APCERT
Asia Pacific Computer Emergency Response Team

TLP: WHITE

APCERT ANNUAL REPORT

2020

APCERT Annual Report 2020

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

CONTENTS

Chair's Message 2020

Disruptive technologies such as the Internet of Things, Artificial Intelligence, Industrial Revolution 4 are now changing the way we work and the way we live our daily lives. This is amplified with the Covid-19 pandemic that impose changes to our social norms requiring us to fall back on the existing digital technologies to keep the society running. Reliance on the digital mediums has tremendously increased as people move their transactions online to abide with the social distancing requirement imposed by governments. With the community being encouraged to work from home, business transactions such as meetings, conferences, and seminars, to name a few, are done online. The increased in digital connectivity has contributed to accelerating the digital transformation, which on the other hand has given cyber criminals a larger attack surfaces to target. The pandemic itself has been used as a subject to commit crimes with impersonation as government and health organization as the desire for more Covid-19 related information rises.

The APCERT is a collaboration of Computer Security Incident Response Teams (CSIRTs) / Computer Emergency Response Teams (CERTs) within the Asia Pacific region representing continuous international collaboration in information sharing to provide effective cybersecurity responses. This APCERT Annual Report is a compilation of members' activities to provide some level of transparency in the efforts to mitigate cyber threats and incidents.

CSIRTs/CERTs organisations worldwide realise that international cooperation will usually be identified as a pillar in cybersecurity frameworks. This has contributed to the expansion of the APCERT membership. In 2020, we welcomed eight new members of various categories which are:

i. Cybersecurity and Infrastructure Security Agency (**CISA**)
ii. Kazakhstan Computer Emergency Response Team (**KZ-CERT**)
iii. Tonga's National CSIRT (**CERT Tonga**)
iv. National Cyber Security Center in the Republic of Korea CERT (**KN-CERT**)
v. The Philippines' National CSIRT (**CERT-PH**)
vi. Africa Computer Emergency Response Team (**AfricaCERT**)
vii. Asia Pacific Network Information Centre (**APNIC**)

viii. Organisation of The Islamic Cooperation – Computer Emergency Response Teams (**OIC-CERT**)

With this, APCERT now has 33 team members from 23 economies. We will continue to welcome and look forward to having new members who share the APCERT vision of creating a safe, clean and reliable cyber space in the Asia Pacific Region.

The APCERT Annual Cyber Drill 2020 shows favourable participations with 32 CSIRT teams from 27 economies taking part:

Australia
Hong Kong
Korea
Myanmar
Thailand
Egypt
Pakistan
Bangladesh
India
Macau
Singapore
Vietnam
Jordan
Tunisia
Indonesia
Japan
Malaysia
Sri Lanka
Benin
Morocco
AfricaCERT
Brunei Darussalam
People's Republic of China
Chinese Taipei
New Zealand
Lao People's Democratic Republic
Nigeria

This exercise is about validating and enhancing communication protocols, technical capabilities, and quality of cyber incident responses. The Cyber Drill is a tradition and hope that it will continue to do so in the years to come. For the APCERT Drill 2021, KrCERT/CC has agreed to take the lead and we are crossing our fingers for another success story.

The APCERT Steering Committee always strive to improve the operational efficiency of this collaboration platform. The Operational Manual was updated in October 2020 to reflect recent changes in the Point-of-Contact Arrangements Policy. This is a continuous process for further improvement of seamless cross border communication among members. In addition, the APCERT Steering Committee is looking at boosting the members' technical networking to improve efficiency in cyber threat mitigation.

The APCERT Annual Conference 2020 which was supposed to be held in Colombo, Sri Lanka, has been postponed to 2021 due to the pandemic. Thanks to Sri Lanka CERT|CC for being able to accommodate the arrangement. In line with this, for the first time in APCERT history, the Annual General Meeting 2020 was conducted online and without the Annual Conference. This, however, did not deter members from participating and maintaining good interactions with each other.

Finally, we would like to express our appreciation to each member for supporting the APCERT, be it as Steering Committee members, working groups team members, and just as members. The collaboration will continue to work on the mission of maintaining a trusted contact network of computer security experts in Asia Pacific to improve the region's awareness and competency in cybersecurity.

Mohd Shamir bin Hashim
Chair, APCERT Steering Committee
CyberSecurity Malaysia

I. About APCERT

1. Objectives and Scope of Activities

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

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

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

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 organisations, we are now working towards its actualization.

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

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

The geographical boundary of APCERT activities is the same as that of the Asia Pacific Network Information Centre (APNIC). These cover the entire Asia Pacific, comprising of 56 economies. The list of those economies is available at:
https://www.apnic.net/about-APNIC/organization/apnics-region

2. APCERT Members

APCERT was formed in 2003 by 15 teams from 12 economies across the Asia Pacific region, and its membership has continued to increase since then. For further information on the APCERT membership structure and criteria, please refer to the APCERT Operational Framework:
https://www.apcert.org/documents/pdf/APCERT_Operational_Framework_-_Sep_2020-1.pdf

As of December 2020, APCERT consists of 33 Operational Members from 23 economies across the Asia Pacific region, 4 Liaison Partners, 2 Strategic Partners, and 4 Corporate Partners.

Operational Members (33 Teams / 23 Economies)

Team	Official Team Name	Economy
ACSC	Australian Cyber Security Centre	Australia
AusCERT	Australian Computer Emergency Response Team	Australia

bdCERT	Bangladesh Computer Emergency Response Team	Bangladesh
BGD e-GOV CIRT	Bangladesh e-Government Computer Incident Response Team	Bangladesh
BruCERT	Brunei Computer Emergency Response Team	Brunei Darussalam
BtCIRT	Bhutan Computer Incident Response Team	Bhutan
CCERT	CERNET Computer Emergency Response Team	People's Republic of China
CERT-In	Indian Computer Emergency Response Team	India
CERT NZ	CERT NZ	New Zealand
CERT-PH	Philippines National Computer Emergency Response Team	Philippines
CERT Tonga	Tonga Computer Emergency Response Team	Tonga
CNCERT/CC	National Computer network Emergency Response technical Team / Coordination Center of China	People's Republic of China
CyberSecurity Malaysia	CyberSecurity Malaysia	Malaysia
EC-CERT	Taiwan E-Commerce Computer Emergency Response Team	Chinese Taipei
GovCERT.HK	Government Computer Emergency Response Team Hong Kong	Hong Kong, China
HKCERT	Hong Kong Computer Emergency Response Team Coordination Centre	Hong Kong, China
ID-CERT	Indonesia Computer Emergency Response Team	Indonesia
ID-SIRTII/CC	Indonesia Security Incident Response Team of Internet Infrastructure/Coordination Center	Indonesia
JPCERT/CC	Japan Computer Emergency Response Team / Coordination Center	Japan
KN-CERT	Korea National Computer Emergency Response Team	Republic of Korea
KrCERT/CC	Korea Internet Security Center	Republic of Korea
LaoCERT	Lao Computer Emergency Response Team	Lao People's Democratic Republic
mmCERT/CC	Myanmar Computer Emergency Response Team	Myanmar
MNCERT/CC	Mongolia Cyber Emergency Response Team / Coordination Center	Mongolia
MOCERT	Macau Computer Emergency Response Team Coordination Centre	Macau, China

MonCIRT	Mongolian Cyber Incident Response Team	Mongolia
SingCERT	Singapore Computer Emergency Response Team	Singapore
Sri Lanka CERT|CC	Sri Lanka Computer Emergency Readiness Team Coordination Centre	Sri Lanka
TechCERT	TechCERT	Sri Lanka
ThaiCERT	Thailand Computer Emergency Response Team	Thailand
TWCERT/CC	Taiwan Computer Emergency Response Team / Coordination Center	Chinese Taipei
TWNCERT	Taiwan National Computer Emergency Response Team	Chinese Taipei
VNCERT	Vietnam Computer Emergency Response Team	Vietnam

Liaison Partners (4 Teams)

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

Strategic Partners (4 Teams)

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

Corporate Partners (4 Teams)

Team	Official Team Name
Bkav	Bkav Corporation
Dell SecureWorks	Dell SecureWorks
Microsoft	Microsoft Corporation

Panasonic PSIRT	Panasonic Product Security Incident Response Team

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

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

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

Team	Term	Other positions
ACSC	2020 - 2022	
CNCERT/CC	2020 - 2022	Deputy Chair
CyberSecurity Malaysia	2019 - 2021	Chair
JPCERT/CC	2019 - 2021	Secretariat
KrCERT/CC	2020 - 2022	
Sri Lanka CERT|CC	2019 - 2021	
TWNCERT	2020 - 2022	

***Newly elected at AGM 2020**

3. Working Groups (WG)

There are currently ten (10) Working Groups (**WG**s) in APCERT.

1) TSUBAME WG (formed in 2009)

- Objectives:
  - Establish a common platform for Internet threat monitoring, information sharing and analyses for the Asia Pacific region and others;
  - Promote collaboration among the CSIRTs in the Asia Pacific region and others using the platform
  - Enhance the capability of global threat analyses by incorporating 3D Visualization features to the platform
- Secretariat (**1**): JPCERT/CC
- Members (**22**): AusCERT, BruCERT, CCERT, CERT-In, CNCERT/CC, CyberSecurity Malaysia, EC-CERT, GovCERT.HK, HKCERT, ID-SIRTII/CC, KrCERT/CC, LaoCERT, maCERT, mmCERT, MOCERT, NCA-CERT, Sri Lanka CERT|CC, TechCERT, ThaiCERT, TWCERT/CC, TWNCERT, VNCERT/CC

2) Information Sharing WG (formed in 2011)

- Objectives:
  - Improve information and data sharing within APCERT, including by improving members' understanding of the value of data sharing and motivating APCERT members to exchange information and data
  - Organize members to establish and enhance the necessary mechanisms, protocols and infrastructures to provide a better environment for members 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 cyber security of their constituent networks
  - Work as the Point of Contact (PoC) for APCERT to other organizations on information sharing
- Convener (1): CNCERT/CC
- Members (18): AusCERT, bdCERT, Bkav Corporation, CERT-In, CNCERT/CC, CyberSecurity Malaysia, GovCERT.HK, HKCERT, ID-CERT, ID-SIRTII/CC, JPCERT/CC, KrCERT/CC, Microsoft, SingCERT, Sri Lanka CERT|CC, TechCERT, ThaiCERT, TWNCERT, VNCERT

3) Membership WG (formed in 2011)

- Objectives:
  - Promote collaboration and participation by all APCERT members
  - Establish the organizational bases to enhance the partnership with cross-regional partners and supporters
  - Guide activities such as checking and monitoring for sustaining the health of the membership structure
  - Promote harmony and cooperation among APCERT members and partners
- Convener (1): KrCERT/CC
- Members (13): ACSC, AusCERT, BruCERT, CNCERT/CC, CyberSecurity Malaysia, HKCERT, ID-CERT, ID-SIRTII/CC, JPCERT/CC, MOCERT, Sri Lanka CERT|CC, TechCERT, VNCERT

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

- Objectives:
  - Promote the vision and mission of APCERT through the development and

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

5) Training WG (formed in 2015)

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

6) Malware Mitigation WG (formed in 2016)

- Objectives
  - Have a better understanding of the malware threats and analysis as well as

  the related potential impacts mainly within the participants' community
  - Educate and improve awareness, preparedness, and readiness in facing malware threats
- Convener (**1**): CyberSecurity Malaysia
- Members (**14**): BdCERT, BGD e-GOV CIRT, Bkav Corporation, BruCERT, CERT-In, GovCERT.HK, HKCERT, ID-CERT, JPCERT/CC, KrCERT/CC, SecureWorks, SingCERT, Sri Lanka CERT|CC, TWCERT/CC

7) Drill WG (formed in 2017)

- Objectives
  - To serve as a permanent Organizing Committee for the annual cyber drills and assist the Lead Organizing CERT
  - To maintain centralized documentation for the drills, their working documents, procedures, handbooks and feedback
  - To allow continuous improvements
- Convener (**1**): ThaiCERT (until August 2020)
- Members (**12**): ACSC, AusCERT, CERT-In, CERT NZ, HKCERT, JPCERT/CC, KrCERT/CC, SingCERT, Sri Lanka CERT|CC, TechCERT, TWCERT/CC, TWNCERT

8) IoT Security WG (formed in 2017)

- Objectives
  - Identification of the threat landscape and security challenges in IoT ecosystem
  - Proposing steps to address the security issues including vulnerabilities tailored for IoT.
  - Recommendations for securing Internet of Things (IoT) ecosystem
  - Incident response mechanisms/measures for responding to cyber physical security incidents impacting human life
  - Discussions on existing Security Standards and gaps for IoT ecosystem and considerations for adoption
  - Development of threat sharing platform and threat sharing mechanism
- Convener (**1**): CERT-In
- Members (**7**): BGD e-GOV CIRT, CERT NZ, HKCERT, IDSIRTII/CC, JPCERT/CC, Panasonic PSIRT, VNCERT

9) Secure Digital Payment WG (formed in 2017)

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

10) Critical Infrastructure Protection WG (formed in 2020)

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

4. APCERT Website

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

II. APCERT Activity Report 2020

1. International Activities and Engagements

APCERT has been dedicated to representing and promoting its activities in various international conferences and events. From January to December 2020, APCERT Teams have hosted, participated and/or contributed in the following events:

- APCERT Drill 2020 (11 March)

  https://www.apcert.org/documents/pdf/APCERT_Drill2020_Press%20Release.pdf

  APCERT Drill 2020, the 15th APCERT Cyber Exercise Drill, was successfully conducted to test the response capabilities of the participating APCERT Teams. 25 CSIRTs from 19 economies of APCERT (Australia, Bangladesh, Brunei Darussalam, People's Republic of China, Chinese Taipei, Hong Kong, India, Indonesia, Japan, Korea, Lao People's Democratic Republic, Macau, Malaysia, Myanmar, New Zealand, Singapore, Sri Lanka, Thailand, and Vietnam) participated in the drill. From the external parties, CSIRTs from 7 economies (Benin, Egypt, Jordan, Morocco, Nigeria, Pakistan and Tunisia) of OIC-CERT and AfricaCERT participated. The theme of the drill was "Banker doubles down on Miner."

- PacSON Session (18 August – Online)

  On behalf of APCERT, MyCERT in CyberSecurity Malaysia conducted an online lecture titled "Android Mobile Malware Case Study During Covid19 Lockdown" as a part of PaCSON's webinar series.

- AP* Retreat (7 September – Online)

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

- APCERT Annual General Meeting (AGM) 2020 (29 September – Online)

  The APCERT Annual General Meeting (AGM) was held online for the first time on 29 September 2020.

- ASEAN CERT Incident Drill (ACID) 2020 (7 October – Online)

  ACID 2020, led and coordinated by SingCERT, entered its 14th iteration with participation including ASEAN CERTs and APCERT Teams. The drill was completed successfully, providing an opportunity for teams to improve their skills on investigating and responding to ransomware incident, including malware analysis to uncover its characteristics and subsequently escalating to the necessary parties for mitigation.

- 32nd Annual FIRST Conference (16-18 November – Online)
  https://www.first.org/conference/2020/
  APCERT teams attended the Annual FIRST Conference and shared valuable experience and expertise through various presentations.

- OIC-CERT 12th Annual Conference 2020 (23-24 November – Online)
  https://www.oic-cert.org/en/events/conference/2020.html#.X-A-RrPgqle
  APCERT participated a session entitled COVID-19 Hardening Security Operation and discussed about the need to balance privacy and security challenges during the COVID-19 pandemic.

Other International Activities and Engagements

- DotAsia
  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 also actively participate in FIRST. APCERT signed MoU with FIRST on 6th of November 2020 to enhance further collaboration.

- STOP. THINK. CONNECT (STC)
  APCERT has collaborated with STOP. THINK. CONNECT (STC) under a Memorandum of Understanding since June 2012 in order to promote awareness towards cyber security and more secure network environment.

- Asia Pacific Network Information Security Centre (APNIC)
  APCERT and Asia Pacific Network Information Centre (APNIC) signed a Memorandum of Understanding in 2015, which was renewed in 2019

- Africa Computer Emergency Response Team (AfricaCERT)

  APCERT and AfricaCERT signed a Memorandum of Understanding in 2019.

2. APCERT SC Meetings

From January to December 2020, SC members held 6 teleconferences to discuss APCERT operations and activities.

Date	Location
15 January	Teleconference
1 April	Teleconference
17 June	Teleconference
5 August	Teleconference
23 September	Teleconference
18 November	Teleconference

3. APCERT Training

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

Date	Title	Presenter
18 February	Identification of information security risks as a sectoral CSIRT and addressing the risks	FinCSIRT
7 April	Getting started with Threat Intelligence Sharing via MISP	CIRCL.LU
11 August	Digital Forensics Procedures & Interesting Artifacts	Sri Lanka CERT|CC
6 October	CTI & IntelMQ	TWNCERT
1 December	ATM Cyber Attack	FSI-CERT

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

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

Email: apcert-sec@apcert.org.

Disclaimer on Publications

The contents of the Activity Report on Chapter III and IV are written by each APCERT members and partners based on their individual analysis. Responsibility for the information and views expressed in each report lies entirely with the authors.

III. Activity Reports from APCERT Members

ACSC

Australian Cyber Security Centre – Australia

1. Highlights of 2020

1.1 Summary of major activities

Throughout 2020, ASD's Australian Cyber Security Centre (ACSC) has remained focused on emerging cyber threats, including those to critical infrastructure and technologies, cloud computing and small and medium-sized enterprises. The COVID-19 pandemic saw an increase in the operational tempo for the ACSC, with more demand from government and the public for cyber security advice and support tailored to meet the challenges of the threat environment. This was especially noticeable with the increase in working from home for business around the country.

1.2 Achievements & milestones

The ACSC worked actively with public and private sector organisations to strengthen cyber security arrangements and build resilience. Key activities included:

- delivery of the Government Uplift Program on 25 select government networks, comprising:
  - ‘Essential Eight’ Sprints conducted between July and December 2019
  - follow-on consolidation of cyber security improvements through administration of the Cyber Security Response Fund
  - improved sharing of cyber security best practice among state, territory and federal governments through the Chief Information Officer / Chief Information Security Officer Forums since June 2019
  - a pilot of ACSC’s Strategic Host Based Sensor Program, to facilitate real time threat monitoring and rapid remediation.
- establishing a pilot scalable, Protective Domain Name Service (PDNS) in February 2020. A number of federal government agencies have been successfully on-boarded to date, including approximately 9,000 users
- the Australian Internet Security Initiative (AISI), providing daily threat information about malware infected or vulnerable networks via 4.2 million Active Compromise Reports and 575.2 million Vulnerable/Open Service Reports on vulnerable networks to over 300 member organisations, including Internet Service Providers, state and

federal government agencies, medium-to-large private organisations and critical infrastructure

- expanding the ACSC Partnership Program, which grew during this reporting period to incorporate 667 organisations across all levels of government, critical industry, business, and the academic, research and not-for-profit sectors
- delivering Operational Technology-Information Exchanges around Australia involving hundreds of organisations responsible for vital control systems including the electricity, water, transport, health and defence sectors.
- providing cyber security support to the Australian Electoral Commission, including vulnerability assessments, advice and assistance, threat briefing and incident response in the lead-up to and during the May 2020 Federal Government regional by-election, and support to the relevant electoral commissions ahead of Northern Territory, Queensland and Australian Capital Territory elections in 2020.

2. About CSIRT

2.1 Introduction

The ACSC within the Australian Signals Directorate (ASD) leads the Australian Government's efforts on national cyber security. It brings together cyber security capabilities from across the Australian Government to improve the cyber resilience of the Australian community and help make Australia the most secure place to connect online.

2.2 Establishment

The ACSC began operations in 2014 as a collaboration between government agencies. Since then, and as part of the Independent Intelligence Review in 2017, the Australian Government identified the need to provide enhanced cyber security capabilities and a single point of advice and support on cyber security.

On 1 July 2018, the ACSC expanded and formally became part of ASD, which also became an independent statutory agency within the defence portfolio. Australian Government cyber security expertise from CERT Australia and the Digital Transformation Agency moved into the ACSC.

2.3 Resources

The ACSC consists of several hundred staff members, including those from partner agencies such as the Australian Criminal Intelligence Commission and the Australia

Federal Police. Department of Home Affairs Cyber Security Policy Division staff are collocated with ACSC staff to better inform policy advice for Government.

2.4 Constituency

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

3. Activities & Operations

3.1 Scope and definitions

The ACSC is a hub for private and public sector collaboration and information-sharing on cyber security, to prevent and combat threats and minimise harm to Australians. We provide advice and assistance across the whole economy, including critical infrastructure and systems of national interest, federal, state and local governments, small and medium businesses, academia, not-for-profit organisations and the Australian community.

Specifically, the ACSC:

- responds to cyber security threats and incidents as Australia's whole of economy computer emergency response team (CERT)
- collaborates with the private and public sector to share information on threats and increase resilience
- works with governments, industry and the community to increase awareness of cyber security
- provides cyber security information, advice and assistance to all Australians.

3.2 Incident handling reports

The ACSC's incident response capabilities span the full range of cyber incidents, from national crises to incidents affecting individual members of the public. In order to manage the broad range of cyber incidents, the ACSC uses a Cyber Incident Categorisation Matrix (see Figure 1) to triage and prioritise the immediate defensive response to mitigate each cyber incident. This allows the ACSC to focus its resources more effectively, ensuring consistent messaging and an appropriate level of response measures are activated.

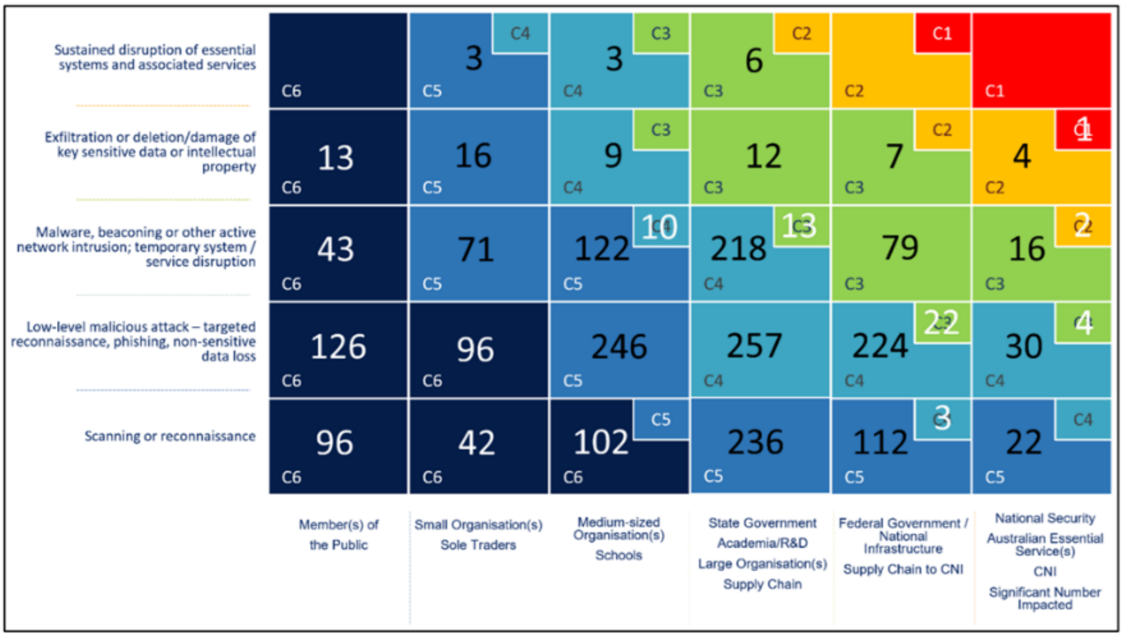


Figure 1

3.3 Abuse statistics

During 2019–20, the ACSC responded to 2,266 cyber security incidents of varying significance. Of the 2,266 incidents, the largest proportion were assessed as being ‘Category 5’ (C5) followed by ‘Category 4’ (C4). These categories broadly represented malicious cyber activity such as targeted reconnaissance, phishing emails and malicious software impacting larger organisations, key supply chain and Commonwealth and state government entities.

3.4 Publications

During 2019–20, the ACSC used a variety of means to provide accurate and timely cyber security advice to Australians including product tailored to address the cyber security challenges across the economy during COVID-19 (see Case Study 1). Publications are available at cyber.gov.au, including:

- the ACSC’s Small Business Cyber Security Guide, accompanied by a suite of supporting publications including 11 Step-by-Step Guides and three Quick Wins publications
- twenty-two new PROTECT publications for public consumption, including updates to several existing publications
- six unclassified Sector Snapshots covering banking and finance, water, education and training, communications, sports and health sectors, designed to inform

decisions about investment and allocation of internal resources by executives and cyber security professionals relevant to that critical infrastructure sector

- fifteen Australian Communications Security Instructions to Australian government agencies and associated contractors tasked with the control, handling and maintenance of cryptographic products used to protect classified government information
- monthly updates to the Information Security Manual ensuring that cyber security principles and guidelines remain relevant and applicable for organisations in managing their own risk framework to protect their systems from cyber threats
- seven Information Security product certifications under the Australasian Information Security Evaluation Program.

3.5 New services

In June 2020, the ACSC launched the new cyber.gov.au website. This consolidated all cyber-enabled reporting channels across government to provide the breadth of services including incident reporting, threat reporting subscription services, customer management and Protective DNS for whole-of-government and select critical industry systems. The site underwent numerous incremental changes during 2019–20 to modernise, replace and consolidate ACSC-related legacy sites and services, including incorporation of the Stay Smart Online Program. The changes improve the delivery of information by customer segmentation and make it easier for the full spectrum of ACSC customers – from individuals, small and medium-sized business, to large organisations, critical infrastructure and government entities – to access relevant cyber security advice, news and alerts, tailored to their needs.

4. Events organized / hosted

4.1 Training

The Partnership Program is primarily delivered through the Joint Cyber Security Centres (JCSCs) located in capital cities around Australia. The JCSCs create a trusted, neutral environment, driving collaboration and information sharing on joint cyber security challenges and opportunities and propagating this across all sectors of the economy.

During 2019–20 the JCSCs built collaboration across the Australian economy, hosting interactive workshops, presentations, training sessions, information exchanges and working groups, as well as providing facilitated space for collaborative working and information sharing. ACSC Partners also collaborate actively on the JCSC Slack channel.

Examples of collaboration and information sharing facilitated by the ACSC Partnership Program and JCSCs include:

- spearphishing training delivered to over 500 attendees
- regular sector and general 'drop-in days' in the Centres, with over 100 partners attending larger sessions
- advance notification for partners of significant ACSC investigations
- support and education provided to small and medium-sized businesses across Australia
- regular threat intelligence exchange sessions for industry and government.

4.2 Drills & exercises

The ACSC's National Exercise Program supported 19 cyber security exercise activities across government and the energy, banking and finance, academia, transport, water, defence industries, health and resource sectors.

4.3 Conferences and seminars

While the COVID-19 pandemic has meant that the JCSCs have been unable to host in-person events and collaboration for much of the final quarter of the reporting period, the ACSC has pivoted to providing events virtually. Between 1 April and 30 June, the JCSC ran 19 virtual events for partners across videoconference and Slack. Events have ranged from smaller discussion groups for partners on areas of specific relevance, such as videoconferencing security, to larger discussions on the general threat environment facing partners, and a question and answer session with ACSC incident response experts to discuss the ACSC's 'Copy Paste' Advisory.

5. International Collaboration

5.1 International partnerships and agreements

Cyber security threats and incidents continue to traverse international borders and impact Australia's domestic and offshore interests. The ACSC maintains strong international relationships with global cyber security counterparts in order to share information, mitigate incidents and enhance Australia's cyber security resilience.

The ACSC participates in numerous international engagement and capacity-building activities, to build our collective resilience to cyber security threats and, ultimately, advance Australia's national cyber security objectives.

5.2 Capacity building

The Pacific Cyber Security Operational Network (PaCSON) is designed to facilitate cooperation and collaboration across the Pacific to strengthen the region's cyber security posture. PaCSON provides a working-level network of cyber security incident response professionals in the Pacific – its members are the people responsible for their respective governments' responses to cyber security incidents. In 2020, COVID-19 impacted planned face-to-face events including a cyber security information exchange, an annual general meeting and a series of technical and strategic workshops. In response, the ACSC – in collaboration with PaCSON Members – transitioned PaCSON activities further online.

5.3 Other international activities

The ACSC supported CERT Tonga to become the first Pacific Island Nation to become APCERT members in April 2020. The ACSC was honored to conduct the site visit in October 2019 and subsequently sponsor CERT Tonga's application.

6. Future Plans

6.1 Future projects

The vision of the 2020 Cyber Security Strategy is 'a more secure online world for Australians, their businesses and the essential services upon which we all depend. Consistent with that vision and emphasis, the strategy is underpinned by the government's investment of $1.35 billion in ASD's Cyber Enhanced Situational Awareness and Response (CESAR) package.

The CESAR package has been designed to boost protection and cyber resilience for all Australians, from individuals and small businesses through to the providers of critical services, including through:

- New capabilities to disrupt and defeat malicious cyber activity, providing greater capacity to take the fight to cybercriminals offshore and to neutralise and block emerging cyber threats to Australia.
- Enhancing our understanding of malicious cyber activity so that emerging cyber threats can be more rapidly identified and responded to.

6.2 Future Operation

The ACSC will be facilitating a National cyber security exercise for Australia’s water and wastewater sector in August 2021 aimed at strengthening cyber security resilience in the sector. This exercise follows the success of the national cyber security exercise for Australia’s electricity sector in November 2019.

7. Conclusion

The ACSC looks forward to continuing to work with the APCERT community to build cyber resilience in the region.

AusCERT

Australian Computer Emergency Response Team – Australia

1. About CSIRT

1.1 Introduction

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

1.2 Establishment

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

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

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

1.3 Resources

AusCERT is self-funded and covers its operating costs through a variety of sources including member subscriptions, the annual AusCERT conference and service contracts.

As an active member of the Forum for Incident Response and Security Teams (FIRST) and Asia Pacific Computer Emergency Response Team (APCERT), AusCERT has access to accurate, timely and reliable information about emerging computer network threats and vulnerabilities on a regional and global basis.

1.4 Constituency

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

This is made possible by providing priority incident handling and additional services to our membership base of which covers all industry definitions under the ANZ Standard Industry Classification.

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

2. Activities & Operations

2.1 Scope and definitions

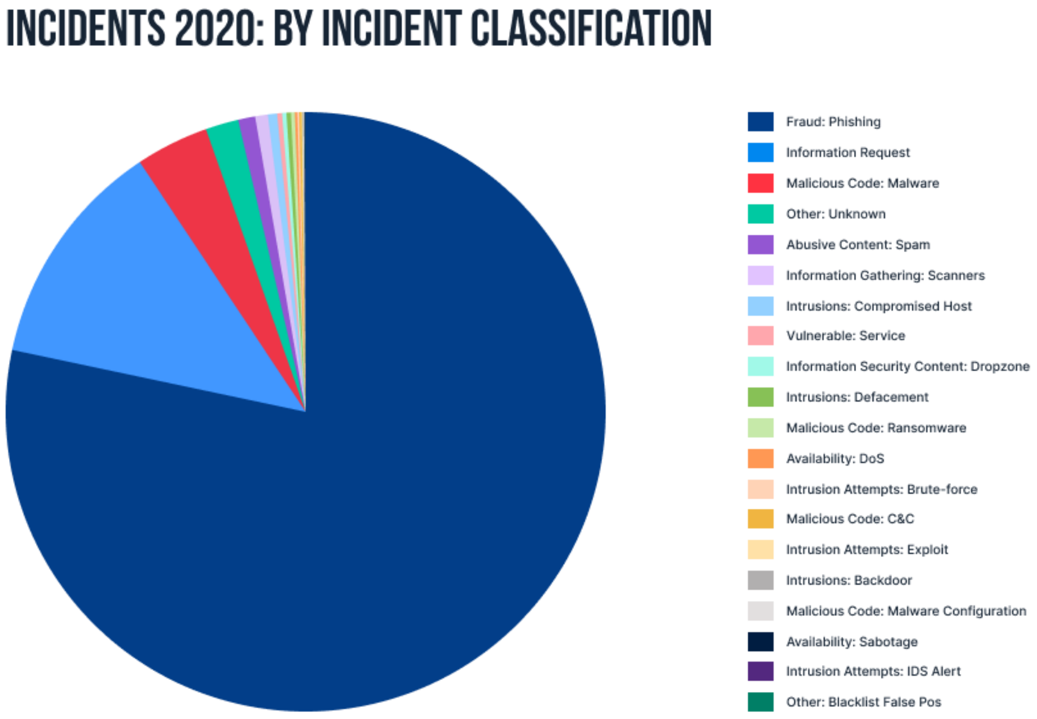
AusCERT monitors and evaluates global cyber network threats and vulnerabilities and remains on-call for members after hours. AusCERT publishes the Security Bulletin Service, drawing on material from a variety of sources, with recommended prevention and mitigation strategies.

Services provided are listed as:

- Incident Management [2.2],
  https://www.auscert.org.au/services/incident-management-service/
- Early Warning Service
  https://www.auscert.org.au/services/early-warning-service/
- Malicious URL Feed
  https://www.auscert.org.au/services/malicious-url-feed/
- Security Bulletin Service [2.3]
  https://www.auscert.org.au/services/security-bulletins /
- Member security incident notification's (MSINs)[2.4]
  https://www.auscert.org.au/services/security-incident-notifications/
- Phishing take-down
  https://www.auscert.org.au/services/phishing-take-down-service/
- Leaked Credential Service
- AusCERT's member only Slack
- AusCERT Conference
  https://conference.auscert.org.au/

2.2 Incident Management Service

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

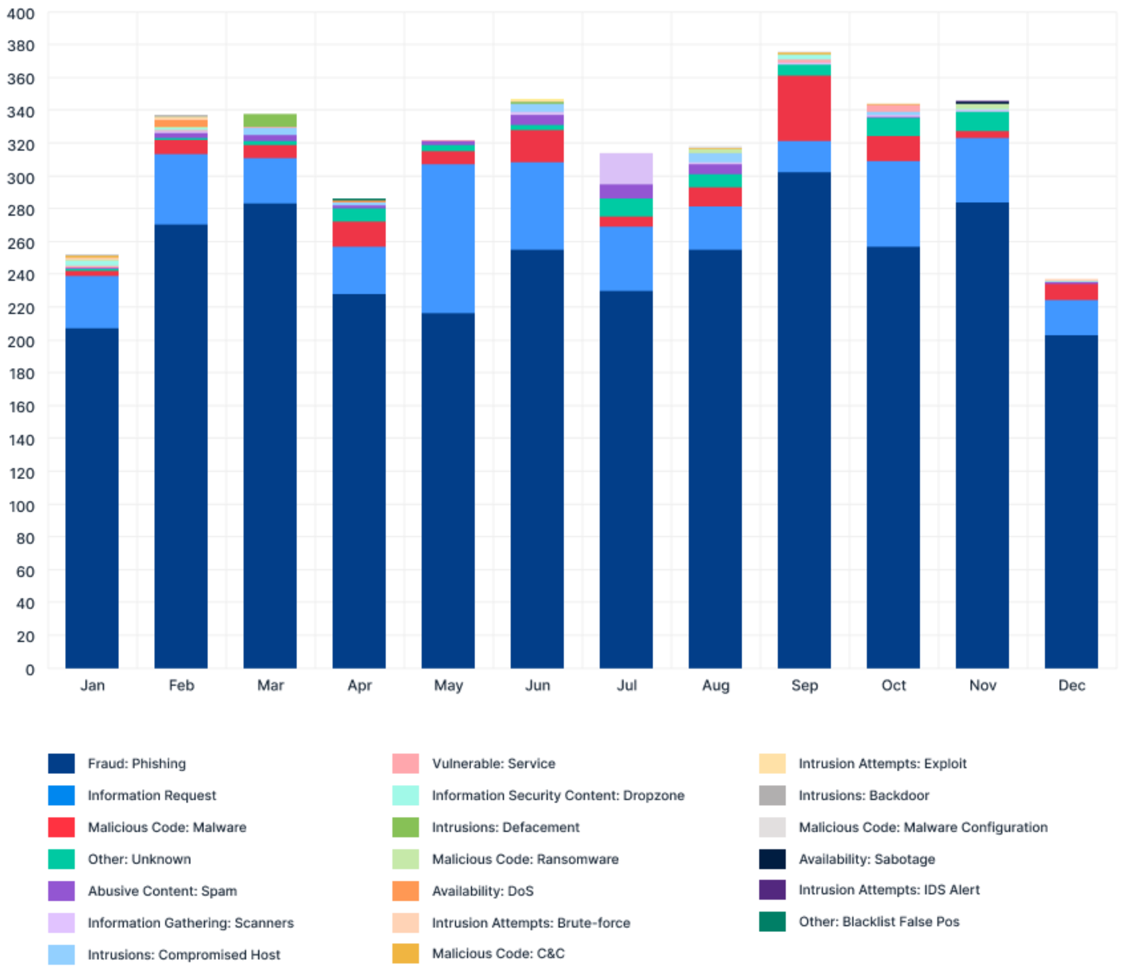


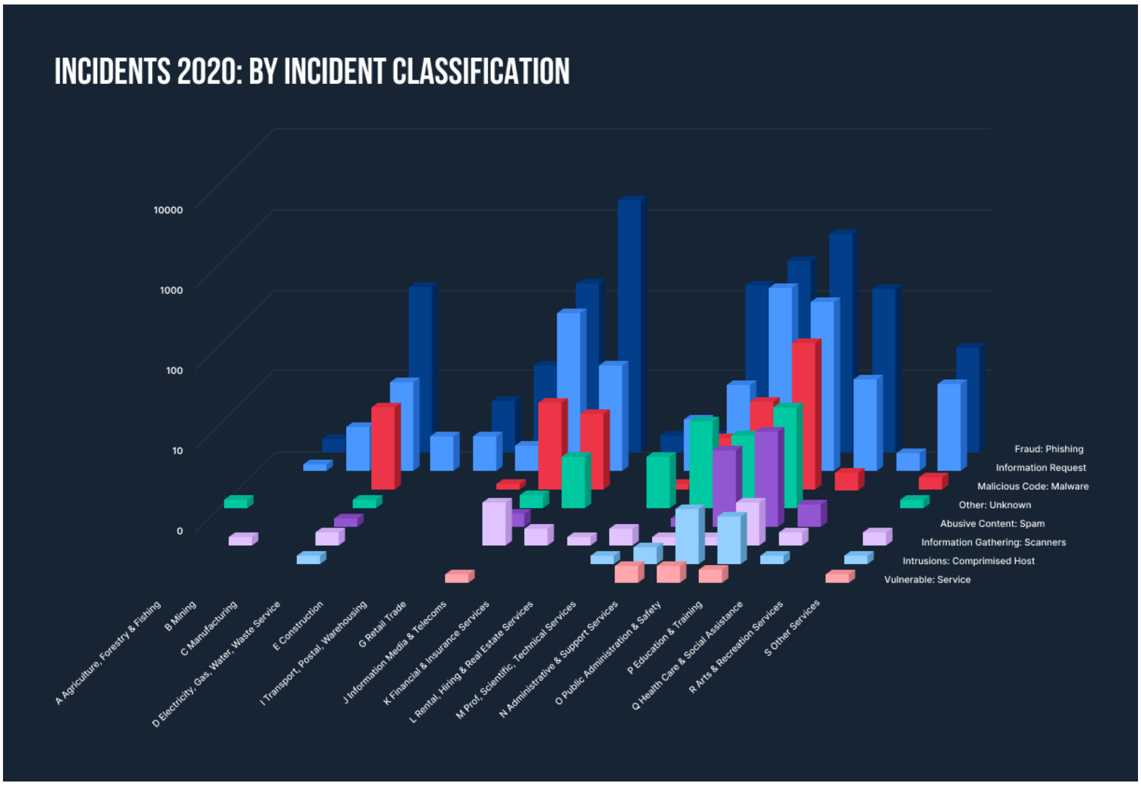
The below diagram is the statistics of incidents that required handling for the calendar year of 2020. Overall, AusCERT serviced 3819 tickets which resulted in an average of approximately 14 tickets per each business day of operation.

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

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

INCIDENTS 2020: INCIDENT CLASSIFICATION BY MONTH





INCIDENTS 2020: BY INCIDENT CLASSIFICATION

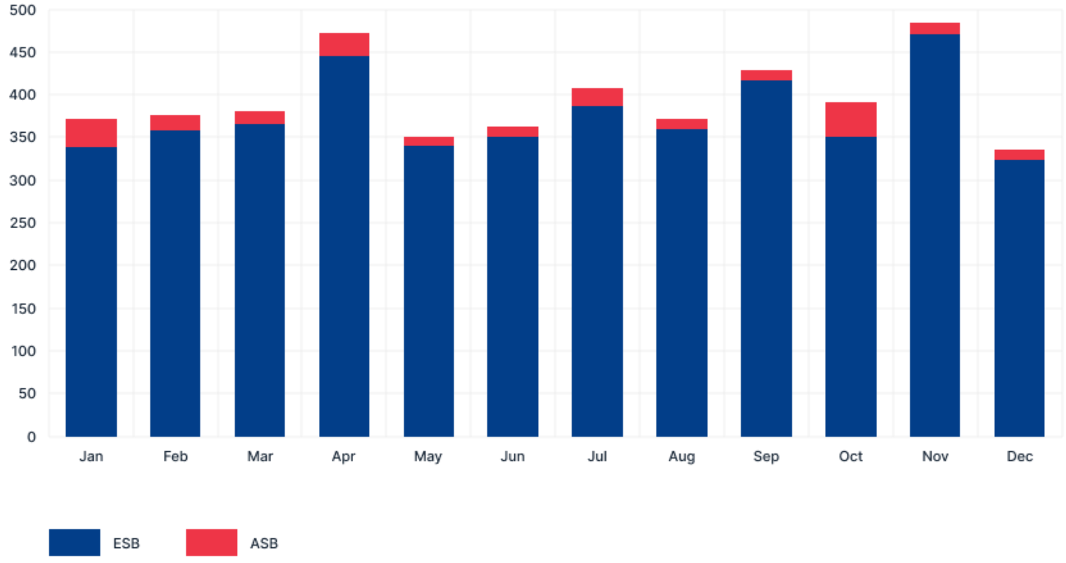
2.3 Security Bulletins

AusCERT distributes security advisories and bulletins to its members by email and publishes a portion of them to its public website.

Bulletins are published in a standardised format with a consistent approach to classifications of vulnerabilities, impacts and affected operating systems.

In 2020, 4504 External Security Bulletins (ESBs) and 226 AusCERT Security Bulletins (ASBs) were published.

BULLETINS 2020

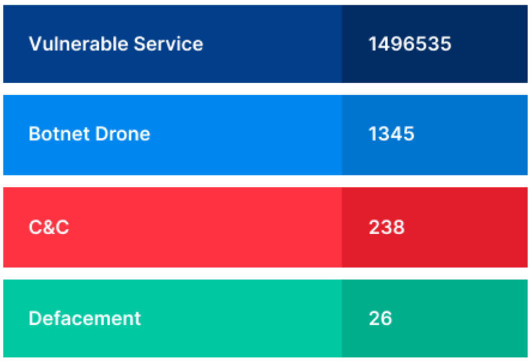


2.4 Member Security Incident Notifications

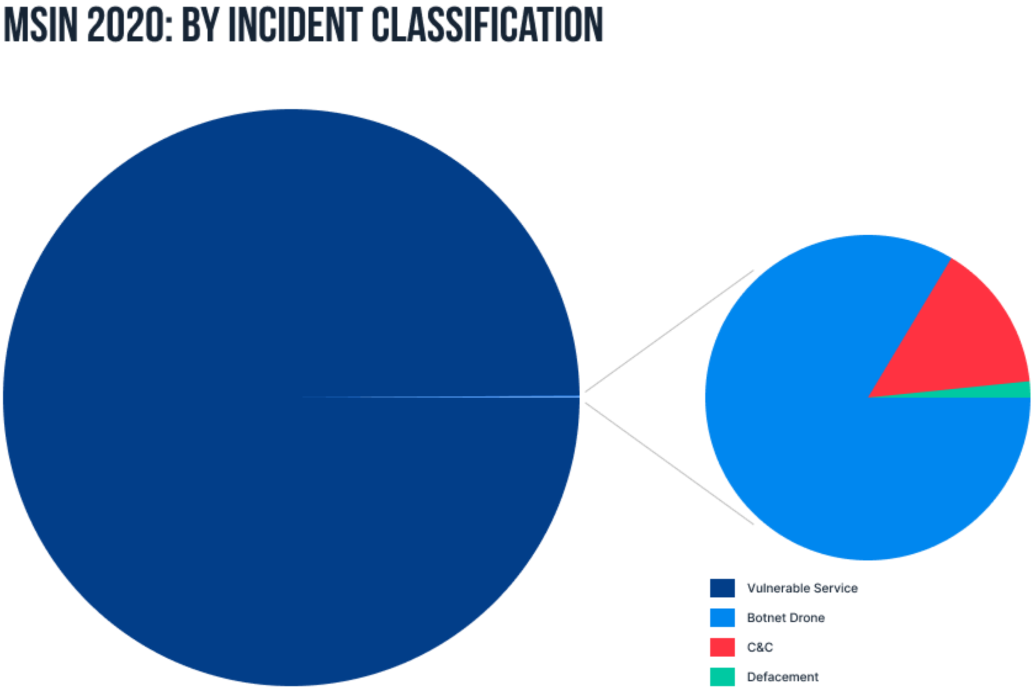
AusCERT members benefit from its considerably large overseas and local threat intelligence feeds with respect to incidents that have been detected by other parties but concern the members.

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

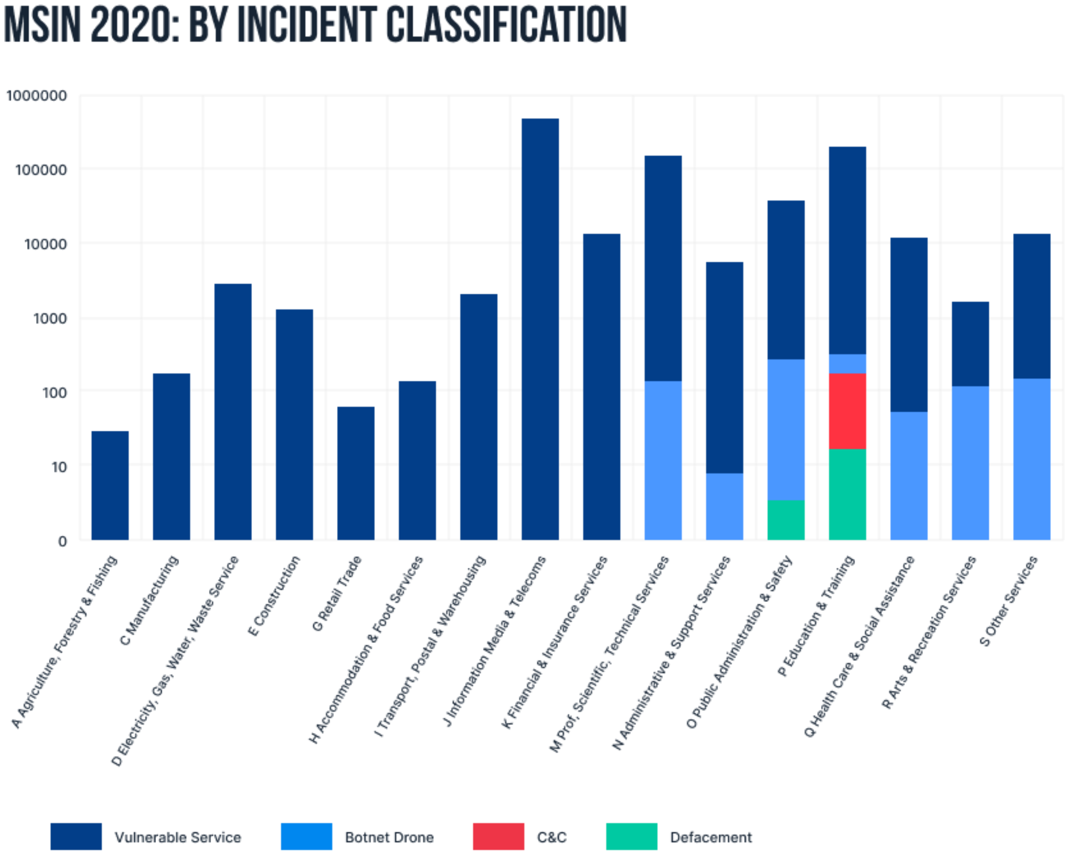
MSIN 2020: BY INCIDENT CLASSIFICATION



Vulnerable Service	1496535
Botnet Drone	1345
C&C	238
Defacement	26



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



2.5 Publications

2.5.1 Week In Review

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

2.5.2 Social Media

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

2.5.3 Newsletter

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

2.5.4 Blog Post

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

3. Events organized / hosted

3.1 Conferences and seminars

3.1.1 AusCERT Conference

The AusCERT Conference 2020, took place from 28th May -31st May 2020 totally online with the theme of "We can be Heros". 4 days of programming, 5 streams, over 80 hours of content, 2 live recording studios, close to 80 remote presenters, over 30 sponsor exhibitors and over 1000 delegate registrations.

Witnessing our delegates, speakers and colleagues rise to the occasion in the spirit of camaraderie and innovation was an amazing experience.

4. International Collaboration

4.1 International partnerships and agreements

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

4.2 Drills & exercises

4.2.1 APCERT Drill 2020

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 "Banker Double doubles down on Miner". The drill fosters communication between the CERTs in the region and beyond. In all, 25 CERT/CSIRT teams from APCERT participated.

4.2.2 ACID 2020

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

5. Conclusion

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

As a membership-based constituency, AusCERT has increased the breadth of organisations that it serves and has been committed to its constituency, quality services and support from membership within AusCERT.

During 2020, and despite the Covid-19 pandemic, AusCERT expanded its operational capacity to provide more information and worked on capability improvement projects for the purpose of improving the value of AusCERT to its constituency.

The AusCERT instance of Malware Information Sharing Platform (MISP), continued to prove itself as a valuable member resource through 2020.

It comes as no surprise to everyone that 2020 has been a particularly challenging year. As a team, we've summarised our key achievements and milestones via the following blogpost which we released late last year.

The point that AusCERT would like to reiterate here is that collaboration and staying connected is even more important than ever, and that is why when we turned towards 2021 and re-defined our strategic goals, Engagement – was one of three key points.

Our other two strategy points cover Cyber Threat Intelligence and Incident Response, which forms the core business of a modern CERT.

bdCERT

Bangladesh Computer Emergency Response Team – Bangladesh

1. Highlights of 2020

1.1 Summary of major activities

In 2020, bdCERT conducted Incident Handling and published alerts on latest cyber threats, vulnerabilities, and best practices.

2. About bdCERT

2.1 Introduction

bdCERT is the Computer Emergency Response Team for Bangladesh and is the primary Point of Contact for handling incidents in Bangladesh. We work for improving Internet security in the country. We provide information about threats and vulnerabilities that could affect the users. We work closely with various organizations and associations such as ISPAB, BASIS, BCS, SANOG, BTRC and Law Enforcement Agencies to stop attacks that are either sourced from Bangladesh or outside. We provide training and awareness programs on Information Security and issues affecting Internet security in Bangladesh.

2.2 Establishment

bdCERT was formed in July 2007. It is a non-government and not for profit organization and our members work on voluntary basis. It was founded by few motivated network professionals working in Internet service providing companies for long years. We had been affected by virus attacks and cybercrimes, but we did not know how to deal with it until we came across the idea of CSIRT. Thus, we came together and formed bdCERT to handle cyber incidents in the country.

2.3 Resources

Since we are a voluntary organization, we often face resource scarcity. Currently bdCERT consists of 6 working team members. We provide security alerts to users via website and mailing lists.

2.4 Constituency

The constituencies of bdCERT are all the Internet user community of Bangladesh. We work closely with all the ICT stake holders particularly with ISP Association of

Bangladesh (ISPAB). We have close working relations with relevant government bodies and law enforcement agencies to mitigate Internet threats.

3. Activities & Operations

3.1 Scope and definitions

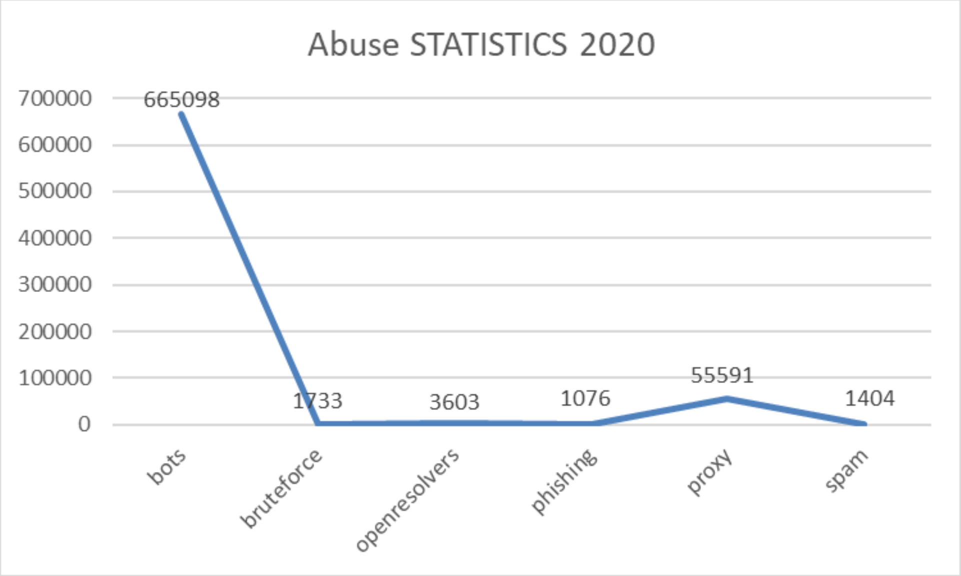
bdCERT works for improving cyber security in Bangladesh by collaborations with domestic and foreign partners. We provide Incident Handling, early warning, and awareness programs.

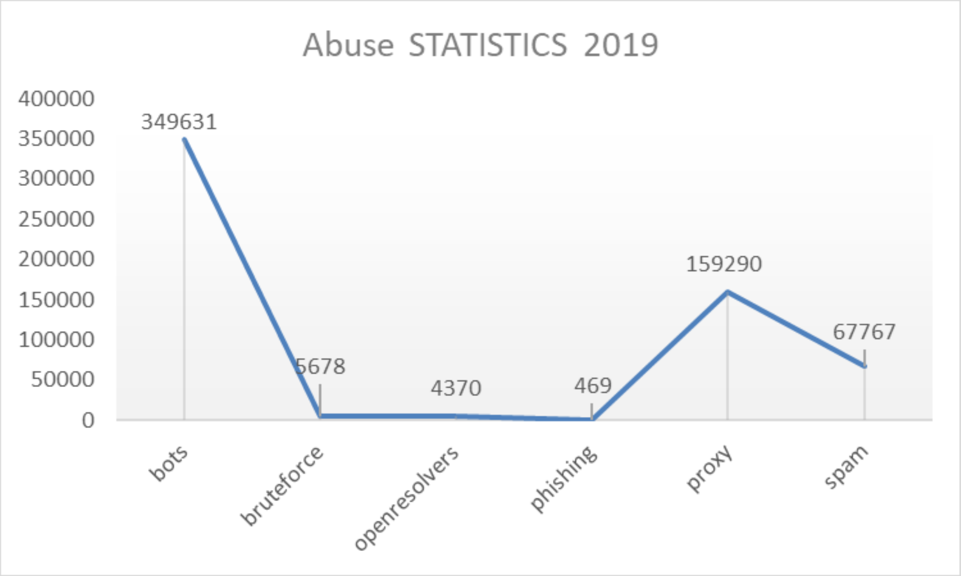
3.2 Incident handling reports

We have received good number incidents on abuse on Social media, Phishing websites and website defacement. We have received about 1000 phishing attack incident report and helped our community to mitigate the incidents. We communicated with stake holders for the incidents and helped to resolve the issues.

3.3 Abuse statistics

We analyze IOCs data in our data management platform. According to the report it shows there is huge number of bots infected hosts in this economy, which led to good number of DDoS incidents. We observe ISPs and Internet users affected with the incidents. Compared to statistics with 2019, number of bots has creased by double fold. Brute force and Phishing attack also were major concern throughout the year. In our statistics we good very small number of spam incidents. Number of Open Proxy also reduced with good numbers, mostly misconfiguration in Mikrotik or other SOHO routers led to open proxy incidents.





3.4 Publications

We did not publish our own publications in this year.

3.5 New services

We are planning to implement a DNS firewall in our platform for the internet users of the economy. As we are seeing good number bots in our economy, we are planning to filter the bots traffic to the C2Cs from DNS infrastructure. Currently we are preparing our infrastructure and will be implemented by next year.

4. Events organized / hosted

Due to Covid-19 pandemic and resource constraint we were unable to organize any events.

5. International Collaboration

5.1 Capacity Building

5.1.1 Training

Participated in numerous distance training conducted by OIC-CERT & APCERT.

Remote Working Security conducted by aeCERT on 29-Apr-2020 was most useful in view of Covid-19 pandemic.

5.1.2 Drills & exercises

Due to resource scarcity, we were unable to participate in the Drill this year.

5.1.3 Seminars & presentations

Participated in Online Conference on CNCERT International Partnership in Emergency Response conducted by CNCERT on 16-Dec-2020.

Collaborated with Military Institute of Science and Technology in preparing their research paper on *Recent Cyber Attacks and Cyber Security Strategies in Bangladesh: A Critical Analysis*

6. Future Plans

- Increase organizational capacity.
- Enhancing CSIRT services.

7. Conclusion

Our aim is to for all Bangladeshi Internet users to better understand and stay resilient to cyber-attacks. We collaborate with international partners so that we can contribute to greater global cyber security.

BGD e-Gov CIRT

Bangladesh e-Government Computer Incident Response Team - Bangladesh

1. Highlights of 2020

1.1 Summary of major activities

- BGD e-GOV CIRT has successfully organized country's First National Cyber Drill 2020.
- BGD e-GOV CIRT has successfully organized Cyber Drill 2020 for Financial Institutes to strengthen their incident handling process.
- Bangladesh has improved eight places to rank 65th among 160 countries on the National Cyber Security Index.
- "COVID-19 Minimizing IT data center risk plan Report" has been prepared.
- Blockchain Technology Based Certificate Management and Verification System has been developed.
- 1119 cyber security incident registered in our tracking system.
- Total 1145 government, non-government and other officials have been trained about cyber security.

1.2 Achievements & milestones

- BGD e-GOV CIRT took part in annual Capture The Flag (CTF) organized by FIRST.Org and achieved 19th position among 278 teams from all over the world.
- BGD e-GOV CIRT has successfully participated on OIC-CERT Cybersecurity Drill 2020 and achieved 85% Score.

2. About CSIRT

2.1 Introduction

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

2.2 Establishment

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

2.3 Resources

Currently 16 people are working in BGD e-GOV CIRT and more people will join.

2.4 Constituency

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

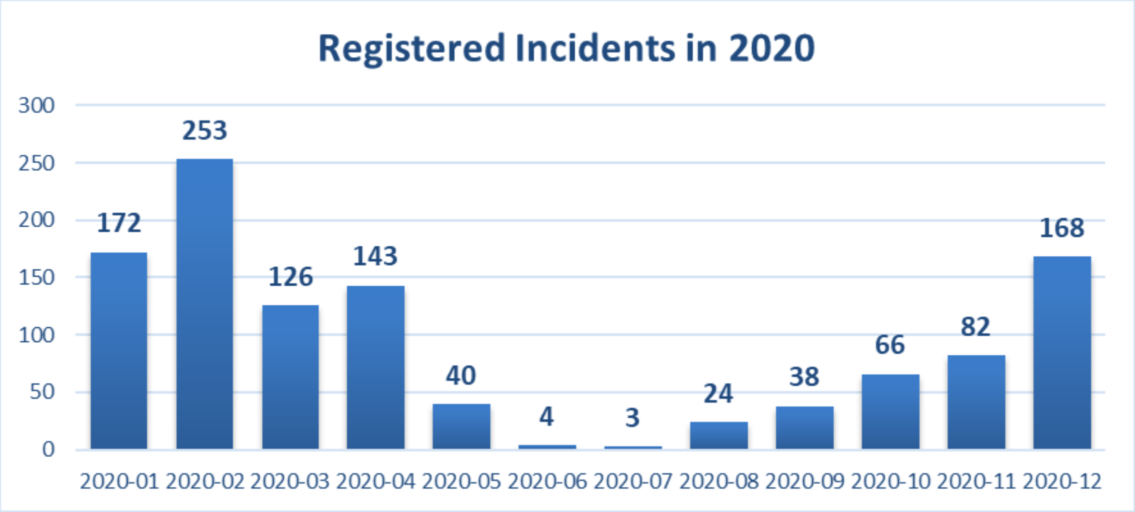
3. Activities & Operations

3.1 Scope and definitions

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

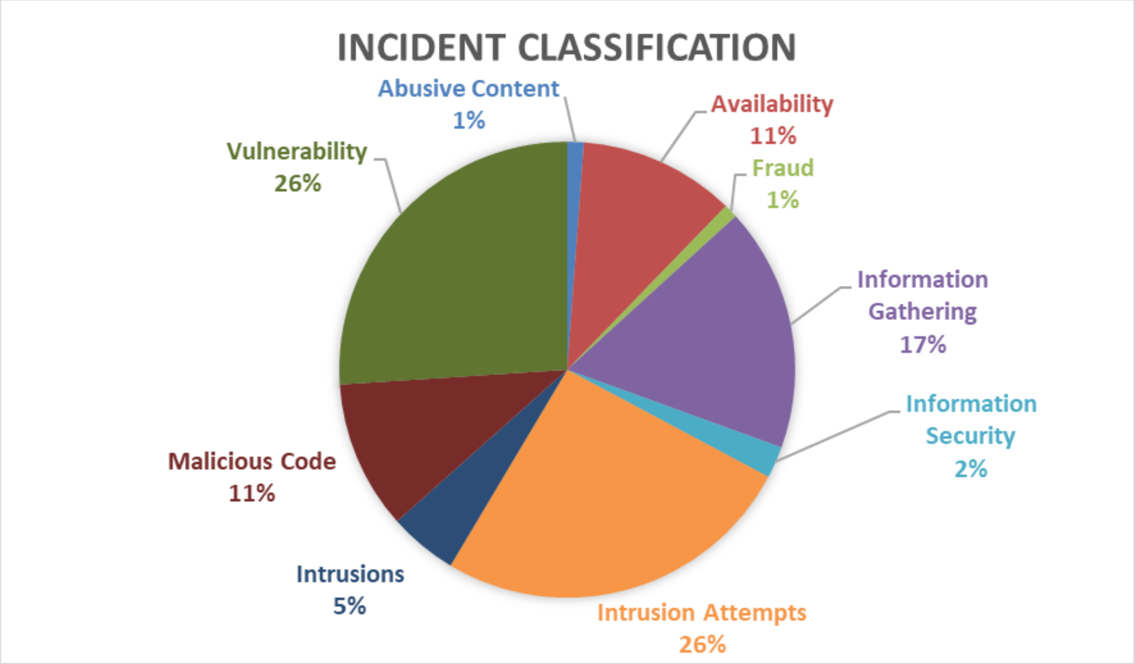
3.2 Incident handling reports

BGD e-GOV CIRT receives information regarding cyber security incidents, triage incidents and coordinate response. Activities related to incident handling includes and not limited to Vulnerability Assessment, Penetration Test, Incident Analysis, Security Threat Notification and Incident Coordination etc. In 2020 we have registered 1119 incidents in our tracking system.



3.3 Abuse statistics

Most common cyber threats observed in Bangladesh are website defacement, crypto mining, ransomware, phishing, DDoS etc.



4. Events organized / hosted

4.1 Training

- Online workshop on Cyber Threat Landscape of Bangladesh
- Training session on Cybercrime, social media awareness & security measures held in the Department of Women Affairs.

- Hands-on training session on DNS & DNSSEC Deployment.
- Special training on Cyber Security, arranged by Startup Bangladesh.

4.2 Drills & exercises

- BGD e-GOV CIRT has successfully organized country's First National Cyber Drill 2020.
- BGD e-GOV CIRT has successfully organized Cyber Drill 2020 for Financial Institutes to strengthen their incident handling process.
- Conferences and seminars

5. International Collaboration

5.1 Capacity building

5.1.1 Training

- Participated in "The Global Cybersecurity Forum Conference-2020" held in Riyadh, Saudi Arabia.
- Attended Program on Cyber Security Studies arranged by George C. Marshall European Center for Security Studies (Online)
- GCCD Cybersecurity Seminar organized by KISA (Online)
- Cyber Security Capacity Building Conference 2020, Australia
- Participated in "Empower the Modern IT with Integrated Security Portfolio" held in Thailand.
- Participated in "Modernizing your cyber security architecture: towards professional CSIRT/SOC" held online.
- Participated in "Cellebrite Analytics Desktop" & "Cellebrite Byte-size Learning" held online.
- Participated in the 2020 APISC Security Training Course by Kr-CERT/CC.

5.1.2 Drills & exercises

- Participated in annual Capture The Flag (CTF) organized by FIRST.Org
- Participated in OIC Drill 2020

6. Future Plans

6.1 Future Operation

- Arrange Cyber Drills for different sectors.

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

7. ATTACHMENT (Photos)

Figure 1: BGD e-GOV CIRT SOC visited by Hon'bl ICT State Minister

Figure 2: National Cyber Drill 2020 prize awarding ceremony inaugurated by Hon'bl ICT State Minister

Figure 3: BGD e-GOV CIRT Team meeting with Hon'bl ICT State Minister

Figure 4: National Cyber Drill 2020 visited by Bangladesh Air Force Officials

Figure 5: National Cyber Drill 2020 organizer team BGD e-GOV CIRT

Figure 6: Participated in the 2020 APISC Security Training Course by Kr-CERT/CC

Figure 7: Training session on Cybercrime, social media awareness & security measures

BruCERT

Brunei Computer Emergency Response Team – Negara Brunei Darussalam

1. About BruCERT

1.1 Introduction

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

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

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

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

1.1.1 BruCERT Services

- 24X7 Security Related Incidents and Emergency Response from BruCERT.
- 24X7 Security Related Incidents and Emergency Response onsite (Deployment response is within 2hrs after an incident is received). This service only applies to BruCERT Constituents.

- Broadcast alerts (Early Warning) of new vulnerabilities, advisories, viruses and Security Guidelines from BruCERT Website. BruCERT Constituents will receive alerts through email and telephone as well as defense strategies in tackling IT Security related issues.
- Promote Security Awareness program to educate and increase public awareness and understanding of information security and technical know-how through education, workshop, seminar and training.
- Coordinating with other CERT, Network Service Providers, Security Vendors, Government Agencies as well as other related organization to facilitate the detection, analysis and prevention of security incidents on the internet.

1.2 BruCERT Establishment

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

1.3 BruCERT Workforce

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

1.4 BruCERT Constituents

BruCERT has close relationship with Government agencies, 2 major ISPs and various numbers of vendors.

Government Ministries and Departments

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

E-Government National Centre (EGNC)

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

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

1.5 BruCERT Contact

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

Telephone: (673) 2458001

Facsimile: (673) 2458002

Email: cert@brucert.org.bn
reporting@brucert.org.bn

website: www.brucert.org.bn

www.secureverifyconnect.info

2. BruCERT Operation in 2020

2.1 Incidents response

In 2020, BruCERT had received a lot of reports from the public as well as from BruCERT security Intelligent sensors. Malware Infection is the most common cyberthreats upon Brunei Darussalam, there are few cases involving Ransomware especially the "Ryuk" type of ransomware. There is an increase in DOS attack as well as Reconnaissance in Brunei from the previous year. The statistic of the security incident is shown as Figure 1.

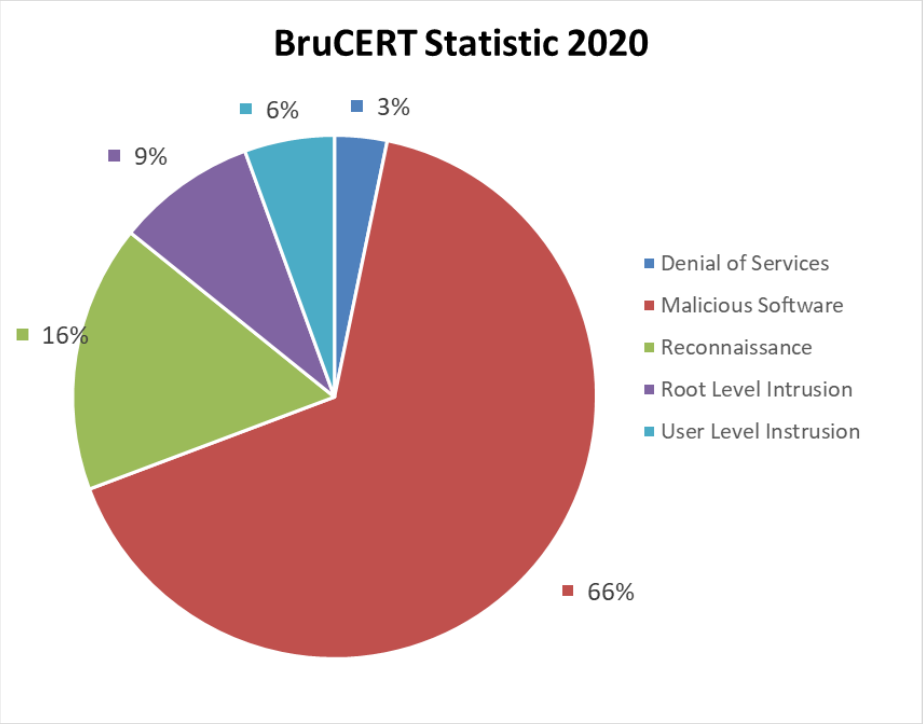


Figure 1

Types of Attack	Count
Denial of Services	174
Malicious Software	3553
Reconnaissance	889
Root Level Intrusion	465
User Level Intrusion	299

Table 1

2.2 BruCERT Honey Pot

In the year 2020, the most attack services which was recorded by BruCERT HoneyPot sensor was Samba services which is around 5505167 attacks. The grand total of attacks on services which was recorded is 7235619. Please refer to Figure 2 and Table 2 for more detail.

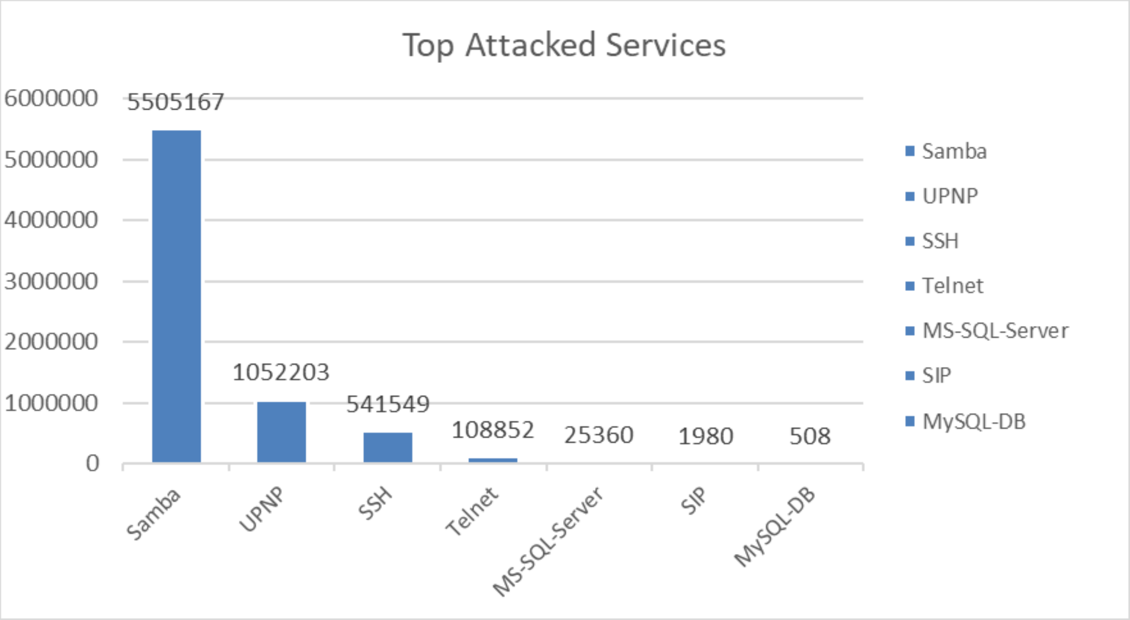


Figure 2

Event Type	Count
Samba	5505167
UPNP	1052203
SSH	541549
Telnet	108852
MS-SQL-Server	25360
SIP	1980
MySQL-DB	508
Total	**7235619**

Table 2

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

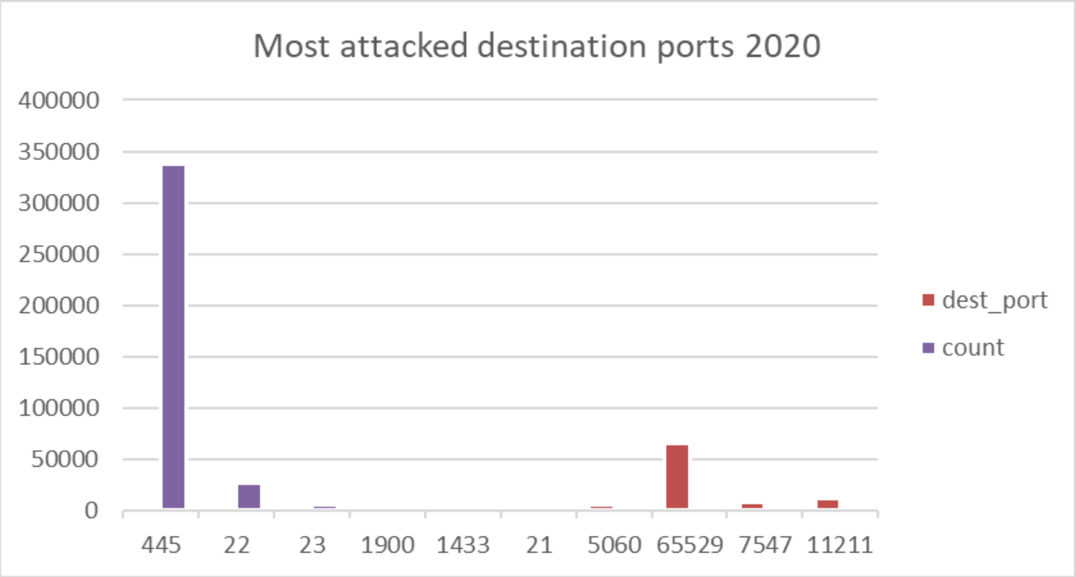


Figure 3

Port No:	Count
445	337252
22	26140
23	4777
1900	4652
1433	1707
21	939
5060	80
65529	58
7547	28
11211	24

Table 3

BruCERT honeypot managed to capture some of the malware hashes, in Figure 4 and Table 4, it show the summary of the most detected malware in BruCERT Honeypot.

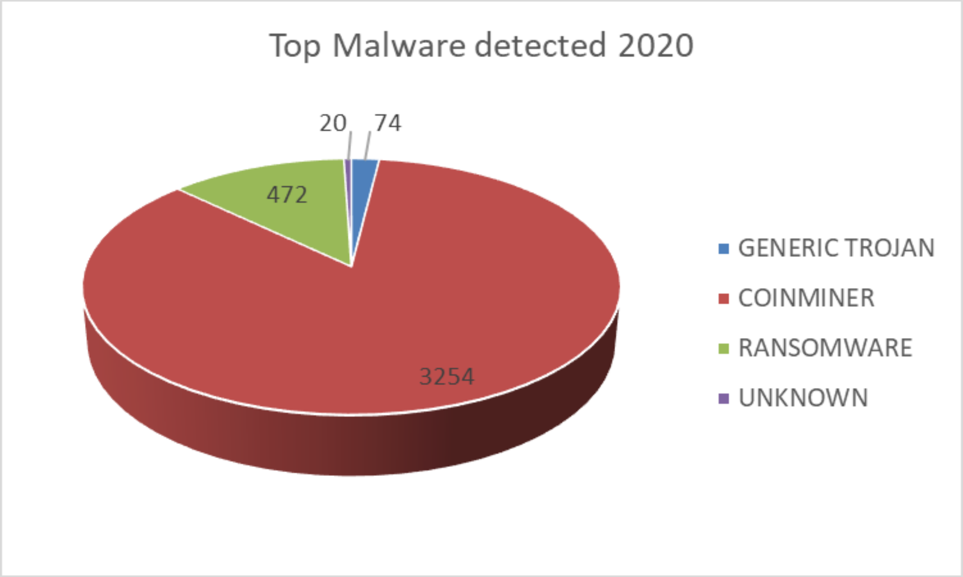


Figure 4

MALWARE TYPE	TOTAL
GENERIC TROJAN	74
COINMINER	3254
RANSOMWARE	472
UNKNOWN	20
TOTAL	**3820**

Table 4

3. BruCERT Activities in 2020

3.1 Seminars/Conferences/Meetings/Visits

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

BtCIRT

Bhutan Computer Incident Response Team – Bhutan

1. Highlights of 2020

1.1 Summary of major activities

In 2020, due to the COVID-19 pandemic, major BtCIRT activities planned for the financial year had to be shelved or postponed. Focus was therefore given to online workshops and online awareness creation considering an increase in scams and phishing attacks pertaining to COVID-19. Articles and alerts on latest cyber trends, threats, vulnerabilities and best practices were also published without any hindrances. Considerable progress has been made with regard to the Bhutan National Cybersecurity Strategy document that was spearheaded by the BtCIRT along with initiating plans for the identification of Critical Information Infrastructure in the country.

1.2 Achievements & milestones:

- Online workshop on Tools for Network & Security Analysis (2nd Dec - 4th Dec, 2020)
- Production and airing of awareness videos on national television and online platforms
- 62 advisories published on latest scams and threats
- 134 incidents handled

2. About BtCIRT

2.1 Introduction

Bhutan Computer Incident Response Team (BtCIRT) is a part of Department of Information Technology and Telecom, Ministry of Information and Communications. The overall mission of BtCIRT is to enhance cyber security in the country by coordinating cybersecurity information and establishing computer security incident handling capabilities in the country. It is also mandated to proactively monitor government systems for attacks and vulnerabilities.

2.2 Establishment

The BtCIRT was formally established on 20 May 2016 as the national central agency for cybersecurity activities and initiatives.

2.3 Resources

Currently, BtCIRT consists of 5 working team members.

2.4 Constituency

BtCIRT constituents are all government institutions which use government network infrastructure to host their IT resources and services. While BtCIRT services like awareness and reactive services are extended to all users within the country.

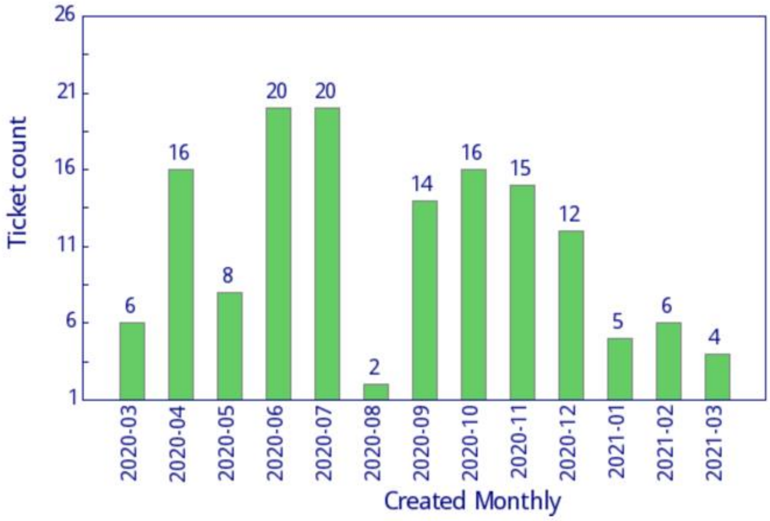
3. Activities & Operations

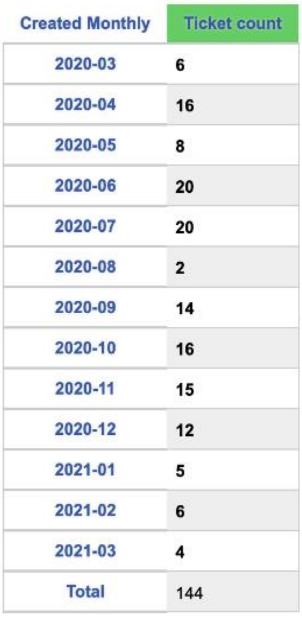
3.1 Scope and definitions:

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

3.2 Incident Handling Report

134 incidents were handled in 2020, majority of which were vulnerabilities, followed by scam incidents and malware. The following graphs provide a number of incidents resolved on a monthly basis in 2020:





Created Monthly	Ticket count
2020-03	6
2020-04	16
2020-05	8
2020-06	20
2020-07	20
2020-08	2
2020-09	14
2020-10	16
2020-11	15
2020-12	12
2021-01	5
2021-02	6
2021-03	4
Total	144

Monthly security assessment of government systems hosted at the Government Data Center.

3.3 Awareness creation:

The BtCIRT has developed 3 awareness videos covering topics related to social media phishing and scams, password security and email security and broadcasted the content on national television channels and through social media platforms.

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 (www.btcirt.gov.bt) and its Facebook page (BtCIRT).

In addition, the team also publishes advisories to assist constituents in resolving the most common threats and vulnerabilities observed. Besides, email advisory are also sent out to government and critical sector ICT officials to notify possible attacks as and when it is detected.

A total of 62 alerts and advisories were published on BtCIRT's website. Of these alerts and advisories, a significant proportion were released to address critical patches released by software vendors to fix the vulnerabilities.

4. Events organized / hosted

4.1 Training/Workshops, Drills & exercises

- Online workshop on Tools for Network & Security Analysis (Incident ResponseMonitoring with ELK & Wazuh,Intrusion Detection and Analysis with Suricata, Enterprise Honeypot & Honey tokens) in collaboration with APNIC from 2nd Dec - 4th Dec, 2020 for ICT officials from the government and private sector was conducted.
- Panel discussion on WhatsApp OTP scam and general cyber hygiene was carried out and broadcasted through the national television channel.
- A series of workshops were held with representatives from the government and corporate sectors to discuss and refine the existing draft National Cybersecurity Strategy document. Some workshops were held online during the national lockdown.
- Participated in ITU's webinar on "NCS Implementation and Monitoring" on 19th October, 2020. BtCIRT presented NCS's lessons learnt while developing Cybersecurity Strategy.
- Stakeholder workshops were conducted to kickstart identification of Critical Information Infrastructure in the country.
- The BtCIRT presented a paper on the "Cybersecurity Initiatives and Recommended areas of collaboration to remediate malware threats" during the annual BtNOG (Bhutan Network Operator's Group) Conference which happened fully virtual on 16th October 2020.

5. International Collaboration

5.1 International partnerships and agreements

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

5.2 Capacity building

5.2.1 Trainings

BtCIRT participated and benefited from the following trainings:

Date	Title	Organiser/Trainer
25Nov-1 Dec 2020	APT Training Course on Security Measures for the Era of Artificial Intelligence	NJUPT, Nanjing, P.R. China
26 Oct – 6 Nov 2020	Cyber Network Defense & Cyber Laws (ONLINE MODE 2	ALTTC, Ghaziabad, India
26th August, 2020	Safeguarding Critical National Infrastructure (CNI) - Risks and Opportunities	ITU

5.2.2 Drills and exercises

BtCIRT participated in ITU Cyber Drill 2020 which was fully virtual. The team attended all the webinars, training and participated in all scenario based incidents.

5.2.3 Seminars, Conference & presentations

Below is the list of international events that BtCIRT participated in 2020

Date	Title	Organiser/Presenter
16-18 November,2020	FIRST Conference 2020	FIRST
20 May,2020	Network Analysis for Network Security	APNIC
28, August, 2020	Email based attacks and Mitigation	APNIC
8-10 September, 2020	APNIC 50 Conference	APNIC
17 July,2020	Incident Response & Threat Sharing	APNIC
February, 2020	APRICOT Conference 2020	APRICOT
8th September,2020	National Cybersecurity Policy: Balancing Risk and Innovation	USTTI

24th September,2020	INCD-COVID19_Experts-Round-Table-A Pandemic Threat Scenario	INCD
26th March,2020	Remote Work Challenges	CERT-IL

6. Future Plans

6.1 Future Operations

BtCIRT also looks forward to collaborating with more organisations internally and internationally to strengthen its cooperation.

- Conduct awareness programs in schools and colleges and through media outlets
- Implement National Cybersecurity Strategy
- Identify Critical Information Infrastructure and conduct risk assessments on selected CII

7. Conclusion:

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

CERT-In

Indian Computer Emergency Response Team – India

1. Highlights of 2020

1.1 Summary of major activities

a) In the year 2020, CERT-In handled 1158208 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.

b) CERT-In tracks latest cyber threats and vulnerabilities. A total of 496 security alerts, 93 advisories and 450 Vulnerability Notes were issued during the year 2020.

c) CERT-In conducted 15 cyber security training and awareness programs for Government, Public and Critical Sector organisations and communication & Information infrastructure providers to educate them in the area of Information Security with the latest security threats, needs and developments & deployment of techniques and tools in order to minimize security risk.

d) CERT-In conducted 6 domestic cyber exercises/drills and participated as a player in 7 International cyber security drills in 2020.

e) CERT-In is a convener of two APCERT working groups namely Internet of Things (IoT) Security and Secure Digital Payments.

1.2 Cyber security during Covid-19

- CERT-In incident response were operational and manned 24x7 during pandemic lock-down
- CERT-In issued 23 advisories on various topics such as Secure use of web conferencing software, Securing mobile devices and apps, Secure use of Virtual Private Network (VPN), Security Best Practices for Working from Home, security measures for Healthcare Sector, Online Safety of Children, various Phishing attack campaigns pretending to be from popular Apps and services, Securely managing Business Continuity during crisis situation due to COVID- 19 Pandemic etc.
- Over 300 threat intelligence alerts were sent to Chief Information Security Officers (CISOs) of key organizations and stakeholders in the country advising Indicators of

compromise for enabling proactive preventive actions and security cyber infrastructure at entity level

- Cyber crisis exercises were conducted for organizations during July and August 2020 to train and guide them to respond to COVID-19 pandemic related cyber-attacks wherein 73 organisations including key stakeholders participated.
- Interaction sessions were conducted with security auditing organizations to formulate security audit guidelines to continue quality audits in pandemic situations. Guidelines have been issued in public domain.
- Workshops conducted in collaboration with Data Security Council of India (DSCI) for CISOs, IT Managers, regarding threat landscape during Covid-19 and work-from-home scenario.
- Workshop on Information Security for hospitals conducted in collaboration with Consortium of Accredited Healthcare Organisations (CAHO).
- Seminar in collaboration with Confederation of Indian Industry (CII) on Cyber security threat landscape, challenges and gaps during COVID-19 and how effective public private partnerships can contribute.

1.3 Achievements & milestones

- CERT-In received the "Cyber Frontliners of the Country" award at the Data Security Council of India (DSCI) Excellence Awards 2020.
- CSIRT-Fin has been established and is operational since 15th May 2020. CERT-In is providing the requisite leadership for the CERT-Fin operations under its umbrella. In addition to responding to, containment and mitigation of cyber security incidents reported from the financial sector, CERT-In is sharing malware and vulnerability feeds on a daily basis in an automated manner with designated Chief Information Security Officers (CISOs) of the respective Financial entities, so as to enable them to take necessary proactive actions at their end for ensuring safety and security of the financial ICT infrastructure.
- Indian Computer Emergency Response Team is conducting cyber security exercises comprising of table top exercises, crisis management plan mock drills and joint cyber security exercises with organizations from key sectors to enable participating organizations to assess their preparedness in dealing with cyber crisis situations. Total of 6 such exercises were conducted in 2020.
- In 2020, CERT-In signed Memorandum of Understandings (MoUs) on cyber security

cooperation with counterpart agencies in Brazil, Israel and France to enable information sharing and collaboration for incident resolution.

- The Cyber Forensics Laboratory at the Indian Computer Emergency Response Team (CERT-In) has been notified as 'Examiner of Electronic Evidence' under section 79A of the Information Technology Act, 2000.
- CERT-In's Botnet Cleaning and Malware Analysis Centre (Cyber Swachhta Kendra) was awarded "Best of Tech 2021" by Coeus Age, supported by Microsoft in July 2020.

2. About CERT-In

2.1 Introduction

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

The Information Technology Act, 2000 designated CERT-In to serve as the national agency to perform the following functions in the area of cyber security:

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

CERT-In creates awareness on security issues through dissemination of information on its website (https://www.cert-in.org.in) and operates 24x7 incidence response Help Desk. CERT-In provides Incident Prevention and Response services as well as Security Quality Management Services.

2.2 Establishment

CERT-In has been operational since January 2004.

2.3 Constituency

The constituency of CERT-In is the Indian cyber community and Indian cyberspace. CERT-In provides services to the organizations in the Government, Public and Private sectors. In addition, CERT-In provides services to the individuals and home users also.

3. Activities & Operations

3.1 Scope and definitions

CERT-In provides:

- Proactive services such as Advisories, Security Alerts, Vulnerability Notes, sharing of Indicators of Compromise, Situational awareness of existing & potential cyber security threats and Security Guidelines to help organisations 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 2020 is given in the following table:

Activities	Year 2020
Security Incidents handled	1158208
Vulnerability Notes Published	450
Advisories Published	93
Security Alerts issued	496
Security Drills	6
Trainings Organized	15

Table 1: CERT-In Activities during year 2020

3.3 Abuse statistics

In the year 2020, CERT-In handled 1158208 incidents. The types of incidents handled were Website intrusion & Malware propagation, Malicious Code, Phishing, Distributed Denial of Service attacks, Website Defacements, Unauthorized Network Scanning/Probing activities, Ransomware attacks, Data Breaches and Vulnerable

Services.

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

Security Incidents	2020
Phishing	280
Unauthorized Network Scanning/Probing/Vulnerable Services	1028881
Virus/ Malicious Code	99986
Website Defacements	25969
Website Intrusion & Malware Propagation	152
Others	2940
Total	**1158208**

Table 2: Breakup of Security Incidents handled

Various types of incidents handled by CERT-In are given in Figure 1.

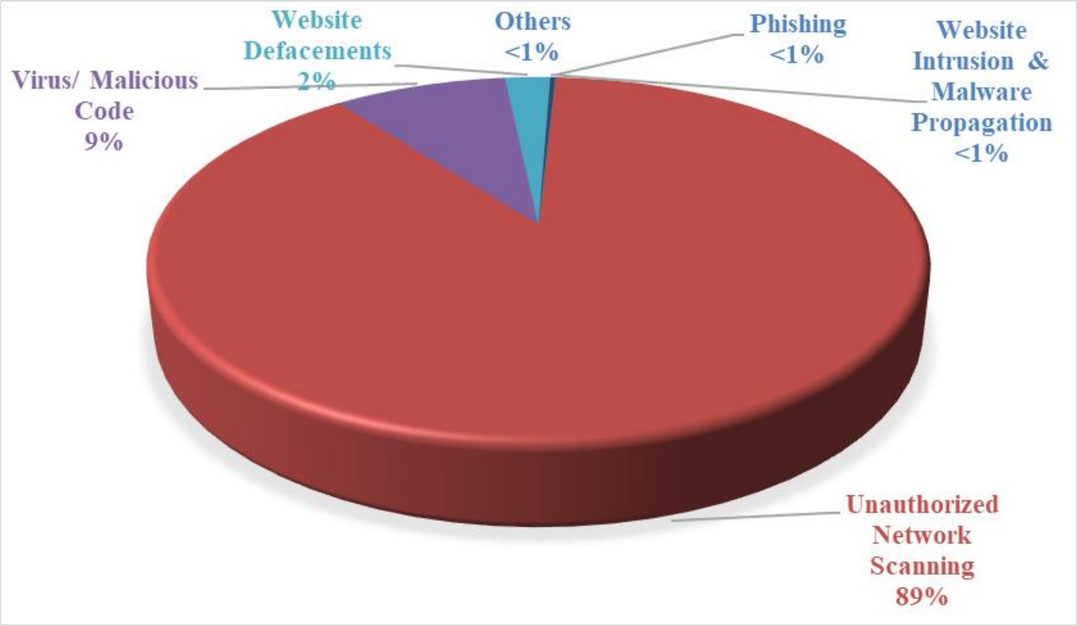


Figure 1: Summary of incidents handled by CERT-In during 2020

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 **25969** numbers of defacements have been tracked.

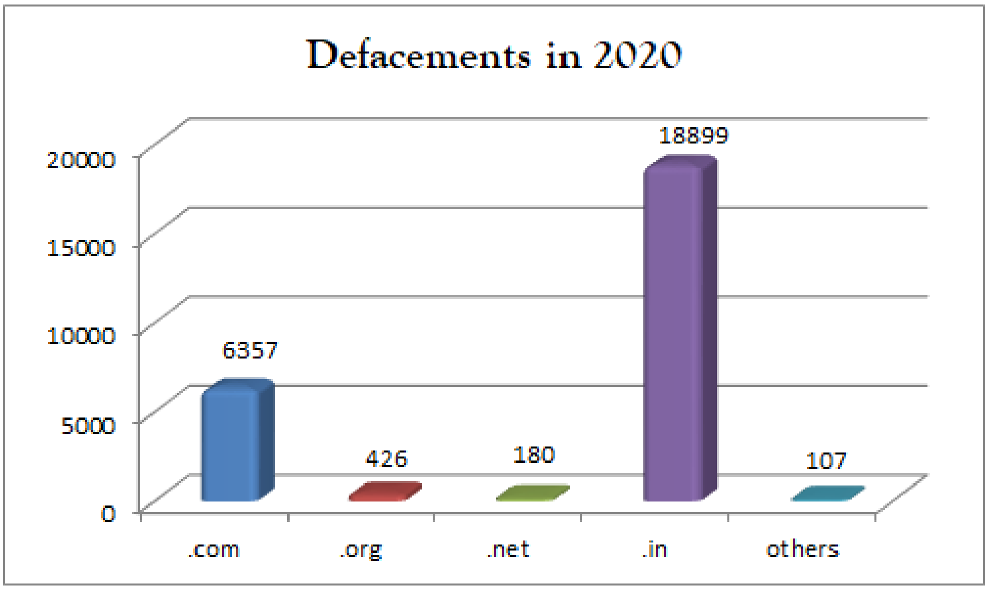


Figure 2: Indian Website Defacements tracked by CERT-In during 2020

3.3.2 Botnet Cleaning Initiatives

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

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

During October 2020, CSK participated in National Cyber Security Awareness Month (NCSAM 2020) in coordination with Internet Service Providers (ISP) and Antivirus Companies for spreading awareness and information regarding cyber security threats, challenges and safeguarding citizens against them.

CSK tracked 27,85,37,556 botnet/malware infections in India and notified end users in collaboration with Internet Service Providers and organizations.

CSK provides two Free Bot Removal Tools (FBRT) developed in collaboration with "QuickHeal" and "eScan" with 13.08 lakh downloads recorded till December 2020.

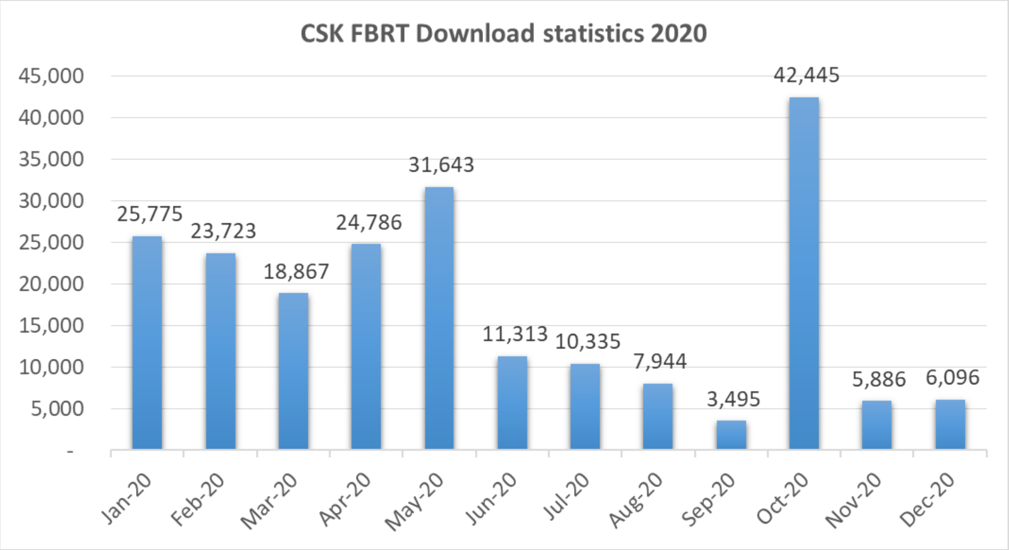


Figure 3: CSK Free botnet removal tools download statistics 2020

Botnets events processed by Botnet Cleaning and Malware Analysis Centre (Cyber Swachhta Kendra) during 2020.

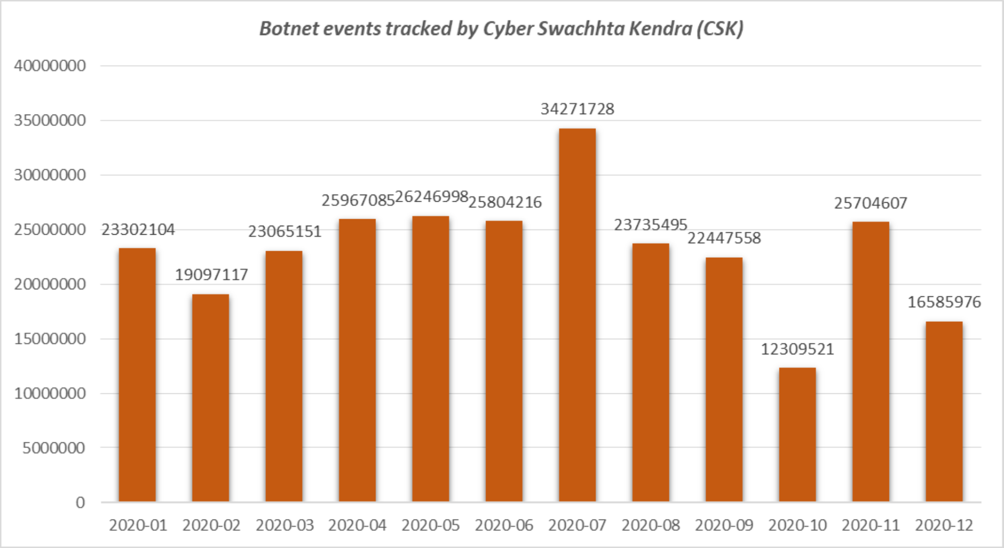


Figure 4: Botnet events tracked by Cyber Swachhta Kendra (CSK)

CSK observed rise botnet/malware infection in India during the lockdown period due to pandemic situations. This rise in infection could be caused due to increasing culture of work from home. After the lockdown period, it is again observed that the infections reduced because of proper remedial measures implemented by the users/organizations.

3.3.3 Security Profiling, Assurance framework and Audit Services

- Under Security Assurance Framework, Indian Computer Emergency Response Team (CERT-In) has created a panel of 'IT security auditing organizations' for auditing, including vulnerability assessment and penetration testing of computer systems, networks & applications of various organizations of the Government, critical infrastructure organizations and those in other sectors of Indian economy.
- Information Security Auditing organizations are empanelled on the basis of stringent qualifying criteria, to carry out information security audit, including the vulnerability assessment and penetration test of the networked infrastructure of government and critical sector organizations. This list of CERT-In empanelled auditing organizations is being consulted frequently by the entities in Government and critical sectors for their auditing requirements.
- CERT-In conducted 2 interaction sessions in June 2020 with 30 empanelled auditing organizations and prepared guidelines for conducting quality cyber security audits in COVID-19 pandemic situation. In addition, CERT-In also completed technical skills re-verification of already empanelled auditing organizations.
- Government and critical sector organizations are implementing the security best practices in accordance with ISO 27001 standard and as per the advice issued by CERT-In. Implementation enabling workshops/interactions are conducted periodically. Services of CERT-In empanelled technical IT security auditors are being used to verify compliance.
- CERT-In has also carried out episodic security audits of key organizations for enhancing their security posture.

3.3.4 Cyber threat Intelligence Sharing

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

CERT-In envisages that implementing threat intelligence profoundly elevates Government/Critical organization's security posture, enabling the respective security team to understand and effectively predict the cyber threats that imperil their organization's key assets. Empowering organizations to anticipate who may attack next, and how, allows security teams to focus on prioritizing resources so they can respond effectively to future cyber-attacks.

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

CISO's of various organizations are getting benefitted by the curated operational and tactical threat intelligence digest shared through an automated platform as well as email for some in the form of indicators of compromise largely covering Advanced Persistent Threats in Indian Cyber space.

The automated platform collects, correlates, enriches, contextualizes, analyses, integrates, tags with Traffic Light Protocol (TLP) and pushes to the partners in near real time. The shared data can be consumed by the recipients into their automated workflows so as to streamline the threat detection, management, analysis, and defensive process and track it through to completion by leveraging its powerful API integrations with supporting SIEMs, firewalls, and other endpoint protection solutions.

During the year 2020, CERT-In via its automatic platform, issued 466 alerts to its constituency.

3.3.5 National Cyber Coordination Centre (NCCC)

Continuously evolving cyber threat landscape and its impact on well being of information technology, National Economy, and Cyber Security necessitates the need for near-real time situational awareness and rapid response to cyber security incidents. Realizing the need, Government has taken steps to set up the National Cyber Coordination Centre (NCCC) to generate macroscopic views of the cyber security threats in the country.

The centre scans the cyberspace in the country at meta data level and generates near real time situational awareness. The centre is facilitating various organizations and entities in the country to mitigate cyber attacks and cyber incidents on a near real time basis.

NCCC aims to create a structured system to facilitate coordination effort among strategic stakeholders by sharing with them strategic inputs in terms of information about threats/attacks and possible extent which in turn enables immediate remedial actions by the stakeholders.

3.3.6 Cyber Forensics

Cyber Forensics Lab at CERT-In is equipped with the equipment and tools to carry out 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. In addition, Cyber Forensics Lab is being utilised 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.

Scientists at Cyber Forensic Lab impart training through training workshops organised by CERT-In on computer forensics and mobile device forensics through lectures, demonstrations and hands on practical sessions, which covers seizing, preservation, processing and analysis of the raw data extracted from the digital items. CERT-In also supports other institutes in imparting trainings on various aspects of cyber forensics by delivering lectures along with demonstrations.

3.4 Events organized / hosted

3.4.1 Security awareness, skill development and 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. This year due to the lockdown caused by the COVID pandemic and subsequent restrictions and the government guidelines of minimizing the gathering of people, CERT-In carried out online trainings/workshops on various issues relating to cyber security.

During the period January 2020 - December 2020, CERT-In has conducted 15 trainings on various specialized topics of cyber security. 708 officers 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.

CERT-In undertook mass citizen outreach campaign through websites and social media channels during the National Cyber Security Awareness Month – October 2020, including via Doordarshan TV channels.

3.4.2 Cyber Security Exercises

Cyber security exercises are being conducted by the Government 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 6 such cyber security exercises in 2020.

CERT-In regularly conduct Cyber Security Exercises for critical sector organizations.

- **“Black Swan” Series of Exercises to counter COVID-19 pandemic induced disruptions and cyber-attacks**

COVID-19 pandemic has caused changes in workplace-culture, data flow and infrastructure of the organizations. CERT-In conducted 3 “Black Swan” Cybersecurity Breach Table Top Exercise on COVID-19 pandemic themed cyber-attacks to sensitize organizations to counter disruptions and cyber-threats in July 2020 to August 2020. 73 organizations including key stakeholders and critical organizations participated in these exercises.

- **Sectoral Cyber Security Drills – FinEx-2020 and TransEx-2020**

CERT-In along with RBI conducted FinEx-2020, a 2 days' exercises on Advanced Persistent Threats for 69 urban cooperative banks in February 2020. Banks were trained for enhancing their cyber monitoring capabilities and incident response to the cyber crisis. Indian Cyber Crisis Exercise (ICCE) - a 3 phased cyber security crisis exercise for 23 cooperative banks has been conducted by CERT-In on "Evolving Cyber Threats in banking Sector". Exercise helped participants to build Incident Response capabilities against emerging cyber threats. CERT-In also conducted TransEx2020 for 50 power sector utilities in February 2020 on hypothetical cyber crisis scenario in which disruption and destruction to the control systems was the primary theme. Exercises helped entities to understand and prepare their cyber crisis management plan.

4. International Collaboration

4.1 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 2020, CERT-In signed bilateral agreements on cyber security cooperation with counterpart agencies in Brazil, Israel and France 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 two working groups across APCERT namely "IoT Security working group" and "Secure Digital Payments working group" to address security threats and evolve best practices to secure these domains. The first report of the "Secure Digital Payments" working group was completed and circulated to the APCERT operational members.

CERT-In is also member of various other working groups under APCERT such as Drill working group and Malware Mitigation working group.

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

4.2 Drills & exercises

CERT-In participated in the APCERT Annual drill 2020 in March 2020 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 this year's APCERT Drill was "Banker doubles down on Miner – Data Breach via cyber-attacks". CERT-In also acted as exercise coordinator (EXCON) for international CERTs in the Drill.

CERT-In participated in the Organization of Islamic Cooperation – Computer Emergency Response Teams (OIC-CERT) Cyber Security Drill in September 2020. This year theme of the exercise was 'Remote working and cyber threats'.

CERT-In participated in ASEAN CERT Incident Drill (ACID) – 2020 in October 2020. The theme of this year's ACID Drill was 'Malware Campaign Leveraging the Pandemic situation'.

CERT-In participated in 6 days International Telecommunication Union (ITU) 2020 Global Cyber Drill in October and November 2020. This year theme of the Drill was 'Cyber threats and Challenges around Healthcare Sector due to Covid-19 Pandemic'.

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

CERT-In participated in the International CyberEx 2020 a Capture the Flag (CTF) exercise which includes several categories of challenges, such as forensics, exploitation, cryptography and reverse engineering organized by the National Cybersecurity Institute of Spain (INCIBE), the Organization of American States (OAS) and the National Center for Infrastructure Protection and Cybersecurity of Spain (CNPIC) for Computer Security Incident Response Teams around the globe. This international cybersecurity competition for Computer Security Incident Response Teams helped participants to strengthen their response and technical analysis capabilities to cyber incidents.

CERT-In participated in 2 days (4 scenarios) International Telecommunication Union (ITU) Pacific Cyber Drill 2020 in December 2020. The theme of this years' drill was 'COVID-19 pandemic situation affecting information and communication technologies (ICTs)'.

4.3 Other international activities

- CERT-In was a member of "Cyber Threat Signal 2021" publication working group. Cyber Threat Signal 2021 is a joint collaborative work of CERT-In along with AusCERT (Australia CERT), KrCERT/CC (South Korea CERT) and Sri Lanka CERT|CC (Sri Lanka CERT) regarding the most pertinent cyber threats that could be witnessed in the year 2021.
- CERT-In presented a research paper on "Metrics for Country-wide Cyber Security Assurance: Experiments and Experiences of Indian Computer Emergency Response Team (CERT-In)" at National Computer Security Incident Response Team (NatCSIRT), Carnegie Mellon University (CMU) for participants from Global CERTs in December 2020.
- CSIRT-Fin is participating in BRICS Rapid Information Security Channel (BRISC) formed as part of BRICS cooperation in the sphere of information security in the banking and finance sector.
- Financial Stability Board (FSB): CSIRT-Fin is contributing to the "Effective Practices for Cyber Incident Response and Recovery" toolkit. This is a range of effective security practices for financial institutions to respond to and recover from a cyber incident to limit any financial stability risks as envisaged by G20 Finance Ministers and Central Bank Governors.
- CERT-In participated in the Asia Pacific Computer Emergency Response Teams (APCERT) Annual General Meeting (AGM) in Virtual Mode held on 29th September

2020.

- CERT-In attended FIRST Annual General Meeting (AGM) 2020 (Virtual) held on 25th June 2020.
- CERT-In participated in Virtual 5th Singapore International Cyber Week (SICW) held during 5 - 9 October 2020.
- CERT-In participated in FIRST Annual Conference 2020 (virtual) held during November 16-18, 2020.
- CERT-In participated in 15th Annual Technical Meeting for CSIRTs with National Responsibility (Virtual) during December 8-9, 2020.
- CERT-In participated in APCERT Online Training on ATM Cyber Attack on 1st December 2020.
- CERT-In participated in APCERT Online Training on Digital Forensics Procedures & Interesting Artifacts held on 11th August 2020.
- CERT-In participated in APCERT Online Training on Identification of information security risks as a sectoral CSIRT and addressing the risks held on 18th February 2020.
- CERT-In participated in FIRST Security Sessions at APNIC 50 (online) held on 9th September 2020.
- CERT-In participated in OIC-CERT 12th Annual Conference 2020 (Virtual) held during 23-24 November 2020.
- CERT-In participated in the Sri Lanka CERT Cyber Security Week 2020 held online from 19 to 22 October 2020.
- CERT-In participated in Global Cybersecurity Center for Development (GCCD) Cybersecurity Seminar 2020 held from 14 to 25th of September 2020.
- CERT-In participated in AVAR Annual Conference 2020 Virtual held during 3rd to 5th December 2020.

5. Collaboration with Industry

CERT-In signed 4 Memorandum of Understandings (MoU) for collaboration in the area of cyber security with Information Sharing and Analysis Center (ISAC), MicroWorld Technologies, K7 Computing and Kaspersky.

Contact Information

Postal Address:

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

Incident Response Help Desk:

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

Incident report to Incident Response Help Desk at:

Email: **incident@cert-in.org.in**
PGP Key Details:
User ID: incident@cert-in.org.in
Key ID: 0xB620D0B4
Key Type: RSA
Expires: 2021-05-24
Key Size: 4096/4096
Finger Print: A768 083E 4475 5725 B81A A379 2156 C0C0 B620 D0B4

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

Email: **info@cert-in.org.in**
PGP Key Details:
User ID: info@cert-in.org.in
advisory@cert-in.org.in
subscribe@cert-in.org.in
Key ID: 0x275CCACF
Key Type: RSA
Expires: 2021-05-24

Key Size: 4096/4096

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

Email: **csk@cert-in.org.in**

PGP Key Details:

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

Key ID: 0x4EE11788

Key Type: RSA

Expires: 2022-05-31

Key Size: 4096/4096

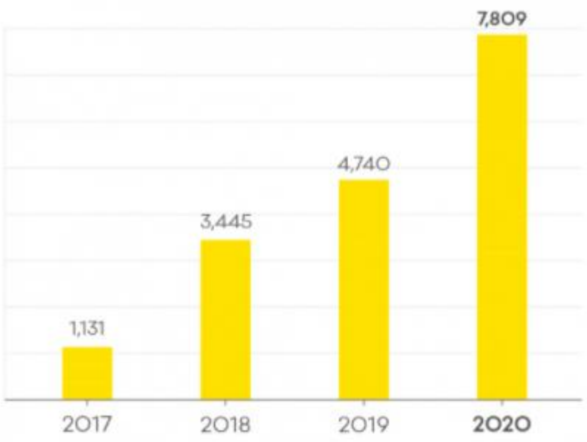
Finger Print: E204 D43D 0296 40FB 8DB9 0290 706D EF4D 4EE1 1788

CERT NZ

CERT NZ – New Zealand

1. Highlights of 2020

- In 2020, a total of 7,809 incidents were reported to CERT NZ, a 65% increase on 2019



- CERT NZ's key annual awareness-raising activity, Cyber Smart Week, was held for the fourth year running, on 19 to 23 October 2020
- We also ran a Trade Smart" campaign targeted at the growing number of businesses going online. We ran this in conjunction with Consumer Protection, New Zealand's agency responsible for informing and educating buyers.
- CERT NZ continues to strengthen its partnerships in the Pacific, including chairmanship of the capacity building working group as a member of the Pacific Cybersecurity Operational Network (PaCSON).

2. About CERT NZ

2.1 Introduction

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

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

2.2 Resources

CERT NZ is a branded business unit within the Ministry of Business, Employment and Innovation. It has 33 FTEs, including operations, communications & engagement, governance & analytical reporting staff. CERT NZ also has a contact centre to receive incident reports.

3. Activities & Operations

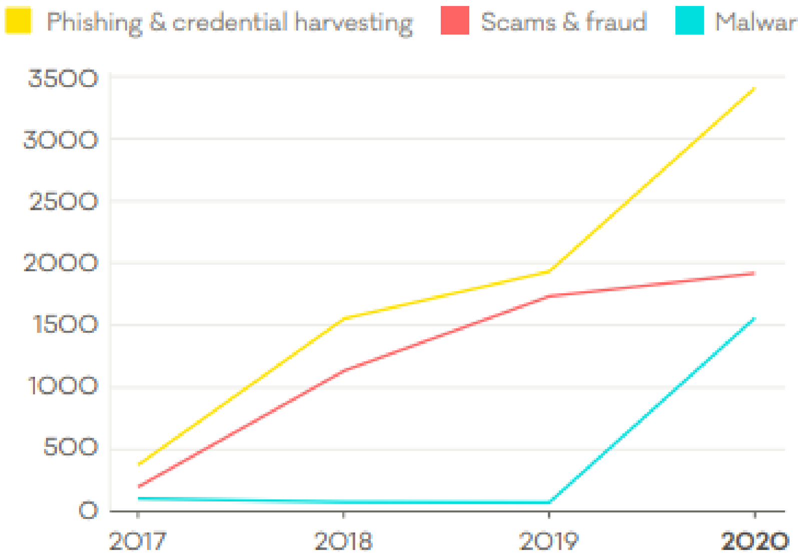
3.1 CERT NZ's key services are:

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

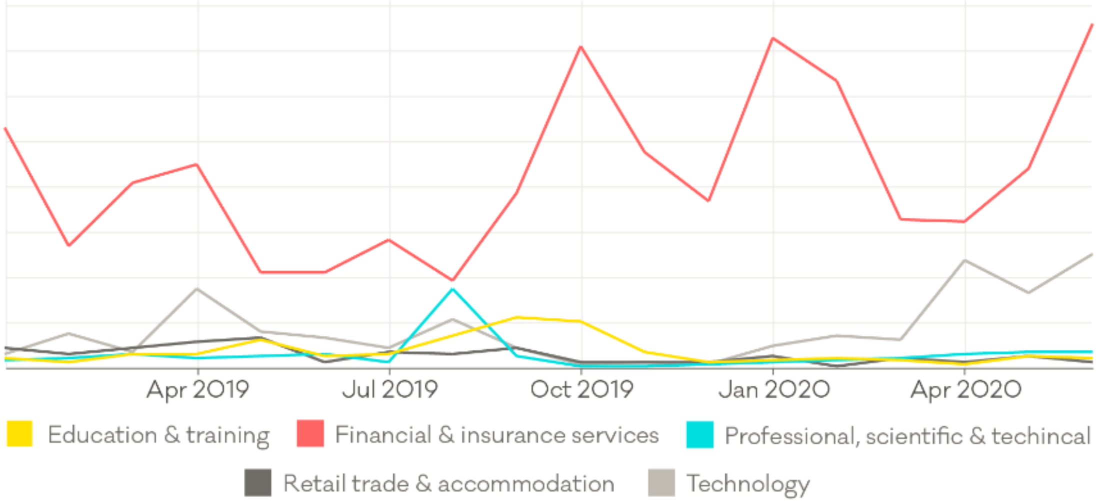
3.2 Top incident categories

Malware has replaced unauthorised access in the top three categories in 2020, with 'Phishing & credential harvesting' and 'Scams & fraud' remaining

CERT NZ received 3,410 Phishing and credential harvesting reports in 2019, up 76% on 2019.



The financial and insurance sector continued to see the largest number of reports. There was a notable increase in reports from the technology sector coinciding with the lockdown in New Zealand.

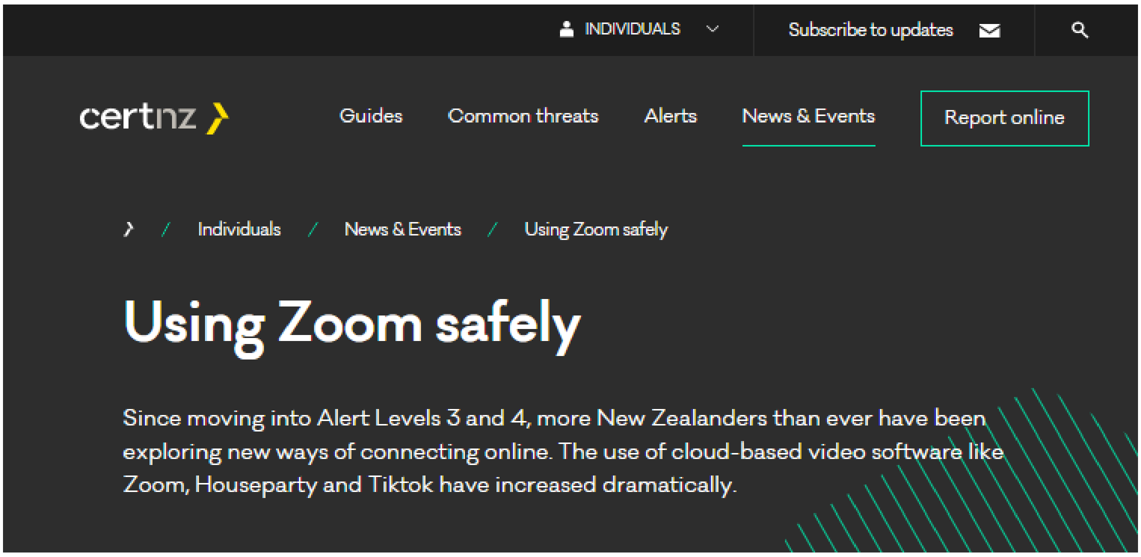


3.3 Publications

CERT NZ’s quarterly reporting continued in 2020, with the publication of two reports each quarter:

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

2020 saw CERT NZ publish our updated critical controls which included "securing internet exposed services" as a control for the first time. CERT NZ also published numerous pieces of content in response to people shifting to remote working arrangements due to the COVID-19 Pandemic.



Using Zoom safely

Since moving into Alert Levels 3 and 4, more New Zealanders than ever have been exploring new ways of connecting online. The use of cloud-based video software like Zoom, Houseparty and Tiktok have increased dramatically.

3.4 Social Media

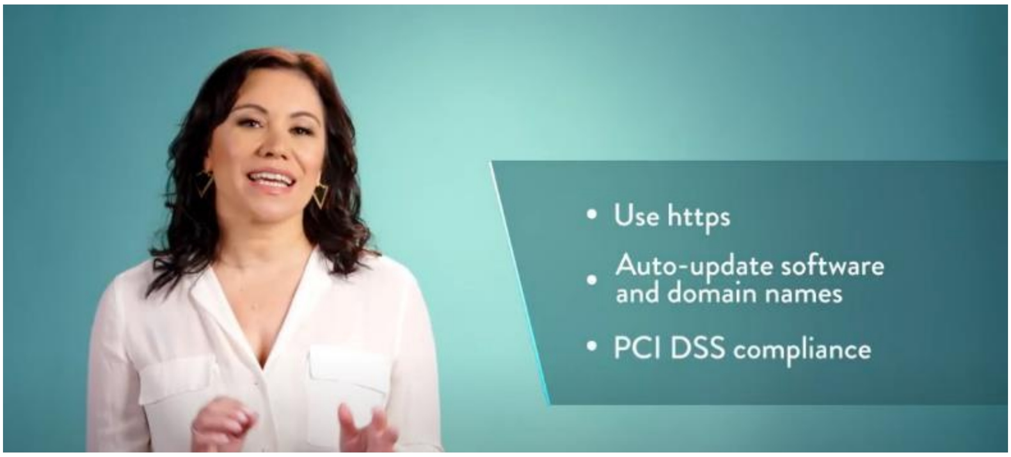
CERT NZ has increased its use of social media in 2020 as a way to reach our constituency. As well as building on our existing use of Twitter (@CERTNZ) CERT NZ launched a Facebook page in October 2020 - https://www.facebook.com/certnzgovt

4. Events organized / hosted

4.1 Campaigns

CERT NZ ran its fourth cyber security awareness campaign, Cyber Smart Week, in October 2020. CERT NZ engaged with partners from across the government and private sectors to share the four simple steps all New Zealanders could take to be more secure online. During the campaign, CERT NZ worked with 122 partner organisations, achieving a combined 5 million impressions. A wide range of resources – from graphics to editorial content – were available for partners to use and share, with the backing of CERT NZ.

For the first time CERT NZ ran a campaign, Trade Smart online, specifically targeted at businesses. This was a joint campaign with Consumer Protection, which promotes secure online trading and shopping practices among businesses and consumers. The campaign was heavily online but also included television ads.



- Use https
- Auto-update software and domain names
- PCI DSS compliance

5. International Collaboration

5.1 International partnerships and agreements

5.2 Capacity building

CERT NZ led the PaCSON Capacity Building Working Group and is working with Pacific partners as part of a wider New Zealand government commitment to support cyber security capacity building across the Pacific region. A great success of this work has been the PaCSON remote session series which allowed us to continue to deliver training while border restrictions are in place.

CERT NZ also participated in two global cyber exercises which helped us test out national and international ability to respond to cyber security incidents.

5.3 Other international activities

Key International presentations:

- GFCE – Pacific Regional Forum
- Strengthening Digital security workshop- Samoa
- EU Cyber Forum 2020
- East Asia Summit Regional Cyber capacity building workshop
- NatCSIRT
- APISC training
- PaCSON remote session series – 10 session's throughput 2020 covering 190+ participants across 16 economies. Including collaboration with two APCERT economies
- Digital Pacific Conference
- Cyber Safety Pasifika.

6. Contact information

Website:

www.cert.govt.nz

Twitter:

@CERTNZ

Facebook:

https://www.facebook.com/certnzgovt

By post:

CERT NZ
PO Box 1473
Wellington 6140

By phone (to report an incident):

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

CERT-PH

Philippines National Computer Emergency Response Team – Philippines

1. Highlights of 2020

1.1 Summary of major activities

- Strengthen information sharing thru the issuance of daily cyber threat feeds to different agencies and security advisories to the public
- Performed Vulnerability Assessment and Penetration Testing to web and mobile applications developed to help fight COVID-19 in the Philippines
- Issuance of security advisories and feeds on COVID-19 related cyber threats and Security Practices for Telecommuting.
- Issuance of Guidelines on CERT-PH Incident Reporting and Request for Technical Assistance on Information Sharing and Analysis to Law Enforcement Agencies during the Declared State of Public Health Emergency in the Philippines in April 2020
- Conducted National Cyber Drill Exercise 2020 with the theme "Strengthening Cybersecurity and Adapting to the New Normal through Incident Response and Collaboration"
- Participation to training, drills, and exercises via online platforms

1.2 Achievements & milestones

- Issuance of Department Circular 003 which further strengthen the establishment of the National Computer Emergency Response Team Division of the Department Information and Communications Technology (DICT) as the Philippines National Computer Emergency Response Team (CERT-PH)
- Became an operational member of the Asia Pacific Computer Emergency Response Team (APCERT)

2. About CERT-PH

2.1 Introduction

The Philippines National Computer Emergency Response Team (CERT-PH) is responsible for receiving, reviewing, and responding to computer security incident reports and activities. CERT-PH monitors the implementation of the information security incident response plan to ensure that detected and reported cybersecurity incidents and events are given appropriate and immediate response.

2.2 Establishment

CERT-PH was established and began its operation in 2018. The establishment of CERT-PH was strengthened through the DICT Department Circular 003 issued in March 2020.

2.3 Resources

CERT-PH currently has 12 full-time employees. The operational funding comes from the Department of Information and Communications Technology – Philippines.

2.4 Constituency

CERT-PH shall lead, manage, and oversee the various Government, Sectoral and Organizational CERTs within the Philippines.

3. Activities & Operations

3.1 Scope and definitions

CERT-PH's key services are:

A. Security Operations Center Section

- Administers the operations of the Cybersecurity Management System Project (CMSP);
- Serves as a centralized facility for detection, monitoring and rapid response to security incidents in the connected agencies
- Responsible in monitoring, detecting, analyzing, remediating and information sharing of computer security incidents within the priority agencies

B. Incident Response Section

- Respond to cybersecurity incidents reported and detected by the team;
- 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.

C. Digital Forensics Section

- Conduct Vulnerability Assessment and penetration testing to Government Agencies;
- Provide technical details and analysis of discovered vulnerabilities and criticality to systems owner;
- Examine and evaluate web and network assets to identify security deficiencies.

D. Cyber Threat Monitoring Section

- Collect and analyze data from publicly available sources and feeds regarding cyber threats;
- Collaborate with international and local communities and organization on existing and new threats in cyberspace;
- Develop an effective implementation approach on monitoring and information sharing of cyber security incidents.

3.2 Incident handling reports

In 2020, CERT-PH responded and handled 100% of all the 957 cybersecurity incidents within the desired response timeframe. Recorded incidents include those reported directly to CERT-PH, monitored through public feeds and open-source intelligence escalated for incident response, and detected thru the National Security Operations Center.

The highest reported and handled incidents were Fake News which accounted for 34.5% of the total number of incidents. The prevalence of fake news was observed around March 2020 during the start of the Community Quarantine in the Philippines due to COVID-19 Pandemic.

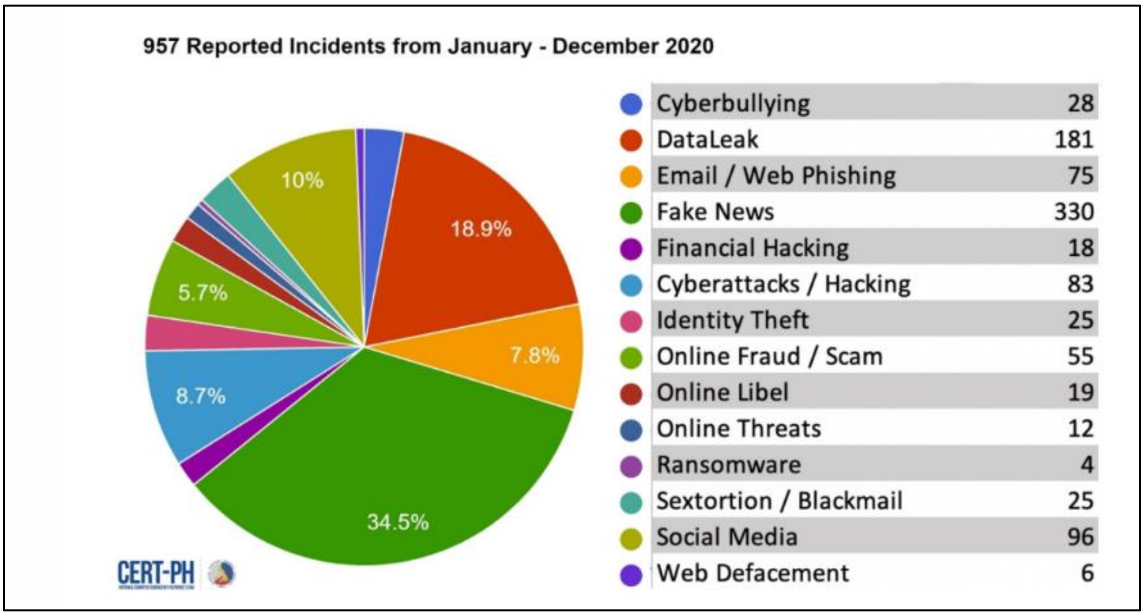


Figure 1. Breakdown of Incident Category

CERT-PH responded to these incidents by notifying the concerned agencies, conducting analysis, and provision of remediation steps to address the issues. Also, all the verified incidents are ticketed for proper tracking and documentation.

Cybersecurity related technical assistance requests and cybercrime reports are also being received by CERT-PH. Technical assistance that can be provided to the stakeholders are limited to the core services that are being offered which include incident response support, cyber threat monitoring and investigation. Cybercrime reports are escalated to the Law Enforcement Agency for proper handling. In 2020, CERT-PH received and handled the following technical requests:

- 18 Technical Assistance Requests
- 858 Cybercrime-related Reports

3.3 Vulnerability Assessment and Penetration Testing

In 2020, CERT-PH conducted vulnerability assessment and penetration testing to 698 systems of 26 different agencies and offices. A total number of 40 requests were received which include those from the Inter-Agency Task Force for Emerging Infectious Diseases members that develop mobile and web applications to help fight COVID-19 in the Philippines.

CERT-PH was also able to issue 74 CVE reports to government agencies. CVE reports consist of vulnerabilities affecting applications, development tools, network and security equipment and other systems that are commonly present to the government agencies.

A total of 258 vulnerable services monitored by the CERT-PH web information gathering system and reported by security individuals were raised to the concerned agencies.

3.4 Cyber Threat Monitoring Reports

In 2020, CERT-PH thru the National Cyber Intelligence Web Monitoring System, monitored a total number of 200,217,792 events based on the country code of the Philippines and Geo-IP pointing to the Philippines. Of those, 1468 were notified of vulnerable service to the concerned agency and 766 were escalated for incident response for verification and remediation. The Vulnerable Service had the highest number of recorded threats which accounted for 65.7% of the threats as shown in Figure 2.

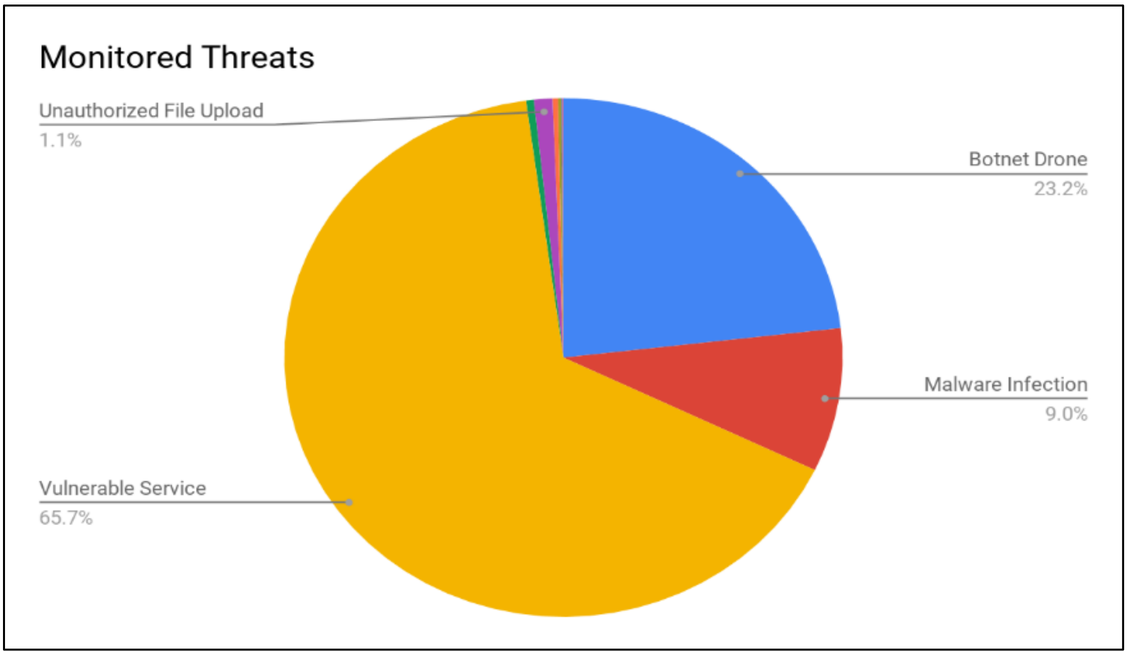
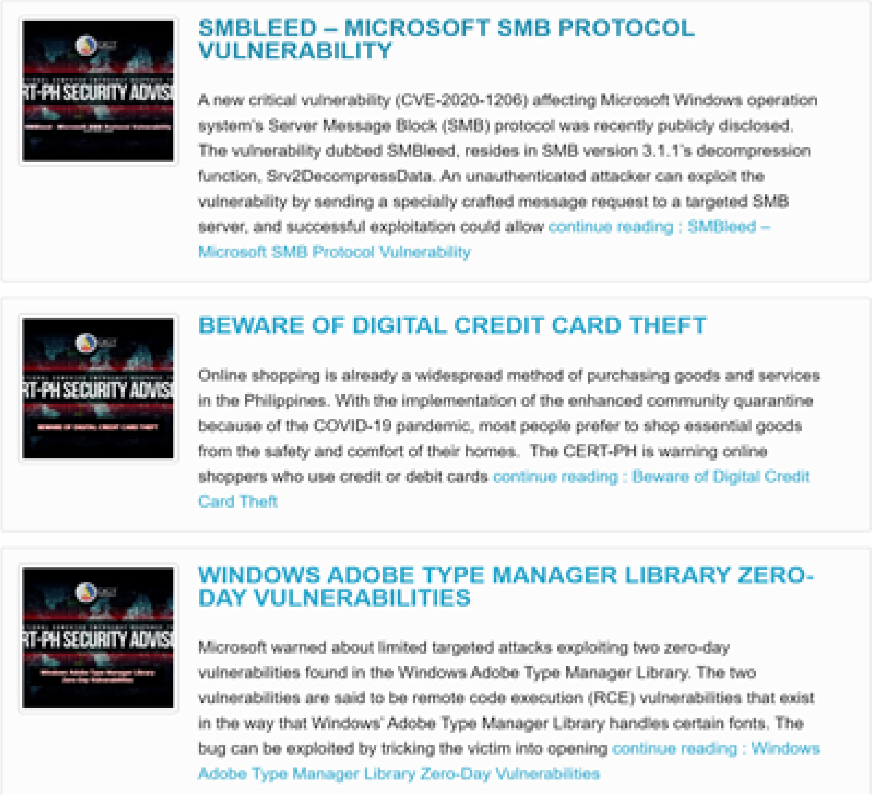


Figure 2. Monitored Threats (January to December 2020)

3.5 Security Advisories and Alerts

Cybersecurity 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 out to our stakeholders so they can protect themselves online. In 2020, CERT-PH issued:

- 188 Cybersecurity Threat Feeds
- 18 Security Advisories for Public



SMBLEED – MICROSOFT SMB PROTOCOL VULNERABILITY

A new critical vulnerability (CVE-2020-1206) affecting Microsoft Windows operation system's Server Message Block (SMB) protocol was recently publicly disclosed. The vulnerability dubbed SMBleed, resides in SMB version 3.1.1's decompression function, Srv2DecompressData. An unauthenticated attacker can exploit the vulnerability by sending a specially crafted message request to a targeted SMB server, and successful exploitation could allow continue reading : SMBleed – Microsoft SMB Protocol Vulnerability

BEWARE OF DIGITAL CREDIT CARD THEFT

Online shopping is already a widespread method of purchasing goods and services in the Philippines. With the implementation of the enhanced community quarantine because of the COVID-19 pandemic, most people prefer to shop essential goods from the safety and comfort of their homes. The CERT-PH is warning online shoppers who use credit or debit cards continue reading : Beware of Digital Credit Card Theft

WINDOWS ADOBE TYPE MANAGER LIBRARY ZERO-DAY VULNERABILITIES

Microsoft warned about limited targeted attacks exploiting two zero-day vulnerabilities found in the Windows Adobe Type Manager Library. The two vulnerabilities are said to be remote code execution (RCE) vulnerabilities that exist in the way that Windows' Adobe Type Manager Library handles certain fonts. The bug can be exploited by tricking the victim into opening continue reading : Windows Adobe Type Manager Library Zero-Day Vulnerabilities

Figure 3. Some of the Issued CERT-PH Security Advisories in 2020

3.6 National Security Operations Center

In 2020, CERT-PH thru the National Security Operations Center (NSOC) operations monitored around 41,855 incidents of which there are 413,970 alerts recorded from the 10 connected agencies. Alerts are malicious activities detected through the Threat Protection System (TPS). After undergoing automatic investigation by the TPS, alerts are considered as incidents for further investigation of the analysts.

Based on the number of NSOC incidents per attack stage category as shown in Figure 4, the Command & Control (C&C) is the most executed attack stage accounting to 41,055

TPS incidents.

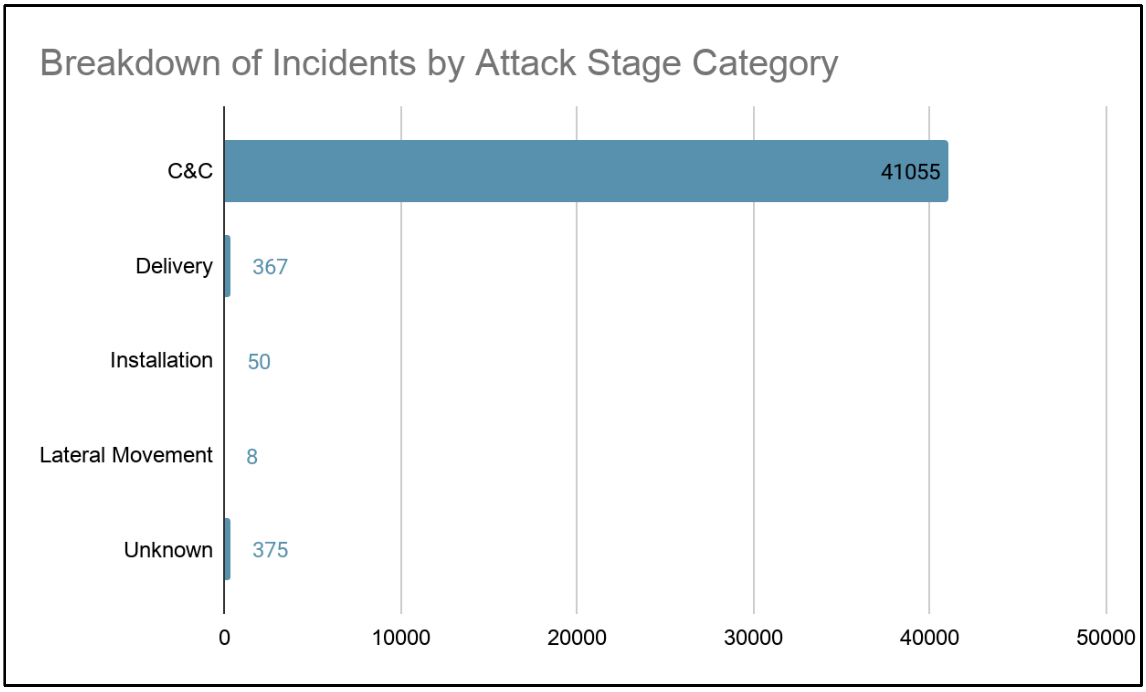


Figure 4. Breakdown of Incidents by Attack Stage Category

4. Events organized / hosted

4.1 Training

In 2020, CERT-PH conducted six (6) training on Setting Up a Computer Emergency Response Team and Basic Incident Handling. To establish and promote computer emergency response in the Philippines and to capacitate the government information and communications technology (ICT) personnel with the appropriate skill in information security, CERT-PH initiated the CERT Training Program which serves as the preparatory stage for government agencies to organize their own CERT. The training program aims to provide knowledge and develop their skills from establishing their CERT up to handling cyberattacks and its impacts.

4.2 Drills & exercises

CERT-PH hosted its annual National Cyber Drill Exercise on 26 November 2020. The remote exercise aims to help assess and improve the participating organizations' incident response capabilities and communication effectiveness during and after a cyberattack. The theme of this year’s drill is “Strengthening Cybersecurity and Adapting to the New Normal through Incident Response and Collaboration.”

208 participants from 74 organizations of the different Critical Infostructure Sectors (Government and Emergency Services, Telecommunications, Energy, Water, Banking and Finance, Business Processing Outsource, Healthcare, Transport and Logistics, and Media), Academe, and Military participated in the online cyber drill.

DICT
CYBERSECURITY BUREAU
CERT-PH
NATIONAL CYBER DRILL 2020
Strengthening Cybersecurity and Adapting to the New Normal through Incident Response and Collaboration
NOVEMBER 25-26, 2020
Zoom Meeting
Rey Linasan
Jun Salcor - PPP...

Figure 5. Snap/Screen Shot taken during NCD 2020

4.3 Conferences and seminars

In 2020, CERT-PH has partnered with other agencies/organizations and/or provided Subject Matter Experts on cyber security to a total of 15 webinars.

5. International Collaboration

5.1 International Partnerships

- CERT-PH became an operational member of the APCERT on September 24, 2020.
- CERT-PH joined the TSUBAME Project

5.2 Capacity building

5.2.1 Training

Attended the following:

- Coordinated Incident Response and Information Sharing Workshop hosted by Carnegie Mellon University – Software Engineering Institute in February 2020

- Workshop on Cybersecurity hosted by Singapore Cooperation Programme on October 27–November 4, 2020
- Incident Management Workshop hosted by Carnegie Mellon University – Software Engineering Institute in November 2020
- 11th and 12th ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC) in November – December 2020
- APT Online Training Course on Quality of Service (QoS) and Security in Internet Network for supporting Telemedicine hosted by Bharat Ratna Bhim Rao Ambedkar Institute of Telecom Training (BRBRAITT) on December 16-22, 2020

5.2.2 Drills & exercises

Participated in the following drills and exercises:

- ASEAN-Japan Cyber Exercise, June 24-25, 2020
- BI-Zone Cyber Polygon, July 8, 2020
- ASEAN CERT Incident Drill (ACID), October 7, 2020
- ITU 2020 Global CyberDrill (Regional Dialogues, Webinar, Training, Scenario-based Exercises), September – November 2020
- 2020 ITU Pacific CyberDrill, December 8-10, 2020

5.2.3 Seminars & presentations

Attended the following:

- 5th CAMP Annual Meeting and 2020 GCCD Cybersecurity Seminar, September 14 – 29, 2020
- APCERT Annual General Meeting, September 29, 2020

6. Future Plans

6.1 Future projects

- Conduct capacity building for new and existing CSIRTs in the Philippines
- Conduct cyber drill exercises designed for different Critical Infostructure (CII) Sectors
- Strengthen collaboration with local and international organizations.
- Apply membership to Forum of Incident Responders and Security Teams (FIRST)

6.2 Future operations

- Offer Source Code Review as an additional frontline service

7. Conclusion

The year 2020 has been a disruptive time for everyone as the world faces a global pandemic which brought not only new threats to public health but also to the cybersecurity landscape. As part of the country's cybersecurity measure against the pandemic, the DICT through CERT-PH is tasked to lead and manage cyber incident response and technical assistance requests, monitoring of cyber threats, and cybersecurity assessment of COVID-19 related applications.

To keep abreast with the rapidly evolving cyber threats, CERT-PH will maintain its focus on enhancing its frontline services, capacity building activities and collaboration with local and international organizations. As the entity mandated to lead, manage, and oversee the various CSIRTs in the Philippines, CERT-PH shall continue to support the establishment of new local CSIRTs to strengthen computer emergency response preparedness.

Contact Information

Email Address: cert-ph@dict.gov.ph
Hotline Number: (+632) 8920-0101 local 2378 (CERT)
Mobile Number: +639214942917 / +639561542042
Facebook: https://www.facebook.com/Ncertgovph
Website: www.ncert.gov.ph

CERT Tonga

Tonga Computer Emergency Response Team – Tonga

1. Highlights of 2020

1.1 Summary of major activities

Tonga's Computer Emergency Response Team (CERT Tonga) under the Ministry of Meteorology, Energy, Information, Disaster Management, Environment and Climate Change (MEIDECC) was able to deliver awareness programs in organizations from Government, Private Sectors and Public Enterprises.

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

1.2 Achievements & milestones

- CERT Tonga is the first country from the Pacific Islands region to become an Operational Member of the Asia Pacific Computer Emergency Response Team (APCERT) on April 2, 2020.
- CERT Tonga facilitated the launching of the GetSafeOnline – Tonga website partnering with GetSafeOnline, which is a not-for-profit organisation from the UK who has been doing similar work in other parts of the world. The website provides advice on how to be safe and secure online.
- They are also partnering in the Ambassador Scheme which trains volunteers on spreading information on cybersafety and cybersecurity.

2. About CSIRT

2.1 Introduction

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

2.2 Establishment

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

2.3 Resources

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

2.4 Constituency

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

3. Activities & Operations

3.1 Scope and definitions

As mandated, CERT Tonga aims to:

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

3.2 Incident handling reports

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

- Brute Force activities
- Botnet Activities
- Darknet Activities

3.3 Publications

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

4. Events organized / hosted

4.1 Trainings

- CERT Tonga, also facilitates training for local system administrators hosted by APNIC.
- Organize and hosted a session on Emotet by the CERT Tonga to local constituents and to the wider Pacific region.

5. International Collaboration

5.1 International partnerships and agreements

- CERT Tonga in an Operational Member of APCERT and a member of PaCSON (Pacific Cyber Security Operational Network).
- CERT Tonga partnered with GetSafeOnline to provide cyber safety and security tips targeting businesses and individuals.

5.2 Capacity building

5.2.1 Trainings

CERT Tonga also joined Online Training courses with APNIC, sessions with PaCSON community, building the level of skills and knowledge of our staff.

5.2.2 Other international activities

CERT Tonga presented on Business Email Compromise (BEC) observed in Tonga at the FIRST TC in Melbourne Australia which was part of the APRICOT Conference.

6. Future Plans

6.1 Future projects

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

6.2 Future Operation

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

7. Conclusion

CERT Tonga recently joined APCERT at the beginning of 2020 and looks forward to continue collaborating and sharing with the APCERT members.

CNCERT/CC

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

1. About CNCERT

1.1 Introduction

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

1.2 Establishment

CNCERT/CC was founded in 2001, and became a member of FIRST and one of the founders of APCERT. As of 2020, CNCERT/CC has established "CNCERT International Cooperation Partnership" with 265 teams in 78 countries and regions.

1.3 Workforce power

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

1.4 Constituency

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

1.5 Contact

E-mail：cncert@cert.org.cn

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

Fax：+8610 82990399

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

2. Activities & Operations

2.1 Incident handling

In 2020 CNCERT/CC received a total of about 103.1 thousand incident complaints, a 4% decrease from the previous year. And among these incident complaints, 772 were reported by overseas organizations, making a 31.3% increase from the year of 2019. As shown in Figure 2-1, most of the victims were plagued by vulnerabilities (35.0%), malware (32.8%) and phishing (18.2%). Vulnerability was the most complained about category.

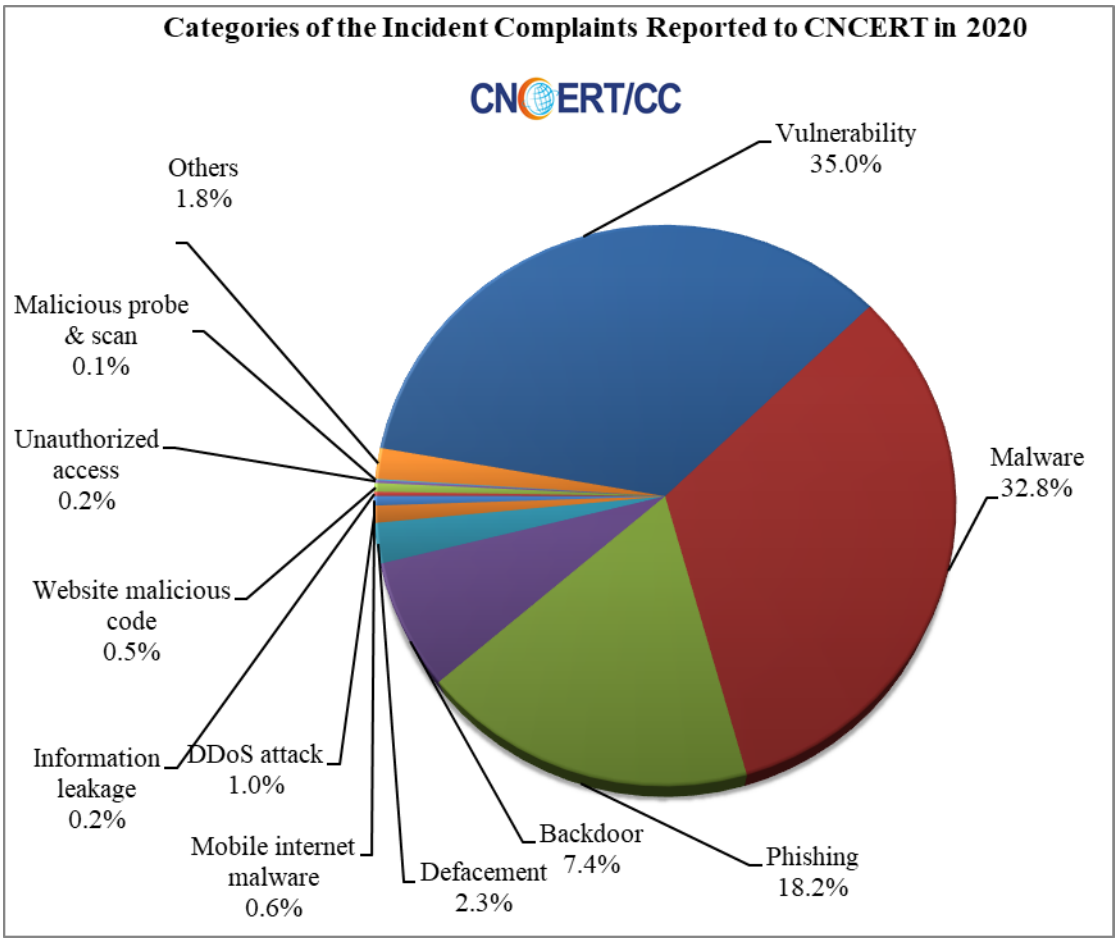


Figure 2-1Categories of the Incident Complaints Reported to CNCERT in 2020

In 2020, CNCERT/CC handled almost 103.1 thousand incidents, a decrease of 4% compared with that in 2019. As illustrated in Figure 2-2, vulnerability (35.0%) dominated the chart about categories of the incidents handled by CNCERT in 2020, followed by malware (32.8%) and phishing (18.2%).

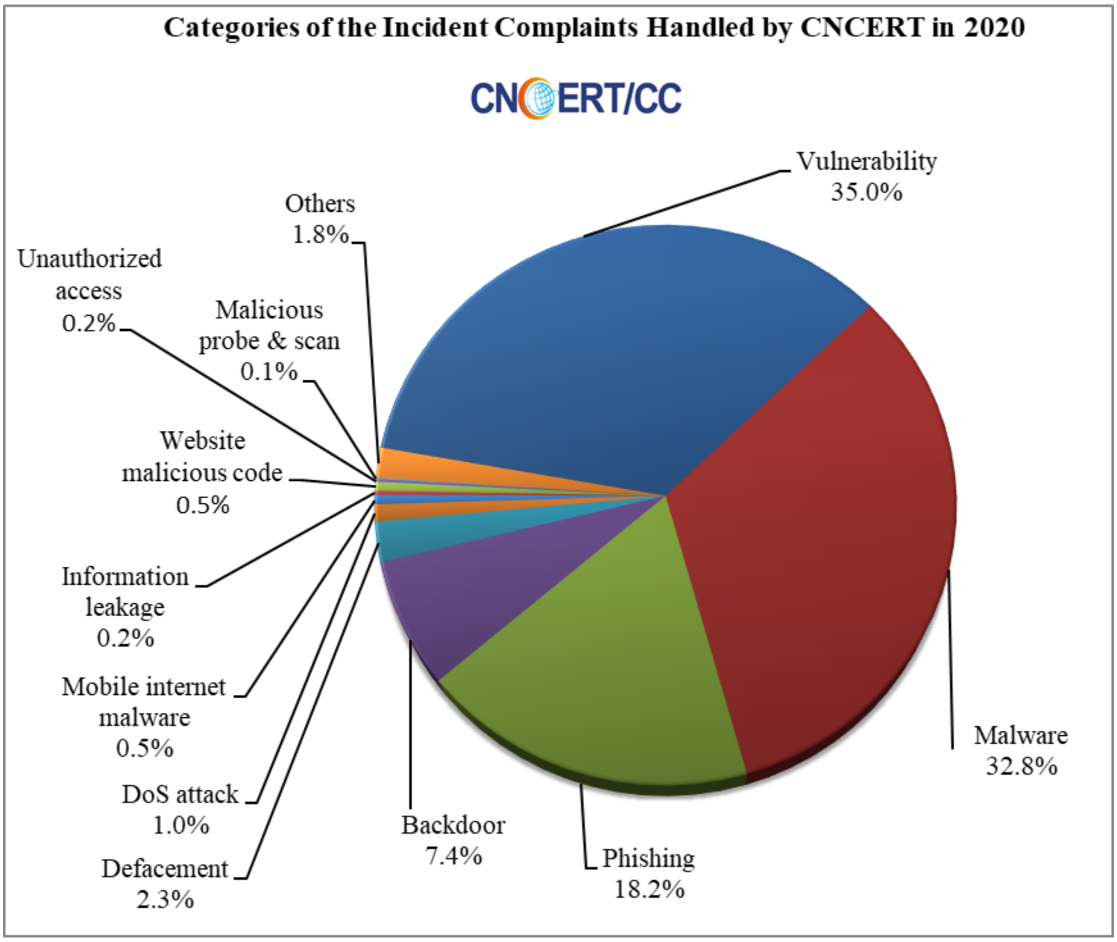


Figure 2-2 Categories of the Incidents Handled by CNCERT in 2020

2.2 Internet Threats

2.2.1 Malware Activities

In mainland China, IPs of the hosts infected with Trojan or Botnet reached about 5.81 million, which decreased by 8.3% compared with that in 2019. We saw more than 53 thousand overseas C&C servers which decreased by 43.1% from 2019. As shown in Figure 2-3, the U.S. hosted the largest number of overseas C&C servers' IPs of Trojan or Botnet, followed by Hong Kong China, Netherlands and Germany.

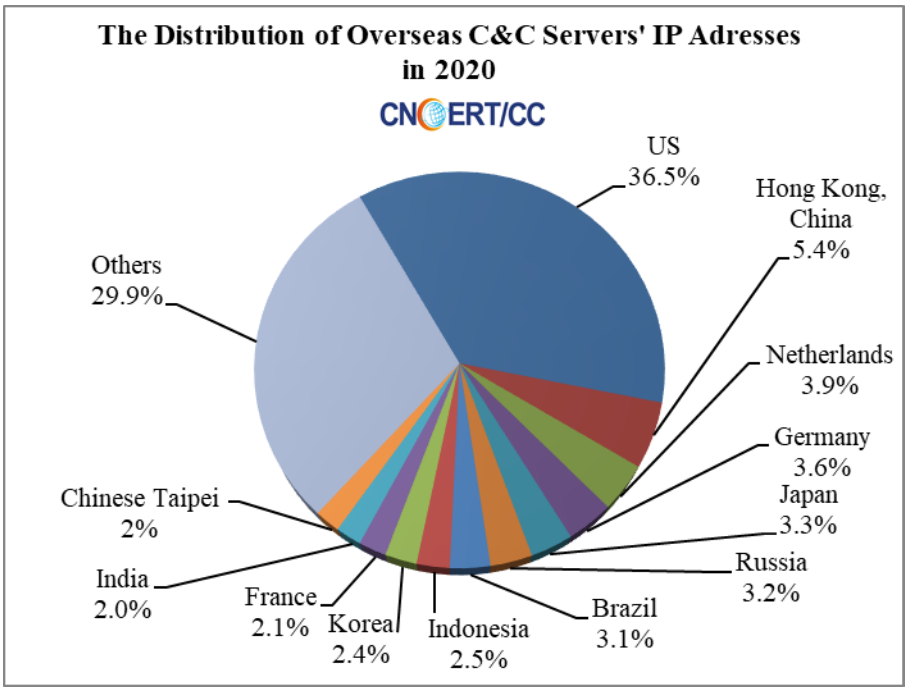


Figure 2-3 Distribution of overseas C&C servers' IP addresses in 2020

Malware-hosting websites are the jumping-off places for malware propagation. The malware-hosting websites monitored by CNCERT/CC in 2020 involved about 92 thousand domains, 129 thousand IP addresses and 1.75 million malware download links. Among the 92 thousand malicious domains, 12% of their TLDs fell into the category of .com. Among the 129 thousand malicious IPs, 33% were located overseas.

2.3 Website Security

About 100.4 thousand websites in mainland China were defaced, a decrease of 45% compared with that in 2019, including 494 government sites. Besides, about 53.1 thousand websites in mainland China were detected to be planted with backdoors and secretly controlled, out of which 256 were government sites.

In 2020, CNCERT/CC found about 100 thousand phishing sites targeting the websites in mainland China. About 3.3 thousand IPs were used to host those fake pages, and 97.8% were out of mainland China. Most of the phishing servers (65%) were located in Hong Kong China.

CNCERT/CC found almost 25.6 thousand overseas IPs conducting remote control on over 52.5 thousand websites in mainland China. As shown in Figure 2-5, 4,969 (19.3%) were located in Philippines, followed with 4,549(17.3%) in US and 2,291 (8.7%) in Hong Kong China.

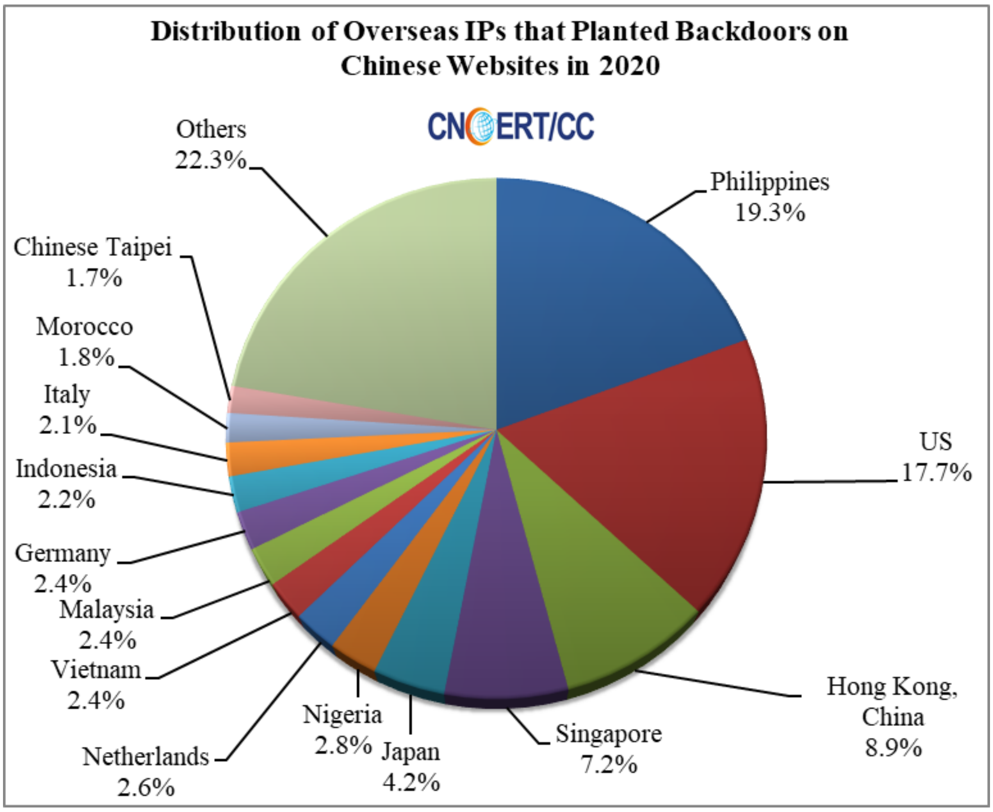


Figure 2-5 Distribution of Overseas IPs that Planted Backdoors on Chinese Websites in 2020

2.4 Mobile threats

In 2020, CNCERT/CC collected about 3.02 million mobile malware samples in total. In terms of the intentions of these mobile malware, rogue behavior took the first place (48.3%), fee consumption (21.1%) secured the second rank, and the next two were those intended for stealing privacy and malicious fee deduction for 12.7% and 12.4% respectively.

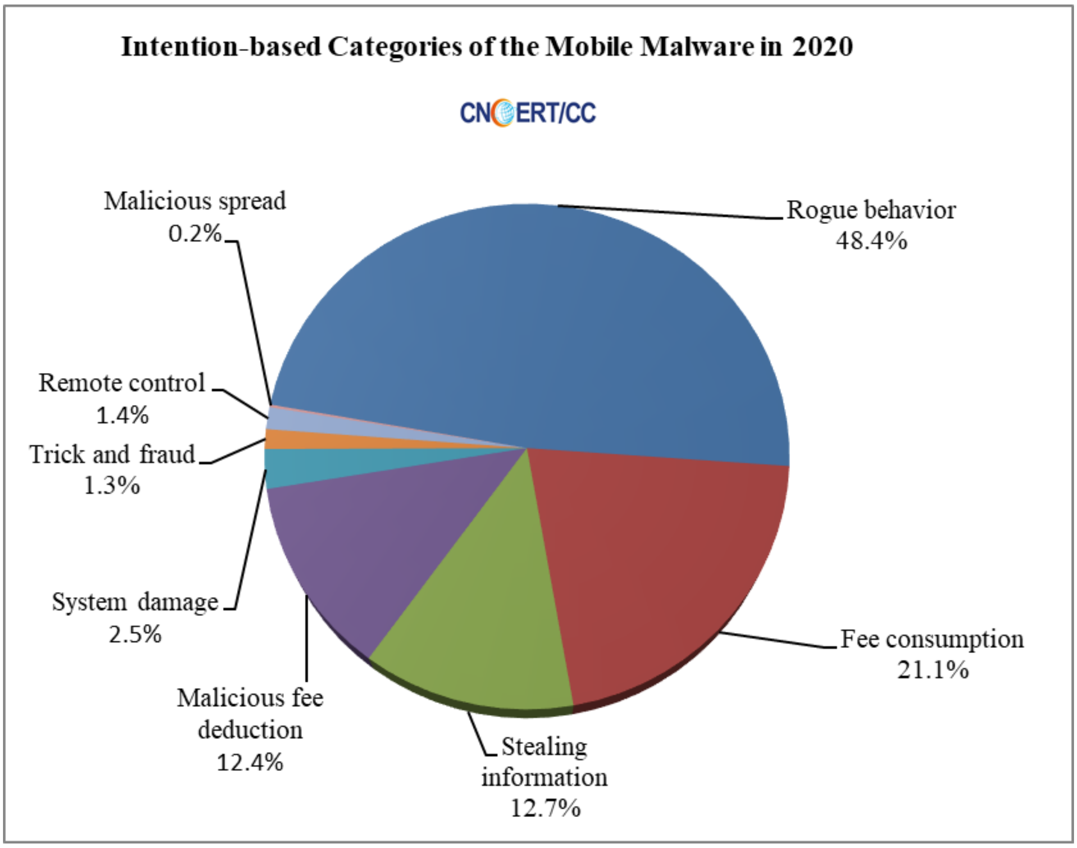


Figure 2-6 Intention-based Categories of the Mobile Malware in 2020

3. Events organized/co-organized

3.1 Conferences

The 2020 CNCERT Annual Conference in Beijing

On Aug 12th, 2020, CNCERT/CC held the 2020 Annual Chinese Conference on Computer and Network Security online. Focusing on the theme "To Confront Challenges Side by Side", the conference invited representatives from government departments, important information system units, research institutes and network security industries to discuss and exchange new trends, problems and ideas of network security, so as to build a nation-wide domestic and international cybersecurity cooperation system.

The 8th China-Japan-Korea CSIRT Annual Meeting for Cybersecurity Incident Response

From Aug 24th to 25th, 2020, the 8th China-Japan-Korea CSIRT Annual Meeting for Cybersecurity Incident Response was held online. Hosted by KRCERT/CC, this annual meeting has offered a platform for CNCERT/CC, JPCERT/CC and KrCERT/CC of KISA to exchange their thoughts and experiences in cybersecurity.

The Online Meeting of the 61st APEC-TEL Steering Group on Cyber Security and Prosperity

On October 9, 2020, the Cyber Security and Prosperity Steering Group (SPSG) meeting of the 61st meeting of the APEC Telecommunications Working Group (APEC-TEL) was held online. Xu Yuan of CNCERT/CC chaired the meeting as SPSG Convenor. At the same time, CNCERT/CC, as the leading unit of China's cybersecurity technology center and emergency response system, supported the APEC-TEL China delegation to complete the work of deputy convenor and convenor of the Cyber Security and Prosperity Steering Group with a four-year term.

Conference on CNCERT International Partnership in Emergency Response

On December 16, 2020, Conference on CNCERT International Partnership in Emergency Response hosted by CNCERT/CC was held online. More than 80 representatives from over 30 organizations of nearly 20 countries and regions attended the conference. Lu Wei, Deputy Director General of CNCERT/CC attended and delivered a speech.

With the theme of "Cooperation on Cybersecurity Emergency Response during COVID-19", the conference included two sessions: "International cooperation" and "Technical experience". Guest speakers from CNCERT/CC, Cybersecurity Malaysia, Information and Communications Technology Security of Ministry of Post and Telecommunications of Cambodia, Asia Pacific Network Information Center (APNIC), Sri Lanka CERT|CC, Pakistan Information Security Association, JPCERT/CC, Kaspersky ICS CERT exchanged their views on international cooperation of emergency response, cross-border cooperation on response among CERTs during the COVID-19, collaboration experience on COVID-19 related cyber incidents, practices and experience on telecommuting for emergency response organization, as well as trends and challenges of industrial cybersecurity.

4. Drill attended

APCERT Incident Drill 2020

On 11th Mar, 2020, CNCERT/CC participated in the APCERT 2020 Drill and completed it successfully. The theme of this year’s APCERT Drill is “Banker doubles down on Miner”. This exercise reflects real incidents and issues that exist on the Internet. The participants handled a case of a local business affected by malware infection which is triggered by data breach.

ASEAN CERT Incident Drill (ACID) 2020

On 7th October, CNCERT/CC participated in ASEAN CERT Incident Drill (ACID) 2020. The theme of this drill is "Malware Activities by virtue of the Pandemic". The participants investigated, analyzed and recommended remediation and mitigation measures towards information leakage incidents. More than 100 participants from 10 AMS and 5 key Dialogue Partners from China, Australia, India, Japan and South Korea participated in this year's drill.

5. Achievements

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

Title	No. of Issues	Description
CNCERT Weekly Reports (Chinese)	52	Emailed to over 400 organizations and individuals and published on CNCERT's Chinese website (http://www.cert.org.cn/)
CNCERT Weekly Reports (English)	52	Emailed to relevant organizations and individuals and published on CNCERT's English website (http://www.cert.org.cn/english_web/documents.htm)
CNCERT Monthly Reports (Chinese)	12	Issued to over 400 organizations and individuals on a regular basis and published on CNCERT's website (http://www.cert.org.cn/)
CNCERT Annual Reports (Chinese)	2	Published on CNCERT's website (http://www.cert.org.cn/)
CNVD Vulnerability Weekly Reports (Chinese)	52	Published on CNCERT's website (http://www.cert.org.cn/)
Articles Analyzing Cybersecurity Threats	308	Published on journals and magazines

Table 5-1 Lists of CNCERT's publications throughout 2020

CyberSecurity Malaysia

CyberSecurity Malaysia – Malaysia

1. HIGHLIGHTS OF 2020

1.1 Summary of major activities

11 Mar 2020	Participated in the APCERT Drill 2020
19 Aug 2020	Conducted an online training titled "*Android Mobile Malware Case Study During Covid19 Lockdown*", hosted by APCERT and the Pacific Cybersecurity Operational Network (PaCSON)
25 August 2020	Participated in a virtual seminar entitled "*Virtual Cloud Security Day*" through the Microsoft Teams application. This virtual seminar organised by Microsoft Malaysia is a platform to discuss cybersecurity issues to help protect business operations as well as empower customers with knowledge in the field of information security
12 Sep 2020	Co-organised the OIC-CERT Cyber Drill with Oman National CERT. Seven (7) APCERT members participated - BruCERT, CERT-IN, BSSN, HKCERT, TWNCERT, Sri Lanka CERT/CC, and VNCERT/CC
29 Oct 2020	Chaired the APCERT Annual General Meeting (AGM) conducted virtually
16 – 18 Nov 2020	Participated in the 32nd Annual FIRST Conference virtually
23 - 24 Nov 2020	Organised the OIC-CERT 12th Annual Conference 2020 (Virtual) with the theme "*Cyber Security Strategies & Practices During COVID-19 Crisis*"
16 Dec 2020	Participated in the CNCERT International Partnership in Emergency Response Conference virtually

2. ABOUT CYBERSECURITY MALAYSIA

2.1 Introduction

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

i. Cybersecurity Emergency Services
   - Security Incident Handling
   - Digital Forensic

ii. Security Quality Management Services
   - Security Assurance
   - Information Security Certification Body

iii. Cybersecurity Professional Development and Outreach
   - Info Security Professional Development
   - Outreach

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

v. Industry and Research Development

2.2 Establishment

CyberSecurity Malaysia started with the formation of the Malaysian Computer Emergency Response Team (MyCERT) on 13 January 1997 under the Ministry of Science, Technology, and Innovation. In 2018, with the restructuring of the government administration, CyberSecurity Malaysia was transferred to the Ministry of Communications and Multimedia Malaysia. CyberSecurity Malaysia is committed in providing a broad range of cybersecurity innovation-led services, programmes, and initiatives to help reduce the vulnerability of digital systems, and at the same time strengthen Malaysia's self-reliance in the cyberspace.

2.3 Cybersecurity Incident Management

CyberSecurity Malaysia managed security incidents through MyCERT, a department within CyberSecurity Malaysia. The agency is a leading point of reference for the Malaysian Internet community when faced with cybersecurity incidents. MyCERT facilitates the mitigation of cyberthreats for Malaysia's Internet users particularly on cyber intrusion, identity theft, malware infection, and cyber harassment, among others. MyCERT operates the Cyber999 Help 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 Help Centre

MyCERT operates the Cyber999 Help 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 help centre are available at MyCERT's website at https://www.mycert.org.my

MyCERT's Cyber999 help centre, has responded to 10,790 incidents in 2020 and most being intrusion and online fraud.

2.3.2 Cyber Threat Research Centre

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

2.4 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, 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 13 advisories and 18 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 intrusion. The following chart shows the reported incidents managed by CyberSecurity Malaysia.

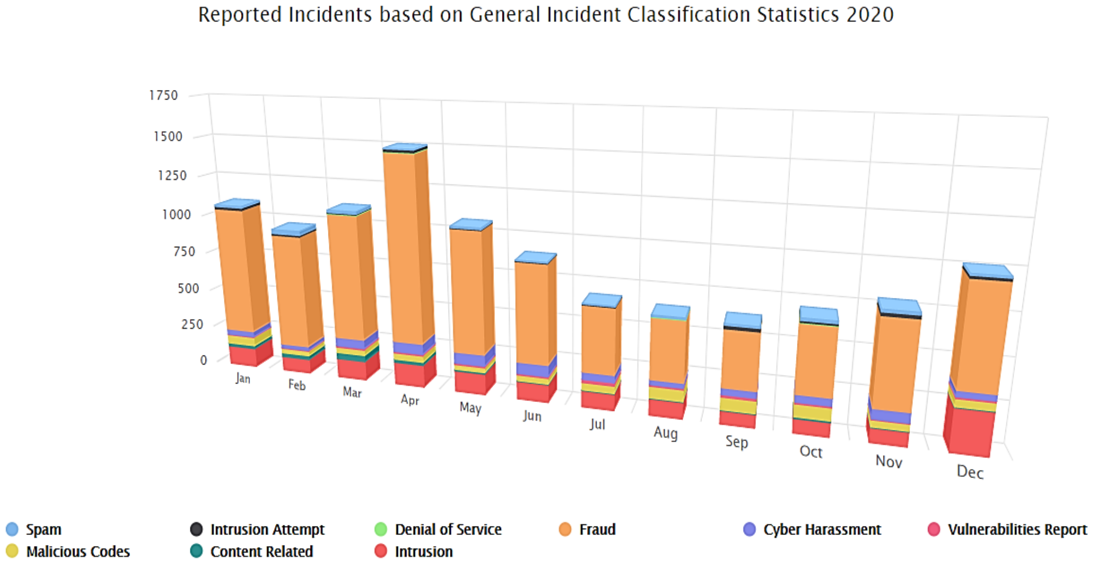


Diagram 1: 2020 Reported Incident

Further information on incidents reported to CyberSecurity Malaysia can be viewed at: https://www.mycert.org.my/portal/statistics-2020

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 on how the exploits functioned as well as to collect malware binaries. Honeypots are computer software mechanism set up to mimic a legitimate site to ensnare malicious software into believing that it is a legitimate site which is in a weak position for attacks. Honeypot allows researchers to detect, monitor, and counter malicious activities by understanding the activities done during the intrusion phase and attacks' payload. It can be viewed at https://dashboard.honeynet.org.my/

The URLs of the LebahNET project are:

- LebahNET portal at https://dashboard.honeynet.org.my/
- Kibana portal at https://es.honeynet.org.my/app/canvas#/workpad/workpad-7802f4ef-34aa-4690-8165-3921160bd371/page/1 by using guest authentication;
  Username: guest
  Password: guest2021!

4. EVENTS INVOLVEMENT AND ACHIEVEMENTS

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

4.1 Cyber Drills

CyberSecurity Malaysia, participated in two (2) international cyber drills in 2020 namely the APCERT Drill, and the OIC-CERT Drill.

4.2 Trainings

Several workshops or hands-on training were conducted by CyberSecurity Malaysia in 2020.

3 Mar 2020	Cloud and Smart Card Security - A Sneak Peak
5 May 2020	WFH: Online Meeting Platform Security Demystified
20 May 2020	Cybersecurity Awareness for All Users
25 Jun 2020	Work from Home 2020
13 Jul 2020	Cybersecurity Technology
29, 30 Jun & 8 Jul 2020	Mobile Incident Response and Digital Forensic

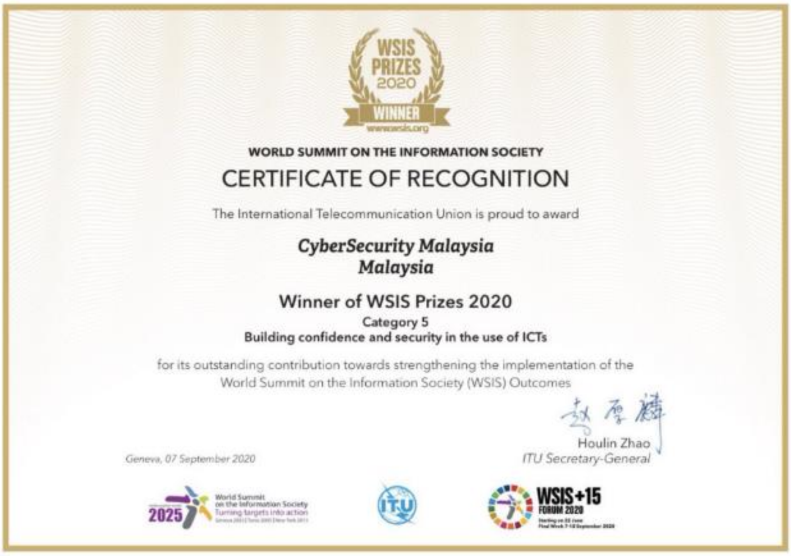
19 Aug 2020	The APCERT and Pacific Cybersecurity Operational Network (PaCSON)
2-5 Nov 2020	Certified Secure Application Professional (CSAP)
5-6 Nov 2020	Digital Forensic Essential
10-11 Nov 2020	Certified Information Security Awareness Manager (CISAM)
16-19 Nov 2020	Certified Secure Application Professional (CSAP)
23-27 Nov 2020	Certified Penetration Tester (CPT)
25 Nov 2020	Global ACE Certification Webinar
2 Dec 2020	Cyber Security Awareness and Risk Governance for CxO & Board Members
8-10 Dec 2020	Malaysia Common Criteria 2.0 (MyCC) - Foundation Evaluator

4.2.1 The Global ACE Certification Scheme as the WSIS Winner 2020

The Global ACE Certification Scheme project was named as one of the World Summit on Information Society Prizes (WSIS Prizes) 2020 Winner at the WSIS Forum 2020 in Geneva, Switzerland.

The prize was given under Category 5 – Action Line C5: '*Building Confidence and Security in Use of ICTs*' in recognition to CyberSecurity Malaysia's initiative on the Global Accredited Cybersecurity Education Scheme: Centre of Excellence for Capacity Building and Lifelong Learning.

The WSIS Forum is the world's largest ICT annual gathering of the '*ICT for development'* community hosted by the International Telecommunication Union (ITU), and co-organised by ITU, UNESCO, United Nations Conference on Trade and Development (UNCTAD) and United Nations Development Programme (UNDP) in close collaboration with all WSIS Action Line Facilitators / Co-Facilitators.



WSIS PRIZES 2020 WINNER www.wsis.org

WORLD SUMMIT ON THE INFORMATION SOCIETY

CERTIFICATE OF RECOGNITION

The International Telecommunication Union is proud to award

CyberSecurity Malaysia
Malaysia

Winner of WSIS Prizes 2020
Category 5
Building confidence and security in the use of ICTs

for its outstanding contribution towards strengthening the implementation of the World Summit on the Information Society (WSIS) Outcomes

Geneva, 07 September 2020

Houlin Zhao
ITU Secretary-General

2025
World Summit on the Information Society
Turning targets into action
ITU
WSIS+15
FORUM 2020

4.3 Presentations

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

i. 25 Nov 2020 - CyberSecurity Malaysia hosted the Global ACE Certification Seminar themed, "Certifying Cyber Security Professionals Towards the Industrial Revolution 4.0".

ii. This virtual seminar is one of the Satellite Events for the 12th Annual Conference of the Computer Emergency Response Team - Organisation of the Islamic Conference (OIC-CERT) 2020 which serves as a platform to understand the needs of cybersecurity professionals towards the fourth industrial revolution.

iii. Through this seminar, CyberSecurity Malaysia exposes the participants to the fourth industrial revolution and the Global ACE Certification Scheme;

iv. 18 Nov 2020 - Mr. Mohd Shamir Hashim, Senior Vice President of International and Government Engagement, represents the OIC-CERT as a panellist at the FIRST virtual conference;

v. 16 December 2021 - Tan Sri General Azumi speaks at the online conference on CNCERT International Partnership in Emergency Response which was held 16 Dec 2020 with the theme of "Cooperation on Cybersecurity Emergency Response during Covid-19".

4.4 Research Papers

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

i. *Mobile Malware Classification for Social Media Application.* Published in IEEE Xplore Digital Library
ii. *Using Text Annotation Tool on Cyber Security News: A Review.* Published in IEEE Xplore Digital Library
iii. *Method for Generating Test Data for Detecting SQL Injection Vulnerability in Web Application.* Published in IEEE Xplore Digital Library
iv. *Ransomware Entities Classification with Supervised Learning for Information Text.* Published in IEEE Xplore Digital Library
v. *Feature Extraction and Selection Method of Cyber Attacks and Threat Profiling in Cybersecurity Audit.* Published in IEEE Xplore Digital Library
vi. *TAGraph Knowledge Graph of Threat Actor*. Published in IEEE Xplore Digital Library
vii. *OTPAF: A Security Requirement Conceptual Model of Cloud SAAS for Malaysian Government Based on Common Criteria*. Published in IEEE Xplore Digital Library
viii. *Cloud Service Provider Security Readiness Model : The Malaysian Perspective.* Published in IEEE Xplore Digital Library
ix. *An Attribution of Cyberattack using Association Rule Mining (ARM)*. Published in The Science and Information Organisation
x. *A Malware Detection Framework Based on Forensic and Unsupervised Machine Learning Methodologies.* Published in ACM Digital Library
xi. *Cryptojacking Classification Based on Machine Learning Algorithm.* Published in ACM Digital Library
xii. *The Capabilities that Terrorist Possess in the Digital Age.* Published in Özgür Öztürk Dakam Yayinlari
xiii. *S-Box Construction Based on Linear Fractional Transformation and Permutation Function.* Published in MDPI
xiv. *Secure Information Hiding Based on Random Similar Bit Mapping.* Published in International Association of Computer Science and Information Technology
xv. *Slid Pairs of the Fruit-80 Stream Cipher.* Published in Institute of Information Technology

xvi. *Mitigating Insider Threats: A Case Study for Data Leakage Prevention.* Published in Academic Conferences and Publishing International Limited

xvii. *OS Kernel Malware Detection through Data Characterization of Memory Analysis.* Published in Academic Conferences and Publishing International Limited

xviii. *A Review of Insider Threat Detection: Classification, Machine Learning Techniques, Dataset, Open Challenges and Recommendations.* Published in MDPI

xix. *Fraudulent e-Commerce Website Detection Model Using HTML, Text and Image Features.* Published in Springerlink

xx. *Malware Behavior Profiling from Unstructured Data.* Published in Springerlink

xxi. *Findings Annihilator(s) via Fault Injection Analysis (FIA) on Boolean Function of LILI-128.* Published in Engineering and Technology Publishing

xxii. *Extended RECTANGLE Algorithm Using 3D Bit Rotation to Propose a New Lightweight Block Cipher for IoT.* Published in IEEE Xplore Digital Library

xxiii. *Randomness Analysis on Lightweight Block Cipher, PRESENT.* Published in Science Publications

4.5 Social Media

In 2020, CyberSecurity Malaysia received continuous invitations to speak in events with regards to cybersecurity at the local radio and television stations. CyberSecurity Malaysia also actively disseminates cybersecurity concerns through social media such as Facebook and Twitter, which is done through MyCERT. As of now, the MyCERT Facebook Page has about 54,057 likes and the MyCERT Twitter has 5,833 followers.

5. INTERNATIONAL COLLABORATION

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

5.1 Working Visits

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

5.2 Memorandum of Understanding (MoU)

CyberSecurity Malaysia has signed MoUs with the following organisations:

i. Backbone Connectivity Networks (Nigeria) Limited, Nigeria;

ii. The State Cybersecurity Service at the "Türkmenaragatnaşyk" Agency, Turkmenistan

5.3 International Roles

Amongst the international roles and contributions by CyberSecurity Malaysia are:

i. The Permanent Secretariat of the Organisation of Islamic Cooperation – Computer Emergency Response Team (OIC-CERT), where a major role is to facilitate cooperation and interaction among the members countries

ii. The lead for the Capacity Building Initiatives in the OIC-CERT

iii. The Chair of the APCERT

iv. The Convenor for the APCERT Malware Mitigation Working Group – addressing malware infection among Internet users and cyber threat general issues. The main objectives are to provide an overview of cyber threats landscape by doing collaborative research to mitigate the cyber threats and sharing regular reports or data on malware attacks and focus on the impact analysis and remedial action.

6. FUTURE PLANS

CyberSecurity Malaysia strives to improve service capabilities and encourage local Internet users to report cybersecurity incidents to the Cyber999 help 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 MoUs and agreements.

Since the Covid 19 pandemic outbreak, CyberSecurity Malaysia has postponed several national events such as the CyberSecurity Malaysia – Awards, Conference and Exhibition (CSM-ACE) and the National ICT Security Discourse. The agency will continue back with these events when the situation permits. At the international arena, CyberSecurity Malaysia as the Permanent Secretariat of the OIC-CERT, continues to spearhead the collaboration 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 ensure 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 that emphasised 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 important facet in mitigating other cybersecurity issues. As the cyber environment does not conform to the physical boundary of the countries, international relations will remain an important initiative. With the rapid development of the internet, the economies are now dependent on public network applications such as online banking, online stock trading, e business, e governments, and the protection of the various national information infrastructures. CyberSecurity Malaysia will continue to establish and support cross border collaboration either through bilateral or multilateral platforms such as the APCERT and the OIC-CERT, and will continuously pursue new cooperation with cybersecurity agencies regionally and globally in the effort to make cyberspace a safer place.

EC-CERT

Taiwan E-Commerce Computer Emergency Response Team - Chinese Taipei

1. Highlights of 2020

EC-CERT is committed to supporting and strengthening e-commerce companies' ability to respond to and handle security incidents, and works

with the e-commerce alliance to promote PII and information security activities. EC-CERT has established a basic checklist of e-commerce information security, promoting e-commerce companies to check the completion of security protection, and encouraged the industry to strengthen security management.

EC-CERT held a workshop in which white hat hackers were invited to exchange views with the CEOs of e-commerce companies. In the past, due to the lack of IT professionals and budgets, many small e-commerce companies were unable to find security-related vulnerabilities on their own. With this activity, they discussed the security vulnerability issues and proposed solutions to security issues, thereby strengthening transaction security protection.

2. About EC-CERT

2.1 Introduction

EC-CERT stands for "Taiwan E-Commerce Computer Emergency Response Team" and is supported by the Ministry of Economic Affairs of the Republic of China. EC-CERT provides services to prevent e-commerce finance fraud in case of monetary loss and smoothly developing of Taiwan's E-commerce market.

2.2 Establishment

EC-CERT was established in 2010. The main role of EC-CERT is to assist the e-commerce industry to enhance information security, help handle information security incidents, avoid hacking, and promote information security and PII protection activities.

2.3 Constituency

EC-CERT aims to enhance the ability of e-commerce companies to respond and deal with security incidents and related issues. EC-CERT provides security counseling for e-commerce platforms, logistics providers and service providers, and provides to enhance information security protection in the event of external attacks.

3. Activities & Operations

3.1 Scope and definitions

EC-CERT continuously releases many information security reports for the e-commerce industry, including website security online consulting records and step-by-step practical case resolution procedures and recommendations.

3.2 Incident handling reports

EC-CERT provides 7 event visits, handling 8 security incidents, providing 32 security advices, and received 45 computer security incident reports from E-commerce companies

3.3 Publications

- Online retail industry information security protection practice case selection
- Online retail industry information security basic checklist

4. Events organized / hosted

4.1 Conferences and seminars

- Information security promotion activities * 2
- Participation Asia PKI Union Conference * 2

5. International Collaboration

5.1 Capacity building

5.1.1 Training

EC-CERT participated and benefited from the following APCERT Training topics:

- Identification of information security risks as a sectoral CSIRT and addressing the risks
- Getting started with Threat Intelligence Sharing via MISP
- CTI & IntelMQ
- ATM Cyber Attack

5.1.2 Drills & exercises

EC-CERT participated in the APCERT Drill in March 2020. The topic of APCERT online drill was “Business email and systems compromise leveraged by a vulnerable service.”

5.2 Other international activities

None.

6. Future Plans

EC-CERT aims to create an E-commerce response centre that can help optimize the capability of security incidents, coordination, response and handling in the face of security incident.

The E-commerce industry's security incidents will easily cause increases in consumer fraud cases, how to help E-commerce industry conduct prevention with other detective controls and follow up improvement is the key point.

7. Conclusion

As long as information technology continues to develop, there will always be scams, but the key to point out is how to continuously strengthen user awareness and security management. EC-CERT will continue to be committed to e-commerce information security in Taiwan.

GovCERT.HK

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

1. Highlights of 2020

1.1 Summary of Major Activities

2020 has been an extraordinarily challenging year for all of us to adapt swiftly to the rapidly changing global conditions. Under the "new normal" amid the Coronavirus Disease 2019 (COVID-19) epidemic, the Government Computer Emergency Response Team Hong Kong (GovCERT.HK) has maintained its smooth operation and contributed in fighting this battle by offering assistance including conducting security risk assessment and vulnerability scanning in time to safeguard newly developed systems and applications of the Government of the Hong Kong Special Administrative Region of the People's Republic of China (the Government) in combating the epidemic. We have also monitored and provided information security advice on the work-from-home arrangement and usage of video conferencing solutions to government users. In response to arising cyber attacks using COVID-19 related themes, we have worked closely with stakeholders to provide security advice in a timely manner. All these measures have been proven to be vital for Hong Kong's integral effort in maintaining a secure cyberspace under the ever-changing global digital environment.

A keen appreciation of the threat landscape could help organisations and individuals to understand better the cyber threat environment so as to adopt early and appropriate mitigation measures. In 2020, we continued publishing threat trends, security alerts and mitigation advice through the GovCERT.HK web portal for the general public's reference. We further tailored specific threat awareness updates for government departments.

To enhance the city's overall defensive capability and resilience against cyber attacks, we continued to leverage the local cross-sector Partnership Programme for Cyber Security Information Sharing (Cybersec Infohub), to promote trusted partnership between local cyber security stakeholders across different sectors for sharing cyber security information and providing actionable insights to the community. We regularised the programme to encourage more participation of organisations from various industries.

We are also committed to promoting information security awareness to various sectors of the community by collaborating with different organisations to regularly hold various cyber security publicity events.

1.2 Achievements and Milestones

Operation under the "New Normal"

In response to the workforce transformation sparked by the COVID-19 epidemic, GovCERT.HK has adopted various initiatives, such as releasing educational videos on cyber conference security and guidelines for remote access and corporate VPN security, to remind organisations and the public to stay alert of cyber threats arose from the epidemic. We have also paid close attention to epidemic-themed cyber risks and collaborated with stakeholders to provide security alerts and advice. In addition, GovCERT.HK has rendered its support to various COVID-19 epidemic related programmes and systems in order to timely launch various government services to combat the COVID-19 epidemic.

Cyber Security Information Sharing

With the objective to facilitate cross-sector collaboration for a better visibility of cyber threats globally and locally, Cybersec Infohub serves well to nurture a culture of sharing cyber security information. Given the positive response from participating public and private organisations of Cybersec Infohub operating for over two years, we regularised the programme and partnered with the Hong Kong Internet Registration Corporation Limited (HKIRC) to encourage more participation from various industries including the small and medium enterprises (SMEs). In 2020, we gathered industry experts to form a new supporting alliance, Cybersec Connect, to offer support and advice on cyber security related problems for the members. The programme has become an essential reference for organisations to obtain cyber security information and meet with various stakeholders to exchange the latest security trends and best practices.

Cyber Threat Intelligence Management

GovCERT.HK has been monitoring cyber security threat trends and sharing relevant information with our constituents and the community for taking early precautions. We have published monthly Cyber Security Threat Trends Report via the GovCERT.HK web portal to highlight observations on the latest cyber security threat landscape for the public's reference. To enhance the capacity and capability of cyber threat intelligence management, we integrated Malware Information Sharing Platform (MISP) instances into the Cyber Risk Information Sharing Platform (CRisP) to enable collection, sharing, storing and correlation of Indicators of Compromise and facilitate collaboration on handling security events with related parties in the Government.

Government IT Security Policy and Guidelines

To ensure that the policy and guidelines tie in with security trends as well as technology advancement, the Government reviewed the "Government IT Security Policy and Guidelines" to cover the latest areas of information and cyber security with reference to international standards and industry best practices. Requirements were strengthened in various security areas including protection of mission critical systems and common applications, remote access control, protection of personal data and adoption of emerging technologies such as Internet of things (IoT) and public cloud. The updated government IT security policy and guidelines were uploaded onto GovCERT.HK's website for reference by the public.

Liaison and Collaboration

We actively participated in the Asia Pacific Computer Emergency Response Team's (APCERT) activities and worked closely with the Computer Emergency Response Team (CERT) community in handling threat information. We have been supporting the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) to produce a series of animations to raise public awareness of cyber security with themes including remote working and video conference, cloud security, phishing and malware, and IoT security.

Awareness Building and Public Education

User awareness of information security plays a vital role in coping with cyber threats. In view of the rising trend of phishing scams and data breaches during the COVID-19 epidemic, GovCERT.HK produced a series of promotional materials including educational animations and smart tips for the public to protect themselves from and defend against cyber threats.

GovCERT.HK also devoted much attention to public education and capacity building in different business sectors and age groups, with some 20 face-to-face and online school visits conducted in 2019/20 and 2020/21 school years. We revamped our Information Security (InfoSec) website to provide a more lively design for better user experience and disseminate security related tips and advice to the public.

2. About GovCERT.HK

2.1 Introduction

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

Since its establishment, GovCERT.HK has profoundly shaped the management framework and coordination mechanism of incident handling; and empowered close collaboration with the industry, critical Internet infrastructure stakeholders, and the CERT community for timely exchange of cyber threat information and coordinated responses. GovCERT.HK also works closely with the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) and local industries on cyber threat intelligence sharing, capability development, public education, and continuous promotion on cyber security through social and mass media.

GovCERT.HK also actively collaborates with other governmental and regional CERTs, and international organisations in sharing cyber threat intelligence and incident information; participating in training events, workshops, forums and drills; and organising activities for public awareness promotion and capability development.

2.2 Establishment

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

2.3 Resources

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

2.4 Mission and Constituency

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

3. Activities and Operations

3.1 Scope of Services

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

3.2 Security News Bulletins

In 2020, GovCERT.HK published the following security bulletins to raise the awareness among government users and the general public.

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

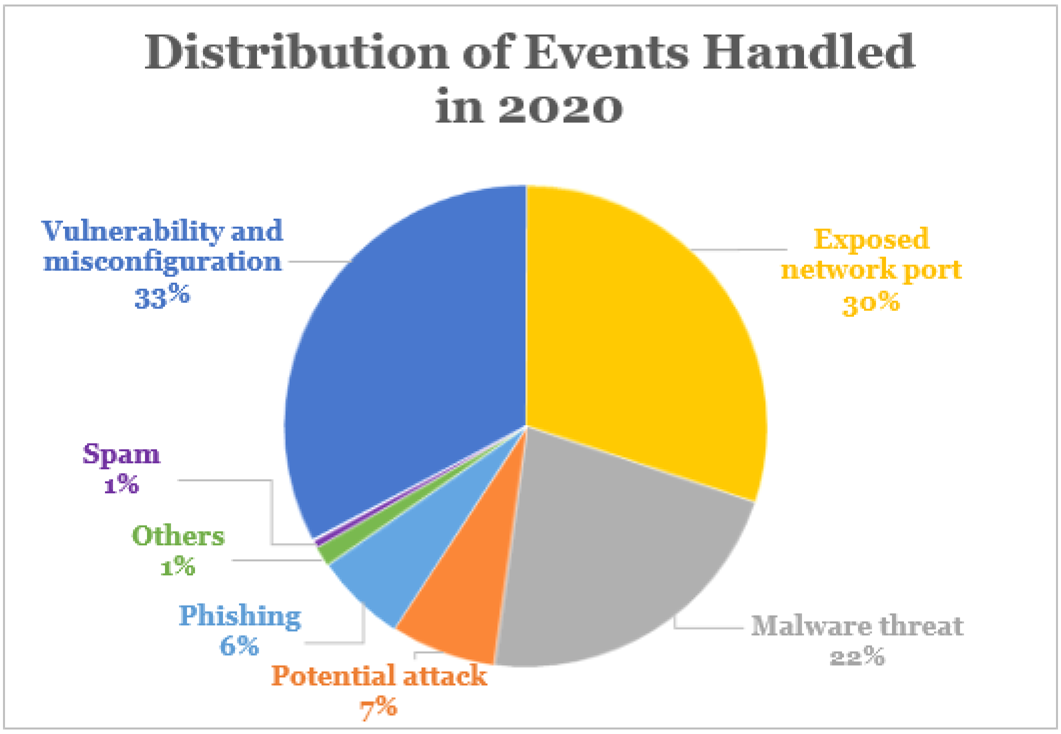
3.3 Alerts and Advisories

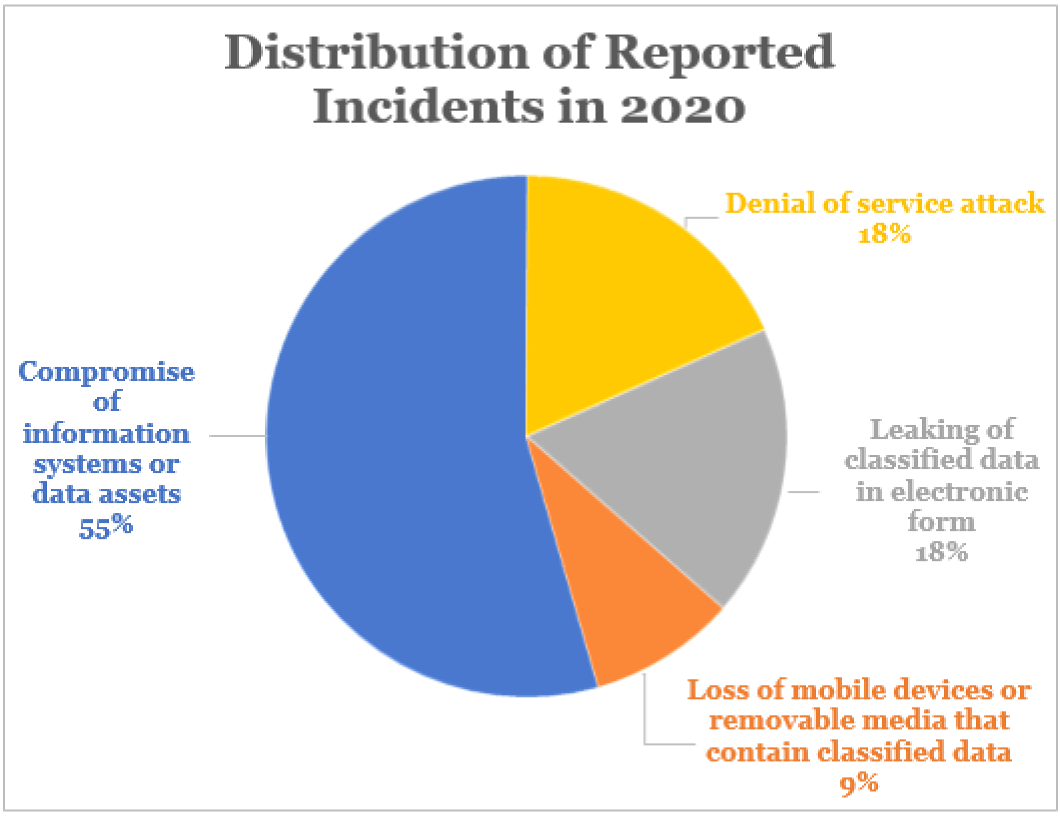
In 2020, GovCERT.HK issued over 90 security alerts associated with computing products widely deployed in government installations. For those security vulnerabilities which were considered highly risky to the Government, we proactively requested government departments to take prompt and appropriate preventive measures against potential information security risks.

We also conducted threat analysis on over 210 security events detected and received from various sources. The threat assessment results and security advice were promptly shared with relevant parties for appropriate follow-ups.

3.4 Security Events and Incident Handling

Security events indicate possible breaches of information security or failure of security controls. Security incidents, however, are in relation to one or multiple events that can harm information systems and/or data assets, or compromise their operations. In 2020, GovCERT.HK dealt with various cyber security events and reported incidents that were related to government installations. The following charts show the distribution of events and reported incidents handled in 2020.



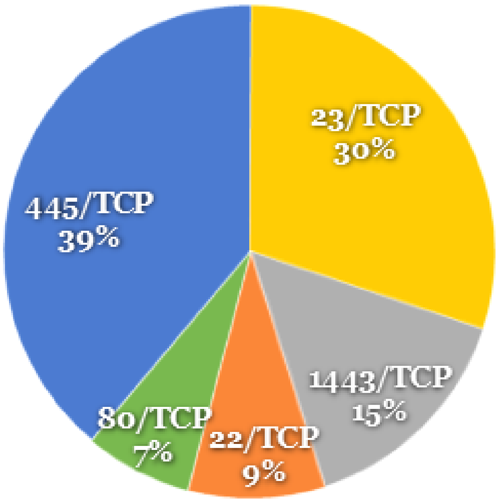


To facilitate public access to the statistics on information security incidents in the Government, relevant data has been made available on the Government's Public Sector Information Portal.
(www.data.gov.hk/en-data/dataset/hk-ogcio-sec_div_01-information-security-incident).

3.5 Abuse Statistics

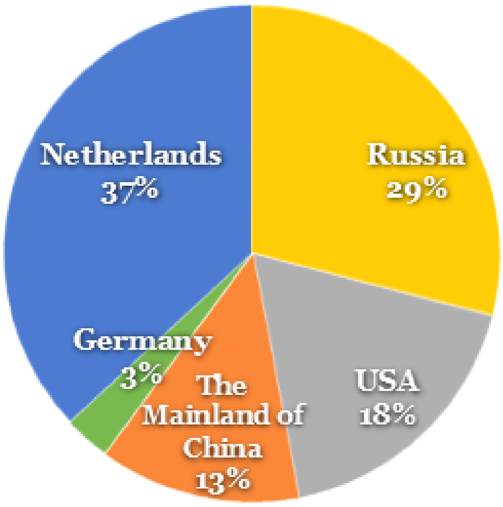
As a member of the TSUBAME project under APCERT, GovCERT.HK has set up sensors to collect and analyse network scanning activities targeting at Hong Kong. The following charts show the top five scanning ports (contributed 13% of all the scanning activities) and the top five source regions (contributed 76% of all the scanning activities) detected by the TSUBAME sensors installed in Hong Kong in 2020.

Top Five Scanning Ports against Hong Kong in 2020



Position in 2020	Port Number	Position in 2019
1	445/TCP	1
2	23/TCP	2
3	1443/TCP	5
4	22/TCP	4
5	80/TCP	-

Top Five Source Regions of Scanning against Hong Kong in 2020

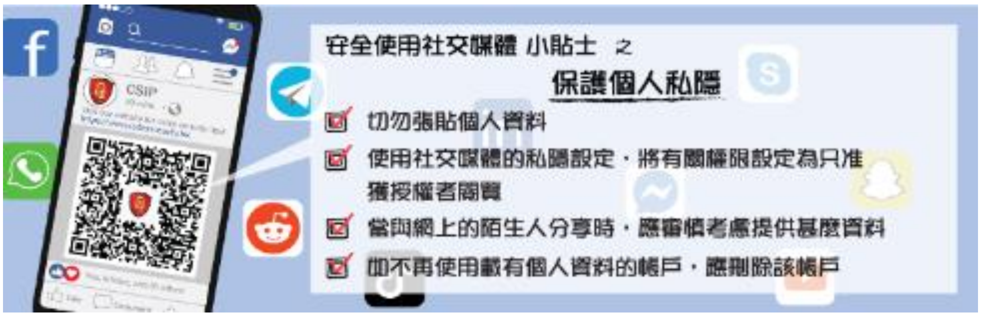


Position in 2020	Source Region	Position in 2019
1	Netherlands	3
2	Russia	1
3	USA	4
4	The Mainland of China	2
5	Germany	-

3.6 Publications and Mass Media

The COVID-19 epidemic has created new challenges in adapting the digitally transformed living. To actively reach out to the general public, various promotion channels including radio broadcast, YouTube, Facebook, Twitter, webinars, and school visits were used to share tips and best practices on using different technologies, such as mobile devices, cloud services, social networking applications and remote working applications under the new normal.

- We broadcasted radio episodes entitled “e-World Smart Tips” to help the public understand more about information security in various aspects and raise their awareness of the issue. The radio episode in each month featured a specific theme and offered associated tips on mitigating the risks of cyber threats through daily life examples and in a lively and interesting way. In 2020, we covered a wide range of topics including data security, phishing attacks, social networking security, IoT devices security, and more.
  (www.cybersecurity.hk/en/media.php#Radio)



安全使用社交媒體 小貼士 之

保護個人私隱

☑ 切勿張貼個人資料

☑ 使用社交媒體的私隱設定，將有關權限設定為只准獲授權者閱覽

☑ 當與網上的陌生人分享時，應審慎考慮提供甚麼資料

☑ 如不再使用載有個人資料的帳戶，應刪除該帳戶

- A series of handy guidelines with different themes were developed to provide practical tips and advice for SMEs to guard against cyber attacks.
  (www.cybersecurity.hk/en/resources.php#leaflets)

Information Security Guide for Small and Medium Enterprises
Security Tips for Remote Working
Secure Your Computing Devices and Remote Working Environment
Protect Your Data
Secure Your Network
Be Aware of Phishing Scam
Protect Your User Accounts
Provide Adequate Support for Remote Working
GovCERT.HK
www.cybersecurity.hk

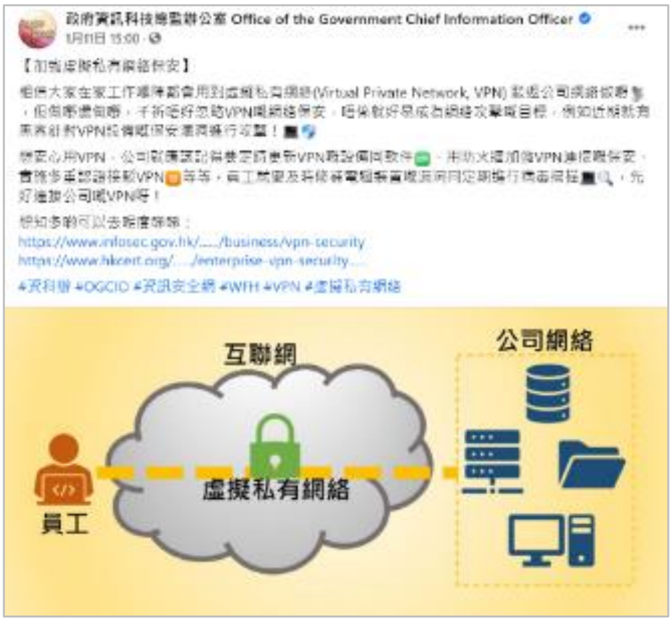
Information Security Guide for Small and Medium Enterprises
Security Tips for
e-Commerce
Security Tips for e-Commerce
GovCERT.HK
www.cybersecurity.hk

- To encourage the public to exercise care when using mobile devices and raise their awareness of mobile device security, we organised the “Secure Use of Mobile Devices” sticker design contest in 2020. Participants fully demonstrated their creativity to design a set of stickers for instant messaging applications to convey the message of taking precautions to protect mobile devices. The winning entries are now available at www.cybersecurity.hk/en/contest-2020.php. Download now and share with your family and friends!

Winning Entries

不明Wi-Fi要小心！
定期備份 安心隱陣
BEWARE OF MALWARE
密碼要夠強

- Leveraging the OGCIO Facebook page, we have shared a series of posts with timely updates and tips on cyber security topics such as precaution of phishing attacks and safe use of remote working applications. The posts were made in a light-hearted manner with eye-catching infographics and animations to strengthen our communications with the public. (www.facebook.com/ogciohk)


政府資訊科技總監辦公室 Office of the Government Chief Information Officer
1月11日 15:00

【加強虛擬私有網絡保安】

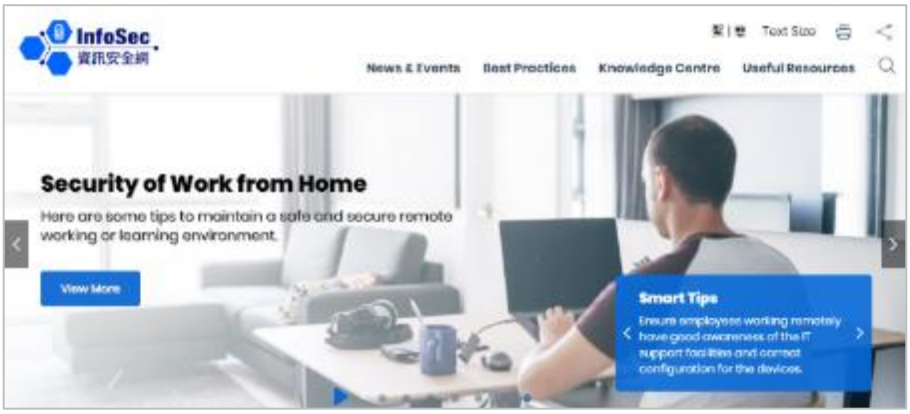
相信大家在家工作期間都會用到虛擬私有網絡(Virtual Private Network, VPN) 駁返公司網絡做嘢，但係需要留意，千祈唔好忽略VPN嘅網絡保安，唔係就好易成為網絡攻擊嘅目標，例如近期就有黑客針對VPN伺服器嘅保安漏洞進行攻擊！

想安心用VPN，公司就應該記得要定時更新VPN嘅設備同軟件，用防火牆加強VPN連接嘅保安，實施多重認證接駁VPN等等，員工就要及時檢查電腦裝置嘅版本同定期進行病毒掃描，先好連接公司嘅VPN呀！

想知多啲可以去睇睇呢度：
https://www.infosec.gov.hk/....../business/vpn-security
https://www.hkcert.org/...../enterprise-vpn-security...

#資科辦 #OGCIO #資訊安全網 #WFH #VPN #虛擬私有網絡

- In 2020, we have also revamped our InfoSec Website to provide a more lively design for disseminating security related tips and advice useful for all members of the public.
  (www.infosec.gov.hk)



Security of Work from Home

Here are some tips to maintain a safe and secure remote working or learning environment.

Smart Tips

Ensure employees working remotely have good awareness of the IT support facilities and correct configuration for the devices.

3.7 GovCERT.HK Technology Centre

To facilitate the Government in developing staff capabilities on more specialised knowledge and skills to tackle evolving cyber threats, our GovCERT.HK Technology Centre offers government departments a controlled environment with relevant facilities and equipment to enable vulnerability scanning, dynamic application security testing, penetration testing and malware analysis for potential security issues of their web applications. The overall security of government web applications and services is enhanced by making use of the tools to identify web vulnerabilities, misconfigurations, compromised passwords, etc.

Web vulnerability scan & dynamic application security testing

Penetration testing platform

Malware analysis corner

Password checker

GovCERT.HK Technology Centre

4. Events Organised/Hosted

GovCERT.HK regularly organises awareness training and solution workshops to share the latest knowledge on security measures, best practices, skills and security solutions with various levels of government users to continuously strengthen their knowledge on cyber attacks and enhance their information security skills, thereby strengthening their capabilities in guarding against cyber attacks.

4.1 Training

In 2020, we organised more than 10 seminars, webinars and trainings for government IT staff and users to raise their information security awareness and update their knowledge on the latest IT security technologies and solutions. More than 1 400 government staff participated in these events to understand the latest cyber security trends and preventive measures. Topics included information security management, IT governance, protection of personal data, security measures and best practices for remote working, defense against phishing, operating system security, promotion of various security solutions, etc.

4.2 Drills and Exercises

Inter-departmental Cyber Security Drill of the Government

To enhance the overall incident response capability of the Government, GovCERT.HK has actively coordinated government departments to conduct cyber security drills to enhance the participants' incident handling capabilities and test their familiarity with the predefined incident response procedures.

This year, we continued to organise the annual inter-departmental cyber security drill to strengthen the cyber security incident response capability of the Government. The drill was held in online mode due to the COVID-19 epidemic. We provided a simulated cyber attack scenario for participants to discuss and propose response actions based on the background information given. An incident response workshop was also organised to enhance the capabilities of participants in handling, investigating and analysing cyber attacks.

Government-wide Phishing Drill Campaign

To further strengthen government users' awareness and capabilities in defending against phishing attack, we have successfully completed the "Government-wide Phishing Drill Campaign" in 2020. More than 1.7 million of pseudo-phishing emails were sent out to all Government Internet email users and a general improvement on awareness of phishing emails was observed upon completion of the exercise. Apart from the drill, we organised a number of webinars to share the common findings and lesson learnt from the drills. We also launched a set of interactive phishing quizzes to continue promoting awareness of the issue in the government.

APCERT Drill

As an Operational Member of the APCERT, GovCERT.HK participated in the APCERT Drill with the theme of "Banker doubles down on Mining" in March 2020. GovCERT.HK played the role of Exercise Controller in addition to Player and Observer in the drill.

4.3 Conferences and Seminars

Build a Secure Cyberspace Promotional Campaign

To promote public awareness of mobile device security, GovCERT.HK adopted "Secure Use of Mobile Devices" as the theme in 2020. A series of promotional activities were organised for businesses, organisations, schools and the public to raise their awareness of adopting security measures proactively to better protect their mobile devices.

- Two webinars were organised under the "Build a Secure Cyberspace" promotional campaign in May 2020 and February 2021, aiming to promote public awareness of cyber security challenges in remote working and online learning during the epidemic, and taking precautions to protect mobile devices.

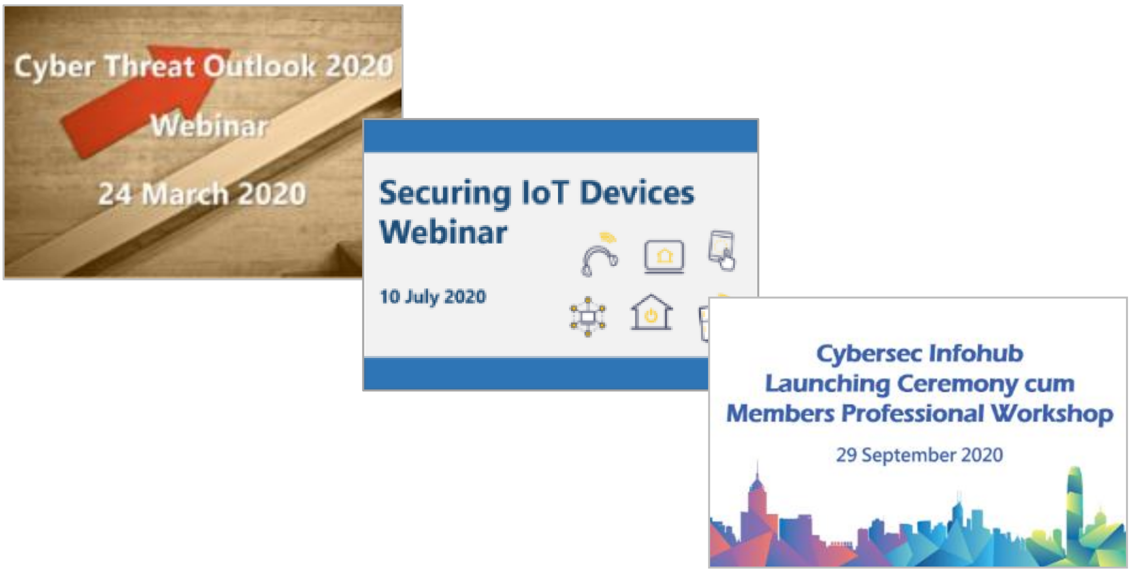
School visits and InfoSec Tours

To promote cyber security awareness and cyber etiquette to our community, GovCERT.HK organised visits to primary, secondary schools and tertiary institutions to deliver information security talks to students, teachers and parents. GovCERT.HK also partnered with the Radio Television Hong Kong (RTHK) to conduct InfoSec Tours, aiming to deliver information security message in a relaxing way by visiting schools and conducting a variety of activities.

- More than 20 face-to-face and online school visits were conducted in the 2019/20 and 2020/21 school years, reaching out to more than 5 000 students and parents for raising their awareness of cyber security and encouraging the proper attitude in using the Internet.
- In response to the increasing adoption of digital technology by the elderly in their daily lives, the OGCIO also conducted seminars for them to raise their cyber security awareness.
- One InfoSec Tour was conducted at a primary school in 2020. In view of the epidemic situation, we produced two InfoSec Tours videos with topics of "Study at home safely" and "Responding to the temptation of the online world" for broadcasting remotely.

Cybersec Infohub Engagement Activities

To encourage trust building, facilitate exchange of cyber security information and promote closer collaboration among different sectors under the Cybersec Infohub partnership programme, sector-specific events, professional workshops and webinars were arranged in 2020 with positive response from participants.



5. Local and International Collaboration

GovCERT.HK has been working closely with HKCERT and other regional and global CERTs to coordinate threat information sharing and incident response.

5.1 Local Collaboration

Cybersec Infohub

GovCERT.HK continued to promote closer collaboration among local information security stakeholders of different sectors to share cyber security information through the Cybersec Infohub programme (www.cybersechub.hk), with over 320 organisations and more than 1 000 representatives from various sectors joined the programme as of 2020. In particular, we have encouraged exchanges of cyber security information within key industries with higher risks to cyber attacks, such as banking and healthcare sectors. We have helped members from these sectors to form private groups for closer collaboration on specific topics of common interest.

The Cybersec Infohub started a new chapter in September 2020 through partnership with HKIRC in running the formalised programme to further encourage more organisations, including SMEs, to join and collaborate so as to bring Hong Kong's cyber security to a new level. A launching ceremony cum members professional workshop was held in September 2020 to embrace the bright future of the Cybersec Infohub and enlighten members on the salience of information sharing.

Cybersec Infohub Launching Ceremony
網絡安全資訊共享夥伴計劃 啟動儀式
29.8.2020
hkirc
.hk
Cybersechub.hk
網絡安全資訊共享協作平台

A cyber security supporting alliance of industry experts gathered, named Cybersec Connect, was also set up under the programme to answer cyber security-related questions from members, especially SMEs, and offer appropriate advice.

Internet Infrastructure Liaison Group (IILG)

To help maintain the healthy operation of the Internet infrastructure of Hong Kong, GovCERT.HK continued to support the IILG which was established and led by the OGCIO to foster closer liaison with the Internet infrastructure stakeholders, aiming to collaborate with the stakeholders for the smooth operation of the local Internet infrastructure. In 2020, the IILG collaboration mechanism was activated five times to support major events and take precautions against cyber threats, such as issuance of reminder to local Internet infrastructure stakeholders to stay vigilant against Distributed Denial-of-Service (DDoS) Extortion Attacks in September 2020.

HKCERT

Building cyber security awareness is one of the keys to defence against cyber attacks. To raise public awareness of cyber threats, we have been working with HKCERT for the new project “HKCERT Digital Campaign for Security Awareness Promotion” to produce and disseminate a series of animations covering topics on remote working and video conference, cloud security, phishing and malware, and IoT security via social media.

(www.youtube.com/watch?v=FH7zWAb4-GQ)

(www.youtube.com/watch?v=Jhzpcr7CeZw)

To nurture more talents to join the information security industry, and to enhance the cyber security awareness of local students, we supported HKCERT in organising a Capture the Flag (CTF) Challenge that provided students the opportunity to compete in cyber security tasks to gain real life experience in computer security.

HKIRC

We have also supported HKIRC to provide a free website scanning service to SMEs to help them identify and mitigate potential information security issues, as SMEs are generally with fewer resources devoted to cyber security and hence more vulnerable to cyber attacks.

5.2 International Collaboration

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

GovCERT.HK participated in the following events in 2020:

- FIRST Annual Conference
- Annual Technical Meeting for CSIRTs with National Responsibility
- CNCERT/CC Annual Conference
- CNCERT/CC Online Conference for International Partnership
- 2020 China Cybersecurity Week
- APCERT Annual General Meeting and Conference
- APCERT Drill
- APCERT Online Training Sessions
- APISC Security Training

6. Future Plans

6.1 Upcoming Projects

To meet the challenges of evolving security threats posed by emerging technologies and keep pace with the development of international standards and industry practices in information security management, we have conducted regular reviews to assess the latest cyber security trends and provide recommendations of necessary updates to the government IT security related regulations, policies and guidelines. We will continue to develop new practice guides on different technology areas for reference by government departments, and share these practice guides with the public where appropriate.

We will also collaborate with HKCERT to organise another CTF competition to nurture the next generation of information security talents and raise their interests in joining the cyber security workforce of the future. The competition will be divided into three groups, including secondary schools, tertiary institutions, and open group to make it more exciting.

6.2 Future Operations

Considering the continual growth of a wider spectrum of organisations in the membership base of Cybersec Infohub, information sharing via the collaborative platform will be further enhanced by integrating external threat intelligence feeds and enabling machine-to-machine sharing via Application Programming Interfaces (APIs). It will facilitate the members to integrate the invaluable cyber security information automatically with their information security systems for more timely response in safeguarding against potential cyber threats.

7. Conclusion

Cyber security attacks are increasingly targeted and sophisticated, with the forms they take becoming more diversified. GovCERT.HK has been proactively collaborating with local and global CERTs to take forward communication and make timely responses in facing the transboundary cyber security threats. In facilitating Hong Kong to become a secure smart city, GovCERT.HK will continue to encourage effective exchange of cyber security information and raise situational awareness of community stakeholders to stay keen of the fast evolving cyber security landscape, with unceasing efforts to enhance the cyber security resilience capability of the community.

Contact: cert@govcert.gov.hk
Websites: www.govcert.gov.hk
www.cybersechub.hk
www.cybersecurity.hk
www.infosec.gov.hk

HKCERT

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

1. Highlights of 2020

1.1 Summary of Major Activities

- Organised the "Build a Secure Cyberspace 2020" campaign with the Government and Hong Kong Police Force. The campaign involved public seminars, and a Mobile Sticker Design Contest.
- Organised the first "Hong Kong Cyber Security New Generation Capture the Flag Challenge 2020". It involved a 48-hours online contest and a public seminar with award ceremony.
- Presented in different international conferences and local press briefing.
  - "Introduction of HKCERT IoT Security Best Practice" in NatCSIRT Conference.
  - "Performing IoT Security Testing" in APCERT Training Workshop.
  - "Cyber Security Status of SMEs in HK" in 2020 APEC SME Cyber Security Forum.
  - "Year Ender" in local medias briefing.
- Published timely security guidelines and advisories in response to the digital transformation during the COVID-19 pandemic period.

1.2 Achievements & Milestones

- Conducted a strategy and service review by external assessor. Findings and improvement areas are shared in the advisory group meeting and incorporated in the strategic plan.
- Revamp the official website for better support of mobile users and improving user experience.
- Produced animation videos and leveraged social media platform to promote cyber security awareness to general public.
- Published IoT Security Study and Best Practices for local enterprises and IoT developers.
- Launched HKCERT LinkedIn Page to target for different user groups.

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 2020, HKCERT had handled 8,346 security incidents which was 12% decrease of the previous year (see Figure 1). Referral cases accounted for 95% of the total number of security incidents.

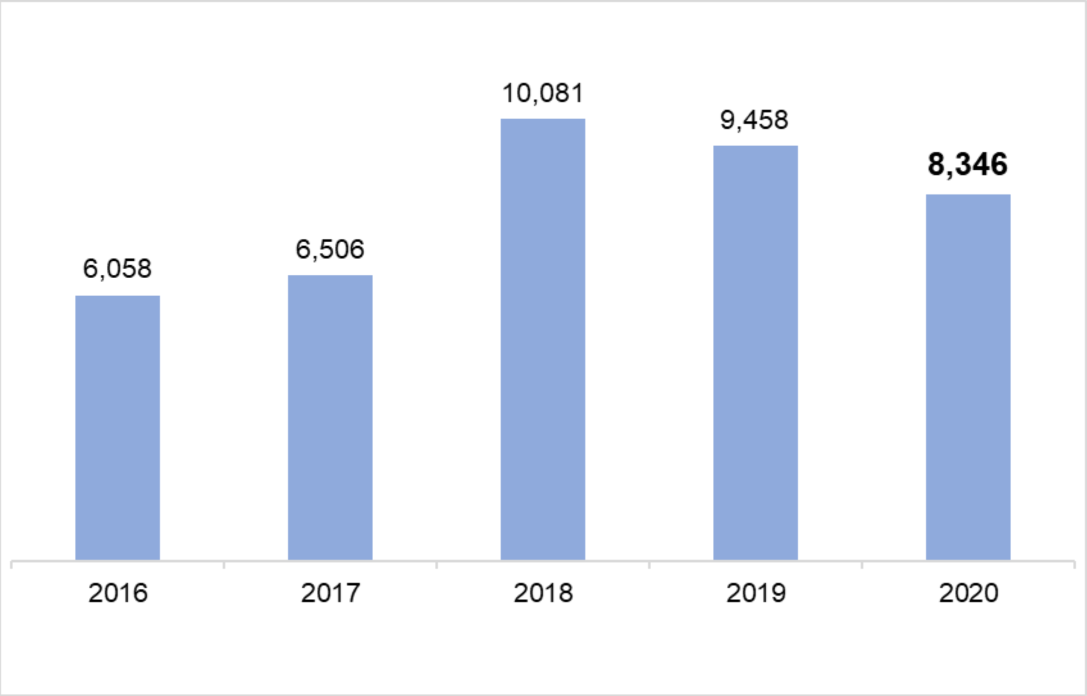


Figure 1. HKCERT Security Incident Reports

While the number of overall security incidents handled by HKCERT reported a drop for the second year running, falling 12% year-on-year to 8,346 in 2020. Phishing (3,483 cases or 42%) went up 35% with cyber criminals exploiting the surge of online activities due to the pandemic. On the other hand, botnets (4,154 cases or 50%), remaining the top source of reported incidents, and malware (181 cases or 2%) fell 16% and 85% respectively. The drop of malware cases was due to more malware targeting enterprises for higher return and the number of individual based reports significantly dropped (see Figure 2).

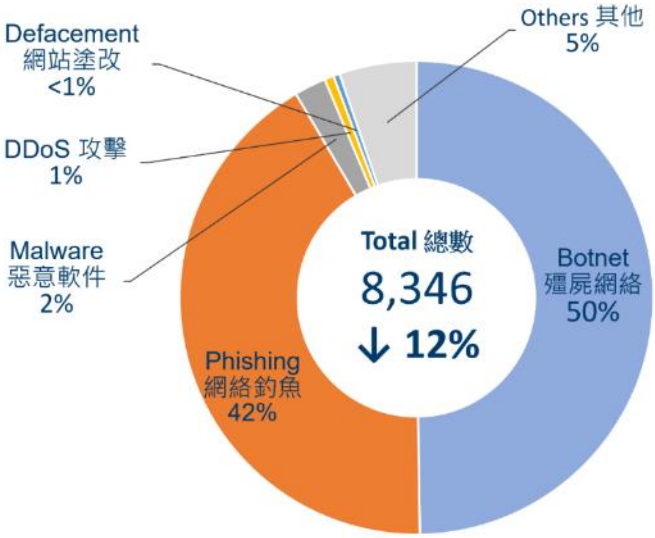


Figure 2. Distribution of Incident Reports in 2020

3.2 Watch and Warning

During the period from January to December of 2020, HKCERT published 315 security bulletins (see Figure 3) on the website. In addition, HKCERT have also published 43 blogs, including security advisories on home office, online conferencing tools, personal VPN service, enterprise VPN security, DDoS extortion attacks, ransomware trends, TLS version upgrade, etc.

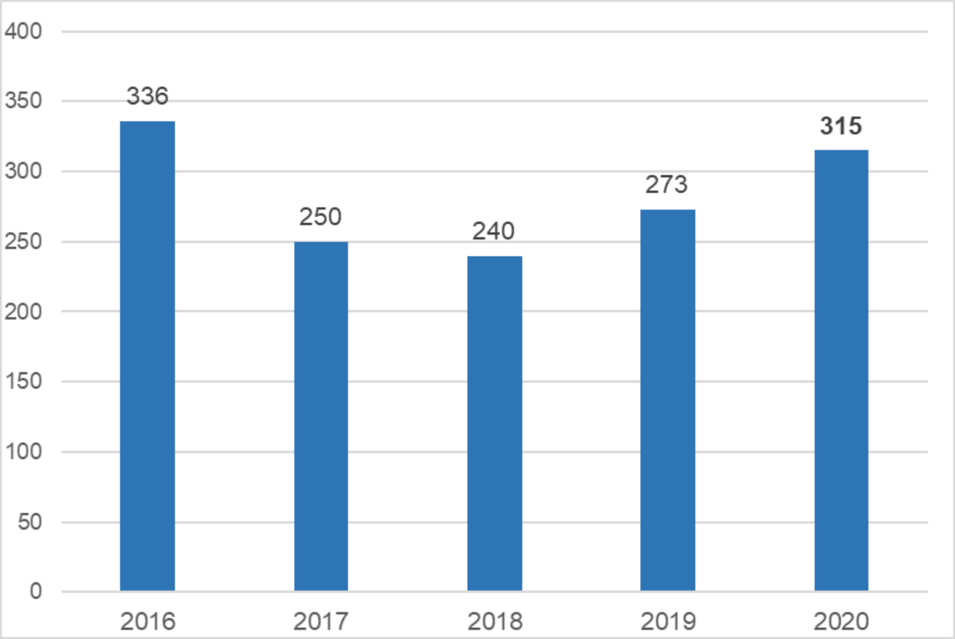


Figure 3. HKCERT Published Security Bulletins

The drop of Security Bulletins in 2017 was mainly due to consolidation of MS & Adobe 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 8,017 in 2020 Q1 and dropped gradually to 4,372 in Q4 2020, largely attributed to the Mirai botnet events as depicted in Figure 5.

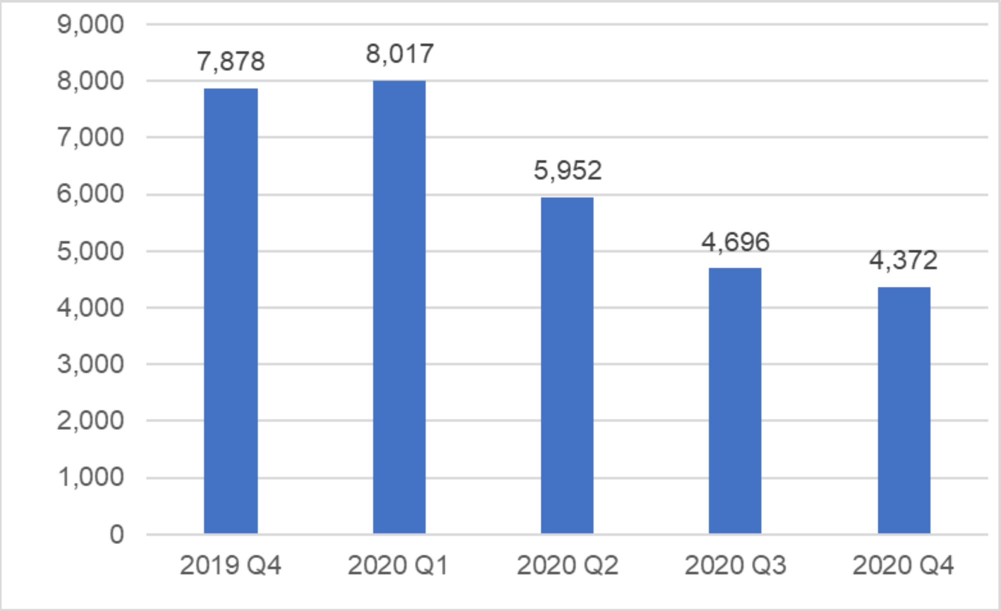


Figure 4. Trend of Bot related security events in the past year
(Source: data feeds from overseas security researchers, not from incident reports)

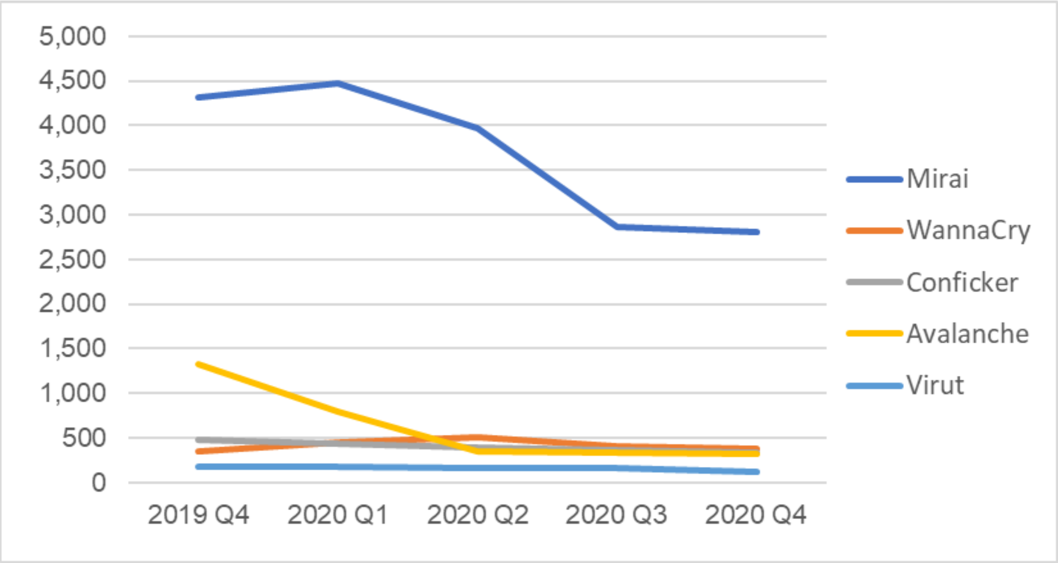


Figure 5. Trend of Top 5 Botnet Families in the past year

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

3.3 Publications

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

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

- HKCERT had published the statistics of incident reports every quarter (see Figure 6) (see https://www.hkcert.org/statistics).

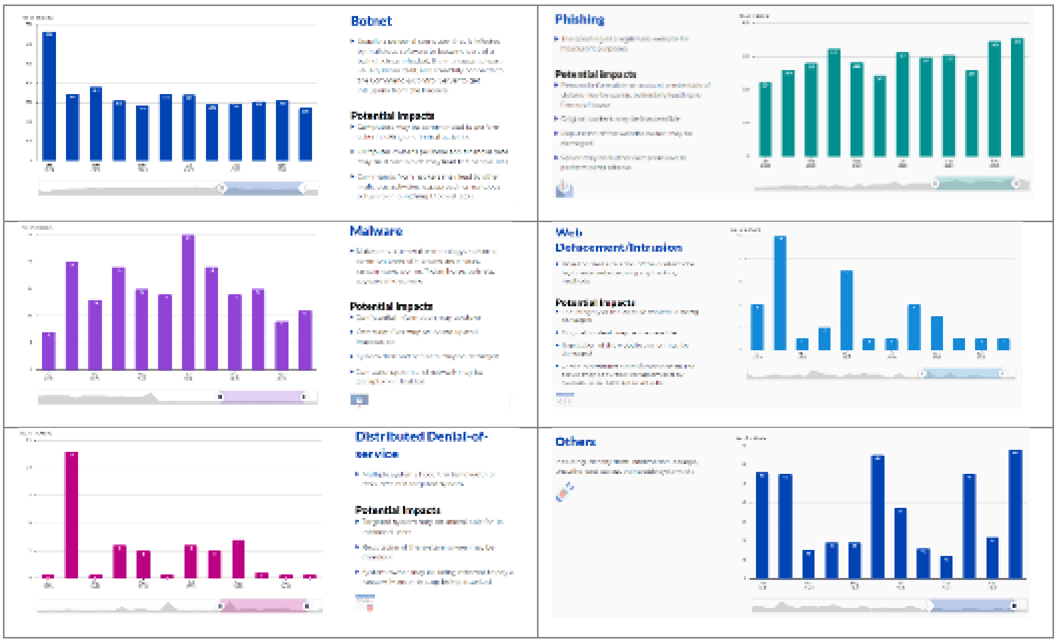


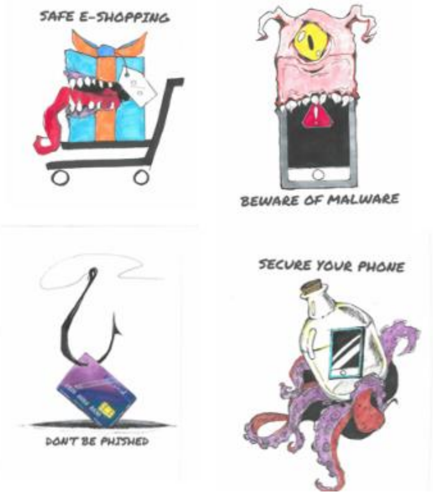
Figure 6. Charts in HKCERT website showing the statistics of different types of incident reports.

4. Events organised and co-organised

4.1 Seminars, Conference and Meetings

HKCERT jointly organised the "Build a Secure Cyberspace 2020" campaign with the Government and Hong Kong Police Force. The campaign involved public seminars, and a Mobile Sticker Design Contest. A public seminar was organised in May 2020.

For the Poster Design Contest, HKCERT received about 546 applications from Open Group, Family Group, Secondary School and Primary School Group. A professional judge panel selected winners with most creative and outstanding poster design (see Figure 7).

Primary Group Champion	Secondary Group Champion
	 SAFE E-SHOPPING BEWARE OF MALWARE DON'T BE PHISHED SECURE YOUR PHONE

Open Group Champion

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

Use this link to access the winning entries online:

https://www.cybersecurity.hk/en/contest-2020.php

4.2 Capture The Flag Contest

HKCERT jointly organised the "Hong Kong Cyber Security New Generation Capture the Flag Challenge 2020" with partner associations in information and education sectors. The 48-hours contest was opened to secondary and tertiary institutions. It was a success with 156 teams and 541 students participating. A public seminar with award ceremony was organised in November 2020.

HKCERT
hkpc
AiTLE
BLACK BAUHINIA
eLEARNING CONSORTIUM
Internet Society Hong Kong Chapter
PISA
VXRL
Hong Kong Cyber Security New Generation Capture the Flag Challenge 2020

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-2020-webinar-and-award-presentation-ceremony
https://www.hkcert.org/press-center/the-capture-the-flag-challenge-2020-award-presentation-ceremony-recognises-cyber-security-future-talents

4.3 Speeches and Presentations

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

4.4 Proactive Approach to Promote Awareness for Different Sectors in HK

HKCERT proactively approached several sectors in HK to promote cyber security awareness, e.g. travel industry, retail and securities, etc.

4.5 Media Promotion, Briefings and Responses

HKCERT invited 4 media agencies for a roundtable sharing on the summary of first half year of 2020 based on Hong Kong Security Watch Report. During the session, HKCERT also shared the cyber security posture and security advices in the New Normal era.

5. Collaboration

5.1 International Collaboration

HKCERT participated in a number of international coordination and collaboration events in year 2020:

- Delivered “Introduction of HKCERT IoT Security Best Practice” presentation in

NatCSIRT Conference

- Delivered “Performing IoT Security Testing” in APCERT Training Workshop
- Delivered “Cyber Security Status of SMEs in HK” presentation in 2020 APEC SME Cyber Security Forum
- Participated in the APCERT AGM and Web Conference
- Participated in the FIRST AGM and Web Conference
- Participated in CNCERT Annual Web Conference
- Participated in the HITCON Annual Web Conference
- Participated in the AusCERT Annual Web Conference
- Participated in (ISC)2 APAC Security Congress
- Participated in APCERT Drill and OIC-CERT Cyber Security Drill Exercise

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

5.2 Local Collaboration

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

- HKCERT continued to work closely with the government (GovCERT.HK) and law enforcement agency and held meetings to exchange information and to organise joint events regularly.
- HKCERT continued to actively participate in the Cyber Security Information Sharing platform ‘Cybersec Infohub” which comprised of over 300 companies, critical infrastructure organisations, banks and other enterprises in Hong Kong.
- HKCERT continued to work with police, ISPs and domain registries on closing down bulletproof hosting, phishing sites and botnet command and control centres in Hong Kong.
- HKCERT collaborated with Microsoft in the Healthcare Cyber Security Watch Programme to promote cyber security situational awareness in healthcare sector. The objective of this programme is to make use of global cyber threat intelligence to inform Hong Kong Healthcare sector of attacks targeting their IT infrastructure so that they can better mitigate security risks. The Programme was officially launched in December 2020 with 12 organisations including the Hospital Authority and most of the private hospitals in Hong Kong joining.

6. Achievements & Milestones

6.1 Strategy and Service Review

HKCERT had conducted a Strategy and Service Review by external reviewer in October 2019. The findings and improvement areas were received by HKCERT and OGCIO Hong Kong SAR Government in 2020.

6.2 Advisory Group Meeting

HKCERT had held the Advisory Group Meeting in October 2020. The meeting solicited inputs from the advisors on the development strategy of HKCERT.

6.3 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.

6.4 HKCERT Website Revamp

HKCERT had revamped the official website (https://www.hkcert.org) in Dec 2020. The new website is enhanced with modern look and feel. It brings several benefits to users including: (1) adopted responsive design which provides greater support for mobile users; (2) enhanced the search function with better result relevance; (3) customisable RSS subscription (4) provided interactive chart for incident report statistic.

6.5 Cyber Security Awareness Video Campaign

HKCERT had produced a series of cyber security animation videos and leveraged social media to promote to local public. The aim was to raise their cyber security awareness. The series had 4 episodes using the theme “Hack me if you can”. The first episode about the security tips for remote work and video conferencing software was published in Dec 2020. The other 3 episodes will be published by Mar 2021.

Remote Work and Web Meeting Security Tips

https://youtu.be/FH7zWAb4-GQ

6.6 IoT Security Study and Best Practice

HKCERT placed more efforts in IoT Security. HKCERT joined the APCERT IoT Security Working Group. Further to the IoT Device (Webcam) Security Study released in 2019, in Q1 of 2020, HKCERT released the IoT Security Best Practice and several studies in IoT wireless network protocols: ZigBee, Wi-Fi and Bluetooth.

6.7 Security Guidelines and Advisories for the COVID-19 Pandemic

HKCERT published different security guidelines and alerts in response to the digital transformation during the COVID-19 pandemic period, such as guidelines for enterprise and personal VPN, remote access services, online meetings, security tips for home office and advisories on COVID-19 themed attacks.

6.8 HKCERT LinkedIn Page

HKCERT launched its LinkedIn page to target for different types of local Internet users and increase visibility.

6.9 Embrace Global Intelligence and Build Security Health Metrics

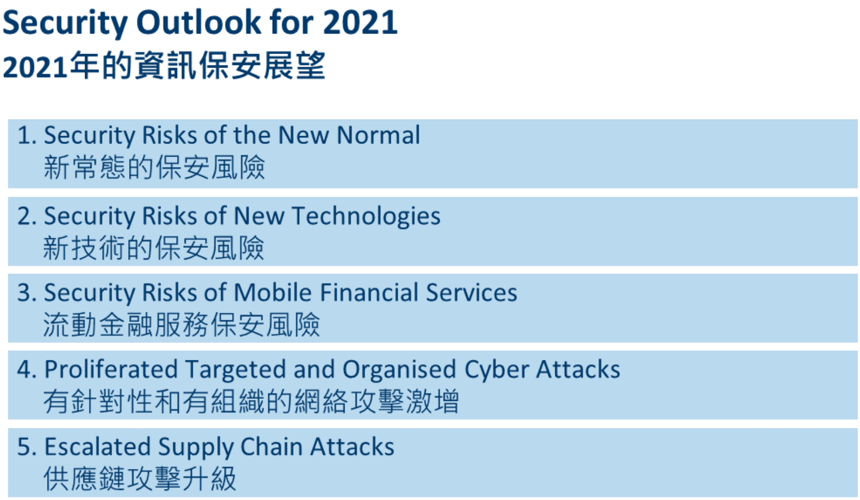
HKCERT had implemented the IFAS to collect intelligence of compromised machines in Hong Kong. The system provided a better picture of security status of Hong Kong and help clean up the botnets and C&C servers in Hong Kong. HKCERT publicised the information to the public quarterly and used the information 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 January 2021 to review cyber security landscape of 2020 and provided an outlook to 2021 to warn the public for better awareness and preparedness. It received very good press coverage.



Security Outlook for 2021
2021年的資訊保安展望

1. Security Risks of the New Normal
新常態的保安風險
2. Security Risks of New Technologies
新技術的保安風險
3. Security Risks of Mobile Financial Services
流動金融服務保安風險
4. Proliferated Targeted and Organised Cyber Attacks
有針對性和有組織的網絡攻擊激增
5. Escalated Supply Chain Attacks
供應鏈攻擊升級

Figure 8. HKCERT at the Year Ender press briefing.

7. Future Plans

7.1 Strategy

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

7.2 Funding

HKCERT had secured Government funding to provide the basic CERT services in 2021/2022. We shall work closely with the Government to plan for the future services of HKCERT and seek their support.

7.3 Enhancement Areas

In the coming year, with the success of the first Capture The Flag (CTF) contest, HKCERT will continue to partner with different associations to organise another CTF in 2021. Beside the local secondary school and tertiary institution groups, HKCERT will also add the open group contest.

HKCERT will enhance internal incident reporting systems to automate the response and handling process. HKCERT will partner with different security organsiations or companies to provide situational threat intelligence information to the general public in order to raise the awareness and improve the cyber hygiene.

8. Conclusion

In 2020, the number of overall security incidents reported to HKCERT recorded a drop for the second year running. Phishing increased by 35% with cyber criminals exploiting the surge of online activities amid pandemics. On the other hand, botnet and malware fell 16% and 85% respectively. The latter was due to a drop of massive individual ransomware cases as cyber criminals moved to target enterprises for higher monetary return.

In 2021, HKCERT urges enterprises to quickly put in place cyber security strategy for the new normal and new technologies, in order to combat an anticipated surge in cyber attacks arising from accelerated digital transformation amid the pandemics and the use of emerging technologies such as 5G communication, Internet of Thing (IoT) and AI. Furthermore, HKCERT also urges enterprises to be ready for an escalation in supply chain attacks in which attackers leverage on the trust of an enterprise on its supply chain partners to bypass traditional defences. HKCERT will also promote cloud security and groom the next generation cyber security talents.

ID-SIRTII/CC

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

1. Highlights of 2020

1.1 Summary of major activities

Activities of Id-SIRTII/CC in 2020 consist of:

- Indonesia as Deputy Chair of OIC-CERT 2018-2020
- Indonesia as Board Member of OIC-CERT 2018-2020
- Establishment of National CSIRT Indonesia (Indonesia Nat-CSIRT)
- 11 March 2020: Participating in APCERT Cyber Drill Test 2020
- 25 June 2020: Participating in ASEAN-Japan Cyber Exercise
- 11-12 August 2020: Participating in Cyber Exercise (CII Cyber-X) 2020
- 21-22 September 2020: Participating in 8th Arab Regional and OIC Cert Cyber Drill
- 7 October 2020: Participating in the 15th ASEAN CERT Incident Drill (ACID) 2020
- The International Telecommunication Union (ITU) Cyber Drill Exercise 27 October - 5 November 2020
- 8 July 2020: Participating in APCERT Meeting "Working Group IoT Report"
- 15-17 September 2020: Participating in Creating and Managing CSIRT Training by CERT Division, Software Engineering Institute (SEI), Carnegie Mellon University
- 23 September - 2 October 2020, participating in Defense Practice Against Cyber Attacks Training, JICA.
- 29 September 2020: APCERT Annual General Meeting
- 16 November 2020: APCERT Meeting "Working Group IoT Report" (Continued)

1.2 Achievements & milestones

- Speaker in Work Group Discussion about cyber security in regional election. (12 August, 25 August, 8 September, 26 October 2020)
- Involved in Cyber security of Regional election 2020.
- Conducted regional CSIRT assistance
- Participated in Indonesia - US Forum

2. About CSIRT

2.1 Introduction

Id-SIRTII/CC (Indonesia Security Incident Response Team on Internet Infrastructure/Coordination Center) is the national CSIRT of Indonesia and has the main duty to socialize with stakeholders related to Internet Security, to do an early monitoring and detection, give an early warning against threats to telecommunication monitoring and detection, give an early warning against threats to telecommunication networks from both inside and out networks from both inside and outside country, particularly in the security measures of side country, particularly in the security measures of network utilization, creating/performing/developing log files and statistics of network utilization, creating/performing/developing log files and statistics of Indonesian's internet security.

2.2 Establishment

Id-SIRTII/CC is established on 4 May 2007 by Minister of Communication and Information Decree number 26 in 2007. Id SIRTII/CC has a function as National CSIRT and Coordination Center for national incident handling and work under Directorate of Telecommunication of the Ministry. Based on Presidential Decree number 53 in 2017, Id SIRTII/CC merged and moved to National Cyber and Crypto Agency and works under its National Cyber Security Operation Center since April 2018.

2.3 Resources

ID-SIRTII consist of 181 staff members who are also the personnel of National Security Operation Center.

As an active member of the Forum for Incident Response and Security Teams (FIRST), Asia-Pacific Computer Emergency Response Team (APCERT), and also Organization of Islamic Countries Computer Emergency Response Team (OIC-CERT), ID-SIRTII has access to accurate, timely, and reliable information about emerging computer network threats and vulnerabilities on regional and global basis.

2.4 Constituency

Id-SIRTII/CC constituencies are:

- ICT Community, which is IT-security teams and professionals.
- Local CSIRT's in Indonesia, which is ACAD-CSIRT an Academic CSIRT forum, Govt-CERT a Government CSIRT under MCIT, Local Government CSIRT and

Industry Sector CSIRT.

- Internet Core Infrastructure, which are Network Access Provider (NAP), Internet Service Provider (ISP) and Local Exchange and Data Center Operator (LEO).
- Law Enforcement Agency (LEA), which is National Police, Attorney at General.
- Government agencies, which is Ministry of Law and Human Rights, Ministry of Communication and Information Technology, etc. and especially to any agencies related with National Critical Infrastructure.
- Basically – as The National CSIRT/CC of Indonesia – Id-SIRTII/CC is mandated to take responsibility to any other constituencies that are not yet be serviced by any other CSIRT. We will engage upon request.
- For awareness purposes, pro-active educational material will be provided to the constituencies, SME's and general public as well.

3. Activities & Operations

3.1 Scope and definitions

In 2020, Id-SIRTII/CC under National Security Operation Center BSSN conducted national monitoring activity, and the report can be summarized as follows:

- Received 1.293 complaint reports in total. Most of report coming from governments sector with 660 (51%) reports. XSS and SQL Injection became the most attacks reported, 464 reports about XSS and 451 about SQL Injection.
- Id-SIRTII/CC recorded 495.337.202 traffic anomalies both from local and overseas, which are dominated by trojan activity, the graph is shown in the following figure.

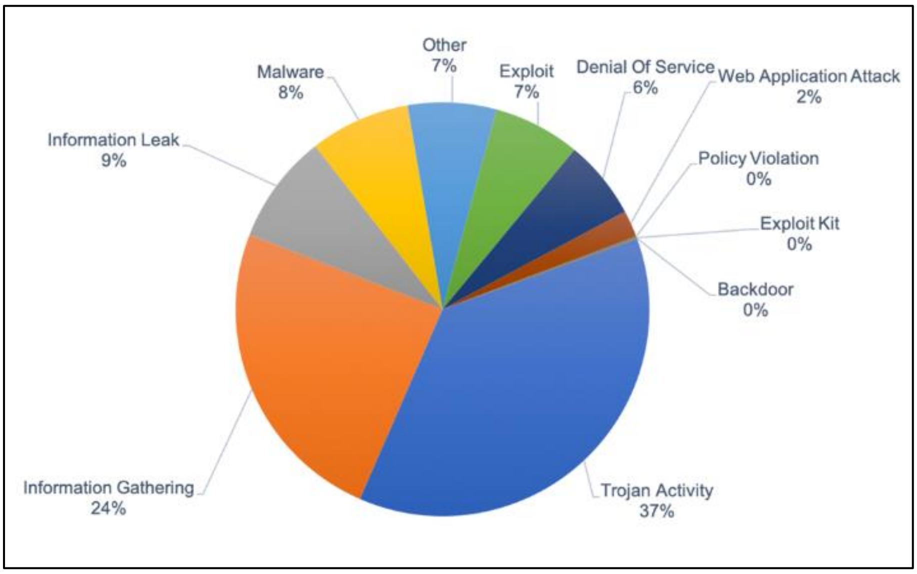


Figure 1. Traffic anomaly category

3.2 Incident handling reports

Incident report to Id-SIRTII/CC in 2020 were categorized as shown in the Figure 2 (attack type) and Figure 3 (reported sector). About 51% of the reports came from government sector, 33% from digital economy sector, and the rest was from national critical infrastructure sector.

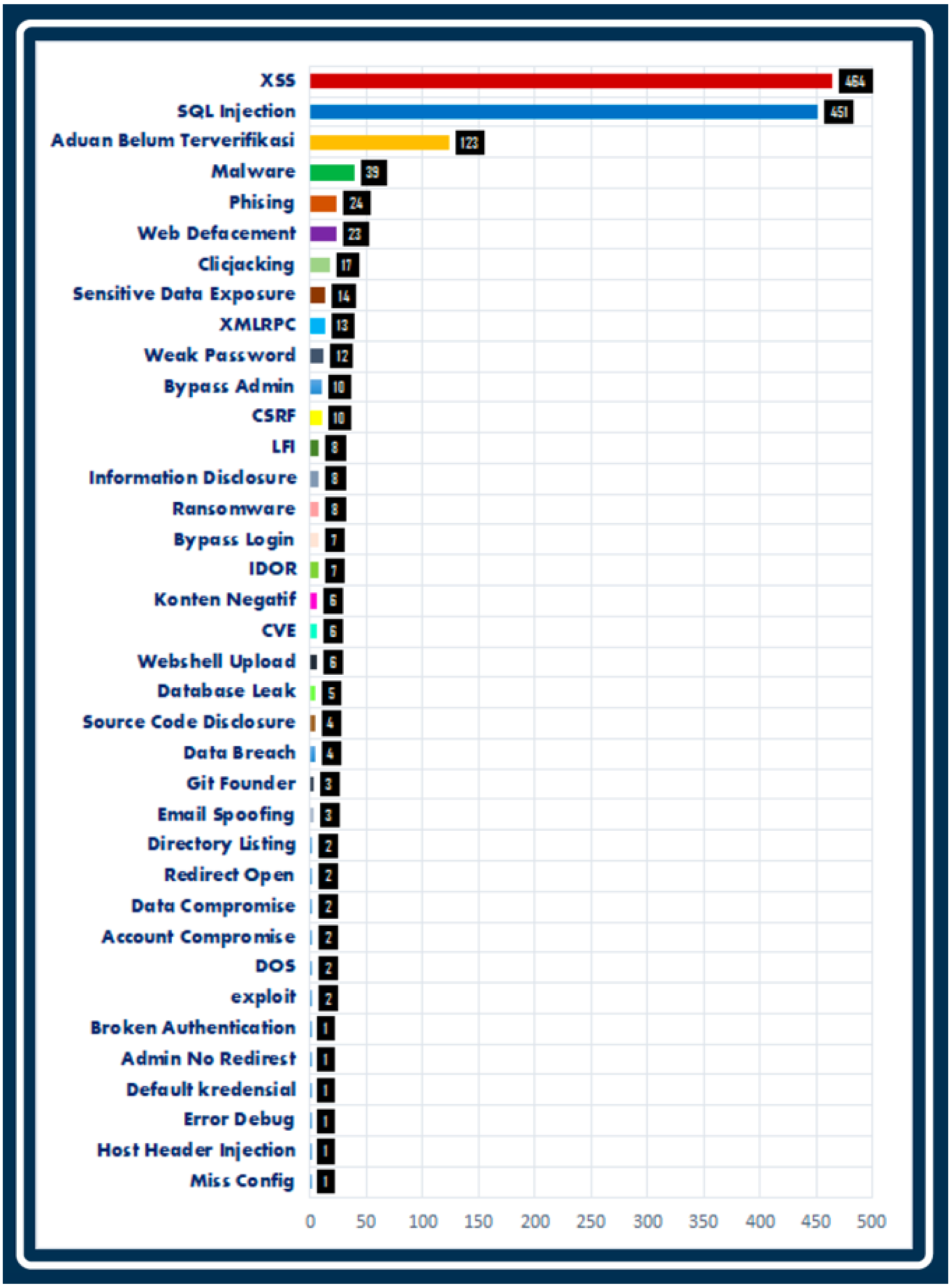


Figure 2. Reports in 2020 based on reported attack type

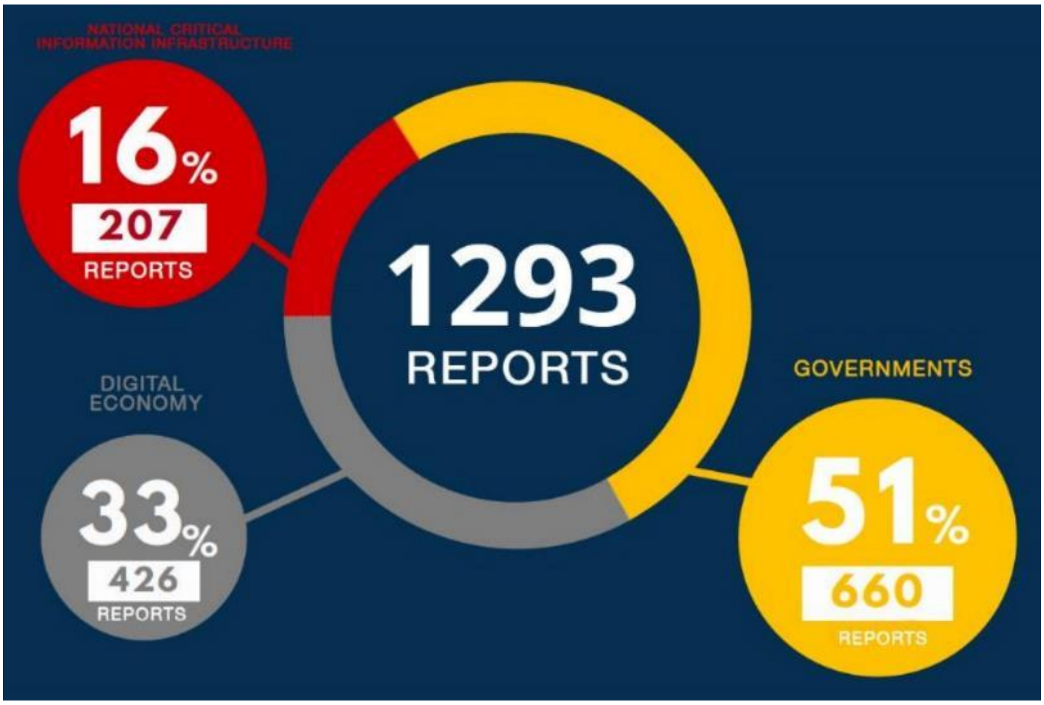


Figure 3. Reports in 2020 based on reported sector

3.3 Abuse statistics

There are many misuses of websites and infrastructure in Indonesia as a (CnC), that has increased significantly in September 2020, this condition persists until October 2020.

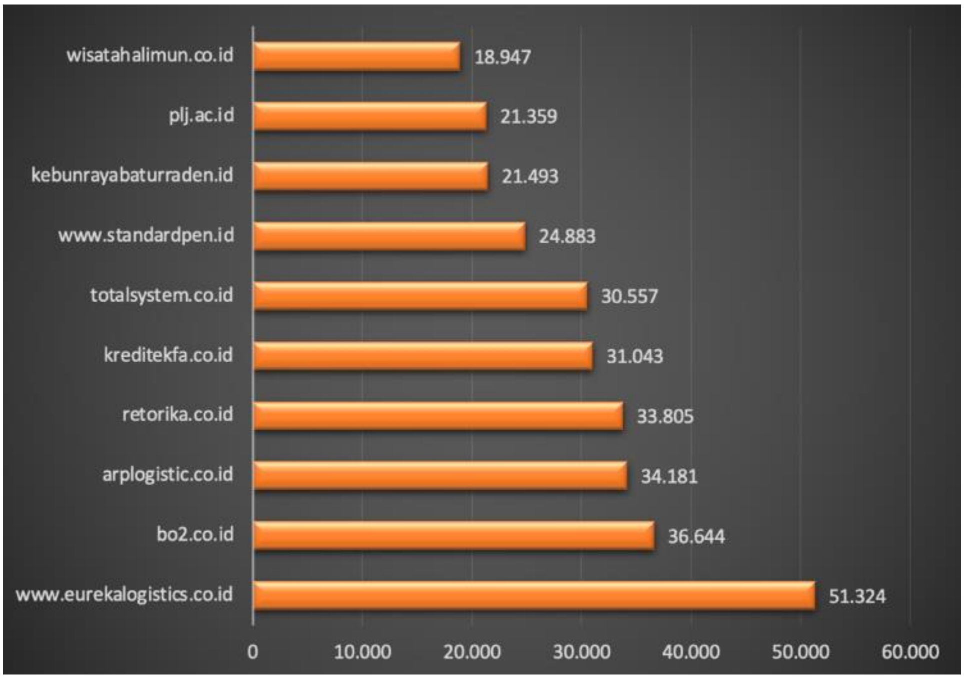


Figure 4. Top 10 Indonesian Domains that are misused as Malware CnC in 2020

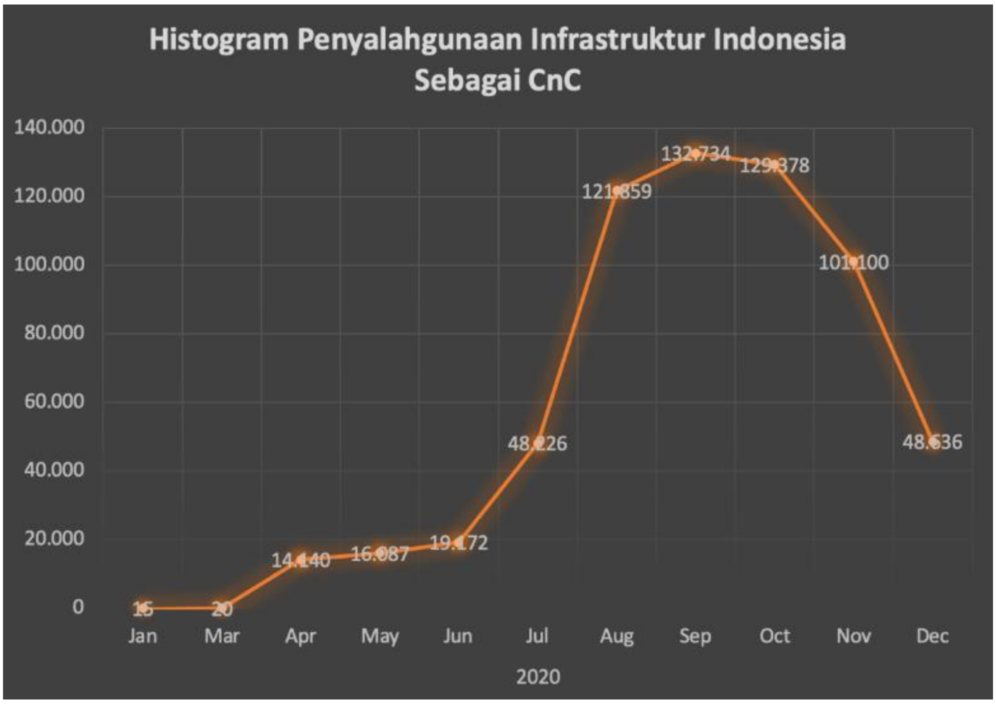
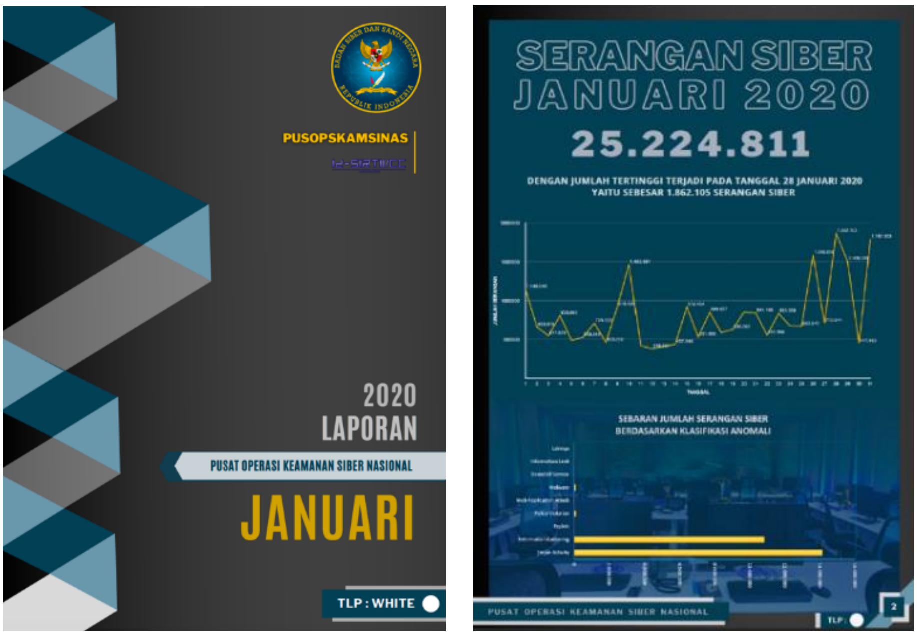


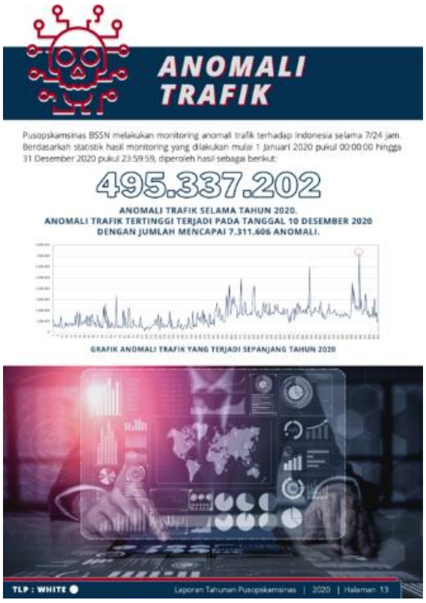
Figure 5. Histogram shows the amount of the misuse to Indonesian website as Malware CnC

3.4 Publications

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


PUSOPSKAMSINAS
2020
LAPORAN
PUSAT OPERASI KEAMANAN SIBER NASIONAL
JANUARI
TLP : WHITE
SERANGAN SIBER
JANUARI 2020
25.224.811
DENGAN JUMLAH TERTINGGI TERJADI PADA TANGGAL 28 JANUARI 2020
YAITU SEBESAR 1.862.105 SERANGAN SIBER
SEBARAN JUMLAH SERANGAN SIBER
BERDASARKAN KLASIFIKASI ANOMALI
PUSAT OPERASI KEAMANAN SIBER NASIONAL
TLP:
2

Id-SIRTII/CC January 2020 monthly report



ANOMALI TRAFIK

Pusopskamsinas BSSN melakukan monitoring anomali trafik terhadap Indonesia selama 7/24 jam. Berdasarkah statistik hasil monitoring yang dilakukan mulai 1 Januari 2020 pukul 00:00:00 hingga 31 Desember 2020 pukul 23:59:59, diperoleh hasil sebagai berikut:

495.337.202

ANOMALI TRAFIK SELAMA TAHUN 2020.
ANOMALI TRAFIK TERTINGGI TERJADI PADA TANGGAL 10 DESEMBER 2020 DENGAN JUMLAH MENCAPAI 7.311.606 ANOMALI.

GRAFIK ANOMALI TRAFIK YANG TERJADI SEPANJANG TAHUN 2020

TLP : WHITE ● Laporan Tahunan Pusopskamsinas | 2020 | Halaman 13

Id-SIRTII/CC 2020 annual report.

3.5 New services

Information Sharing in Id-SIRTII/CC portal and social media (Twitter).

4. International Collaboration

4.1 International partnerships and agreements

- Indonesia - US Cyber Meeting

4.2 Capacity building

4.2.1 Training

- 26 January - 7 February 2020: Participating in Capacity Building in Policy Formation for Enhancement of Measures to Ensure Cybersecurity in ASEAN Region, organized by Japan International Cooperation Agency (JICA).
- 23 September - 2 October 2020: Participating in Defense Practice Against Cyber Attacks Training, Japan International Cooperation Agency (JICA) (Online Program).

4.2.2 Drills & exercises

- 11 March 2020: Participating in APCERT Cyber Drill Test 2020
- 25 June 2020: Participating in ASEAN-Japan Cyber Exercise
- 11-12 August 2020: Participating in Cyber Exercise (CII Cyber-X) 2020

- 21-22 September 2020: Participating in 8th Arab Regional and OIC Cert Cyber Drill
- 7 October 2020: Participating in the 15th ASEAN CERT Incident Drill (ACID) 2020
- The International Telecommunication Union (ITU) Cyber Drill Exercise 27 October - 5 November 2020

4.2.3 Seminars & presentations

- 29 September 2020: APCERT Annual General Meeting

4.3 Other international activities

- 8 July 2020: Participating in APCERT Meeting "Working Group IoT Report"
- 16 November 2020: APCERT Meeting "Working Group IoT Report" (Continued)

5. Future Plans

5.1 Future projects

ID-SIRTII on behalf of the National Security Operation Center, BSSN, is currently working on establishing 121 CSIRT (industry, company, and regional). On March 2021, there are 15 CSIRT that are already established and launched.

5.2 Future Operation

- Collaborating with relevant ministries about establishing CSIRT, especially the critical infrastructure sectors.
- Collaborating with Bank of Indonesia (BI) & and Indonesia Financial Services Authority (OJK) on handling data breach in financial sector

Office address:

Jl.Harsono RM 70 Ragunan, Pasar Minggu, Jakarta Selatan 12550
URL: https://www.idsirtii.or.id/ https://www.bssn.go.id/
E-mail:info@idsirtii.or.id bantuan70@bssn.go.id
Telp. +62 21 780 5814 or +62 21 788 33610

JPCERT/CC

Japan Computer Emergency Response Team / Coordination Center – Japan

1. Highlights of 2020

1.1 Summary of major activities

- Released EmoCheck, an Emotet detection tool

  JPCERT/CC developed EmoCheck, an Emotet detection tool, and released it on February 3. If a computer is infected with Emotet, this tool will locate the malware so that it can be removed. After the tool's initial release, new versions of Emotet which evade the detection were found on the Internet, and EmoCheck's detection method was updated multiple times as well.

  GitHub: JPCERT/CC / EmoCheck
  https://github.com/JPCERTCC/EmoCheck

  JPCERT/CC Eyes: How to Respond to Emotet Infection (FAQ)
  https://blogs.jpcert.or.jp/en/2019/12/emotetfaq.html

- Released Business E-mail Compromise Survey Report

  On 25 March, JPCERT/CC released the Business E-mail Compromise Survey Report, which summarized the results of a survey it conducted to investigate the actual situation of Business E-mail Compromise (BEC) in Japan with the cooperation of Japan Foreign Trade Council ISAC, the Japan Petrochemical Industry Association, and other organizations. The English version of the report was later published on 11 June.

  Business E-mail Compromise Survey Report
  https://www.jpcert.or.jp/english/pub/sr/BEC-survey.html

- Released IoT Security Checklist (English version)

  On 6 November, JPCERT/CC released the English version of IoT Security Checklist. It lists 39 essential security functions that enable IoT devices to be operated safely. By using this checklist to evaluate an IoT system that is under development or planned to be deployed, it is possible to determine quickly whether the functions necessary to ensure security of the IoT system are provided, and identify any matters that need further consideration.

IoT Security Checklist
https://www.jpcert.or.jp/english/pub/sr/IoT-SecurityCheckList.html

1.2 Achievements & milestones

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

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

2. About JPCERT/CC

2.1 Introduction & Establishment

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

2.2 Constituency

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

3. Activities & Operations

3.1 Incident Handling Reports

In 2020, JPCERT/CC received 43,823 computer security incident reports from Japan and overseas.

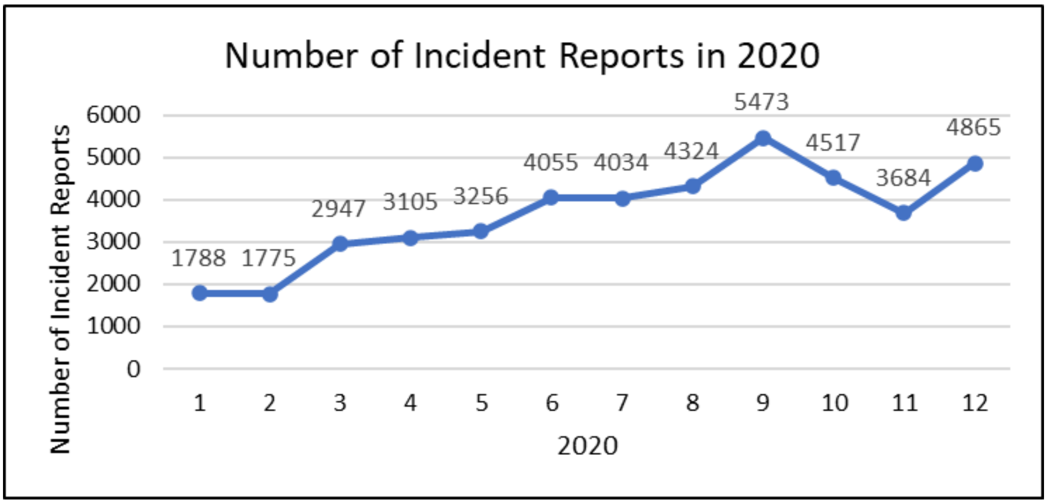


Figure 1. Number of Incident Reports (2020)

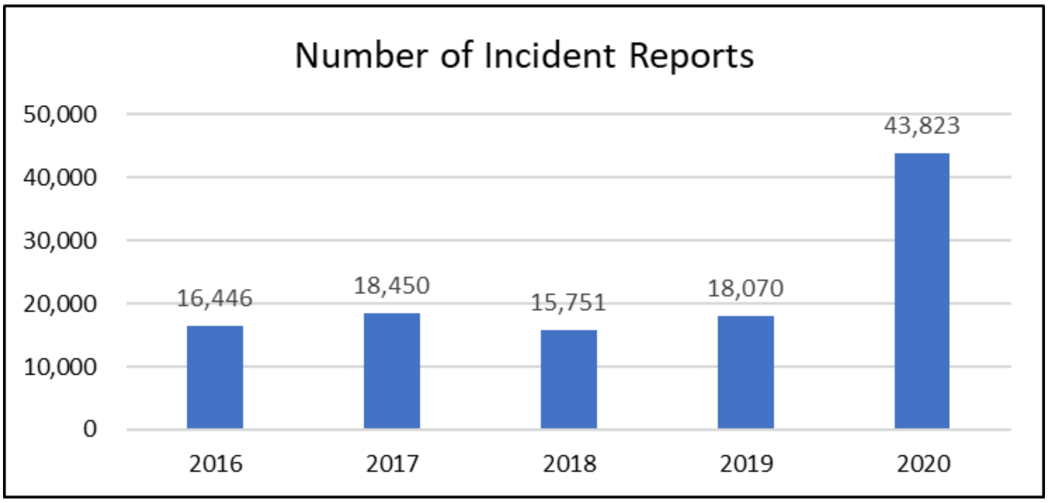


Figure 2. Incident reports to JPCERT/CC (2016-2020)

3.2 Abuse statistics

Incidents reported to JPCERT/CC during the last quarter of 2020 were categorised as in Figure 3. About 70% of the reports were on phishing site, followed by scan and website defacement.

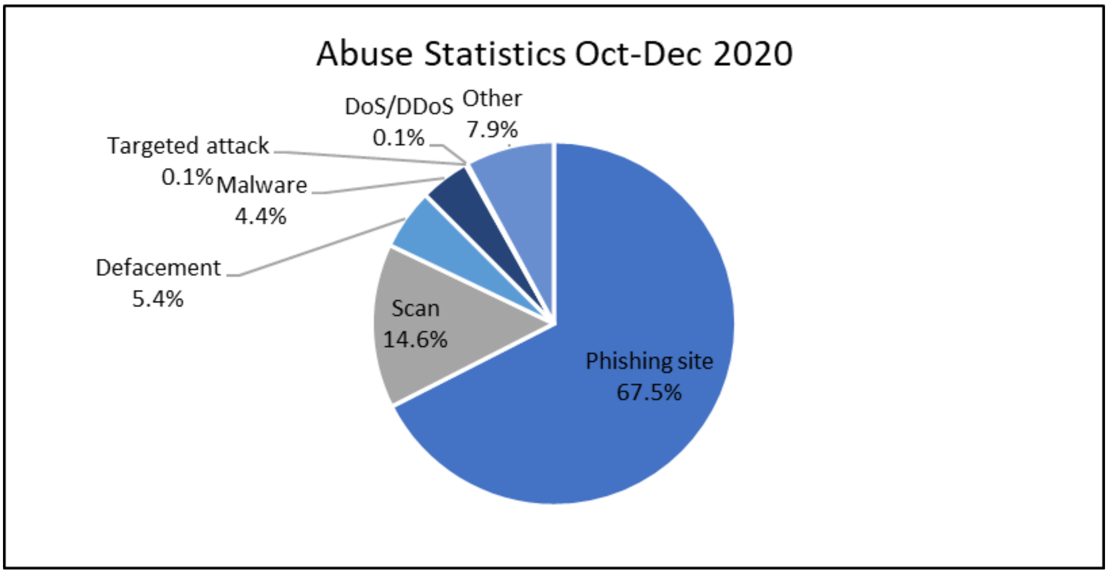


Figure 3. Abuse Statistics of Oct-Dec 2020

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 2020, 68 security alerts were published.

- Early Warning Information

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

- Japan Vulnerability Notes (JVN)

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

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

  For products that affect a wide range of developers, JPCERT/CC coordinates with

CERT/CC, ICS-CERT, CPNI, NCSC-FI and NCSC-NL.

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

In 2020, 338 vulnerabilities coordinated by JPCERT/CC were published on JVN. 91 were cases published with IPA through the Information Security Early Warning Partnership, and 247 were published through partnerships with overseas coordination centers, developers, researchers, etc.

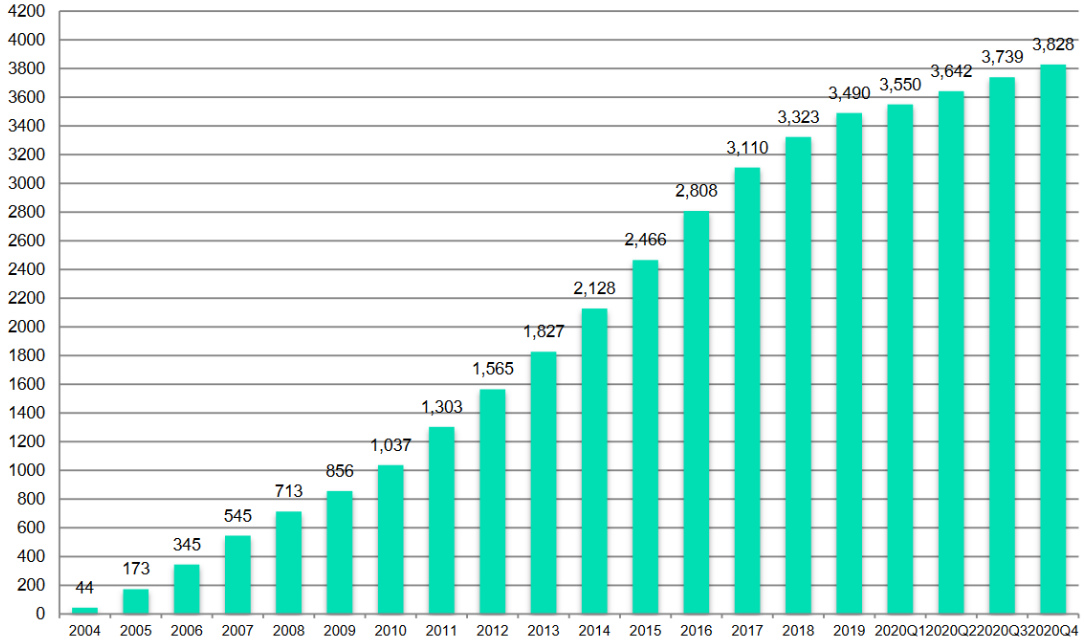


Figure 4. Number of vulnerabilities published on JVN by year

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

JPCERT/CC's Vulnerability Handling and Disclosure Policy is available here (English):
https://www.jpcert.or.jp/english/vh/2018/20180330-vulpolicy.pdf

- JPCERT/CC Weekly Report

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

- JPCERT/CC Official Blog
  https://blogs.jpcert.or.jp/en/
  Since September 2010, JPCERT/CC has been providing security news and technical observations related to Japan, as well as updates of international activities that JPCERT/CC engages in on the blog.

- Quarterly Activity Reports
  https://www.jpcert.or.jp/english/menu_documents.html
  JPCERT/CC publishes quarterly activity reports and study/research reports both in Japanese and English.

- JPCERT/CC on Twitter
  https://twitter.com/jpcert_en
  Since January 2009, JPCERT/CC has been providing Security Alerts, Blog updates, etc. via Twitter.

- JPCERT/CC GitHub
  https://github.com/JPCERTCC
  JPCERT/CC's analysis tools and other resources are available on GitHub.

3.4 Services

- Industrial Control System Security

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

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

- TSUBAME (Internet Threat Monitoring Data Sharing Project)
  https://www.apcert.org/about/structure/tsubame-wg/index.html

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

- Demonstration Test: Internet Risk Visualisation – Mejiro
  https://www.jpcert.or.jp/english/mejiro/

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

3.5 Associations and Communities

- Nippon CSIRT Association
  https://www.nca.gr.jp/en/index.html (English)

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

- Council of Anti-Phishing Japan
  https://www.antiphishing.jp/ (Japanese)

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

4. Events

4.1 Trainings, Seminars and Workshops

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

5. International Collaboration

5.1 International partnerships and agreements

- MoU

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

- FIRST (Forum of Incident Response and Security Teams)
  https://www.first.org

JPCERT/CC contributes to the international CSIRT community FIRST. JPCERT/CC also supports CSIRTs who wish to become a member of FIRST. In 2020, JPCERT/CC supported MELCO PSIRT and NEC-CIRT to become a full member.

- APCERT (Asia Pacific Computer Response Team)
  https://www.apcert.org/

Since its establishment, JPCERT/CC has been serving as a Steering Committee member and Secretariat. JPCERT/CC is also the convener of the TSUBAME Working Group, which aims to establish a common platform for Internet threat monitoring, information sharing & analysis within the region.

5.2 Capacity building

5.2.1 Drills & Exercises

JPCERT/CC participated in the following drills in 2019 to test our incident response capability:

- APCERT Drill 2020 (11 March)
- ASEAN CERTs Incident Drill (ACID) 2020 (7 October)

5.2.2 Seminars & presentations

In 2020, JPCERT/CC delivered presentations at the following international cyber security events:

- APRICOT 2020 (February, Melbourne)
- EU Cyber Forum (September, Online)
- FIRST & AfricaCERT Virtual Symposium for Africa and Arab Regions (October, Online)
- Geneva Peace Week 2020 (November, Online)

- 32nd Annual FIRST Conference (November, Online)
- Botconf 2020 (December, Online)

...and more

5.3 Other international activities

Below are some of the international events that JPCERT/CC attended in 2020:

- S4x20 (January)
- TF-CSIRT meeting & FIRST Regional Symposium Europe (January)
- M3AAWG 48th General Meeting (February)
- M3AAWG 49th General Meeting (June)
- Blackhat USA 2020 (August)
- Defcon 28 (August)
- 29th USENIX Security Symposium & Workshop (August)
- SANS Threat Hunting & IR Summit 2020 (September)
- HITCON2020 (September)
- AusCERT2020 (September)
- Blackhat Asia (September)
- Virus Bulletin Conference 2020 (September)
- M3AAWG 50th General Meeting(October)
- ACNS 2020 (October)
- CS3STHLM 2020 (October)
- OSDFCon (November)
- AVAR2020 (December)
- Blackhat Europe 2020 (December)
- 15th Annual NatCSIRT Meeting (December)

…and many more

- International Standard (ISO/IEC JTC 1/SC 27 Information technology – Security techniques)

JPCERT/CC contributes to the following International Standards being developed under ISO/IEC JTC 1/SC 27 WG3:

ISO/IEC 29147: Vulnerability Disclosure

ISO/IEC 30111: Vulnerability Handling Processes and WG4:

ISO/IEC 27035-1: Principles of incident management

ISO/IEC 27035-2: Guidelines to plan and prepare for incident response

ISO/IEC 27035-3: Guidelines for incident response operations

6. Future Plans

6.1 Future projects/operation

- Enhance collaboration with partners on the remote work basis

Due to the global COVID-19 pandemic, it is expected that JPCERT/CC's employees will have to work from home in 2021 as well. In 2020, most of the operations of JPCERT/CC became optimized for the remote work environment, and the employee became trained for such operation. Moving the events such as JSAC from onsite to online setting, JPCERT/CC will further enhance the collaboration with partners even in this difficult time. Employees will also actively speak at and/or participate in various online conferences and other events to reach out new audience.

- TSUBAME system update

JPCERT/CC is planning a large-scale system update for TSUBAME in the coming financial years for more effective incident detection. Currently, the team is designing the system specification.

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 – Korea

1. Highlights of 2020

1.1 Summary of major activities

- Detected 1.5 million cyber attack attempts on average per day
- Held the 2nd Cyber Security Contest for Critical Information Infrastructure
- Shared cyber threat information with about 200 organizations
- Evaluated 192 organizations on management of information security

2. About CSIRT

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 17 years since its establishment in 2004.

2.2 Establishment

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

3. Activities & Operations

3.1 Scope and definitions

- Policy Establishment and Consulting
  - Establishment of cyber security policies 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 attack detection and issuance of warnings

- Incident Investigation and Damage Control
  - Analyzing the causes and identifying responsible actors
  - Support for recovery and prevention of recurrence
- Information Sharing and Cooperation
  - Domestic and international sharing of cyber threats and responses
  - Raising public awareness and establishing cooperative channels at home and abroad

4. Events organized / hosted

4.1 Training

The KN-CERT offers training courses at the Cyber Security Training and Exercise Center to enhance job expertise and incident response capabilities for cybersecurity workers at government and public organizations.

4.2 Drills & exercises

The KN-CERT conducts drills each year to improve cyber attack response capabilities for public organizations operating industrial control systems (ICS) designated as important information and communications infrastructure.

From August 18-21, 2020, 55 ICS management organizations participated in ICS-cyber attack response drills. The exercises focused on each of the four response phases during cyber attacks against 126 industrial control systems: detection, quarantine, eradication and recovery.

4.3 Conferences and seminars

Since 2017, the KN-CERT has been holding the Cyber Security Thesis Competition(the Competition) in collaboration with the Korea Institute of Information Security and Cryptology and the Korean Association of International Studies to improve the quality of research on cyber security and recruit talented individuals.

In Addition, The KN-CERT holds the Cyber Security Academy (the Academy) in cooperation with the National Security Research Institute and the International Cyber Law Studies in Korea to cultivate human resources in the cyber security field and share awareness of cyber threats.

5. International Collaboration

5.1 International partnerships and agreements

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

5.2 Capacity building

5.2.1 Seminars & presentations

The KN-CERT, together with the Ministry of Foreign Affairs and the National Security Research Institute, hosted "the International Conference on Building Global Cyberspace Peace Regime" to seek ways to jointly respond to cyber security threats.

6. Conclusion

Keeping cyberspace safe from hackers should never be an idealistic concept. It can become a reality if the government and the private sector, including academia and businesses, work together to create a strong cyber defense shield and join hands with the international community. In 2021, the KN-CERT will continue its efforts to strengthen cyber security.

KrCERT/CC

Korea Internet Security Center – Korea

1. Highlights of 2020

1.1 Summary of major activities

The COVID-19 situation has caused people's daily lives to rely more on digital technology for working from home and online school classes. There have also been cyberattacks in such situation. We at KrCERT/CC cope with cyber threats closely related to people's daily lives like spreading smishing (a phishing text message) or malicious apps or provide COVID-19-related information while striving to maintain the system of cooperation between the public and private sectors including establishment of hotline for sharing information. We also launched My PC Dolbomi (it means a nanny), a project for checking the security of people's PCs, to prevent cyber threats targeting individuals' PC in the COVID-19 era which is increasing non-face-to-face services.

1.2 Achievements & milestones

COVID-19 changed people's lives drastically. There was the rapid digital transformation. People suffered from cyber. In July 2020, the South Korean government announced the Korean New Deal (www.knewdeal.go.kr), a national project designed for the recovery of the economy, which went south amid the COVID-19 pandemic. The Digital New Deal, one of the core policies of the Korean New Deal, included the establishment of K-Cybersecurity Strategy for the operation of a safe cyber space. This strategy was published in February 2021 by the Ministry of Science and ICT. We at KrCERT/CC, as the implementing organization of the strategy under the Ministry, pushed forward with the establishment of safe cyber infrastructure by stressing the need for detection and checks of software vulnerabilities.

- Collaboration: In the early stage of online classes, we at KrCERT/CC prepared against the possibilities of interruption of classes due to mishaps by establishing the hotline linked to the Ministry of Science and ICT (MSIT), Ministry of Education (MOE), and Korea Education and Research Information Service (KERIS). We also strived to respond to hacking incidents and prevent further impacts in cooperation with the National Information Society Agency (NIA), which sought to maintain the operation of the service normally, to provide COVID-19-related information and secure website app services.

- Prevention of loss incurred by people: We checked services closely related to people's daily lives and blocked URLs and malicious apps by strengthening the monitoring of texts disguised as COVID-19 information. We also checked whether mask selling apps were laden with malicious functions. Moreover, to cope with smishing, we provide the service of checking whether cases reported by users are smishing or not in cooperation with domestic businesses. We announced as well the rules to be observed for the protection of information amid an increase in the number of people working from home. KISA, the parent organization of KrCERT/CC, has operated the homepage for the provision of COVID-19-related information (www.kisa.or.kr/covid19) since the outbreak of COVID-19.
- Provision of support for businesses: We strived to prevent security incidents such as ransomware by checking out vulnerable points, including whether the obligations for the protection of personal information are observed toward businesses with focus on their videoconferencing, remote collaboration, or bio research institute amid the COVID-19 situation. We believe this information would help fostering safe remote working environment, working from home.

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 and one center with fourteen 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 started out in 1996 as a small team responsible for hacking incidents under the Korea Information Security Agency (formerly KISA). Since its foundation, it has responded to and handled numerous security issues and tasks. The first major incident was the Internet Crisis caused by the so-called "slammer worm" in 2003. At that time, KrCERT/CC had difficulties in communicating efficiently with a telecommunication carrier, which marked 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, we came up with an organizational structure for an incident response team similar to that of the present in December 2003. With nationwide serious security incidents occurred in 2007, 2009, and 2013, the team was reformed in order to cope more effectively with such, and its size and budget were expended to today's KrCERT/CC (for analysis, response, and sharing). Domestically, it is usually called KISC or Korea Internet Security Center.

2.3 Resources

As of December 2020, 150 employees from 3 divisions and 1 center 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, 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.

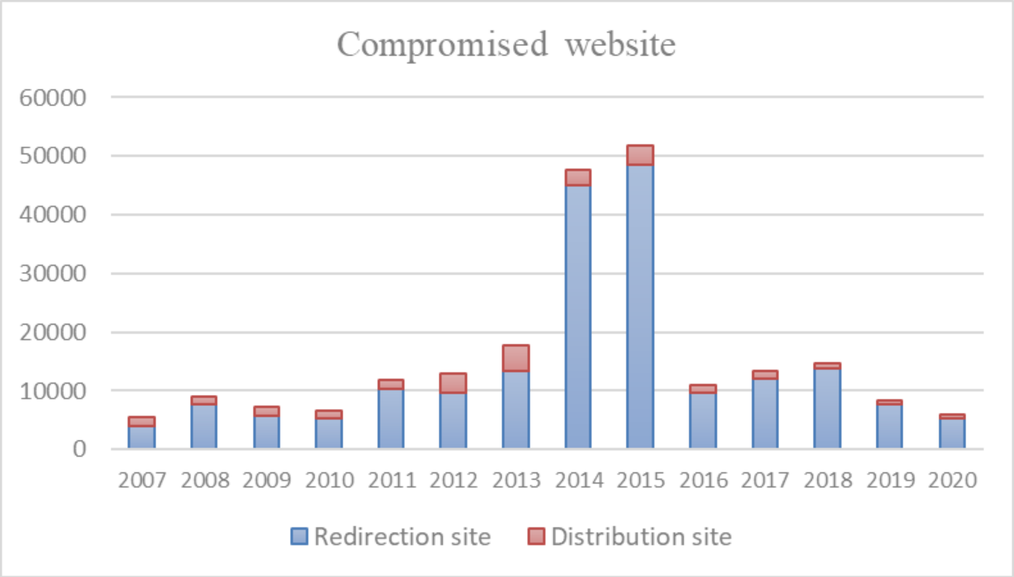
3. Activities & Operations

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, etc.) in 24/7 Monitoring, Early Detection/Response with regard to cyberattacks in the private sector.

3.2 Incident handling reports & Abuse statistics

Compared with last year's figure, the number of compromised websites distributing hidden malware increased 30% from 566 to 738 in 2020. The number of redirection sites also decreased 31% from 7,733 to 5,296.



3.3 Publications

We at KrCERT/CC disclosed a series of reports analyzing the strategies of threat actors through our homepage in 2020. In April 2020, we disclosed up to Series 4 including Series 1 about controlling the local network through vulnerable websites, and Analysis Bookcodes RAT C2, Analysis on attackers' strategy for malware usage. In addition, those announced by us included the following: reports like cases of ransomware incidents targeting businesses and analysis of scenarios on damages by targets of spear phishing; response to DDoS attacks, ransomware guidelines, etc. We released a total of 180-plus software vulnerability security recommendations (150 in Korean, 30 in English). These materials are available at www.boho.or.kr (Korean) and www.boho.or.kr/krcert/publicationList.do (English). The work of translating the Korean materials into English is underway.

3.4 New services

In the second half of the year, we carried out a total of 1,670,000 checks through My PC Dolbomi and created jobs at SMEs in the course of conducting checks for PCs across the country including local welfare centers for children to cope with cyber threats against households amid the COVID-19 pandemic. The service provided by professionals for security checks of PCs and treatments went a long way in reducing threats associated with COVID-19 in a situation wherein the number of those working from home increased drastically. In 2021, we plan to expand the service to digitally less privileged people.

4. Events organized / hosted

4.1 Training

We at KrCERT/CC provided educational sessions designed to enhance domestic businesses' CISO security awareness level. We intended to help them enhance the capability of those experiencing difficulties due to restrictions in budget or their locality. Our education, provided on/offline, put more emphasis on SMEs rather than large-sized businesses, cities rather than the Greater Seoul area. A total of one thousand people attended the education sessions, which were provided on a total of six occasions in seven months between April and October.

4.2 Drills & exercises

We at KRCERT/CC have held cyber exercise designed to inspire businesses to have a firm sense of cyber security twice a year since 2005. In 2020, a total of 90,000-plus people from 130-plus businesses attended the semiannual training session. The content of the session was preparedness against BEC (Business Email Compromise), DDoS attack, and infiltration into homepages. The training was carried out by simulating a real situation in cooperation with communications/vaccine/security businesses. It was noteworthy that the result of re-training carried out among 5,000-plus people from 21 businesses showed a 9% infection rate among those from the most vulnerable businesses taking part in BEC; this was an improvement from the initial rate (15%), suggesting the effects of the cyber exercise.

4.3 Conferences and seminars

- Seminar for Web security trends & cases analysis on Nov. 6
- Cyber threats network intelligence seminar (each month)
- Quarterly seminar for sharing the use of cyber security

5. International Collaboration

5.1 International partnerships and agreements

In 2020, KISA, which is the parent institution of KrCERT/CC, signed an MOU with NASK of Poland—where CERT Polska belongs—for mutual cooperation in coping with security incidents.

5.2 Capacity building

5.2.1 Training

APISC Incident Response Online Training

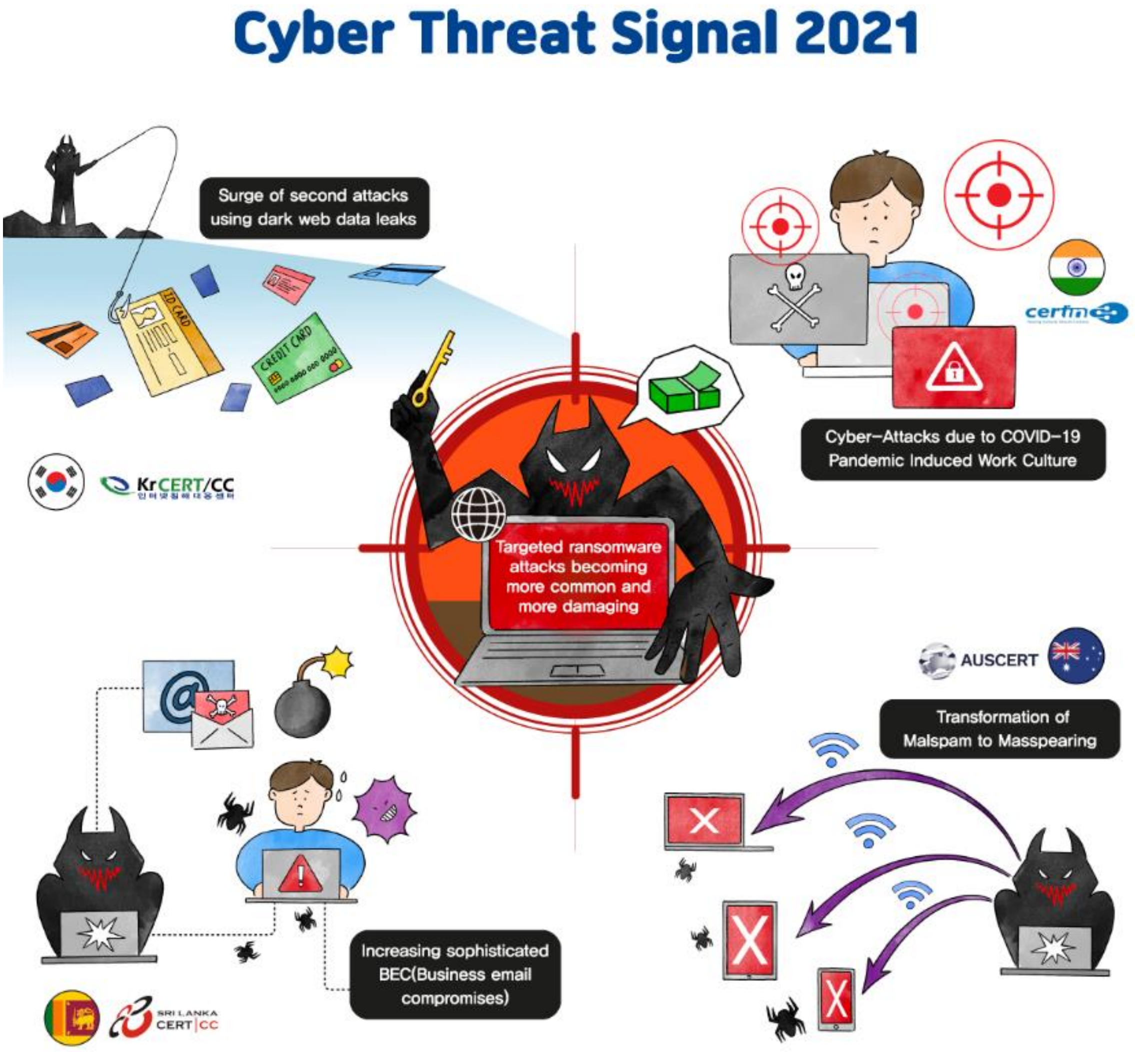
5.2.2 Drills & exercises

APCERT Annual Drill

ACID Drill

5.3 Other international activities

We presented the 'Cyber Threat Signals 2021' jointly with the Cyber Threat Intelligence Network and AusCERT, CERT-In, and Sri Lanka CERT|CC.


Cyber Threat Signal 2021
Surge of second attacks using dark web data leaks
ID CARD
CREDIT CARD
KrCERT/CC
Cyber-Attacks due to COVID-19 Pandemic Induced Work Culture
cert-in
Targeted ransomware attacks becoming more common and more damaging
AUSCERT
Transformation of Malspam to Masspearing
Increasing sophisticated BEC(Business email compromises)
SRI LANKA CERT|CC

6. Future Plans

6.1 Future projects

The Ministry of Science and ICT (MSIT) will provide support for enhancement of awareness of security on the part of SMEs and ordinary people to ensure success in Digital New Deal, with part of the support to be assumed by KrCERT/CC.

- New installation of service for checking software development-related security-vulnerable points
- Expansion of opening/sharing cyber threats big data
- Expansion of My PC Dolbomi Service (PC to mobile)

7. Conclusion

2020 saw the rapid digital transformation amid the pandemic and the need for anti-epidemic steps in digital spaces. We at KrCERT/CC made utmost efforts to minimize the loss suffered by people by strengthening existing projects and starting new ones. We experienced lots of difficulties but felt rewarded in the course of fulfilling our duties.

LaoCERT

Lao Computer Emergency Response Team – Lao People's Democratic Republic

1. Highlight of 2020

1.1 Summary of Activities

- Training on Network Monitoring System Installation on 17-21 February 2020 at LaoCERT.
- Seminar on Cyber4Dev engagement program on 2-5 March 2020 at LaoCERT.

1.2 Achievements & milestones

- Instruction to raise awareness on the use via online social media security.

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 2020.

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.

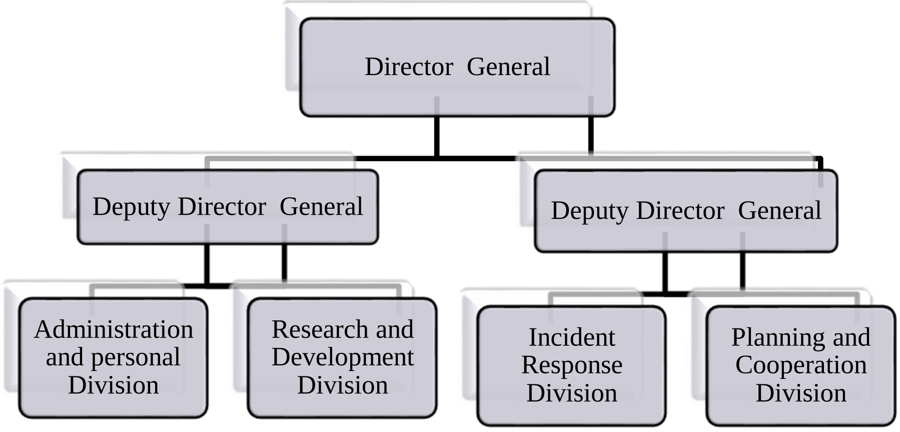
2.3 Resource

LaoCERT currently contains 30 staffs, 8 females and divide into 4 Divisions and technical staff currently holds professional information security certificate as follow:

- Celebrate Certified Physical Analyst

- Computer Hacking Forensic Investigator

LaoCERT Organization Charts


Director General
Deputy Director General
Deputy Director General
Administration and personal Division
Research and Development Division
Incident Response Division
Planning and Cooperation Division

2.4 Constituency

LaoCERT is a coordination center of cyber security within Laos and also cooperation with international CERT organizations in the field of cyber security. 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.

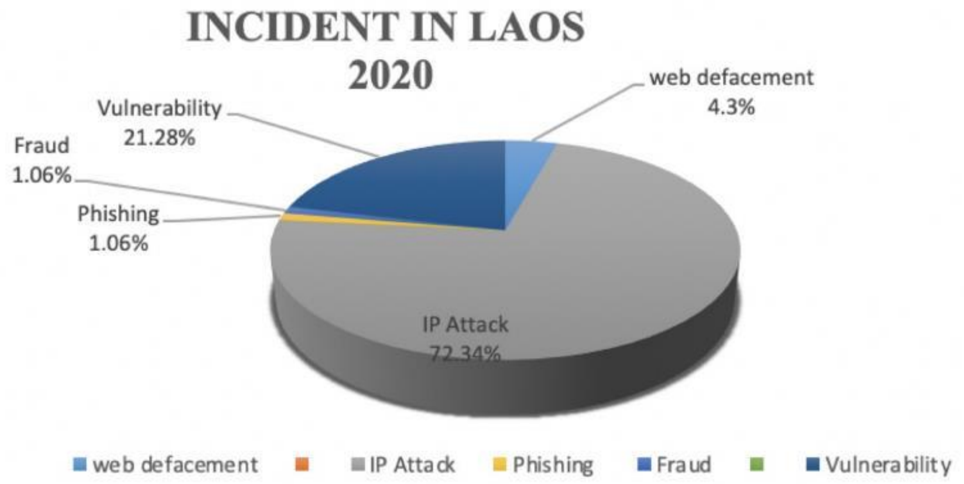
3. Activities & Operations

3.1 Scope and definition

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.

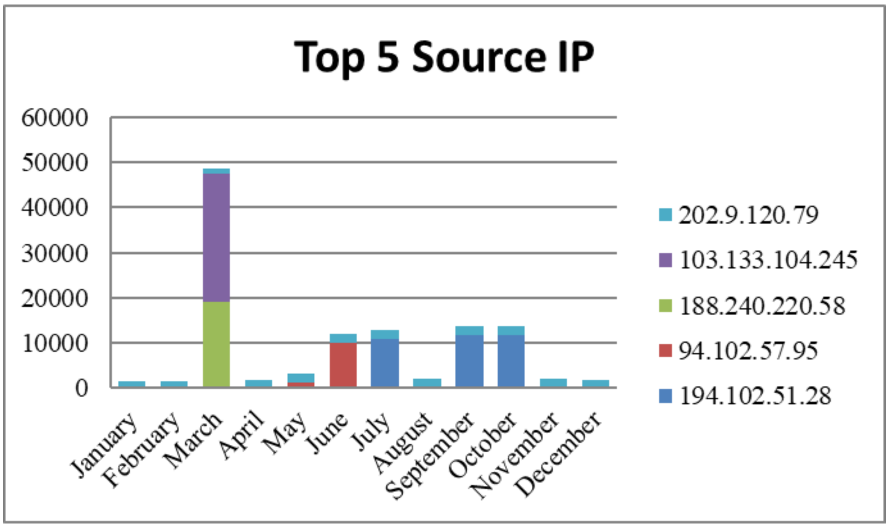
3.2 Incident handling report

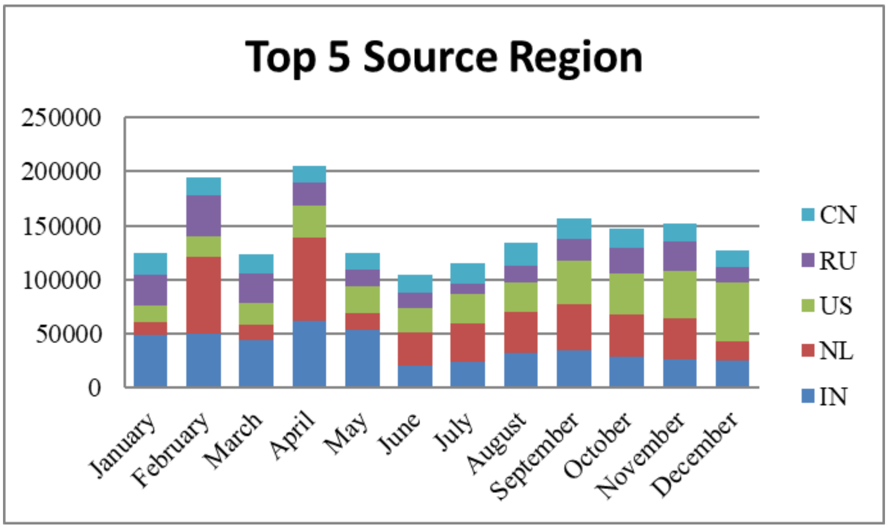
The following graph shows the statistic of incidents that happened in 2020.

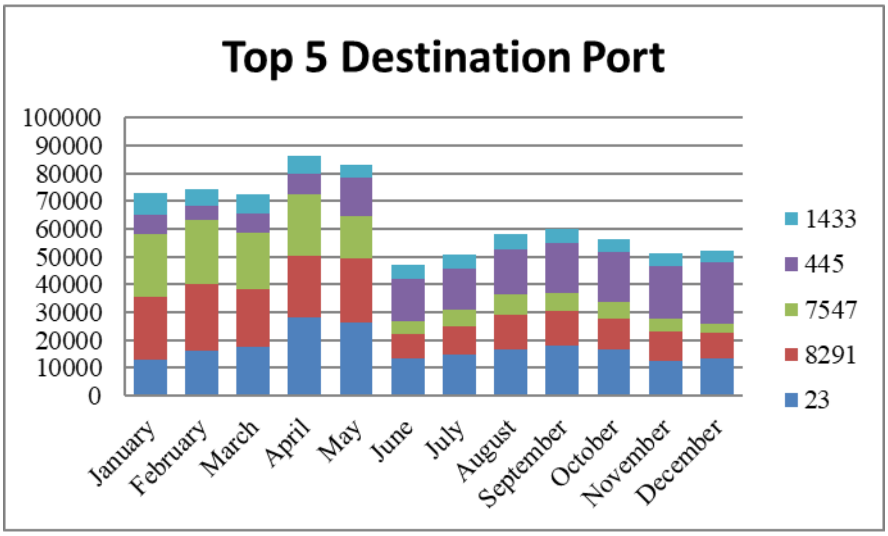


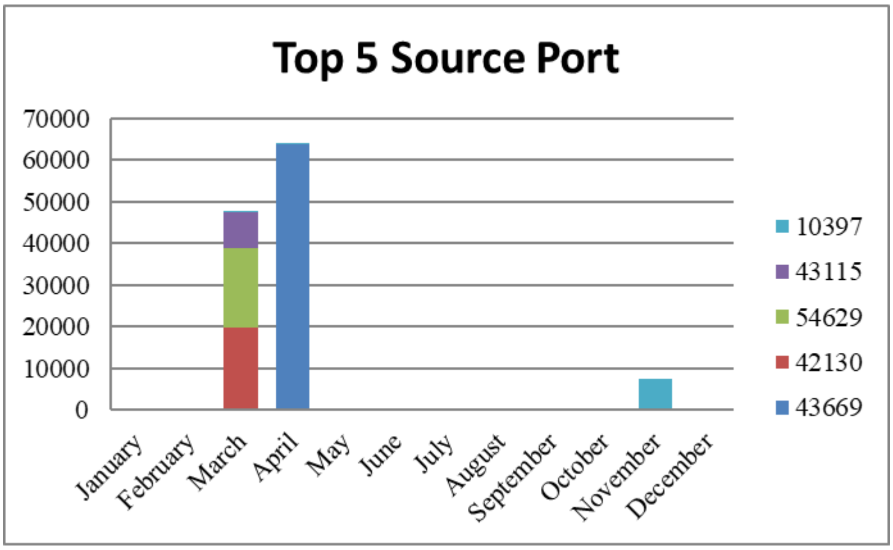
3.3 Abuse Statistics (TSUBAME Sensor)

The following graph shows the top 5 of Source IP Address, top 5 of Source region, top 5 of Destination port and top 5 of Source port statistics obtained by TSUBAME Sensor in 2020.




Top 5 Source Region
250000
200000
150000
100000
50000
0
January
February
March
April
May
June
July
August
September
October
November
December
CN
RU
US
NL
IN


Top 5 Destination Port
100000
90000
80000
70000
60000
50000
40000
30000
20000
10000
0
January
February
March
April
May
June
July
August
September
October
November
December
1433
445
7547
8291
23


Top 5 Source Port
70000
60000
50000
40000
30000
20000
10000
0
January
February
March
April
May
June
July
August
September
October
November
December
10397
43115
54629
42130
43669

3.4 Publication

Website: www.laocert.gov.la

E-mail: admin@lacert.gov.la

Tel: +85621 254508 (08:00-16:00) Working hour

Incident report: report@laocert.gov.la

(+ 85630 5764222) 24 x 7

3.5 New Services

- Create 32 posters on how to use computers safely and disseminate to society.
- Translate the Self-learning Material on Cybersecurity into Local Language in the ASEAN- MIC, Japan activities framework.

4. Events organized / hosted

4.1 Training

- Co-Organized the training on Training on Network Monitoring System Installation on 17-21 February 2020 at LaoCERT.

4.2 Conferences and seminars

- Co-Organized the Seminar on Cybersecurity Awareness on 15 January 2020 at LaoCERT.
- Co-Organized the Seminar on Cyber4Dev engagement program on 2-5 March 2020 at LaoCERT.

5. International Collaboration

5.1 International partnership and agreement

In 2021, LaoCERT did not sign any agreement on cooperation plan due to the pandemic of COVID-19 and other inconveniences, however, we are now planning to prepare the contract for joint activities in cybersecurity field with ASEAN countries, international organizations and the national CERT.

5.2 Capacity Building

5.2.1 Training

The following has shown the statistic for attended the training in 2020:

- Capacity Building in Policy Formation for Enhancement of Measures to Ensure Cybersecurity in ASEAN Region on 26 January - 07 February 2020 in Japan.

- Integrated Cybersecurity Management and System on 03-07 February 2020 in Singapore.
- APCERT Incident Handling Drill on 11 March 2020.
- Trend Micro Advance Threat Defense Training Course on 16-20 March 2020.
- Email Based Attacks and Mitigation webinar on 28 August 2020.
- Self-Learning Course Fundamentals of Cybersecurity on 30 August 2020.
- The 11th ASEAN Network Security Council Action 15 September 2020.
- APCERT Incident Handling Drill on 06 October 2020.
- The 11th Online ASEAN-Japan Cybersecurity Building Centre Training (AJCCBC) on 03-06 November 2020.
- The 12th Online ASEAN-Japan Cybersecurity Building Centre Training (AJCCBC) on 15-18 December 2020.

5.2.2 Drills and Exercises (Online)

The following has shown the statistic for participated Drills and Exercises in 2020:

- APCERT Incident Handling Drill on 03 March 2020.
- APCERT Incident Handling Drill on 06 October 2020
- CSA SingCERT Incident Handling Drill on 10 July 2020.

5.2.3 Seminar and presentation

The following has shown the statistic for participated the Seminar in 2019:

- Seminar on Cybersecurity Awareness on 15 January 2020.
- The 1st ASEAN-Japan Cybersecurity Working Group Meeting on 26-27 February 2020 in Cambodia.
- The 2nd ASEAN Conference on Crime Prevention and Criminal Justice on 26-29 February 2020 in Bangkok.
- Workshop on Building Strategic Communication Capacity to Counter Disinformation on 03-05 March 2020.
- Cyber Norm and UN Processes Mad Easy Webinar on 22 May 2020.
- The 2nd ASEAN-Japan Cybersecurity Working Group Meting (Web Meeting) on 3-4 June 2020.
- The ASEAN Digital Integration Index (ADII) Technical Brief Workshop on 02 July 2020.
- The Cyber4Dep Steering Committee Meeting on 09 July 2020.

- China-ASEAN Artificial Intelligence Symposium on 29 July 2020.
- The Frontline Heroes Meeting on 29 July 2020.
- Southeast Asia Virtual Cyber Dialogue on 06 August 2020.
- International Law of Cybersecurity Operation on 19-26 August 2020.
- The 5th Annual Meeting of the Cybersecurity Alliance for mutual Progress (CAMP) on 14-20 September 2020.
- Global Cybersecurity Center for Development Cybersecurity Seminar Program on 14-25 September 2020.
- East Asia Summit Workshop "Regional Cyber Capacity Building Seizing the Fourth Industrial Revolution on 21-22 September 2020.
- The 5th Singapore International Cyber Week and the ASEAN Ministerial Conference on Cybersecurity on 05-09 October 2020.
- The ASEAN CERT Incident Drill and Cybersecurity R&D Workshop on 07 October 2020.
- Cybersecurity Business online Meeting on 12-13 October 2020.
- Cybersecurity Exchange Seminar of 2020 China-ASEAN Year of Digital Economy Cooperation on 28-30 October 2020.
- The 1st ASEAN Cybersecurity Coordinating Committee on 5 November 2020.

6. Future Plans

- Continue to provide training and seminar on Cybersecurity to provincial both public and private sector throughout the country via online platform during the pandemic of COVID-19.
- Continue to collaboration to exchange the lessons and experiences on the development of legislation, laws and information on developing an online social media management system among National CERT, international organization and related sectors in the field of cybersecurity.
- Drafting Cyber Security Law.
- 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 for asking for cooperation.
- Planning for Establishing Government Threats Monitoring (GTM).
- Planning to set up the Network Monitoring System.
- Planning and studying to set up the Honeypot, HoneyNet.

7. Conclusion

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 the training which aim to improve the technical skill of staff as well as to disseminates awareness-raising on legislation and Law and the instruction on how to use social media or computer network securely without cyber-attacks.

mmCERT

Myanmar Computer Emergency Response Team – Myanmar

1. Highlights of 2020

1.1 Summary of major activities

- Conducted Incident Handling and CSIRT Management Courses to government organizations twice in February and March.
- Hosted "Cybersecurity Awareness Webinar" mainly to Ministry of Information and other government organizations on October 2, 2020. And also uploaded awareness video clips with white TLP in mmCERT Facebook page.
- Organized the Myanmar Cybersecurity Month 2020 in cooperation with Myanmar Computer Federation, US ICT Council for Myanmar and participated panel discussion on "Road to National Cybersecurity Framework" in October 2020.
- Participated "National Cybersecurity Webinar" in November 2020.
- Shared about "Reverse Engineering the PlugX APT Malware" at BSides Information Security Conference in December 2020.

1.2 Achievements & milestones

- Participating in "First Challenge 2020" and stood 12th rank among 200 participants.

2. About CSIRT

2.1 Introduction

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

2.2 Establishment

mmCERT was established on July 23 2004 under Information Technology Department, Myanmar Posts & Telecommunications (MPT), Ministry of Communications, Posts & Telegraph (MCPT). MPT was state-own telecom operator and mmCERT mainly handled computer incidents of MPT and government agencies. On December 15 2010, mmCERT extended its service coordination center (cc). In 2011, mmCERT became a member of APCERT. In 2015, Information Technology and Cyber Security Department

(ITCSD) was formed in order to accelerate E-Government Services and to enhance the cyber security of government agencies and private sectors. And mmCERT/cc was restructured under National Cyber Security Center (NCSC), ITCSD. In 2016, newly elected government restructured ministries and Ministry of Transport and Communications (MoTC) was reformed by merging three ministries Ministry of Communications and IT, Ministry of Transport and Ministry of Railway Transportation. ITCSD was moved to Ministry of Transport and Communications (MOTC).

2.3 Resources

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

2.4 Constituency

Since establishment, mmCERT has been serving for propagating cyber security information and advisories and providing technical assistance to government agencies, telecom operators, internet service providers (ISP), universities and individual users in Myanmar. It has been planned to extend the service to the constituency to financial institutions, banks, online services/ shopping, research and development center and vendors.

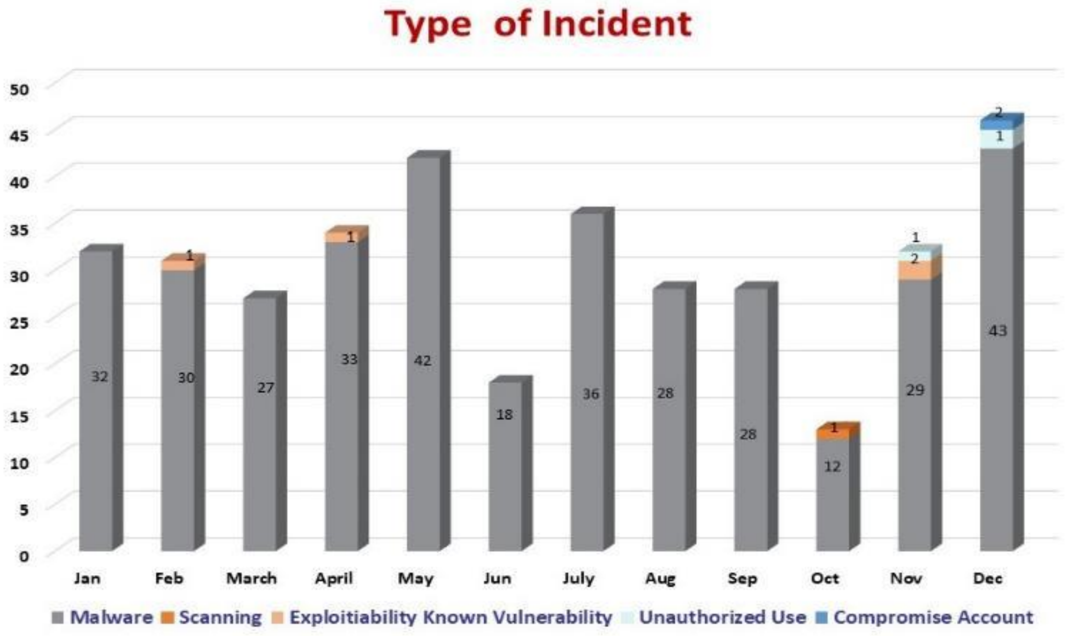
3. Activities & Operations

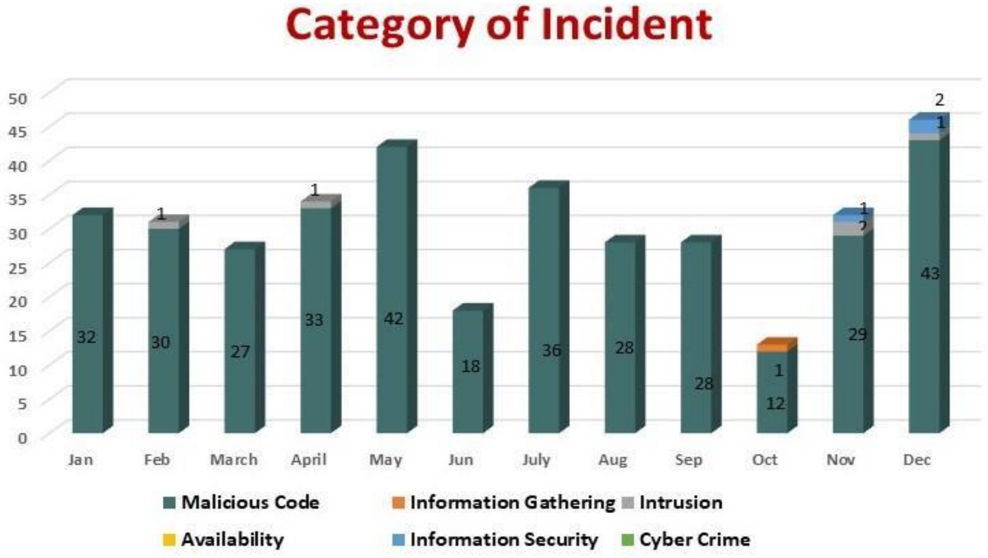
3.1 Scope and definitions

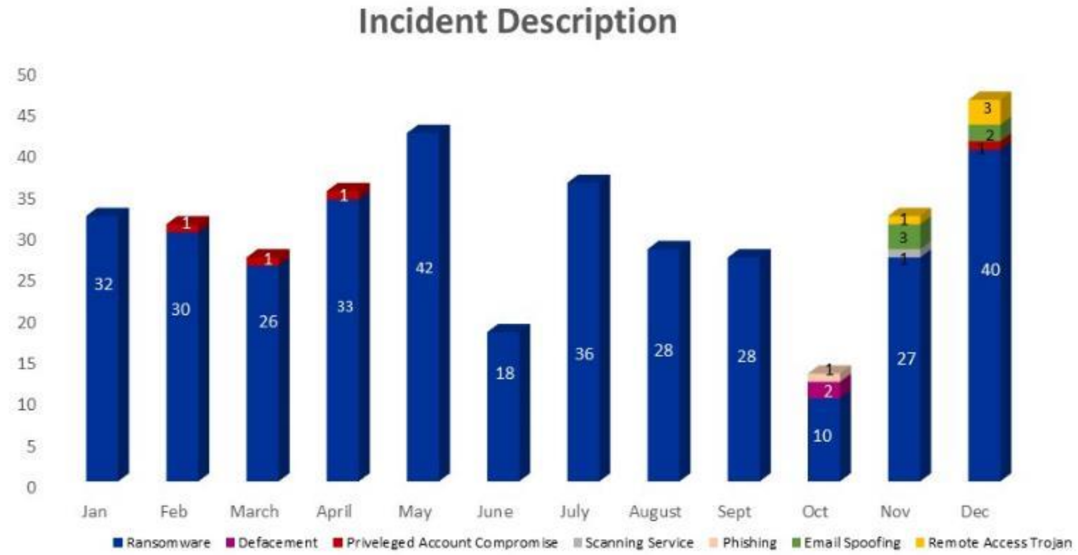
- Create National IT image by cooperating with international CERT teams for cyber security and Cyber crime
- Disseminate Security Information and Advisories
- Provide technical assistance
- Cooperate with law enforcement organizations for cyber crime

3.2 Incident handling reports

The following graph shows the incidents handled by mmCERT in 2020. According to the results on incident analysis by mmCERT, Ransomware Attacks were the most prominent incident cases in 2020.







3.3 Publications

- Published Stop Ransomware Guide version 1.4
- Published PlugX Removal Guide 1.1

3.3.1 Social Media

As Myanmar people are widely using Facebook at current time and thus, mmCERT supports through that platform. mmCERT releases reliable, accurate and timely information about emerging cyber threats and vulnerabilities in its official Facebook page.

During the Covid-19 Pandemic, new normal working environments were developed and thus mmCERT frequently provides alert and awareness raising about cyber security. mmCERT official Facebook page is as follow:

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

3.3.2 Website

Current events and activities of mmCERT can be known from its website.

The update cyber trends and Covid-19 related cyber incidents and articles were also translated into Myanmar language and published appropriately.

CVE for computer network and system can also be reviewed in mmCERT website:

- Website: https://www.mmcert.org.mm

3.3.3 Articles

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

“PlugX Removal Guide (Version 1.0)” was also released to help the victims of PlugX RAT to know the tactic of this RAT and eradication method.

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

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

3.4 New services

In this year, mmCERT/cc had been reported many ransomware cases especially STOP, Dharma, Phobos. Another prominent incidents are PlugX RAT cases which are mostly targeted to government organizations in Myanmar. mmCERT/cc developed “PlugX Remover Tool” to reveal the name of stolen files from victim’s PCs. Throughout this year, mmCERT/cc mainly responded to STOP ransomware cases and PlugX RAT cases. To provide prompt assistance for incidents, mmCERT provides contact point as follow:

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

4. Events organized / hosted

4.1 Training

- Provided Incident Handling and CSIRT Management Courses to all CIO and interested persons in government organizations in February and March 2020 at Training Center of Information Technology and Cyber Security Department, Ministry of Transport and Communications.
- Sharing the knowledge of Cyber Crime Investigation and Forensics to Myanmar Police Force, March 2020.
- Shared about “Reverse Engineering the PlugX APT Malware” at BSides Information Security Conference in December 2020.

4.2 Drills & exercises

mmCERT/cc hosted Myanmar Cyber Security Challenge Server for the youth who interested in cyber security to take exercise for CTF and enhance their skills.

4.3 Conferences and seminars

- Hosted "Cyber Security Awareness Webinar" to Ministry of Information and other government organizations on 2nd October 2020.
- Organized the Myanmar Cybersecurity Month 2020 in cooperation with Myanmar Computer Federation, US ICT Council for Myanmar and participated panel discussion on "Road to National Cybersecurity Framework" in October 2020.
- Participated "National Cybersecurity Webinar" in November 2020.

5. International Collaboration

5.1 Capacity building

5.1.1 Training

- A member of mmCERT also attended Information Security JICA ICT Course-C in January to June 2020
- Members of mmCERT attended the Certified Network Defender v1 Course supported by JICA in January 2020
- Attended the Fundamentals of Cybersecurity Course (AJCCBC) Online course in March 2020
- Attended the Online Training on "Safeguarding Critical National Infrastructure (CNI) Risks and Opportunities" on August 26, 2020.
- Member of mmCERT attended the Defense Practice against Cyber-Attacks (JICA) in September 2020 – October 2020
- Members of mmCERT attended the Certified Ethical Hacker v11 Course supported by JICA in October 2020
- Members of mmCERT attended CTI & IntelMQ Training APCERT Live Streaming / Webinar Training Program (APCERT) in October 2020
- Members of mmCERT attended the Cybersecurity Training and Exchange Seminar of 2020 China-ASEAN in October 2020
- Members of mmCERT attended the APT Training Course on Cyber Network Defense & Cyber Laws conducted by India in October – November 2020
- Member of mmCERT attended the APISC Security Training Course at Seoul,

Republic of Korea provided by KISA and KrCERT/CC in November 2020.

- New mmCERT staff members attended ASEAN-JAPAN CYBERSECURITY CAPACITY BUILDING (AJCCBC) which provides CYDER Course, Digital Forensic and Malware Analysis in February, November, and December 2020.

5.1.2 Drills & exercises

- Participating in APCERT Drill on March 11, 2020.
- Participating in ASEAN –JAPAN Cyber Remote Exercise on June 24, 2020.
- Participating in ACID Drill on October 7, 2020.
- Participating in ITU 2020 Global CyberDrill Scenario-Based Exercises from October 27, 2020 to November 5, 2020.

5.1.3 Seminars & presentations

- Members of mmCERT attended the Seminar on "Role of National CERT/ Gov SOC/ IT Sections and Required Skills of Their Staff Members" organized by JICA and presented by University of Indonesia and ID-SIRTII/CC in February 2020.
- Attended the Regional Cyber Capacity Building: Seizing the Fourth Industrial Revolution, East Asia Summit Workshop in September 2020.
- Members of mmCERT participated the ITU 2020 Global Cyberdrill Webinar: National CIRTs, Measuring and Improving Maturity (ITU) September 2020 – November 2020
- Attended International Conference on Promotion of International Cooperation in Ensuring Cyber Security and Preventing Cyber Crime ASEAN+3 on December 28, 2020.

5.2 Other international activities

- Participating in "First Challenge 2020" in June and stood 12th rank among 200 participants.
- Members of mmCERT participated the Cyber SEA GAME 2020 - ASEAN Cybersecurity Competition by AJCCBC on December 4, 2020.

6. Future Plans

6.1 Future projects

- Government Secure Service Network
- Penetration Testing Labs
- Digital Forensics

6.2 Future Operation

Being a developing team, mmCERT is striving hard to be a developed and matured team by elaborately doing Incident Handling, Cyber Security Researches, efficiently providing Technical Advisories, Trainings, Seminars and Workshops to Constituencies. Cyber Range Projects will encourage Computer and Technological Universities' Students and other young people who interest in cyber security to get effective Capacity Building and to enhance their skills. And then we keep on enhancing Public Awareness Activities and promoting International and National Co-operations for CERT Activities and doing Research on Log Data Analysis as much as we can.

7. Conclusion

In this year, due to COVID-19 pandemic, we faced many pros and cons of it. The speed of transiting to Digitalization and E-government platform among government agencies in Myanmar was promoted and Work from Home (WFH) – new normal working culture had been developed. People are willing to use internet more than last year and the necessity of secure and reliable services are more prominent. Thus, mmCERT/cc will expand capacity and enhancing operations to combat emerging cyber threats and to ensure proactive cyber resilience. mmCERT/cc will also collaborate with international parties to impose the safe and trusted cyber environment.

Contact Information

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

MNCERT/CC

Mongolia Cyber Emergency Response Team / Coordination Center – Mongolia

1. Highlights of 2020

1.1 Summary of major activities

Due to the global Covid-19 pandemic, all of the activities moved to online. MNCERT/CC has successfully organized its annual event and cyber security competition virtually. MNSEC 2020 cyber security virtual event has covered larger scope of participants than the past years.

“Kharuul Zangi 2020” cyber security virtual competition has been held successfully by MNCERT/CC.

1.2 Achievements and milestones

Year 2020 was full of achievements for MNCERT/CC. One of the main activities was providing its member organizations with threat intelligence and indicator information, recommendations, consulting and training.

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

We continued providing our member organizations with threat intelligence, indicators, threat actor information using MISP open source threat intelligence and sharing platform. Totally, 72,134 of threat intelligence and indicator information provided by CIRCL and FIRST had been shared with our constituency in 2020.

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

Key achievements continued to MNSEC 2020 event which has been organized virtually and made us a full of experience of hosting virtual event which was reached to 456 audiences.

2. About MNCERT/CC

2.1 Introduction

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

2.2 Establishment

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

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

2.3 Resources

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

2.4 Constituency

Our constituencies are:

- Internet Service Provider Companies
- Banks
- Mobile Operator Companies
- Universities
- MonCIRT and DCERT
- General public

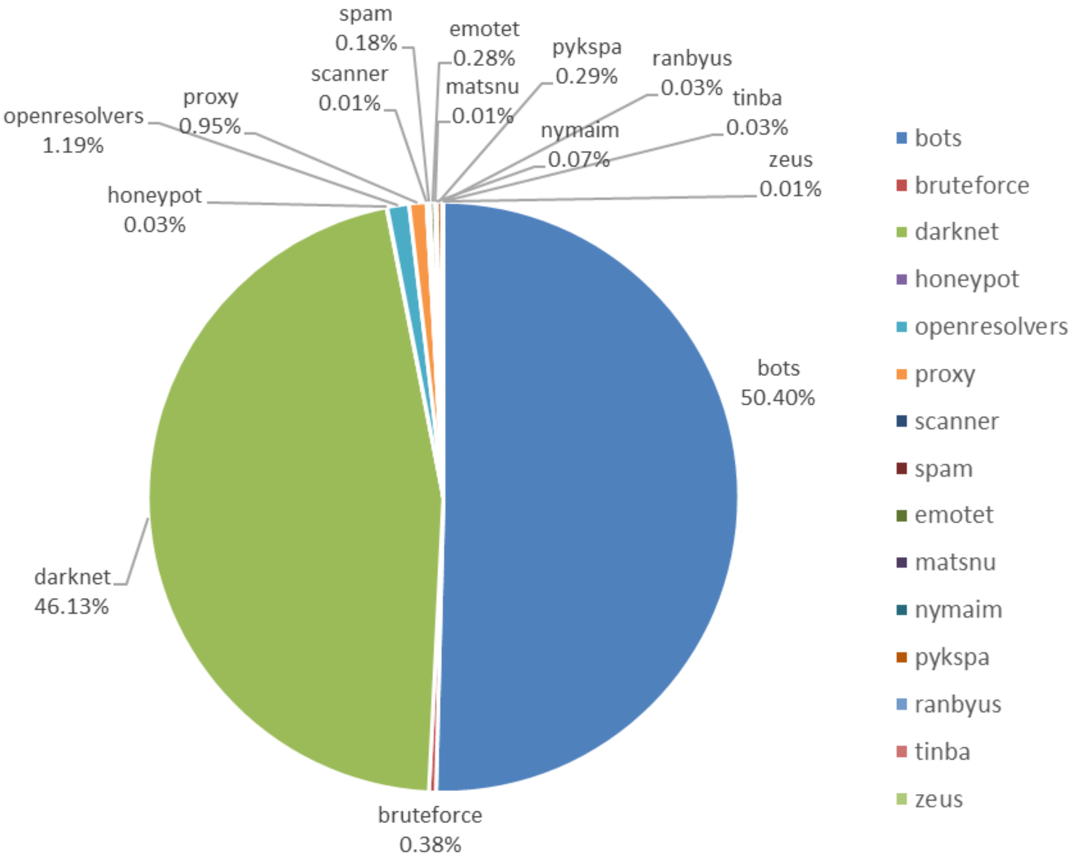
3. Activities & Operations

3.1 Scope and definitions

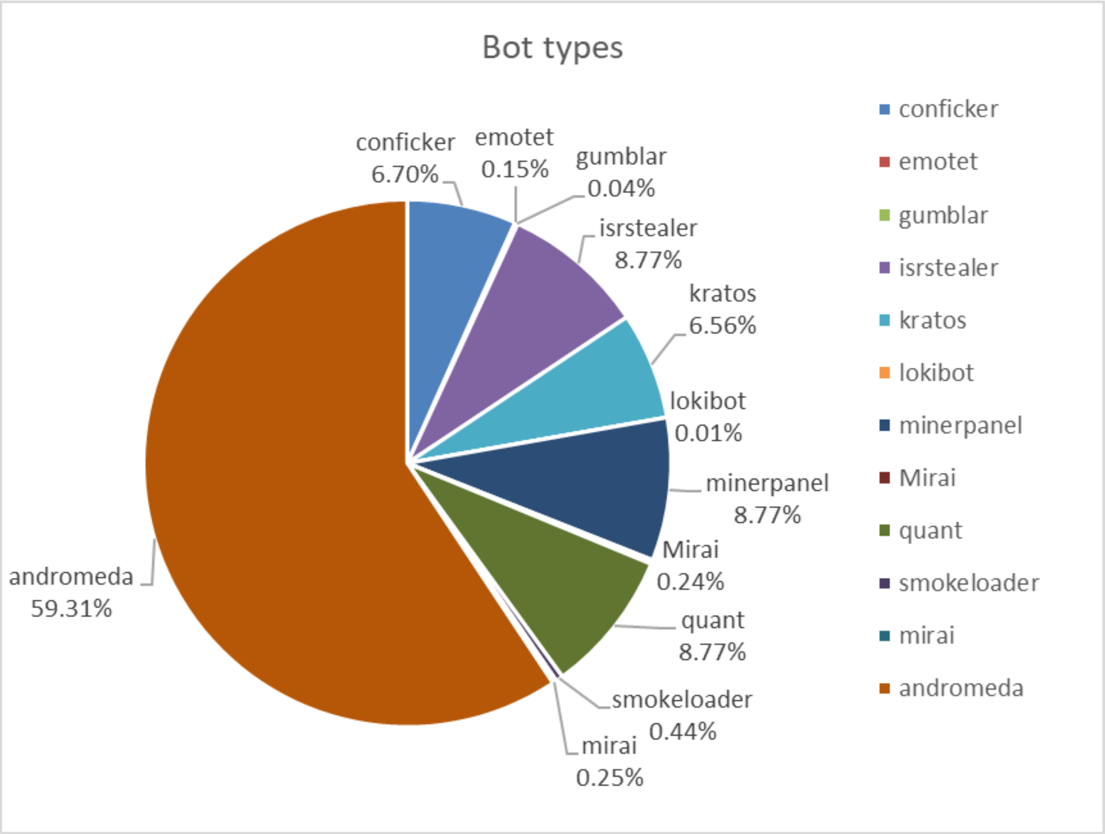
MNCERT/CC's constituency covers various types of organizations such as business companies, private sector organizations, banks, universities, non-governmental organizations and general public. MNCERT/CC provides services such as cyber security related discussion, training, security information and feed,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

3.2 Abuse statistics

The summary of malware types faced to Mongolia during the year 2020 is given in the following chart. This chart shows about summary of the malware, bot and vulnerability that were registered outbound traffic from Mongolia. Malware types are dominated by bots 50,40% and darknet 46,13%, followed by open resolver 1,19% and proxy vulnerability 0,95%.



The following chart shows the types of bots that were registered outbound traffic from Mongolia. Bots types are dominated by andromeda 59,31% and followed by isrstealer 8,77%, minerpanel 8,77%, quant 8,77%, conficker 6,7% and kratos 6,56%.



4. Events organized / hosted

4.1 Training

4.1.1 Members meeting and training

We have organized monthly meetings among IT engineers, cyber security officers and experts of member organizations. MNCERT/CC initiates a discussion and presents specific topics at each meeting such as Remote working security, Playbooks of Incident Response, Web API Security, Understanding the threats (risk analysis basic), Threat models and MITRE ATT&CK and Two factor authentication. After the training, participants discuss information security related issues and problems faced to them. The goal of this meeting and training is to develop a security community within cyber security officers and experts as well as to share their experience.

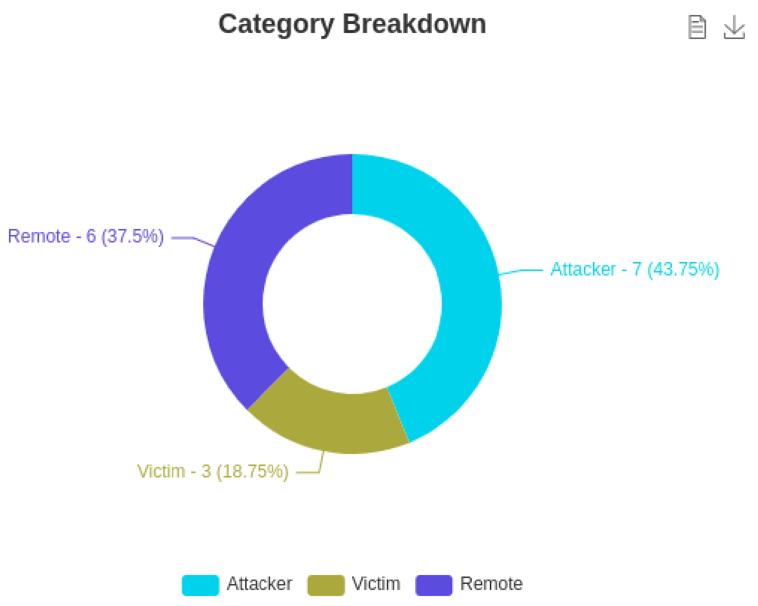
4.2 Drills & Exercises

4.2.1 “Kharuul Zangi 2020” National Cyber Security Competition

MNCERT/CC organizes a cyber security contest named “Kharuul Zangi” in order to promote the real life challenges and proper knowledge of cyber security to students and cyber security engineers. We have successfully organized “Kharuul Zangi 2020” competition between 24th October to 29th October of 2020, in collaboration with Golomt Bank.

Both the 1st and final stages had been held virtually. Out of 161 teams of 385 members, 14 teams qualified from the 1st stage and the two of 14 teams were high school team. Total of 16 tasks of 3 categories named covid-19, marvel and tenet have been given to be completed at 1st stage.

At final stage, 13 teams have participated the contest and the organizing team of competition prepared 15 tasks of 3 categories which are attacker, victim and remote. The tasks are shown in the following chart.



4.3 Conferences and seminars

4.3.1 MNSEC 2020 Virtual Event

Information technology (IT) benefits the business world by allowing organizations to work more efficiently and maximize productivity. Faster communication, electronic storage and the protection of records are advantages that IT can bring in the enterprise. Nevertheless, there are challenges to overcome in order to continue the development of IT sector. The lack of skilled human resource, legal environment, software and hardware infrastructure for the Information Technology sector in Mongolia and information security is one of them. Therefore, we have organized MNSEC 2020 event on 29th and 30th October of 2020 virtually.

Event consisted from 9 speeches and 1 workshop of local and overseas cyber security experts including foreign speakers from Avast security and Secureworks and local speakers who work at IBM and Clever llc. After each speech, Q&A session was continued with the questions collected via IM during the speech. Overseas speakers participated Q&A session making online video calls using hopin.to platform.

The speeches covered following topics:

Mongolian Threat Landscape

Analyzing Source Code for Bug Bounty

Security Orchestration, Automation and Response

APT Group Targeting East Asia Governmental Institutions

Monitoring Windows Events and Logs

Mindset of Hacking

Hardening O365 to Reduce Attack Surface for Small Business Companies

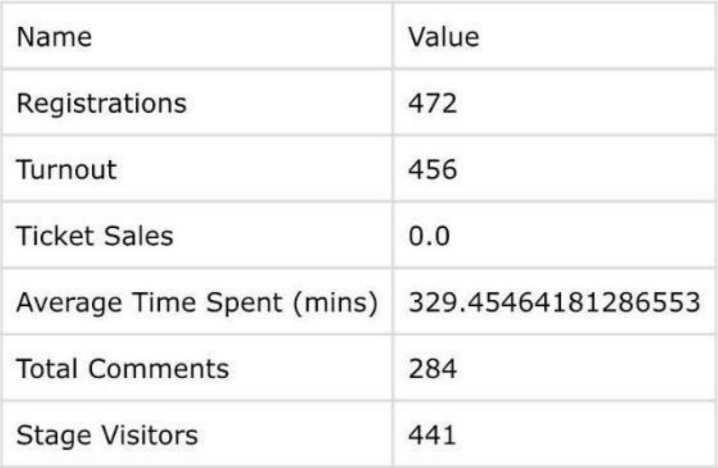
Diving into the Darknet (Card fraud) and

Belt and Road, the new colonialism?

In order to broadcast the event, we used hopin.to platform which allowed the broadcast for registered participants.

As shown the table below, Hopin.to gave us a report which said that total of 472 participants registered, 456 of them had turnout and average spent time was 329 minutes. Total comments with questions reached to 284. Please find the MNSEC2020 virtual event screenshots and hopin.to report from the attachment below.

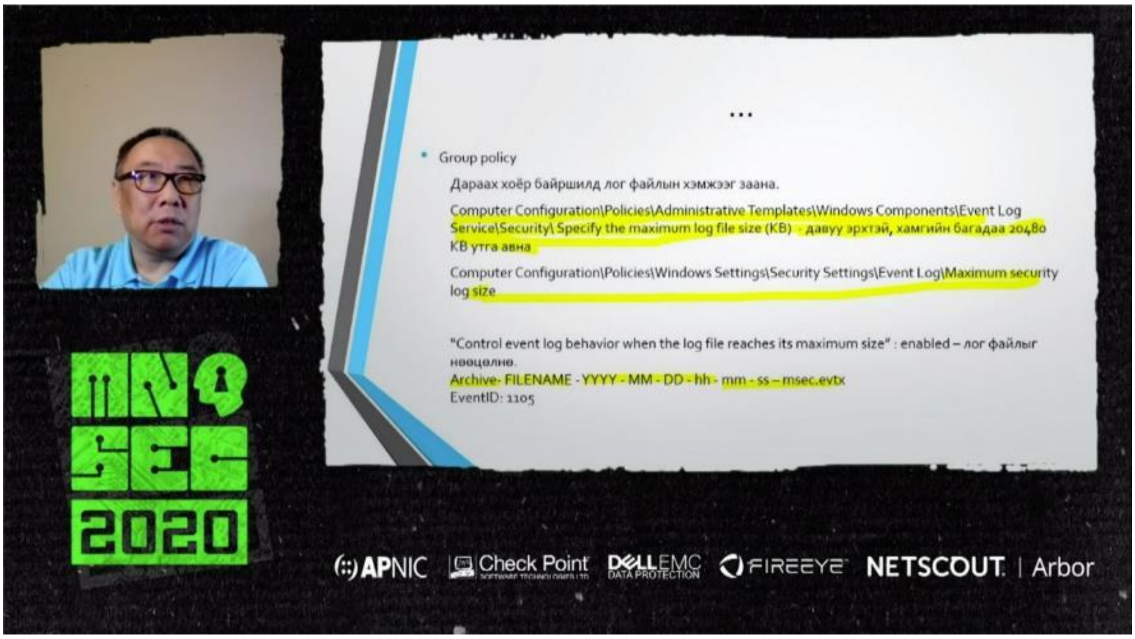
Hopin.to report



Name	Value
Registrations	472
Turnout	456
Ticket Sales	0.0
Average Time Spent (mins)	329.45464181286553
Total Comments	284
Stage Visitors	441

Main stage of the event

Speaking session



...

- Group policy

Дараах хоёр байршилд лог файлын хэмжээг заана.

Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\Security\ Specify the maximum log file size (KB) - давуу эрхтэй, хамгийн багадаа 20480 KB утга авна

Computer Configuration\Policies\Windows Settings\Security Settings\Event Log\Maximum security log size

"Control event log behavior when the log file reaches its maximum size" : enabled – лог файлыг нөөцөлнө.
Archive- FILENAME - YYYY - MM - DD - hh - mm - ss – msec.evtx
EventID: 1105

5. International Collaboration

5.1 International partnerships and agreements

- APCERT
- TEAM CYMRU

- FIRST
- APWG
- MICROSOFT
- NCFTA

5.2 Capacity building

5.2.1 Training

- MNCERT/CC attended to Japan - US Industrial Control Systems Cybersecurity Week (FY2020).

5.2.2 Seminars & presentations

- MNCERT/CC attended to APCERT VIRTUAL AGM 2020.

6. Future Plans

6.1 Future Operations

MNCERT/CC planned the following activities in 2021.

Events, conferences and drill to participate are as follows:

- APCERT Annual General Meeting 2021.
- APCERT Drill 2021.

Local activities to organize are as follows:

- MNSEC 2021 Cyber Security Event
- "Kharuul Zangi 2021" Cyber Security Contest among security engineers.
- Local cyber drill among member organizations.
- Local training for our constituency.

7. Conclusion

Due to the covid-19 pandemic situation, 2020 was the year of experiencing online activities including meeting, event, competition and other communication. The more our activities go online, the more it requires to keep an eye on cyber security.

We are looking forward the year 2021 to be a more progressive year in both local and international stage and greater collaboration with APCERT and other international organizations.

MonCIRT

Mongolian Cyber Incident Response Team – Mongolia

1. About MonCIRT

1.1 Introduction

A Mongolian Cyber Incident Response Team (MonCIRT) is a Non-Governmental, Nonprofit organization with the objective of securing Mongolian education and public cyber space. MonCIRT provides Incident Prevention and Response services as well as Security Quality Management Services. We perform the following functions in the area of cyber security:

- Collection, analysis and dissemination of information on cyber incidents, internet threats
- Forecast and alerts of cyber security incidents
- Emergency measures for handling cyber security incidents
- Issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents
- Improve information security awareness, literacy, provide comprehensive trainings.
- Provide a comprehensive view of network security risks, attack methods, vulnerabilities, and the impact of attacks on information systems and networks;
- Provide information on incident and vulnerability trends and characteristics
- Build an infrastructure of increasingly competent security professionals who respond quickly to attacks on Internet-connected systems and are able to protect their systems against security compromises
- Such other functions relating to cyber security as may be prescribed

MonCIRT services are available for society and educational sector.

The MonCIRT helps the Internet community deal with its immediate problems and analyzes the scope and nature of the problems. To increase awareness of security issues and help organizations improve the security of their systems, we continue to disseminate information through multiple channels:

- Telephone and email
    - hotline: + 976 - 70113151
    - email: info@moncirt.org.mn

- World Wide Web: http://www.moncirt.org.mn/

1.2 Establishment

MonCIRT was established in 2006 as NGO. From 2006 till 2011 MonCIRT operate as sole national CSIRT of Mongolia. From 2012 operate MNCERT/CC at Data Center as NGO.

Now MonCIRT acts as the focal point for cyber security for the Mongolian internet society, especially educational sector.

1.3 Workforce

MonCIRT currently has a total of 6 constant staffs such as: 1 executive director, 3 experts, 1 bookkeeper, 1 system administrator. Most of our staffs works part-time.

1.4 Constituency

Currently MonCIRT‘s constituency encompasses the Public users (citizens, business companies, private sector organizations, NGO and general public) of Mongolia and whole universities, institutes, colleges, high schools and other educational organizations.

2. Activities & Operations

2.1 Summary

The year 2020 will be one that we will all remember for a very long time. Twelve months ago, very few of us could have foreseen the global disruption that would be caused by COVID-19, the worst pandemic in over a century. The seismic changes that affected our lives almost overnight continue to be felt, and will stay with us through 2021 and beyond.

The internet enabled us to keep our world running. Businesses in Mongolia surprised themselves with the speed and success of their digital initiatives: it is estimated that during 2020, digital transformation has accelerated and advanced by up to ten years. What was once thought to be almost impossible was achieved in just a few months.

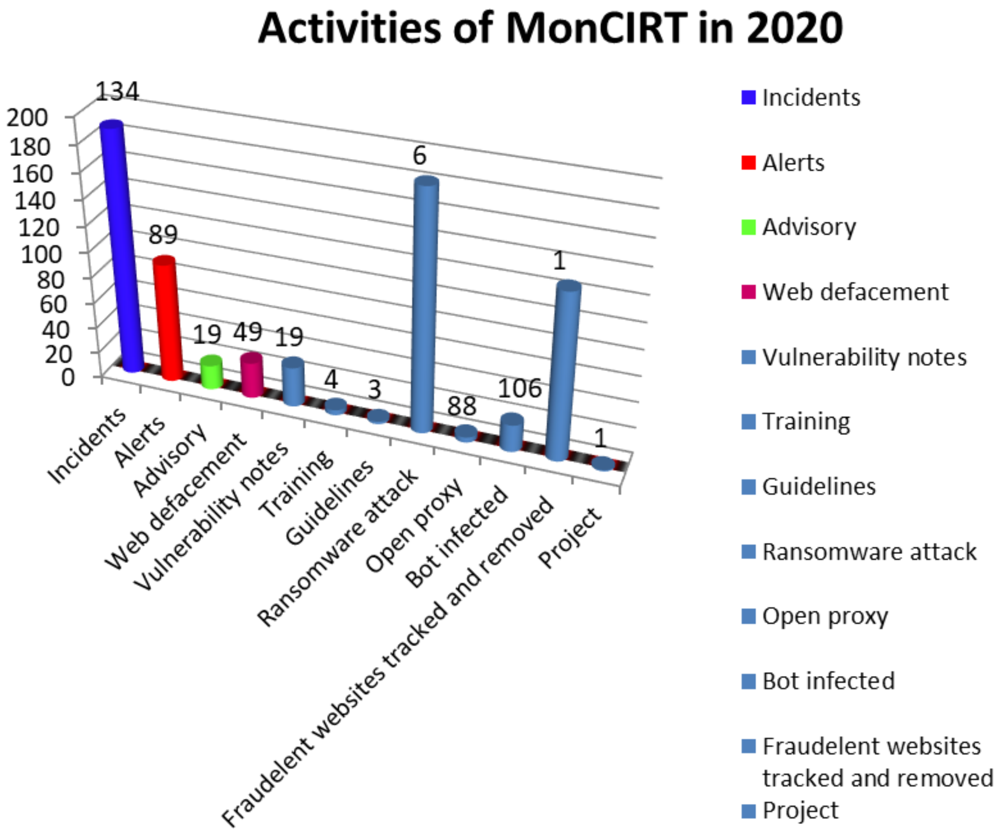
Of course, this giant leap in connectivity and our growing reliance on technology in our everyday lives has created new challenges and problems. Just as organizations have transformed their ways of working, threat actors and cyber criminals also changed their tactics so that they could take advantage of the pandemic’s disruption.

We saw huge spikes in attacks against Mongolian organizations' new remote working capabilities. We witnessed surges in phishing attacks targeting home workers and consumers, aiming to steal their personal details. There were major increases in shameless ransomware exploits and sophisticated hacking attempts targeting Mongolian Government bodies and private organizations, and the companies.

The summary of activities carried out by MonCIRT during the year 2020 is given in the following table:

Activities	Year 2020
Security Incidents handled	189
Security Alerts issued	93
Advisories Published	19
Vulnerability Notes Published	21
Security Guidelines Published	2
Online trainings Organized	3
Mongolian Website Defacements tracked and advised	28
Fraudulent Website (phishing site) hosted within Mongolia tracked and removed	128
Ransomware attacks tracked	184
Open Proxy Servers tracked	4
Bot Infected Systems tracked	21
Projects	1

The following chart depicts the distribution of various types of activities of the MonCIRT.



2.2 Incident trends

The results of 2020 do not seem to be too reassuring and one can see how they coincide in pointing to a boom in the number of incidents that seems to have no end.

The number of cyber incidents related to Covid-19 and ransomware attacks increased fivefold in 2020 in Mongolia.

As far as the months of May to December are concerned, around 60% of the emails and Facebook chats that users received had a fraudulent purpose, including phishing or malware campaigns, generally with the Covid-19 as a hook.

In addition, approximately 40% of emails and Facebook chats sent per month that are related to the Covid-19 are spam or seek to obtain confidential information from users.

During the year 2020 MonCIRT received 12 times more information on ransomware attacks, handled 32 incidents related with ransomware attacks, supported more than 120 organizations in removing ransomware and decrypt files. In cooperation with Net craft takedown response team we removed more than 120 phishing sites from Mongolian servers.

In the first part of this 2020, the threat that has experienced the most growth has been

Ransomware, that have multiplied by 12 compared to the first part of 2019.

On the other hand, there has also been a change in the operations of cybercriminals who, when using ransomware, first steal the data before encrypting it. The aim is to threaten to make the information public unless the amount required for the ransom is paid.

At a sectoral level, ransomware has an equal impact on all types of industries and it is also worth noting that many of these attacks have been linked to Covid-19, in large part caused by basic security failures, related to the use of authentication systems, passwords or email security protocols, etc.

The number of cybersecurity incidents threatening to Mongolian educational institutes and business organizations is climbing at an alarming rate.

Although ransomware attacks are the most common and fastest growing threat, they are not the only threat that we handled or received information on. 2020 comes with a whole new level of threats to cyber security that we observed in Mongolian Internet segment, including university's infrastructure:

- Credential stuffing: We observed firstly the Credential stuffing attacks in August of 2020. Another three cases reported to MonCIRT in October and November. These attacks have increased in recent years and have become a major problem, especially for online universities.
- Cloud Jacking: Cloud Jacking was likely to emerge as one of the most important cyber security threats in 2020 due to the increasing dependence of Mongolian companies on cloud computing due to remote works. Collected by us data suggests that misconfiguration will cause most incidents.
- Zoom Credentials Hack: Zoom has emerged as one of the most used online training and conference platform in Mongolia during pandemic of 2020, but it's had a few problems along the way too. About 11 cases of stolen passwords on Zoom surfaced in 2020.

Organizations are beginning to understand that a security compromise is not a matter of if, but when. But they need better tools that will enable them to fight back with the same level of sophistication as the cybercriminals who attack them.

2020 was also a watershed year for data breaches, with hacks targeting the systems of universities and business companies like National University of Mongolia, National Medical University, few small companies etc. MonCIRT observed that more than 4500 records were compromised in just those few incidents.

In 2020, the number of data breaches decrease 18 percent from 2019.

Advanced Persistent Threats

Advanced persistent threats (APT) are especially worrisome for Mongolian Government agencies IT teams because the e-office system Able that they widely use has been subjected to an APT attack from Chinese IP addresses, these attacks persisted, stealthily, for months and even years.

Many anti APT protections of Mongolian companies and universities are ineffective.

While many security solutions focus on network-level APT attacks, the most prevalent and successful attacks tend to come through applications, such as email and web access.”

Phishing

Phishing is not a new cybercrime tactic, but despite growing awareness of the problem, organizations are still struggling to stay ahead of the sophisticated social engineering techniques used in phishing attacks. In 2020 more than 1200 students and citizens became a victims of phishing attacks like email attachments or links, web-based drive-by or download (multiple responses were permitted), Facebook chats and AI-driven Cyber-attacks.

Scammers are not missing a beat. Often masquerading as trusted providers, they bait users into disclosing sensitive personal information. These techniques are also used to insert malware and bots into corporate networks — therefore we organized 2 trainings in organizations on how to avoid phishing attacks.

We teach online IT specialists of Universities and companies on new technology that can protect remote browser isolation, anti-ransomware controls, measures.

Identity theft

Nearly 180 Mongolians have been affected by identity theft, according to a 2020 online survey organized by us.

Publicly available numbers from Cybercrime department of Mongolian Policy tell a similar story.

2.3 New services

2.3.1 Multi factor authentication for remote work

Our study showed how attacks against credentials, data and other resources are outpacing investments targeted at stopping them. The December 2020 report showed that more than 80% of enterprises have experienced at least one personal data attack in

2020, but only 19% of security budgets are allocated to protect personal data, database. Therefore, we started to develop "Multi factor authentication for remote work" project and deployed digital certificate based authentication system in 6 companies and 2 universities in cooperation with MonPass Certification Authority. We expected that thanks to this authentication system the number of cyber-attacks to educational networks and business organizations will decrease about 60 percent.

3. Events organized / co-organized

3.1 Training / Education

To create awareness and to enable users to implement best practices, MonCIRT is organizing workshops and training programs on focused topics for targeted audience such as CISOs, financial and banking sector officers, System Administrators, ISPs etc.

Due to COVID19 lockdowns we organized below online trainings in this year for system administrators.

Courses offered in 2020 included the following:

- Organize secure remote works
- Remove Ransomware and decrypt, restore files

In addition, MonCIRT organized following online workshops:

- Workshop on " Cyber Threat Intelligence" on August 19, 2020

3.2 Drills

In 2020 MonCIRT organized local network security drill-VIII involving all state universities and 14 private universities, institutes.

Cyber Drill VIII was planned and culminated in the conduct of a three days exercise between September 14-16, 2020. It was conducted as a 'no-fault' exercise, with the strategic level objective being to test and evaluate Mongolia's educational sector's incident management arrangements in order to most effectively address a cyber threats.

The exercise was run, as much as possible, with participants playing from their normal operating environments using everyday communications. It was coordinated from a central control cell in Mongolian University of Science and Technology, where events from a consolidated master list were passed on to the players for their responses. The problems or incidents in the exercise were all simulated – no live systems were involved.

Cyber Drill VIII became the powerful contribution in communicating of security officers, incident handlers, network administrators of universities and in security information sharing. In addition, it was the second successful experience in incident coordination.

3.3 Conferences, Seminars

In 2020 we cannot organize conferences, seminars, workshops within the constituency. We participated in few online conferences including FIRST online conference.

4. Achievements

4.1 Presentations

In this year we cannot participated and presented in Information security conferences. But we actively participated in development of draft laws on “Cyber security”, “Personal data protection” and amendments to “e-Signature law”.

4.2 Publications

The MonCIRT published 19 advisories and 21 vulnerability notes in 2020 on our Facebook page (https://www.facebook.com/MonCIRT/). Among the criteria for developing an advisory are the urgency of the problem, potential impact of intruder exploitation, and existence of a software patch or workaround.

MonCIRT Security Practices

MonCIRT security practices are easy-to-implement guidance for experienced system administrators. The practices are technology-neutral, so they apply to many operating systems and platforms. Practices developed in this year include the following:
Removal of DJVU versions, Dharma ransomware and restore, decrypt files
Remove phishing and mirror sites.

4.3 Certification & Membership

No Certification and Memberships obtained in 2020.

5. International and Domestic Collaboration

5.1 MoU

No Memorandum of Understandings signed in 2020.

5.2 International incident coordination

Upon request of and in cooperation with Net craft takedown service team we removed 128 phishing web sites installed illegally in Mongolian web servers which was increases 16 times than 2019.

6. Future Plans

6.1 Future projects

No future projects planned in 2021.

6.2 Future plan

We plan to ask for technical and financial support from Mongolian Government, because Mongolian prime minister announced digital transformation year and the Government drafted IT laws, plan to establish Government Cyber Security Operation Center. Following are the future plans:

- Support in establishment & deployment of Government Cyber Security Operation Center
- Establish close cooperation with Government Cyber Security Operation Center

7. Conclusion

For MonCIRTs' constant and developing activity it is necessary some financial support. In 2020 MonPass CA LLC financed most of expenses of MonCIRT.

Due to constant financial difficulty MonCIRT gives the basic attention on the new financing strategy, some Government support and updated services including educational program, awareness campaigns, presentations and publications.

Henceforth, MonCIRT shall focus on extending and empowering its constituency area involving more and more companies, creating membership. Thus, MonCIRT will act as a real general private sector oriented CSIRT.

All the online events organized by MonCIRT during the year 2020 were very successful. We will continue to conduct the Annual "Security Open Day" and plan to organize National Conference on Cyber Security in autumn of 2021 online.

MonCIRT shall continue to participate in regional events such as the Annual APCERT drill and will join to FIRST.

Contact Information

Postal Address: Mongolian Cyber Incident Response Team (MonCIRT).

PEPSI office, 4th floor. Manlaibaatar Damdinsuren street. Bayanzurkh district. Ulaanbaatar, Mongolia.

Incident Response Help Desk

Phone: +976-70113151

Fax : +976-70113151

SingCERT

Singapore Computer Emergency Response Team- Singapore

1. Highlights of 2020

The Singapore Computer Emergency Response Team (SingCERT) is part of the Cyber Security Agency of Singapore (CSA). SingCERT serves as a trusted point of contact for cyber incident reporting for the members of the public, private businesses and international CERTs around the world.

Against the backdrop of the rising trend in cyber incidents, in part due to the global COVID-19 pandemic, CSA launched two initiatives aimed at promoting cybersecurity awareness and fostering a more secure cyberspace in 2020:

i. 4th Edition of Singapore Cyber Landscape
Highlights facts and figures on significant cyber threats and incidents in Singapore for 2019.

ii. Cybersecurity Awareness Campaign – "Go Safe Online C.A.F.E"
Encourages the adoption of good cybersecurity habits in fun and engaging ways.

iii. Safer Cyberspace Masterplan 2020
Outlines a blueprint for the creation of a safer and more secure cyberspace in Singapore.

2. About SingCERT

2.1 Introduction

The Singapore Computer Emergency Response Team (SingCERT) is Singapore's national CERT, serving as a trusted point of contact for cyber incident reporting to the members of the public, private businesses and international CERTs around the world.

It was set up to facilitate the detection, resolution and prevention of cyber security related incidents on the internet. Besides providing technical assistance and identifying trends in hacking activities, SingCERT also works closely with other security agencies and Internet Service Providers (ISPs) to resolve cybersecurity incidents.

SingCERT's Contact Information:

- Website: https://www.csa.gov.sg/singcert
- Email: singcert@csa.gov.sg

2.2 Establishment

SingCERT was first set up in October 1997 by the then-Infocomm Development Authority of Singapore (IDA), in collaboration with the Centre for Internet Research, National University of Singapore (NUS). SingCERT transited to the Cyber Security Agency of Singapore (CSA) when it was established on 1 April 2015.

CSA is the national body overseeing cybersecurity strategy, operation, education and outreach, technology and industry development for Singapore's critical information infrastructure. It is managed by the Ministry of Communications and Information and reports to the Prime Minister's Office.

2.3 Resources

SingCERT publishes specific threat alerts and advisories on cyber threats and trends that affects its constituency on the SingCERT website (https://www.csa.gov.sg/singcert). These are broadcasted through the SingCERT subscribers' mailing list, and CSA's Facebook and Twitter platforms.

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

2.4 Constituency

SingCERT primarily serves the local constituency comprising members of the public and private businesses in Singapore.

3. Activities & Operations

3.1 Scope and definitions

SingCERT provides technical assistance, facilitates communications in response to cybersecurity related incidents, and collaborates with foreign CERT partners in handling cross border cyber threats.

SingCERT also monitors and evaluates global cyber threats and vulnerabilities. It publishes alerts and technical advisories with recommended preventive measures.

3.2 Incident handling reports

SingCERT receives incident reports via our incident reporting channels. Upon receipt of report, SingCERT will assess the incident and advise the victim and any other relevant entity on appropriate steps to take.

In 2020, SingCERT received reports of 4,686 incidents, a 30.2% increase from the 3,598 incidents reported to SingCERT in 2019. The table and graph below show the number of incidents received in each quarter.

	Jan – Mar	Apr – Jun	Jul – Sep	Oct – Dec	Total
Number of Incident Reports	1,069	1,391	1,194	1,032	4,686

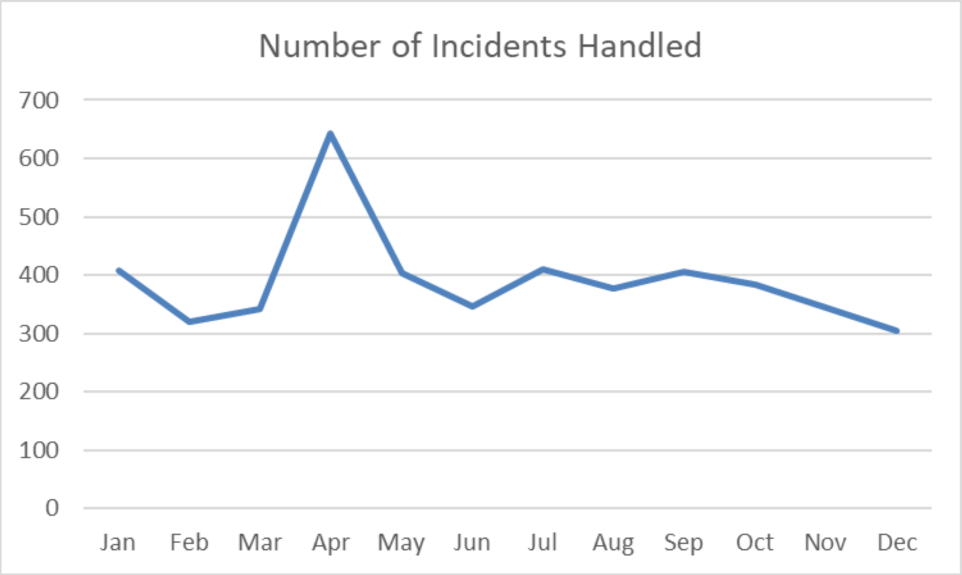


Figure 1: Number of Incidents Reported to SingCERT (2020)

3.3 Abuse statistics

SingCERT receives numerous incident reports on different types of cyber attacks. The most common types of cyber incidents handled by SingCERT are phishing, intrusion attempts / attacks, and malware infection.

In 2020, phishing was the most prevalent cyber threat in Singapore. This has been a trend that we have 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.

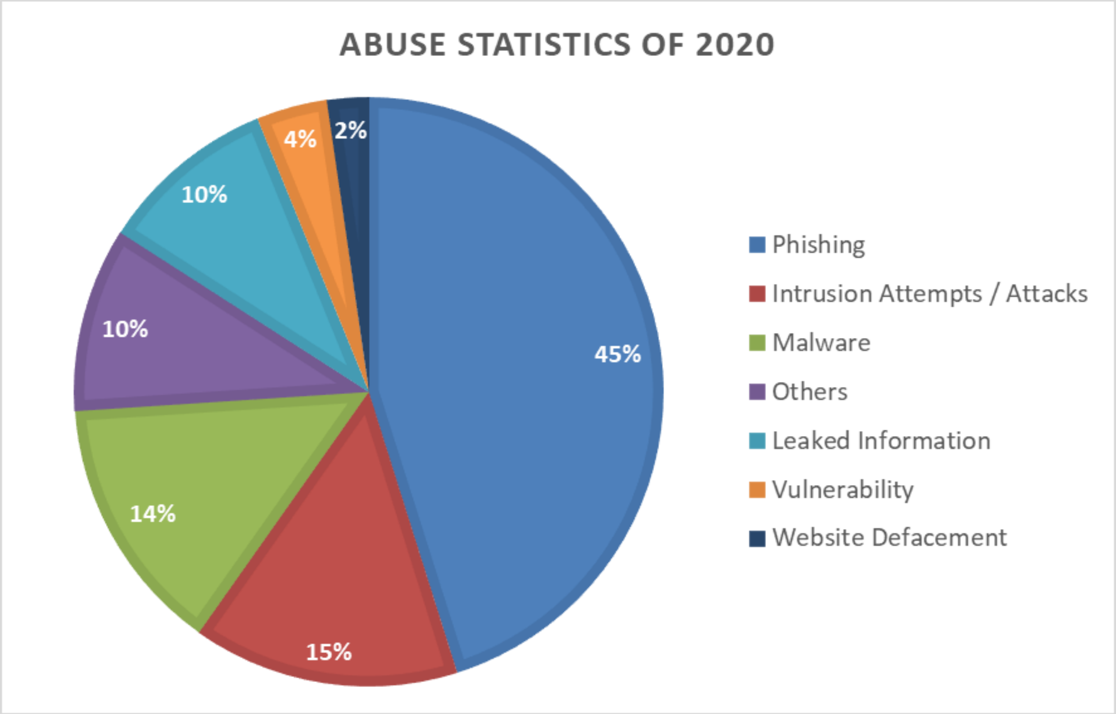


Figure 2: Abuse Statistics (2020)

3.4 Publications

3.4.1 Alerts and Advisories

SingCERT publishes alerts and advisories to raise the awareness and knowledge of our constituents to the current threats and trends, as well as to provide information on emerging threats and vulnerabilities and the recommended mitigation measures to adopt. SingCERT also publishes a weekly Security Bulletin providing a summary of new vulnerabilities.

In 2020, SingCERT published a total of 79 alerts and advisories on SingCERT's website https://www.csa.gov.sg/singcert. This is an increase from the 63 alerts and advisories published in 2019. The chart below shows the month-by-month comparison between 2020 and 2019.

	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Total
2019	8	3	2	9	4	5	6	2	8	8	5	3	63
2020	10	5	8	6	8	11	6	2	5	5	9	4	79

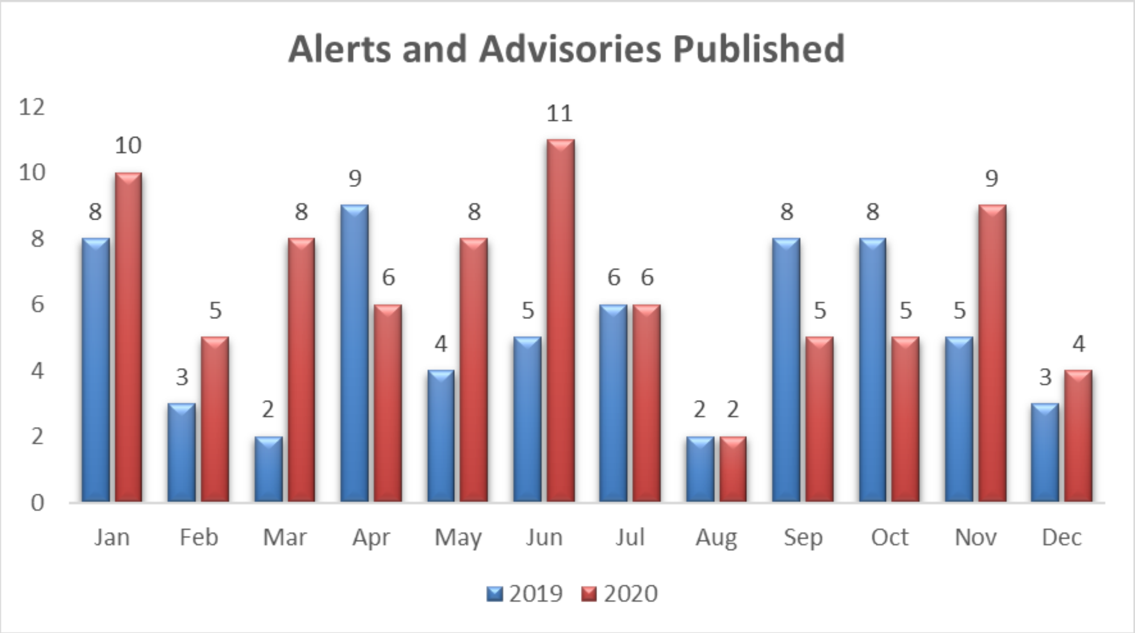


Figure 3: Comparing the Number of Alerts and Advisories Published (2019 to 2020)

Of the 79 alerts and advisories, 59 of them were published to address critical vulnerabilities discovered by software vendors, and the notification of patches released to fix the vulnerabilities. The list of alerts and advisories are tabulated below:

Date	Title
07 Jan	Critical Vulnerabilities in Cisco Products (CVE-2019-15975, CVE-2019-15976, CVE-2019-15977)
09 Jan	Microsoft Windows 7, Windows Server 2008 and 2008 R2 End of Support
10 Jan	Advisory on Risks of Shortened URLs
14 Jan	Critical Vulnerabilities in Citrix ADC, Citrix Gateway, Citrix SD-WAN WANOP (CVE-2019-19781) and Pulse Secure VPN (CVE-2019-11510)
15 Jan	Critical Vulnerabilities in Microsoft Windows Operating System
15 Jan	Oracle Security Patches Update for Administrators
16 Jan	Intel Security Patches
29 Jan	Critical Vulnerability in Cisco Product (CVE-2019-16028)
30 Jan	Critical Vulnerabilities in Magento Commerce Software

31 Jan	Malicious Cyber Activities Leveraging COVID-19 Situation
06 Feb	High Severity Cisco Discovery Protocol Vulnerabilities (CVE-2020-3110, CVE-2020-3111, CVE-2020-3118, CVE-2020-3119, CVE-2020-3120)
12 Feb	Microsoft February 2020 Patch Tuesday
21 Feb	Critical Vulnerability in Cisco Product (CVE-2020-3158)
24 Feb	Good Hygiene Practices for Group Chats
26 Feb	High-Severity Vulnerability in Google Chrome (CVE-2020-6418)
02 Mar	Critical Vulnerability in Apache Tomcat (CVE-2020-1938)
05 Mar	Importance of Valid Digital Certificates For Websites
06 Mar	Multiple Vulnerabilities in Bluetooth Low Energy (BLE) Devices
11 Mar	March 2020 Monthly Patch Release
17 Mar	Critical Vulnerabilities in Trend Micro's Products
24 Mar	Critical Vulnerabilities in Microsoft Windows Adobe Type Manager Library
27 Mar	Tips for Staying Cyber-Safe While Telecommuting
29 Mar	Critical Vulnerabilities in DrayTek Vigor2960/3900/300B Networking Products
06 Apr	Critical Vulnerabilities in Mozilla Firefox and Firefox ESR
13 Apr	Alert on Magento 1 End-Of-Life
15 Apr	April 2020 Monthly Patch Release
24 Apr	Zero-Day Vulnerabilities in iOS
24 Apr	Bringing Your Business Online Securely
28 Apr	High Severity Vulnerability in WordPress Real-Time Find and Replace Plugin
04 May	Advisory on Good Security Practices Against Web Shell Attacks
05 May	Critical Vulnerabilities in SaltStack Management Framework

06 May	Large-Scale Attempts to Attack WordPress Sites
13 May	Vulnerability in vBulletin Connect (CVE-2020-12720)
13 May	May 2020 Monthly Patch Release
14 May	Critical Vulnerabilities in Adobe Acrobat, Reader and DNG Software Development Kit
25 May	Critical Vulnerability in Apache Tomcat (CVE-2020-9484)
27 May	High-Severity Vulnerability in Android Devices (CVE-2020-0096)
05 Jun	Critical Vulnerabilities in Cisco IOS Software
09 Jun	Advisory to Political Parties on Phishing Attacks Reportedly Targeting US Presidential Campaigns
10 Jun	Critical Vulnerability in Exim Mail Server (CVE-2019-10149)
10 Jun	June 2020 Monthly Patch Release
12 Jun	Fake Malicious Mobile Applications Imitating Contact-Tracing Applications
17 Jun	Critical Vulnerabilities in Treck TCP/IP stack software
18 Jun	High-Severity Vulnerabilities in Google Chrome
18 Jun	High Severity Vulnerabilities in Cisco Webex Meetings Desktop Application
19 Jun	Singapore Businesses Reportedly Among Targets of Global Phishing Campaign
28 Jun	Tips to Stay Cyber-Safe for the Singapore General Election 2020
30 Jun	Critical Vulnerability in Palo Alto Networks PAN-OS (CVE-2020-2021)
04 Jul	Critical Vulnerability in BIG-IP Application Delivery Controller (CVE-2020-5902)
04 Jul	Vulnerabilities in Apache Guacamole (CVE-2020-9497 and CVE-2020-9498)
14 Jul	Critical Vulnerability in SAP NetWeaver Application Server Java (CVE-2020-6287)
15 Jul	July 2020 Monthly Patch Release
16 Jul	Critical Vulnerabilities in Cisco Products

30 Jul	High-Severity Vulnerability in GRand Unified Bootloader version 2 (CVE-2020-10713)
07 Aug	High Severity Vulnerability in Cisco DNA Center Software
12 Aug	August 2020 Monthly Patch Release
03 Sep	Zero-Day Vulnerability in WordPress File Manager Plugin
04 Sep	Global Ransom DDoS Campaign
09 Sep	September 2020 Monthly Patch Release
15 Sep	Active Exploitation of ZeroLogon - Critical Vulnerability in Netlogon Remote Protocol (CVE-2020-1472)
18 Sep	Multiple vulnerabilities in Citrix ADC, Citrix Gateway, and Citrix SDWAN WANOP
14 Oct	October 2020 Monthly Patch Release
14 Oct	Critical Vulnerability in SAP CA Introscope Enterprise Manager (CVE-2020-6364)
16 Oct	Critical Vulnerabilities in Magento Commerce and Open Source (CVE-2020-24407 and CVE-2020-24400)
22 Oct	Active Exploitation of MobileIron's Mobile Device Management (MDM) solution
30 Oct	Active Exploitation of Oracle WebLogic Server Vulnerabilities (CVE-2020-14882 and CVE-2020-14883)
03 Nov	Remote Code Execution (RCE) vulnerability in Oracle WebLogic Server (CVE-2020-14750)
04 Nov	Critical Vulnerabilities in Adobe Acrobat and Reader
04 Nov	Protecting Yourself From WhatsApp Hijacking
06 Nov	Zero-Day Vulnerabilities in iOS
06 Nov	Protecting Your Enterprise from Business Email Compromise Attacks
11 Nov	November 2020 Monthly Patch Release
13 Nov	Protecting Individuals and Businesses From Data Breaches
24 Nov	Critical Vulnerabilities in VMware Products
30 Nov	Critical Vulnerabilities in Drupal 7, 8.8, 8.9, and 9.0

09 Dec	December 2020 Monthly Patch Release
14 Dec	Active Exploitation of Vulnerability in SolarWinds Orion Platform
28 Dec	Remote Command Execution Vulnerability in SolarWinds Orion Platform
28 Dec	Protect Your Systems and Data From Ransomware Attacks

3.4.2 Singapore Cyber Landscape

The 4th edition of the Singapore Cyber Landscape publication was released on 26 June 2020. The publication highlights the facts and figures of significant cyber threats and incidents in Singapore for 2019.

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

More information about the publication, including a downloadable copy, is available via https://www.csa.gov.sg/news/publications/singapore-cyber-landscape-2019

Figure 4: Singapore Cyber Landscape 2019

3.4.3 National Cybersecurity Awareness Campaign

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

Cybersecurity Awareness Campaign – "Go Safe Online C.A.F.E"

On 14 Jan 2020, CSA launched the "Go Safe Online C.A.F.E (Cybersecurity Awareness for Everyone)" campaign. The campaign builds on the momentum from past years and reinforces the adoption of good cybersecurity habits such as:

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

More information about the campaign is accessible via
https:/csa.gov.sg/gosafeonline/go-safe-for-me/homeinternetusers/go-safe-online-2019

To extend the reach of the campaign, a series of roadshows were organised. The roadshows featured interactive activities for visitors to get hands-on practice of key cybersecurity habits that help them stay safe online. The activities include:

i. 'Block the Viruses' – an activity to educate players on the impact of malware infection in devices,
ii. 'Spot Signs of Phishing' – an activity to educate players on how to identify real versus phishing emails or websites, and
iii. 'Password Journey' – an activity to educate players on how to create a strong and memorable password.

3.4.4 Safer Cyberspace Masterplan 2020

CSA launched the Safer Cyberspace Masterplan 2020 on 6 October 2020 at the opening ceremony of the 5th Singapore International Cyber Week (SICW). The Masterplan was developed in consultation with industry and academic partners and builds on the 2016 Singapore Cybersecurity Strategy. It outlines a blueprint for the creation of a safer and more secure cyberspace in Singapore by raising the general level of cybersecurity for individuals, communities, enterprises, and organisations. The Masterplan comprises three strategic thrusts:

i. Securing our core digital infrastructure;
ii. Safeguarding our cyberspace activities; and
iii. Empowering our cyber-savvy population.

CSA aims to implement the initiatives within the Masterplan from 2021 to 2023. The

Masterplan will also be reviewed regularly to keep up with the prevailing cyber threat landscape.

More information about the Masterplan, including a downloadable copy, is available via https://www.csa.gov.sg/news/publications/safer-cyberspace-masterplan

4. Events organised & hosted

4.1 Drills & Exercises

4.1.1 ASEAN CERT Incident Drill 2020

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 7 October 2020, SingCERT successfully conducted the 15th iteration of ACID. CERT representatives from all ten ASEAN Member States (AMS) and five Key Dialogue Partners participated in the drill. The theme "*Malware Campaign Leveraging the Pandemic Situation*" was chosen in view of the proliferation of malicious campaigns leveraging the COVID-19 pandemic as lures across multiple sectors, in many countries in the earlier part of the year. Participants were given a series of scenario injects that were designed based on the Emotet malware campaign, given its prevalence, and the range of cybersecurity events that may occur following a successful Emotet malware infection. During the pre-drill dialogue, participants agreed that it was an opportune time to raise awareness and preparedness against such opportunistic campaigns.

4.2 Conferences and seminars

4.2.1 Singapore International Cyber Week 2020

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 5th SICW was held from 5 to 9 October 2020, with the theme "Co-operation in a Post-COVID Future". The event focused on how countries can work together to build a secure and resilient cyberspace that serve as an enabler of economic progress in the digital future.

Due to the ongoing COVID-19 pandemic, SICW was held as a hybrid event with a series of inter-linked virtual meetings that allowed key leaders from governments, industry, academic and non-government organisations to explore the future of cyberspace cooperation from a broader range of perspectives. SICW successfully concluded with more than 6,000 participants from across 60 countries, as well as 138 speakers from across governments, industry and academia. Details about the event can be found at https://www.sicw.sg.

4.2.2 Cybersecurity Awareness Alliance

One of the ways in which CSA drives cybersecurity awareness efforts, is through the Cybersecurity Awareness Alliance - a collaboration between public and private sector organizations as well as trade associations to raise awareness and adoption of cybersecurity measures. Alliance members actively give talks to schools, businesses and the community at various platforms.

5. International Collaboration

5.1 Training

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

Date	Title	Presented by
18 Feb	Identification of information security risks as a sectoral CSIRT and addressing the risks	FinCSIRT
07 Apr	Getting started with Threat Intelligence Sharing via MISP	CIRCL.LU
11 Aug	Digital Forensics Procedures & Interesting Artifacts	Sri Lanka CERT | CC

5.2 Drills & Exercises

5.2.1 Asia Pacific Computer Response Team (APCERT) Cyber Security Drill 2020

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 11 March 2020 with the theme “Banker doubles down on Miner”. The drill evaluated the response capabilities of member teams in responding to real incidents and issues that exist on the internet. As a member of the APCERT Drill Working Group, SingCERT was part of the Exercise Controller Team conducting the drill.

5.2.2 ASEAN-Japan Cyber Exercise

The ASEAN-Japan Cyber Exercise seeks to develop an information sharing framework and enhance the cyber cooperation amongst the ASEAN Member States (AMS) and Japan. CSA is a member of the ASEAN-Japan Cybersecurity Working Group which conducts two exercises annually, namely (a) the Cyber Exercise, and (b) the Table Top Exercise.

SingCERT participated in the Remote Cyber Exercise held on 25th June 2020 which aims to enhance the skills of incident handling and coordination of cyber incidents between countries. The Table Top Exercise was not conducted in 2020.

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 virtual FIRST Conference from 16-18 November 2020.

5.3.2 APCERT Annual General Meeting (AGM) and Conference 2020

The APCERT AGM and Conference is an annual event where CERTs from the Asia Pacific region gather to exchange information on the latest cybersecurity issues and incident response methodologies. SingCERT attended the APCERT Annual General Meeting (AGM) held on 29 September 2020. However, due to the ongoing COVID-19 pandemic, the AGM was conducted virtually, and the Conference was postponed till 2021.

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 2021:

S/n	Description	Category
1	Singapore Cyber Landscape 2020	Publications
2	6th Singapore International Cyber Week (SICW)	Events Organising & Hosting
3	16th iteration of ASEAN CERT Incident Drill (ACID)	Events Organising & Hosting

Sri Lanka CERT|CC

Sri Lanka Computer Emergency Readiness Team Coordination Centre – Sri Lanka

1. ABOUT SRI LANKA CERT|CC

1.1 Introduction

The Sri Lanka Computer Emergency Readiness Team | Coordination Centre (Sri Lanka CERT|CC) is the National Centre for cyber security in Sri Lanka, mandated to protect Sri Lanka's Information and Information Systems Infrastructure. Its services range from responding to investigating information security breaches, in order to prevent security breaches through awareness, security assessments, Managed services, Forensics and capability building.

1.2 Establishment

As the National CERT of Sri Lanka, Sri Lanka CERT acts as the focal point for cyber security of the nation. It is the single trusted source of advice about 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 1st of July 2006 as a subsidiary of Information and Communication Technology Agency of Sri Lanka (ICTA). Currently Sri Lanka CERT functions under the purview of Ministry of Technology.

1.3 Workforce

At the end of 2020, the Sri Lanka CERT team comprised of twenty-three (23) staff members. This includes the Chief Executive Officer, Chief Operating Officer, Head of Research, Policy and Projects, Chief Information Security Engineer, three Information Security Engineers, five Associate Information Security Engineers, two project managers, four Information Security Analysts, two Associate Information Security Analysts, Head of Human Resources and Administration, Admin & Account Assistant and a driver cum office assistant. In addition, there are six undergraduate interns assisting the operation of the organizations. Eight staff members were recruited during the year 2020. During the period, six undergraduate interns completed their internships at the organization (June 2020).

All the staff are highly skilled and experienced in different areas of information security and have achieved corresponding Information Security certifications which are widely recognized in the industry, such as SANS GCIH, Microsoft MCSE, EC-Council CEH and CHFI, Red Hat RHCSA, RHCE, Cisco CCNA and CCSP and CISSP by International Information Systems Security Certification Consortium; (ISC)^2.

1.4 Constituency

Sri Lanka CERT 's Constituency encompasses the whole of the cyber community of Sri Lanka (private & public sector organizations, and the general public). Sri Lanka CERT maintains a good rapport with government and private sector establishments, and extends assistance to the general public as permitted by available resources. In accordance with its mandate, Sri Lanka CERT | CC gives priority to requests for assistance from government agencies. Based on availability of human resources and necessary skills, requests from private sector are handled free of charge or on a paid basis, depending on the type of service provided.

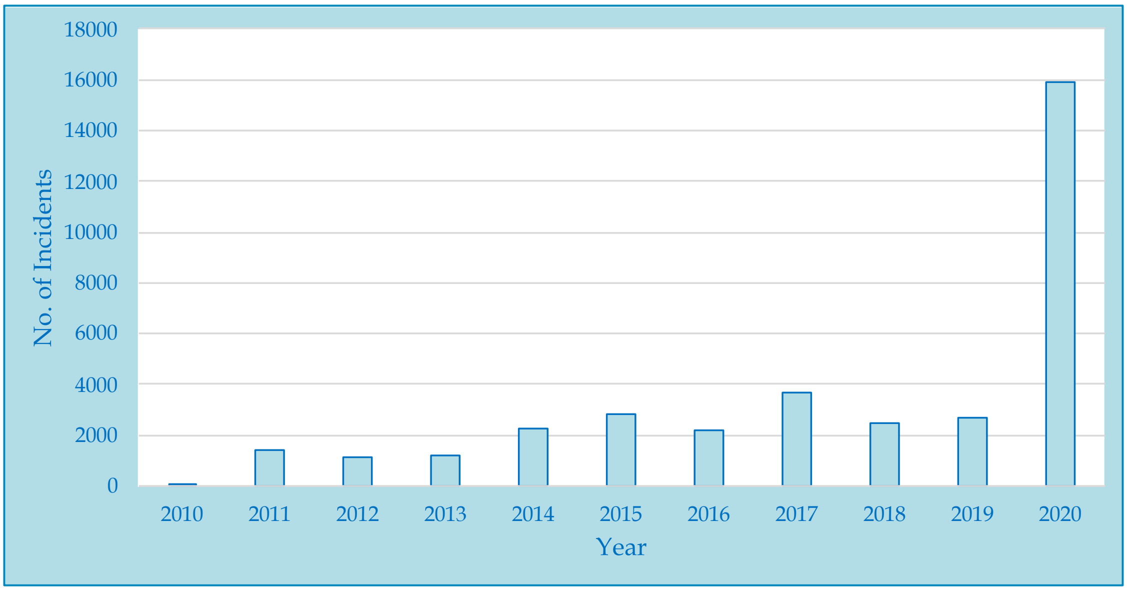
2. Activities & Operations

2.1 Incident Handling Summary

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

The types of incidents received by Sri Lanka CERT include incidents related to social networks, email compromise, phishing, web site compromise, scams, malicious software issues and ransomware, privacy violations, financial frauds, compromised unique IP's extracted from the information collected by automated systems operated by international organizations.

Majority of the reported incidents fall into the category of social media related incidents and on average more than 1000 cases reported each month. Among the social media incidents, as usual Facebook related incidents were the highest. This may be due to increased use of social media, due to COVID-19 pandemic situation.



Graph 1: Total number of social media related incidents

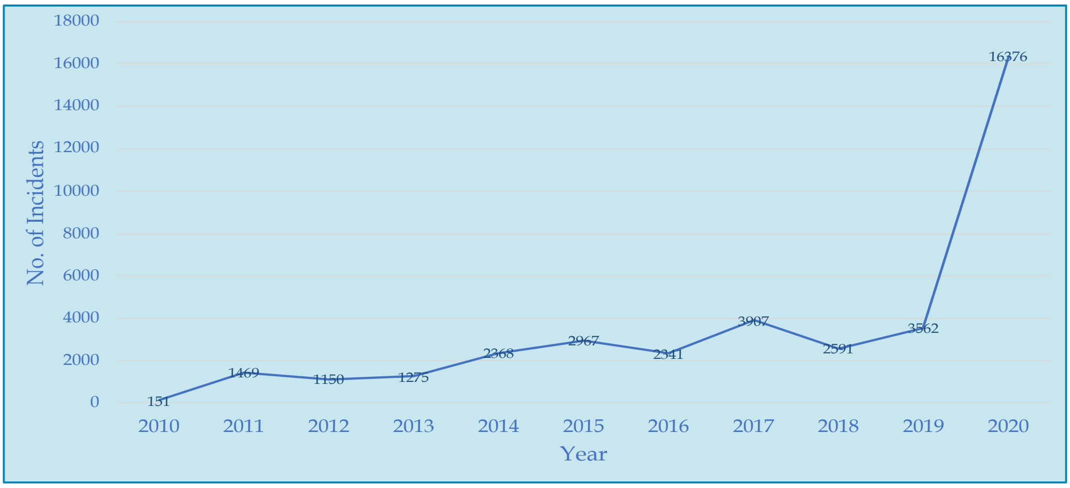
The following table depicts the distribution of various types of incidents reported to Sri Lanka CERT in the years 2019 and 2020. All the incidents reported to Sri Lanka CERT have been resolved satisfactorily.

Incident Type	No of Incidents - 2019	No of Incidents - 2020
DDOS	2	1
Ransomware	6	24
Abuse/Hate/Privacy violation	307	70
Malicious Software issues	8	9
Phone Hacking	1	6
Scams	5	157
Phishing	5	17
Website Compromise	175	85
Financial/Email frauds	7	57
Intellectual property violation	1	1
Server Compromised	2	6
Social media	2662	15895
Other	364	48

Table 1: Number of reported incidents in years 2019 & 2020

Through an analysis of the cyber security related data collected by the Sri Lanka CERT|CC during the years 2019 and 2020 following observations can be made;

i. Number of reported cases related to privacy violations has been decreased during the year 2020.
ii. Financial frauds targeting local importers and exporters have seen a massive upturn during the year 2020 compared to 2019.
iii. There has been a significant increase in the spread of ransomware and malicious software during the year of 2020, where sensitive data belong to both individuals as well as corporate businesses have been made unavailable through encrypting, erasing or modifying data.
iv. A significant number of web site compromises targeting government and private sector organizations were recorded in 2020. However, there is a notable 48% decrease when comparing to year 2019.
v. Incidents reported to Sri Lanka CERT have increased to 16,376 in the year 2020. In the year 2019, 3566 incidents were reported. This is nearly a 460% increase in reported incidents compared to the year 2019.



Graph 2: Total number of reported incidents

2.2 Consultancy Services

Sri Lanka CERT continues to provide consultancy services in response to requests made – particularly from government departments. Below are the main consultancy assignments undertaken by CERT during the year;

i. Technical Review Committee (TEC) member of procurement of email solution for a Bank

ii. TEC member of Privileged Access Management (PAM) for a Bank

iii. TEC member of procurement of email solution for a Bank

iv. TEC member of procurement of AV for ATM network of a Bank

v. TEC member of Central Bank of Sri Lanka Procurement of Reserve Management System

vi. Technical Expert of the Presidential Commission on Easter Sunday attack

vii. Curriculum development for Certificate Course in Cyber Security conducted by a National University

viii. Conducted a training program on 'Cyber security incident response' for an Asian Country's Government Cyber Security Bureau.

2.3 Information Security Managed Services

i. CERT was able to deliver security managed services with following services;

- External penetration testing
- Internal penetration testing
- Device configuration reviews
- Network architecture reviews
- Application security assessments
- Sever OS configuration reviews

ii. Managed services were provided for on private organization and two government organizations during the year.

2.4 Application security audits

i. Over 41 Application Security Audits were performed. This includes both Web and Mobile Security Audits.

ii. Daily monitoring of Defaced Websites was done and identified 71 such sites.

iii. Continuous monitoring for potential cyber-attacks related to COVID-19 pandemic and Defaced Websites.

iv. Monitoring of security breaches before the identified special dates of the year.

v. Completed 83 Annual Website Assessments.

vi. Security assessments for 102 Urgent Government Website Audits were completed before November 2020.

3. Training/Education services

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

3.1 Awareness Programs and Training sessions

During the year 2020 Sri Lanka CERT conducted the following training and awareness programs successfully:

i. Cyber security awareness session for Internet Society of Sri Lanka.

ii. Session on online safety for ICT teachers.

iii. Session on cyber security fundamentals for government officers.

iv. Participated in the webinar 'Ignite educational Forum 2020' organized for general public.

v. Session on Information security and social media ethics for Postal department.

vi. Webinar on 'Digital forensic procedures and interesting artifacts' for APCERT Community.

vii. Social Media Campaign for the public through the official Sri Lanka CERT|CC Facebook page.

viii. Work from Home Guidelines and awareness webinar for the public and Administrators shared through Official Public channels.

ix. Information Security and Digital Signatures online session for Law student and Government officers.

x. Awareness session for Inland Revenue Department on Introduction to Cyber Threats, Social Media and Mitigation.

xi. Countermeasures and Forensics Webinar for university students participated as a panelist.

xii. Webinar on Cyber security and cyber bullying for public awareness.

xiii. Webinar on Cyber Hygiene & Safety for public awareness.

xiv. Webinar on Introduction to CERT & Cyber safety to University Students.

xv. Cyber Guardian e-Newsletter published every month for School Children.

xvi. Participated as panelists at Women IGF 2020 Webinar.

3.2 Awareness through electronic/ print media

Conducted following awareness sessions.

i. Fifteen voice cuts for radio channels
ii. Six video cuts for TV channels
iii. Two Radio programs
iv. Three live TV programs
v. Information for seven newspaper articles
vi. Seven Facebook live sessions

3.3 Annual cyber security week 2020 (eCSW 2020)

Following activities were completed during the e-Cyber Security Week (eCSW 2020);

i. Conducted Hacking Challenge –28th October 2020
ii. This year's theme was "Pandemic… the new Cyber norm"
iii. More than 900 participants for the online sessions- 19th to 23rd October 2020
iv. Following presentations were delivered during the conference

- Cyber security strategy of Sri Lanka -by Sri Lanka CERT
- Covid-19, SARS and Ebola Vs Defacement, Phishing and DDoS-What's the difference? -by Cyber4Dev, EU
- ATM frauds on the rise -by Sri Lanka CERT
- Understanding malicious activities from distributed honeypots -by APNIC
- Impact of the telecommunications network on national security -by TRC, Sri Lanka
- Cyber security during Covid-19 -by ST Engineering
- How to safeguard from cyber related crimes in Sri Lanka -by Sri Lanka Police
- A way forward to secure your website -by Sri Lanka CERT
- DNS ecosystem security-by ICANN
- Business email compromise cases/money laundry/cyber profiling -by Interpol
- Virtual learning environments and the impact to the learning today and beyond -by University of Queensland
- Security analytics -Detecting threat evading the radar -by CISCO

v. Panel Discussions;

- Challenges faced during COVID-19 lockdown period in Sri Lanka
- Challenges in addressing cybercrime in Sri Lanka

3.4 Security Alerts

i. An Average of 1000 compromised IPs per month were informed to ISPs.
ii. 38 critical security alerts were published and sent to subscribers.

4. Publications

4.1 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.

4.2 E-mails

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

4.3 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.

5. Infrastructure development & capacity building of CERT staff

5.1 Internal Infrastructure & process improvement

i. Implemented few proposed recommendations of SIM3 Maturity Model assessed by Estonian experts.
ii. Developed the new website for Sri Lanka CERT|CC which is at the final stage.
iii. Performed Server Hardening for Web hosting in the LGC Premises.
iv. Configured the CERT Internal Systems.
v. Developed a Training Book for Interns.
vi. Developed guideline for "best practices for secure website development".
vii. Drafted the communication Specialist SOP with the support of Cyber4Dev.

5.2 Local

Staff members of Sri Lanka CERT participated in following capacity building activities;

i. RTIR Configuration workshop (CERT/Cyber4Dev)

ii. Crisis Management (Cyber4Dev)

iii. Workshop on presentations (Cyber4Dev)

5.3 International

i. DNS Ecosystem Security (Teleconference)

ii. Training on "Safeguarding Critical National Infrastructure (CNI) – Risks and Opportunities" (ITU) (Teleconference)

iii. Webinar on Broken Access Control (Open webinar)

iv. Webinar on SQL injection attacks (Open webinar)

v. Webinar on Network Penetration Test (Open webinar)

vi. New Approach for modern threat detection, investigation and response webinar

vii. Webinar on Advanced Network Exploitations (Open webinar)

viii. OWASP May webinar on Network Penetration testing

ix. Webinar on Digital Forensics - Volatility & Autopsy (Open webinar)

x. Webinar on Hacking Docker Containers (Open webinar)

xi. Webinar on Cyber Incident Planning and Response (ISACA)

xii. Webinar on Learn to Think Like a Hacker to Stop Attacks Faster Strengthen Your Security Posture with the MITRE ATT&CK Framework (ISACA)

xiii. Webinar on Hacking iOS apps for beginners (Open webinar)

xiv. Webinar by ISMG on Cloud Security

xv. Webinar on Why Patch if you don't Fix it? (ISACA)

xvi. Webinar on Introduction to the Risk IT Framework (ISACA)

xvii. Webinar on 'Hacking and Protecting My Wi-Fi by condition zebra (Open webinar)

xviii. Webinar on Android application hacking for beginners (Open webinar)

xix. Webinar on Mac forensics, Drone Forensics, FTK tutorial (by Credence Security)

xx. Teleconference on Combatting Financial Frauds through Effective Money Interception Mechanisms (Interpol)

xxi. Email based Attacks and Mitigation (Teleconference)

xxii. Blue team training (Webinar by Soteria)

xxiii. Cyber Emergency Preparedness & Management Training (by Cyber4Dev)

xxiv. Webinar on Intellectual Property and Patent Rights (FITIS)

xxv. Advanced CSIRT Technical Training (by Cyber4Dev)

xxvi. Web Log Analysis Training (by Cyber4Dev)

xxvii. Webinar on 'Sharpen up Cyber Security Defenses for the New Normal with an Agile, Flexible, and Predictive Strategy' (ISACA)

6. Projects

6.1 Special projects

Cyber Security Projects with European Union (Cyber4Dev)

i. Sponsored two CERT staff to participate for APRICOT conference (Australia)

ii. Supported SIM3 implementation work to develop communication stratify, incident classification, RFC for CERT

iii. Following training programs were conducted for CERT staff in February 2020

- Workshop on ticketing
- Briefing on UK Incident Management Model & Briefing on Incident Exercising
- Technical Exercise Run through & PM Planning session

iv. Following training programs were conducted for CERT staff in Nov-Dec 2020

- Advanced CSIRT Training (3 days)
- Ticketing System (1/2 day)
- Log Analysis (2x ½ days)

6.2 National projects

Project Name	Project Status
National Cyber Security Operations Center-NCSOC (on-going)	i. Procurement of Physical space for the monitoring center- Procurement - Completed ii. Procurement of hardware for the production data center – On going iii. Procurement of Production data center – In progress iv. Procurement of building material for monitoring center implementation- In progress v. Supply, delivery and installation of raised floor- In

	Progress
Implementation of National Certification Authority-NCA (in progress	i. Conducted the key generation ceremony in February 2020 ii. Completed the point-in-time audit. iii. Initial registration for Registering NCA Root CA in the Common CA Database (CCADB), Completion of the period-in-time audit – In Progress
Cyber Security Capacity and infrastructure development	i. Completed the procurement of computer hardware and software ii. Completed the procurement of event manger and conducted CSW 2019 iii. Completed the procurement and conducting training
National Survey on Information and Cyber Security (In Progress)	i. Public Officer's Information and Cyber Security Readiness Survey - Conducted the survey for 117 organizations ii. Critical Information Infrastructure Readiness Survey - Completed the CI survey for 59 organizations - Data validation was completed for 51 organizations iii. Supply and Demand of Cyber Security Professionals Survey - In Progress iv. Citizen's awareness of information & cyber security including most vulnerable communities - In Progress
Improving the Information and Cyber Security Readiness of the Government Organizations Maintaining Critical Information Infrastructure (10 organizations)	Project in Progress
Development of a Web Portal to increase citizens' awareness on cyber security (www.onlinesafty.lk)	i. Completed the procurement of the website developer ii. Prototype of the web portal is completed iii. Domain name obtained as (www.onlinesafty.lk) from LK domain registry
Development of National Vocational Qualification (NVQ) Standards for Cyber Security	i. Developed the curriculum and the module outline for NVQ level 5 ii. Project in Progress
Development Online	Project in Progress

Modules on e-Learning for Government Officers	
Cyber Security Capacity building program	Project in Progress

7. International Collaboration

7.1 Activities with APCERT

i. Participated for six APCERT steering committee meetings including at APRICOT 2020 (Australia)

ii. Continuing with network monitoring project “Tsubame” with JPCERT|CC

iii. Organized and conducted meetings with the working group members as the Convener of APCERT working group – Critical Infrastructure Protection

iv. Participated for APCERT working group teleconferences- Policy and Planning, Membership

v. Conducted APCERT online training on “Digital forensic procedures and interesting artifacts” for the APCERT members

vi. Participated for APCERT cyber drill 2020 working group discussions

vii. Participating APCERT cyber drill 2020

viii. Participated for APCERT AGM Program Committee Meeting

ix. Sponsored FIRST and APNIC to obtain the APCERT membership

x. APCERT AGM and Conference 2020 (Teleconference)

- Member of the program committee of AGM
- Presented the progress of Critical Infrastructure Protection working group at the AGM
- Contributed to several APCERT working groups
- Proposed to have 2021 APCERT AGM to be in Sri Lanka
- Participated for the APCERT steering committee election 2020-2022

7.2 Activities with camp

i. Re-elected as a member of the CAMP Operations Committee for the year 2020-2021

ii. Participated for four CAMP operations committee meetings

iii. CAMP AGM and GCCD Cyber Security Seminar

iv. Leading processes and procedures relevant to membership component in CAMP OC

v. Won the Best Operations Committee Member Award during the AGM

vi. Made new contacts with cyber security related organization

vii. Reviewed membership application of Nicaragua TELCOR

viii. Prepared an article on "Key Generation Ceremony of the National Certification Authority of Sri Lanka" for CAMP Newsletter

ix. Participated in offline discussions on CAMP AGM 2020

x. Prepared an award acceptance speech video (Best OC member) to present in AGM 2020

xi. Participated for CAMP AGM 2020 and GCCD seminar (online)

xii. Reviewed membership application of Nepal CSRI

xiii. Participated for CAMP Regional Forum for Arabic Region representing CAMP OC

xiv. Reviewed and discussed about R&R arrangements

xv. Reviewed, discussed and finalized the suggestions for implementing Working Groups within CAMP

7.3 Other activities

Delivered a presentation on ITU Session on "National experiences and implications for the future related to COVID-19"

8. Achievements

8.1 Cyber security bill

The Cyber Security Bill was drafted, revised and finalized. Several meetings were held with the stakeholders before finalizing the bill.

8.2 Information security framework

Under the development of Information security Framework for government organizations following policies were developed by Sri Lanka CERT and is currently in the review process.

i. Handbook of Information Security – An Implementation Guide

ii. Baselines Security Standards (BSS)

iii. Web Application and Hosting Guidelines

iv. Access Control Policy

8.3 Certification & membership

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

i. (ISC)2 Colombo Sri Lanka Chapter the local representative organization of International Information Systems Security Certification Consortium.
ii. Membership for Threat Intelligence from ShadowServer.
iii. Membership of FIRST
iv. Membership of APCERT
v. Membership of CAMP, Korea
vi. Membership of TF-CSIRT

9. Future Plans

9.1 Future projects to be implemented

The following projects are to be initiated, and are intended to serve the constituency directly;

i. Establishment of a Sectoral CERT for Education Sector (EduCERT)

9.2 Projects in CONCEPTUAL STAGE

The following projects are in the conceptual design stage,

i. Establishment of Cybersecurity Call center
ii. Outreach and Awareness Activities
iii. Cyber Security Threat landscape in Sri Lanka
iv. Introduce Post Graduate Programs on Information and Cyber Security in collaboration with a State University

10. Summary

Sri Lanka CERT believes that it is necessary to conduct awareness campaigns to educate citizens on Information security and basic cyber hygiene in order to enable a secure and trustworthy cyber eco system within the country. It was possible to achieve this up to some extent via online awareness sessions. Even with the Covid-19 pandemic situation Sri Lanka CERT managed to conduct the Cyber Security week in electronic media with the theme “Pandemic… the new Cyber norm” with very good participation.

During this year a majority of the incidents reported to Sri Lanka CERT were related to social networking sites especially Facebook. The web site compromises were also a significant issue to the government organizations and therefore CERT as the agency responsible for incident handling, took steps to conduct website vulnerability assessments of the government organizations and directed the responsible parties to make arrangements to secure their websites.

Sri Lanka CERT is in the process of implementing the National Information and Cyber Security Strategy of Sri Lanka with the involvement of relevant stakeholders. To implement some of the proposed activities of the strategy, Sri Lanka CERT|CC has partnered with NI-CO (Northern Ireland Cooperation Overseas) of European Union to participate in a project called Cyber Resilience for Development (Cyber4Dev) which is jointly supported by the Foreign and Commonwealth Office of UK, Dutch Ministry of Foreign Affairs, and Estonian Information System Authority.

The establishment of National Certification Authority, Drafting the Cyber Security Bill, Development of the Information Security Framework for the government organizations, and the deployment of surveys are some of the main activities carried out during the year targeting the implementation of the National Information and Cyber Security Strategy.

Sri Lanka CERT shall continue to participate in regional events such as the Annual APCERT drill, conferences and also welcomes opportunities to collaborate with its sister CERTs in incident coordination and resolution.

In addition to securing Sri Lanka's cyber space, Sri Lanka CERT is committed to support in securing the information environment in the Asia Pacific region and world with the help of all the CERTs and information security organizations through APCERT and FIRST respectively.

TechCERT

TechCERT – Sri Lanka

1. About TechCERT

1.1 Introduction to TechCERT

TechCERT, Sri Lanka's first and largest Computer Emergency Readiness Team (CERT) helps public and Sri Lankan organizations keep their computer systems and networks secure. TechCERT celebrated their 14th Anniversary on 01st of September 2020.

TechCERT originated as a pioneering project of the LK Domain Registry and its academic partner to provide a safety net for organizations – large and small – against cyber-attacks and emergency situations. TechCERT has collaborative partnerships with several national and global information security organizations that provide latest data on computer and network security threats and vulnerabilities. Issuing security advisories for the public, conducting security and cyber-crime related workshops and public awareness programs on safe use of computers and the Internet, and providing engineering consultancy services are also in its repertoire of services.

1.2 Establishment

TechCERT was originally formed in 2006 and has its origins as a pioneering project of the LK Domain Registry and its academic partners, as a way of providing a safety net for large and small organizations against cyber-attacks and emergency situations. To improve the operations and to further develop TechCERT, it was incorporated as an independent not-for-profit organization, affiliated with LK Domain Registry, on 05th September 2016 (Company registration no. GA 3238).

1.3 Resources

TechCERT currently has a technical team of over 30 qualified and experienced professionals. The details of the academic/professional qualifications held by all members of the technical team are given below (most of the team members have multiple qualifications in different areas of information security, computer systems security, network security etc.):

Name	Designation	Qualification
Prof. Gihan Dias	Chairman	PhD, MSc, BSc Eng (Hons), MIE (SL), Ceng
Dr.Shantha Fernando	Director/ Co-Founder	PhD (TU Deift), Mphil (Moratuwa), MCS (SL), BSc.Eng.Hons (Moratuwa), MIET (UK), MIE (SL), CEng
Mr Dumindra Ratnayaka	Director	BSc.Eng.Hons(Moratuwa)
Dileepa Lathsara	Chief Executive Officer	MSc. BSc Eng(Hons), MIE (SL), CEng, CISSP, C|EH, CPISI (PCI DSS), Certified ISMS Auditor
Kushan Sharma	Chief Operating Officer	MBA (Colombo), MSc. (Moratuwa), BSc. Eng (Moratuwa), C|EH, AMIE (SL), MCS (SL)
Kasun Chathuranga	Principal Engineer	MSc. (Moratuwa), BSc. Eng (Moratuwa), RHCE, RHCSA, AMIE(SL), MIEEE
Nalinda Herath	Principal Engineer	MSc. (Moratuwa), BSc. Eng (Moratuwa), C|EH, CPISI, ITIL, CCNA (Security), AMIE(SL)
Kalana Guniyangoda	Principal Engineer	MSc. (Moratuwa), BSc. IT (Hons), GCFA, C|HFI
Sashika Suren	Principal Engineer	MSc in InfoSec (UCSC), BICT (UCSC), RHCE v8, RHCSA, MCTS, GDip in Bus Mgmt, Red Hat Certified Ansible Automation Specialists, Certified Payment Card Industry Security Implementer (CPISI), RedHat Certified Troubleshooting Specialist v7
Geethika Wijerathne	Senior Manager HR and Administration	MSc in Information System Management (Colombo), PMP
Mishra De Silva	Head of Enterprise Business	MBA (Colombo), BBA (U.S.A), AS (U.S.A), MSLIM
Vijan Herath	Project Manager	BSc in Computer Science, HND in Computing (UK), ORACLE HCM

		(Cert), Project Management & SCRUM Immersion (Cert)
Chathuranga Gunatillake	Senior Information Security Engineer	Msc Information Security (UCSC), BEng (Hons) Computer Networks & Security, MBCS, E|NSA, C|EH, CPISI(PCI-DSS), ISO/IEC 27001 Lead Auditor
Vishvajith Ihalagama	Information Security Engineer	BSc (Hons) Eng in Computer Engineering (Peradeniya), C|EH
Priyankara Bandara	Information Security Engineer	BSc (Hons) Eng in Computer Engineering (Peradeniya), C|EH
Asanka Dhananjaya	Information Security Engineer	BSc (Hons) Eng in Computer Engineering (Peradeniya), ECSA
Dushan Chathuranga	Senior Information Security Engineer	BSc (Hons) Eng in Computer Engineering (Peradeniya)
Dilusha Bandara	Information Security Engineer	BSc Information and Communication Technology, CCNA, C|HFI, RHCSA
Ayodya Balasuriya	Information Security Analyst	BSc. Information Systems (UCSC), CPISI(PCI-DSS)
Yenuka Sachintha	Information Security Engineer	BSc. Information Systems (UCSC), C|EH
Chalana Madusanka	Information Security Engineer	BSc (Hons) Eng in Computer Engineering (Peradeniya)
Thusitha Kumarage	Information Security Analyst	BSc. (Hons) in Information Technology (Cyber Security)
Darshana Kithulgoda	Information Security Analyst	Bachelor of Information Technology (UCSC), SSCP
Hirushan Thilanka	Information Security Analyst	BSc. Information Systems (UCSC)
Radeesha Bandara	Senior Information Security Engineer	Bsc. Computer Systems and Networking (Curtin), RHCSA, CCNA security
Pubudu Ranasinghe	Associate Information	BSc. (Hons) in Information Technology

	Security Analyst	(Cyber Security)
Dilshan Umindu	Associate Information Security Analyst	BSc. (Hons) in Information Technology (Cyber Security)
Nisal Priyanka	Information Security Specialist	BSc. (Hons) in Information Technology (Cyber Security)
Umesh Erangana	Information Security Analyst	BSc. (Hons) Computer Security (Plymouth), C|EH
Shenal Roshli Perera	Information Security Specialist	BSc. (Hons) in Information Technology (Cyber Security), C|EH, Microsoft Certified Azure Security Engineer Associate
Janani Kehelwala	Information Security Specialist	BSc. (Hons) in Computer Security (Plymouth), C|EH

Table 1 Details of the technical team

1.4 Constituency

TechCERT‘s constituency comprises its member organizations, private sector organizations, selected governmental organizations and the general public of Sri Lanka. In accordance with the mandate of TechCERT, it provides effective incident response to malicious Cyber threats, widespread security vulnerabilities identify and respond to Cyber security incidents, conduct training and awareness to encourage best practices in information security and disseminate Cyber threat information among Sri Lankan organizations and the public.

2. Activities & Operations

2.1 Service Provided

Member of Emergency Cyber Security Coordination Center

In 2019 May SL CERT and Sri Lankan Air Force have been started this Emergency Cyber Security Coordination Center to handle every critical incident which will happen on Sri Lankan government or nation. As an information security leader in Sri Lanka, TechCERT also the member of Emergency Cyber Security Coordination Center after it has been initiated.

Managed Security Services

TechCERT Managed Security Services include a range of engineering and consultancy services listed below:

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

2.2 TechCERT Activities and Operations

The details of activities and operations conducted by TechCERT during the year 2020 are as follows:

2.2.1 Security Assessment

Activity Type	Count
External Vulnerability Assessments	2967
Web-based Security Vulnerability Assessments	997
Internal Vulnerability Assessments	2803
Firewall Rule Review and Security Assessments	185
Other Assessments (DF investigations, Wireless, Network, etc.)	402

Table 2 Number of Conducted Security Assessments

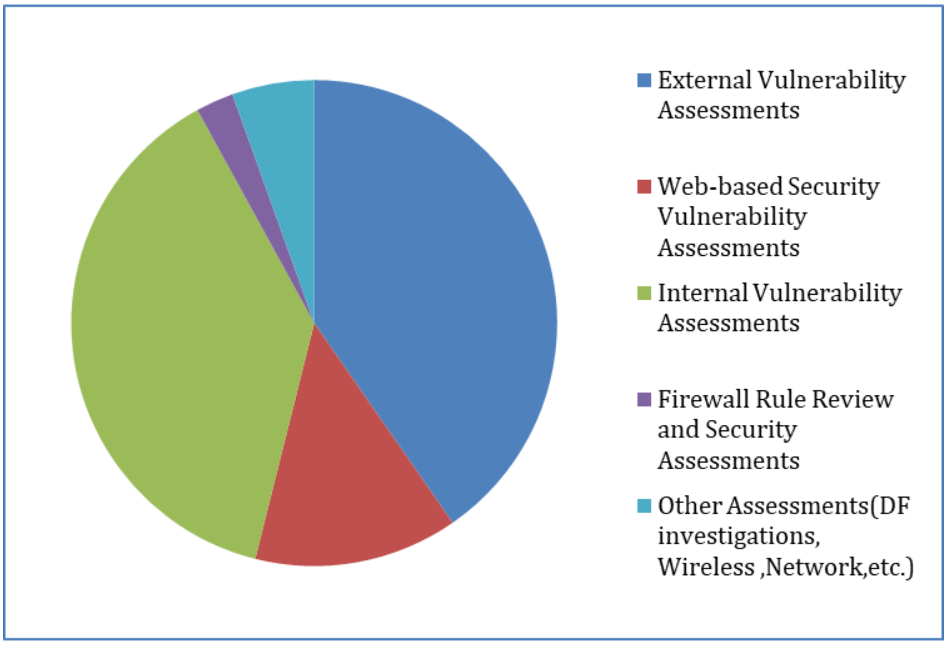


Figure 2 Number of Conducted Security Assessments

2.2.2 Incident Report

Types of Incident Response	**Count**
Social network related incident responses	145
Phishing incident responses	16
Ransomware related incidents	43
Other incident responses	117

Table 3 Number of Responded Incidents

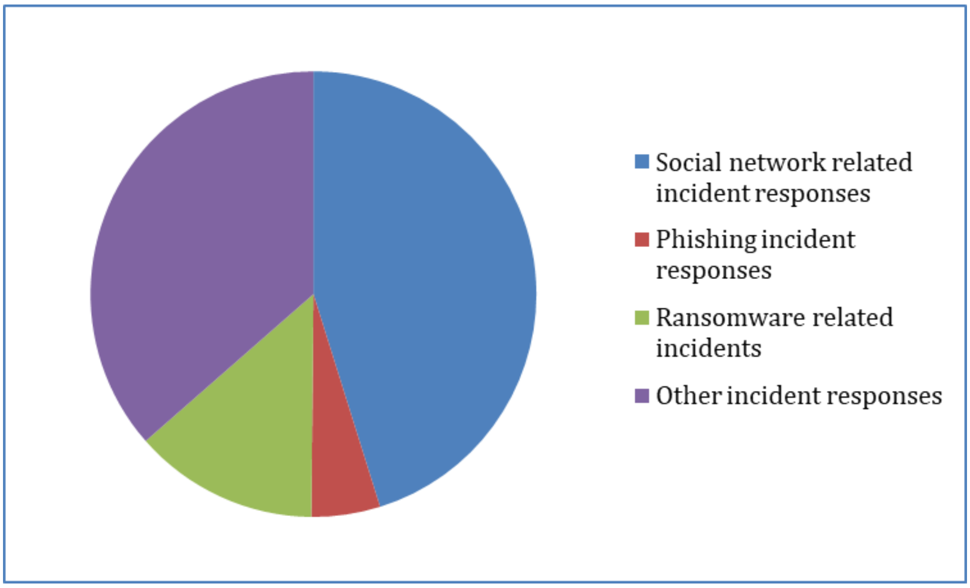


Figure 3 Number of Responded Incidents

3. Event Organized by TechCERT

3.1 Organizing Trainings, Seminars, Workshops and Demonstrations

- Dileepa Lathsara, Chief Executive Officer of TechCERT addressed in the, “Ransomware Readiness for Corporates”, on June 9th, 2020
- Kalana Guniyangoda, Principal Engineer of TechCERT conducted webinar in the, “Ransomware Readiness for Corporates”, on June 9th, 2020
- Kushan Sharma, Chief Operating Officer of TechCERT conducted workshop in the, “Live & Breathe with COVID-19”, on November 12th, 2020
- Kalana Guniyangoda, Principal Engineer of TechCERT conducted workshop in the, “Incident Response for Corporates”, on November 19th, 2020
- Sashika Suren, Principal Engineer of TechCERT conducted workshop in the, “Securing the Container Environment”, on November 26th, 2020
- Dushan Chathuranga, Senior Information Security Engineer of TechCERT

conducted workshop in the, “Securing Your Mobile Application”, on December 3rd, 2020

- TechCERT has organized a webinar on “Securing Payment Card Data from a Global to Local Perspective”, on September 22nd, 2020

3.2 Participation in Conferences, Workshops and Training Programs

- Sashika Suren, Principal Security Engineer of TechCERT participated in the, APTLD conference in Melbourne, Australia on February 20th, 2020.
- 8 engineers from TechCERT participated in the, “SonicWall: Next-Gen Firewalls & Cybersecurity Solutions” hands-on training on October 22nd, 2020.
- Kushan Sharma, Chief Operating Officer of TechCERT participated in the, AusCERT conference on September 14th – 18th, 2020

3.3 Cyber Security Drills

3rd of March 2020	**APCERT Cyber Security Drill 2020: Banker Doubles Down on Miner** TechCERT actively participated in the APCERT Drill 2020 as the leader of the Organizing Committee and a member of EXCON team.
17th September 2020	**Cyber Security Drill for Sri Lankan Banking Sector** TechCERT conducted a Cyber security drill for the Banking Sector in Sri Lanka on the Theme “New Cyber Challenges after COVID-19”.
25th November 2020	**Cyber Security Drill for Sri Lankan Finance & Insurance Organizations** TechCERT conducted a Cyber security drill for the Finance and Insurance Sector in Sri Lanka on the Theme “New Cyber Challenges after COVID-19”.
10th December 2020	**Cyber Security Drill for Sri Lankan Telcos And ISP’s** TechCERT conducted a Cyber security drill for the Telco Sector in Sri Lanka on the Theme “New Cyber Challenges after COVID-19”.

Table 4 Number of Drills

4. Future Plans

- In 2021, TechCERT will continue to focus on Information security emergency response work and strengthen the cooperation with other security organizations to contribute our strength for Internet security.
- Red Teaming and Blue Teaming exercises has to be performed on year 2021.
- Enrich and widen the Cyber Threat Intelligence Sharing with connected entities.

5. Conclusion

While the year 2020 was being a uniquely disruptive year due to Covid-19, TechCERT was able to consistently improve and expand its capability to respond and assist its constituency in information security incidents and handle emergencies in a timely and professional manner.

TechCERT successfully responded to constantly evolving cyberthreats which includes a huge increase in phishing attacks and website defacement/hacking incidents in Sri Lanka in 2020. TechCERT is confident of its ability and readiness to successfully assist its constituency in computer emergencies by providing pro-active response. According to the organizational objectives, TechCERT already planned to continue to increase its employees and develop the strength and abilities of their staff, acquire advanced training and tools, and improve its standards to provide a faster and more efficient service to the clients as well as the public through global collaboration as performing well known Sri Lankan performer in this field.

ThaiCERT

Thailand Computer Emergency Response Team – Thailand

1. Highlights of 2020

1.1 Summary of major activities

During the year 2020, ThaiCERT received reports on incidents related to the Covid-19 relief program, such as

- Fake Thai COVID-tracing android application (Thaichana)
- Fraudulent Email, impersonating the government healthcare organization, with malware as attachment
- Covid-19 related applications with a data-leak vulnerability

There were also several incidents about data breaches at major organizations and ransomware incidents at critical infrastructure such as the healthcare and energy sector. In such cases, ThaiCERT works closely with related organizations such as the National Cyber Security Committee (NCSC) or regulator to help respond to the incident.

In aspect of capacity building, ThaiCERT organized a Healthcare Cybersecurity Online Exercise 2020 (HCOX 2020) to test incident handling on various types of incidents such as ransomware. More than 30 organizations participated in the event. The event was also used as a platform for discussion on how organizations in the healthcare sector collaborate to handle and prevent cyberthreats.

2. About CSIRT

2.1 Introduction and Establishment

Founded in 2000, ThaiCERT, a non-profit government funded organization, is the Computer Security Incident Response Team (CSIRT) for Thailand, providing an official point of contact for dealing with computer security incidents in the Internet Community of Thailand. Apart from coordination and handling the reported incidents, ThaiCERT also provides an advisory service to both organizations and individuals, releasing cybersecurity alerts and news, and organizes academic trainings for the public to enhance knowledge and to raise awareness to people on information security. With the increase of security incidents in the Internet Community of Thailand, ThaiCERT expanded its service not only to the governmental units but to the private organizations as well. Currently, ThaiCERT is an operational security organization under the public organization Electronic Transactions Development Agency (ETDA), which falls under the supervision of the Ministry of Digital Economy & Society, Thailand.

2.2 Constituency

The constituents of ThaiCERT are all public, private and home sectors of Internet users in Thailand. ThaiCERT also provides the incident coordination service to other international entities, where the sources of attacks originate from Thailand.

3. Activities & Operations

3.1 Incident handling reports

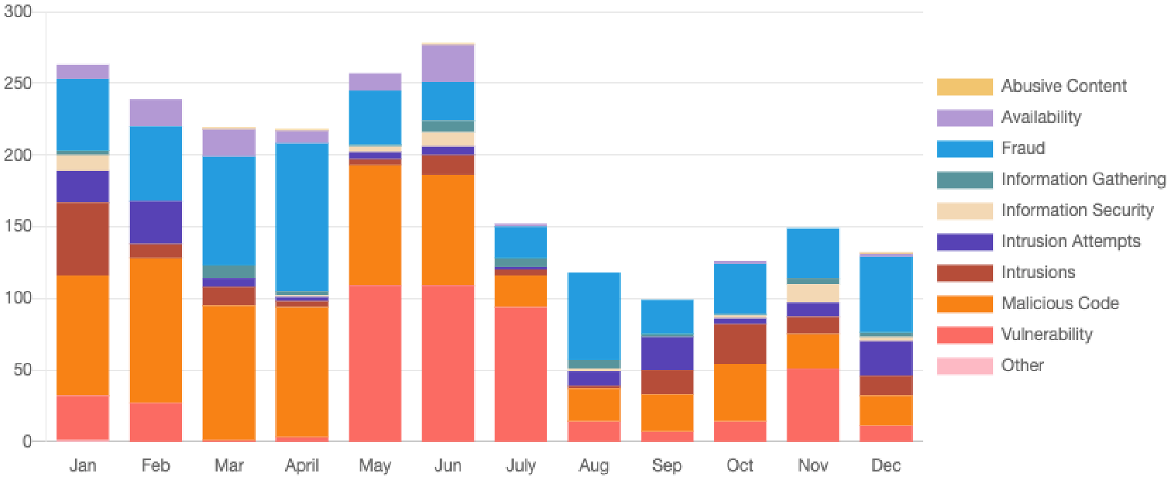


Figure 1: The number of reported incidents in 2020

Via triage, ThaiCERT handled a total of 2,250 reported incident cases (tickets) in 2020, which are 9% decrease from those of 2019 (2,470 cases). The received reports per month are around 187 cases.

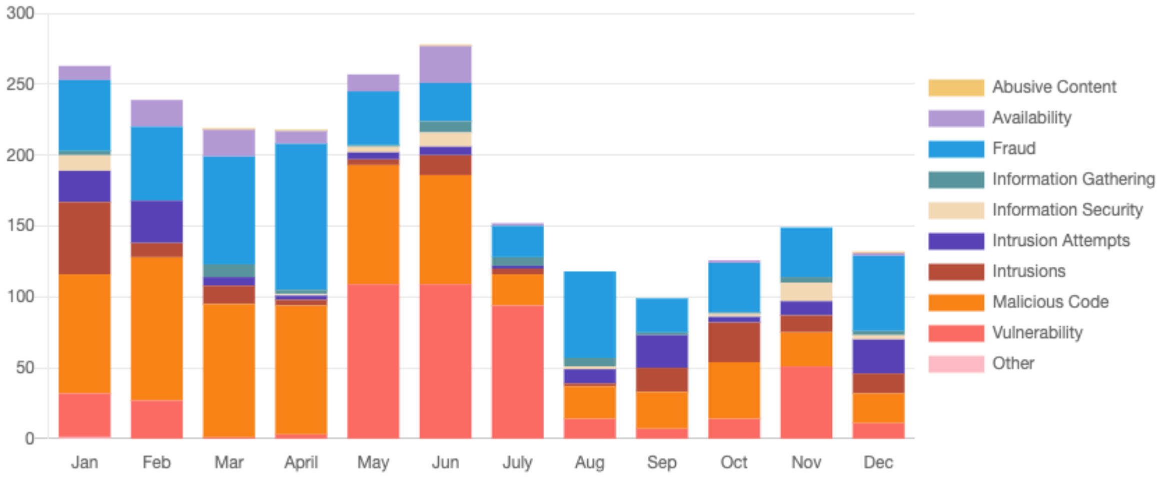


Figure 2: The proportion of reported incidents by incident type in 2020

According to the reported incidents in 2020, classified by the eCSIRT incident classification, Malicious Code dominated with 31%, where all cases were mostly botnet or hacked websites that redirect victims to other malicious website, followed by Intrusion Attempts at 26% and Information Security at 21%. All such information was handled and notified to the relevant parties through e-mail channels.

3.2 Publications

In 2020, ThaiCERT published a ransomware response guideline and self-assessment for government agencies and infographics about ransomware advices in the Thai language. For the details, please see https://www.thaicert.or.th/downloads/downloads.html
In 2020, ThaiCERT also launched the Threat Group Cards portal:
https://apt.thaicert.or.th/

4. Events organized / hosted

4.1 Training

Organized:

- AJCCBC Trainings, Feb Nov and Dec 2020

Trainer:

- 2020 APISC Security Training Course, Nov 2020

4.2 Drills, exercises

Participated:

- APCERT Drill 2020, Mar 2020
- ASEAN CERT Incident Drill (ACID) 2020, Oct 2020

Organized:

- Healthcare Cybersecurity Online eXercise 2020, Sep 2020

4.3 Conferences and seminars

Organized:

- Cyber SEA Game 2020, Dec 2020
- Healthcare

Participated:

- Annual AusCERT Information Security Conference, Sep 2020 (Virtually held event)
- APCERT AGM 2020, Sep 2020 (Virtually held event)
- Annual FIRST Conference 2020, Nov 2020 (Virtually held event)
- NatCSIRT Annual Conference, Dec 2020 (Virtually held event)
- CNCERT International Partnership in Emergency Response, Dec 2020 (Virtually held event)

5. Future Plans

- Cyber SEA Game 2021 Event
- ThaiCERT Government Monitoring System service improvement

TWCERT/CC

Taiwan Computer Emergency Response Team / Coordination Center – Chinese Taipei

1. Highlights of 2020

1.1 Summary of Major Activities

In 2020, the Taiwan Computer Emergency Response Team / Coordination Center (TWCERT/CC) shared nearly 15 million IOCs of cyber intelligence to international and domestic CERT organizations, organizations of cybersecurity, private enterprises and cybersecurity communities. By intelligence sharing, TWCERT/CC helped foster Taiwanese and the global defense capacity, strengthen the synergy of TWCERT/CC and its partners.

This year, TWCERT/CC published 12 cybersecurity information newsletters for 5,131 subscribers, 80 cybersecurity issues of software, 77 cybersecurity trends, 61 vulnerabilities news, 40 international hacked incidents intelligence, 38 social media and mobile cybersecurity sharing as well as information of 57 seminars, campaigns, and contests, to raise awareness and reveal the importance of incident reporting to public. Especially in this year when the COVID-19 is raging, TWCERT/CC builds a security Column of work from home for the mass and the enterprise in Taiwan.

As a Numbering Authority of the Common Vulnerabilities and Exposures (CVE®), we assigned 58 CVE IDs this year, and issued Taiwan Vulnerabilities Annual Report 2020. By assisting Taiwanese venders with vulnerabilities mitigation, and issuing annual report to unveil major vulnerabilities, TWCERT/CC helped enterprises and individual review and fortify cybersecurity protection, reduce the risk of and loss from information incidents. Honorably TWCERT/CC is evaluated a contributor both in CVSS and CWE items by NIST this year.

About the cybersecurity activities, TWCERT/CC joined 18 domestic and international cybersecurity conferences and seminars, an international drill, and hosted the 2020 Conference of Taiwan Cyber Security Notification and Response, Working Meetings and security training of Taiwan CERT/CSIRT Alliance and 5 cybersecurity conferences for Taiwan's small and medium enterprises. TWCERT/CC have been actively communicating and exchanging with its multilateral partners, dedicating to the prosperity of Taiwan CERT/CSIRT Alliance, and engaging in international campaigns, promoting itself to the global stage.

1.2 Achievements & Milestones

- Shared nearly 15 million incident reports separated in 11 categories; intrusion and botnet are the top two common types of attacks of cybersecurity in 2020.
- Issued 12 monthly e-newsletters, 80 cybersecurity issues of software, 77 cybersecurity trends, 61 vulnerabilities news, 40 international hacked incidents intelligence, 38 social media and mobile cybersecurity sharing as well as information of 57 seminars and campaigns.
- According to more than twelve hundred vulnerabilities collected in the Taiwan Vulnerabilities Annual Report 2020, SQL-injection, Remote code execution, and information leakage are the top three most common types of vulnerabilities in 2020.
- As a Number Authority of Common Vulnerabilities and Exposures, 58 CVE IDs were assigned in 2020.
- Participated in 7 international and assisted 11 domestic cybersecurity conferences and seminars, hosted the 2020 Conference of Taiwan Cyber Security Notification and Response and 3 regular meetings and training of Taiwan CERT/CSIRT.
- Optimized the Phishing Check system and released to public. This year we checked 1,990 files and reported phishing websites from 356 offshore and 344 domestic IPs.

2. About TWCERT/CC

2.1 Introduction

To build up a stronger and more secure cyberspace in Taiwan, the 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 partners around the world. In the year 2020, TWCERT/CC has accomplished several provisional goals and missions:

- To operate a wider international cooperation with partner cybersecurity teams, expand the source of intelligence and continue sharing.
- To issue monthly e-newsletters regarding cybersecurity, release safety tips and security advocacies.
- To vigorously participate in international and domestic conferences, seminars and campaigns, and assemble the Taiwan CERT/CSIRT alliance.
- To assist enterprises with information security incidents responding, and raise their awareness of cybersecurity.
- To provide Virus Check, CVE reporting, phishing reporting, malicious emails

reporting and information incident reporting channels.

2.2 Constituency

TWCERT/CC provides cybersecurity services to enterprises and individuals in Taiwan, including incident reporting and handling, intelligence collection and publication, consultation, and assistance.

To enhance Taiwan's cybersecurity capacity, TWCERT/CC leads the promotion of cybersecurity incident reporting, provision of cybersecurity educational resources, and cybersecurity outreaches. TWCERT/CC collaborates and integrates resources with cybersecurity organizations, academic institutions, civil communities, governmental institutions, private enterprises, and CERTs/CSIRTs all over the world. To realize the vision "develop a secure Internet environment, towards a high-quality Internet society", TWCERT/CC devotes itself to protect and promote Taiwan's cyber security with emphases on safety, convenience, and efficiency, hence to establish the national cybersecurity collaborative defense system, enhance self-protecting capacity in cyber security industry, cultivate high quality cybersecurity human resources, and strengthen the public-private partnership on cybersecurity issues.

3. Activities & Operations

3.1 Incident Handling & Cyber Intelligence Sharing

In order to against hackers' intrusions and the spread of cyber threats, TWCERT/CC receives cybersecurity incident reports from CERTs, public and private sectors, cybersecurity companies, and individual researchers beyond and behind the border.

TWCERT/CC also keeps expanding its intelligence resources and detecting more malicious or hacked domain names and IPs through collaborations with CERTs, government authorities, enterprises, ISPs, cyber security companies, researchers, and so on while playing the coordinating role among those different organizations to handle cybersecurity incidents happen in Taiwan.

After being analyzed, intelligence will be compiled and shared to international and domestic cybersecurity organizations. In 2020, TWCERT/CC shared about 15 million cyber intelligence, the monthly numbers and types of incident reports shared are shown respectively in Figure 1 and Figure 2.

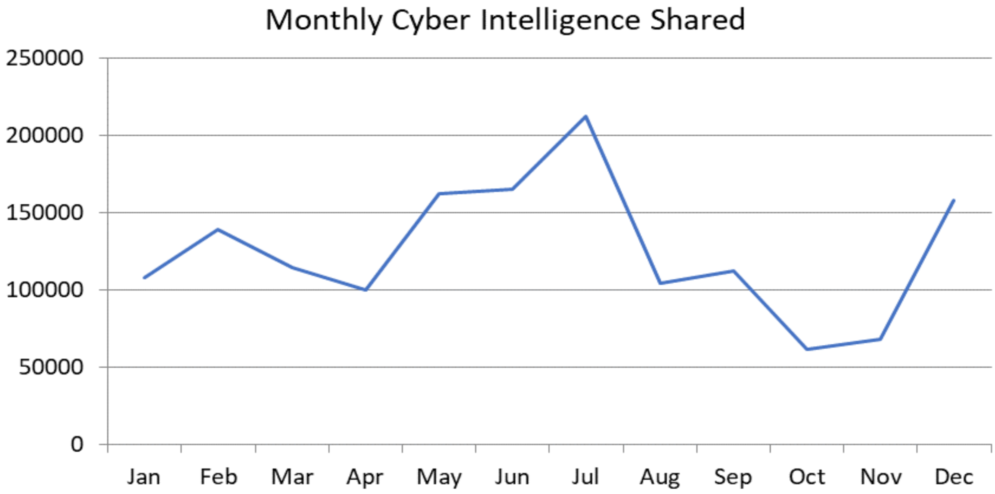


Figure1. Numbers of cyber intelligence TWCERT/CC shared in 2020

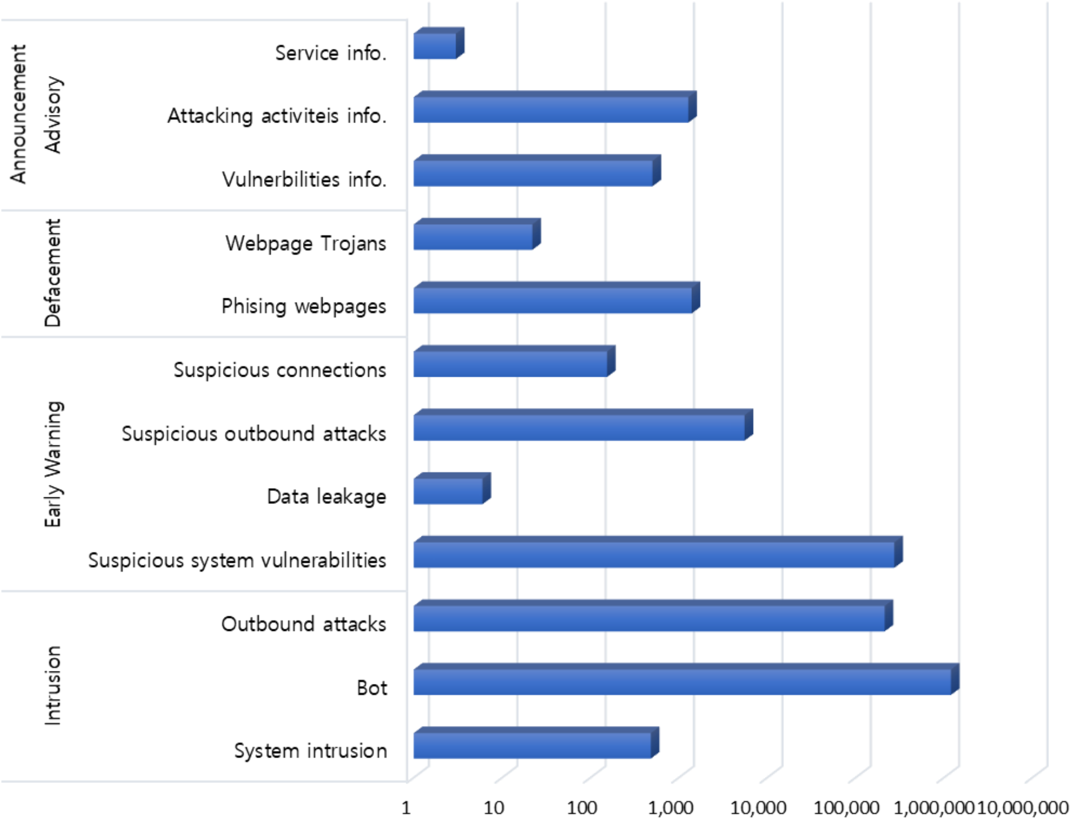


Figure2. Types of cyber intelligence TWCERT/CC shared in 2020

TWCERT/CC consistently seeks its progress on:

- Prevention: to provide advices and early warnings to avoid the occurrence of similar cybersecurity incidents.

- Reporting: to issue an immediate warning at the time a cybersecurity incident is disclosed or occurs.
- Handling: to provide the technical support and consultation needed and to coordinate the actions of a cybersecurity incident damage control and recovery.

3.2 Publications

To raise Taiwanese's cybersecurity awareness, every month TWCERT/CC releases an e-newsletter covering important cyber intelligence in the previous month through e-mail as well as TWCERT/CC's official website, Facebook fans page, and Pixnet blog. The e-newsletter contains TWCERT/CC's recent activities, cybersecurity policies, cyber threats and trends, cyberattacks, vulnerabilities, cybersecurity seminars and events, and the statistics of cybersecurity incident notification

In the year 2020, TWCERT/CC issued 12 monthly e-newsletters. Furthermore, 80 cybersecurity issues of software, 77 cybersecurity trends, 61 vulnerabilities news, 40 international hacked incidents intelligence, 38 social media and mobile cybersecurity sharing as well as information of 57 seminars., campaigns, contests referring to cybersecurity were, by TWCERT/CC, promulgated to public, which offering valuable information to those interesting in the very aspect.

3.3 News Services

- Vulnerability Announcement

In 2020, TWCERT/CC collected nearly 1,070 vulnerabilities intelligence separated in 23 categories.

1. Source Statistics of Vulnerabilities by TWCERT/CC

The source of a majority of vulnerabilities regards civil business enterprises, which the number is followed by of academic organizations and of governmental departments, shown in Figure 3.

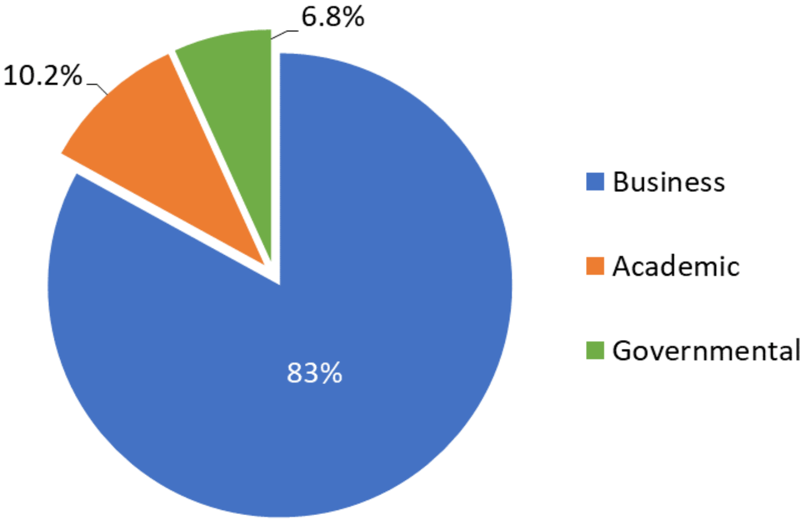


Figure 3. Source Statistics of Vulnerabilities

2. Categorization Statistics of Vulnerabilities by TWCERT/CC

Vulnerabilities categorization is shown in Figure 4. SQL Injection, Remote Code Execution, Information Leakage, Reflected Cross Site Scripting and File Download are top 5 of vulnerabilities collected.

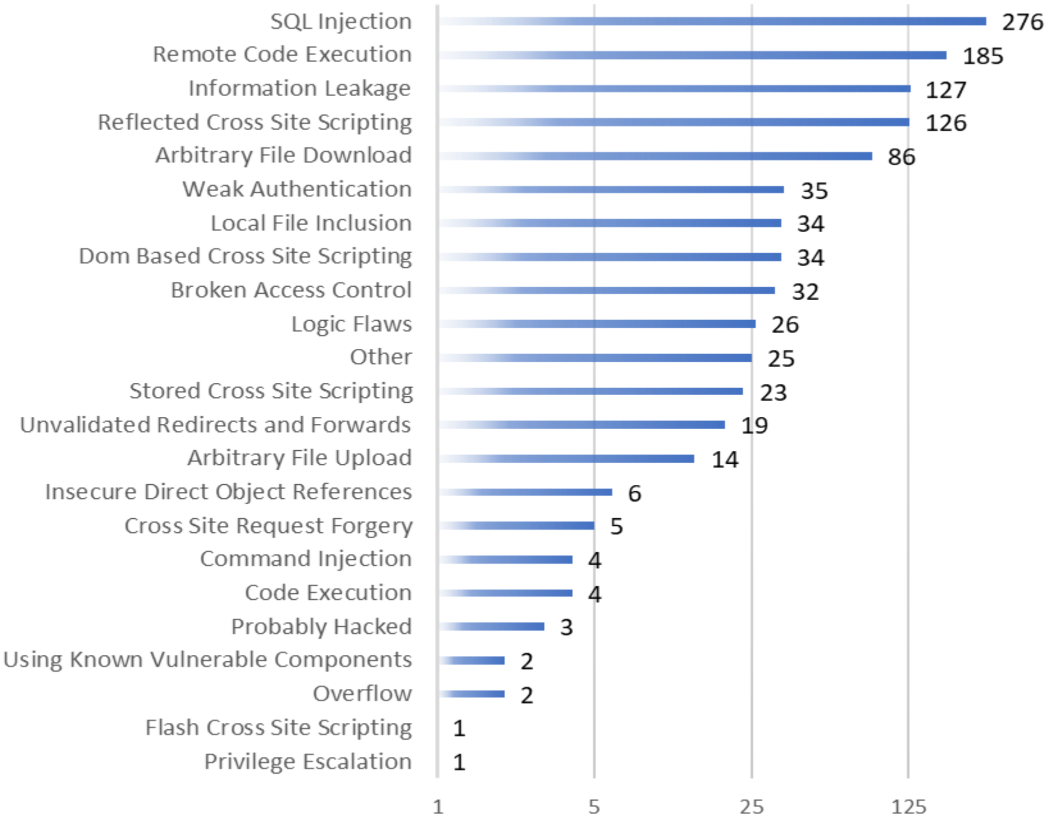


Figure 4. Categorization Statistics of Vulnerabilities

- Cyber Vulnerability Disclosure

To help enhance information security in Taiwanese ICT products, TWCERT/CC provide a publicly available email address, allows researchers beyond and behind the border to report vulnerabilities discovered, and TWCERT/CC also maintains Taiwan Vulnerability Note (TVN) to unveil vulnerabilities regarded information.

As a Numbering Authority of Common Vulnerabilities & Exposures program, TWCERT/CC reviews and assigns CVE IDs to those vulnerabilities which meets the criteria. In the year 2020, 58 vulnerabilities were assigned with CVE IDs, which includes seven, eleven, night IDs respectively from netcom products, IOT devices and software service systems, the assigned CVE IDs are shown in Table 1.

Table 1. CVE IDs assigned

Category	Amount	CVE ID
IOT devices	16	CVE-2020-3920, CVE-2020-3921, CVE-2020-3923, CVE-2020-3924, CVE-2020-3928, CVE-2020-3929, CVE-2020-3930, CVE-2020-3931 CVE-2020-3932, CVE-2020-3936, CVE-2020-10513, CVE-2020-10514 CVE-2020-12773, CVE-2020-12774, CVE-2020-24552, CVE-2020-25847
Software service systems	42	CVE-2020-3922, CVE-2020-3925, CVE-2020-3926, CVE-2020-3927 , CVE-2020-3933, CVE-2020-3934, CVE-2020-3935, CVE-2020-3937, CVE-2020-3938, CVE-2020-3939, CVE-2020-10505, CVE-2020-10506, CVE-2020-10507, CVE-202-10508, CVE-2020-10509, CVE-2020-10510, CVE-2020-10511, CVE-2020-10512, CVE-2020-12776, CVE-2020-12777, CVE-2020-12778, CVE-2020-12779, CVE-2020-12780, CVE-2020-12781, CVE-2020-12782, CVE-2020-17384,

		CVE-2020-17385, CVE-2020-17386, CVE-2020-24551, CVE-2020-25842, CVE-2020-25843, CVE-2020-25844, CVE-2020-25845, CVE-2020-25846, CVE-2020-25848, CVE-2020-25849, CVE-2020-25850, CVE-2020-35740, CVE-2020-35741, CVE-2020-35742, CVE-2020-35743, CVE-2020-35851

Apart from being a man in the middle of source reporters and manufactories, and being a consultant of venders' repairing tasks, TWCERT/CC proactively reaches and assists any organizations or parties who utilizes a known vulnerable product to imply remediation and prevent from malicious attacks.

- Virus Check

In cooperation with National Center for High-performance Computing and Trend Micro Inc., TWCERT/CC have developed a malicious file detecting system. Virus Check is a system which integrated static analysis, blocking known malwares by antivirus applications, and dynamic program analysis, detecting unknown files in a Sandbox, to offer a comprehensive testing for any anomaly. As long as any of high risk is detected, our cooperative partners Trend Micro, CyCarrier and TeamT5 will be notified and further analysis will be conducted. Once a new type of malware is confirmed, a corresponding virus pattern will be assigned to help eradicate and prevent against further aggravation and dissemination.

- Phishing Check

Optimized the Phishing Check system offer the more services to the Internet Service Provider, likes feedback web platform, phishing webpages analysis and the deal time of incident report. those function make us know more about the phishing attacks trend and urge the Internet Service Provider to remove it.

4. Events organized / co-organized / hosted

4.1 Information Security Activity

Aim to raise awareness of information security enterprises holds and their willingness to report, TWCERT/CC stays passionate about participating in domestic campaigns regarding information security, provides speeches and keynotes about working experiences of incident handling for eleven times: Cryptology and Information Security Conference 2020,Info Security 2020, InfoSec Taiwan 2020, HITCON Defense 2020, The Forum of IOT Technique and Application, The E-Commerce cybersecurity Forum 2020, TANET Conference 2020, cybersecurity forum for TSSIA(Taiwan Safety and Security Industry Association), Cyberspace Conference 2020, Taiwan Smart Agriweek 2020 and Taichung Information Technology Month 2020 propagating the key of incident reporting and responding to public.

4.2 Conferences and Seminars

TWCERT/CC has organized the annual conference, "2020 Conference of Taiwan Cyber Security Notification and Response" at NTUH International Convention Center on the 27th, October 2020. The theme of the conference was "Early Deployment of Cyber Joint-Defense and Incident Response", in correspondence to the rapid development of IoT, AI and 5G technology in the recent years. Cybersecurity experts were invited from different fields of industry, public-sector and academic fields to share their valuable knowledge and experience with the audience. Our honourable speakers include Dr. Yeali Sun, Commissioner of NCC; Hsiang Cheng Lee, CISO of SinoPac Holdings and Birdman, Co-Founder of CyCarrier Technology.

In addition, the conference also held two forums with themes: Overview of International Cyber Security, and Enterprise Product Cybersecurity for PSIRTs; facilitating dialogue between the host and audience regarding both international and domestic cyber security trends.

International cybersecurity session was hosted by Kenny Huang, CEO of TWNIC; Chang, Yu-Jen, Department of Cybersecurity from Ministry of Justice Investigation Bureau, Dannielle Andrews, Economic Section Chief of American Institute in Taiwan, Chih Kai Yang, Senior Officer of Netherlands Innovation Network from Netherlands Office Taipei, Tslil Lahav, Head of Israel Economic & Trade Mission in Taipei from Israel Economic & Trade Mission in Taipei and Stasia Tan, Deputy Director of Regional Affairs, Australian Office Taipei.

The Enterprise Product Cybersecurity for CSIRTs session was hosted by Chi Wen, Wu, Director, National Center for Cyber Security Technology as the moderator, and Edward Yu, CISO, Zyxel; Dennis Kung, CTO, QNAP and Ken Lee, Manager and Product Security Officer, Synology, as the main speakers, sharing their practical experience on product security in order to strengthen Taiwan's cyber defense and joint-defense.

427 participants attended the 2020 Conference, and 27% of them were from the industry of information services. According to a post conference survey, 99.1% of them highly evaluated the Conference, meanwhile, 99.4% of the people willing involved the next time conference. By these positive feedbacks, it could tell that the Conference has evidently enhanced the knowledge of cybersecurity held by business enterprises and attained a high prestige of TWCERT/CC to public, which helped elevate people's willingness to incident reporting, and helped dwindle organizations' loss of assets caused by information threats.

Figure 6. Representatives attended the 2020 Conference of Taiwan Cyber Security Notification and Response

In the year 2020, TWCERT/CC also hosted two regular Taiwan CERT/CSIRT meetings and one cybersecurity training, not only keynotes and incidents experiences were shared, in which members of the Taiwan CERT/CSIRT Alliance were able to have complementary intelligence exchanges and synergetic improvement in emergency responding.

5. International Collaboration

5.1 International Partnerships and Agreements

Currently, TWCERT/CC is the member of FIRST, APCERT and a Numbering Authority of the Common Vulnerabilities and Exposures (CVE®). Aside from its constant participation to the events held by international cybersecurity organizations, TWCERT/CC also collaborates with other CERTs in the world to handle cybersecurity incidents and exchange intelligence. This year, as one of the CNA members TWCERT/CC is honored to be evaluated a contributor both in CVSS and CWE items by NIST.

5.2 Other International Activities

TWCERT/CC has been vigorous in global technology communication with its international partners and following the ongoing trend of cybersecurity. This year TWCERT/CC participated in eight international conventions. TWCERT/CC will continuously interact with its global partners and keep strengthening its capacity in cybersecurity.

Table 2. international conferences and seminars TWCERT/CC participated in 2020

Date	Conference/Seminar
2020/Feb/22~28	RSA Conference 2020
2020/Mar/11	APCERT Drill
2020/Sep/9	APNIC 50 FIRST Technical Colloquia
2020/Sep/29	APCERT Conference 2020
2020/Sep /16, 23, 30 2020/Oct /7	CISA 3rd Annual National Cybersecurity Summit
2020/Oct /9	APEC Security and Prosperity Steering Group Online Conference
2020/Nov /16~18	FIRST Annual Conference 2020
2020/Dec /8~9	NatCSIRT Annual Conference 2020

6. Future Plan

In the future, TWCERT/CC will dedicate to advance its services and raise people's awareness of cybersecurity with the following promises:

1. Publish prompt vulnerability information and cybersecurity incidents, monthly cybersecurity e-newsletter, and annual report;
2. Release trends, policies, threats about cybersecurity from time to time;
3. Collect and release the latest information of conferences, seminars, and trainings relative to cybersecurity;

4. Keep noticing and assisting of cybersecurity incidents as well as improving our technical capability.

7. TWCERT/CC Contact Information

Website: https://www.twcert.org.tw/

Facebook: https://www.facebook.com/twcertcc/

Telephone: 0800-885-066 / +886-2-2528-6786

E-Mail: twcert@cert.org.tw

TWNCERT

Taiwan National Computer Emergency Response Team – Chinese Taipei

1. Highlights of 2020

1.1 Summary of major activities

TWNCERT (Taiwan National Computer Emergency Response Team) aims to support and enhance the government's ability to respond and deal with cyber security incidents. In 2020, TWNCERT issued more than two thousand notice advisories to government agencies. TWNCERT also provided consulting and training services for government agencies and critical infrastructure sectors.

In order to strengthen the preparedness against cybercrimes, technology failures as well as Critical Information Infrastructure incidents, TWNCERT conducted a national cyber security exercise, Cyber Offensive and Defensive Exercise, including social engineering exercise, information system penetration exercise, and energy-field industry control system penetration exercise.

Besides, TWNCERT launched a series of cyber security competitions in 2020 to nurture cyber security talents and promote cyber security awareness. There are more than thirty thousand students and the general public participated.

In 2020, TWNCERT participated in APCERT Drill 2020, OIC-CERT Cyber Drill 2020, and INCIBE-CERT CyberEx 2020. Through the drill and exercise, we are enhancing cybersecurity technical skills and incident response competencies. Moreover, we are strengthening the connections with international cybersecurity organizations.

1.2 Achievements & milestones

TWNCERT instructed the very first N-ISAC workshop in December for our sector ISAC members. Through the workshop, our sector ISAC members are not only learning how to process and share the cyber security information, but also building trust relationships with other sectors.

TWNCERT developed three online courses to improve cyber security protection and awareness among government agencies in 2020. There are more than twenty thousand government staff attended the online courses and took course exams.

As the convener of APCERT Training Working Group, TWNCERT convened five online training sessions. A total of twenty-three APCERT member teams had participated in these programs.

2. About TWNCERT

2.1 Introduction

As a national CERT, TWNCERT acts as the point of contact for the CSIRTs in CI sectors in Taiwan and worldwide for the nation. We aim to enhance the government and CI sectors' ability to respond and deal with cyber security incidents, as well as to conduct technical and consulting services to government agencies.

2.2 Establishment

TWNCERT was established in 2001, formed by the National Information and Communication Security Taskforce (NICST). TWNCERT is also known as the National Center for Cyber Security Technology (NCCST) domestically, led by the Department of Cyber Security of the Executive Yuan, which is in charge of cyber security policy of Taiwan. The formation of TWNCERT aims to create a government cyber response center that can help optimize the capability of continuous monitoring, task coordination, and incident response and handling in the face of cyber security threats.

2.3 Resources

TWNCERT currently has around 140 full-time employees, and the operation funding comes from the Department of Cyber Security of the Executive Yuan.

2.4 Constituency

TWNCERT dedicates to enhance the capability of incident report and response among government authorities and major CI sectors. Moreover, TWNCERT coordinates information sharing with various stakeholders such as Financial ISAC, Academic ISAC, National Communications Commission ISAC, major MSSPs, law enforcement agencies, other CSIRTs in Taiwan as well as cyber security industries in Taiwan and worldwide.

3. Activities & Operations

3.1 Scope and definitions

Our critical mission activities are

- Incident Response

Responsible for cyber security incident response in the government and CI sectors and provide effective assists and supports to related agencies to counter when under cyber-attacks or facing threat situations.

- Information Gather

National Information Sharing and Analysis Center (N-ISAC) provides a central resource for gathering information on cyber threats to critical infrastructure and providing two-way sharing of information between the private and public sector.

- Cyber Security Drill & Audit

Hold large-scale cyber offensive and defensive exercises, pairing with cyber security audits, cyber health check and penetration test services, to discover cyber security problems of the government and critical infrastructures in time.

- Education & Training

Plan cyber security series competitions and training programs to enhance cyber security education effects and raise cyber security awareness.

- Coordination and Collaboration

Build coordination and communication channels with domestic and foreign incident response organizations; Coordinate with international CSIRTs, cyber security vendors, and other cyber security related organizations.

3.2 Incident handling reports

In the year 2020, TWNCERT received nearly eight hundred reports on cyber security incidents from Taiwan government agencies. We also received about one thousand and two hundred cyber security incident reports from international CERTs/CSIRTS and cyber security organizations.

Moreover, there are more than four hundred thousand cyber security incidents and critical information were shared among N-ISAC members, including CI sector ISACs, MSSPs, LEAs, and CSIRTs in Taiwan.

3.3 Abuse statistics

- Government agencies

In 2020, TWNCERT received nearly eight hundred reports on cyber security incidents from government agencies. More than 50% of the reported security incidents are in the category of Intrusion as shown in Figure 1.

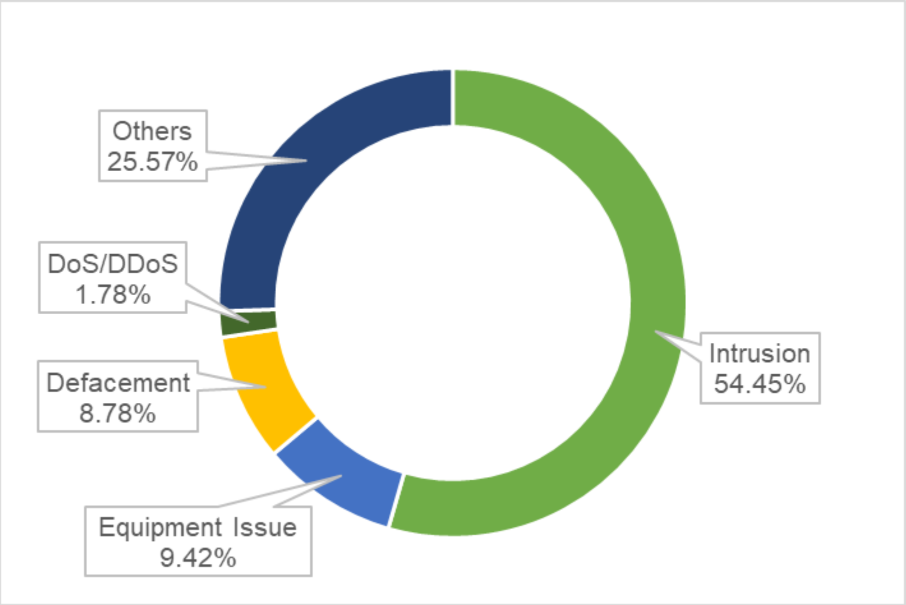


Figure 1 Security Incidents from Government Agencies

- International incident report

In 2020, TWNCERT received about one thousand and two hundred cyber security incident reports from international CERTs/CSIRTS and cyber security organizations. The incident reports were categorized as shown in Figure 2. About 53% of the incident reports were Malware infected system, followed by Attack, Spam, and Phishing.

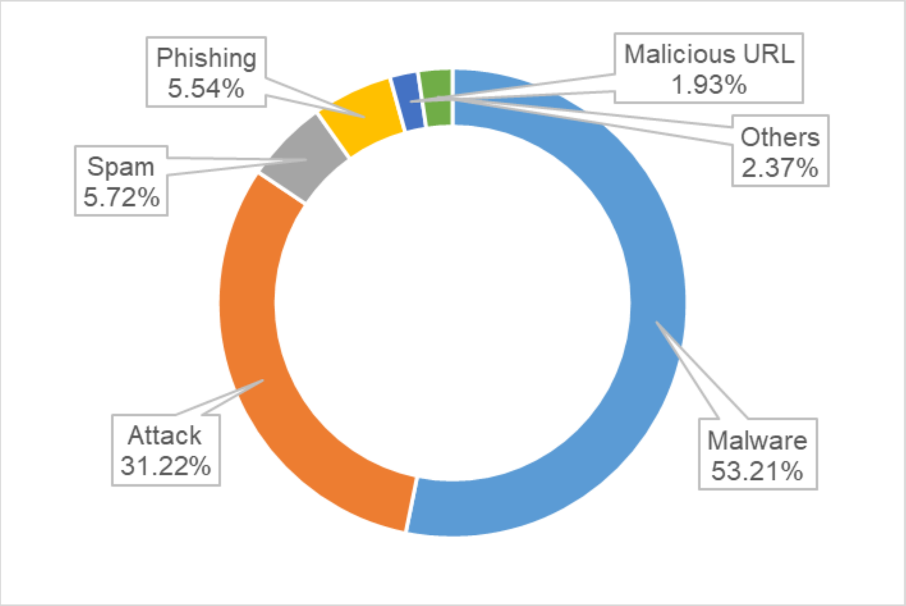


Figure 2 Category of International Incident Reports

- N-ISAC information sharing

N-ISAC members shared more than four hundred thousand cyber security incidents and critical information. The Early Warning is the most shared cyber security information in 2020, as shown in Figure 3.

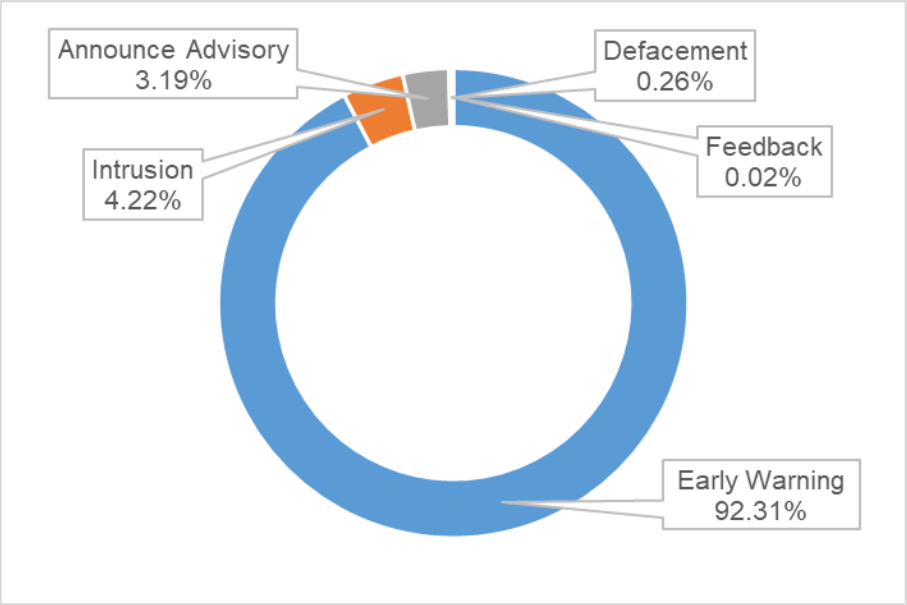


Figure 3 Distribution of N-ISAC Information Sharing

3.4 Publications

- Website publication

TWNCERT collects and publishes cyber security advisories, news, and guidelines on the website. In 2020, TWNCERT published more than ninety articles including cyber security news and security alerts on the website.

- Government agencies

In 2020, TWNCERT issued more than two thousand notice advisories to government agencies. The categories were distributed as in Figure 4.

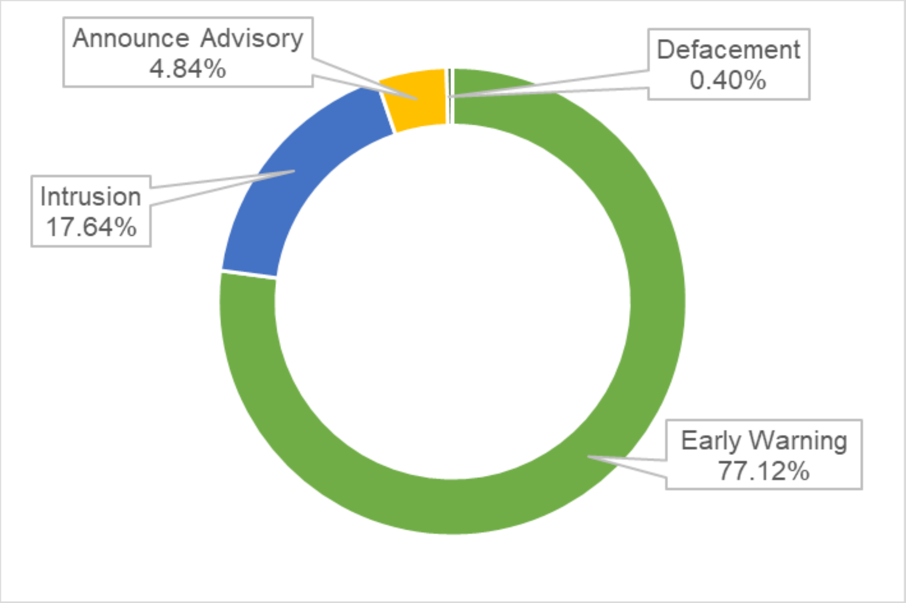


Figure 4 Distribution of Government Notice Advisories

- International incident report sharing

In 2020, TWNCERT shared more than twenty-eight thousand incident reports to fifty-five CERTs/CSIRTS, as shown in Figure 5.

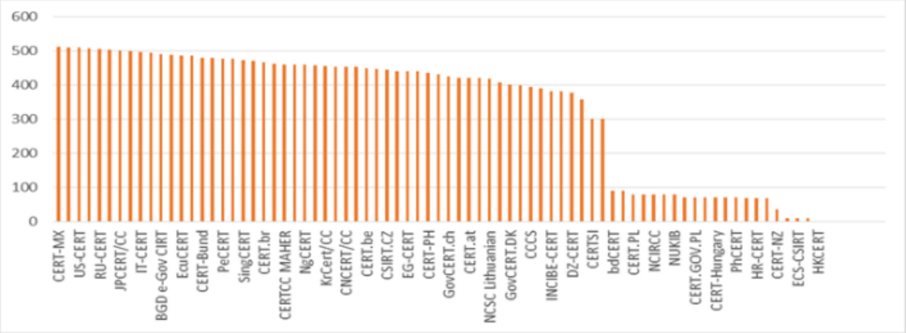


Figure 5 International Incident Report Sharing

4. Events organized/hosted

4.1 Training

TWNCERT developed three online courses to improve cyber security protection and awareness among government agencies in 2020. There are more than twenty thousand government staff attended the online courses and took course exams.

Figure 6 Producing of Cyber Security Courses

4.2 Drills & exercises

- Drill

In order to strengthen the preparedness against cybercrimes, technology failures as well as Critical Information Infrastructure (CII) incidents, TWNCERT conducted a national cyber security exercise, Cyber Offensive and Defensive Exercise (CODE). This year, the CODE included social engineering exercise, information system penetration exercise, and energy-field industry control system penetration exercise.

- Cyber security competition

To nurture cyber security talents and to promote cyber security general awareness, TWNCERT launched a series of cyber security competitions in 2020. There are more than thirty thousand students and the general public participated.

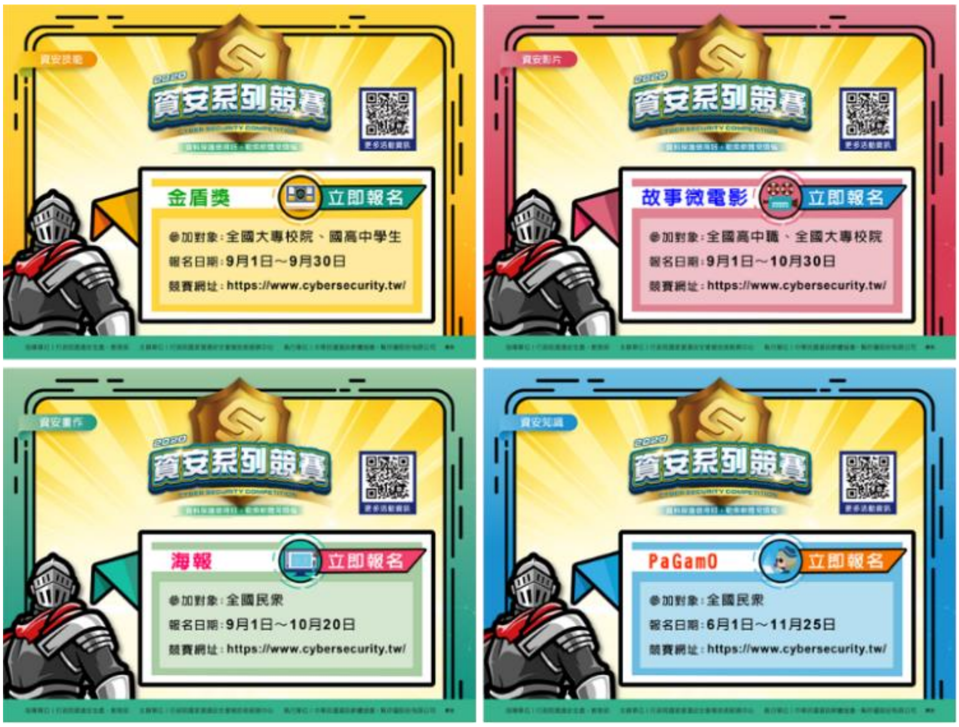


Figure 7 Cyber Security Competition

4.3 Conferences and seminars

In 2020, TWNCERT held N-ISAC meetings in June and December. Through the regular meetings, we not only discuss issues and problems, but also improve information sharing efficiency and effectiveness. During the N-ISAC annual meeting in December, the experts from public and private sectors in Taiwan were invited to share valuable insights and experiences with N-ISAC members. Moreover, we instructed the very first workshop for our sector ISAC members. The topics covered intelligence collecting, incident processing, and information sharing. Through the workshop, our sector ISAC members are not only learning how to process and share the cyber security information, but also building trust relationships with other sectors.

109年國家資安資訊分享與分析中心(N-ISAC)年會
109年國家資安資訊分享與分析中心(N-ISAC)年會

Figure 8 N-ISAC Annual Meeting

Figure 9 N-ISAC Workshop

5. International Collaboration

5.1 International partnerships and agreements

TWNCERT is the member of international organizations listed below and actively participates in member activities including meetings, working groups, annual conferences, and other cooperation.

- Asia Pacific Computer Emergency Response Team (APCERT)
- Forum for Incident Response and Security Teams (FIRST)
- APEC TEL
- Meridian

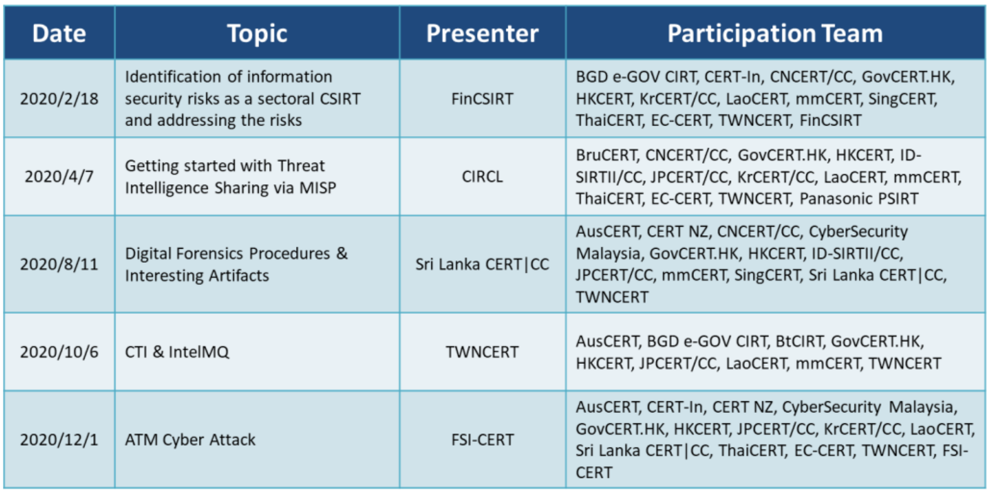
To further strengthen cooperation, TWNCERT currently has Government Security

Program Source Code Agreement with Microsoft, NDA with Fortinet, MOU with six CERTs/CSIRTs, and Team Cymru for CSIRT Assistance Program.

5.2 Capacity building

5.2.1 Training

As the convener of APCERT Training Working Group, TWNCERT coordinated member teams for online training sessions every other month. This year, TWNCERT convened five online training sessions. Year around, a total of twenty-three APCERT member teams had participated in these programs.



Date	Topic	Presenter	Participation Team
2020/2/18	Identification of information security risks as a sectoral CSIRT and addressing the risks	FinCSIRT	BGD e-GOV CIRT, CERT-In, CNCERT/CC, GovCERT.HK, HKCERT, KrCERT/CC, LaoCERT, mmCERT, SingCERT, ThaiCERT, EC-CERT, TWNCERT, FinCSIRT
2020/4/7	Getting started with Threat Intelligence Sharing via MISP	CIRCL	BruCERT, CNCERT/CC, GovCERT.HK, HKCERT, ID-SIRTII/CC, JPCERT/CC, KrCERT/CC, LaoCERT, mmCERT, ThaiCERT, EC-CERT, TWNCERT, Panasonic PSIRT
2020/8/11	Digital Forensics Procedures & Interesting Artifacts	Sri Lanka CERT|CC	AusCERT, CERT NZ, CNCERT/CC, CyberSecurity Malaysia, GovCERT.HK, HKCERT, ID-SIRTII/CC, JPCERT/CC, mmCERT, SingCERT, Sri Lanka CERT|CC, TWNCERT
2020/10/6	CTI & IntelMQ	TWNCERT	AusCERT, BGD e-GOV CIRT, BtCIRT, GovCERT.HK, HKCERT, JPCERT/CC, LaoCERT, mmCERT, TWNCERT
2020/12/1	ATM Cyber Attack	FSI-CERT	AusCERT, CERT-In, CERT NZ, CyberSecurity Malaysia, GovCERT.HK, HKCERT, JPCERT/CC, KrCERT/CC, LaoCERT, Sri Lanka CERT|CC, ThaiCERT, EC-CERT, TWNCERT, FSI-CERT

Figure 10 APCERT Training Programs

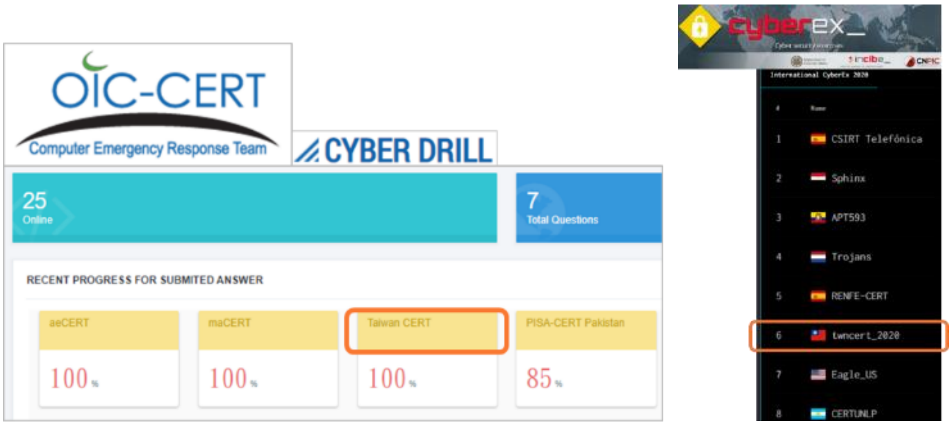
5.2.2 Drills & exercises

TWNCERT participated in APCERT Drill under the theme "Banker doubles down on Mining" on March 11th, and solved a set of drill scenarios within the given time limit.

Figure 11 APCERT Drill 2020

TWNCERT also participated in the Cyber Drill held by the Organisation of The Islamic Cooperation - Computer Emergency Response Teams (OIC-CERT) and the

International CyberEx held by the Spanish National Cybersecurity Institute - Computer Emergency Response Team (INCIBE-CERT).



25 Online

7 Total Questions

RECENT PROGRESS FOR SUBMITED ANSWER

aeCERT	maCERT	Taiwan CERT	PISA-CERT Pakistan
100%	100%	100%	85%

International CyberEx 2020

#	Name
1	CSIRT Telefónica
2	Sphinx
3	APT593
4	Trojans
5	RENFE-CERT
6	twncert_2020
7	Eagle_US
8	CERTUNLP

Figure 12 OIC-CERT Cyber Drill 2020 and INCIBE-CERT CyberEx 2020

Through the drill and exercise, we are enhancing cybersecurity technical skills and incident response competencies. Moreover, we are strengthening the connections with international cybersecurity organizations.

5.2.3 Seminars & presentations

Below is the list of international events that TWNCERT participated in 2020.

- ENISA CTI-EU 2020
- RSA2020 Conference
- APEC TEL 61 Conference (online)
- FIRST 2020 AGM (online)
- APCERT AGM 2020 (online)
- AusCERT2020 Cyber Security Conference (online)
- CERT-EU 2020 Annual Conference (online)

6. Future Plans

For the APCERT online training program, TWNCERT will continue to coordinate trainers and participants to provide bi-monthly online training, expands the coordination with other APCERT Working Groups, and participate in APCERT activities such as APCERT Drill. Possible collaboration opportunities with other international organizations will also continue to be a key emphasis to enhance the depth and broadness of the training program further.

7. Conclusion

TWNCERT will continuously enhance the collaboration with government agencies, particularly critical information infrastructure sectors, to build the public-private partnerships and collaborate with local and global CSIRTs to strengthen the cyber security awareness and incident handling capabilities. The critical elements of this strategy will be

- Enhance agency accountability and guide resource allocation
- Expand public-private partnership and introduce quality services
- Defense-in-depth deployment and toward government-wide situation awareness
- Harden IT infrastructure and reduce cyber-attack surfaces
- Check and evaluate regularly, improve through lessons learned
- Cultivate future talents to raise the bar for cyber security

Within the region, TWNCERT dedicates to contribute to the APCERT mission as well as looks forward to domestic and international cooperation opportunities, to achieve the goal of establishing a safe and secure cyberspace for the prosperity of the society.

VNCERT

Vietnam Computer Emergency Response Team – Vietnam

1. Highlights of 2020

The national and government CERT of Vietnam was named Vietnam Computer Emergency Response Team (VNCERT) and was under the Ministry of Information and Communications (MIC). Now it has been merging with the Authority of Information Security (AIS) (also under MIC) and has a new name as Vietnam Cybersecurity Emergency Response Team/Coordination Center (VNCERT/CC).

From November 2019 VNCERT/CC belongs to AIS, MIC. In 2019, VNCERT/CC continued to deploy the annual activities like drills, workshops, training and complete the responsibility of incident response coordination.

In 2020, VNCERT/CC focus on activities: deploy the anti-spam activities, assessment information security product.

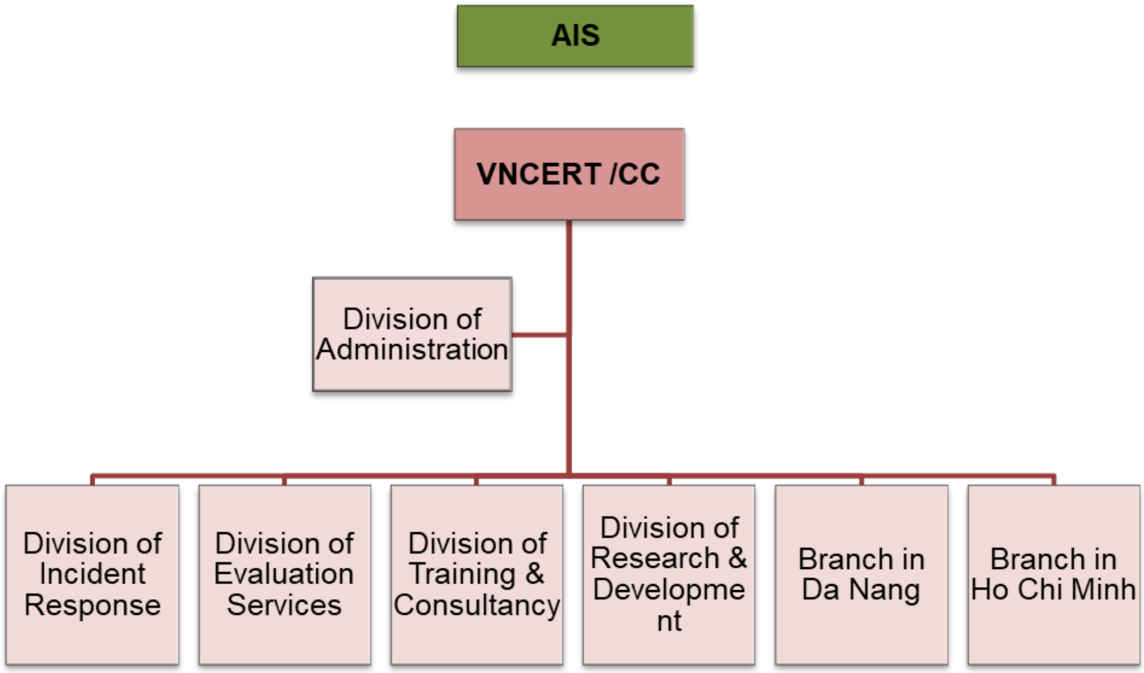
2. About VNCERT/CC

VNCERT/CC was established in 2019 by a Decision signed by the Minister of MIC. VNCERT/CC has been reorganized from VNCERT (Vietnam Computer Emergency Response Team) established in 2005 by the Prime Minister's decision.

VNCERT/CC is a center belong to AIS, which has functions as a coordinator of computer incident response activities in nationwide; timely warnings of computer network security issues; coordination of the development of standards and technical regulations on computer network safety; evaluation services; encourage the formation of CERT systems in agencies, organizations, and enterprises; being the contact point with the foreign computer rescue organizations (CERTs).

VNCERT/CC has more 60 employees at the Head Office in Hanoi, the Middle Region Branch in Danang city and the Southern Region Branch in Hochiminh city.

VNCERT/CC is the leader and the coordination center of the national CSIRTs network (VNCSIRTs Network) that consists of 216 members from departments of information technology of provinces and cities, from IT centers of ministries and central agencies. VNCERT/CC is a full member of the Forum of Incident Response and Security Teams (FIRST)


AIS
VNCERT /CC
Division of Administration
Division of Incident Response
Division of Evaluation Services
Division of Training & Consultancy
Division of Research & Developme nt
Branch in Da Nang
Branch in Ho Chi Minh

Organizational structure of VNCERT/CC

3. Activities & Operations

3.1 Scope and definitions:

VNCERT/CC has the roles of:

- Being Coordination Center of Vietnam CSIRTs (VNCSIRTs) Network with 216 members (including incident response center, information security center or information technology centers of Ministries, ministerial agencies, governmental agencies, telecommunication enterprise, Internet service providers, the Finance Organizations, Banks, the organizations in charge of information systems of national importance).
- Coordinating national computer incident response activities.
- Watching and warning computer network security problems.
- Building and coordinating to build computer network security technical standards.
- Promoting to build CERTs in the organizations, enterprises, and agencies in Vietnam.
- VNCERT/CC is the point of contact of Vietnam with the other CERTs in the world.
- Supporting the Ministry of Information and Communications of Vietnam with

activities in information security state management.

- Implementing and deploying the anti-spam activities.

3.2 Incident handling reports

Security Incidents	2020
Phishing	2025
Deface	6801
Malware	2556
Total	**11382**

Statistics of incidents by VNCERT/CC

4. Events organized / hosted

4.1 Training

VNCERT/CC had organized:

- 1 training courses on Network Security Monitoring for CuBaCERT in Hanoi
- 27 internal training courses for staffs of VNCERT/CC
- 3 training courses for technicians at provinces
- 7 training courses for members of VNCSIRTs Network.

4.2 Drill & exercises

10 other information security exercises and training courses for different government agencies.

4.3 Conference & seminars

VNCERT/CC cooperated with other organizations to organize annual events such as "Security World 2020", "National Information Security Day 2020" and organized 13 other conferences for CSIRTs Network members and information security departments from all over the country.

5. International Collaboration

5.1 International partnerships and agreements

- Completed a connection with Russia's national CERT organization and is discussing the signing of a Memorandum of Understanding.
- Built a channel connecting smoothly with 9 CERT of ASEAN countries.

5.2 Capacity building

5.2.1 Training

- Provided 01 training course for CuBaCERT
- Attended online courses of foreign organizations, International organizations such as JICA, Kaspersky, Korean companies ...

5.2.2 Drills & exercises

Attended 3 drills of APCERT 2020, ASEAN-Japan, and ACID.

5.2.3 Seminars & presentations

- Attended FIRST conference, NatCSIRT meeting, ASEAN-Japan meetings, CAMP meeting and other regional workshops in ASEAN.
- Connected students from ASEAN countries to the online contest organized by VNISA.

6. Future Plans

- Develop technical human resource of VNCERT/CC
- Continue to deploy the project of development VNCSIRTs Network according to the
- Prime Minister's Decision 05/2017/QĐ-TTg dated on 16th March 2017
- Improve the cybersecurity service quality and quantity for community
- Develop cooperation with other CERTs in the world
- Project of Children Protection on Cyberspace.
- Improve inspection and assessment of information security.
- Improve Anti-spam.

7. Conclusion

VNCERT/CC had a transition in terms of directorate and management organization. Besides the responsibility of completing all the missions and tasks assigned by AIS, MIC, and the Government, VNCERT/CC is making a plan to provide more services to local communities and develop cooperation with all the incident response teams in the world.

IV. Activity Reports from APCERT Partners

CISA

Cybersecurity and Infrastructure Security Agency - United States of America

1. About the Organization

The United States Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) serves as the national risk advisor, working with partners to defend against today's threats and collaborating to build more secure and resilient infrastructure for the future. CISA builds the national capacity to defend against cyber-attacks and works to provide cybersecurity tools, incident response services and assessment capabilities to safeguard networks that support essential operations. CISA leads efforts to protect the federal ".gov" domain of civilian government networks and collaborates with the ".com" domain of the private sector to increase the security of these critical networks through services such as capability delivery, threat hunting, operational collaboration, vulnerability management, capacity building, and cyber defense education and training. On the international front, CISA pursues collaboration with international partners to promote an open, interoperable, reliable and secure interconnected world within a global, operational and policy environment where network defenders and risk managers can collectively prevent and mitigate threats to critical infrastructure. As described in *CISA Global* – the agency's first-ever international strategy – CISA is committed to working with international counterparts and other U.S. government agencies to do four things:

1. Advance operational cooperation with international partners;
2. Build international partner capacity;
3. Strengthen collaboration with international partners through stakeholder engagement and outreach; and
4. Shape the global policy ecosystem.

For more information on *CISA Global*, see www.cisa.gov/global.

2. Activities & Operations

Incident Response: In the wake of a cyber incident involving the United States, CISA helps potentially impacted entities, analyzes the potential impact across critical infrastructure, investigates those responsible in conjunction with law enforcement partners, and coordinates the national response to significant cyber incidents. In 2020, the following highlight notable incident response activities:

- Alert (AA20-049A) Ransomware Impacting Pipeline Operations
    - CISA responded to a cyberattack affecting control and communication assets on the operational technology (OT) network of a natural gas compression facility.
- Alert (AA20-206A) Threat Actor Exploitation of F5 BIG-IP CVE-2020-5902
    - CISA has conducted incident response engagements at U.S. Government and commercial entities where malicious cyber threat actors have exploited CVE-2020-5902—an RCE vulnerability in the BIG-IP Traffic Management User Interface (TMUI)—to take control of victim systems.

CISA also works in close coordination with international partners to ensure greater unity of effort and offers technical assistance on a global scale. To sign up for CISA Alerts, go to https://us-cert.cisa.gov/ncas.

Vulnerability Management: CISA's Coordinated Vulnerability Disclosure (CVD) program coordinates the remediation and public disclosure of newly identified cybersecurity vulnerabilities in products and services with the affected vendor(s). This includes new vulnerabilities in industrial control systems (ICS), Internet of Things (IoT), and medical devices, as well as traditional information technology (IT) vulnerabilities. The goal of CISA's CVD program is to ensure that CISA, the affected vendor(s) and/or service provider(s), and the vulnerability reporter all disclose simultaneously, to ensure that users and administrators receive clear and actionable information in a timely manner. In September 2020, the Common Vulnerabilities and Exposures (CVE®) Program granted CISA authority and designated it a Top-Level Root CVE Numbering Authority for industrial control systems (ICS) and medical device vendors participating as CVE Numbering Authorities (CNA). As the Top-Level Root for ICS and medical devices, CISA is now responsible for ensuring the effective assignment of CVE IDs, implementing the CVE Program rules and guidelines, and managing the CNAs under its care.

Information Sharing: Considering the risk and potential consequences of cyber events, CISA routinely shares resources such as Emergency Directives, Malicious Activity Reports, Alerts, and other awareness products intended to help partners strengthen their cybersecurity and resilience by relaying significant details on the event and mitigation advice. CISA frequently shares resources via its Homeland Security

Information Network (HSIN) and Automated Indicator Sharing (AIS) Program.

Notable 2020 Publications:

- **COVID-19 Activity:** CISA was active in educating the population against COVID-19 scams, tracking activity against research and development entities, and participating in "Operation Warp Speed" to ensure an effective rollout of a COVID-19 vaccine. CISA created a main landing page, https://www.cisa.gov/coronavirus, for all relevant information.
    - **Alert (AA20-126A) APT Groups Target Healthcare and Essential Services** – This is a joint alert from the United States Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and the United Kingdom's National Cyber Security Centre (NCSC).
    - **CISA Insights: Cybersecurity Perspectives Healthcare and Public Health (HPH) Response to COVID-19** - This provides observations and findings derived from an analysis of HPH entities enrolled in CISA's free vulnerability scanning service from March to November 2020.
    - **TIC 3.0 Interim Telework Guidance** – Released April 8, this guidance focuses on remote federal employees connecting to private agency networks and cloud environments in a secure manner.
    - **The CISA Insights: Risk Management for Novel Coronavirus (COVID-19)** – This provides executives with a tool to help them think through physical, supply chain, and cybersecurity issues that may arise from the spread of Novel Coronavirus, or COVID-19.

- **Election Security:** CISA's multiyear elections efforts, titled "Protect 2020," were a focus in the lead up to the elections. CISA built strong relationships with state and local elections officials, worked to combat misinformation, and ensured a safe and trustworthy elections process. Elections officials released a statement that "The November 3rd election was the most secure in American history." CISA created a main landing page, https://www.cisa.gov/election-security, for all relevant information.
    - **#Protect2020 Rumor vs. Reality** – CISA released a guide to debunk common misinformation and disinformation narratives and themes that relate broadly to the security of election infrastructure and related processes.

  - **Real Fake** – This is a graphic novel that communicates the dangers and risks associated with dis- and misinformation campaigns. The plot shows how threat actors capitalize on political and social issues to plant doubt in the minds of targeted audiences and steer their opinion.
  - **Physical Security of Voting Locations and Election Facilities** – This is a general guide with resources and four actionable steps election officials should consider improving the physical security posture and enhance resilience of election operations in their jurisdiction.
  - **AA20-283A APT Actors Chaining Vulnerabilities Against SLTT, Critical Infrastructure, and Elections Organizations** – A joint advisory with the FBI on actors exploiting multiple legacy vulnerabilities in combination with a newer privilege escalation vulnerability.
  - **Alert (AA20-304A) Iranian Advanced Persistent Threat Actor Identified Obtaining Voter Registration Data** – CISA and the FBI are aware of an Iranian advanced persistent threat (APT) actor targeting U.S. state websites—to include election websites.

- **SolarWinds / Supply Chain Compromise:** In response to the reveal of a hack of SolarWinds Orion software, CISA quickly put together rich and detailed information and guidance for federal government entities, international and industry partners, and state, local, tribal, and territorial entities, which are available at https://www.cisa.gov/supply-chain-compromise.
  - **Emergency Directive (ED) 21-01 and Supplemental Guidance** – Guidance given to Federal departments and agencies on mitigating the SolarWinds Orion Code Compromise. Includes required actions for agencies to undertake.
  - **CISA Insights and Webpage on Ongoing Cybersecurity Incident** – CISA released a webpage to serve as a consolidated repository of information on this incident and related malicious cyber activity. CISA also created a "CISA Insights" report to provide executive-level information on the SolarWinds Orion compromise.
  - **CISA Releases Free Detection Tool for M365/Azure Environment** - CISA created a free tool for detecting unusual and potentially malicious activity that threatens users and applications in an Azure/Microsoft O365 environment. The tool is intended for use by incident responders and is narrowly focused on

activity that is endemic to the recent identity- and authentication-based attacks seen in multiple sectors.

  - Alert (AA20-352A) Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations – Focused on alerting the public to the threat of compromise of specific versions of SolarWinds Orion.

- **Ransomware** – CISA has a consolidated website highlighting ransomware concerns, accessible at https://www.cisa.gov/ransomware.
  - **CISA/MS-ISAC Ransomware Guide-** CISA and the Multi State Information Sharing and Analysis Center (MS-ISAC) released a Ransomware Guide to help our State, local, tribal, and territorial (SLTT) and industry partners defend against the threat of ransomware in their networks.

- **Malware Analysis Reports –** CISA released 28 Malware Analysis Reports (MARs) and 8 Malware Initial Findings Reports (MIFRs) during 2020. These reports can be found at https://us-cert.cisa.gov/ncas/analysis-reports. Some highlights include:
  - Malware targeting COVID-19 Vaccine Development
    - MAR-10296782-1.v1 – SOREFANG
    - MAR-10296782-2.v1 – WELLMESS
    - MAR-10296782-3.v1 – WELLMAIL
  - Joint MARs with Cyber National Mission Force (CNMF)
    - MAR-10310246-1.v1 – ZEBROCY Backdoor
    - MAR-10310246-2.v1 – PowerShell Script: ComRAT
    - MAR-10303705-1.v1 – Remote Access Trojan: SLOTHFULMEDIA
  - North Korean Activity
    - MAR-10295134-1.v1 - North Korean Remote Access Trojan: BLINDINGCAN
    - MAR-10301706-1.v1 - North Korean Remote Access Tool: ECCENTRICBANDWAGON
    - MAR-10301706-2.v1 - North Korean Remote Access Tool: VIVACIOUSGIFT
    - MAR-10257062-1.v2 - North Korean Remote Access Tool: FASTCASH for Windows

  - MAR-10288834-3.v1 – North Korean Trojan: PEBBLEDASH
  - MAR-10288834-2.v1 – North Korean Trojan: TAINTEDSCRIBE
  - MAR-10288834-1.v1 – North Korean Remote Access Tool: COPPERHEDGE
  - MAR-10265965-3.v1 – North Korean Trojan: CROWDEDFLOUNDER
  - MAR-10265965-1.v1 – North Korean Trojan: BISTROMATH
  - MAR-10265965-2.v1 – North Korean Trojan: SLICKSHOES
  - MAR-10271944-1.v1 – North Korean Trojan: HOTCROISSANT
  - MAR-10271944-3.v1 – North Korean Trojan: BUFFETLINE
  - MAR-10135536-8.v4 – North Korean Trojan: HOPLIGHT
  - MAR-10271944-2.v1 – North Korean Trojan: ARTFULPIE
- Iranian Activity
  - MAR-10297887-1.v1 on Iran-Based Threat Actor Exploits VPN Vulnerabilities
  - MAR-10297887-1.v2 – Iranian Web Shells

Training: Despite the COVID-19 pandemic, CISA was able to offer various virtual training offerings to our international partners. Notably, CISA began offering its Industrial Control Systems (ICS) Cybersecurity: 301 level training in a virtual format beginning in April 2020. Details about the training and a calendar of upcoming offerings can be found at https://us-cert.cisa.gov/ics/Training-Available-Through-ICS-CERT. By the end of 2020, 188 participants from 12 APCERT member countries completed this training.

3. Collaboration with APCERT Members/Partners

Bilateral CERT-to-CERT Analyst Exchanges: CISA held bilateral CERT-to-CERT Analyst Exchanges with APCERT members in 2020, reviewing such topics as vulnerability management, enhanced information sharing, ICS critical infrastructures, and the Solar Wind supply chain compromise.

Exercises: In August 2020, CISA executed Cyber Storm 2020, the seventh iteration of the national capstone cyber exercise that brings together the public and private sectors to simulate response to a cyber crisis impacting critical infrastructure. APCERT members Australia, New Zealand, Japan, and Singapore participated, exercising their information sharing and incident response coordination.

Expansion of Incident Response Engagement in the Asia Pacific: Expanded in 2020, CISA has an Interagency Agreement with the State Department focused on capacity building in the Indo-Pacific region. Under this agreement, CISA will provide cybersecurity capacity building technical assistance for eligible countries in the Indo-Pacific region through expert-to-expert workshops and seminars on a range of cybersecurity priority issues, to include hunt and incident response. CISA is also working to expand access to U.S.-based ICS training for countries in the Indo-Pacific region and encourage regional offerings as well. Additionally, CISA was officially accepted as a Pacific Cyber Security Operational Network (PaCSON) Partner in December 2020. CISA will use this partnership to augment the strong operational relationship with Australia and New Zealand, strengthen engagement with Pacific Island Countries' (PICs) cyber entities involved in incident response, and improve awareness of threat activity observed by PICs in the Indo-Pacific region.

Capacity Building Engagements with APCERT Member Countries: In October 2020, CISA participated in the U.S.-Singapore Third Country Training Programme (TCTP) intended to provide cybersecurity technical assistance for Southeast Asian participants, open to cyber policymakers and CERT/ other civilian incident response personnel. CISA provided the public sector perspective along with industry representatives to review the importance of public-private partnerships and the criticality of cyber threat information sharing. CISA also engaged with the Asia Pacific Economic Cooperation (APEC) in October 2020 through the Telecommunications and Information Working Group to provide a well-received presentation on U.S. Cyber Security Awareness Activity and participated in a Policy Roundtable in December 2020 to promote better alignment of approaches to address cybersecurity challenges stemming from increased reliance on digital technologies during the COVID-19 pandemic.

FSI-CERT

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

1. About FSI-CERT

1.1 Introduction

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

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

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

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

1.2 Establishment

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

1.3 Resources

As of Dec. 2020, around 200 employees from 7 divisions and 3 centers, work for FSI.

1.4 Constituency

FSI-CERT is in charge of cyber threat detection, cyber attack response, and vulnerability analysis for digital financial infrastructure to keep the Korean financial industry safe from cyber threats.

1.5 Contact Information

Tel: +82-2-3495-9431

Fax: +82-2-3495-9399

Email: cert@fsec.or.kr

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

2. Activities & Operations

2.1 Summary of major activities

2.1.1 Ransom DDoS Attack defense targeting the Financial Sector

Since August 2020, ransom DDoS attacks have continuously occurred targeting Korea's financial sector. The capacity and frequency of DDoS attacks have increased due to the proliferation of cloud-based services and IoT devices. In response, FSI-CERT successfully defended ransom DDoS attacks targeting Korea's financial sector by establishing a large-scale DDoS attack response system linked to cloud DDoS Cyber shelters.

2.1.2 Covid-19 Cyber Threat Trend in Financial Sector

FSI-CERT published a report on cyber threat trends on social engineering attacks targeting financial companies related to Covid-19. In particular, FSI-CERT conducted detailed analysis on major types and patterns of malicious e-mail, attacker's IP addresses, and domains that are used in social engineering crimes.

2.1.3 Cloud Digital Forensic Research

With the recent increase of shift to cloud computing in Korea's financial sector, FSI-CERT conducted a digital forensic research of the environment of major domestic and global cloud service providers*.

* AWS, Microsoft Azure, GCP, KT Cloud, Naver Cloud Platform, NHN Toast

2.1.4 Credit card information shared on the Dark Web

FSI-CERT quickly collected and analyzed information of 1 million credit card records on the Dark Web. FSI-CERT contributed to preventing financial accidents through cooperating with related organizations.

2.1.5 AI-based malware analysis system

FSI-CERT set up an AI-based malware analysis system to preemptively and actively respond to intelligent malware. It is possible to systematically respond to unknown and variant malicious codes by collecting large amounts of malware and correlation analysis.

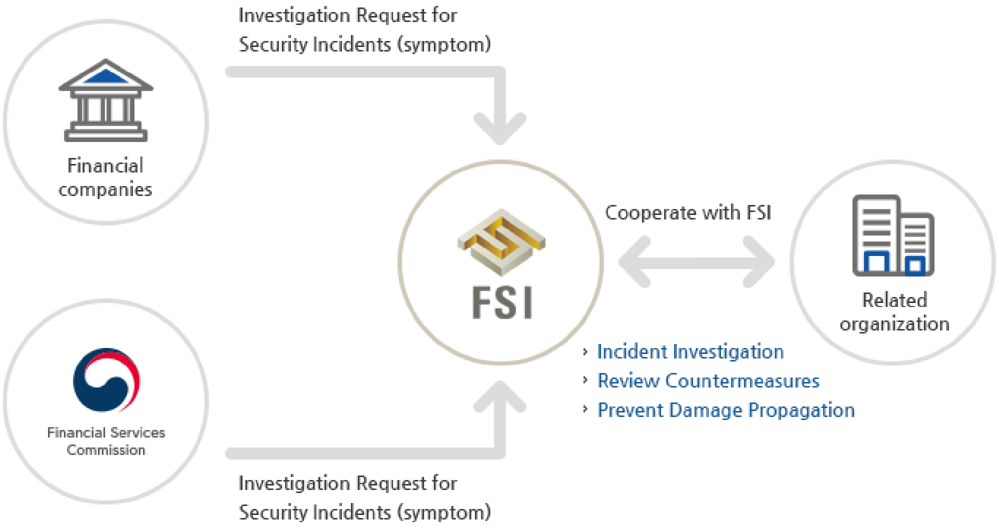
2.1.6 Phishing Detection

In 2020, the upgraded FSI-CERT's phishing site detection system has detected and shared 37,000 voice phishing applications distributed on malicious sites. Through strengthening cooperation between finance, telecommunications, security, and public industries, FSI-CERT has newly built a voice phishing fraud information sharing system to share information such as smishing text, malicious apps, and phone numbers used for voice phishing scams. FSI-CERT has proactively blocked new types of phishing scams utilizing this system.

2.2 Incident Response

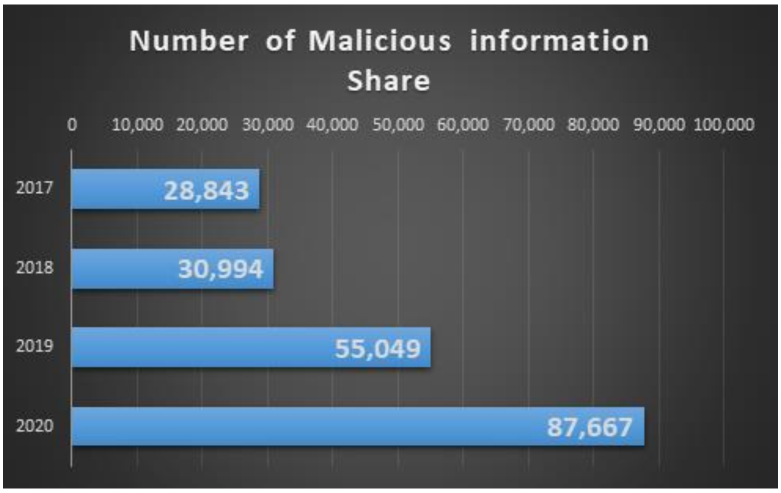
2.2.1 Incident analysis and response

When cyber intrusions occur in financial companies, FSI-CERT gets on the scene immediately to gather digital evidence and analyze the cause of the accident through digital-forensics. FSI-CERT also establishes measures to prevent damage propagation and enhance cyber threat response capabilities of related financial companies by conducting incident prevention digital forensic analysis on PCs that are likely to be targeted.


Investigation Request for Security Incidents (symptom)
Financial companies
FSI
Cooperate with FSI
Related organization
Incident Investigation
Review Countermeasures
Prevent Damage Propagation
Financial Services Commission
Investigation Request for Security Incidents (symptom)

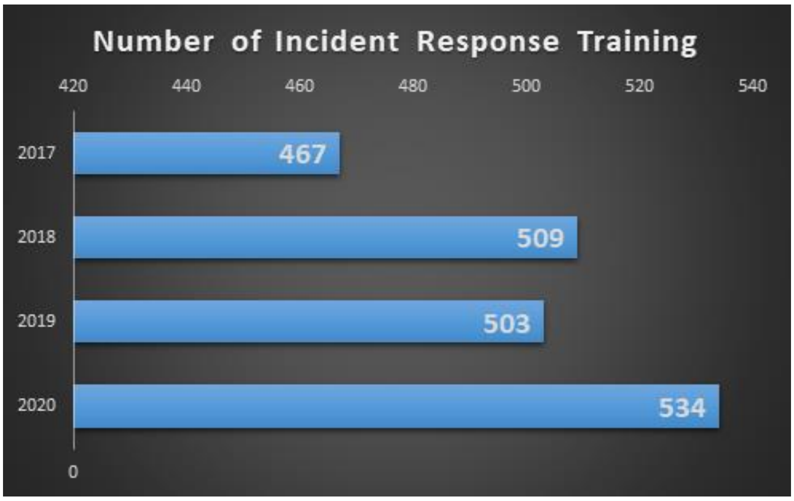
2.2.2 Collection, analysis, and response to malicious code information

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



2.2.3 Cyber Security Incident Simulation Training

FSI-CERT performs cyber security incident simulation training for financial companies. The training simulates the conditions of real cyber attacks. During the training, the testers from FSI-CERT attack the servers and web pages in operation, using attack techniques that real-world hackers commonly exploit. FSI-CERT serves 'blind training' if finance companies want to do incident simulation training without prior notice. Through the training, FSI-CERT has contributed to improving the security awareness and response capabilities of the financial sector against real cyber-attacks and intrusion.



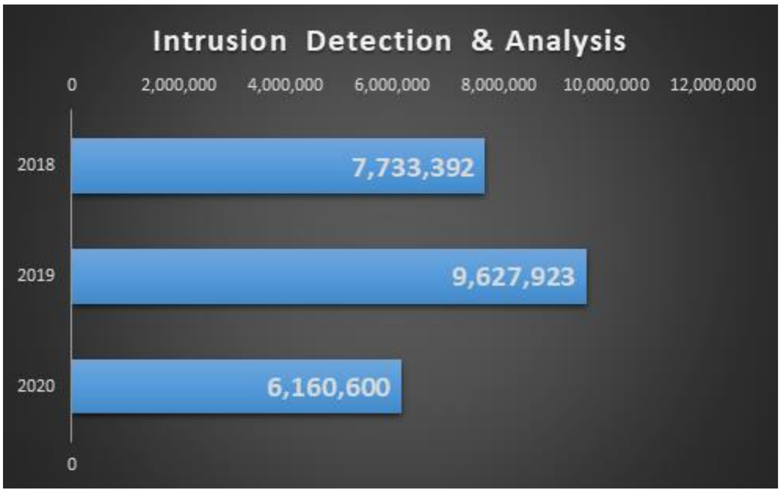
2.2.4 Operation of DDOS Attack Emergency Response Center

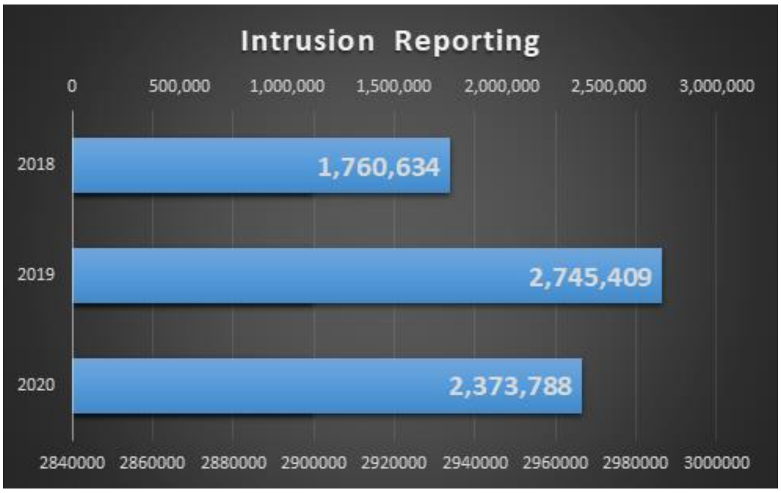
In the event of large-scale DDoS Attacks that cannot respond to financial companies, FSI-CERT supports them by filtering DDoS attacks and sending back valid network traffic to the financial companies.

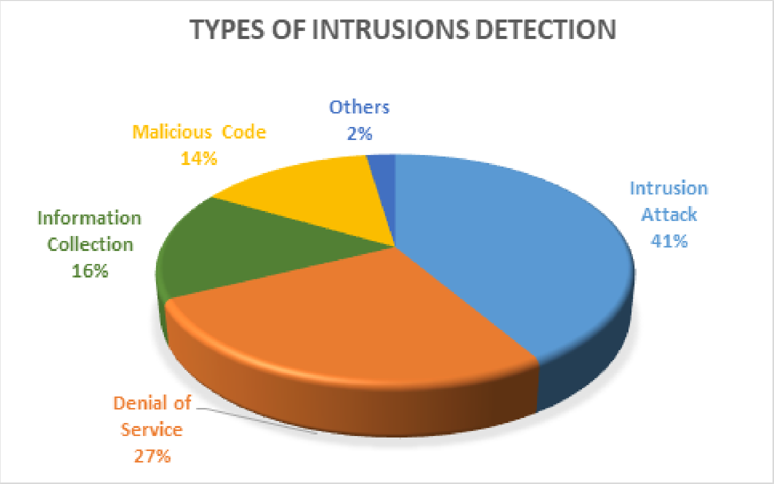
In 2020, FSI-CERT established a system that can defend DDoS attacks by connecting with cloud-based DDoS cyber shelters. The cloud-based DDoS cyber shelters block large-scale bandwidth attacks in advance. Then FSI-CERT's DDoS attack emergency response center blocks application-layer attacks on critical services.

2.2.5 Integrated Security Monitoring

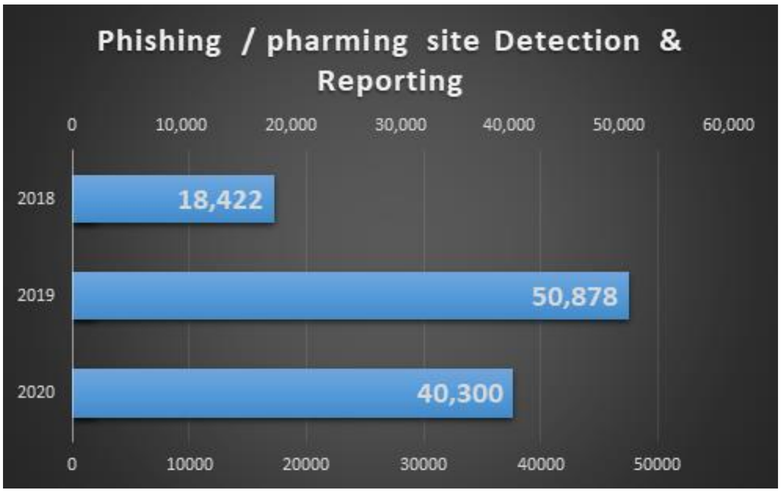
FSI-CERT operates a Financial sector Information Sharing and Analysis Center (ISAC) and uses AI and big data-based security monitoring system to detect cyber threats against the entire financial industry 24/7. In 2020, FSI-CERT has quickly and successfully responded to ransom DDoS attacks targeting Korean financial companies.


Intrusion Detection & Analysis
0
2,000,000
4,000,000
6,000,000
8,000,000
10,000,000
12,000,000
2018
7,733,392
2019
9,627,923
2020
6,160,600
0


Intrusion Reporting
0
500,000
1,000,000
1,500,000
2,000,000
2,500,000
3,000,000
2018
1,760,634
2019
2,745,409
2020
2,373,788
2840000
2860000
2880000
2900000
2920000
2940000
2960000
2980000
3000000


TYPES OF INTRUSIONS DETECTION
Others 2%
Malicious Code 14%
Information Collection 16%
Intrusion Attack 41%
Denial of Service 27%

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



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.

ARR-V-2020-@-198

Present and Future of
Financial Mobile Malware

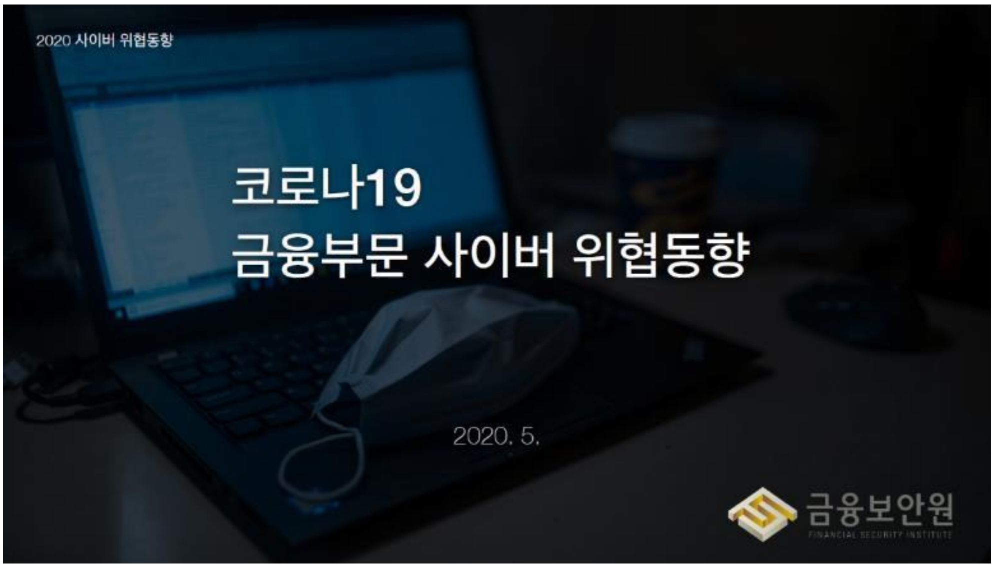
2020 Cyber Threat Intelligence Report

FINANCIAL
SECURITY
INSTITUTE

- Present and Future of Financial Mobile Malware

This report identified critical threats to malicious mobile apps and suggested countermeasures for these threats. FSI-CERT has collected about 100 samples of representative android mobile banking malicious apps that have been discovered from all around the world such as Anubis, BlackRock, Cerberus, EventBot, KRBankBot, MysteryBot, RoamingMantis, Zitmo. In this report, FSI-CERT identified overall distribution types, basic structures, execution flow, and critical malicious features of mobile financial malware through dynamic and static analysis.

Download: http://www.fsec.or.kr/common/proc/fsec/bbs/163/fileDownLoad/2812.do



- Covid-19 cyber threat trends in the financial sector

This report focused on cyber threat trends related to Covid-19 between February and April 2020 in Korea. The report was created by tracking malwares of major APT threat groups and analyzing around 6.8 million e-mails.

Download: http://www.fsec.or.kr/common/proc/fsec/bbs/163/fileDownLoad/2500.do

4. Events Organized / Hosted

- Bug bounty program for the financial sector
- Seminar on Information Security Day for CEOs of financial companies
- Financial Security Camp 2020 for College Student
- FIESTA 2020 (Financial Institutes' Event on Security Threat Analysis)
- FISCON 2020 (Financial Information Security Conference)

- Financial ISAC Research Exchange Meeting (Financial ISAC JAPAN)
- Financial Sector Threat Identification Working Group Meeting
- Malware Working-level Meeting
- "Fintech & Financial Security" Field Meeting

5. Conferences and Presentation

In 2020, FSI-CERT dispatched speakers to the following international events:

- Virus Bulletin 2020, hosted VB(Online, Sep)
- APCERT online Training (Online, Dec)

6. Future Plans

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

7. Conclusion

Due to COVID-19, the transition to contactless environments is accelerating, and these changes will result in financial companies becoming exposed to cyber threats. FSI-CERT has continuously reinforced cyber attacks response systems to respond to increasing cyber threats. FSI-CERT will faithfully fulfill its role and function for the safe development of the financial industry in the future.

OIC-CERT

Organisation of The Islamic Cooperation – Computer Emergency Response Teams

1. ABOUT ORGANIZATION OF THE ISLAMIC COOPERATION – COMPUTER EMERGENCY RESPONSE TEAM (OIC-CERT)

1.1 Introduction

The Organization 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 2020, the OIC-CERT has a network and strategic collaboration with 51 members from 27 OIC countries. This alliance is further supported through the presence of 4 Commercial Members, 5 Professional Members, 1 Fellow Member, 1 Affiliate Member, and 1 Honorary Member.

The membership categories are as follows:

1.2.1 Full Members

These are CERTs, Computer Security Incident Response Teams (CSIRTs) or similar entities that are located and/or having the primary function within the jurisdiction of the OIC-CERT member countries that is wholly or partly owned by the government with the authority to represent the country's interest.

1.2.2 General Members

These are other related government organizations, non- governmental organizations or academia that deals with cybersecurity matters. However, these parties do not have the authority to represent the country's interest.

1.2.3 Affiliate Members

These are not-for-profit organizations that deals with cybersecurity matters from non OIC-CERT member countries.

1.2.4 Commercial Members

These are industrial or business organizations that deals with cybersecurity matters from the OIC and non-OIC member countries.

1.2.5 Professional Members

Individual professionals mainly in cybersecurity not restricted to the OIC community.

1.2.6 Fellow Members

These are individual who are considered as co-founders of the OIC-CERT and have actively represent their organization as an OIC-CERT member for a minimum period of 5 years.

1.2.7 Honorary Members

Individuals or organizations who has demonstrated extraordinary contribution, support, and exemplary leadership to the OIC-CERT.

Details of the members can be found at www.oic-cert.org

2. ACTIVITIES & OPERATIONS

2.1 OIC-CERT 12th Annual Conference 2020 (Virtual)

Due to pandemic COVID-19 issue, this annual event was conducted virtually via YouTube Live from 23 to 25 Nov 2020. Malaysia as the OIC-CERT Permanent Secretariat took the initiative to host the 2020 event. Ms. Yukako Uchida represented the APCERT as a speaker at the event. Twelfth (12) papers were presented, and viewed by 522 viewers on 23 Nov, 643 viewers and 1164 views respectively on 24 and 25 Nov.

2.2 Online Trainings

To raise awareness on cybersecurity within OIC-CERT member states, a series of online trainings were conducted in 2020 as follows:

Date	Topic	Host
29 Apr 2020	Remote Working Security	UAE
18 May 2020	Social Engineering	UAE
4 Jun 2020	Malware	UAE
14 Jul 2020	Managing Technical Journal Online 4th Industrial Revolution	Malaysia
21 Sep 2020	Mobile Security	UAE
21 Oct 2020	Computer Security	UAE
27 Oct 2020	Responding to Data Breach: Challenges and Strategies	Indonesia
18 Nov 2020	Social Media Security	UAE
14 Dec 2020	Email Security	UAE

3. EVENTS INVOLVEMENT AND ACHIEVEMENTS

The OIC-CERT actively participated in cybersecurity events such as trainings, seminars, conferences, and meetings. The agency has contributed its competencies in the following events.

3.1 Cyber Drills

As in the previous years, the OIC-CERT organizes an international cyber drill for the members and partners. In 2020, Oman collaborated with Malaysia in organising the drill with the theme “Remote Working and Cyber Threats” on 22 Sep 2020. The objective of this drill is to measure the readiness of the participants in facing cyber attacks specifically on remote working and cyber threats during the COVID-19 pandemic. The drill received participations from 16 OIC-CERT members, 5 APCERT members and 2 AfricaCERT members. The APCERT members who participated in the drill were CERT-In, TWNCERT, HKCERT, Sri Lanka CERT/CC, and VNCERT/CC.
In return, OIC-CERT members from Egypt, Jordan, Morocco, Nigeria, Pakistan, and Tunisia participated in the APCERT Drill that was held on 11 Mar 2020.

3.2 OIC-CERT Journal of Cyber Security

The growth in cybersecurity research has encouraged the collaboration between the academia and industry practitioners. The OIC has a substantial pool of resources and expertise both from the academia and industry practitioners that can produce quality research papers in the field of cybersecurity and can be published as a journal contributing to the body of knowledge in cybersecurity. The OIC-CERT Journal of Cyber Security (JCS) is an initiative under the OIC-CERT led by CyberSecurity Malaysia and the Technical University of Malaysia Melaka, Malaysia.

In 2020, the OIC-CERT has published Volume 2, Issue 1 in Feb 2020. The journal contained 8 papers. The OIC-CERT welcomed contribution from APCERT members for this journal. More details at https://www.oic-cert.org/en/call-for-paper.html

3.3 Cyber Security Guidelines

The OIC-CERT has published several cyber security guidelines in 2020. The guidelines are as follows:

i. Guidelines for Securing Cloud Implementation by Cloud Service Subscriber

ii. Guidelines for Secure Industrial Control System (ICS)

iii. Guidelines for Secure Software Development Life Cycle (SSDLC)

iv. Guidelines for Secure Internet of Things (IoT)

v. Guidelines for Secure Industry 4.0

vi. Guideline for Establishing A National Cyber Security Ambassador Program for Children

vii. National Guideline for Building an Organizational Information Security Awareness Program

3.4 Awareness

A set of cybersecurity awareness materials has been developed for OIC-CERT member covering 6 topics, which are social engineering, malware, mobile security, computer security, social media security and email security.

The materials included awareness presentations, tips for social media as well as posters.

4. Collaboration with APCERT members/partners

4.1 Memorandum of Understanding (MoU)

- MoUs with FIRST
- MOU with AfricaCERT

4.2 OIC-CERT Malware Research and Coordination Facility

The Malware Research and Coordination Facility Project (Project) is facilitated by CyberSecurity Malaysia, which is the Permanent Secretariat of the OIC-CERT and the Convenor of the APCERT Malware Mitigation Working Group.

Analysis from the data provides early detection of malware, assist to provide awareness to the public, and for the cybersecurity personnel to act accordingly based on the shared information.

The Project uses LebahNET as the data sources for research as the captured botnet activities are from the worldwide source and Kibana as the data analysis tool for the user to visualise the data from the LebahNET data.

To date, about 15 organisations are participating in this project and 7 are APCERT members.

Disclaimer on Publications

The contents of the Activity Report on Chapter III and IV are written by each APCERT members and partners based on their individual analysis. Responsibility for the information and views expressed in each report lies entirely with the authors.

TLP: WHITE

APCERT ANNUAL REPORT

2020

APCERT
Asia Pacific Computer Emergency Response Team