Domestic Cybersecurity Events

TWCERT/CC actively participated in domestic cybersecurity events, the Cryptology and Information Security Association (CISC) 2023, the ICANN APAC-TWNIC Engagement Forum, the 38th TWNIC IP Open Policy Meeting, and the ISACA ITAF Promotion Conference and HICON PEACE 2023. TWCERT/CC also presented at ten domestic cybersecurity events for

Taiwan's enterprises. The events covered cyber defense, case studies, and cyber awareness promotion, including organizing a Taiwan CERT/CSIRT Alliance Conference and three cybersecurity training events for private enterprises in Taiwan. Topics explored included cybersecurity drills, emerging cyber threats, vulnerability reports, incident response etc. In addition, TWCERT/CC organized the 2023 Conference of Taiwan Cyber Security Notification and Response (figure 2) with the theme "Resilient Cyber and Sustainable Taiwan" (韌性資安 永續台灣). Cybersecurity experts were invited from different fields of industry, government-sector, and academic fields to share their valuable knowledge and experience with the audience. Broad cybersecurity topics were discussed, such as dark web observation and international cybersecurity trends. Several honored guests from Microsoft, CyCraft, Insikt Group Recorded Future, and Panasonic were invited to share their expertise and experience.

One of the panel discussions entitled "International cybersecurity trends" was hosted by Kenny Huang, the CEO of TWNIC. Experts from the Taiwan CISO Alliance shared their experiences coordinating cyber joint defense in their constituency.

Figure 2

4.2 International Cybersecurity Events

TWCERT/CC has been actively engaged with our international partners and cybersecurity events. In 2023, TWCERT/CC participated in the following international events:

- 35th Annual FIRST Conference
- APNIC 56
- NatCSIRT 2023 Annual Conference
- RSA conference
- Blackhat USA 2023
- DEFCON 31

- ICANN78 Annual General Meeting

TWCERT/CC participated in APCERT Cyber Drill 2023. The theme was "Digital Supply Chain Redemption", and this exercise reflected real incidents and issues that exist on the Internet. This drill included the need for the teams to interact locally and internationally with CSIRTs/CERTs and targeted organizations. Participants coordinated the suspension of malicious infrastructure, performed analysis of malicious code, as well as notifying and assisting the affected entities. This incident response exercise was coordinated across 24 CSIRTs from 21 economies. This reflects the collaboration amongst the economies in mitigating cyber threats and validates the enhanced communication protocols, technical capabilities, and quality of incident responses that APCERT fosters in assuring Internet security and safety.

5. Future Work

TWCERT/CC is dedicated to optimizing its services and raising awareness of cybersecurity. In 2024 and beyond, we will continue to:

i. Disseminate vulnerability and cybersecurity incident information, including publishing our monthly cybersecurity e-newsletter, and annual cybersecurity report.
ii. Regularly notify our constituency of emerging cyber threats and policies.
iii. Collect, analyze, and release the latest information regarding cybersecurity conferences, seminars, and training.
iv. Actively strengthen cooperation with international and domestic cybersecurity partners to improve cybersecurity capabilities.

6. TWCERT/CC Contact Information

- Website: https://www.twcert.org.tw/
- Facebook: https://www.facebook.com/twcertcc/
- E-Mail: twcert@cert.org.tw

TWNCERT

Taiwan National Computer Emergency Response Team

1. Highlights of 2023

1.1 Summary of major activities

TWNCERT (Taiwan National Computer Emergency Response Team) aims to support and enhance the government's ability to respond to and deal with cybersecurity incidents. In 2023, TWNCERT issued more than 1,600 advisories and alerts to government agencies and provided consulting and training services for government agencies and critical infrastructure (CI) providers.

To strengthen preparedness against cybercrimes, technology failures, and critical information infrastructure (CII) incidents, TWNCERT conducts an international cybersecurity exercise called Cyber Offensive and Defensive Exercise (CODE) every two years. TWNCERT also keeps conducting social engineering exercises and information system penetration drills to enhance the cyber defense capabilities of Taiwan government agencies.

In addition, TWNCERT launched a series of cybersecurity competitions in 2023 to nurture talents and promote cybersecurity awareness, and over two thousand people participated.

1.2 Achievements & milestones

In 2023, TWNCERT developed 21 cybersecurity competency courses to improve cybersecurity protection and awareness among government agencies. Civil servants can enroll in these courses and take exams. Moreover, as the convener of the APCERT Training Working Group, TWNCERT held four online training sessions this year with a total of fourteen APCERT member teams participating.

2. About TWNCERT

2.1 Introduction

As the national CERT, TWNCERT acts as the point of contact between the worldwide CSIRT and Taiwan in the CI sectors. We aim to enhance the government and CI providers' ability to respond to cybersecurity incidents by offering technical and consulting services.

2.2 Establishment

TWNCERT was established in 2001 by the National Information and Communication Security Taskforce. TWNCERT is currently managed by the National Institute of Cyber Security (NICS), a public body overseen by Taiwan's Ministry of Digital Affairs (MoDA). As a government computer security incident response team (CSIRT), TWNCERT continuously fosters capabilities in cyber threat monitoring, incident coordination, and incident response.

2.3 Resources

TWNCERT currently has over two hundred full-time employees. Operational funding mainly comes from Taiwan's Ministry of Digital Affairs.

2.4 Constituency

TWNCERT is dedicated to enhancing the capabilities of incident reporting and response among government agencies and CI sectors. TWNCERT coordinates information sharing with various stakeholders such as Financial ISAC (F-ISAC), Academic ISAC (A-ISAC), Communication ISAC (C-ISAC), Energy ISAC (E-ISAC), Transportation ISAC (T-ISAC), Health and Welfare ISAC (H-ISAC), High-Tech Park ISAC (HT-ISAC), major MSSPs, law enforcement agencies, other CSIRTs in Taiwan as well as cybersecurity vendors and organizations worldwide.

3. Activities & Operations

3.1 Scope and Definitions

Our critical mission activities are:

Incident Response

Responsible for responding to cybersecurity incidents in the government agency and CI sectors and providing practical and effective assistance to related agencies to counter threats or cyberattacks.

Information Sharing

The National Information Analysis Center (N-ISAC) provides a central resource for gathering information on cyber threats to CI. It offers two-way information flows between the private and public sectors.

Cybersecurity Drill and Audit

Hold large-scale cyber attack and defense exercises, and provide cybersecurity audits, cyber health checks, and penetration test services to discover cybersecurity weaknesses of government agencies and CI providers in time.

Education & Training

Plan a series of cybersecurity competitions and training programs to enhance the effectiveness of cybersecurity education and raise cybersecurity awareness.

Coordination and Collaboration

Build communication channels with domestic and foreign incident response organizations; coordinate with international CSIRTs, cybersecurity vendors, and other cybersecurity organizations.

3.2 Incident handling reports

In 2023, TWNCERT received more than one thousand incident reports from Taiwan government agencies. We also received more than one thousand incident reports from international CERTs/CSIRTs and cybersecurity organizations. In addition, more than 780,000 critical information reports were shared among National-ISAC members (CI sector ISACs, MSSPs, and Taiwanese CSIRTs).

3.3 Abuse statistics

Government agencies

Among the cybersecurity incident reports TWNCERT received from government agencies in 2023, about 54% were

categorized as “intrusion”, as shown in Figure 1.

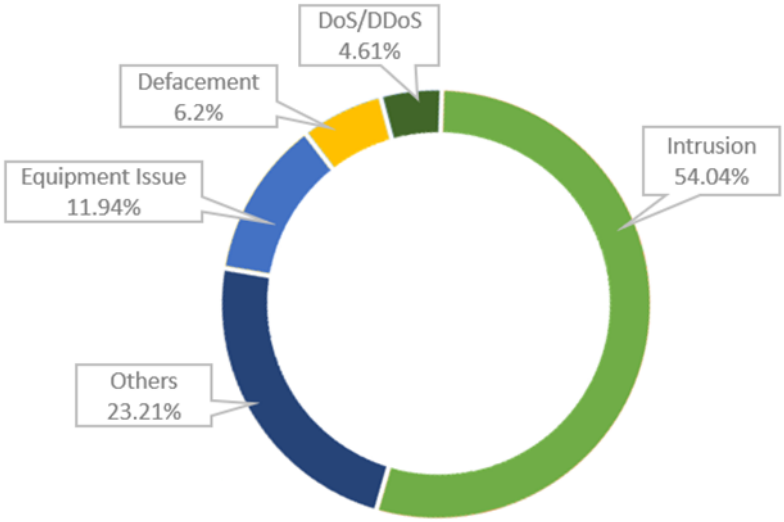


Figure 1. Cybersecurity Incidents reported by Government Agencies

International cyber incident report

In 2023, TWNCERT received about one thousand cybersecurity incident reports from international CERTs/CSIRTs and cybersecurity organizations. The cybersecurity incident reports were categorized as shown in Figure 2. About 83.6% of the incident reports were system infected by malware, followed by phishing and malicious URLs.

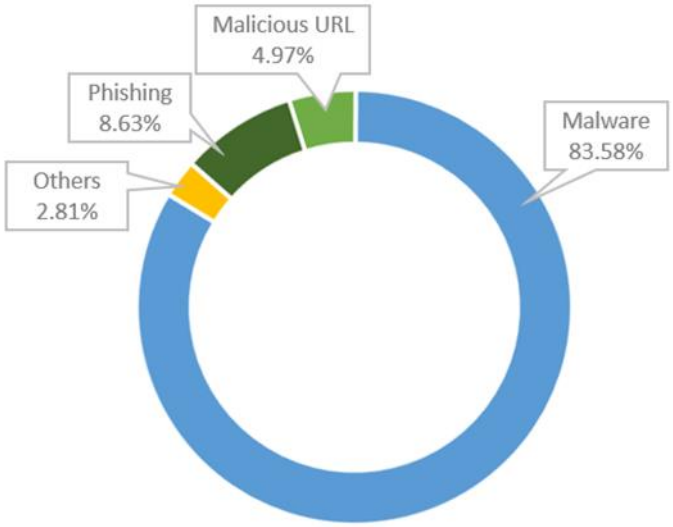


Figure 2. Cybersecurity Incidents reported by international organizations

N-ISAC information sharing

N-ISAC members shared more than 780,000 cybersecurity incidents and critical information. About 98.57% of these

reports were incidents, and about 1.43% were early warnings.

3.4 Publications

Website publication

Based on the information collected and analyzed, TWNCERT published 45 articles in 2023, including cybersecurity early warnings, news, and guidance.

Advisory and Alert

TWNCERT issued more than 1,600 advisories and alerts to government agencies in 2023. Figure 3 shows the distribution among different categories.

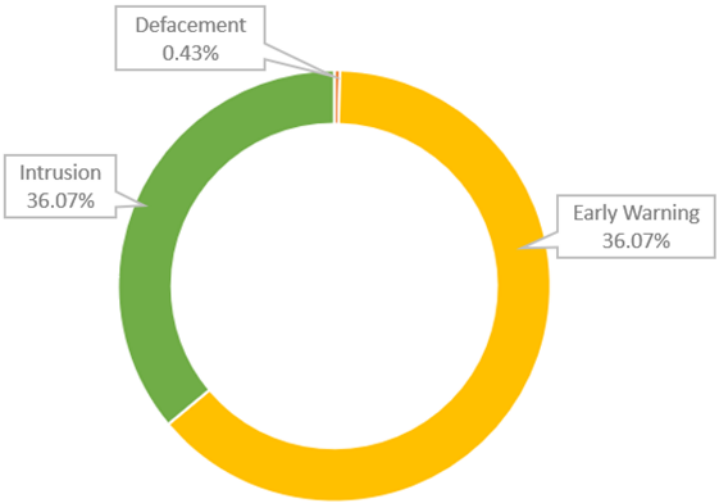


Figure 3. Distribution of Government Notice Advisories

International incident report

In 2023, TWNCERT shared more than 24,000 incident reports with other national CERTs/CSIRTs. Most of them were SSH brute-force attacks detected by TWNCERT.

4. Events organized/hosted

4.1 Training

In 2023, TWNCERT developed 21 cybersecurity competency training courses. We provided these courses and exams to civil servants, and assisted government agencies in promoting cybersecurity protection and awareness.

4.2 Drills & exercises

Drill

To strengthen the readiness against cybercrimes, technology failures, and other cybersecurity incidents in CIIs, TWNCERT conducts the Cyber Offensive & Defensive Exercise (CODE) every two years. We also continue to conduct social engineering exercises and information system penetration drills to help promote the preparedness of Taiwan government agencies.

CODE 2023 coordinated the red and blue team's live-action confrontation in the water resource CI sector. A total of 18 nations were represented, and 45 domestic governmental and private organizations participated.

Figure 4. CODE

Cybersecurity competition

To nurture cybersecurity talents and promote public awareness of cybersecurity, TWNCERT launched a series of cybersecurity competitions in 2023, attracting more than two thousand students and the public to participate.

Figure 5. Cybersecurity Skill Competition

4.3 Conferences and seminars

TWNCERT held the N-ISAC meeting to discuss recent cybersecurity issues and information sharing efficiency in December 2023.

This meeting is the annual meeting of all members. Experts from the public and private sectors were invited to share valuable insights and experiences. Moreover, we held workshops for the N-ISAC members to collaborate. Workshop topics focused on strategies and practices for protecting CI and key resources and building trust relationships with other sectors.

5. International Collaboration

5.1 International partnerships and agreements

TWNCERT actively participates in membership activities of international organizations, including meetings, working groups, annual conferences, and other cooperation opportunities. The organizations that TWNCERT participates in are as follows:

- Asia Pacific Computer Emergency Response Team (APCERT)
- Forum for Incident Response and Security Teams (FIRST)
- Telecommunications and Information Working Group, Asia-Pacific Economic Cooperation (APEC TEL)
- Meridian

5.2 Capacity building

5.2.1 Training

As the convener of APCERT Training Working Group, TWNCERT coordinated member teams for online training sessions and convened 4 training sessions in 2023.

Date	Title	Presenter
2023/3/28	DNS Security and Threats for Incident Responders	ICANN
2023/5/9	5G Vulnerability Analysis	KrCERT/CC
2023/7/14	Cyberspace Search Engine – Overview and Applications	TWNCERT
2023/10/11	Exploring Machine Learning on Phishy Domains	AusCERT

Figure 6. APCERT Training

5.2.2 Drills & exercises

The APCERT Drill was conducted on August 16, 2023. TWNCERT participated in the drill with the theme “Digital Supply Chain Redemption” and solved a set of drill scenarios within the given time limit.

5.2.3 Seminars & presentations

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

- APEC TEL Conference
- FIRST 2023 AGM
- APCERT AGM 2023 (online)

6. Future Plans

For the APCERT online training program, TWNCERT will continue to coordinate trainers and participants to provide bimonthly online training, expand coordination with other APCERT Working Groups, and participate in APCERT activities such as APCERT drills. Possible collaboration opportunities with other international organizations will also continue to be a pivotal emphasis to enhance the depth and broadness of the training program in the future.

7. Conclusion

TWNCERT will continue to enhance collaboration with government agencies, particularly CII sectors. We will build further public-private partnerships and collaborate with local and global CSIRTs to strengthen cybersecurity awareness and incident handling capabilities. The essential elements of our ongoing strategy are:

- Enhance government agency accountability and guide resource allocation
- Expand public-private partnerships to enhance the resilience of critical infrastructures
- Defense-in-depth deployment and governmentwide situational awareness
- Harden IT infrastructure and reduce cyberattack surfaces
- Check and evaluate regularly, improve through lessons learned
- Cultivate future talents to improve cybersecurity

In the Asia-Pacific region, TWNCERT is committed to contributing to the APCERT mission and looks forward to all cooperation opportunities to build a safe and secure cyberspace for the prosperity of society.

VNCERT/CC

Viet Nam Cybersecurity Emergency Response Teams/Coordination Center

1. Highlights of 2023

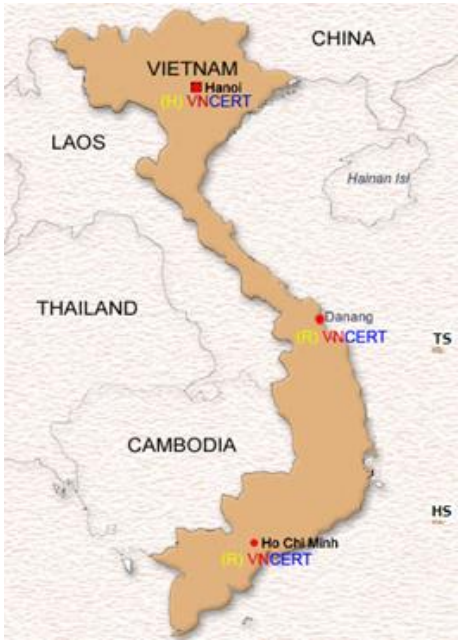
In 2023, VNCERT/CC has focused on capacity building for CISRTs. Besides, VNCERT/CC has some activities such as:

- Launched a digital investigation support platform, a platform providing knowledge and specialized tools for digital investigation.
- Developed and provided tools to check, review and support incident response activities https://github.com/VNCERT-CC/digital-forensics-lab?tab=readme-ov-file.
- Operated the Anti-Spam Portal (chongthurac.vn)
- Implemented tools to support child online protection (vn-cop website mirroring tool and secure website lookup tool).
- Established a set of criteria to promote the development of incident response teams.

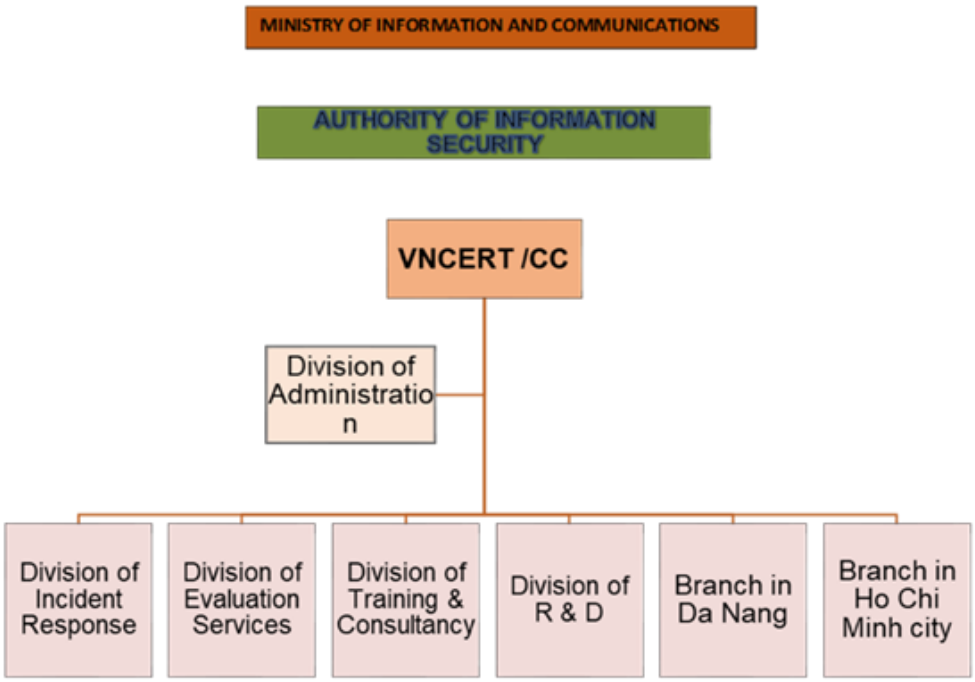
2. About VNCERT/CC

2.1 Introduction

- The Viet Nam Cybersecurity Emergency Response Teams/Coordination Center (VNCERT/CC) has been reorganized and renamed since 2019 from VNCERT (The Vietnam Computer Emergency Response Team), which was established in 2005 by the Prime Minister.
- VNCERT/CC has functioned as a coordinator of computer incident response activities nationwide; timely warnings of computer network security issues; coordination of the development of standards and technical regulations on computer network safety; security evaluation services; encourage the formation of CERT/CSIRT in agencies, organizations, and enterprises; being the contact point with the international CERT organizations (CERTs).
- VNCERT/CC has more than 70 employees at the Head Office and two branches.

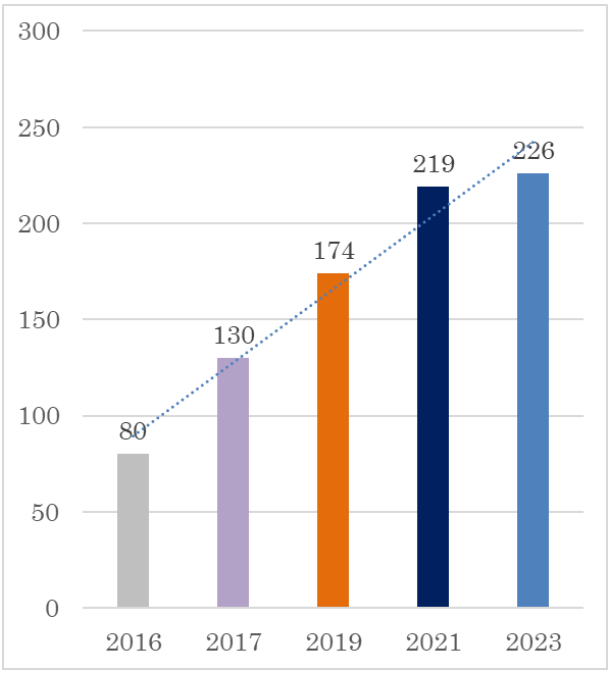


- VNCERT/CC is a member of the Forum of Incident Response and Security Teams (FIRST), APCERT, Cybersecurity Alliance for Mutual Progress (CAMP)



The organizational structure of VNCERT/CC

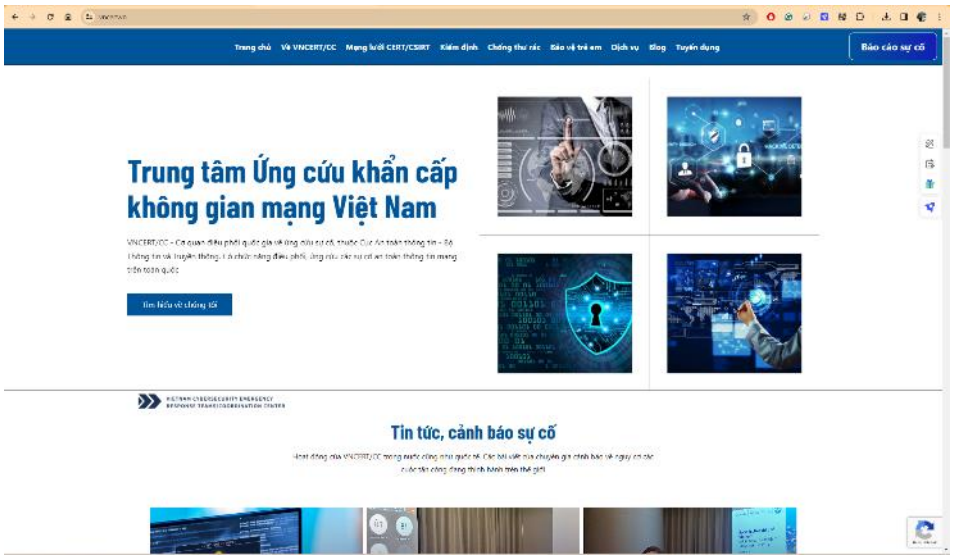
- VNCERT/CC is a leader and coordinator of the National Cybersecurity Incident Response Network of Vietnam which consists of 226 organizational members with more than 4,000 technicians.



Vietnam Cybersecurity Incident Response Network Members

2.2 Contact Information

- Website: http://www.vncert.gov.vn/
- E-mail: international@vncert.vn
- Tel: +84-24-3640 4421 (08:00-17:00 - Working hour)
- Incident report: ir@vncert.vn
- Hotline: + 84-86 810 0317 (24x7)

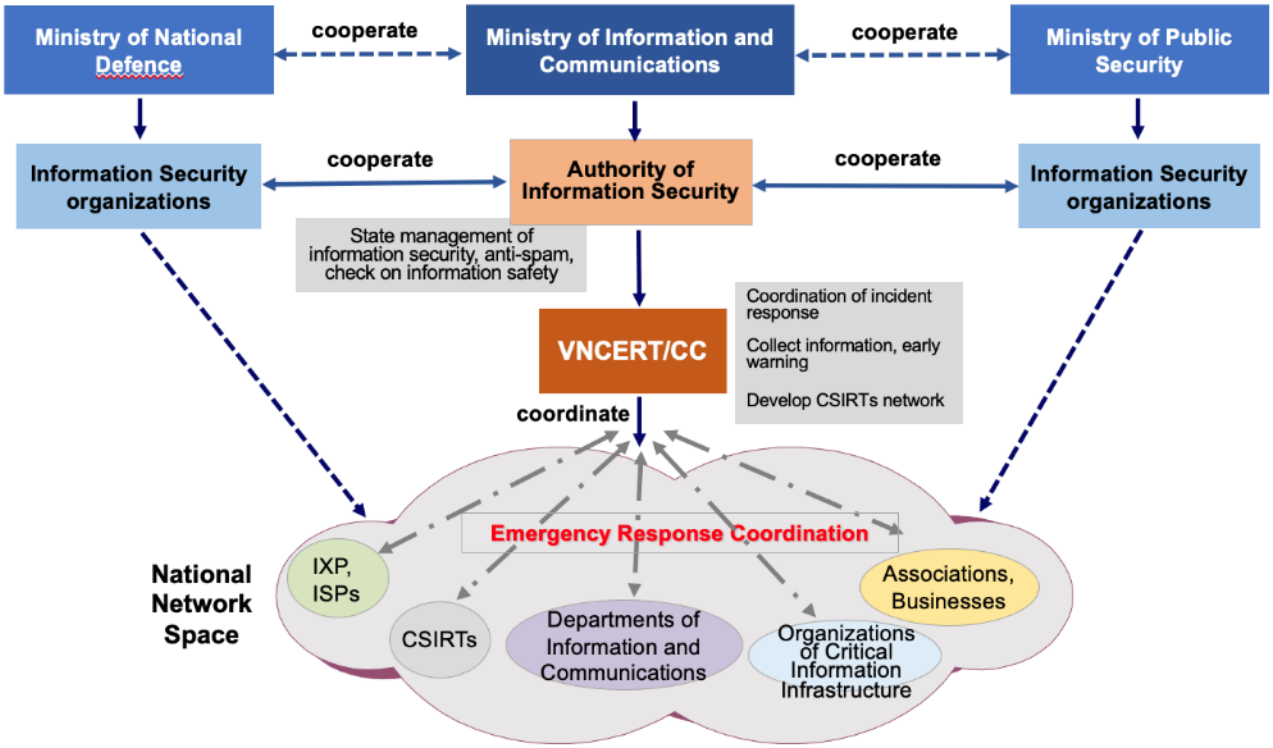


3. Activities & Operations

3.1 Scope and definitions

VNCERT/CC has the roles of:

- Receiving reports of security incidents and warning
- Coordinating national cybersecurity incident response activities.
- Promoting to build of CERTs/CSIRTs in Vietnam's organizations, enterprises, and agencies.
- Operating activities of the National Cybersecurity Incident Response Network of Vietnam with 226 members (including incident response center, information security center or information technology centers from Ministries, ministerial agencies, governmental agencies, telecommunication enterprises, Internet service providers, Finance Organizations, Banks, critical information infrastructure organizations, and organizations in charge of national information systems).
- Being the point of contact of Vietnam with the other CERTs in the world.
- Implementing and deploying the anti-spam activities.
- Enhance and safeguard the operations of children on internet as a being an operation member of the Viet Nam's Network for Child Online Protection (VN-COP), be established in 2021 with 24 organizations as members.



3.2 Incident handling reports

Security Incidents	2023
Phishing	1332
Deface	285
Malware	254
Vulnerability	218
Data leak	248
Total	2,223

Received and handled 1,801 international requests of supporting, coordinating for sources of threat, attack, and be compromised in Vietnam, in which 74% requests related to phishing, 14% to malware.

3.3 New services

- Incident response lab – IRLab https://irlab.vn/
- Digital forensics lab DFLab and tools in https://df.irlab.vn/docs/
- Supports and protection for Viet Nam Child Online Protection Network.

4. Events organized/hosted

4.1 Training

Participated and/or organized:

- Supported 34 ministries, branches, and localities to organize security real cybersecurity exercise.
- Connected with international organizations to participate cybersecurity training programs.

4.2 Drills & exercises:

Participated:

- VNCERT/CC participated in the APCERT cyber drill on 16 August 2023, based on the theme "Digital Supply Chain Redemption", and forwarded to organizational members of National Cybersecurity Incident Response Network of Vietnam participation at the same time as APCERT drill.

- VNCERT/CC participated in the ASEAN CERTs Incident Response Drill (ACID) on 18 and 19 October 2023, based on the theme "Responding to Multi-Pronged Attacks Arising from Hacktivism", forwarded to organizational members of National Cybersecurity Incident Response Network of Vietnam

Organized:

Organized 05 national drills/exercises (02 international drills, 03 Real Cybersecurity Exercises) for organizational members of the National Cybersecurity Incident Response Network of Vietnam. The three national cybersecurity exercises in real model have discovered 517 critical and high-severity security vulnerabilities.

Supported and joined:

Supported and participated in 80 Cybersecurity Exercises according the new real model of Information Technology /Information Security agencies of ministries, provinces and cities, and organizations with the participation of about 2,410 technical and management staffs, discovered 739 security vulnerabilities in totals with many critical and high-severity security vulnerabilities.

4.3 Conferences and seminars

VNCERT/CC cooperated with other organizations to organize annual events such as "Security World 2023", "National Information Security Day 2023", Vietnam Security Summit 2023 and organized other conferences for members of the National Cybersecurity Incident Response Network of Vietnam.

5. International Collaboration

5.1 International partnerships and agreements

- Bilateral exchange cooperation with CERT-In.

- Exchanged information, connect with CyberCX (Australia), built the 2024 operating plan of the two parties.

- Collaborate with other incident response teams on troubleshooting, including SingCERT, JPCERT/CC, ….

5.2 Capacity building

5.2.1 Training

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

5.2.2 Drills & exercises

Attended 2 drills of APCERT 2023, and ACID 2023.

5.2.3 Seminars & presentations

Attended ASEAN-Japan meetings, CAMP meeting and other regional workshops in ASEAN.

5.3 Other international activities

Contacting and cooperating with international organizations and businesses for security data sharing, coordinating, protecting, mitigating, etc.

6. Future Plans

6.1 Future projects

Building Platform for Real Cybersecurity Exercise.

6.2 Future Operation

- Develop technical human resources of VNCERT/CC;
- Continue to develop the National Cybersecurity Incident Response Network of Vietnam, to improve the cybersecurity service quality and quantity for the community; to develop guidelines for implementing the criteria for incident response team development; to evaluate the development of incident response teams with Vietnamese criteria for CSIRTs.
- Develop cooperation with other CERTs in the world
- Project of Children Protection on Cyberspace.
- Improve Anti-spam.
- Continue to collaborate to exchange lessons and experiences on the development of legislation, laws, and

information on developing an online social media management system among National CERT, international organizations, and related sectors in the field of cybersecurity.

7. Conclusion

The mission of VNCERT/CC is to assist Vietnam organizations and internet users in implementing proactive measures to reduce the risks of security incidents and to assist them in responding to such incidents when they occur.

Besides, VNCERT/CC is planning to provide more services to local communities and develop cooperation with all the incident response teams in the world to contribute to greater global cyber security.

VNCERT/CC is also interested in and looking to connect with organizations on child protection issues online.

Activity Reports from APCERT Partners

CERT-GIB

Computer Emergency Response Team Group-IB

1. Highlights of 2023

1.1. Summary

- The number of phishing and scam resources detected by CERT-GIB increased by 3 and 8% percent, respectively.
- CERT-GIB responded to 114,637 phishing resources and 343,379 scam resources. 99% of violations were successfully solved.
- Released two comprehensive annual reports on threat landscapes and more than 20 other analytical and technical reports.
- Group-IB took part in a global INTERPOL-led law enforcement operation named Synergia, aimed at combating the surge of phishing, banking malware, and ransomware attacks in more than 50 countries, and in the cross-border cybercrime fighting operation Digital Skimming Action, coordinated by Europol, and featuring the European Union Agency for Cybersecurity (ENISA), law enforcement authorities from 17 countries, and other private sector partners.
- Organized 4 events and participated in 22 industry & third-party events in the APAC region.
- Group-IB's flagship Unified Risk Platform (URP) has been revamped to improve threat detection efficacy, enhance intelligence gathering, and fortify AI capabilities across its modules.

1.2 Awards

- Singapore Police Force Alliance of Public Private Cybercrime Stakeholders (APPACT) Appreciation Award 2023
- 6th Regulation Asia Awards for Excellence 2023: Anti-Fraud Project of the Year
- Recognized by Gartner in the 2023 Market Guide for Digital Forensics and Incident Response Services as a representative vendor for incident response services
- Frost & Sullivan’s 2023 Competitive Strategy Leadership Award
- Frost & Sullivan recognized Fraud Protection as the most complete anti-fraud solution currently on the market
- Group-IB’s Anastasia Tikhonova, Jennifer Soh and Vesta Matveeva named among Top 30 Women in Security ASEAN Region 2023

2. About the Organization

2.1. Introduction

CERT-GIB 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.

In 2023, CERT-GIB team merged with the Group-IB's Digital Risk Protection (DRP) team, which was engaged in the detection and mitigation of external web violations, such as scam, brand abuse, VIP impersonations, and data leakages. The merger made it possible to utilize the rich experience of the DRP team, strengthen the competence of both teams and significantly expand the landscape of threats that are covered by CERT-GIB.

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).

2.2. Establishment

CERT-GIB was established on March 10, 2011.

2.3. Resources

2.3.1. Digital Crime Resistance Centers

Group-IB has a global presence in 60 countries with 5 Unique Digital Crime Resistance Centers in the Asia-Pacific, Middle East and Africa, Europe, and Central Asia, and this network is set to expand further over the coming years.

DCRCs operate independently of one another and are staffed with highly experienced researchers who are tasked with investigating cybercrimes, responding to incidents, monitoring local threats, and assessing regional trends to support its client base and growing partner network.

More than 50 analysts of CERT-GIB are also part of DCRCs. It allows CERT-GIB to analyze local threat landscapes, predict cyber risks, promptly respond to threats, and share adversary-centric intelligence with other regions non-stop.

Within DCRCs CERT-GIB works closely with other Group-IB's teams, including Digital Risk Protection, Digital Forensics Laboratory, Fraud Protection, Attack Surface Management, Threat Intelligence & Attribution, and Investigations.

2.3.2. Proprietary technology

Group-IB Threat Hunting Framework allows CERT-GIB experts to manage incidents effectively and efficiently and reduce time spent on incident analysis. CERT-GIB operations are enhanced with data collected by Group-IB Threat Intelligence & Attribution and Digital Risk Protection platform.

Combined, Group-IB technological capabilities include:

- Internal and external threat hunting
- Graph analysis
- Data storage
- Correlation and attribution
- Event analysis

2.3.3. Expertise

Group-IB has provided more than 1,300 successful investigations and has spent over 70,000 hours responding to incidents of various complexity all over the globe. Group-IB has conducted extensive research on APT groups, ransomware operators, and general cybersecurity trends across all major industries. Group-IB's combined technological capabilities and human intelligence means the company is always aware of cyber criminals' latest tools, TTPs, and movements. CERT-GIB is an integral part of these activities.

2.4. Constituency

CERT-GIB provides its services to protect more than 400 corporate brands. It also cooperates with government organizations and law enforcement agencies on issues related to cyber attacks and protecting Internet users from cyber crimes.

3. Activities & Operations in 2023

3.1. Anti-Phishing and Anti-Scam Statistics

In 2023, the number of phishing and scam resources detected by CERT-GIB increased by 3 and 8% percent, respectively. At the same time, the top 5 countries in the APAC region attacked by phishing were Indonesia (26,4%), India (16,2%), Singapore (15,6%), Australia (12,9%), Vietnam (12%). Among the TLDs which criminals preferred to register phishing domains, the top 5 were .com (42,1%), .id (9,6%), .app (9,4%), .net (2,8%), .top (2,2%).

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 2023, CERT-GIB responded to 114,637 phishing resources and 343,379 scam resources. 99% of violations were successfully solved.

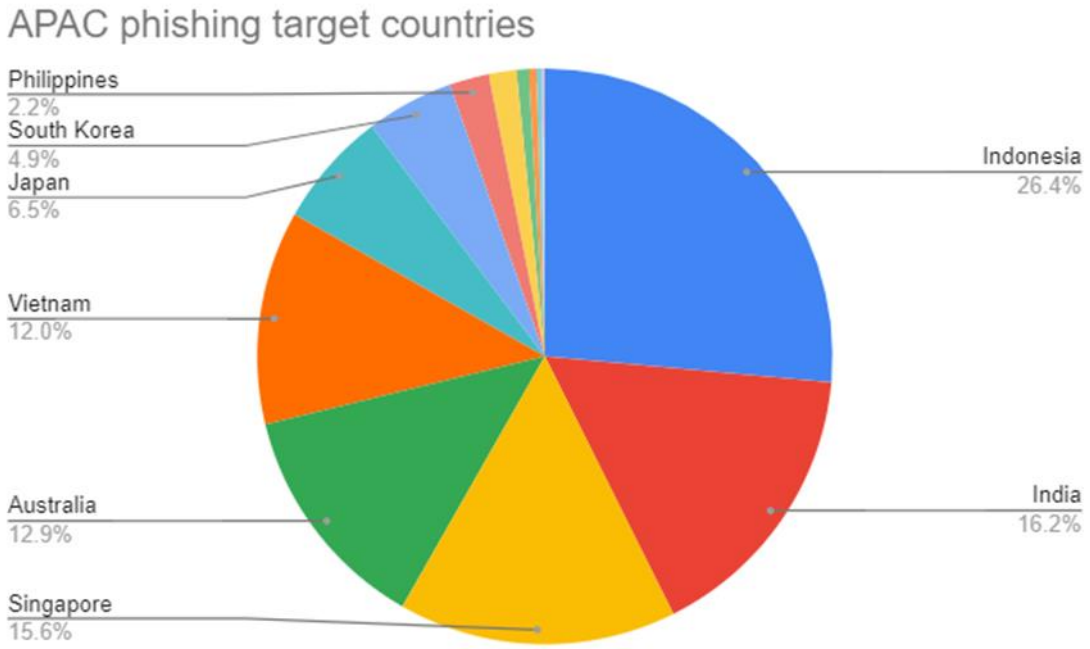


Fig. 1. Phishing resources, breakdown by target countries

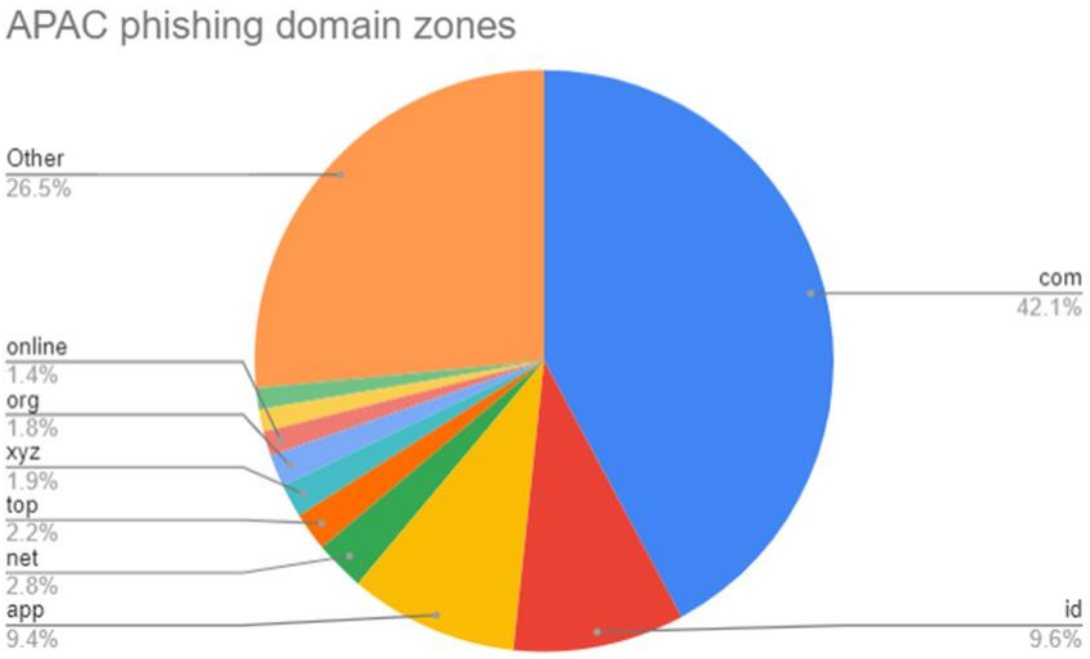


Fig. 2. Phishing resources, breakdown by top domain zones

3.2. Special Operations

- Group-IB took part in a global INTERPOL-led law enforcement operation named Synergia, aimed at combating the surge of phishing, banking malware, and ransomware attacks in more than 50 countries. As part of the global operation, the Group-IB team identified more than 500 IP addresses hosting phishing resources and over 1,900 IP addresses associated with ransomware, Trojans, and banking malware operations. This information was then shared with the task force for further coordinated action. The operation, which ran from September to November 2023, resulted in the apprehension of 31 individuals, the identification of an additional 70 suspects, and the takedown of hundreds of command-and-control (C2) servers.
- Group-IB took part in the cross-border cybercrime fighting operation Digital Skimming Action, coordinated by Europol, and featuring the European Union Agency for Cybersecurity (ENISA), law enforcement authorities from 17 countries, and other private sector partners. This helped Europol and its partners to detect and issue notifications to 443 online merchants in total with whom customers' credit or payment card data had been potentially stolen.

3.3. Events

3.3.1. Events and Trainings organized by Group-IB

- 'Respond Like a Rockstar' DFIR Webinar
- CXO Roundtable - Bengaluru, India
- Cybersecurity Day & CTF Battle Royale - Hanoi, Vietnam
- 20th Anniversary CTF
- Blue Team Analyst for DTI (Thailand)
- Incident Responder for DTI (Thailand)

Additionally, Group-IB has special training programs for commercial customers and government organizations which include:

- Complex 4-months training on cyber security for SOC analysts
- Threat Intelligence Analyst
- Threat Hunter
- Windows DFIR Analyst
- Anti-Fraud Analyst

3.3.2 Industry & Third-Party Events Involvement

- Australian Cyber Conference 2023 - Canberra
- Misoft Partner Connect 2023
- Pacific Tech Singapore Product Launch 2023
- Pacific Tech Indonesia Solutions Day 2023

- Ngee Ann Polytechnic's Industry Partners Appreciation
- MOU Signing with Thai Defence Technology Institute (DTI)
- VMware Security Connect - Malaysia
- Pacific Tech 'Defense of the Era' - Kuala Lumpur, Malaysia
- 'Power of P' Event by NAT Absolute Technologies - Bangkok, Thailand
- GBG User Group Meeting - Bangkok, Thailand
- ATxSG (Asia Tech & Singapore) 2023
- TechSauce Global Summit 2023 - Bangkok, Thailand
- Smart Banking Summit - Hanoi, Vietnam
- Cyber Security Agency (CSA) Innovation Day 2023
- WCIT 2023 - Sarawak, Malaysia
- INTERPOL Global Cybercrime Conference 2023
- GovWare 2023 - Singapore
- Thailand Cyber Top Talent 2023
- nForce Secure Annual Expo 2023 - Bangkok, Thailand
- Merchant Risk Council - Singapore
- Employee Provident Fund (EPF) Cybersecurity Day 2023
- Singapore Police Force International Economic Crime Course (IECC) 2023

3.4. Publications

In 2023, Group-IB actively participated in cyber threat research, including studies of new phishing and scam schemes, malware and ransomware, APT groups, and their attack vectors. The results of these studies were presented in the form of analytical and technical reports, press releases, blogs, and other publications.

In particular, two comprehensive annual reports were released:

- Hi-Tech Crime Trends 2022/2023 illustrating the actual threat landscape, specifying valuable data, and sharing major insights.
- Digital Risk Trends 2023 provides a detailed analysis of trends in scams and phishing across different industries and regions.

Threat reports that have generated significant industry interest include:

- W3LL done: uncovering hidden phishing ecosystem driving BEC attacks
- Beyond OWASP Top 10: The ultimate guide to web application security (2023 and onwards)
- Old Snake, New Skin: Analysis of SideWinder APT activity in 2021
- Ace in the Hole: exposing GambleForce, an SQL injection gang
- Curse of the Krasue: New Linux Remote Access Trojan targets Thailand
- Ransomware manager: Investigation into farnetwork, a threat actor linked to five strains of ransomware
- Let's dig deeper: dissecting the new Android Trojan GoldDigger with Group-IB Fraud Matrix

- Dusting for fingerprints: ShadowSyndicate, a new RaaS player?
- From Rags to Riches: The illusion of quick wealth in investment scams
- Stealing the extra mile: How fraudsters target global airlines in air miles and customer service scams
- New hierarchy, heightened threat: Classiscam's sustained global campaign
- Traders' Dollars in Danger: CVE-2023-38831 zero-Day vulnerability in WinRAR exploited by cybercriminals to target traders
- Breaking down Gigabud banking malware with Group-IB Fraud Matrix
- Demystifying Mysterious Team Bangladesh
- Busting CryptosLabs: a scam ring targeting French speakers for millions
- Dark Pink. Episode 2
- Dark Pink
- The distinctive rattle of APT SideWinder
- You've been kept in the dark (web): exposing Qilin's RaaS program
- Tech (non)support: Scammers pose as Meta in Facebook account grab ploy
- Investigation into PostalFurious: a Chinese-speaking phishing gang targeting Singapore and Australia
- SimpleHarm: Tracking MuddyWater's infrastructure
- The old way: BabLock, new ransomware quietly cruising around Europe, Middle East, and Asia
- 36gate: supply chain attack
- Venomous vacancies: Job seekers across MEA hit by sting in scammers' tail
- Bleak outlook: Mitigating CVE-2023-23397
- Package deal: Malware bundles causing disruption and damage across EMEA
- Nice Try Tonto Team

3.5. Technology

Group-IB's flagship Unified Risk Platform (URP) has been revamped to improve threat detection efficacy, enhance intelligence gathering, and fortify AI capabilities across its modules.

- Fraud Protection module has been upgraded with a whole new Fraud Matrix framework. Based on the MITRE ATT&CK® model, Group-IB's Fraud Matrix allows users to deconstruct and catalog fraud schemes, regardless of their complexity and number of stages, to better understand TTPs leveraged by fraudsters. Precise fraud categorization is achieved through the enrichment of another brand-new feature, Fraud Intelligence.
- Digital Risk Protection module has been empowered with AI algorithms to improve the detection efficiency of phishing and scam websites that impersonate legitimate companies. An enhanced AI-infused engine helps in the automated creation of signatures to speed up the detection of typosquatting and illicit use of brand logos. The implementation of the large-scale computer vision system has improved the detection rate of unauthorized brand logo usage by 40%, while, at the same time, implementing a three-fold decrease in the neural network's training time.

- Smart Abuse Tool has been released. It is a managed takedown assistant that enables CERT-GIB analysts, customers, and managed security service providers (MSSP) partners to eliminate IP violations seamlessly and independently.
- Threat Intelligence module has been supercharged to improve the efficiency of the company's patented Graph Network Analysis tool. Group-IB has further expanded its intelligence-gathering network by implementing real-time cybersecurity news monitoring and IOCs filtering and extraction capability. The module now offers extended coverage of scanning hosts, VPN hosts, DDoS, and augmented phishing attacks.
- MXDR (Managed Extended Detection & Response) has been extended its functionality to Linux and MacOS systems as well as remediation functionality for Windows EDR. Malware detonation has undergone a series of AI-driven optimizations to enhance the detection of "malware-free" attacks.
- Attack Surface Management's capabilities has been extended to cover typosquatting detection. Another new feature is the introduction of Group-IB's live Telegram bot for notification alerts and remediation guidance.

4. Collaboration with APCERT members/partners

Key Partnerships:

- Extended strategic partnership with the International Criminal Police Organization (INTERPOL).
- Became a member of the newly formed Cyber Security Action Task Force (CSATF), led by the Hong Kong Police Force. The task force marks the significant collaboration between prominent cybersecurity companies, public service providers, and law enforcement agencies to strengthen the exchange of critical cyber threat intelligence, to prevent attacks in the early stages, and to facilitate the investigations of digital crimes.
- Signed a Memorandum of Understanding (MoU) with AFRIPOL. Group-IB will share its technological advancements and specialized knowledge in cyber investigations, reverse engineering, and incident management with AFRIPOL's personnel throughout the African member states, as the organization intensifies its efforts to address cybercrime continent-wide.
- Signed a memorandum of understanding with the United Arab Emirates Cyber Security Council.
- Signed a memorandum of understanding with the Defence Technology Institute (DTI), a government agency under the supervision of the Minister of Defence of Thailand.

5. Planned activities in 2024

5.1. Future plans

- Opening of Digital Crime Resistance Centers in new regions and countries.
- Strengthening CERT-GIB through deepening cooperation with the Threat Intelligence team.
- Further improvement and implementation of AI-based solutions in detection, automated collection of evidence, as well as response.

- Establishing new partnerships with government and law enforcement agencies in different countries.

5.2. Future events

- Hong Kong Police Force Cyber Command Course 2024
- Hong Kong Fraud Protection C-Level Roundtable
- National Cyber Security Agency of Thailand (NCSA) Training
- OT-ISAC (Operational Technology Information Sharing & Analysis Center) TTX
- Seamless Asia 2024 - Singapore
- Pacific Tech Solutions Day 2024 - Jakarta, Indonesia
- Cambodia Launch with Pacific Tech - Phnom Penh
- Laos Launch - Vientiane
- Statebank Event - Ho Chi Min City, Vietnam
- Singapore Fraud Protection C-Level Roundtable
- CyberSec Malaysia
- Regulation Asia Fraud & Financial Crime Event 2024 - Singapore
- IndoSec 2024 - Jakarta, Indonesia
- TechSauce Global Summit 2024 - Bangkok, Thailand
- Partner Universe
- GovWare 2024 - Singapore
- Cybersecurity Day 2024 - Hanoi, Vietnam
- Australian Cyber Conference 2024 - Melbourne

FIRST

Forum of Incident Response and Security Teams

1. About the Organization:

FIRST aspires to bring together incident response and security teams from every country across the world to ensure a safe internet for all. Founded in 1990, the Forum of Incident Response and Security Teams (FIRST) consists of incident response teams and practitioners from over 700 corporations, government bodies, universities, and other institutions across over 100 countries in the Americas, Asia, Europe, Africa, and Oceania.

Apart from the trust network that FIRST forms in the global incident response community, FIRST also provides value added services. Some of these include:

- technical colloquia for security experts
- hands-on classes
- annual incident response conference
- publications and web services
- special interest groups
- community and capacity building

2. Activities and Operations in 2023:

- Physical attendance at FIRSTCON23 in Montreal - 795
- 679 teams and 127 liaison members

3. Collaboration with APCERT members/partners:

FIRST has been an APCERT Strategic Partner since 2021 and enjoys strong shared membership with APCERT and mutual engagement across our events and activities. Select recent collaboration with APCERT members and partners has included:

- In February 2023, **APNIC** hosted a FIRST Technical Colloquium as part of the APRICOT 2023 Conference in Kyoto, Japan.

- With the support of the PaCSON Secretariat, hosted within the **ACSC**, and **CERT Vanuatu**, FIRST organized a Regional Symposium for the Pacific in Port Vila, Vanuatu. The event took place from 20 to 22 September and included presentations and trainings from several APCERT members. The event was kindly supported by PaCSON, the Government of Vanuatu, Office of the Government CIO, **CERT VU**, the U.S. State Department, and the APNIC Foundation. More information is available at: https://www.first.org/events/symposium/pacific2023/
- In 2023, FIRST also became a partner of PaCSON (Pacific Cyber Security Operational Network).
- The FIRST has engaged with **CERT-PH**, **CERT Tonga**, **CERT VU**, and **VNCERT/CC** as participants in the FIRST Suguru Yamaguchi Fellowship Program in 2023.
- Throughout 2023, FIRST has worked closely with **JPCERT/CC** as the local host for the FIRST Annual Conference 2024, planned for Fukuoka, Japan from 9 to 14 June 2024. More information is available at: https://www.first.org/conference/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: +82-2-3495-9431
- Fax: +82-2-3495-9399
- Email: cert@fsec.or.kr
- Website: https://www.fsec.or.kr/en

2. Activities & Operations

2.1 Summary of major activities

2.1.1 Operate a financial threat response intelligence platform

FSI-CERT built the Cyber Threat Intelligence platform using open source in October 2022. The platform systematically stores and manages cyber incidents and malware reports analyzed by FSI-CERT itself.

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 bug bounty program to discover unprecedented security vulnerabilities and strengthen preemptive prevention activities against cyber infringement threats. The program was broadened to cover mobile apps of financial companies and internet banking security software in addition to websites and HTS.

2.1.4 Operation of a next-generation financial ISAC system

The next-generation Financial Information Sharing and Analysis Center(ISAC) system operated by FSI-CERT leads security control technology by advancing the application of artificial intelligence(AI), producing and providing threat intelligence, and establishing private clouds.

2.1.5 Information sharing of voice phishing threats

FSI-CERT established a voice phishing fraud information sharing system using information sharing APIs between the financial, communication, security related institutes to prevent and respond to advancing voice phishing threats.

2.1.6 Operation of an integrated analysis system for financial mobile app

To prevent financial app-related security incidents and ensure a safe user environment, FSI-CERT developed and operated a system which classifies and manages mobile security function modules to analyze security threats and vulnerabilities.

2.2 Incident Response

2.2.1 Incident analysis and response

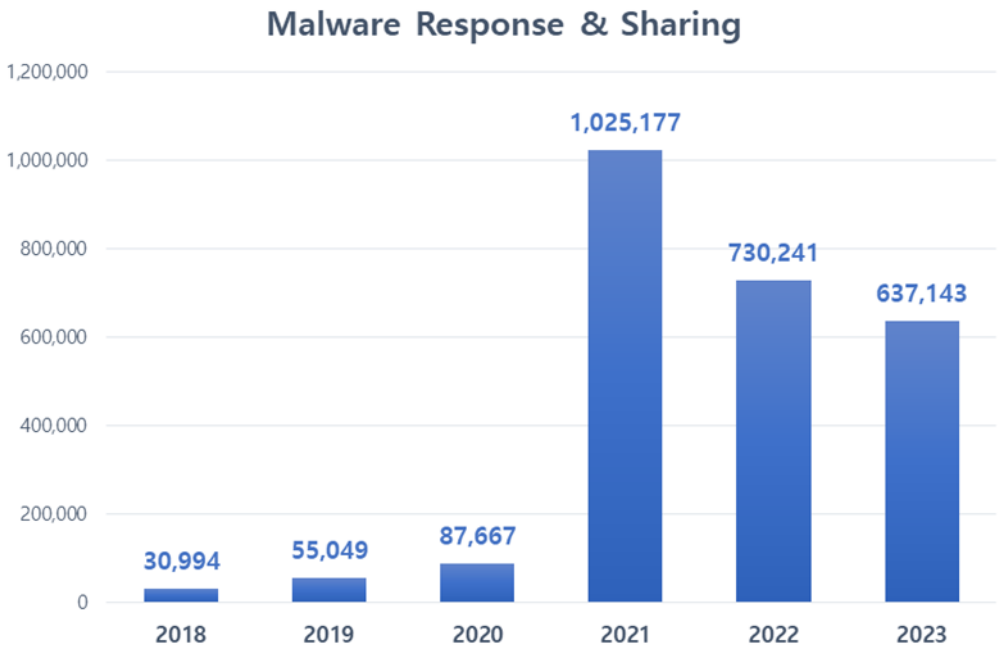
When cyber attacks occur in financial companies, FSI-CERT gathers digital evidence and utilizes digital forensics on scene to analyze the cause of the incident. FSI-CERT also establishes measures to prevent damage propagation and enhance financial companies' cyber threat response capabilities by conducting incident prevention digital forensic analysis on PCs that are likely to be targeted.

[Figure 1] Incident Response Process

2.2.2 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.

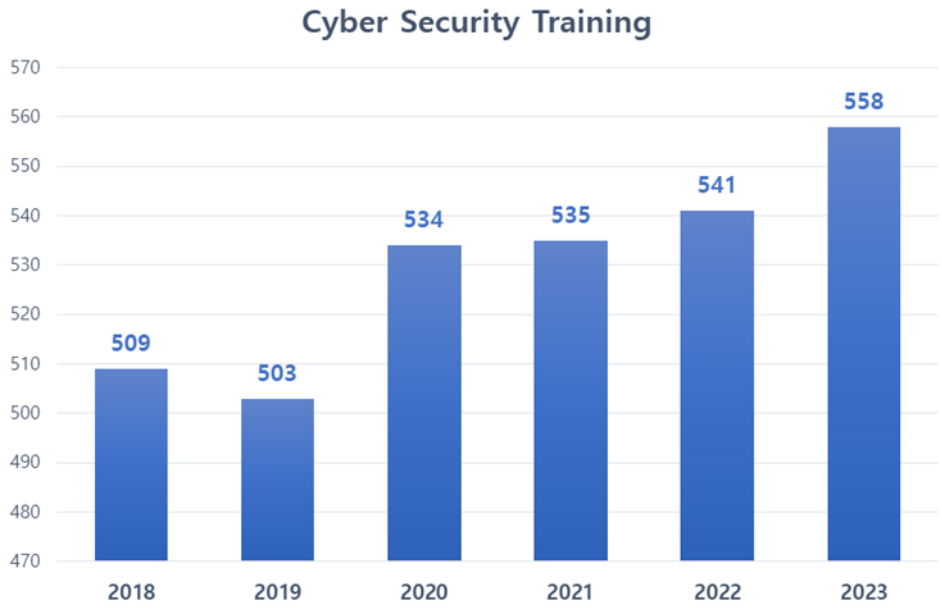
Furthermore, FSI-CERT provided correlation analysis information by systematically managing a multitude of collected/analyzed results of malicious codes.



[Figure 2] Total Malware Response and Sharing Cases

2.2.3 Simulation training on cyber security incidents

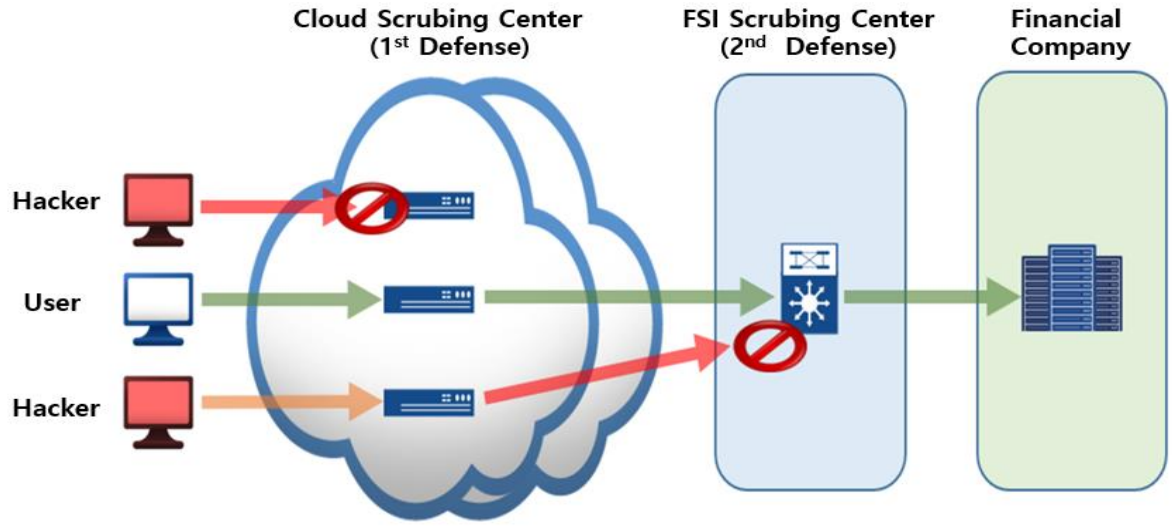
FSI-CERT conducted simulation training on cyber security incidents for financial companies. Through trainings on various types of cyber attacks such as DDoS attacks, server hacking, and APT attacks, FSI-CERT inspected the incident response system of financial companies and contributed to improving security awareness.



[Figure 3] Total Cyber Security Training Sessions

2.2.4 Operation of DDoS Attack Emergency Response Center

When large-scale DDoS attacks to which financial companies cannot respond on their own occur, FSI-CERT 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.

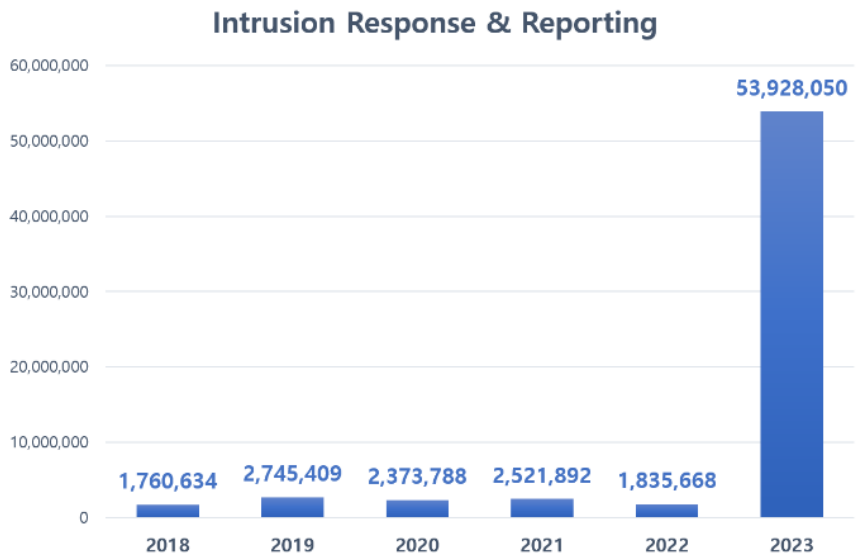


[Figure 4] DDoS Attack Response Process

2.3 Operation of an integrated security monitoring system

FSI-CERT operates a next-generation integrated security control system based on AI, Big data and Cloud, and has advanced control technologies such as AI-based threat intelligence and financial cyber threat hunting to lead the intelligent security control and real-time sharing system for cyber threats in the financial sector in 2023.

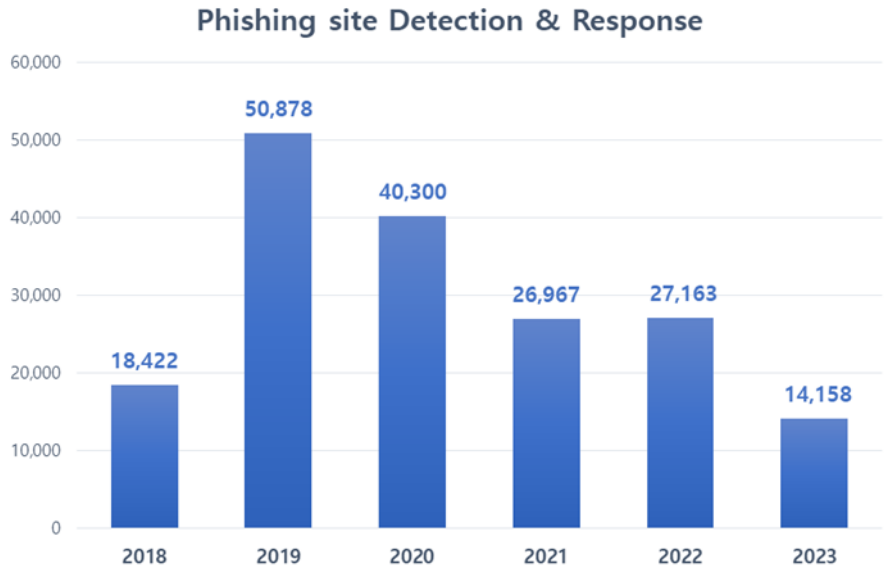
**Increased number of responses compared to 2022, due to introduction of next-generation financial security control system*



[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.

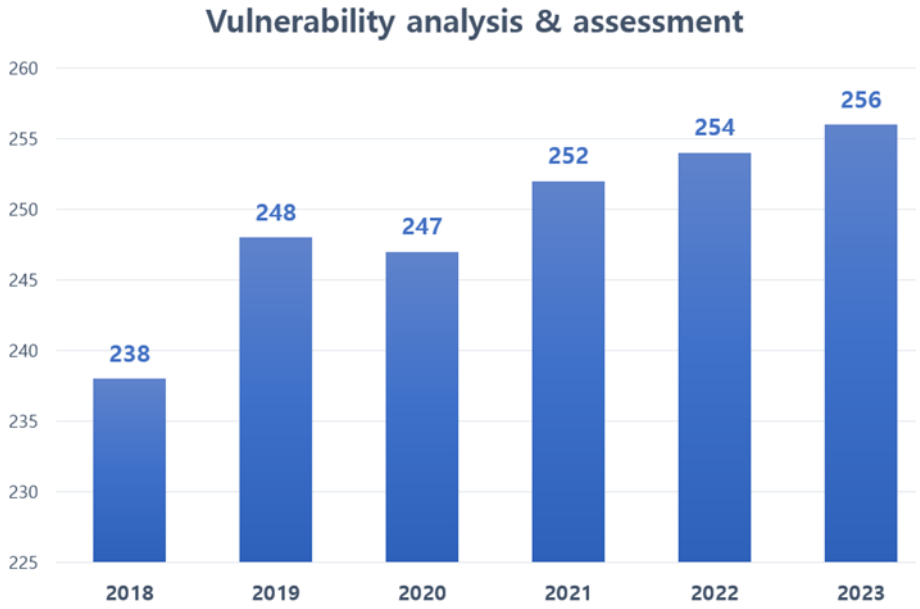
In addition, by signing MOU with major specialized organizations (police, telecommunication companies, security companies) on voice phishing response, we strengthened our cooperation system to eradicate electronic financial fraud such as voice phishing.



[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.

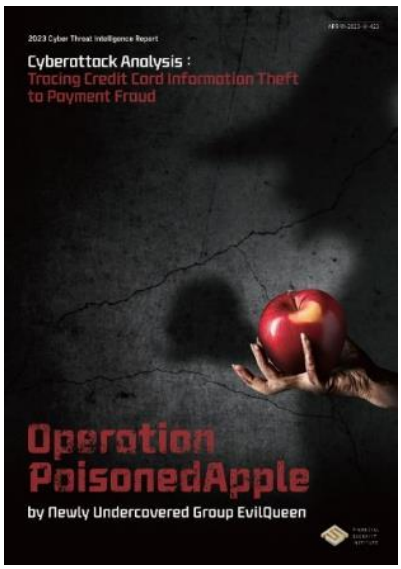


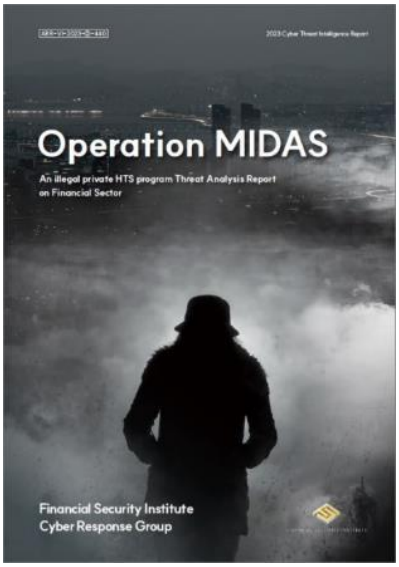
[Figure 7] Total Vulnerability Analyses and Assessments

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.





Tracing credit card information theft to payment fraud

In September and November 2022, FSI-CERT received reports that phishing web page disguised as payment web page was inserted into the websites of different shopping malls, and through a program developed by ourselves, we investigated about 50 online shopping malls with phishing web pages.

In the report, we analyzed the entire attack process of stealing credit card information through phishing web page and cashing out after fraudulent payment and named the attack group and operation as “EvilQueen” and “PoisonedApple” respectively.

- The report will be released online following the conclusion of the related investigation.

An illegal private HTS program threat analysis report on financial sector

This report profiles the organizations that supply and operate illegal private HTS programs and provides a detailed analysis of their fraudulent schemes, including user recruitment, program dissemination, and money extortion.

- The report will be released online following the conclusion of the related investigation.

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

5. Conferences and Presentations

- 2023 Fall Conference, hosted by F-ISAC(Japan, November)
- Cyber Threat Trends and Incidents in South Korea's Financial Sector

6. Collaboration with APCERT

At the 2020 APCERT online training session, FSI-CERT presented on the topic “ATM Cyber Attack.” FSI-CERT looks forward to participating continuously in various seminars of APCERT to share research and information of the financial security sector.

7. Conclusion

Cyber security threats such as the dark web, cloud security threats, COVID-19, and cyber warfare are increasing day by day. Accordingly, FSI-CERT will continue to enhance cyber security systems—such as the financial ISAC(Information Sharing and Analysis Center), digital forensics, malware analysis, etc.—to combat such increasingly developing security threats. In addition, FSI-CERT will follow by its mission of providing a safe environment for the financial industry by incorporating new technologies (ex. big data, AI, etc.) into cyber security.

KZ-CERT

Kazakhstan Computer Emergency Response Team

1. Introduction

National Computer Emergency Response Team (KZ-CERT) is a single center for national information systems users and Kazakhstani Internet segment providing collection and analysis of cyber incidents report as well as consultative and technical assistance to Kazakhstani users in prevention of cyberthreats.

1.1 Establishment

KZ-CERT was established in 2011 on the basis of republican state enterprise with the right of economic management "Center for Technical Support and Analysis in Telecommunications".
On January 28th, 2013, the government of Kazakhstan adopted a decree to rename the republican state enterprise with the right of economic management "Center for Technical Support and Analysis in Telecommunications" as the republican state enterprise with the right of economic management "State Technical Service". Eventually, in 2020, the RSE with REM "State Technical Service" had undergone its final reformation into the joint-stock company "State Technical Service" (hereinafter – STS JSC) by another governmental decree.
Apart from that, in 2017, there was also an establishment of the National Coordination Center for Information Security (NCCIS) now which combines the operation of both KZ-CERT and Government SOC.

1.2 Resources

NCCIS, which is a structural subdivision of STS JSC, currently employs more than 60 people of various profiles. KZ-CERT Team, in turn, as a functioning unit of NCCIS, comprises around 20 employees.

2. Activities and Operation over 2023

KZ-CERT is responsible for detecting, processing, and neutralizing the following cybersecurity incidents:

- brute-force attacks;
- botnets;
- malware;
- phishing, spam attacks;
- vulnerability exploitation;
- unauthorized access and modification of network infrastructure and information resource data.

2.1 Incident Handling Report

In 2023, KZ-CERT has handled over 34 thousand cybersecurity incidents. The majority of incidents are associated with the creation and distribution of malware. Figure 1 shows a more detailed informarion on their types.

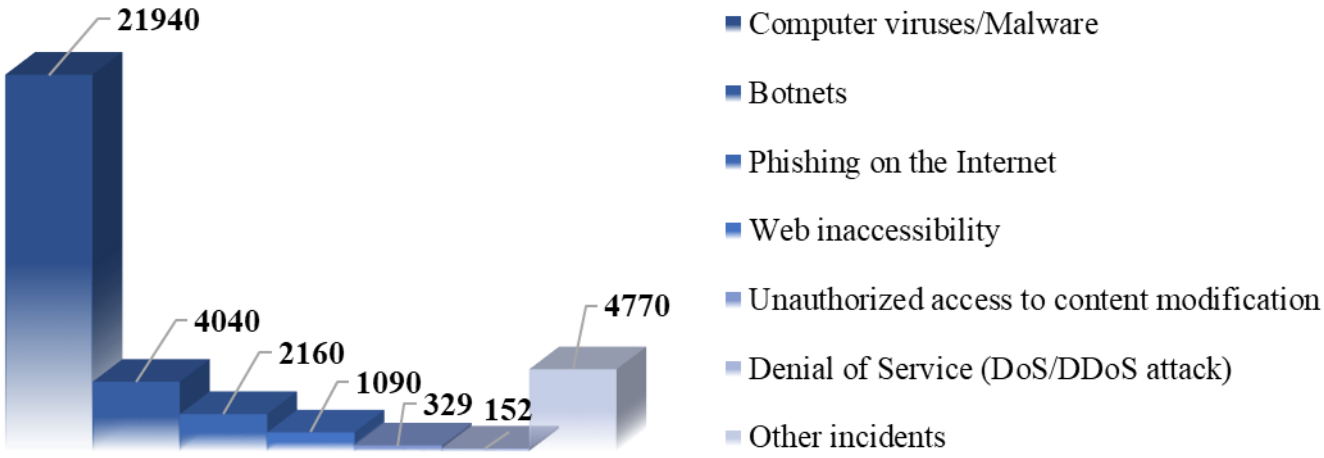


Figure 1. Types of the incidents handled by KZ-CERT over 2023.

2.2 2023 Cybersecurity Incident Case Example

In 2023, KZ-CERT Team received an appeal from a Kazakhstani government agency with the request to provide assistance in investigating a cybersecurity incident.

During the examination of the affected laptop's disk image, several malicious software types were detected inside – a botnet, a Trojan, and the CrazyCryp ransomware.

Malicious files were found in the "Workpace¥metadata¥FluidVoid¥bin¥Debug¥Рабочий¥готовые" directory as well.

№	File name	SHA1 base32
1	\FluidVoid\bin\Debug\Build0_2.ex_	622RHQGQC3PEOTJV5J7TKIDQTW2GFXRO
2	\FluidVoid\FluidVoid\bin\Debug\Build1_2.ex_	HMX7VHMIIEEAKSMWIUJVJH74ICV67XII
3	\FluidVoid\FluidVoid\bin\Debug\Build0_1.ex_	U4YILJVTG3TRNABZGEHEXSU6N2IU4HAJ
4	\FluidVoid\FluidVoid\bin\Debug\Build0_3.ex_	JEFJSVL76PZODZRB6MLYYNAAOUZREKEJ
5	\FluidVoid\FluidVoid\bin\Debug\Build4_3.ex_	AFKGBUKDMOTFLYYZN7HQU7SOYEV26365
6	\FluidVoid\FluidVoid\bin\Debug\Build4_1.exe_	WBF4YCELRKJJGPQQ3AGHGVXDRAN3RIAA
7	\FluidVoid\FluidVoid\bin\Debug\Build1_1.ex_	WQD2P5IBZ4Z5CWZKRDRW23ANMRPYASHN
8	\FluidVoid\FluidVoid\bin\Debug\Build1_3.ex_	2YQBHSSYLBLYTNINNITQO2AK6PPOAEQU
9	\FluidVoid\FluidVoid\bin\Debug\154.exe	Y52J4TNFQFV7GJ4SQGW4EGTYNYUOOROK
10	\FluidVoid\FluidVoid\bin\Debug\Build4_2.ex_	R5JHGHRJCNCXO45JOJCSTUENL5KKCFMC
11	\FluidVoid\FluidVoid\bin\Debug\llvann49.ex_	YVGI2MNXPXXPW2SOAPWOYYJ3OX3VYIFL
12	\FluidVoid\FluidVoid\bin\Debug\OvKSMx860.dll	332BIF6PBV34BDG5NTT34ORKJAFK74ZB
13	\FluidVoid\FluidVoid\bin\Debug\p2BBDVx861.dll	73DNKK5G2KZRBVOSDOKRPDCV76DLXODD
14	\FluidVoid\FluidVoid\bin\Debug\QHT4XDx861.dll	QOU2LFK7S4ZCWCBL4SWOXDJQ2SSF4FGE
15	\FluidVoid\FluidVoid\bin\Debug\Qa0mruyx860.dll	IMFHNRMFWGYSOOUZSIF743HAVY7UBBWT
16	\FluidVoid\FluidVoid\bin\Debug\Osiris_auto2.ex_	2JCU5NPBR7MWCXVDXRSPRWLXUTRBNWUC
17	\FluidVoid\FluidVoid\bin\Debug\t4me9m863.dll	77DLHTQBPL6XVDJUBVKNL4RISNNVJCBD
18	FluidVoid\FluidVoid\bin\Debug\vidar_business10.ex_	YJFTUKSPHBLHUJADL4TZFLSBNK2MKZKD
19	\FluidVoid\FluidVoid\bin\Debug\Cuddling36.ex_	ZVTSB7NJHSEEZZGQM4YUTQ35UOKDWSBV

Table 1. Malicious Files.

KZ-CERT carried out the procedures of localization and neutralization of the malware software and prepared recommendations on preventing similar threats in future.

2.3 KZ-CERT Statistics on International Alert Exchange

In 2023, KZ-CERT has sent 1859 alerts to foreign organizations and partners of 48 countries and received 771 alerts from foreign organizations of 31 countries.

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

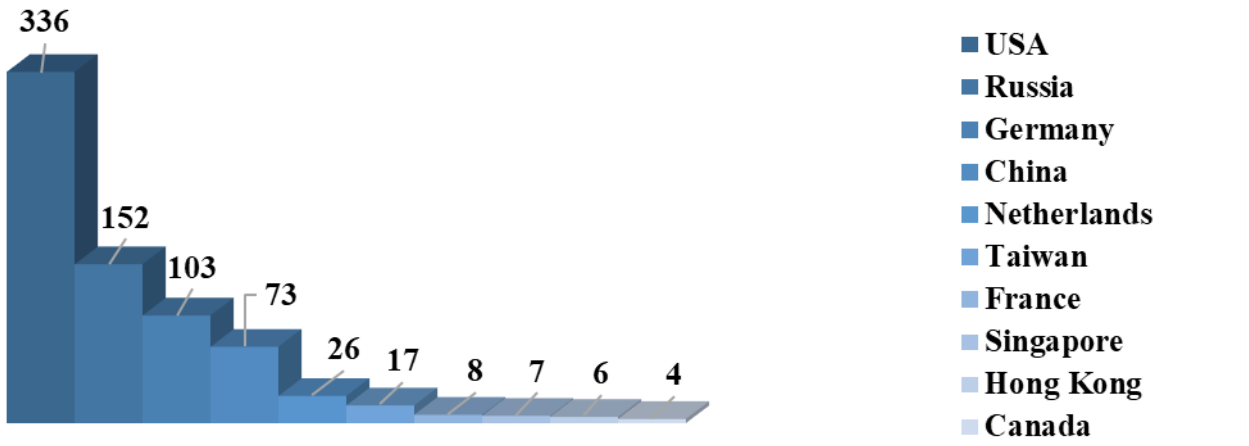


Figure 2. Incoming foreign alert statistics for 2023

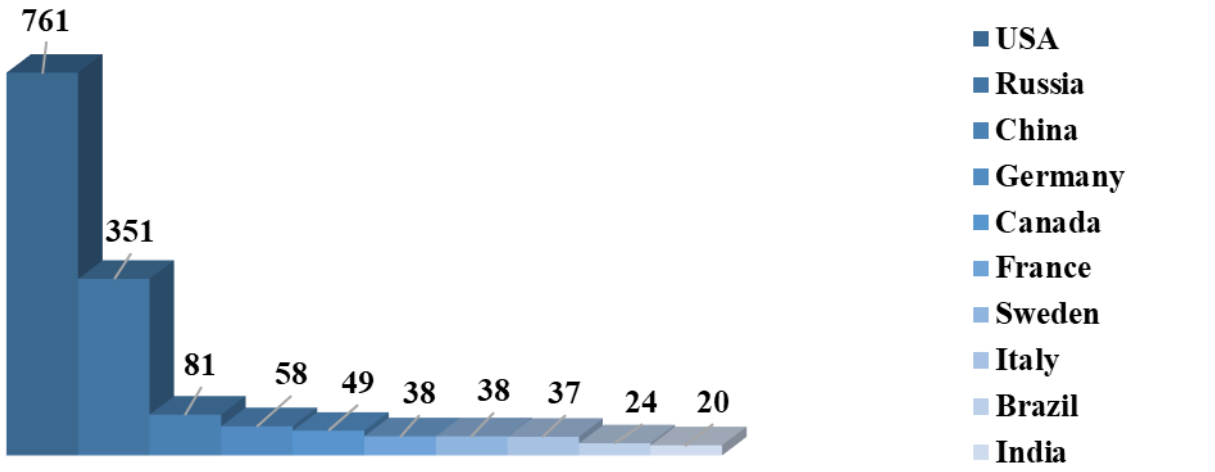


Figure 3. Outcoming foreign alert statistics for 2023

2.4 Publications

We consistently inform our citizens on the detected information security incidents, potential and perceived computer security threats, as well as on the necessity of taking measures to eliminate, mitigate, and prevent such threats. The official website of KZ-CERT (cert.gov.kz), along with the newsfeed, features regularly published articles with recommendations on cyberhygiene and cybersecurity.

All materials are usually provided in three languages – Kazakh, English, and Russian.

For instance, you can find the following articles published in 2023:

- Microsoft: Exchange Server 2013 Support Service will end in 90 days (cert.gov.kz/news/13/2297)
- Recommendations for companies using Geoserver Software (cert.gov.kz/news/13/2356)
- Over 17 thousand routers in Kazakhstan are potentially vulnerable to Mikrotik RouterOS Vulnerability (cert.gov.kz/news/13/2413)
- Recommendations for protecting WhatsApp and Instagram accounts with 2FA (cert.gov.kz/news/13/2455)

- Technical details: Analysis of SSL/TLS cipher suites in the national top-level domain zone .kz (cert.gov.kz/news/13/2460)
- Important information for 1C-Bitrix CMS users (cert.gov.kz/news/13/2465)
- Vulnerability in all versions of Exim – no patch yet (cert.gov.kz/news/13/2471)
- Cisco vulnerability (cert.gov.kz/news/13/2475)
- Recommendations on protecting Telegram accounts (cert.gov.kz/news/13/2480)
- Recommendations for the users of Citrix products (cert.gov.kz/news/13/2491)
- How to be safe during Black Friday: KZ-CERT recommendations (available in Russian) (cert.gov.kz/news/13/2524)
- Recommendations for the users of Microsoft Office Professional Plus 2019 Excel (available in Russian) (cert.gov.kz/news/13/2538)
- Frequent fraudulent cases on WhatsApp (available in Russian) (cert.gov.kz/news/13/2543)
- Information for the users of PostgreSQL (cert.gov.kz/news/11/2522)
- Two-factor authentication is an extra layer of security (cert.gov.kz/news/11/2457)

2.5 Awareness-raising activities

In 2023, KZ-CERT Team members organized lectures, webinars, workshops, and cybersecurity trainings for the government agencies, quasi-government organizations and various companies of Kazakhstan. The program involved presentations on the following topics:

- “Main aspects of information security”;
- “Cyber Hygiene basics”;
- “The tricks of cyber fraudsters. How not to get caught on their hook?”;
- “Cyber attacks trends. International cases”.

Apart from that, KZ-CERT Team members also contribute to raising awareness on cybersecurity through the national television. Accordingly, several appearances were made with the following presentations:

- “Combating fraud on the Internet”
- “Current information security threats”
- “Cyber Hygiene”

As part of the ongoing activities to cover the cybersecurity issues in our country, dedicated meetings involving the government agencies of Kazakhstan are also held regularly to discuss matters related to strengthening the level of information security in these organizations that play a significant role in domestic policy.

3. International Events and Cooperation

KZ-CERT recognizes the importance of cooperation with teams and organizations that have similar competency and constituency. Therefore, our Team is always open to invitations and opportunities to participate in various events dedicated to the information security matters.

International cooperation plays a big role in establishing communications with the global IT and cybersecurity communities, circulating important information, as well as maintaining the status of a national computer emergency response team on the global stage through the participation in different international information security conferences and other events.

3.1 Cyber Drills and Trainings

OSCE Sub-regional training event on cyber/ICT security

In May 2023, KZ-CERT Team members participated in Sub-regional trainings on cybersecurity and information and communication technologies security for representatives of Central Asian countries and Mongolia. The event was organized jointly with the Organization for Security and Co-operation in Europe (OSCE) and the Ministry of Digital Development, Innovation and Aerospace Industry of the Republic of Kazakhstan, with the support of the United Kingdom. These trainings have become an important platform for international cooperation aimed at ensuring cybersecurity and the development of information and communication technologies in the region;

CTF Cyber Kumbez at the "KazHackStan-2023"

From September 13 to 15, 2023, at the CyberKumbez cyber range in Almaty, Kazakhstan a CTF event was held that had 24 Kazakhstani teams as participants.

The purpose of the Cyber Kumbez CTF was to detect vulnerabilities in the exclusively designed infrastructure of a virtual city and implement unacceptable events (business risks);

Kuban CTF at the IV "Kuban CSC-2023" International Conference on Information Security

The IV International Information Security Conference Kuban CSC 2023 was held from October 12 to 13, 2023 in Sochi, Russia, on the territory of the Krasnaya Polyana resort.

Traditionally, this conference organized the final of the Kuban CTF-2023 practical information security championship, in which the KZ-CERT Team also took part;

11th Regional Arab, CIS, OIC-CERT Cyber Drill

Cyber trainings and workshops were held as part of the 15th OIC-CERT Annual Conference for 2 days from October 9 to October 10, 2023. KZ-CERT formed a team of 3 employees to participate in the event.

The OIC-CERT Cyber Drill, parts of which were independent of each other, were conducted on online platforms such as cybertask and cyberrangers.

3.2 Events

Every year KZ-CERT maintains efforts to conclude agreements with strategically important partners in the field of cybersecurity in order to formalize mutually beneficial cooperation in responding to threats and incidents of information security. Thus, in 2023, KZ-CERT has concluded 1 Memorandum of Understanding in the field of cybersecurity.

Apart from that, KZ-CERT Team members also actively attended various international conferences and meetings. The following events can be mentioned in this regard:

- Security Analyst Summit in Phuket, Thailand (in person, as a speaker);
- "Infoforum-2023" event in Moscow, Russia (in person, as a speaker);
- "Positive Hack Days 2023" cyber festival in Moscow, Russia (in person, as a listener);
- Annual "SOC-Forum 2023" event in Moscow, Russia (in person, as a listener);
- 35th Annual FIRST Conference & NatCSIRT 2023 meeting in Montreal, Canada (in person, as a listener);
- Annual "KazHackStan 2023" conference in Almaty, Kazakhstan (in person, as a speaker);
- FIRST Cyber Threat Intelligence Symposium 2023 in Berlin, Germany (in person, as a listener);
- CAMP 8th Annual Meeting 2023 (in person, as a listener);
- 15th Annual OIC-CERT Conference and Regional Cybersecurity Week 2023 in Abu-Dhabi, UAE (in person, as a listener);
- "National Cyber Incident Classification" workshop in Tashkent, Uzbekistan (in person, as a speaker).

OIC-CERT

Organisation of The Islamic Cooperation – Computer Emergency Response Teams

1. About the OIC-CERT

1.1 Introduction

The Organisation of the Islamic Cooperation - Computer Emergency Response Team (OIC-CERT) was established through the Organization of the Islamic Cooperation (OIC) Resolution No 3/35-INF Collaboration of Computer Emergency Response Team (CERT) Among the OIC Member Countries. It was passed during the 35th Session of the Council of Foreign Ministers of the OIC in Kampala Uganda on 18-20 June 2008.

In 2009 through the Resolution No 2/36-INF Granting the Organization of the Islamic Cooperation –Computer Emergency Response Team an Affiliated Institution Status, the OIC-CERT became an affiliate institution of the OIC during the 36th Session of the Council of Foreign Ministers of the OIC Meeting in Damascus, Syrian Arab Republic on 23-25 May 2009.

Vision

Envisioning the OIC-CERT to be a leading cybersecurity platform to make the global cyber space safe.

Mission

A platform to develop cybersecurity capabilities to mitigate cyber threats by leveraging on global collaboration.

1.2 Membership

As of Dec 2023, the OIC-CERT has a network and strategic collaboration with 63 members from 28 OIC countries. This include the support from 6 Commercial Members, 5 Professional Members, 3 Fellow Member, 1 Affiliate Member, and 1 Honorary Member.

The membership categories are as follows:

1.2.1 Full Members

These are CERTs, Computer Security Incident Response Teams (CSIRTs) or similar entities that are located and/ or having the primary function within the jurisdiction of the OIC CERT member countries that is wholly or partly owned by the government with the authority to represent the country's interest.

1.2.2 General Members

These are other related government organizations, non-governmental organizations or academia that deals with cybersecurity matters. However, these parties do not have the authority to represent the country's interest.

1.2.3 Affiliate Members

These are not-for-profit organizations that deals with cybersecurity matters from non OIC-CERT member countries.

1.2.4 Commercial Members

These are industrial or business organizations that deals with cybersecurity matters from the OIC and non-OIC member countries.

1.2.5 Professional Members

Individual professionals mainly in the cybersecurity domain not restricted to the OIC community.

1.2.6 Fellow Members

These are individual who are considered as co-founders of the OIC-CERT and have actively represent their organization as an OIC-CERT member for a minimum period of 5 years.

1.2.7 Honorary Members

Individuals or organizations who has demonstrated extraordinary contribution, support, and exemplary leadership to the OIC-CERT.

Details of the members can be found at www.oic-cert.org

2. Activities & Operations

2.1 OIC-CERT 15th Annual Conference & FIRST Symposium, Abu Dhabi, United Arab Emirates

The OIC-CERT 15th Annual Conference was held in Abu Dhabi, United Arab Emirates from 9-13 October 2023 in conjunction of regional Cybersecurity Week. The event organized in conjunction with the ITU Arab Regional Cybersecurity Centre (ITU-ARCC) & the FIRST Symposium for Africa and Arab Regions with theme "Cybersecurity Innovation and Industry Development".

2.2 Online Trainings

To raise awareness on cybersecurity within the OIC-CERT member states, 11 sessions of online trainings (opened to APCERT members) were conducted in 2023 as follows:

Date	Topic	Host
15 Feb	External Attack Surface Management	AeCERT/ TDRA, UAE
14-16 Mar	Covering GISEC Sessions	UAE
31 Mar	The Role of ISACs in Improving Cybersecurity and Resilience: Introduction and Implementation of Best Practice	NCCA, Indonesia
12 Apr	DNS: Prevention, Detection, Disruption and Defense	ICANN
24 May	Responding to the Ever-Evolving Threat Landscape	AeCERT/ TDRA, UAE
31 Jul	Webinar Serumpun: Susah-Susah Cari Rezeki, Senang-Senang Scammer Curi	CyberSecurity Malaysia
26 Jul	From Information to Action: Leveraging Threat in Intelligence to Stay Ahead in the Cyber Warfare Game	AeCERT/ TDRA, UAE
16 Aug	Empowering Security Through Automated Governance, Risk, And Compliance	TDRA, UAE
5 Oct	CY-X is a Form of Terror: What That Means and Where It's Going	AeCERT/ TDRA, UAE
25 Oct	Webinar Global Digital Security and Forensic 2023	UTeM & CyberSecurity Malaysia
27 Nov	Data Protection in Cybersecurity: A Critical Imperative	NCCA, Indonesia

3. Events Involvement and Achievements

The OIC-CERT actively participated in cybersecurity events such as trainings, seminars, conferences, and meetings. The collaborative platform has contributed its competencies in the following events.

3.1 Cyber Drills

As in the previous years, the OIC-CERT organizes an international cyber drill for the members and partners (including APCERT members). In 2023, Oman National CERT and ITU-ARCC organized the drill with the theme "Applied Learning for Emergency Response Teams (ALERT)" on 9-10 Oct 2023. The event was held in conjunction with the 11th Arab Regional. The objective of this drill is to measure the readiness of the participants in facing cyber-attacks.
The OIC-CERT members also participated in the APCERT Drill that was held on 16 Aug 2023.

3.2 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 contribution from all parties especially the APCERT members for this journal. More details at https://www.oic-cert.org/en/call-for-paper.html

3.3. Cyber Security Guidelines/Procedures

The OIC-CERT has published several cybersecurity guidelines in 2023. The guidelines are as follows:

- Awareness posters and presentations
- The Essential Cybersecurity Controls and Essential Cybersecurity Framework
- Cloud Security Guidelines
- Guideline on 'Cyber Security Laws for OIC Members'
- NISSA - Libya: National Policies for Information Security and Safety
- Malware Protection and Threat Intelligence Policy
- Guidelines for Securing Cloud Implementation by Cloud Service Subscriber
- Harmonized and Unified Cybersecurity Certification System. A Guidance of Part 3 of OIC-CERT 5G Security Framework

3.4 OIC-CERT 5G Security Working Group

The OIC-CERT 5G Security Working Group was established in 2021 co-lead by Huawei (OIC-CERT Commercial Member) and Malaysia. The WG consist of 10 members i.e., Bangladesh, Brunei, Indonesia, Pakistan, Somalia, Tunisia, Malaysia, Morocco, Oman and UAE.

The objectives of the WG are as following:

- Identifying 5G cybersecurity risks taking in account different perspectives from the stakeholders and maintaining a risk register
- Developing recommendations for our members, a 5G security standard that be a reference model for member states to develop their own National 5G cybersecurity standards
- Developing recommendations for developing an OIC-level 5G security framework that harmonize the requirements that allow for cross-recognition among OIC member states; and
- Develop an ISAC (Information Sharing and Analysis Centre) capability for CERT response in the era of 5G and Cloud

for OIC member states under OIC-CERT

In 2023, the WG has developed the Harmonized and Unified Cybersecurity Certification System (HUCCS) - A Guidance of Part 3 of OIC-CERT 5G Security Framework.

3.5 OIC-CERT Cloud Security Working Group

The OIC-CERT Cloud Security Working Group was established in 2022 co-lead by UAE and Egypt. The WG consist of 11 countries/member i.e., UAE, Egypt, Malaysia, Indonesia, Jordan, Nigeria, Pakistan, Somalia, Tunisia, Turkiye and Huawei. In 2023, the WG has developed the OIC-CERT Cloud Security Framework.

3.6 OIC-CERT BlockChain Security Working Group

The OIC-CERT BlockChain Security Working Group was established in 2023 co-lead by UAE and Brunei. The WG consist of 11 countries/member i.e., UAE, Brunei, Egypt, Malaysia, Indonesia, Jordan, Nigeria, Pakistan, Somalia, Tunisia, Turkiye and Huawei.

6. Participation with APCERT Activity

3.7 APCERT Cyber Drill

The OIC-CERT members have participated in the APCERT Cyber Drill 2023 theme “Digital Supply Chain Redemption” held on 16 August 2023. The objective of the Drill exercise is to provide the opportunity for participating organisations to:

- test the communication contact points
- check the contingencies of their processes and procedures
- gauge their technical competencies
- be exposed to the coordination of cross border information security incidents

4. Future Plans

4.1 Future projects

- OIC-CERT Supply Chain Security Working Group
- Artificial Intelligence Security Study Group

Disclaimer on Publications

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

APCERT ANNUAL REPORT 2023

TLP:CLEAR

APCERT
Asia Pacific Computer Emergency Response Team