APCERT
Asia Pacific Computer Emergency Response Team

TLP: WHITE

APCERT ANNUAL REPORT 2019

TLP: WHITE

APCERT Annual Report 2019

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

CONTENTS

Chair's Message 2019

The advancement in digital information has kept information security professionals on their toes since the introduction of computer networks. Nowadays, it is a rare phenomenon to see stand-alone computers that are isolated from the rest of the world. The digital information networks are so seamless today that access to information is always available through personal highly mobile devices that we now take such availability for granted. It does not stop here as emerging technologies such as the Internet of Things, Artificial Intelligence and the Industrial Revolution 4 will totally disrupt how we managed information and our present way of life.

International relation is a must in mitigating cyber security. In any national cyber security strategies, policies or guidelines, establishing cross border collaboration is identified as one of the major areas of concerned, simply because the cyber domain does not conform to the physical boundary of a nation. Therefore, international and regional platforms such as APCERT, which is a collaborative efforts of Computer Emergency Response Team (CERTs) in information sharing and incident handling, is vital.

It has been 17 years since APCERT formation in 2003. We started with 15 CERT teams from 12 Asia Pacific economies which have now grown to 30 teams from 21 economies. Last year alone we welcomed 3 new members: one (1) corporate partner and two (2) as liaison partners. Meanwhile, we hope to attract more new members in the years to come, especially from the industry, as this will increase our reach in global cooperation which will realize our vision to help create a safe, clean and reliable cyber space for the Asia Pacific Region through global cooperation.

In improving the efficiency of the APCERT, the Operational Framework has been updated and the Information Sharing Working Group has finalized the Information Sharing and Handling Policy. This is one of the continuous efforts in improving our current policies and processes to maintain our relevancy in keeping the cyber space 'cleaned'.

This would be the 3rd time CyberSecurity Malaysia is at the helm as the APCERT Chair and it is becoming more and more challenging. For one, the previous Chair, the Australia

Cyber Security Centre, has set the leadership bar high for us to maintain. However, we believe with the support of all the members especially the Steering Committee and the Working Group Conveners, APCERT will thrive in mitigating cyber threats and cyber security.

In addition to the parties mentioned above, we would also like to express our gratitude to SingCERT for hosting the 2019 APCERT Annual General Meeting and Conference in September 2019, and for next year, Sri Lanka CERT|CC has agreed to host the 2020 event in Colombo, Sri Lanka. Our expression of thanks will not be complete if we do not extend one to JPCERT/CC, the Secretariat who act as the cohesive force keeping us all together as a team.

With the rise of the digital domain, we can anticipate disruptive technologies which will shape our future working and communication environment. APCERT will maintain a trusted contact network of computer security experts to improve the region's awareness and competency in relation to computer security incidents and towards creating a safe, clean and reliable cyber space in the Asia Pacific Region through global collaboration.

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%20Operational%20Framework%20-%20Oct%202018.pdf

As of December 2019, APCERT consists of 30 Operational Members from 21 economies across the Asia Pacific region, 2 Liaison Partners, and 4 Corporate Partners.

Operational Members (30 Teams / 21 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
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
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 (2 Teams) *formerly referred to as Supporting Members

Team	Official Team Name	Economy
FINCSIRT	Financial Sector Computer Security Incident Response Team	Sri Lanka
FSI-CERT	Financial Security Institute – Computer Emergency Response Team	Republic of Korea

Corporate Partners (4 Teams) *formerly referred to as Supporting Members

- Bkav Corporation
- Microsoft Corporation
- SecureWorks
- Panasonic PSIRT

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

At the APCERT AGM 2019, 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	2018 - 2020	
CNCERT/CC	2018 - 2020	Deputy Chair
CyberSecurity Malaysia	2019 - 2021	Chair
JPCERT/CC	2019 - 2021	Secretariat
KrCERT/CC	2018 - 2020	
Sri Lanka CERT|CC*	2019 - 2021	
TWNCERT	2018 - 2020	

*Newly elected at AGM 2019

3. Working Groups (WG)

There are currently nine (9) 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; and
  - 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, MNCERT/CC, MOCERT, NCA-CERT, Sri Lanka CERT|CC, TechCERT, ThaiCERT, TWCERT/CC, TWNCERT

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; and
  - 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; and
  - Promote harmony and cooperation among APCERT members.
- 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 meet its intended effect, and provide advice to the SC;
  - Review associated policies and procedures in relation 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 WG where appropriate; and
  - 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; and
  - 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 (10): CERT-In, 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
  - Share information on the malware infections of each participating economies to analyse type of malware infecting the economies as the character and motive of each infection may differ from one to another;
  - Share the resources for the initiatives taken in reducing the number of malware infections, including potential funding, cost, personnel and time; and
  - Increase collaborative efforts in mitigating malware infections affecting APCERT economies – as a group, collaboration among economies is easier as trust has been created for information sharing in mitigating malware infection.
- Convener (1): CyberSecurity Malaysia
- Members (11): Bkav Corporation, BruCERT, 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; and
- To allow continuous improvements.

- Convener (1): ThaiCERT
- 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
  - Propose steps to address the security issues including vulnerabilities tailored for some of the priority sectors;
  - Incident response mechanisms/measures for responding to cyber physical security incidents impacting human life; and
  - Discussions on existing Security Standards and gaps for IoT Ecosystem and considerations for adoption in specific sector.
- 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
  - Understand the products and services as well as the infrastructure and platforms in the digital payments space;
  - Understand the digital payment ecosystem/supply chain; and
  - Incident response mechanisms/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

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 2019

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 2019, APCERT Teams have hosted, participated and/or contributed in the following events:

- APCERT Drill 2019 (31 July)
  https://www.apcert.org/documents/pdf/APCERT_Drill2019_Press%20Release.pdf
  APCERT Drill 2019, the 15th APCERT Cyber Exercise Drill, was successfully conducted to test the response capabilities of the participating APCERT Teams. 26 teams from 20 economies of APCERT (Australia, Bhutan, Brunei Darussalam, People's Republic of China, Chinese Taipei, Hong Kong, India, Indonesia, Japan, Republic of Korea, Lao People's Democratic Republic, Macau, Malaysia, Mongolia, Myanmar, New Zealand, Singapore, Sri Lanka, Thailand, and Vietnam) participated in the Drill. The theme of the drill was "Catastrophic Silent Draining in Enterprise Network."

- APEC-TEL 59 (2-7 March, June – Santiago, Chile)
  APCERT participated APEC TEL 59 and presented the APCERT's overview and latest activities for a safer cyber space base on the regional framework.

- 31st Annual FIRST Conference (16-21 June – Edinburgh, Scotland)
  https://www.first.org/conference/2019/
  APCERT Teams attended the Annual FIRST Conference in Edinburgh, Scotland, and shared valuable experience and expertise through various presentations.

- National CSIRT Meeting (21-22 June – Edinburgh, Scotland)
  APCERT teams attended the National CSIRT Meeting, hosted by CERT/CC and exchanged various activity updates as well as recent projects and research.

- ASEAN CERT Incident Drill (ACID) 2019 (4 September)

  ACID 2019, 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.

- APCERT Annual General Meeting (AGM) & Conference 2019 (29 September – 2 October – Singapore)

  https://www.apcert2019.sg/

  The APCERT Annual General Meeting (AGM) & Conference 2019 was held on 29 September – 2 October 2019 at Grand Copthorne Waterfront Singapore. (APCERT Open Conference on 2 October was held side-by-side with Singapore International Cyber Week 2019 at Suntec Singapore Convention & Exhibition Centre.)

  Programme Overview:

29 September (Sun)	AM:	Steering Committee Meeting
	PM:	Working Group Meetings, Gala Dinner
30 September (Mon)	AM:	Training Workshop
	PM:	Closed Conference
1 October (Tue)	AM:	Annual General Meeting
	PM:	APCERT Team Building Event
2 October (Wed)	AM:	Open Conference

- Asia-Pacific Telecommunity Symposium on Cybersecurity 2019 (8-10 October, Kuala Lumpur, Malaysia)

  APCERT participated in the Asia-Pacific Telecommunity Symposium on Cybersecurity 2019 and introduced the APCERT's activity overview to cyber security stakeholders in the region.

- APEC-TEL 60 (13-18 October – Seoul, South Korea)

  APCERT participated at APEC TEL 60 and presented the APCERT's overview and latest activities.

- 8th Regional Cyber Security Summit (27-28 October – Muscat, Oman)
  APCERT was invited to 8th Regional Cyber Security Summit and participated in the panel session on international cooperation in cyber security among other leaders of international organisations.

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.

- **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 2019, SC members held 4 teleconferences and 2 face-to-face meeting to discuss APCERT operations and activities.

24 February	Face-to-face meeting concurrently held at APRICOT 2019 in Daejeon, South Korea
8 May	Teleconference
17 July	Teleconference
5 September	Teleconference
29 September	Face-to-face meeting at APCERT AGM 2019 in Singapore
27 November	Teleconference

3. APCERT Training

APCERT held five (**5**) training calls and one (**1**) training workshop in 2019 to exchange technical expertise, information and ideas.

Date	Title	Presenter
12 February	Digital Forensic Analysis with Free and Open Source Tools	TechCERT
9 April	Web Application Penetration Testing Techniques	VNCERT
4 June	Web Penetration Testing 101	TWNCERT
6 August	Digital Forensics (Storage Media & Mobile Phones)	CERT-In
30 October	Introduction to Honeypots Workshop	APNIC
10 December	Zero Day Malware - Static Analysis	mmCERT

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.

III. Activity Reports from APCERT Members

ACSC

Australian Cyber Security Centre – Australia

1. Highlights of 2019

1.1 Summary of major activities

2019 was ASD's first full calendar year of operation as a statutory agency performing whole of economy functions.

1.2 Achievements and Milestones

In 2019, the ACSC worked actively with public and private sector organisations to strengthen cyber security arrangements and build resilience. Key activities included:

- commencing an Energy Sector Cyber Security Readiness and Resilience Program, which supported the vision outlined in the Independent Review into the Future Security of the National Electricity Market: Blueprint for the Future (Commonwealth of Australia, 2017), for a National Electricity Market that has a strong cyber security posture
- initiating and implementing a Whole of Government Cyber Uplift for Federal Government Systems for government agencies
- continuing to proactively engage with international counterparts both bilaterally and through international fora. This included supporting the nominations of partners to international bodies. A key example being the ACSC sponsorship of CERT Tonga for APCERT Operational Membership.

2. About the ACSC

2.1 Introduction

The ACSC leads the Australian Government's efforts to improve cyber security. Its role is to help make Australia the safest place to connect online. The ACSC collocates staff with a cyber security remit from Australian Government agencies.

The ACSC monitors cyber threats across the globe 24 hours a day, seven days a week, in order to alert Australians early and provide them with advice on how to protect themselves and their business online.

During a cyber security incident, the ACSC provides clear and timely advice to

individuals, small to medium business, big business and critical infrastructure, and the Australian government operators.

The ACSC works with business, government and academic partners and experts in Australia and overseas to investigate and develop solutions to cyber security threats.

2.2 Establishment

The ACSC began operations in 2014. 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 its remit to the provision of cyber security advice and assistance across the whole of the economy and became part of ASD.

2.3 Resources

The ACSC consists of several hundred staff members, including those from partner agencies: the Australian Criminal Intelligence Commission; Australia Federal Police; Australian Security Intelligence Organisation; Australian Signals Directorate; and the Defence Intelligence Organisation. Department of Home Affairs Cyber Security Policy Division staff are collocated with ACSC staff to better inform policy advice for Government.

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 drives cyber resilience across the whole of the economy, including critical infrastructure and systems of national interest, federal, state and local governments, small, medium and large business, academia, the not for profit sector and the Australian community.

The ACSC is a hub for private and public sector collaboration and information-sharing to prevent and combat cyber security threats and to minimise harm to all Australians.

More specifically, the ACSC:

- responds to cyber security threats and incidents as Australia's 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, and
- provides information, advice and assistance to all Australians.

3.2 Incident handling

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 appropriate response measures are activated.

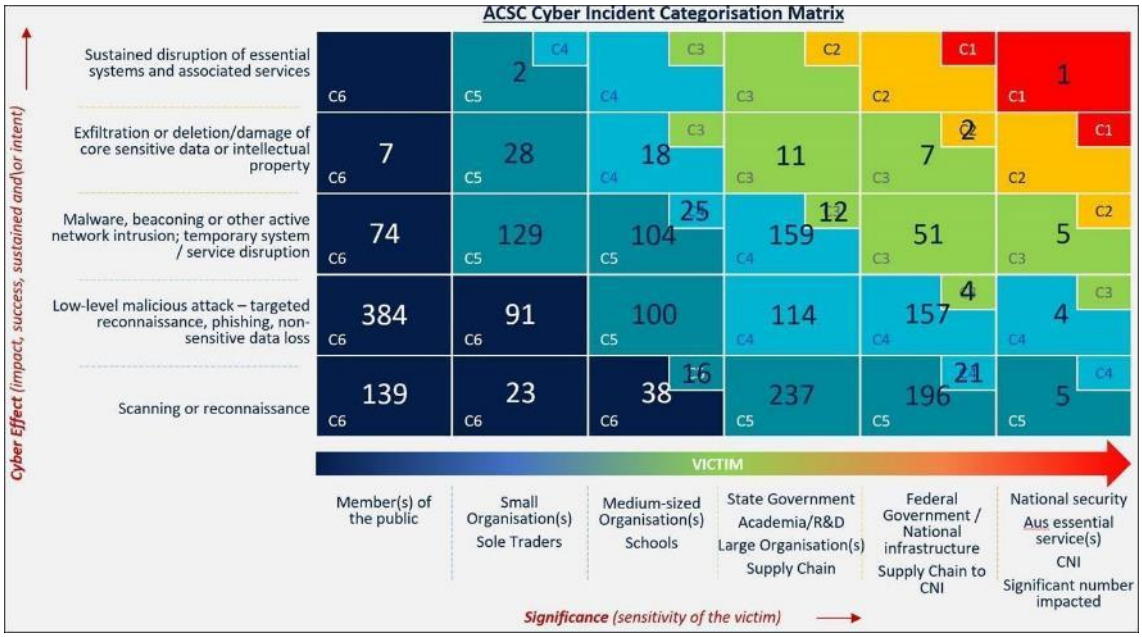


Figure 1: Cyber Incident Categorisation Matrix

Note - The matrix includes incidents between 1 July 2018 and 30 June 2019 due to Australia's reporting timelines.

During 2018–19, the ACSC responded to 2164 incidents of varying significance, including Australia's first national cyber crisis (C1).
Of the other incidents reported to the ACSC, 40 percent were low-level malicious attacks, including targeted reconnaissance, phishing emails and non-sensitive data loss. Members of the public reported the highest number of incidents, making up approximately one quarter of all reports received.

3.3 Publications

During 2018-19, the ACSC used a variety of means to provide accurate and timely cyber security advice to Australians.

The ACSC produced:

- sixty PROTECT publications on cyber.gov.au for public consumption, including appropriate updates to several existing publications
- the unclassified Sector Snapshot, designed to inform decisions about investment and allocation of internal resources by executives and cyber security professionals
- a Practitioners Guide and an Executive Companion used to inform organisations about key cyber security issues related to cyber supply chain management
- updates to the Essential Eight Maturity Model
- six 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
- a new version of the Information Security Manual which provides significant updates to its risk management framework
- seven Information Security product certifications under the Australasian Information Security Evaluation Program
- The Small Business Cyber Security Guide was developed to help small businesses protect themselves from the most common cyber security incidents.

3.4 New services

In support of Australia's whole-of-government approach to securing the 2019 Federal Election from interference, the ACSC, the Australian Electoral Commission, Department of Finance, Department of Home Affairs, Department of the Prime Minister

and Cabinet, Department of Communication and the Arts, the Attorney-General's Department, Australian Federal Police and the National Intelligence Community worked together as the Electoral Integrity Assurance Taskforce (the Taskforce). The ACSC provided physical resourcing by facilitating colocation of Taskforce members.

The ACSC also launched a Critical Infrastructure Laboratory to raise awareness of security issues in critical infrastructure and research best practice in system configuration. The laboratory currently comprises tabletop exercise and learning components, as well as a small-scale functioning system emulating that used by Australian Critical Infrastructure providers (see Figure 2). Extensions to the laboratory are planned to increase research efforts on security issues around smart cities and emerging technologies.

Figure 2: Defending a mini-village run by Industrial Control Systems

4. Events organised / hosted

4.1 Training

ASD designs and delivers bespoke training to support ASD's mission and facilitates access to external development opportunities for ASD staff.

The ACSC also offers training to external stakeholders, for example the “how to conduct a discussion exercise” training to enable organisations to test their own cyber security response capability.

4.2 Drills and exercises

The ACSC amplified Australia's National Exercise Program, which supported 25 cyber security exercises across government and the energy, banking and finance, telecommunications, transport, water, health and resource sectors.

4.3 Conferences and seminars

The ACSC partnered with the Australian Information Security Association to host the 2019 Australian Cyber Conference in Melbourne 7-9 October. The event was attended by 3,500 delegates from academia, industry and government.

Additionally, the ACSC collaborated with industry and government stakeholders on cyber security matters, including:

- working with the Australian Energy Market Operator to develop the Australian Energy Sector Cyber Security Framework
- providing cyber security advice in support of the foreign investment applications and licence condition reviews, primarily associated with systems of national significance
- contributing expertise to the Department of Home Affairs' critical infrastructure protection policies.

5. International Collaboration

5.1 International partnerships and agreements

Cyber security threats and incidents often traverse international borders and there is a growing mutual reliance on maintaining strong international relationships to address these threats.

The ACSC has strong international relationships with cyber security counterparts around the world in order to share information, mitigate incidents and enhance Australia's cyber security resilience. In addition, the ACSC leads numerous international engagement and capacity-building activities in its region to build the collective regional resilience to cyber security threats and, ultimately, further 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 individuals responsible for their respective governments' responses to cyber security incidents. In 2019, the ACSC facilitated the second annual face-to-face meeting of PaCSON members — in Nuku'alofa, Tonga, from 29 April to 3 May 2019. The meeting included a cyber security information exchange, an annual general meeting and a series of technical and strategic workshops.

5.2.1 Drills & exercises

Cyber incident responders from across the ASEAN region tested their defensive cyber skills at the ACSC's Perth Joint Cyber Security Centre (JCSC) in the first ACSC-ASEAN Capture the Flag exercise, hosted by the ACSC.

A first for Australia, ASEAN and Perth, the event was part of the ACSC's commitment to regional cyber uplift and building awareness of its cyber security incident response capability.

Sharing skills is integral to the mutual achievement of regional cyber security goals, enabling us to take advantage of the opportunities a safe cyberspace offers both Australia and the ASEAN group of economies.

5.2.2 Seminars & presentations

The ACSC is an active participant in the global cyber security community and attend events where appropriate. Examples include ACSC attendance at the Asia Pacific Regional Internet Conference on Operational Technologies (APRICOT) in Daejeon in February and chairing of the APCERT Conference in Singapore in September/October 2019.

5.3 Other international activities

Throughout 2019, the ACSC also presented at and/or participated in several other international forums including:

- RSA Security Conference – USA FIRST Conference; National CSIRTs Meeting ('Second Conference') – Scotland
- Blackhat – USA
- Other closed events organised by international government organisations and CERTs.

6. Conclusion

The ACSC values its ongoing engagement with the APCERT community and remains an active and collaborative member.

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.

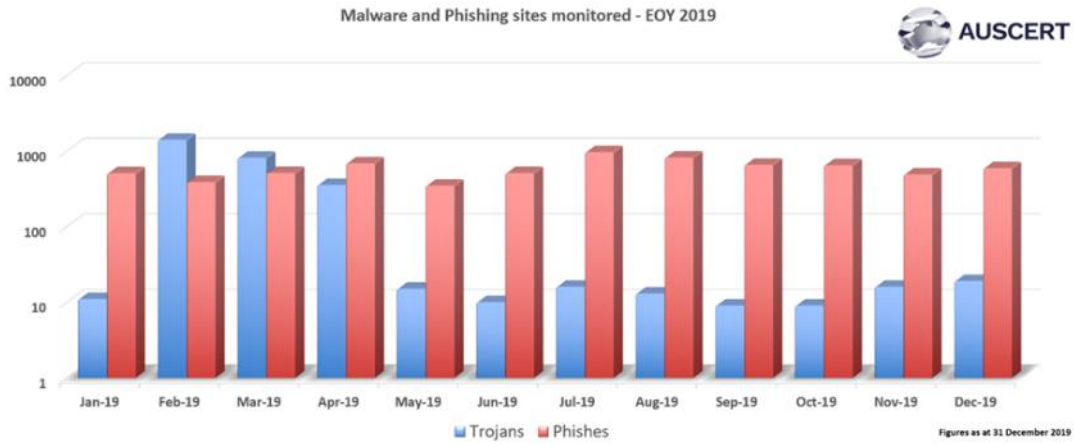
Services provided are listed as:

- Incident Management [2.2], https://www.auscert.org.au/services/incident-management-service/
- Early Warning Service [2.3] https://www.auscert.org.au/services/early-warning-service/
- Malicious URL Feed [2.4] https://www.auscert.org.au/services/malicious-url-feed/
- Member security incident notification's (MSINs)[2.5.1] https://www.auscert.org.au/services/security-incident-notifications/
- Phishing take-down [2.6] https://www.auscert.org.au/services/phishing-take-down-service/
- Security Bulletin Service [2.7] https://www.auscert.org.au/services/security-bulletins /
- Leaked Credential Service [2.8]
- AusCERT's member only IRC channel
- AusCERT Conference https://conference.auscert.org.au/
- AusCERT Certificate Service

https://cs.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 subscription services.



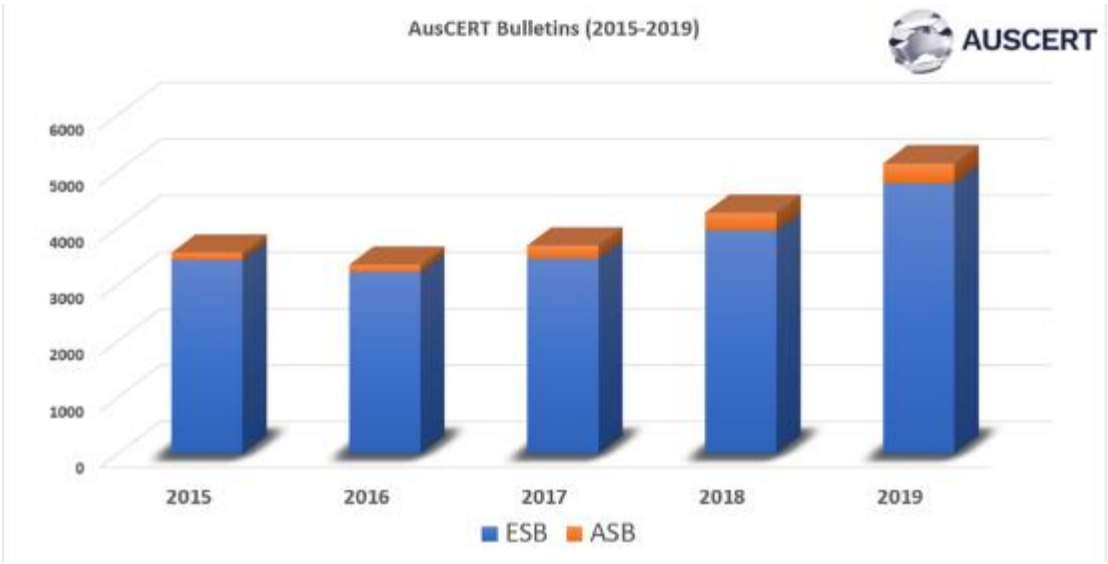
The above diagram is the statistics of incidents that required handling either of phish site or that of malware, for the calendar year of 2019. These tallies are sites that are located around the world in a manner that affects the operation of the constituency that AusCERT is serving

2.3 Early Warning System

Members can subscribe to receive urgent SMS notifications, when AusCERT's Security Bulletin Service identifies a vulnerability that has reached critical stages. In most circumstances this occurs when AusCERT is aware of active, in-the-wild exploitation of a vulnerability.

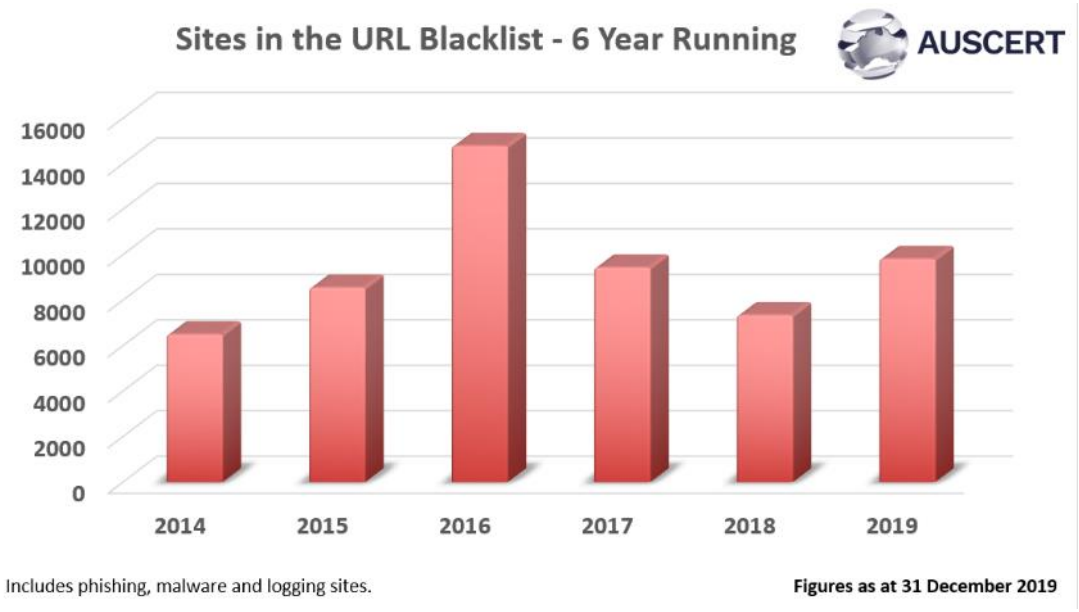
Alerts are sent along with Bulletins, with additional flagging of the Bulletins. These Bulletins are given special importance with respect to the nature of the issue.

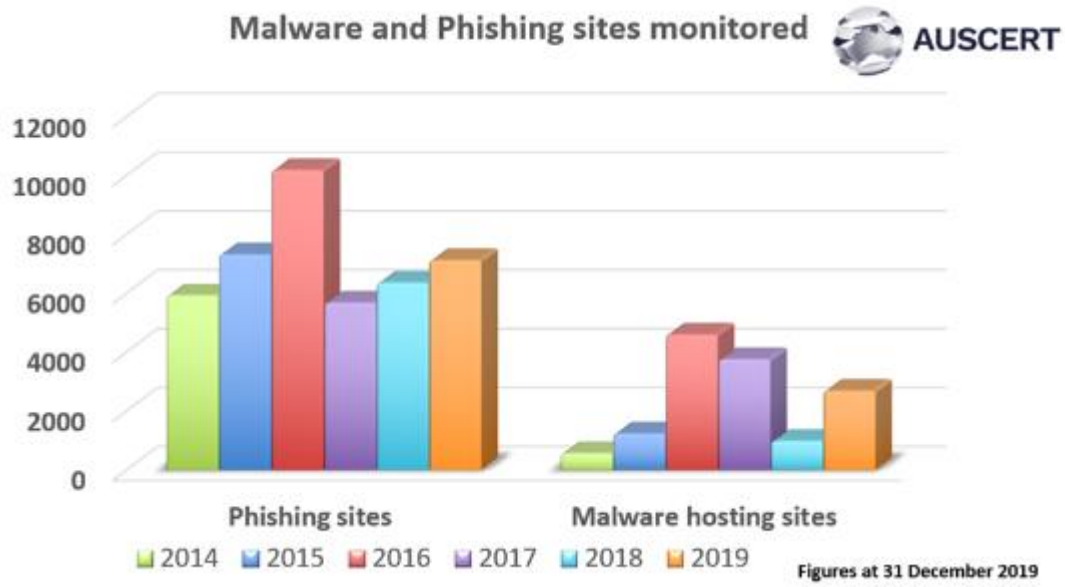
Of note is the growing number of bulletins that are being handled, this being in line with the increased capacity at AusCERT to process additional streams of advisories.



2.4 Malicious URL Feed

On a daily basis, AusCERT encounters numerous phishing, malware, malware logging or mule recruitment web sites, including those directed at Australian Internet users. We collect this information and provide a feed that can be added to your firewall blacklist to prevent inadvertent compromise to client computers on your network; or you can check your web log files to see if any client computers on your network may have already connected to these web sites as a way to detect potential compromises to client computers on your network.



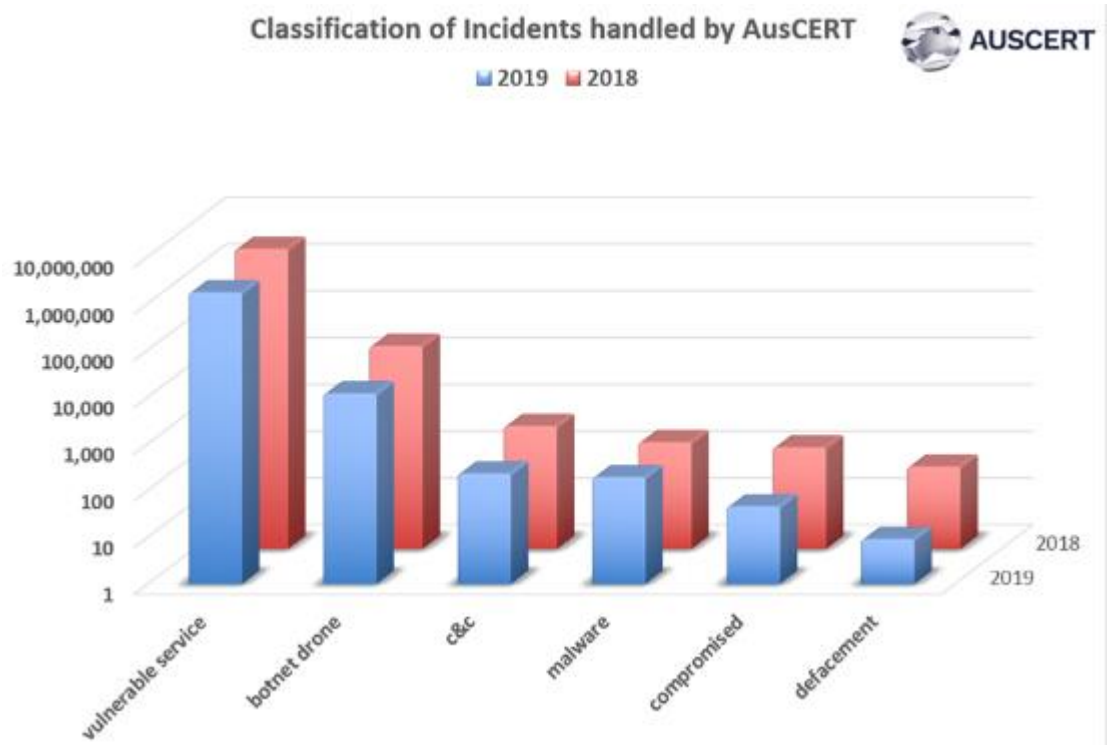


2.5 Notifications

2.5.1 Member Security Incident Notifications

AusCERT Members benefits from AusCERT's 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. In 2019, as compared with 2018, follows the same distribution of incidents, except for numbers of compromised host and defaced sites.

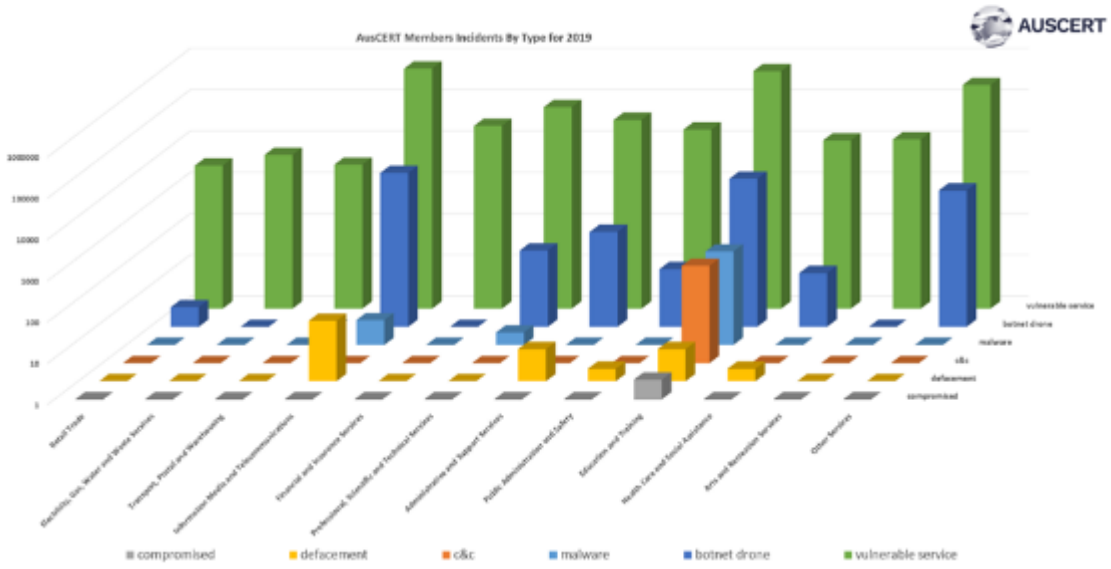
These notifications are a mix of Indicators of Vulnerabilities (IoV) and Indicators of Compromise (IoC). The numbers of IoV far outweigh the other categories and hence to be able to better display all the categories of the graph of the notifications are done on a logarithmic scale.



Indicators of Vulnerabilities such as the notification that services that are running by members are vulnerable, were made at a staggering one million, six hundred and eighty-seven thousand, nine hundred and four (1,687,904) times.

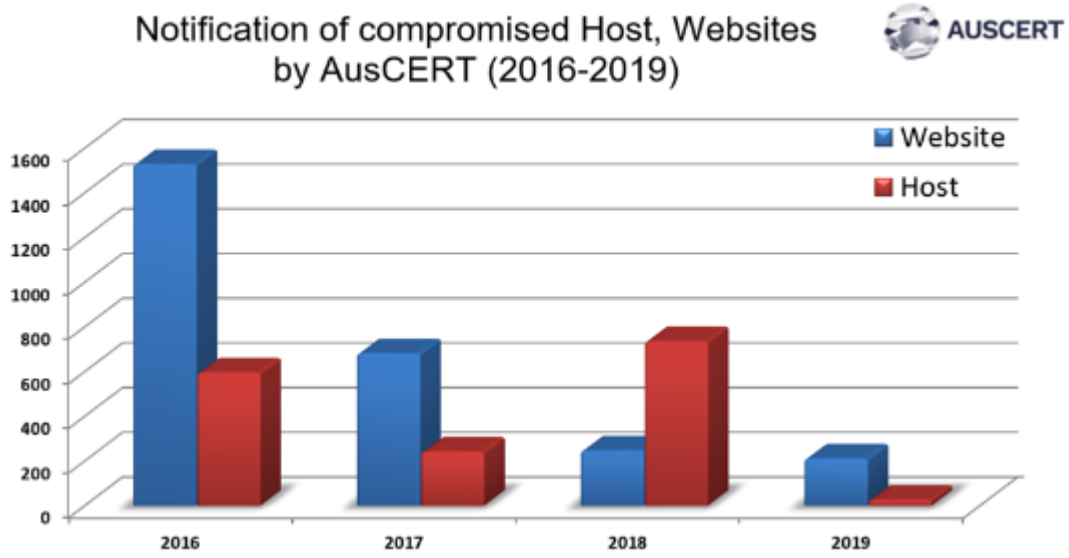
The numbers of other types of notifications are not as many but are just as important. Botnet drones tallied down from last year at eleven thousand five hundred and thirty-four (11,534), Command and Control were down from last year at two hundred and twenty-six (226) unique instances, Defacement down at forty-five (45) and compromised hosts down at four (4) instances.

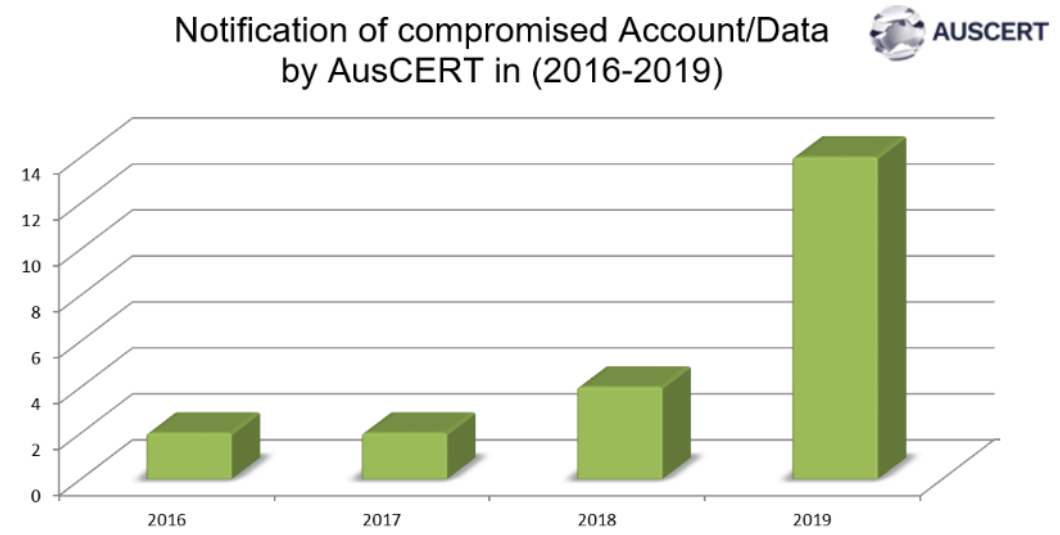
In the year 2019, further in-depth reporting is provided where the types of incidents are spanned out to show the different industry classifications of AusCERT members affected.

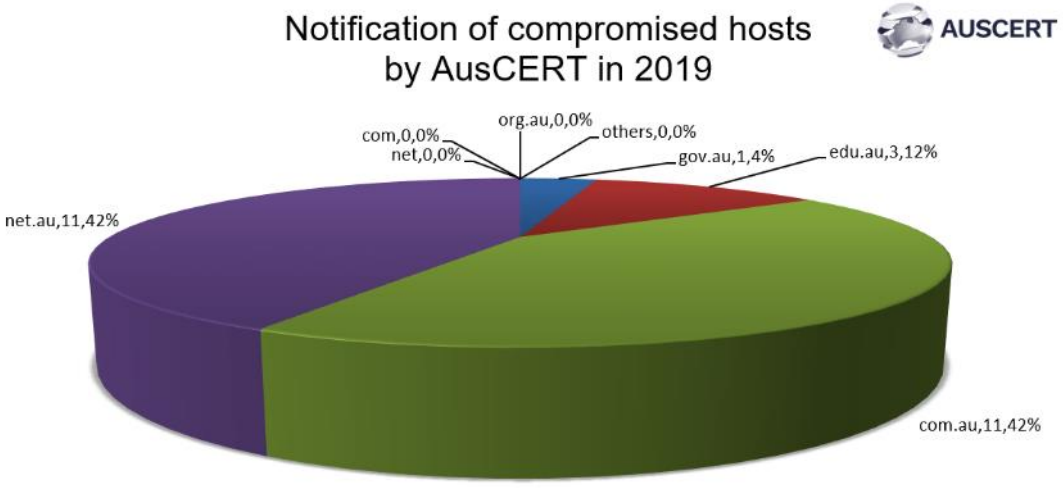


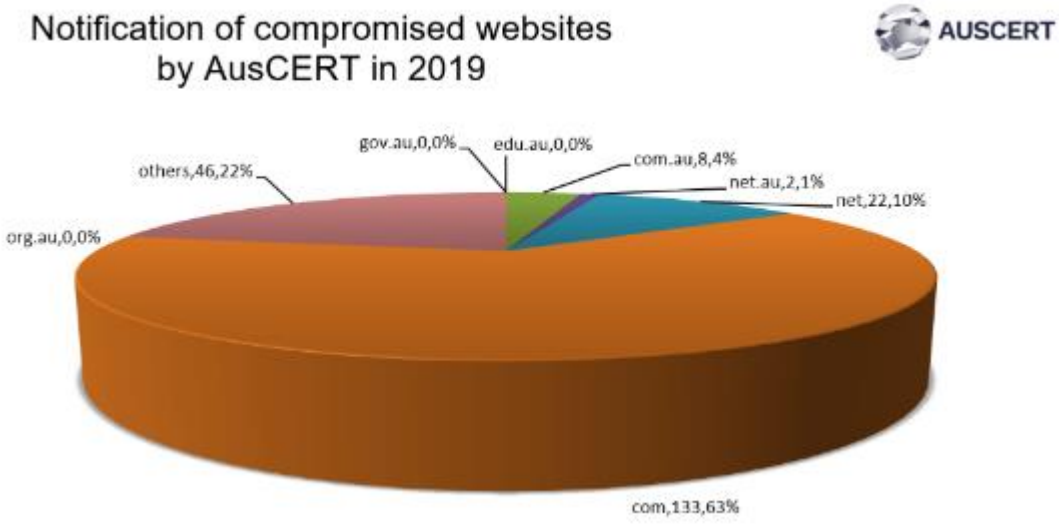
2.5.2 Legacy notification and reporting system.

To be able to compare notes of the continued notification of compromised host and websites the following graphs are still provided for reference. These numbers are and graphs are provided this year as a bridge to the new system and its reporting capability.



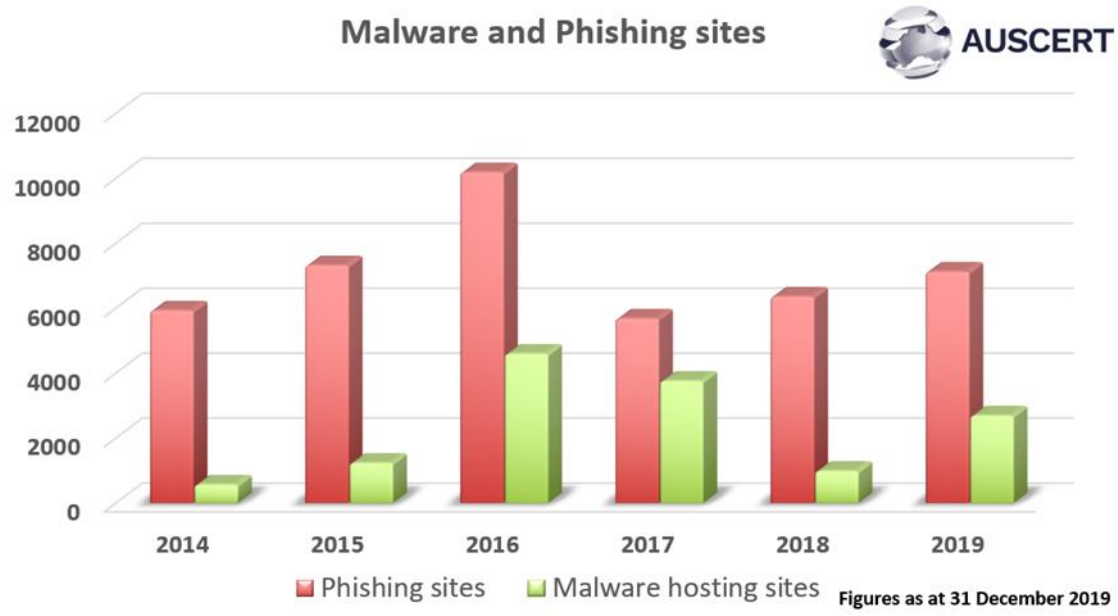

Notification of compromised Account/Data
by AusCERT in (2016-2019)
AUSCERT
14
12
10
8
6
4
2
0
2016
2017
2018
2019


Notification of compromised hosts
by AusCERT in 2019
AUSCERT
org.au,0,0%
com,0,0%
net,0,0%
others,0,0%
gov.au,1,4%
edu.au,3,12%
net.au,11,42%
com.au,11,42%


Notification of compromised websites
by AusCERT in 2019
AUSCERT
gov.au,0,0%
edu.au,0,0%
com.au,8,4%
others,46,22%
net.au,2,1%
net,22,10%
org.au,0,0%
com,133,63%

2.6 Phishing Takedown

AusCERT Members can utilise AusCERT's considerably large overseas and local contact network for removal of phishing and malware sites. The number of sites that were handled in the year 2019 has already been graphed in the section Malware URL. Specifically, for Phish site, the tally is seven thousand one hundred and twenty-one (7,121). This service is not limited to taking down phishing sites but also of takedowns of sites that are serving malware. Of those malware sites, two thousand six hundred and ninety (2,690) sites have been reported in the calendar year of 2019. This can be seen from the diagram below.

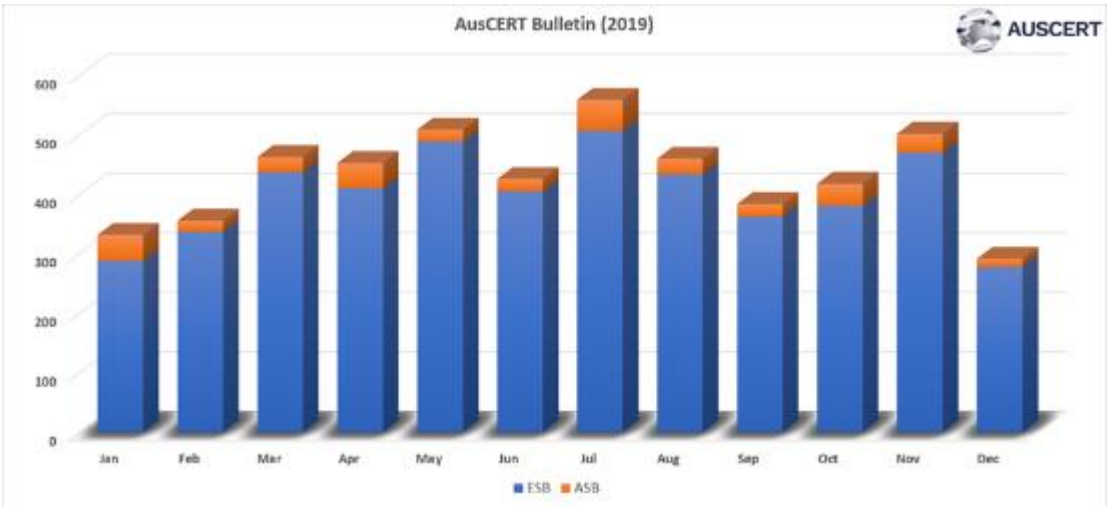


2.7 Security Bulletins

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.

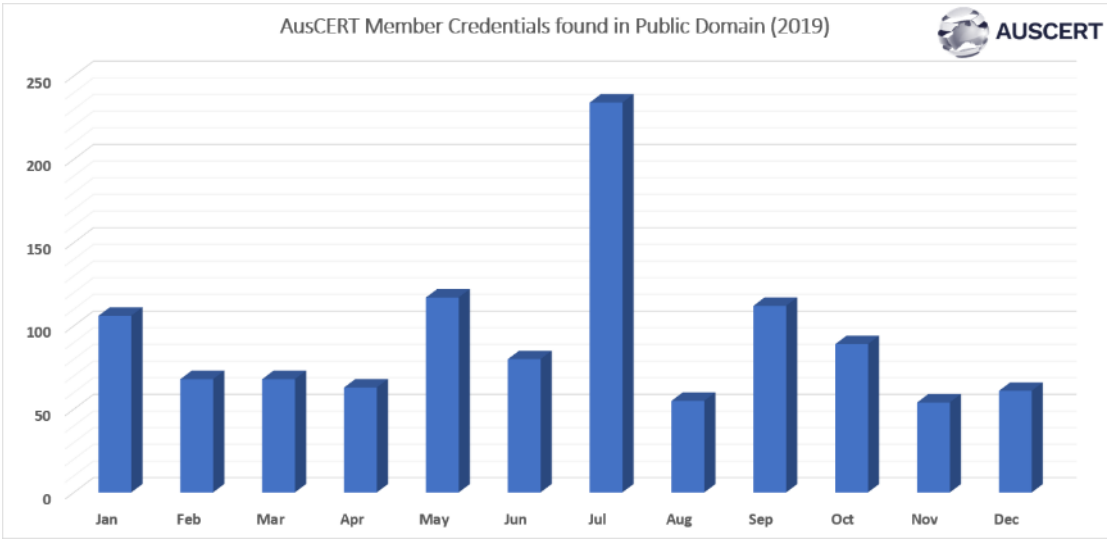
During 2019, four thousand seven hundred and eighty-eight (4,788) External Security Bulletins (ESBs) and three hundred and fifty-four (354) AusCERT Security Bulletins (ASBs) were published.

The ESBs are made publicly available immediately however the ASBs are available to members only for a period of one month after release, beyond which time they are made public.



2.8 Leaked Credential Service

A service that AusCERT has been offering Since 2016 has been leaked credential reports. On occasion, AusCERT finds credentials of members that have been leaked on the internet. As soon as these credentials are found then a report is sent to the owner organisation so that they may invoke their security processes for leaked credentials. The following graph shows the tally of unique credentials that have been reported back to members.



2.9 Publications

2.9.1 Week In Review

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

2.9.2 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.

2.9.3 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.

2.9.4 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 2019, took place from 28th May -31st May 2019 in Surfers Paradise Gold Coast, Australia with the theme of "It's Dangerous to go Alone". Against a backdrop of evolving technologies and emerging threats, AusCERT2019 will encourage the information security community to devise new ways of building cyber security resilience. Will a new technology solution emerge, such as advanced machine learning to defend against unknown unknowns? Or perhaps we'll find a new way of looking at an old problem, such as blocking known threats. Maybe we'll even solve the problem of building resilience in modern environments where traditional borders no longer exist, such as extended work forces using BYOD. AusCERT2019 will explore these questions and more through world-class speakers, presentations and tutorials. the conference covered areas such as:

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 2019

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 "Catastrophic silent draining in enterprise network". The drill fosters communication between the CERTs in the region and beyond. In all, 26 CERT/CSIRT teams from APCERT participated.

4.2.2 ACID 2019

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

This year of 2019 was for AusCERT marked by further growth in capacity. This was immediately reflected in the number of bulletins that were able to be processed in the year, up to almost five thousand. AusCERT has been committed in providing back its constituency quality services from the support that the membership provides AusCERT. This direct feedback allows AusCERT to improve in doing its part in keeping the internet a safe and reliable resource.

BGD e-Gov CIRT

Bangladesh e-Government Computer Incident Response Team - Bangladesh

1. Highlights of 2019

1.1 Summary of major activities

- 910 cyber security incidents registered in our tracking system.
- Arranged 10 cyber security training / workshop.
- 5 Cyber Sensor units have been deployed to Critical Information Infrastructures.
- Provided more than 15 digital forensic case report to several government organization.
- Development of self-assessment tool kit for cyber risk assessment for CII organizations.
- Conducted risk assessments in CII organizations.
- Developed and published "Bangladesh Cyber Threat Landscape 2019".
- Cyber Range provided training to 100 Govt. officials in 2019.
- Total 5 major IT Audit activities were completed successfully for 5 (Five) Govt. organization.
- Providing monthly threat intelligence report to several government stake holder.
- Publishing monthly cyber bulletins for stakeholders.

1.2 Achievements & milestones

- Participated in OIC Drill 2019.
- National Data Center (NDC) ISO 27001 re-certification Audit successfully done under supervision of IT Audit team and received the ISO 27001 certification.
- Received TF-CSIRT Accreditation certificate.

2. About CSIRT

2.1 Introduction

Bangladesh Government's Computer Incident Response Team (BGD e-GOV CIRT) is acting as the National CIRT of Bangladesh (N-CIRT) 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. BGD e-GOV CIRT has a very strong tie with international organizations and cybersecurity communities and working as a focal point of Bangladesh for trans-border cyber issues.

2.2 Establishment

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

2.3 Resources

Currently 13 people are working in BGD e-GOV CIRT and more people will join soon.

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 CIRT of Bangladesh with a mandate to serve whole of Bangladesh.

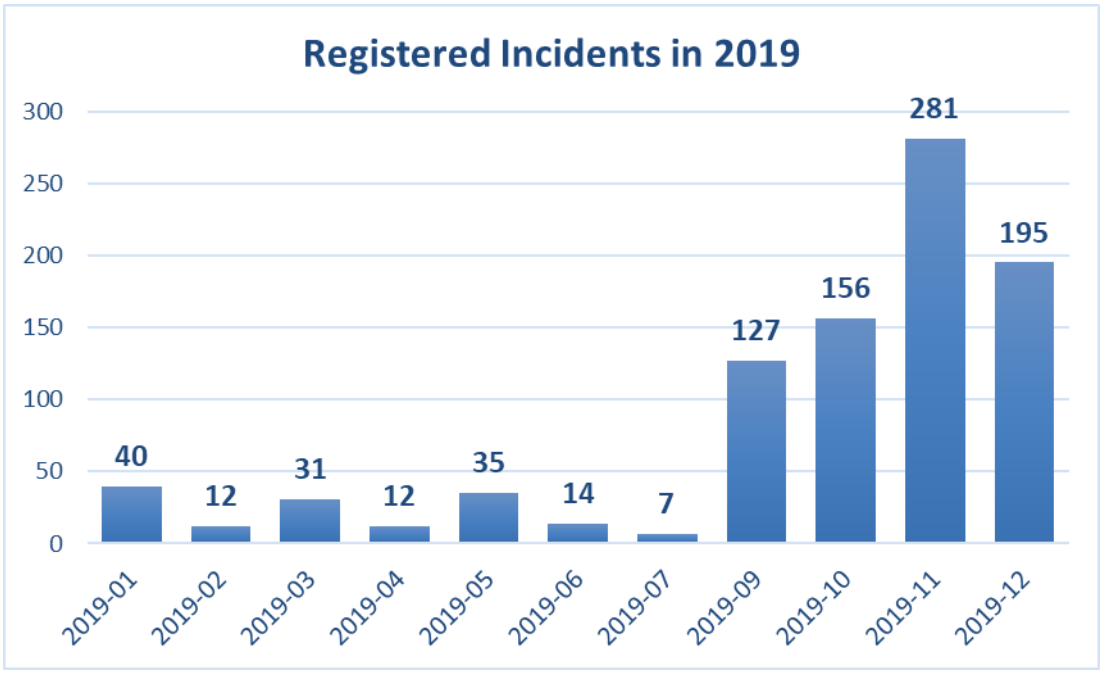
3. Activities & Operations

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.

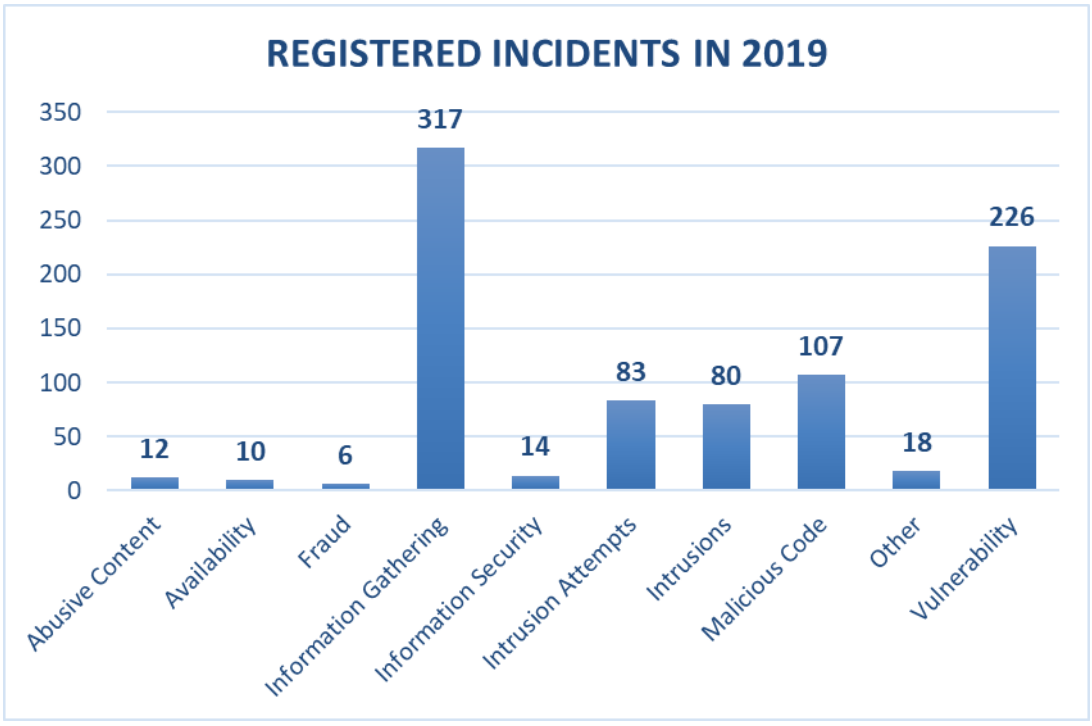
3.2 Incident handling reports

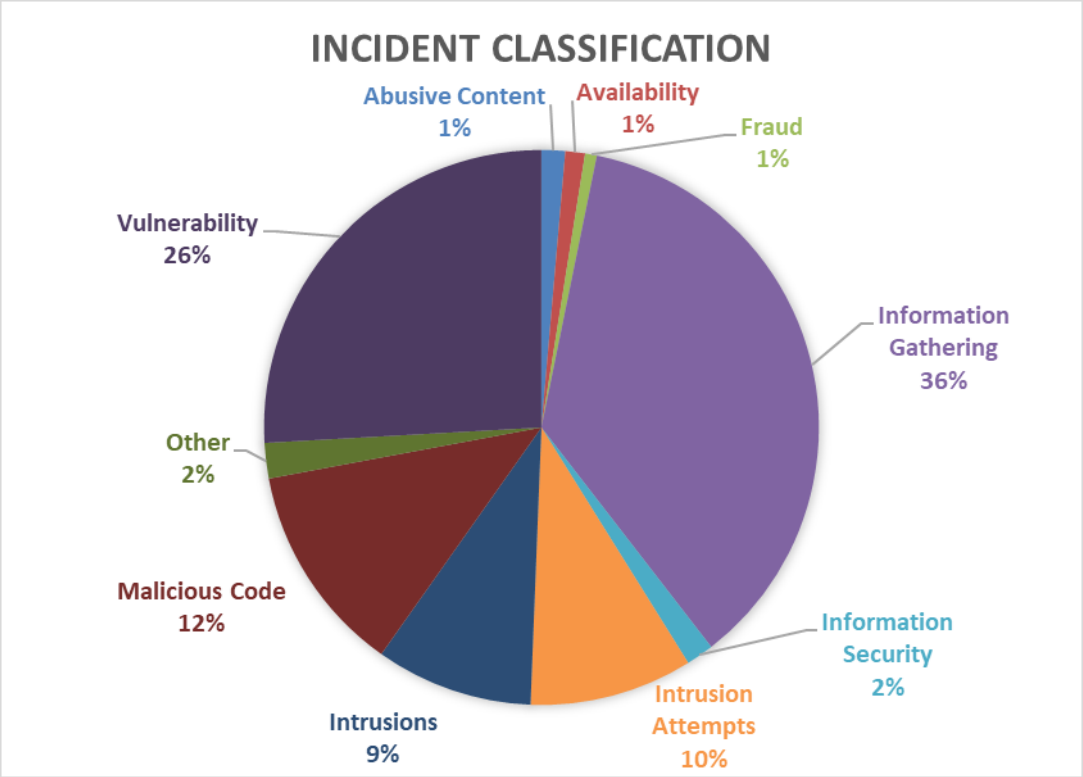
BGD e-GOV CIRT receives information regarding cyber security incidents, triage incidents and coordinate response. Activities related to incident handling includes and not limited to Vulnerability Assessment, Penetration Test, Incident Analysis, Security Threat Notification and Incident Coordination etc. In 2019 we have registered 910 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

- Bangladesh threat landscape workshop for Critical information Infrastructure (CIIs).
- Arranged workshop on "Cyber Range Operation" for all government bank, Bangladesh Air Force & Military Institute of Science & Technology of Bangladesh.
- Conducted Training on Digital Forensics at Military Institute of Science & Technology, Bangladesh.
- Conducted Training on Cyber Security at Prime Ministers' Office, Bangladesh.
- Conducted 2 (two) security awareness session for National Data Center employees and 1(One) session for ISACA local chapter.
- Conducted training on Cybersecurity & Social Media Awareness in Department of Women Affairs, Dhaka, Bangladesh. Etc.

5. International Collaboration

5.1 Capacity building

5.1.1 Training

- Participated in "International law in cyber space" program arranged by George C. Marshall European Center for Security Studies, Germany.
- Participated in "Program on Cyber Security Studies" training arranged by George C. Marshall European Center for Security Studies, Germany.
- Attended in "International Workshop on Cybersecurity Education and Workforce Development Capacity Building" arranged by George C. Marshall European Center for Security Studies, Germany.
- Attended training in "Japan -US Industrial Control Systems Cybersecurity Training" arranged by Industrial Cyber Security Center of Excellence, Japan.
- Attended "Cyber Range Training Administration", Australia from 14-18 August 2019.
- Attended 12th Annual Cyber Security Week 2019, Colombo, Sri Lanka.
- Attended "Cisco Security Scape", India from 11-12 January 2019

5.1.2 Drills & exercises

- Participated in OIC Drill 2019.

5.1.3 Seminars & presentations

- Attended 11th OIC-CERT Annual Conference 2019 conjunction with the 8th Regional Cybersecurity Summit and FIRST & ITU-ARCC Regional Symposium held in Muscat, Oman (27–31th October 2019).
- Attended "Black Hat Asia 2019 Conference, Singapore". Etc.

6. Future Plans

6.1 Future Operation

- Upgrade Cyber Risk assessment framework.
- Perform risk assessment to critical infrastructure (CIIs).
- Provide regular cyber sensor analysis reports (Intrusion, Suspicious activity) to Critical Information Infrastructure where Cyber sensor deployed.
- Provide training about Industrial Control System (ICS) in Public sector.
- Mobile applications penetration test.

- ISO 20000 Certification for National Data Center Tier-III.
- Audit plan for Eight (8) Govt organizations.

7. ATTACHMENT (Photos)

Figure 1: 11th OIC-CERT Annual Conference 2019

Figure 2: Participants from BGD e-GOV CIRT attended 3 weeks long PCSS course in George C. Marshall European Center for Security Studies

Figure 3: PCSS course participants in George C. Marshall European Center for Security Studies

Figure 4: 12th Annual National Cyber Security Week, 2019 Colombo, Sri Lanka

Figure 5: Conducting training on Digital Forensics (hands-on) at Military Institute of Science & Technology, Dhaka, Bangladesh.

Figure 6: Participated in Applicability of International Law to State Behavior in Cyberspace Course, PCSS, George C. Marshal European Center for Security Studies, Germany.

Figure 7: Conducting training on Cybersecurity & Social Media Awareness in Department of Women Affairs, Dhaka, Bangladesh.

Figure 8: Receiving ISO 27001 certificate

BruCERT

Brunei Computer Emergency Response Team – Negara Brunei Darussalam

1. About BruCERT

1.1 Introduction

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.

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.

1.4.1 Government Ministries and Departments

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

1.4.2 E-Government National Centre (EGNC)

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

1.4.3 AITI

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

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

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

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

1.5 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 2019

2.1 Incidents response

In 2019, 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 and coin miner type of malware. The statistic of the security incident is shown as Figure 1.

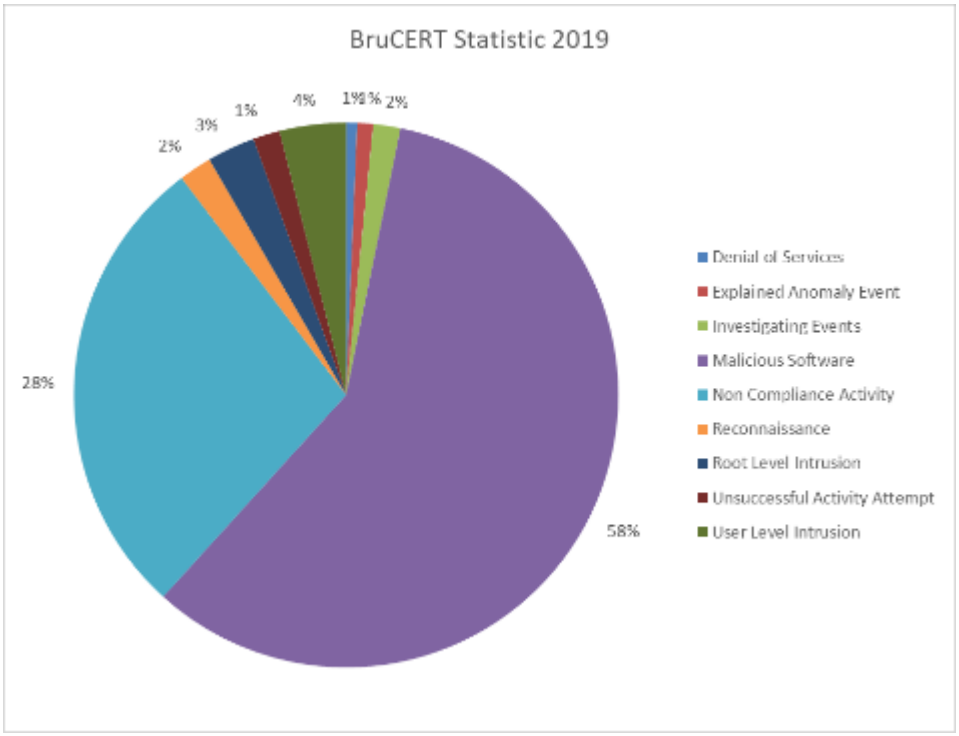


Figure 1

Types of Attack	Count
Denial of Services	2
Explained Anomaly Event	36
Investigating Events	62
Malicious Software	2243
Non-Compliance Activity	1071
Reconnaissance	75
Root Level Intrusion	109
Unsuccessful Activity Attempt	61
User Level Intrusion	151

Table 1

2.2 BruCERT Honey Pot

In the year 2019, the most attack services which was recorded by BruCERT HoneyPot sensor was Telnet services which is around 33909549 attacks. The grand total of attacks on services which was recorded is **69851021**. Please refer to Figure 2 and Table 2 for more detail.

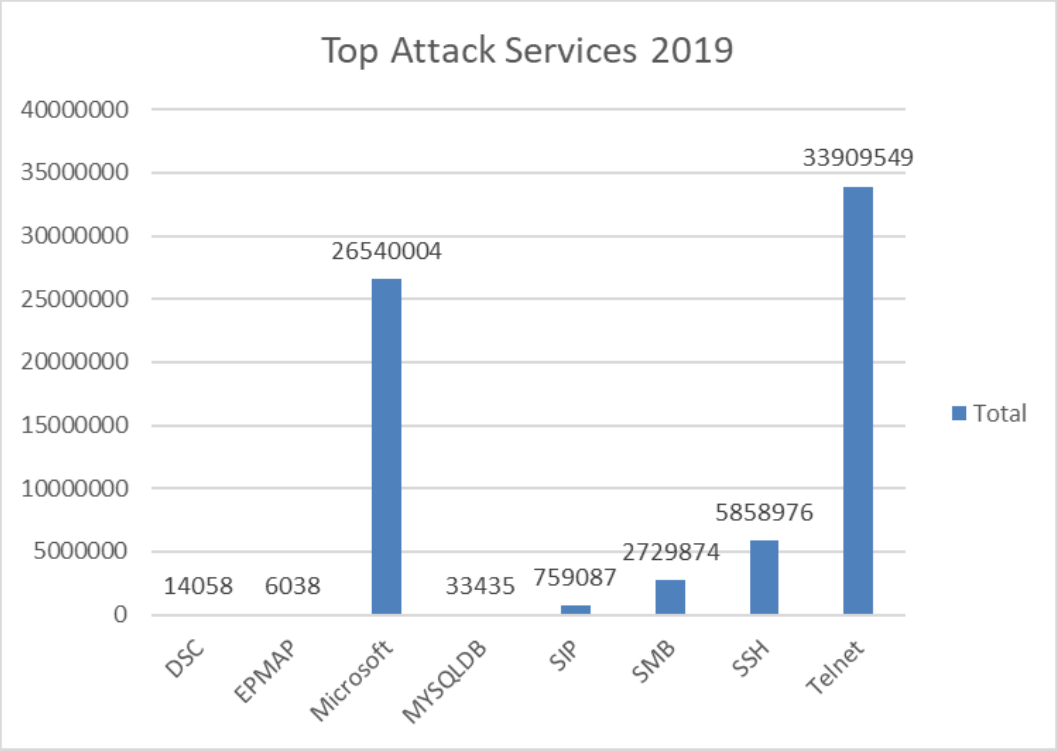


Figure 2

Event Type	Count
DSC	14058
EPMAP	6038
Microsoft	26540004
MYSQLDB	33435
SIP	759087
SMB	2729874
SSH	5858976
Telnet	33909549
Total	**69851021**

Table 2

The most attack port recorded for the year 2019 is the port number 1433, which is usually used by Microsoft SQL Server. It might be the work of a new variant of a worm, trying to infect the Microsoft SQL server. Please refer to Figure 3 and Table 3 for more info.

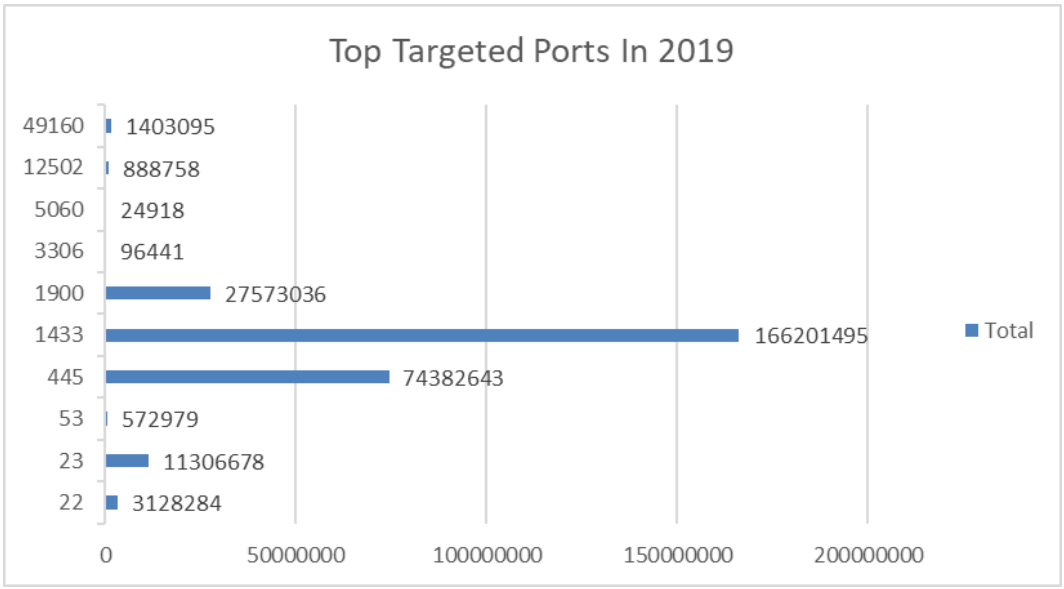
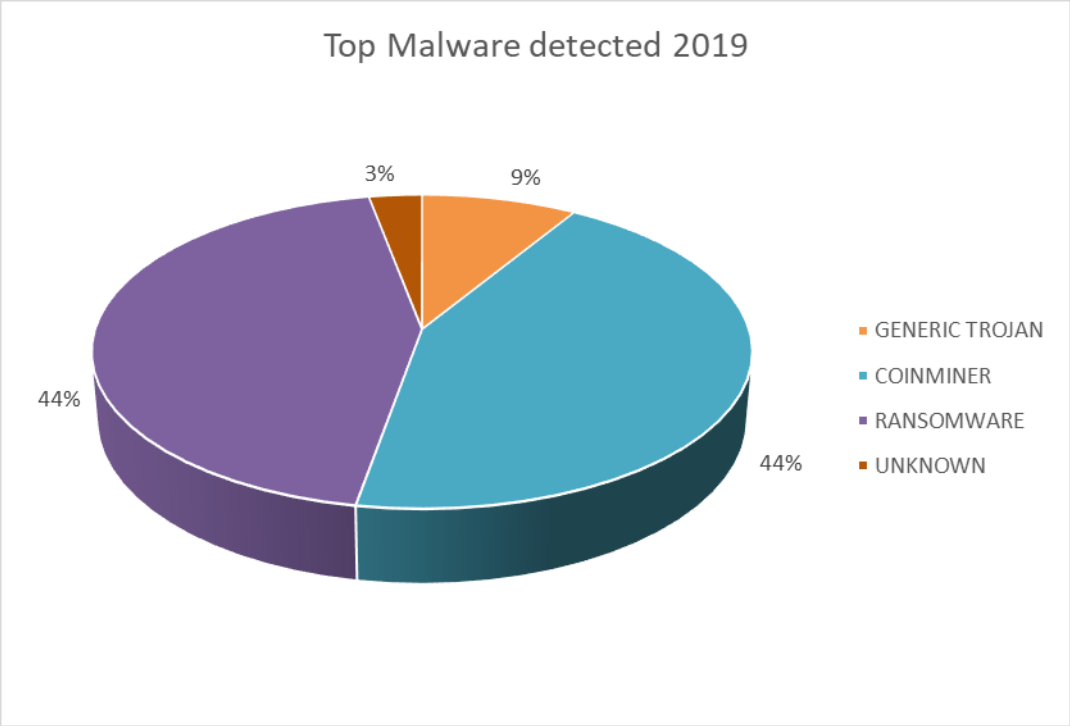


Figure 3

Port	Count
22	3128284
23	11306678
53	572979
445	74382643
1433	166201495
1900	27573036
3306	96441
5060	24918
12502	888758
49160	1403095

Table 3

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



MALWARE TYPE	TOTAL
GENERIC TROJAN	47
COINMINER	237
RANSOMWARE	238
UNKNOWN	16
TOTAL	**538**

3. BruCERT Activities in 2019

3.1 Seminars/Conferences/Meetings/Visits

BruCERT attended and presented at various seminars, conferences and meetings related to the field of ICT security.

- On 27th October 2019 until 31st October 2019 - Three BruCERT delegates attended the OIC-CERT AGM and Annual Conference 2019 which takes place at Muscat, Oman, hosted by OMAN CERT.
- On 29th September 2019 until 2nd October 2019 - Two BruCERT delegates attended the APCERT AGM and Annual Conference 2019 which takes place at Singapore, hosted by SingCERT.

3.2 Awareness Activities

3.2.1 Cyber Battle : Capture The Flag 2019 and Awareness Talk

August 3 2019

BruCERT/ ITPSS Sdn Bhd has the pleasure of hosting the 5th annual **Cyber Battle: Capture The Flag** (CTF), a hacking competition which aims to highlight the importance of cybersecurity, and the increasing need for information security specialists in Brunei.

Participants will attempt to solve challenges in a variety of real-life scenarios, in a race against time to obtain 'flags' and submit them on the CTF scoring server.

For the first time, this year the competition is also open to solo participants!

BtCIRT

Bhutan Computer Incident Response Team – Bhutan

1. Highlights of 2019

1.1 Summary of major activities

In 2019, BtCIRT conducted security workshops, published articles and alerts on latest cyber trends, threats, vulnerabilities and best practices. BtCIRT also conducted vulnerability assessment, post-incident analysis, and awareness programs.

1.2 Achievements & milestones:

- Workshop on Secure Coding conducted.
- Child Online Protection: survey was conducted in 45 schools with 2400 students aged ranging from 12 to 17 to understand the overall situation of students on cyberspace. The survey also looked at how prepared students are to tackle issues they face online including intrusion of their privacy, cyberbullying.

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's mandate was approved by the Lhengye Zhungtshog/Cabinet on 20 May 2016 formally identifying the team as the national focal point for cybersecurity activities and initiatives.

2.3 Resources

Currently, BtCIRT consist 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.

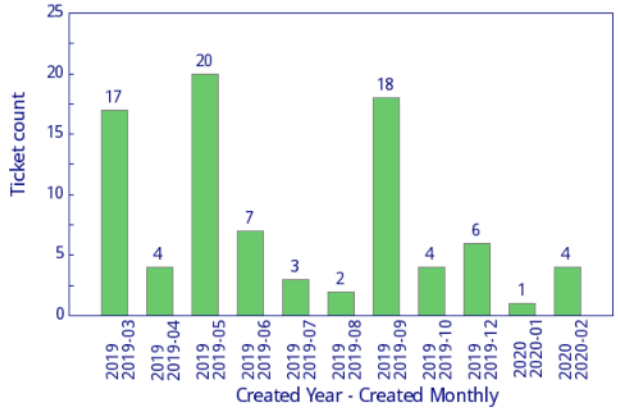
3.2 Incident Handling Report

This year saw a decrease in the number of incidents handled by the BtCIRT as compared to 2018 with 81 total incidents. This is attributed to frequent trainings and workshops on security related topics for the government and corporate ICT Officials.

131 government websites were assessed for security vulnerabilities and security flaws.

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

The following graphs provide a number of incidents resolved on a monthly basis in 2019. It also depicts the types of incidents resolved by the team during the year.



Created Year	Created Monthly	Ticket count
2019	2019-03	17
	2019-04	4
	2019-05	20
	2019-06	7
	2019-07	3
	2019-08	2
	2019-09	18
	2019-10	4
	2019-12	6
2020	2020-01	1
	2020-02	4
Total		86

3.3 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 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 is also sent out to government and critical sector ICT officials to notify possible attacks as and when it is detected.

4. Events organized / hosted

4.1 Training/Workshops, Drills & exercises

i. The BtCIRT presented on the various cyber security initiatives of the government, challenges and technical recommendations to around 300+ ICT officials (Private, government and corporate sectors) at the annual BtNOG (Bhutan Network Operator's Group) Conference on 3rd June, 2019. The presentation was a good initiative in expanding the reach of the team and its mandates and to create awareness on cybersecurity in the country.

ii. A workshop on Secure Coding was conducted from 19th to 23rd August 2019 for 50 participants involving ISPs, Banks, Colleges, Pvt Sectors, and Government Agencies.

iii. BtCIRT participated in the annual APCERT drill on the theme "Catastrophic Silent Draining in Enterprise Network". This year's scenario was inspired by a latest security attack on an organization, which relates to the vulnerability that could allow attackers to completely take over vulnerable websites to deliver malware backdoor and cryptocurrency miners.

iv. The BtCIRT presented on the theme "Managing Cyber Security Risk and Mitigation in Bhutan" at the Annual ICT Conference on 2nd December 2019, further improving the reach of the team and its mandates.

5. International Collaboration

5.1 International partnerships and agreements

BtCIRT is a member of two international organisations, Asia Pacific Computer Emergency Response Team (APCERT) and Forum of Incident Response and Security Teams (FIRST) as of now.

5.2 Capacity building

5.2.1 Seminars & presentations

BtCIRT has attended following conference/seminars/workshops:

- APAN48-CSIRT Capacity Building in Asia: TRANSITS I

6. Future Plans

i. BtCIRT also looks forward to collaborating with more organisations internally and internationally to strengthen its cooperation.
ii. Conduct awareness programs in schools and colleges and through media outlets.
iii. Establish new cyber policies and standards and strengthen existing ones.

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.

CCERT

CERNET Computer Emergency Response Team - People's Republic of China

1. About CCERT

1.1 Introduction

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

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

1.2 Establishment

China Education and Research Computer Network Emergency Response Team (CCERT) was founded in May 1999 and is the earliest CERT in China.

1.3 Resources

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

1.4 Constituency

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

2. Activities & Operations

2.1 Scope and definitions

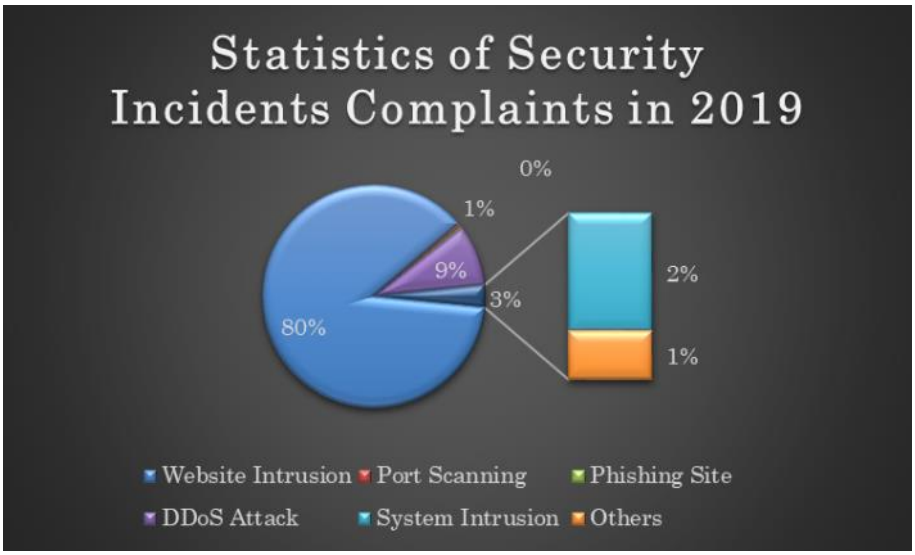
Currently, CCERT mainly deal with security events for CERNET users, which include:

- CERNET Network Monitoring
- Complaint from Other CERT Organizations

- Information Sharing with Other Security Manufacturers

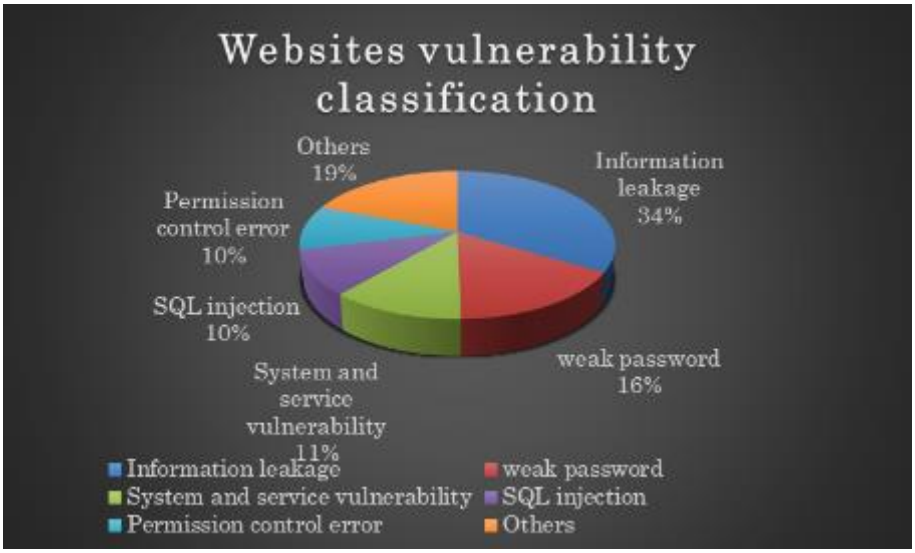
2.2 Incident handling reports

In 2019, CCERT handled 3400 security incident complaints, which include 2965 for Website Intrusion, 13 for Port Scanning, 11 for Phishing Site Complaints, 305 for DDoS Attack, 75 for System Intrusion and 31 for other network security complaints.



2.3 Abuse statistics

Through the analysis of 2965 website attacks, we classified the types of website security vulnerabilities. For details, please refer to the following figure:

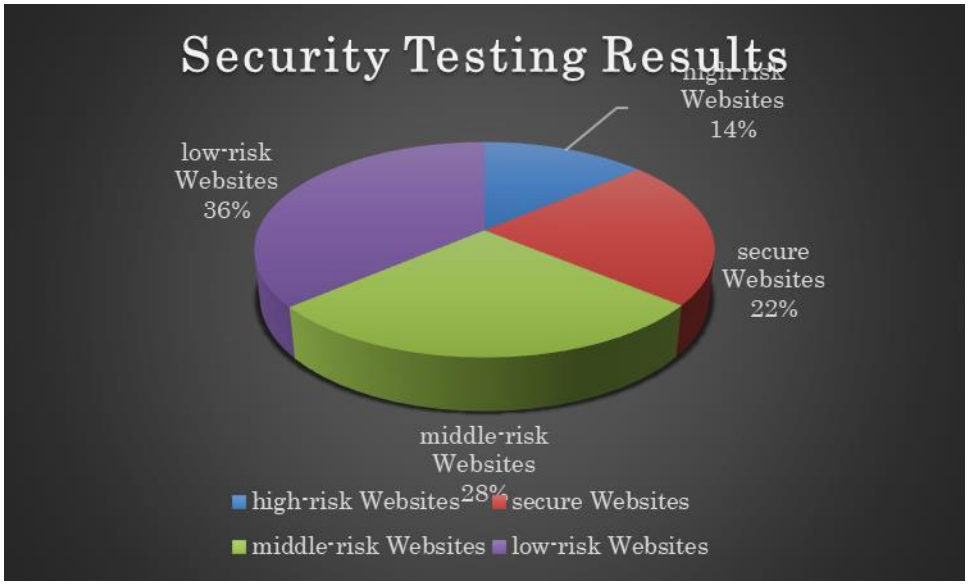


2.4 Publications

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

2.5 Security services

In 2019, CCERT provided security scanning service (free of charge) to 2522 websites. and found that there are about 589 websites with high-risk vulnerabilities (14%), 1192 websites with middle-risk vulnerabilities (28%), and 1561 websites with low-risk vulnerabilities (36%). No security problem was detected on 961 websites (22%)



3. Events organized / hosted

3.1 Training

Organized 6 trainings, which includes:

- Network Security and Strategies
- Network security emergency response
- Network security emergency drill
- DNS Security on IPv6
- Privacy Data Protection
- Data security of University Users

3.2 Conferences and seminars

- Attend the 26th annual meeting of CERNET Users, January 12th, 2019,Hangzhou
- China Network Security annual meeting 2019, July 17th, 2019, Guangzhou
- Internet Security Conference 2019, August 19th, 2019, Beijing
- Attend the Informationization Security Annual Meeting of Colleges and Universities, 6 December 2019, Xi`an

4. Future Plans

4.1 Future projects

- Strengthen team building for CCERT
- Enhancing the Construction of CERNET Security System

4.2 Future Operation

In 2020, CCERT will keep devoting to network security emergency response work and strengthen the cooperation with other security organizations, so as to make more contribution to Internet security.

CERT-In

Indian Computer Emergency Response Team – India

1. Highlights of 2019

1.1 Summary of major activities

iv. In the year 2019, CERT-In handled 394499incidents. The type of incidents handled were Website Intrusion & Malware Propagation, Malicious Code, Phishing, Distributed Denial of Service attacks, Website Defacements, Unauthorized Scanning activities and vulnerable service. Remedial measures for handling incidents were suggested and implemented in coordination with relevant stakeholders.

v. CERT-In tracks latest cyber threats and vulnerabilities. 204 security alerts, 38 advisories and 202 Vulnerability Notes were issued during the year 2019.

vi. CERT-In conducted 23 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.

vii. CERT-In participated as a player in 3 International cyber security drills and in 1 bilateral cyber crisis simulation exercise in 2019.

viii. CERT-In is in a convener of two APCERT working groups namely IoT Security and Secure Digital Payments.

1.2 Achievements & milestones

- Indian Computer Emergency Response Team is conducting cyber security exercises comprising of tabletop 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 **12** such exercises were conducted in 2019.
- In 2019, CERT-In signed Memorandum of Understandings (MoUs) on cyber security cooperation with three countries namely Finland, Estonia and South Korea to enable information sharing and collaboration for incident resolution.
- CERT-In has set up its own automated Threat Information and Intelligence sharing platform for sharing Indicators of Compromise (IoCs) among its stake holders for

taking immediate remedial actions.

- CERT-In has operationalized its Threat and Situational Awareness Project to generate necessary situational awareness of existing and potential cyber security threats and enable timely information sharing for proactive, preventive and protective actions by individual entities.

2. About CERT-In

2.1 Introduction

CERT-In is a functional organization 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

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 2019 is given in the following table:

Activities	Year 2019
Security Incidents handled	394499
Security Alerts issued	202
Advisories Published	38
Vulnerability Notes Published	204
Trainings Organized	23

Table 1: CERT-In Activities during year 2019

3.3 Abuse statistics

In the year 2019, CERT-In handled **394499** incidents. The types of incidents handled were Website intrusion & Malware propagation, Malicious Code, Phishing, Distributed Denial of Service attacks, Website Defacements, Unauthorized Scanning activities and Vulnerable Services.

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

Security Incidents	2019
Phishing	472
Unauthorized Network Scanning/Probing/Vulnerable Services	305276
Virus/ Malicious Code	62163
Website Defacements	24366
Website Intrusion & Malware Propagation	417
Others	1805
Total	394499

Table 2: Breakup of Security Incidents handled

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

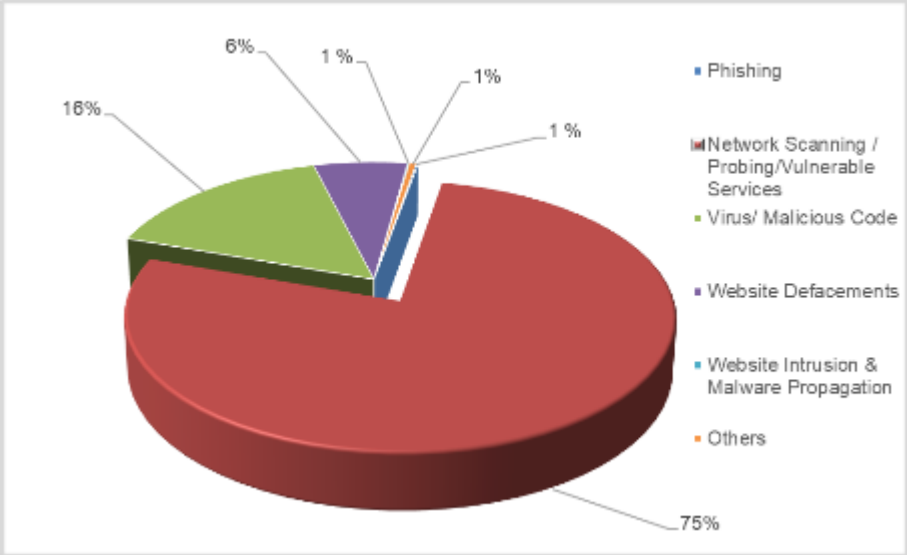


Figure 1: Summary of incidents handled by CERT-In during 2019

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 24366 numbers of defacements have been tracked.

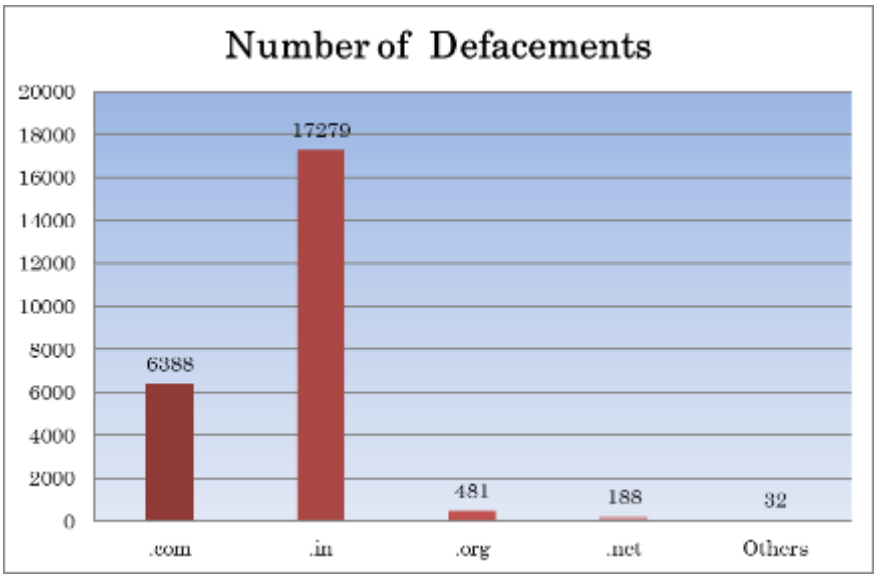


Figure 2: Indian Website Defacements tracked by CERT-In during 2019

3.3.2 3Botnet Cleaning Initiatives

Botnet Cleaning and Malware Analysis Centre (Cyber Swachhta Kendra - www.cyberswachhtakendra.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, academia and Industry.

Botnet Cleaning and Malware Analysis Centre shares data of infected systems with the Internet Service Providers (ISPs) for sending notification to citizens. Free Bot removal tools have been provided for citizens on the website. The number of downloads of the tools by users during the year 2019 are as follows:

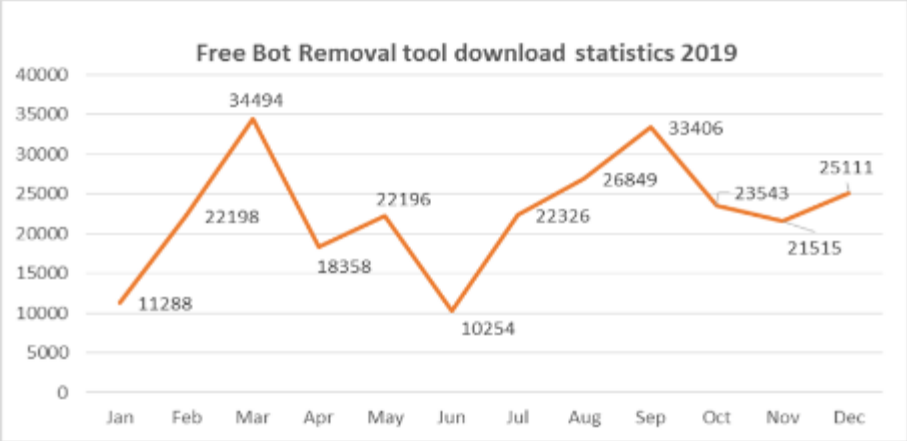


Figure 3: Free botnet removal tools download statistics 2019

Botnets events processed by Botnet Cleaning and Malware Analysis centre (Cyber Swachhta Kentra) during 2019.

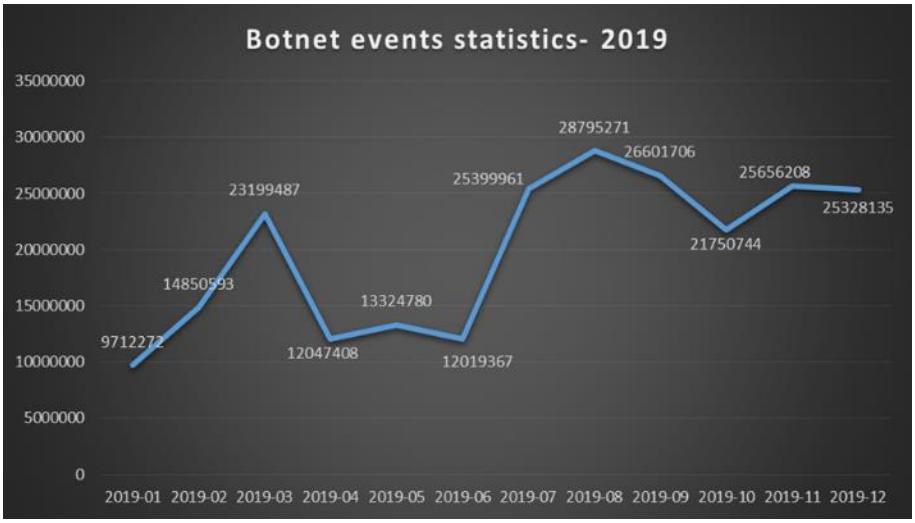


Figure 4: Botnet events tracked by Botnet Cleaning and Malware Analysis Centre

3.3.3 Security Profiling, Assurance framework and Audit Services

- Under Security Assurance Framework, CERT-In has empaneled 90 technical IT security auditors to carry out information security audit, including the vulnerability assessment and penetration test of the network infrastructure of government and critical sector 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 empaneled 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.

4. Events organized / hosted

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. In 2019, CERT-In conducted 23 trainings on various specialized topics of cyber security. The target audience includes system/Network Administrators, Database Administrators, Application Developers, IT Managers, Chief Information Security Officers (CISOs)/ Chief information officers (CIOs), and IT Security professional.

4.2 4Cyber 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 12 such cyber security exercises in 2019.

4.3 Cyber Forensics

CERT-In is equipped with the tools and equipment to carry out retrieval and analysis of the data extracted from the digital data storage devices using computer forensics and

mobile device forensic techniques. CERT-In's facility for Digital Forensics data extraction and analysis is being utilized in investigation of the cases of cyber security incidents, submitted by central and state government ministries, departments, public sector organizations, law enforcement agencies, etc. CERT-In imparts training through workshops organized by CERT-In on computer forensics and mobile device forensics through lectures, demonstrations and hands on practical sessions, which covers seizing, preservation, imaging and analysis of the data retrieved from the digital data storage devices. CERT-In also provides support to the other training institutes in imparting training by delivering lectures with demonstrations on various aspects of cyber forensics.

5. International Collaboration

5.1 International partnerships and agreements

Strengthening International cooperation to effectively deal with cyber security issues has been one of the main focus areas of the Government. As such, this aspect is being dealt with by way of security cooperation arrangements in the form of Memorandum of Understandings (MoU) 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 2019, CERT-In signed MoU on cyber security cooperation with three countries namely Finland, Estonia and South Korea 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.

5.2 Drills & exercises

CERT-In played the role of EXCON and also participated as a player in APCERT Drill 2019 conducted in July 2019 based on the theme "**Catastrophic Silent Draining in Enterprise Network**" to test the response capability of leading Computer Security Incident Response Teams (CSIRT) from the Asia Pacific economies. The objective was to enables CERTs to review, practice and strengthen computer security incident handling mechanism and exercise coordination with multiple parties (internal and external) when handling computer security incidents.

CERT-In participated in the ASEAN CERTs Incident Response Drill (ACID) in September 2019 wherein the objective was strengthening cyber security preparedness of

ASEAN member states and Dialogue partners in handling cyber incidents and reinforce regional coordination to test incident response capabilities. The theme of the drill was "**Combat Evolving Cyber Threats with Good Cyber Hygiene**".

CERT-In participated in The Organisation of The Islamic Cooperation – Computer Emergency Response Teams (OIC-CERT) drill in September 2019. The theme of the drill was "**The Rise of Malware Intelligence**".

5.3 Other international activities

- CERT-In participated in Asia Pacific Regional Internet Conference on Operational Technologies (APRICOT) Conference and APCERT SC Meeting from 24 to 28 February 2019 at Kathmandu, Nepal.
- CERT-In participated in the Asia Pacific Computer Emergency Response Teams (APCERT) Annual General Meeting (AGM), Steering Committee (SC) Meeting and Conference 2019 from 29 September to 2 October 2019 at Singapore.
- CERT-In is participating and actively contributed as task force member in the Cyber Incident Management and Critical Information Protection working group of the Global Forum for Cyber Expertise (GFCE), a global platform for countries, international organization and private companies to exchange best practices and expertise on cyber capacity building by identifying successful policies, practices and ideas so as to multiply these on a global level.
- CERT-In conducted a Tabletop Exercise for the participants of the GFCE. The theme was "Cross border, cross sector collaboration for countries cyber incidents.
- CERT-In is participating and actively contributing as a member in the Financial Stability Board (FSB) Working Group on Cyber Incident Response and Recovery (CIRR), to develop guidance and policies related to cyber resilience and cyber security. The FSB was created by G20 to coordinate at the international level the work of national financial authorities and international standard setting bodies and to develop and promote the implementation of effective regulatory, supervisory and other financial sector policies in the interest of financial stability.

Contact Information

Postal Address:

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

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: 0x3386DBA0
- Key Type: RSA
- Expires: 2020-05-23
- Key Size: 4096/4096
- Fingerprint: 4604 0698 6802 80E4 13E0 091D 4C31 F91E 643B 5C9F

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:

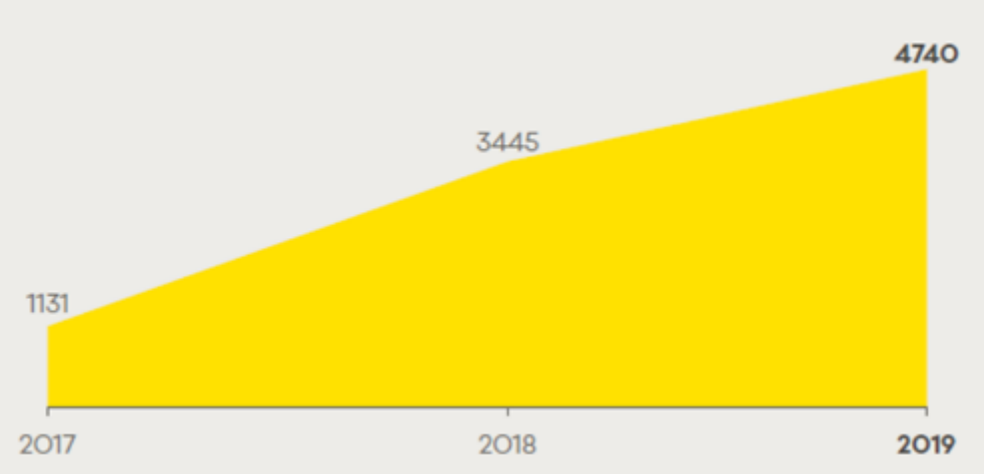
- User ID: info@cert-in.org.in
- Key ID: 0x1EFC37E1
- Key Type: RSA
- Expires: 2020-05-23
- Key Size: 4096/4096
- Fingerprint: 9486 28E6 0268 8DD2 47AF DE72 579D 0C18 CCA2 0F32

CERT NZ

CERT NZ – New Zealand

1. Highlights of 2019

- The total number of incidents reported to CERT NZ during 2019 was 4,740, an increase of 38% on 2018.



- CERT NZ's key annual awareness-raising activity, Cyber Smart Week, was held for the third year running, on 14 to 18 October 2019. The overarching theme was 'Think you're secure online? Make sure of it.', and 122 partners joined us in promoting the four simple steps all New Zealanders could take to be more secure online. Partner reporting showed approximately 5 million impressions had been achieved.
- CERT NZ continues to strengthen its partnerships in the Pacific, including active engagement 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 23 FTEs, including operations, communications & engagement, governance & analytical reporting staff. CERT NZ also has a contact centre to receive incident reports.

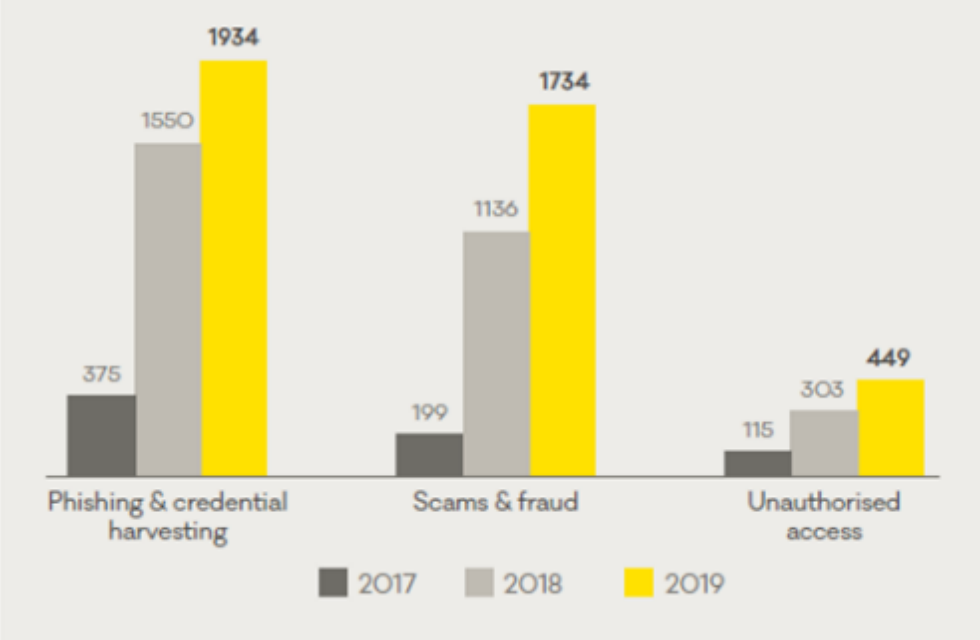
3. Activities & Operations

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 oragnisations, with the reporter's consent.
- **Response coordination**: We lead the response to some incidents, coordinate the response to others and we support the national emergency response process.
- **Readiness support**: We raise awareness of cyber security risks, mitigations and impacts and deliver up-to-date, actionable advice on cyber security best practice.

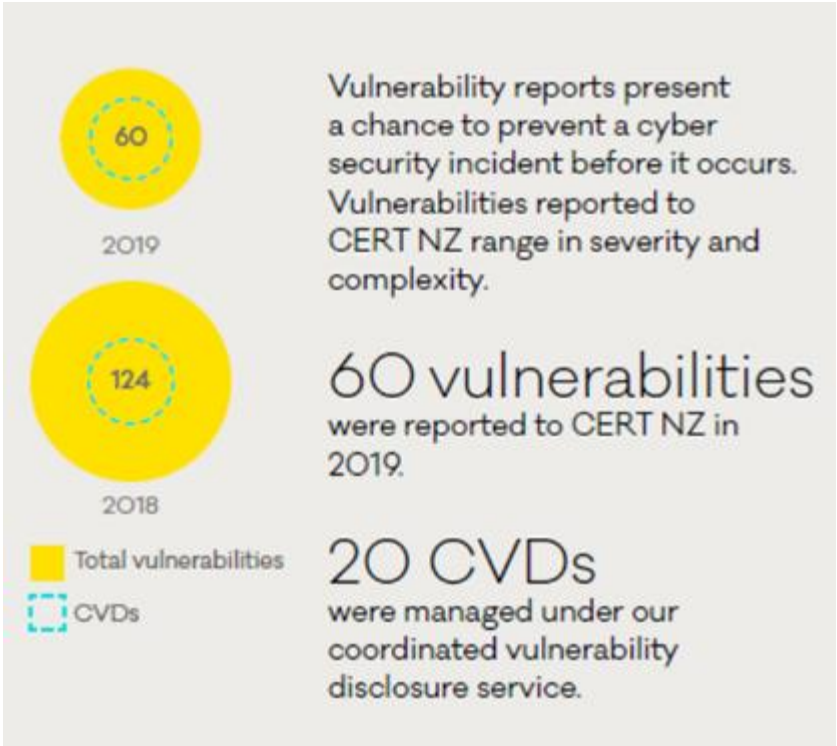
3.2 Top incident categories

Phishing and credential harvesting; scams and fraud; and unauthorised access represent the largest number of incidents reported to CERT NZ in 2019. Reports of phishing and credential harvesting incidents were up 25% on 2018, scams and fraud had the largest proportionate increase (53%) on 2018, with unauthorised access reports increasing by 48%.



3.3 Vulnerability reporting

In 2019 60 vulnerabilities were reported to CERT NZ, 20 of which were managed under CERT NZ's Co-ordinated Vulnerability Disclosure (CVD) service. The CVD policy is used when the person reporting the vulnerability doesn't want, or has been unable, to contact the vendor directly themselves.



4. Publications

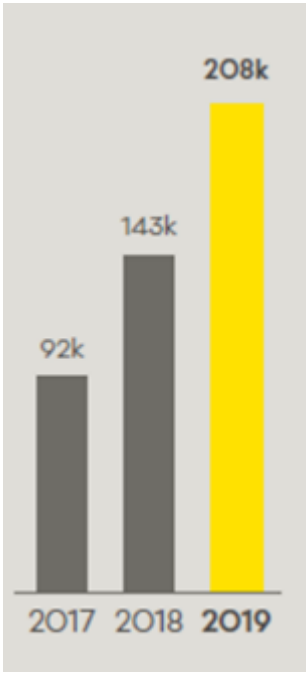
4.1 Advisories

CERT NZ publishes two types of public advisories – one for everyday New Zealanders, and one for a more technical audience. The former is targeted at the general public, media and for organisations to communicate with their customers or staff. The latter has more technical detail and readers are assumed to understand industry-specific jargon. CERT NZ determines what type of advisory to publish according to the type of threat and its relevance to a particular audience.

In 2019 CERT NZ published five advisories for everyday New Zealanders and nine to IT specialists.

4.2 Website

Visits to the cert.govt.nz website were 208,000 in 2019 – a 45% increase on 2018. The most popular page for IT specialists was the advisories page, with 38,000 page views. For businesses and individuals the top guides were the *Top 11 cyber security tips for your business and Keep your data safe with a password manager*.



4.3 Quarterly reports

CERT NZ's quarterly reporting continued in 2019, 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.

Accompanying the Quarter 4 report is the 2019 Report Summary, giving an overview of what CERT NZ has seen and done in 2019.

These reports include high level analysis, deep dives into trending issues, case studies and details of the numbers of cases being referred to partner agencies. This allows others to learn from CERT NZ's incident data, and the information received from the international CERT community.

4.4 Quarterly news updates

CERT NZ produces a subscription-based e-newsletter that is sent out quarterly, providing subscribers with first access to the CERT NZ quarterly reports, information on recent threats, and updates on new content available from CERT NZ.

4.5 CERT NZ social media

CERT NZ's Twitter account @CERTNZ, is an important and growing information sharing channel.

4.6 CERT NZ Critical Controls

To help organisations and IT specialists prioritise their security controls, CERT NZ's provides ten critical controls annually, based on the incident data received that year. These controls would prevent, detect, or contain most of the attacks CERT NZ sees in the past year.

4.7 Other publications

CERT NZ has produced a range of resources help keep New Zealanders safe online, such as 11 tips for businesses to protect themselves online and Cyber Security Risk Assessments for business.

5. Events

5.1 Campaigns

CERT NZ ran its third cyber security awareness campaign, Cyber Smart Week, in October 2019, with the overarching theme of 'Are you secure online? Make sure of it.' 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.

98% of respondents to the 2019 campaign survey said they would take part again in 2020.

In March 2019, 95 organisations partnered with CERT NZ to help spread the word about

'getting password smart'. Partners used campaign content in their e-newsletters, on social media, for events, and on websites.

6. International Collaboration

6.1 International partnerships and agreements

CERT NZ is a member of the Asia Pacific CERT forum (APCERT), the Forum of Incident Response Teams (FIRST), the International Watch and Warning Network (IWWN) and the Pacific Cyber Security Operational Network (PACSON). We have also signed a number of bilateral agreements with counterpart CERTs.

7. Capacity building

7.1 Training

CERT NZ has been selected to convene the recently established 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.

7.2 Drills & exercises

CERT NZ participated in the APCERT Drill in 2019.

7.3 Seminars & presentations

Key presentations made by CERT NZ in 2019 included:

- PaCSON, May 2019
- IWWN, June 2019
- NatCSIRT, June 2019
- APCERT, September 2019
- ACSC conference, September 2019

8. Future Plans

8.1 A budget increase received in 2019 means CERT NZ can grow the team and expand our services, particularly in the data, outreach and incident response areas.

9. Conclusion

CERT NZ is now established and in a growth phase. Alongside our aim of helping all New Zealanders better understand and stay resilient to cyber attacks, we maintain a strong focus on developing and fostering our international partnerships so that we can contribute to greater global cyber security.

Contact Information

Website:

www.cert.govt.nz

Twitter:

@CERTNZ

By post:

CERT NZ

PO Box 1473

Wellington 6140

By phone (to report an incident):

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

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 was founded in 2001 and became a member of FIRST and one of the founders of APCERT. As of 2019. CNCERT has established "CNCERT International Cooperation Partnership" with 260 teams in 78 countries and regions.

1.3 Workforce power

CNCERT, 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 strives to improve the nation's cybersecurity posture and protect critical infrastructure cybersecurity. CNCERT 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 2019, CNCERT received a total of about 107.8 thousand incident complaints, a 1.0% increase from the previous year. And among these incident complaints, 588 were reported by overseas organizations, making a 13.1% down from the year of 2018. As shown in Figure 2-1, most of the victims were plagued by vulnerabilities (31.3%), malware (25.8%) and phishing (21.5%). Vulnerabilities overtook Malware to be the most complained about category.

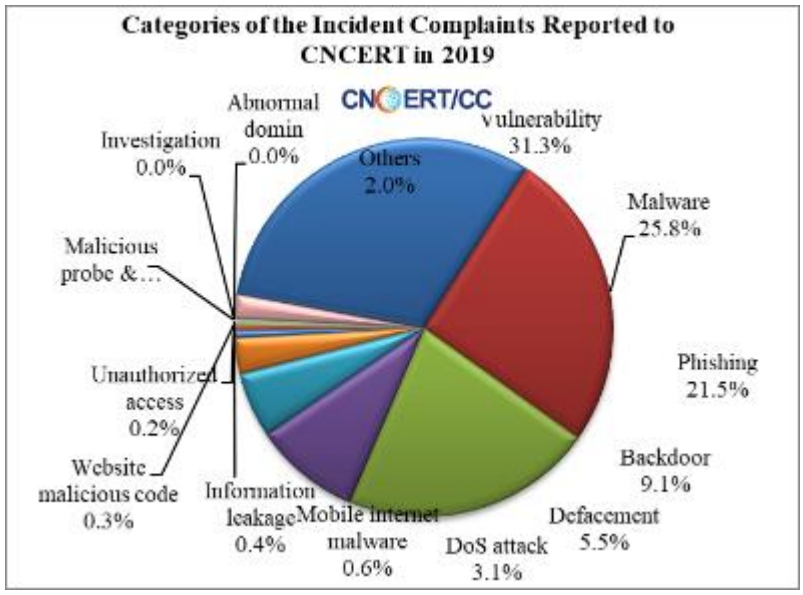


Figure 2-1Categories of the Incident Complaints Reported to CNCERT in 2019

In 2019, CNCERT handled almost 107.6 thousand incidents, a rise of 3.9% compared with that in 2018. As illustrated in Figure 2-2, vulnerability (31.3%) dominated the chart about categories of the incidents handled by CNCERT in 2019, followed by malware (25.8%) and phishing (21.5%).

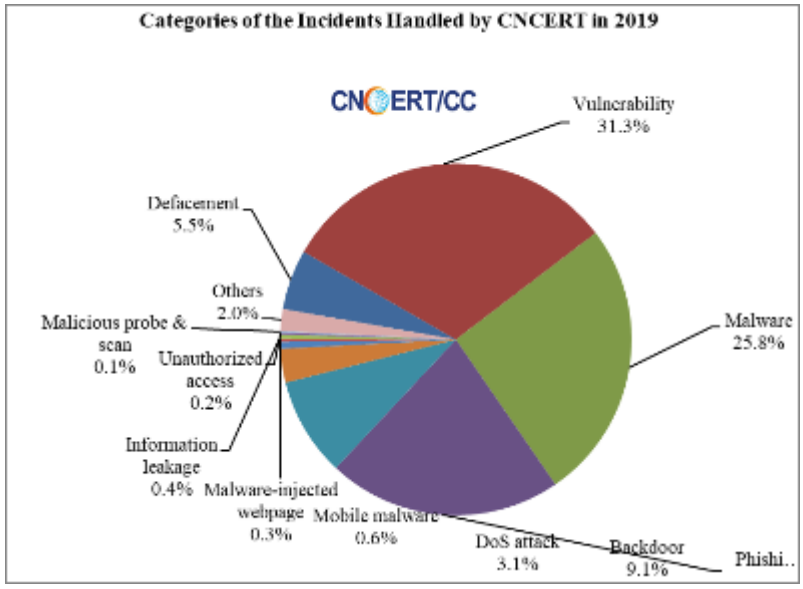


Figure 2-2 Categories of the Incidents Handled by CNCERT in 2019

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 11.3% compared with that in 2018. We saw more than 88.2 thousand overseas C&C servers which increased by 78.3% from 2018. 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 Japan, British and India.

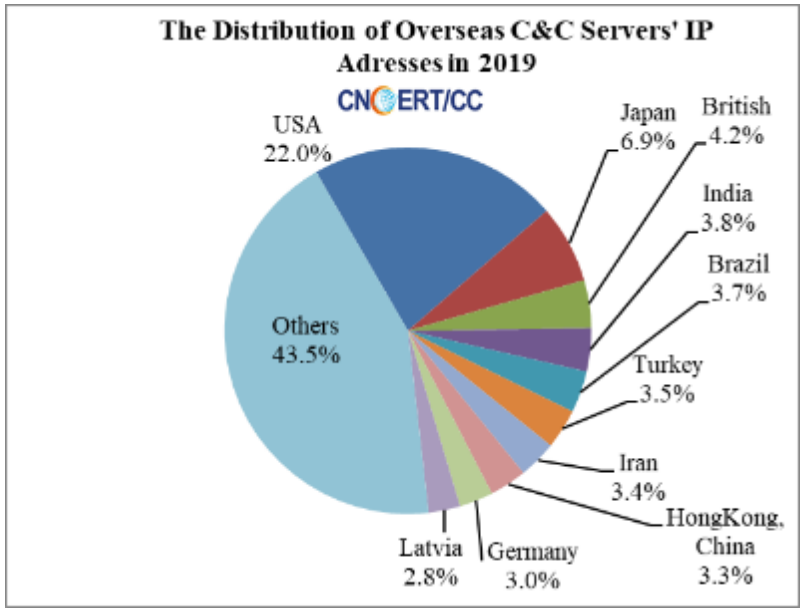


Figure 2-3 Distribution of overseas C&C servers' IP addresses in 2019

By CNCERT's Conficker Sinkhole, over 10.5 million hosts were suspected to be compromised all over the world, among which 2.0 million were located in mainland China. As shown in Figure 2-4, mainland China (19.3%) had the most infection, followed by India (8.2%), and Russia (4.7%).

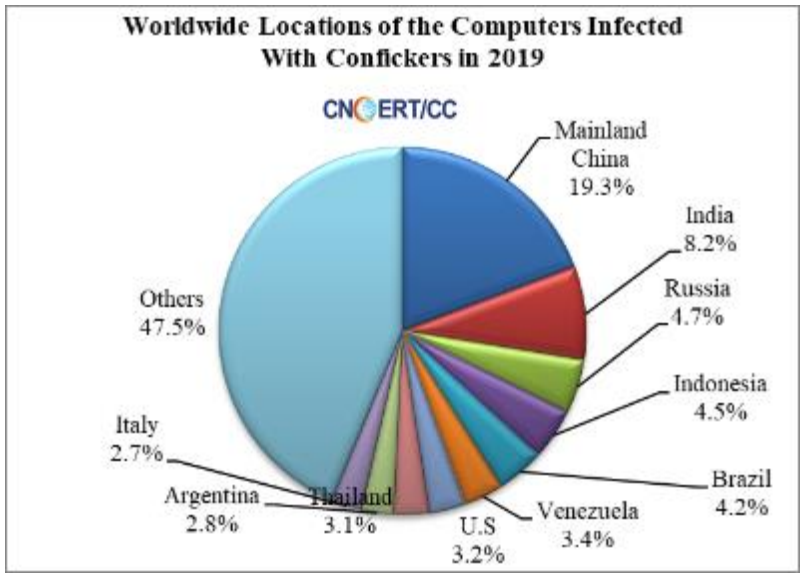


Figure 2-4 Worldwide Locations of the Computers Infected with Conficker in 2019

Malware-hosting websites are the jumping-off places for malware propagation. The malware-hosting websites monitored by CNCERT in 2019 involved about 424 thousand domains, 202 thousand addresses and 1.5 million malware download links. Among the 424 thousand malicious domains, 74.4% of their TLDs fell into the category of .com. Among the 202 thousand malicious IPs, 20.8% were located overseas.

2.3 Website Security

About 185.6 thousand websites in mainland China were defaced, an increase of 2532.6% compared with that in 2018, including 515 government sites. Besides, about 84.9 thousand websites in mainland China were detected to be planted with backdoors and secretly controlled, out of which 717 were government sites.

In 2019, CNCERT found about 84.7 thousand phishing sites targeting the websites in mainland China. About 7.1 thousand IPs were used to host those fake pages, and 95.8% were out of mainland China. Most of the phishing servers (19.3%) were located in U.S.

CNCERT found almost 40.7 thousand overseas IPs conducting remote control on over 80.1 thousand websites in mainland China. As shown in Figure 2-5, 13,628 (33.5%) were

located in the U.S., followed with 4,644 (11.4%) in Britain and 3,198 (7.9%) in Hong Kong, China.

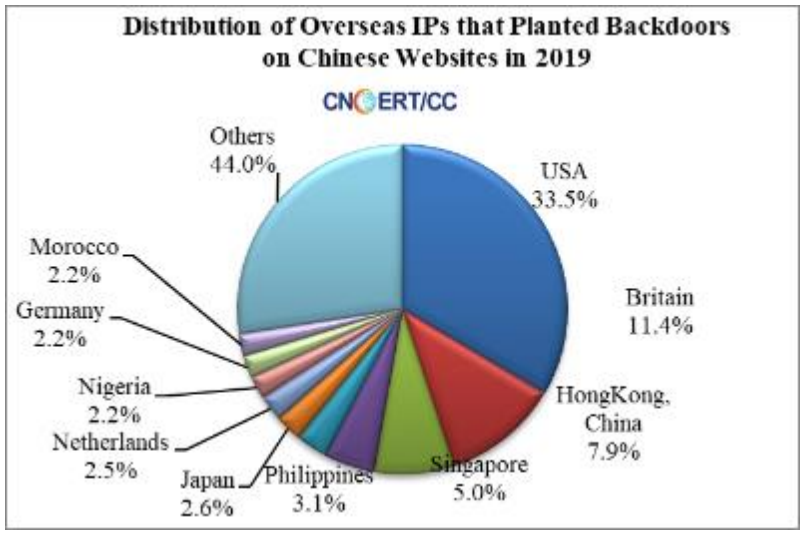


Figure 2-5 Distribution of Overseas IPs that Planted Backdoors on Chinese Websites in 2019

2.4 Mobile threats

In 2019, CNCERT collected about 2.79 million mobile malware samples in total. In terms of the intentions of these mobile malware, rogue behavior took the first place (36.1%), fee consumption (33.2%) secured the second rank, and the next two were those intended for stealing privacy and malicious fee deduction for 11.6% and 9.8% respectively.

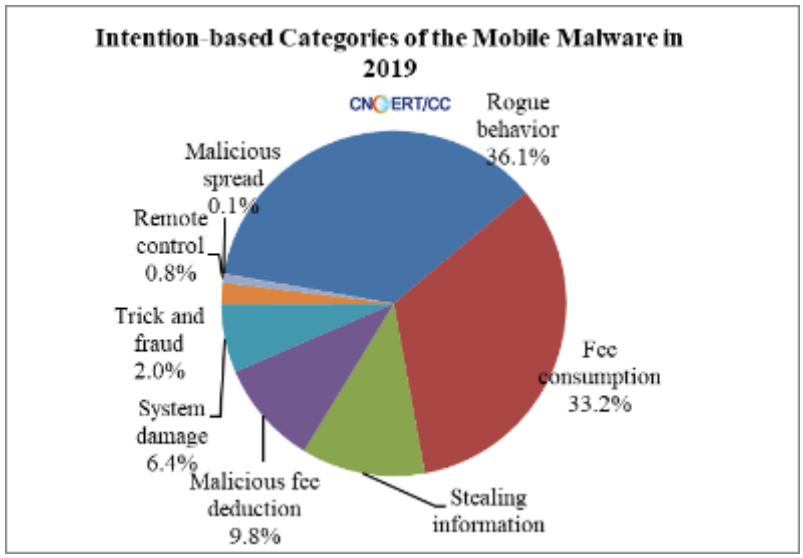


Figure 2-6 Intention-based Categories of the Mobile Malware in 2019

All of these mobile malwares identified by CNCERT ran on Android system, recording

about 0.12 million (100.0%).

3. Events organized/co-organized

3.1 Conferences

The 2019 CNCERT Annual Conference in Beijing

On July 17th, 2019, CNCERT held the 2019 Annual Chinese Conference on Computer and Network Security in Guangzhou. Focusing on the theme "To enhance Intelligent Situation Awareness for Cyber Security", 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 bridge for communication between network security and all sectors of society.

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

From Aug 27th to 28th, 2019, the Seventh China-Japan-Korea CSIRT Annual Meeting for Cybersecurity Incident Response was held in Beijing. Hosted by CNCERT/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 6th World Internet Conference: The Business Leader's Dialogue

On 20th October, CNCERT organized the Business Leader's Dialogue of the 6th World Internet Conference in Wuzhen, Zhejiang Province. The dialogue, themed with "Innovative Economy, Shared Community", had an in-depth discussion of the opportunities and challenges that emerge during the development of digital economy. The session, which invited the leading icons from world internet industries to exchange on integration and innovation, was co-hosted by the China Telecommunications Corporation and the World Intellectual Property Organization. More than 300 attendees from various countries and regions joined the dialogue.

The 6th World Internet Conference: Cybersecurity Forum for Technology Development and International Cooperation

On 21st October 2019, CNCERT hosted the Cybersecurity Forum for Technology Development and International Cooperation of the 6th World Internet Conference in Wuzhen, Zhejiang Province. Themed "Gather for Good", this sub-forum focused on two

major fields: development of cybersecurity technology and cybersecurity international cooperation. Through keynote speeches and expert dialogues, the participants exchanged experiences and shared the best practices. It also called on each country and region to work together for a joint force and implement Chinese President Xi Jinping's four principles and five proposals on global development and governance of the Internet.

The roundtable penal of "Cyber Security" of the Third Conference of CICA Non-governmental Forum

On December 19th, 2019, the roundtable penal of "Cyber Security" of the Third Conference of CICA Non-governmental Forum was held in Chongqing. Themed "Openness and Cooperation for Common Security — Jointly Build a Community with a Shared Future in Cyberspace", this roundtable penal offered the participants from foreign CERTs and domestic enterprises a platform to share their thoughts. Broad consensus was made after in-depth exchange of views on international and regional issues concerned by all.

4. Drill attended

APCERT Incident Drill 2019

CNCERT participated in the APCERT 2019 Drill on 31th July, 2019 and completed it successfully. The theme of the APCERT Drill 2018 was "Catastrophic Silent Draining in Enterprise Network". This drill was based on the real events and situations on the Internet, simulated the scene of the security attack on an organization, analyzed and coordinated the vulnerability that could allow attackers to deliver malware backdoor and cryptocurrency miners.

ASEAN CERT Incident Drill (ACID) 2019

On 4th September, CNCERT participated in ASEAN CERT Incident Drill (ACID) 2019. The theme of this drill is"Combat Evolving Cyber Threats with Good Cyber Hygiene". The participants investigated, analyzed and recommended remediation and mitigation measures towards data breach 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.

2019 China-ASEAN Cyber Security online Training

From November 25th to 29th, 2019, CNCERT/CC conducted the three-day field training on cybersecurity in Kuala Lumpur, Malaysia. The training was carried out to implementing the specific measures for China-ASEAN Information Port and the "China-ASEAN Cyber Security Field Training Initiative" adopted by China and ASEAN.

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.

Table 5-1 Lists of CNCERT's publications throughout 2018

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	355	Published on journals and magazines

CyberSecurity Malaysia

CyberSecurity Malaysia – Malaysia

1. HIGHLIGHTS OF 2019

1.1 Summary of major activities

18 February 2019	Participated in Asia Pacific Internet Conference on Operational Technologies (**APRICOT**) & FIRST Technical Colloquium, organised by the Asia Pacific Internet Association (**APIA**), APNIC, and Korea Institute of Science and Technology (**KISTI**) in Daejeon, Korea.
26-29 Feb 2019	Participated in the Cyber Intelligence Asia 7th Annual conference and exhibition, organised by Intelligence-Sec Limited (**UK**) together with Thailand 's National Electronics and Computer Technology Center (**NECTEC**) in Bangkok, Thailand.
27–31 May 2019	Participated in 6th ASEAN-Japan Cybersecurity Capacity Building Centre (**AJCCBC**) training programme in Bangkok, Thailand.
28 – 31 May 2019	Participated in the AUSCERT2019 Cyber Security Conference in Gold Coast, Australia.
25 – 27 Jun 2019	Participated in the ASEAN Capture the Flag (**CTF**) competition in Perth, Australia
31 July 2019	Participated in the APCERT Drill 2019.
17-26 September 2019	Conducted a capacity building training under the Malaysian Technical Cooperation Program (**MTCP**) attended by selected APCERT members titled "Certified Cyber Defender Associate" in Cyberjaya, Malaysia.
4 September 2019	Participated in ASEAN CERT Incident Drill (**ACID**).
17 September 2019	Co-organized the OIC-CERT Cyber Drill with Oman National CERT and 4 APCERT members participated - BruCERT, CERT-IN, and NCCA (IDSIRTII/CC), Sri Lanka CERT/CC.
23-26 September 2019	Organised the Cyber Security Malaysia - Awards, Conference & Exhibition (**CSM-ACE**) 2019 in Kuala Lumpur, Malaysia.
25 September 2019	Organised the National ICT Security Discourse (**NICTSeD**) in Kuala Lumpur, Malaysia.

29 September-2 October 2019	Participated in the APCERT Annual General Meeting (**AGM**) & Annual Conference 2019 in Singapore.
26-29 November 2019	Conducted the OIC-CERT Annual Conference 2019 (In conjunction with The Regional Cybersecurity Week 2019) with the theme "Cybersecurity Revolution" in Muscat, Oman.

2. ABOUT CYBERSECURITY MALAYSIA

2.1 Introduction

CyberSecurity Malaysia is the national cyber security specialist agency under the Ministry of Communications and Multimedia Malaysia (MCMM) with a vision of being a globally recognised National Cyber Security and Specialist Centre by the year 2020. CyberSecurity Malaysia provides specialised cyber security services which among them are:

ix. Cyber Security Emergency Services:
- Security Incident Handling; and
- Digital Forensic.

x. Security Quality Management Services:
- Security Assurance; and
- Information Security Certification Body.

xi. Cyber Security Professional Development and Outreach:
- Info Security Professional Development; and
- Outreach.

xii. Cyber Security Strategic Engagement and Research:
- Government and International Engagement; and
- Strategic Research.

xiii. 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 (**MCMM**). CyberSecurity Malaysia is committed in providing a broad range of cyber security 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 cyber space.

2.3 Cyber Security Incident Management

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

MyCERT operates the Cyber999 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 viewed 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 cyber security incidents that threatens their 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/portal/full?id=9eb77829-7dd4-4180-814f-de3a539b7a01

MyCERT's Cyber999 help centre, has responded to approximately 10,772 incidents since establishment. Majority of the incidents reported in 2019 were related to 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 (**CTRC**). The centre has been in operation since December 2009 and functions as a research network for analysing malware and cyber security threats. The centre conducts research and development work for mitigating malware threats, producing advisories, monitoring threats and collaborating with other malware research bodies.

2.3.3 Constituency

CyberSecurity Malaysia's constituency is the Internet users in Malaysia. Cyber security 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

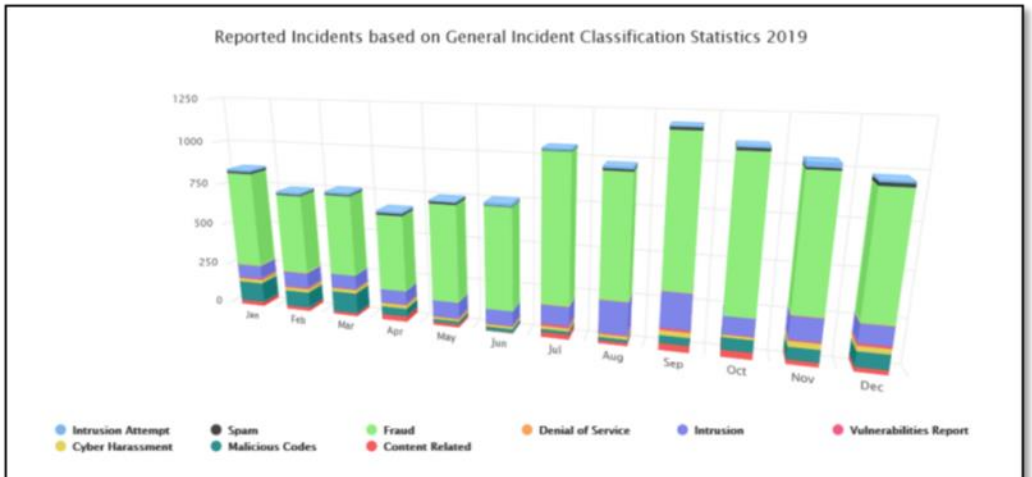
3.1 Incident Handling Reports and Abuse Statistics

CyberSecurity Malaysia receives reports from various parties within its constituency as well as from other constituencies. These include 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's staff.

CyberSecurity Malaysia through MyCERT in 2019 had proactively produced 18 advisories and 25 alerts to inform its constituency on issues relating to cyber security. The specific list of the advisories, alerts and summary reports can be viewed at: https://www.mycert.org.my/portal/advisories2019

There was a decreased in intrusion incident in 2019 as compared to 2018. Most of the incidents reported were related to fraud. This was followed by intrusion.

The following chart shows the reported incidents managed by CyberSecurity Malaysia for 2019:



#	JAN	FEB	MAC	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC	TOTAL
Intrusion Attempt	6	9	10	9	6	11	5	9	4	6	20	9	104
Spam	12	7	8	10	10	5	5	11	15	17	13	16	129
Fraud	567	472	477	447	570	594	846	698	835	851	735	682	7,774
Denial of Service	2	1	1	1	1	0	1	3	3	2	3	1	19
Intrusion	81	92	84	82	93	89	111	188	205	100	129	105	1,359
Vulnerabilities Report	9	7	2	3	5	4	16	8	13	3	7	14	91
Cyber Harassment	21	22	23	22	13	17	18	17	28	14	34	31	260
Malicious Codes	121	97	123	49	19	20	20	19	47	70	70	83	738
Content Related	26	22	20	32	19	4	28	18	39	40	24	26	298
	845	729	748	655	736	744	1,050	971	1,189	1,103	1,035	967	10,772

Chart 1: Reported Incidents in 2019

Further information on Cyber999 statistics can be viewed at:
https://www.mycert.org.my/portal/statistics-2019

3.2 Cyber Threat Research Centre (CTRC)

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

Other activities at 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 organizations.

3.3 Lebahnet Project

Lebahnet which is under CTRC is a part of the Honeynet project where a collection of distributed honeypots to study how exploits function 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 allow researchers to detect, monitor and counterattack malicious activity by understanding activities completed during intrusion phase and attacks' payload.

The URL of the Lebahnet project is as the following:

https://dashboard.honeynet.org.my/

4. EVENTS INVOLVEMENT AND ACHIEVEMENTS

CyberSecurity Malaysia actively participated in cyber security events such as trainings, seminars, conferences and meetings. The agency has contributed its competencies in the following events.

4.1 Cyber Drills

CyberSecurity Malaysia, participated in three (3) cross-national Cyber Drills in 2019 namely the APCERT Drill, the ACID Drill, and the OIC-CERT Drill. The agency was the Exercise Controller of the Malaysia National Cyber Drill.

4.2 Trainings

Several workshops or hands-on training were conducted by CyberSecurity Malaysia in 2019. One of the topics is "Honeynet Data Analysis through LebahNet".

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. The APCERT Malware Mitigation Working Group held during the 2019 APCERT AGM & Conference in Singapore;
ii. APRICOT & FIRST TC in Daejeon, Korea;
iii. AUSCERT 2019 Cyber Security Conference in Gold Coast, Australia; and
iv. 31st Annual First Conference in Edinburgh, Scotland.

4.4 Research Papers

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

i. A Systematic Review on Cloud Security Auditing. Published in Institute of Institute of Advanced Scientific Research
ii. Finding Annihilator(s) via Fault Injection Attach (FIA) on Boolean Function of Grain v0. Published in EDP Sciences
iii. A Review of Security Assessment Methodologies in Industrial Control Systems. Published in Emerald Publishing Limited
iv. Towards Implementing Scalable and Reconfigurable SCADA Security Testbed in Power System Environment. Published in Inderscience Online
v. A Comparative Analysis Study: Open Data Concepts in Smart Cities. Published in IRAJ Publisher
vi. Malware Forensic Analytics Framework Using Big Data Platform. Published in Springer
vii. Terrorism Indoctrination via Social Media: A Malaysian Case Study. Published in Academic Conferences and Publishing International Limited
viii. Man-in-the-Middle Attacks on Electrical Power Grid SCADA System. Published in IEEE Xplore Digital Library
ix. Enhanced Automated-Scripting Method for Improved Management of SQL Injection Penetration Tests on a Large Scale. Published in IEEE Xplore Digital Library
x. Development of Denial of Service (DoS) Mitigation for Internet of Things (IoT) Sensor Node. Published in Global Academy of Training & Research
xi. Instilling Digital Citizenship Skills Through Education: A Malaysian Perspective. Published in Academic Conferences International Limited
xii. Smart Energy Monitoring System for Residential in Malaysia. Published in Association of Computing Machinery [ACM]
xiii. A New Cryptojacking Malware Classifier Model Based on Dendritic Cell Algorithm. Published in Hong Kong Society of Robotics and Automation [HKSRA]
xiv. Malware Classification for Cyber Physical System (CPS) Based on Phylogenetics. Published in Blue Eyes Intelligence Engineering & Science Publication

xv. Mobile Malware Classification Based on Phylogenetics. Published in Blue Eyes Intelligence Engineering & Science Publication

xvi. Android Malware Classification Using XGBoost On Data Image Pattern. Published in IEEE Xplore Digital Library

xvii. Enhanced Statistical Analysis Evaluation Using CSM Randomness Test Tool. Published in Malaysian Society for Cryptology Research

xviii. Design Consideration of Malay Text Stemmer Using Structured Approach. Published in Springer

xix. Enhanced Text Stemmer with Noisy Text Normalize for Malay Text. Published in Springer

xx. Endpoint Detection and Response: Why Use Machine Learning? Published in IEEE Xplore Digital Library

xxi. Cryptographic Randomness Analysis on Simon 32/64. Published in Malaysian Society for Cryptology Research

xxii. New Vulnerabilities Upon Pomaranch Boolean Function Through Fault Injection Analysis (FIA). Published in Malaysian Society for Cryptology Research

4.5 Social Media

In 2019, CyberSecurity Malaysia received continuous invitations to speak in events with regards to cyber security at the local radio and television stations. CyberSecurity Malaysia also actively disseminates security concerns through social media such as Facebook and Twitter, which is done through MyCERT. As of now, the MyCERT Facebook Page has about 53,153 likes and the MyCERT Twitter has 4,281 followers.

5. INTERNATIONAL COLLABORATION

Malaysia's National Cyber Security Policy identified international cooperation as one of the areas in enhancing cyber security. In line with this, CyberSecurity Malaysia is active in establishing collaborative relationships with foreign parties.

5.1 Working Visits

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

This agency also received working visits from foreign organisations that have similar

objectives. Among them are:

i. Ministry of Transport and Infocommunications, Brunei;
ii. Various Agencies from Dong Nai Province, Vietnam;
iii. National Cyber and Crypto Agency (Badan Siber Sandi Negara - (BSSN)), Indonesia;
iv. Nation-Building Institute, Thailand
v. Havelsan, Turki

5.2 Memorandum of Understanding (MoU)

CyberSecurity Malaysia in 2019 has signed MoUs with the following organisations in matters pertaining to cyber security:

i. Gujarat Forensic Science University, India; and
ii. InterExchange Solutions Limited , Bangladesh.

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), CyberSecurity Malaysia is facilitating cooperation and interaction among the member countries;
ii. The Chair of the APCERT; and
iii. 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 cyber security 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 achieve world-class capabilities, CyberSecurity Malaysia will relentlessly encourage its employees to obtain certifications in cyber security. In addition, the personnel are encouraged to attend trainings, give presentations and write publications at

international IT security platforms. This will assist them to improve their contribution in knowledge and experience sharing in the cyber security field. The personnel are also encouraged to develop in-house tools used for mitigating security threats to assist the public and industry to secure and utilise their assets when performing online activities.
To encourage a safer cyber environment, CyberSecurity Malaysia realises the need to work together with the local and international security organisations through the establishment of formal relationship arrangements such as the MoUs and agreements.
This agency will continue to organise national events such as the Cyber Security Malaysia – Awards, Conference and Exhibition (**CSM-ACE**), which is an annual event providing awareness, training and awards to information security professionals, and the National ICT Security Discourse to boost the cyber security awareness among the youth.
At the international arena, CyberSecurity Malaysia as the Permanent Secretariat of the OIC-CERT, will spearhead the collaboration and organise international events such as the OIC-CERT Annual Conferences. The event will be held on 29th October 2020 at Kuala Lumpur.
With such understanding, CyberSecurity Malaysia supports newly established local and international Computer Security Incident Response Team (**CSIRT**) by providing advice and assistance especially in becoming members to international security community such as the APCERT, FIRST and OIC-CERT.

7. CONCLUSION

CyberSecurity Malaysia observes a reduction in cyber incidents that were reported to the Cyber999 Help Centre in 2019 compared to the previous year. This agency will continuously work with international allies to generate useful cooperation in safeguarding the cyber environment.
In line with the Malaysia's National Cyber Security Policy that emphasised on capacity and capability building, mitigation of cyber threats and international collaboration, CyberSecurity Malaysia will continue to enhance existing and develop new cyber security processes, human capability and technology. CyberSecurity Malaysia will also continue its commitment to seek for new edges in cyber security and to be a catalyst in developing the industry.
International cooperation and collaboration are important facet in mitigating other cyber security issues. As the cyber environment does not conform to the physical boundary of the countries, international relations will remain an important initiative. 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. CyberSecurity Malaysia will continuously pursue new cooperation with cyber security agencies regionally and globally in the effort to make cyber space a safer place for all.

EC-CERT

Taiwan E-Commerce Computer Emergency Response Team - Chinese Taipei

1. Highlights of 2019

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 27 event visits, handling 17 security incidents, providing 26 security advices, and received 15 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:

- Digital Forensic Analysis with Free and Open Source Tools
- Web Application Penetration Testing Techniques
- Web Penetration Testing 101
- Forensics (Storage Media & Mobile Phones)

5.1.2 Drills & exercises

EC-CERT participated in the APCERT Drill in March 2019. The topic of APCERT online drill is " Catastrophic Silent Draining in Enterprise Network"

5.2 Other international activities

EC-CERT attended APCERT AGM and Conference 2019.

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 of EC-CERT in 2020.

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 2019

1.1 Summary of Major Activities

To enhance the city's overall defensive capability and resilience against cyber attacks, we continue to leverage the first local cross-sector Partnership Programme for Cyber Security Information Sharing named "Cybersec Infohub" and organise a number of seminars and workshops with a view to promoting trusted partnership between local cyber security stakeholders across prominent sectors for sharing cyber security information and providing actionable insights to the community.

Within the Government of the Hong Kong Special Administrative Region of the People's Republic of China (the Government), we organised the annual inter-departmental cyber security drill for government users. To help our government staff familiarise with hands-on analytical skills against cyber security incidents, the drill of this year adopted a model whereby participants were required to analyse a series of log files and recommend actions in response to the simulated cyber attack scenarios. In addition to the inter-departmental cyber security drill, a government-wide phishing drill campaign was also launched to raise awareness of all government users and their capabilities in defending against phishing attacks.

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 2019, we continued publishing threat trends, security alerts and mitigation advice through the Government Computer Emergency Response Team Hong Kong (GovCERT.HK) web portal for reference by the general public. We further tailored specific threat awareness updates for government departments.

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 to raise public awareness and capability development.

1.2 Achievements and Milestones

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 as an enabler to nurture culture in sharing cyber security information. The programme has been operating for more than one year and more than 150 public and private organisations have joined the programme, covering a wide range of sectors, including finance and insurance, public utilities, transport, healthcare, telecommunications, innovation and technology, information security, tertiary education institutions, etc. In 2019, we introduced artificial intelligence elements into the collaborative platform of Cybersec Infohub, which facilitated members to easily acquire the required information for timely dissemination of relevant cyber security information to the public. The programme has become an essential reference for organisations in gathering cyber security information and meeting with information security stakeholders to share 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 and together reinforcing Hong Kong's cyber security. We publish monthly Cyber Security Threat Trends Report via the GovCERT.HK web portal to highlight the observations of latest cyber security threat landscape for reference by the public to enhance their situational awareness.

Liaison and Collaboration

We proactively participate in the Asia Pacific Computer Emergency Response Team's (APCERT) activities and work closely with the Computer Emergency Response Team (CERT) community in handling threat information. We have been working closely with the Hong Kong Internet Registration Corporation Limited (HKIRC), one of our local Internet infrastructures stakeholders, to provide them with technical advice in launching a free website scanning service for local small and medium enterprises (SMEs) to assist them to identify and mitigate their information security issues as early as possible.

Capability Development

To facilitate in developing staff capabilities to tackle evolving cyber threats, we have further enriched the services available at the GovCERT.HK Technology Centre. The centre offers government departments relevant tools and network facilities in a controlled environment to enable vulnerability scanning and security testing for potential information security issues of their web applications.

Awareness Building and Public Education

User awareness of information security plays a vital role in coping with cyber threats. In response to the worsening threat of phishing attacks, we launched the "Government-wide Phishing Drill Campaign" in 2019 to raise awareness of government users on phishing and strengthen their capabilities in defending against phishing attacks.

In view of the rising trend of phishing scams and data breaches, GovCERT.HK has produced a series of promotional materials including educational videos and smart tips for the public to protect themselves from and defend against cyber threats.

GovCERT.HK also devotes much attention to public education and capacity building in different business sectors and age groups. In the 2018/2019 school year, we organised more than 40 school visits to reach out to some 10 000 students, parents and teachers.

2. About GovCERT.HK

2.1 Introduction

The Government Computer Emergency Response Team Hong Kong (GovCERT.HK) is a governmental CERT responsible for coordinating incident response for over 80 departmental Information Security Incident Response Teams of the Government of the Hong Kong Special Administrative Region of the People's Republic of China (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 infrastructures, 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 industry on cyber threat intelligence

sharing, capability development, public education, and continuous promotion on cyber security and resilience through social and mass media.

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

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 will centrally manage incident responses within the Government and develop 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 government's information infrastructure would be well protected.

3. Activities and Operations

3.1 Scope of Services

GovCERT.HK is the computer emergency response team 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 locally and in the region.

3.2 Security News Bulletins

In 2019, 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 highlight top two to three hot security news and summarise vulnerabilities by products for easy reference by security practitioners. These Bulletins were distributed to registered subscribers through emails and posted at the GovCERT.HK website as public information.
  (www.govcert.gov.hk/en/secbulletins.html)

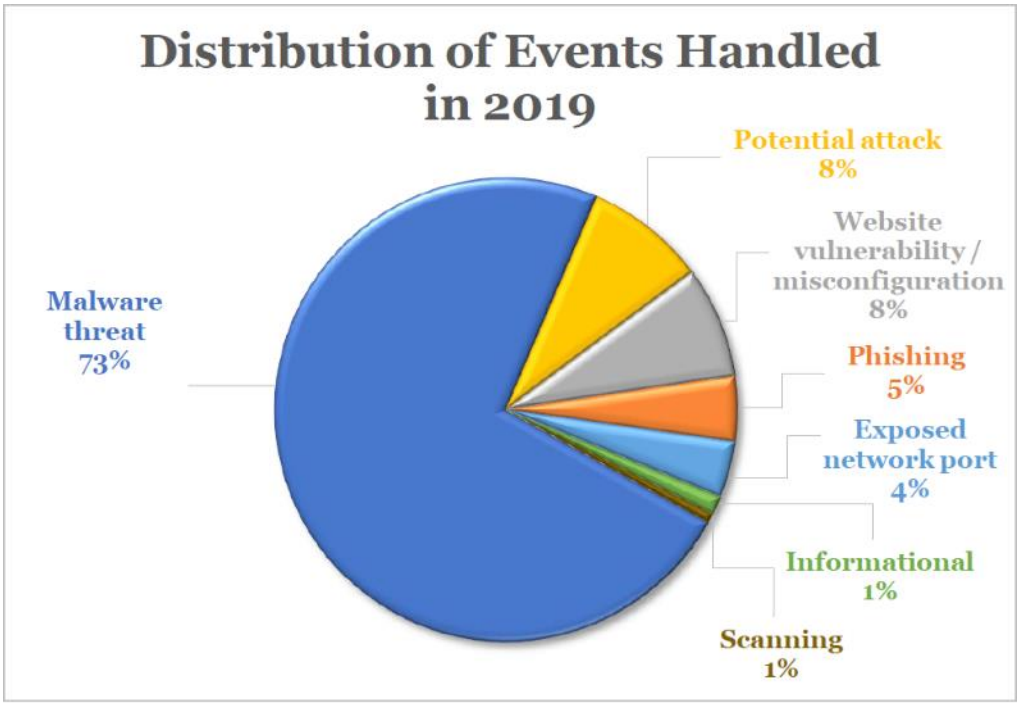
3.3 Alerts and Advisories

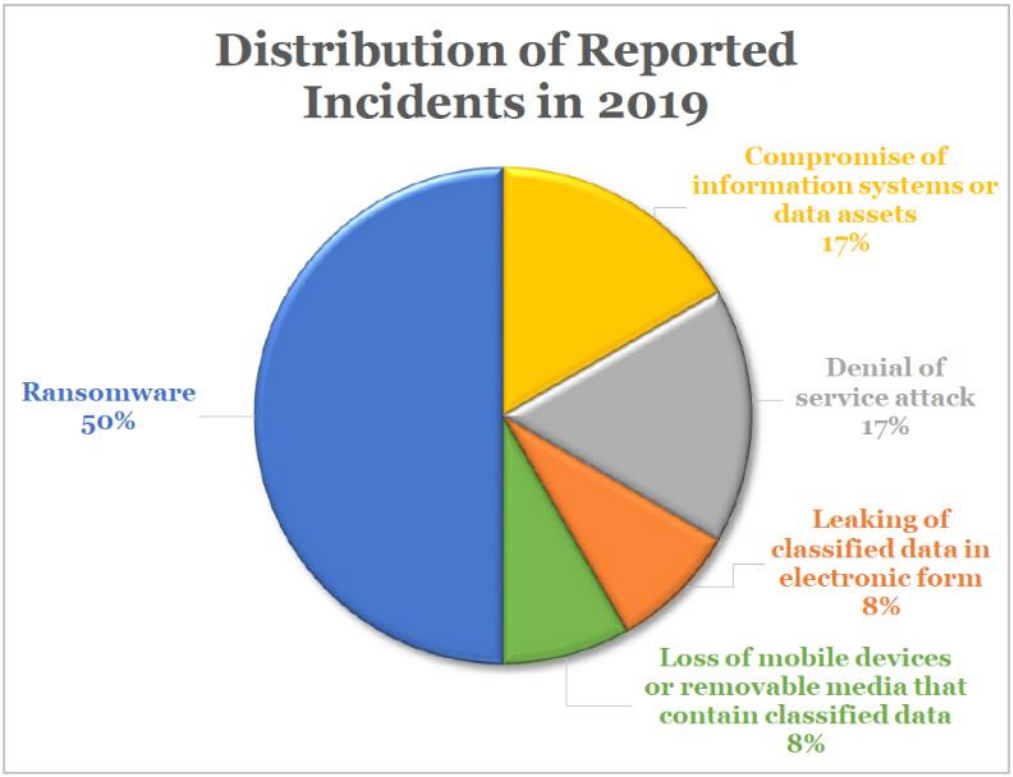
In 2019, GovCERT.HK issued around 90 security alerts associated with computing products widely deployed in government installations. In case the security vulnerabilities were considered highly risky to our environment, we would proactively request government departments to take prompt and appropriate preventive measures against potential information security risks.

We also conducted threat analysis on over 150 security events detected and received from various sources. The threat information was extracted and shared with relevant constituents 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 2019, 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 2019.

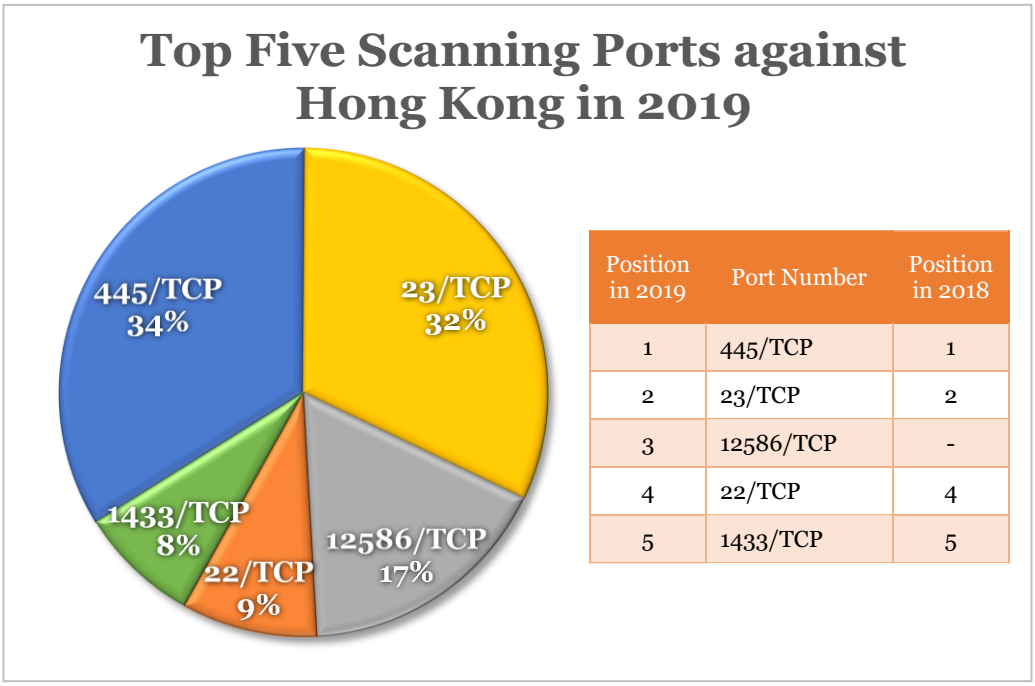




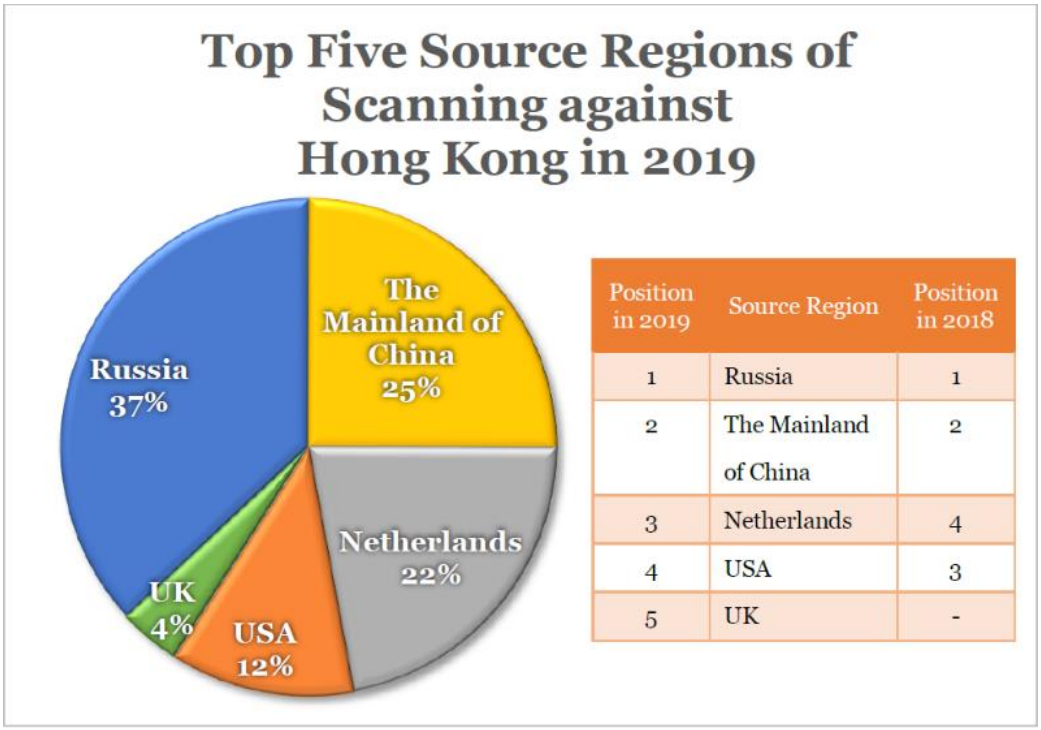
To facilitate the public to access the statistics on information security incidents in the Government, relevant data has been released to the Government's Public Sector Information Portal (www.data.gov.hk/en-data/dataset/hk-ogcio-sec_div_01-information-security-incident).

3.5 Abuse Statistics

As a member of the TSUBAME project, GovCERT.HK has set up sensors to collect and analyse network scanning activities targeting Hong Kong. The following charts show the top five scanning ports (contributed 19% of all the scanning activities) and the top five source regions (contributed 69% of all the scanning activities) detected by the TSUBAME sensors installed in Hong Kong in 2019.



Position in 2019	Port Number	Position in 2018
1	445/TCP	1
2	23/TCP	2
3	12586/TCP	-
4	22/TCP	4
5	1433/TCP	5

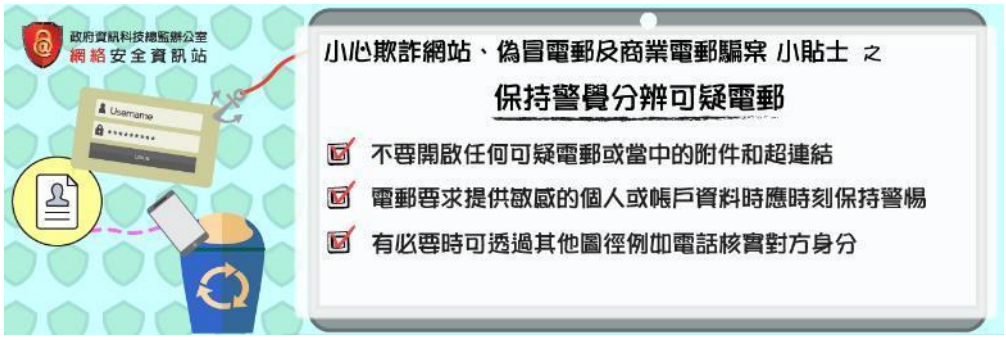


Position in 2019	Source Region	Position in 2018
1	Russia	1
2	The Mainland of China	2
3	Netherlands	4
4	USA	3
5	UK	-

3.6 Publications and Mass Media

As cyber attacks continue to increase in number and sophistication, members of the public face cyber security risks when using different technologies, such as mobile devices, cloud services and social networking applications. We have made use of different promotion channels to reach out to our target audience and collaborated with industry players during the process.

- 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 information security. 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 2019, we covered a wide range of topics including data security, password management, phishing attacks, endpoint security, and more.
  (www.cybersecurity.hk/en/media.php#Radio)



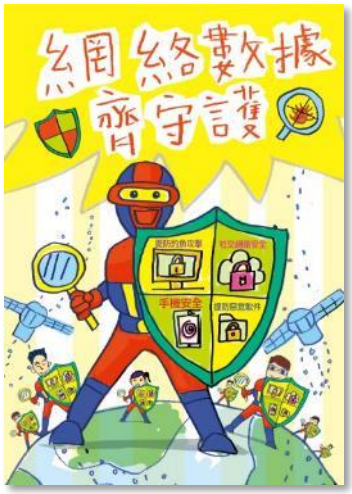
- A series of handy guidelines with different themes were developed to provide practical tips and advice for SMEs and the general public to defend against cyber threats.
  (www.cybersecurity.hk/en/resources.php#leaflets)

- To encourage the public to adopt data protection best practices, enhance their awareness of cyber security and draw their attention to the importance of

information security, we organised the "We Together! Secure Data!" poster design contest in 2019. Participants fully demonstrated their creativity to get across data protection message to the public and the industry in a creative manner. The winning and shortlisted entries have been published to the Cyber Security Information Portal website for public reference as well.

(www.cybersecurity.hk/en/contest-2019.php)

Winning Entries



- Leveraging the OGCIO Facebook page as newly launched in 2019, we have

published a series of posts with infographics and videos to reach out to the general public with timely updates and tips on cyber security topics such as identifying phishing websites and safe use of online banking. This is an effective social media channel for engaging the community in enhancing their security awareness. (www.facebook.com/ogciohk)

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, we established the GovCERT.HK Technology Centre. The centre offers government departments a controlled environment with relevant facilities and equipment to enable vulnerability scanning and security testing for potential security issues of their web applications. This year, we enhanced the capability of the centre with more services offered, such as the dynamic application security testing service to facilitate users in examining their web applications. Users can benefit by making use of the tools to identify web vulnerabilities, misconfigurations, compromised passwords, etc.

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 2019, we organised a total of 16 seminars, trainings and solution showcases for government IT staff and users to raise their awareness of the latest security vulnerabilities and update their knowledge in information security technologies. More than 1 800 government staff participated in these events to understand the latest cyber security trends and preventive measures.

- Seminars, trainings and showcases were conducted for government IT staff and users to raise their security awareness and introduce the latest IT security technologies and solutions. Topics included industry best practices on the security of mobile and Internet of Things (IoT) devices, defence against phishing, promotion of various security solutions, etc.
- Seminars were organised for departmental IT security officers to refresh their security knowledge and update them on the Government's latest requirements and

approaches in dealing with cyber security threats and adopting mitigation measures.

4.2 Drills and Exercises

Inter-departmental Cyber Security Drill of the Government

GovCERT.HK has coordinated government departments to conduct cyber security drills to assess the participants' capabilities of incident analysis and test their incident response procedures with a view to enhancing the overall incident response capability.

With the ever-changing cyber threat landscape, it is imperative to enhance the competencies in mitigating cyber threats. This year, we continued to organise the annual inter-departmental cyber security drill with some 45 departments participated to strengthen the readiness and capabilities of departments to respond to cyber security incidents. The drill adopted a model whereby participants were required to analyse a series of log files in order to strengthen their technical and analytical skills in handling cyber security incidents. In form of table-top exercises, participants discussed and presented their way of responding to any data breach and malware infection arouse in the simulated cyber attack scenarios.

Government-wide Phishing Drill Campaign

In defending against the ever-growing phishing attacks, this year we launched the "Government-wide Phishing Drill Campaign" to raise government users' awareness of phishing. All government users under the drill would receive simulated phishing emails and immediate feedback explaining the proper way to handle emails if the users clicked the hyperlinks in these emails. We also organised seminars, thematic websites, education videos and quizzes to introduce different ways to identify phishing emails in order to raise their awareness of phishing and strengthen their capabilities in defending against potential phishing attacks.

APCERT Drill

As an Operational Member of the APCERT, GovCERT.HK participated in the APCERT Drill with the theme of "Catastrophic Silent Draining in Enterprise Network" in July 2019. 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 information security, especially data protection, GovCERT.HK adopted the slogan "We Together! Secure Data!" as the theme in 2019. 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 digital assets.

- Two seminars were organised under the "Build a Secure Cyberspace" promotional campaign in May and September 2019, aiming to promote public awareness of information security and adoption of security best practices, in particular the risks of phishing scams and strategies in protecting data assets.

- More than 40 school visits were conducted at primary and secondary schools in the 2018/19 school year, reaching out to some 10 000 students, parents and teachers for raising their awareness of cyber security and encouraging the proper attitude in using the Internet.

Cybersec Infohub – Partnership Programme for Cyber Security Information Sharing

To encourage trust building and promote closer collaboration among different sectors under the Cybersec Infohub programme, activities ranging from sector-specific face-to-face meetings, closed group meetings, professional workshops and webinars were arranged in 2019 with positive response from participants.

5. Local and International Collaboration

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

5.1 Local Collaboration

GovCERT.HK is keen on fostering exchanges and experience sharing among the local information security industry. We continue to leverage the Cybersec Infohub programme to promote closer collaboration among local information security stakeholders across different sectors. Under the programme, we have provided a community-driven collaborative platform (Cybersechub.hk) and organised various industry events to facilitate the exchange of cyber security information. As of 2019, more than 150 public and private organisations across various sectors have joined the programme. (www.cybersechub.hk)

To celebrate Cybersec Infohub's anniversary since its launch, we held the first anniversary celebration-cum-professional workshop in November 2019 to recognise the positive contributions and cyber security experts.

The Internet is critical to communications, conduct of e-business and access to e-services. GovCERT.HK has been acting as a supportive role in the Internet Infrastructure Liaison Group (IILG) established and led by OGCIO. The key roles of the IILG are to maintain close liaison with Internet infrastructure stakeholders and strive in collaboration with the stakeholders for the healthy operation of the Internet infrastructure of Hong Kong. In 2019, the IILG collaboration mechanism was activated ten times to strengthen monitoring of cyber security of large-scale events and provide support events to protect the local Internet infrastructure against alleged cyber attacks. Particularly in January and March 2019, local Internet stakeholders were reminded through the IILG collaboration mechanism to monitor the healthiness of their DNS resolvers regarding the revocation and removal of the Old Key Signing Key (KSK-2010) of DNSSEC Root Zone.

SMEs are generally less adequately allocated with IT and security resources to enhance their cyber security protections. We have been working closely with HKIRC to provide them with technical advice in launching a free website scanning service to assist SMEs to identify and mitigate their information security issues as early as possible. Apart from scanning malware in the system and providing information security improvement solutions, a number of seminars and workshops have also been arranged with overwhelming response from the community.

5.2 International Collaboration

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

information security and data privacy policies, cyber crime initiatives and technological researches.

In November 2019, GovCERT.HK officials, along with representatives of HKCERT, received a visit from delegates of the National Center of Incident Readiness and Strategy for Cybersecurity (NISC) of Cabinet Secretariat, the Government of Japan and the Consulate General of Japan in Hong Kong. There was an in-depth exchange of experiences and views on cyber security policy and security incident response strategies.

GovCERT.HK participated in the following events in 2019:

- FIRST Annual Conference
- Annual Technical Meeting for CSIRTs with National Responsibility
- CNCERT/CC Annual Conference
- 2019 China Cybersecurity Week
- APCERT Annual General Meeting and Conference
- APCERT Drill
- Five APCERT on-line training sessions

6. Future Plans

6.1 Upcoming Projects

The accelerated development of emerging technologies is spurring continuous innovation, however, it could also bring along different cyber security threats. GovCERT.HK will continue to stay vigilant in defending against potential cyber attacks. In particular to the rapid development of technology such as artificial intelligence, big data and Internet of Things, we are conducting a new round of review on the "Government IT Security Policy and Guidelines", covering the latest areas of information and cyber security as well as smart city development with reference to the latest international standards and industry best practices.

To enhance the capability of cyber threat intelligence management, we would continue to enhance our Cyber Risk Information Sharing Platform (CRisP) with integration of a Malware Information Sharing Platform (MISP) instance to enable sharing, storing and correlation of Indicators of Compromise.

We are also revamping our existing Information Security (InfoSec) Website to provide a

more lively design for better user experience and facilitate dissemination of information security related tips and advices to the public.

6.2 Future Operations

In view of the positive response from the participating organisations of Cybersec Infohub and industries, we would regularise the programme and partner with HKIRC to promote the participation of more public and private organisations and sharing of cyber security information. This would also facilitate enterprises including SMEs to gather cyber security information and defend against 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, making timely responses and enhancing appropriate defensive measures to the inevitable cyber security threats. In facilitating Hong Kong to become a secure smart city, GovCERT.HK will continue to foster all stakeholders to take forward communication and exchange of cyber security information so as to keep abreast of the fast-evolving cyber security landscape and be more vigilant to take prompt and appropriate measures to protect their information systems and data assets, with a view to continuously enhancing the cyber security resilience capability of the community.

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

HKCERT

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

1. About HKCERT

1.1 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.

1.2 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.

1.3 Mission and Constituency

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

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

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

2. Activities and Operations

2.1 Incident Handling

During the period from January to December of 2019, HKCERT had handled 9,458 security incidents which was 6% decrease of the previous year (see Figure 1). Referral cases accounted for 92% of the total number of security incidents.

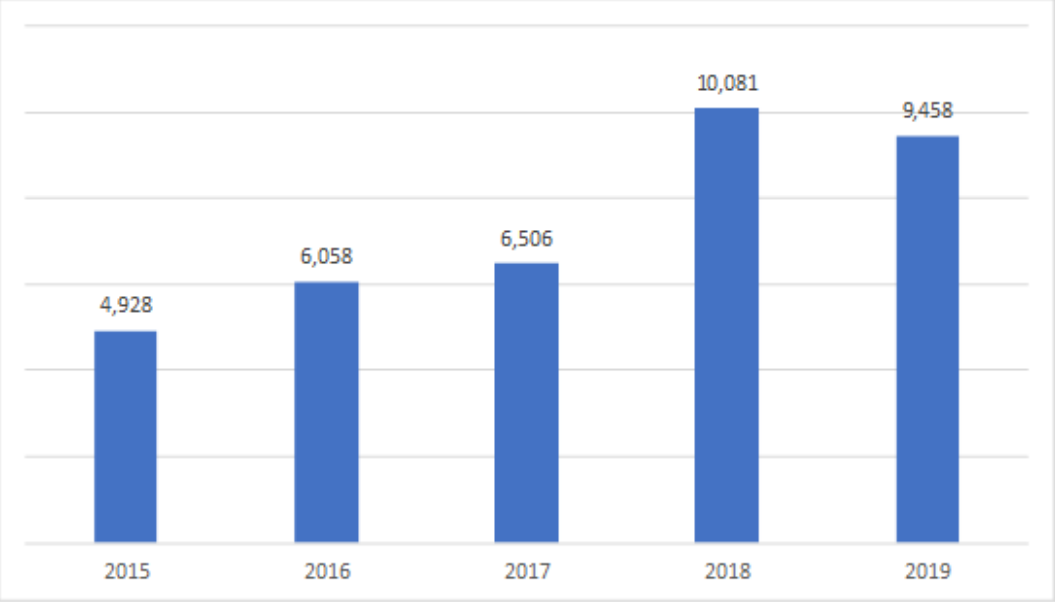


Figure 1. HKCERT Security Incident Reports

While the number of overall security incidents handled by HKCERT reported a 6% year-on-year drop in 2019, totally 9,458, Botnet (4,922 cases or 52%) and phishing websites (2,587 cases or 27%), two principal sources of reports, still went up 30% and 23% respectively which were mainly attributed to rise in financial crime-related Botnets and phishing targeting financial organizations and enterprises. On the other hand, malware reports (1,219 cases or 13%) fell 62% as more malware stayed stealthy after infection and ransomware targeted more on global enterprises for higher return instead of massive untargeted attacks. (see Figure 2).

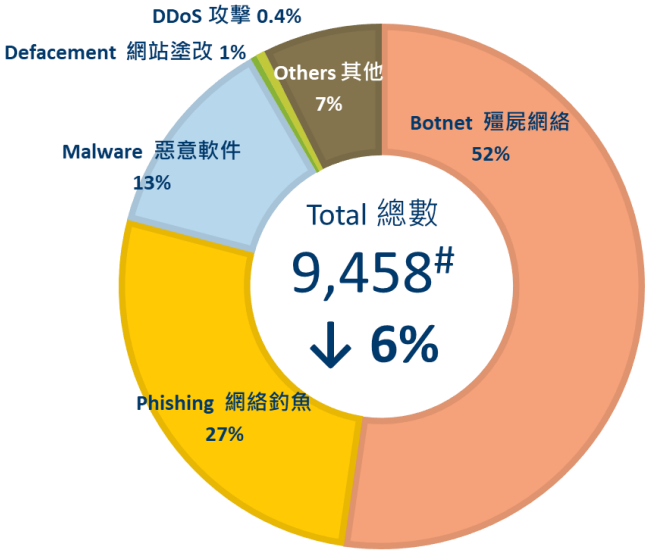


Figure 2. Distribution of Incident Reports in 2019

2.2 Watch and Warning

During the period from January to December of 2019, HKCERT published 273 security bulletins (see Figure 3) on the website. In addition, HKCERT have also published 48 blogs, including security advisories on GDPR, ransom email attacks, IoT security risks at home, ransomware, webcam etc.

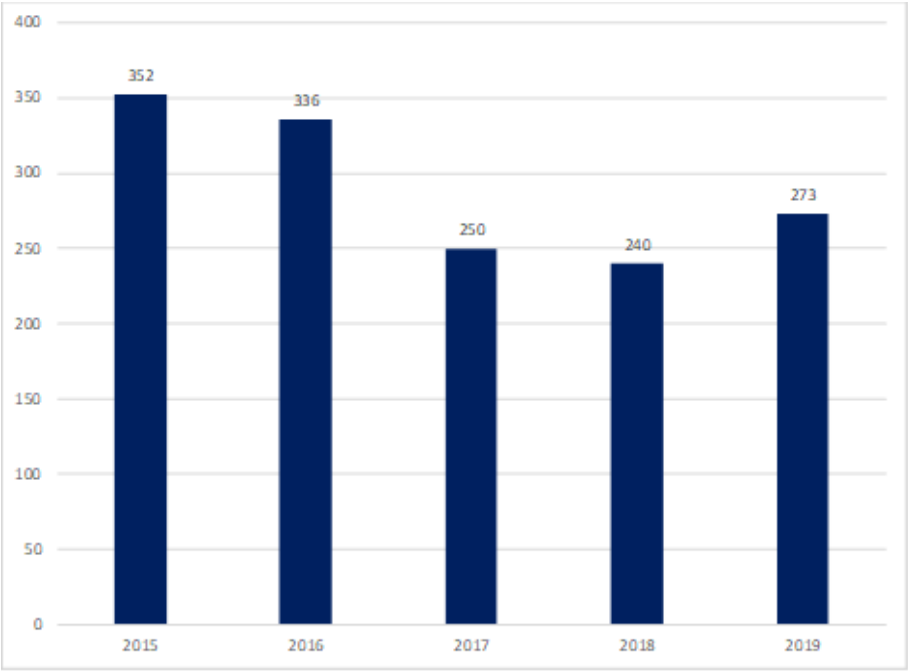


Figure 3. HKCERT Published Security Bulletins

The drop of Security Bulletins in 2017 was mainly due to consolidation of MS & Adobe security bulletins

HKCERT used the centre website (www.hkcert.org), RSS, HKCERT mobile app, and Hong Kong Government Notification mobile app 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.

2.2.1 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 record high of 11,554 in 2019 Q2 and finally dropped to 6,831 in Q4 2019), largely attributed to the significant rise of Mirai events as depicted in Figure 5.

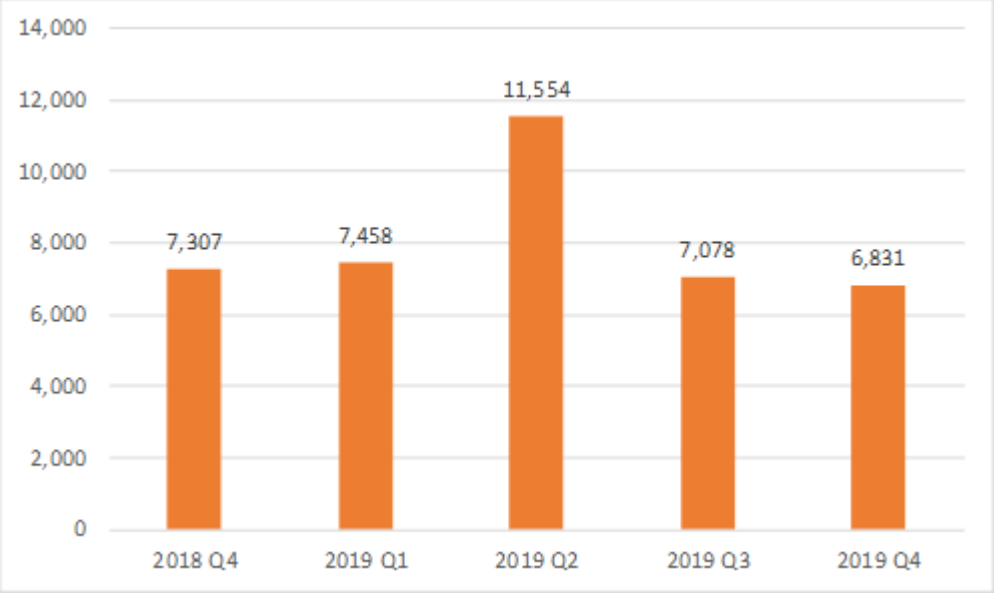


Figure 4. Trend of Bot related security events in the past year
(Source: data feeds from overseas security researchers, not from incident reports)

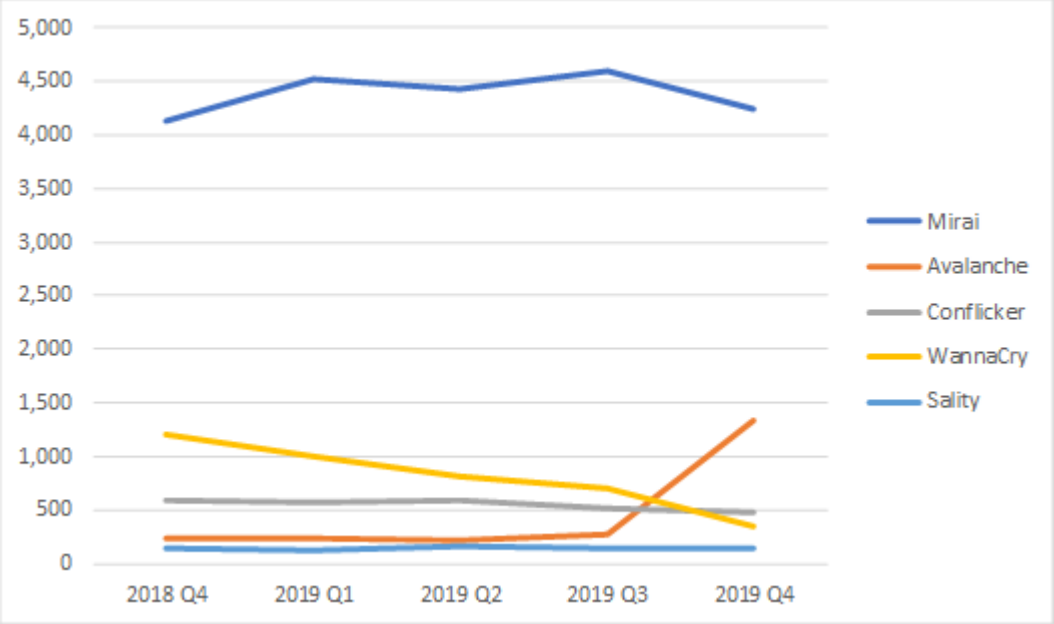


Figure 5. Trend of Top 5 Botnet Families in the past year

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

2.3 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 and security bulletins every quarter (see https://www.hkcert.org/statistics).

3. 3. Events organised and co-organised

3.1 Seminars, Conference and Meetings

HKCERT jointly organised the "Build a Secure Cyberspace 2019" campaign with the Government and Hong Kong Police Force. The campaign involved public seminars, and a Poster Design Contest. Two public seminars were organised in May and September 2019.

For the Poster Design Contest, HKCERT had 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 6).

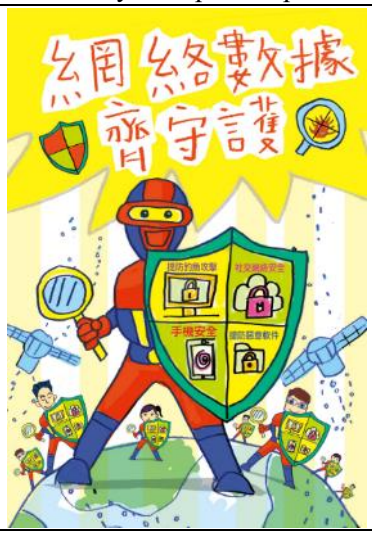
Primary Group Champion	Family Group Champaign
	
Secondary Group Champion	Open Group Champion
	

Figure 6. 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-2019.php

We co-organised the 2-day Information Security Summit 2019 with other information security organisations and associations in October 2019, inviting local and international speakers to provide insights and updates to local corporate users.

3.2 Speeches and Presentations

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

3.3 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.

3.4 Media promotion, briefings and responses

- HKCERT published an advertorial in September 2019 to promote the public seminar and the Poster Design Contest.

4. Collaboration

4.1 International Collaboration

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

Participated in the APCERT AGM and Conference in Singapore

- Participated in the FIRST Meeting and Conference, and the National CSIRT Meeting in Edinburgh, UK
- Participated in the CNCERT Conference in Guangzhou
- Participated in the HITCON Security Conference in Taipei
- Participated in (ISC)2 APAC Security Congress

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

4.2 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.
- To promote cyber security information sharing among industries in Hong Kong, the Hong Kong SAR Government launched the Cyber Security Information Sharing platform called 'Cybersec Infohub". As of December 2019, over 150 Information

Security companies and critical infrastructure organisations had joined the platform. Cyber security information and intelligence were shared among the members. HKCERT joined as a member of the Programme and shared security intelligence with the members. Through the platform, HKCERT also shared security alerts with the public. HKPC, the parent organisation of HKCERT, is the programme manager of the Programme.

- 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 2019 with 11 organisations including the Hospital Authority and most of the private hospitals in Hong Kong joining.

5. Other Achievements

5.1 Strategy and Service Review

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

5.2 Advisory Group Meeting

HKCERT had held the Advisory Group Meeting in October 2019. The meeting solicited inputs from the advisors on the development strategy of HKCERT.

5.3 Three Year Strategic Plan

HKCERT 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 would be updated annually. HKCERT based on this plan to prepare the annual work plan and budget to solicit funding support from the government.

5.4 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.

5.5 IoT Security Study and Best Practice

HKCERT placed more efforts in IoT Security. We joined the APCERT IoT Security Working Group. In 2019 HKCERT released an IoT Device (Webcam) Security Study. In Q1 of 2020, HKCERT planned to release the IoT Security Best Practice and three other studies in IoT network protocols.

5.6 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.

5.7 Year Ender press briefing

HKCERT organised a year ender press briefing to media in January 2020 to review cyber security landscape of 2019 and provided an outlook to 2020 to warn the public for better awareness and preparedness. It received very good press coverage.

Figure 7. HKCERT at the Year Ender press briefing.

6. Future Plans

6.1 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.

6.2 Funding

HKCERT had secured Government funding to provide the basic CERT services in 2020/2021. We shall work closely with the government to plan for the future services of HKCERT. We shall continue to propose new initiatives to the government and seek support from the government.

6.3 Enhancement Areas

In the coming year, HKCERT will invest on more digital campaign for security awareness promotion. HKCERT will collect inputs from incident reporters via survey. HKCERT will re-design and revamp its website to replace the old design to enhance user experience and engagement.

7. Conclusion

HKCERT recorded significant hikes in botnet and phishing website reports in Hong Kong for 2019. In 2020, the wider use of new technologies such as IT/OT, AI deepfake and 5G are expected to contribute to bring about new cyber security challenges. HKCERT will continue to put effort in IoT security and advise enterprises to adopt a "Security by Design" approach to manage cyber risk.

Moreover, computers running an older version of Microsoft operating systems and Transport Layer Security (TLS) protocols will face more security threats with the end of official technical support and security patch. HKCERT will urge enterprises to plan upgrade/migration for end of support operating systems and protocols and implement them when required.

ID-CERT

Indonesia Computer Emergency Response Team

1. ABOUT ID-CERT

1.1 INTRODUCTION

ID-CERT (Indonesia Computer Emergency Response Team) is an independent team which is from and for community. ID-CERT is the first CERT in Indonesia and founded by Budi Rahardjo, MSc., PhD. in 1998. ID-CERT together with JP-CERT (Japan), AusCERT (Australia), is one of the founders of the APCERT (Asia Pacific Computer Emergency Response Team) forum.

1.1.1 ESTABLISHMENT

In 1998 there was no CERT in Indonesia. Based on that Budi Rahardjo, MSc., PhD., an internet security expert, encouraged himself to establish ID-CERT. At the same time, countries around Indonesia began to establish their own CERTs and this continued into Asia-Pacific forum which later became the APCERT.

ID-CERT wishes to remain standing as a non-governmental organization, independent, but received an allocation of government funding as a contribution to the CERT. ID-CERT is just being reactive (not active) in responding and handling a case of incoming or reported incident by complainers, either locally and internationally. ID-CERT does not have the authority to investigate a case thoroughly, but just become a liaison who can be trusted, especially by those who reported incident.

In 2013 ID-CERT has been officially incorporated.

1.1.2 WORKFORCE POWER

Chairman:	Budi Rahardjo, MSc., PhD.
Vice Chairman:	Andika Triwidada
Manage:	Ahmad K. Alkazimy
Incident Response HelpDesk:	Rahmadian L. Arbianita

Technical Editor:

- Emil Yakhya
- Bainul
- Iqbal

Volunteers:

- Setia Juli Irzal (Malware Analyst)
- Ikhlasul Amal
- Maman Sutarman
- Oryzandi
- Other volunteers

1.1.3 CONSTITUENCY & ETC

Constituent

ID-CERT Membership is open to all Indonesia Internet community who are concerned in the internet security, either from the ISP or non-ISP, such as government organizations (ministries, local goverments, state enterprises, enterprises, etc.) as well as private citizens.

Respondent

ID-CERT has 41 respondents participating in Incident Monitoring Report. ID-CERT still welcome to new respondents who wish to join in the various researches or studies conducted by ID-CERT.

Volunteer

From the beginning, ID-CERT are supported by many volunteers who work selflessly to contribute and concern for internet security in Indonesia. Generally, ID-CERT volunteers are individual one.

2. ACTIVITY AND OPERATION

2.1 INCIDENT HANDLING REPORT

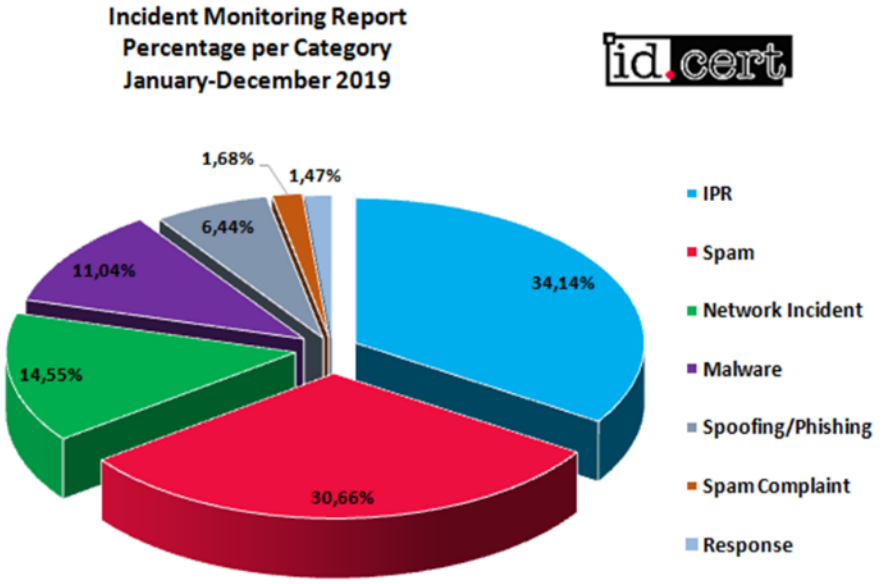
Total incident reports: 124.731

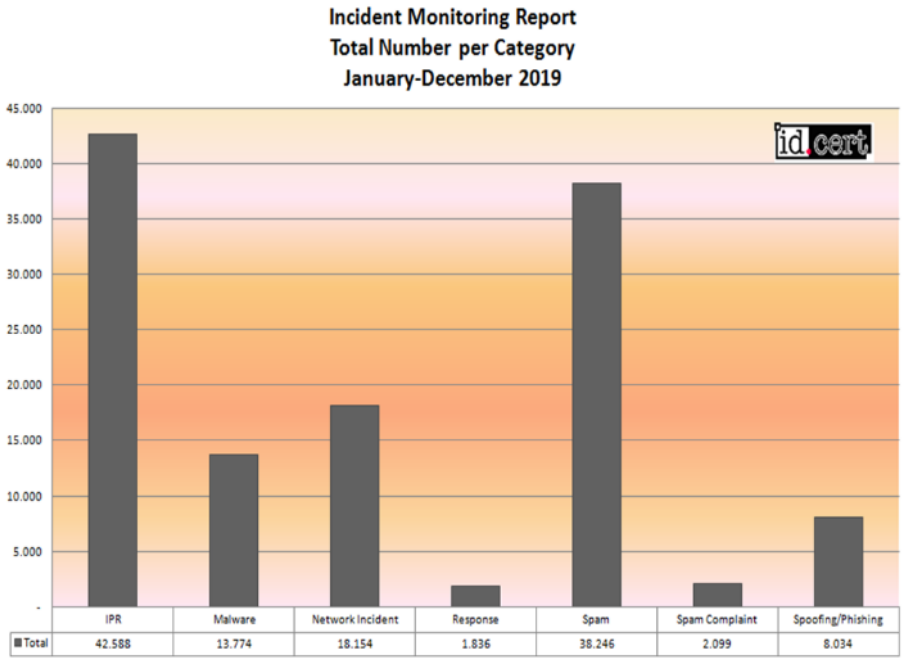
Incident handling: 1.836

2.2 ABUSE STATISTIC

Percentage

IPR (Intellectual Property Rights):	34,14%
Spam:	30,66%
Network Incident:	14,55%
Malware:	11,04%
Spoofing/Phishing:	6,44%
Spam Complaint:	1,68%
Response:	1,47%





Total number

IPR (Intellectual Property Rights) : 42.588

Spam: 38.246

Network Incident: 18.154

Malware: 13.774

Spoofing/Phishing: 8.034

Complaint Spam: 2.099

Response: 1.836

2019	IPR	Spam	Network Incident	Malware	Spoofing/ Phishing	Spam Complaint	Response
January	2.771	4.193	1.719	777	404	162	29
February	2.039	3.807	1.565	943	373	145	28
March	1.661	4.380	2.218	1.221	384	194	50
April	1.480	4.285	1.657	775	367	254	37
May	727	4.029	1.217	1.326	404	209	37
June	5.309	4.141	954	1.155	647	130	37
July	5.985	3.492	1.815	1.356	1.002	173	155
August	5.741	3.089	1.872	1.331	803	146	205
September	4.001	2.948	1.160	1.271	121	148	229
October	3.350	236	1.244	1.264	849	215	156
November	5.425	1.874	1.265	1.251	1.177	212	368
December	4.099	1.772	1.468	1.104	1.503	111	505
Total	**42.588**	**38.246**	**18.154**	**13.774**	**8.034**	**2.099**	**1.836**
Average	**3.549**	**3.187**	**1.513**	**1.148**	**670**	**175**	**153**
%	**34,14%**	**30,66%**	**14,55%**	**11,04%**	**6,44%**	**1,68%**	**1,47%**

Average number

IPR (Intellectual Property Rights): 3.549

Spam: 3.187

Network Incident: 1.513

Malware: 1.148

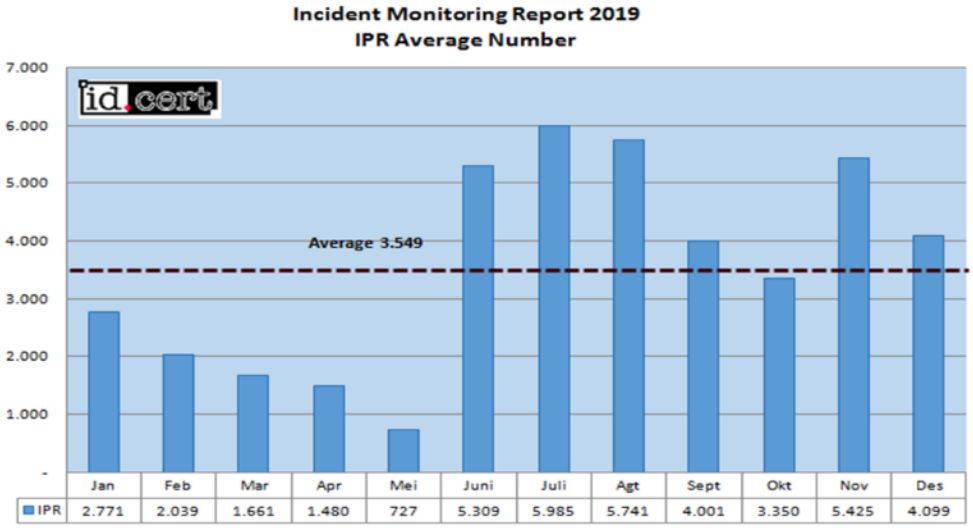
Spoofing/Phishing: 670

Complaint Spam: 175

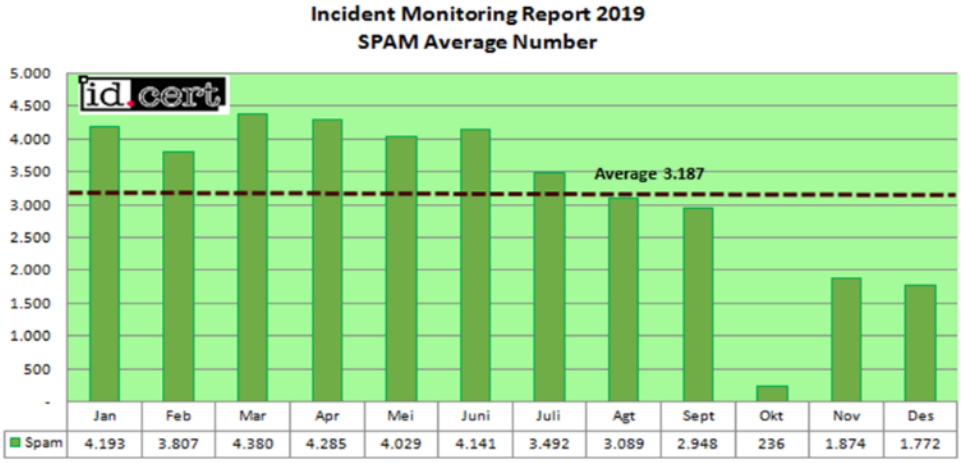
Response: 153

IPR (Intellectual Property Rights)

- 100% reports from abroad.
- Movies and music sharing P2P at Indonesia IPs.
- Request to take down the files.

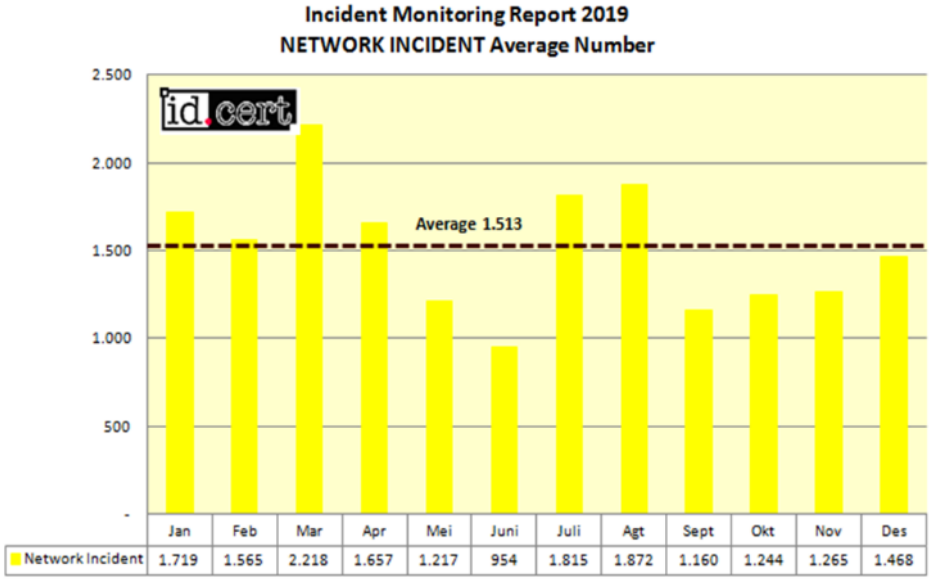


Spam



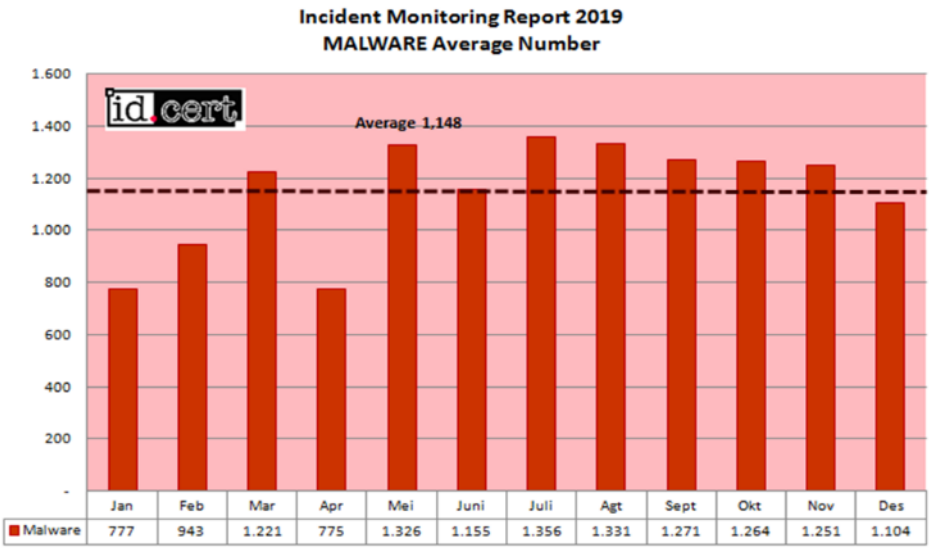
Network Incident

- Mostly brute force attack.
- Login succeed then:
  - Web/IP is infiltrated by malware.
  - Web/IP is infiltrated by hacking tools.
  - Web/IP is made into C&C.
  - Stealing data.
  - Hacking/deface.

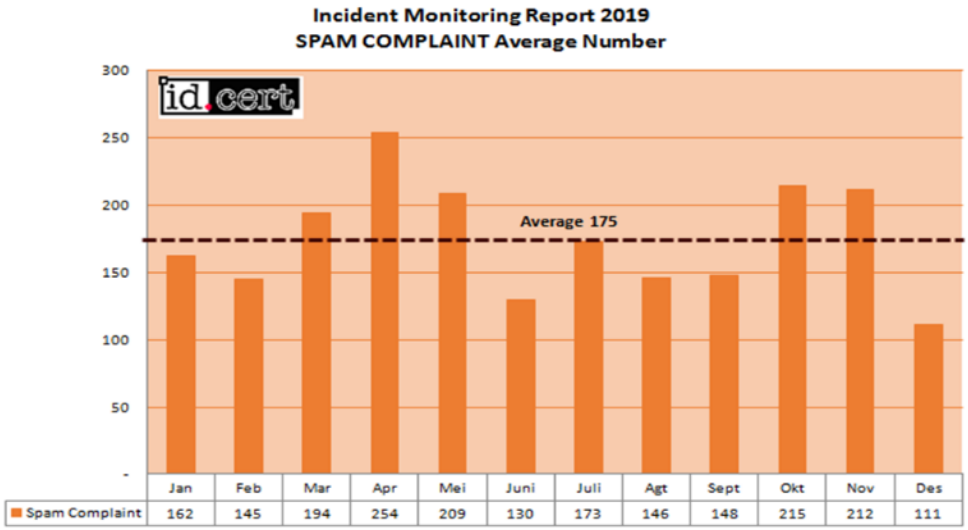


Malware

Some cases a malware was attached to a phishing email.

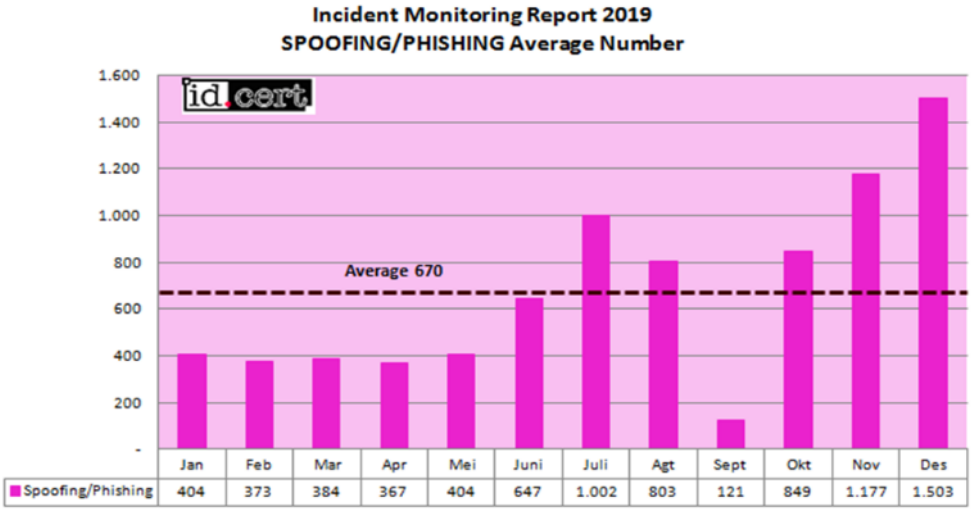


Complaint Spam

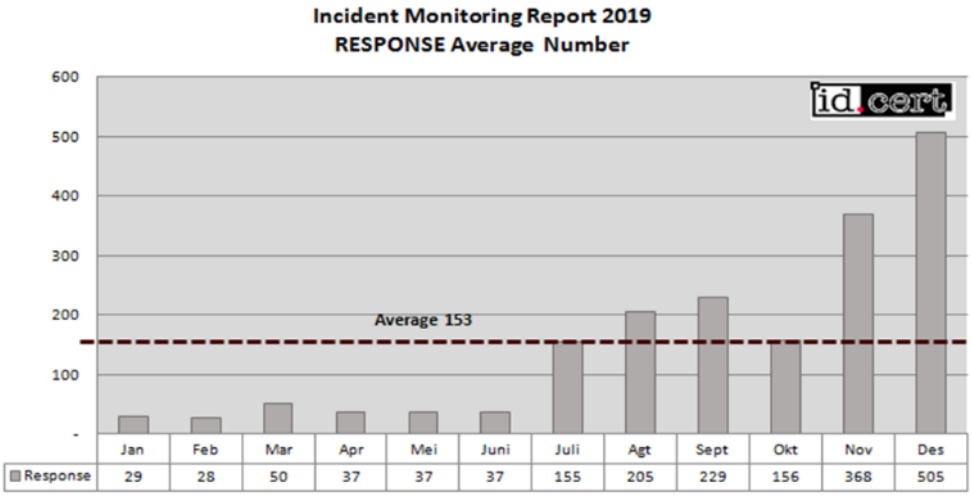


Spoofing/Phishing

- Phishing at Indonesia IP to fake login to, for example, NetFlix.
- Phishing abroad banking at Indonesia IP.
- Phishing at Indonesia government websites.



Response



3. EVENT

3.1 DRILL

- ID-CERT participated in APCERT Drill, held on July 31, 2019.
- ID-CERT together with BSSN had a CIIP Drill, held on September 2019 at Bali.

3.2 SEMINAR & ETC

- January 2019
  - ID-CERT as Advisor for BSSN, cooperate with PT Xynexis in drafting CSIRT regulations.
- February 2019
  - ID-CERT Annual Gathering XI, held on February 14, 2019 at Bandung.
  - ID-CERT Chairman, Budi Rahardjo MSc., PhD., attended Cyber Intelligence Asia VII held on February 27-28, 2019 at Bangkok as keynote speaker.
- September 2019
  - ID-CERT Manager, Ahmad Alkazimy, attended APCERT Annual General Meeting 2019 held on September 29 – October 2, 2019 at Singapore.

4. FUTURE PLAN

4.1 FUTURE PROJECT

- Malware Survey
- Malware Wiki
- Malware Advisory

4.2 FRAMEWORK

4.2.1 FUTURE OPERATION

- Incident Handling
- IMR respondent addition
- Internal infrastructure improvement/development
- ID-CERT Annual Gathering XII
- Training

5. CONCLUSION

ID-CERT wants to focus on Malware Research and hopes that other CERTs could help and give some input, suggestion, or advice about it.

ID-SIRTII/CC

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

1. Highlight of 2019

1.1 Summary of major activities

Activities of Id-SIRTII/CC last year consist of:

- Indonesia as Deputy Chair of OIC-CERT 2018 – 2020.
- Indonesia as Board Member of OIC-CERT 2018 – 2020.
- Establishment Government CSIRT Indonesia (Indonesia Gov-CSIRT).
- 22 January 2019 : Speaker for Technical Guidance Cyber Security for Election in General Elections Commissions, Indonesia.
- 26-27 February 2019 : Participated in 2019 1st ASEAN – Japan Cyber Security Working Group Meeting in Vietnam.
- 13 March 2019 : Speaker for sharing knowledge related to Intrusion Detection System (IDS) in Jakarta.
- 23-24 April 2019 : Participated in the 2019 2nd ASEAN-Japan Cyber Security Working Group Meeting in Malaysia.
- 16-21 June 2019 : Participated in 31st Annual FIRST Conference in Edinburgh.
- 21-22 June 2019 : Participated and Speaker in 14th Annual Technical Meeting for CSIRTs with National Responsibility (NatCSIRT).
- 27 – 28 June 2019 : Speaker for German Indonesia Chamber of Industry and Commerce in Jakarta.
- 12 July 2019 : Speaker for Swiss German University in Jakarta.
- 31 July 2019 : Participated in APCERT 2019 Online Cyber Security Drill.
- 3-5 September 2019 : Participated and Speaker in National Cyber Security Seminar for Timor Leste Computer Security Incident Response Team (TL-CSIRT).
- 4 September 2019 : Participated in Online ASEAN CERT Incident Drill (ACID) 2019.
- 11 September 2019 : Speaker for accompaniment NSOC project for Head of Dept. of ICT DKI Jakarta.
- 15 September 2019 : Participated in FIRST and ITU-ARCC Regional Symposium for Africa and Arab Regions,Oman.
- 25 September 2019 : Speaker for Directorate General of Civil Aviation, Ministry of Transportation

- 29 September-2 October 2019 : Participated and Speaker in APCERT Annual General Meeting 2019 in Singapore.
- 27-31 October 2019 : Participated and Speaker in OIC-CERT 11th Annual Conference 2019 in conjunction with The Regional Cybersecurity Week 2019, Oman.
- 30 October 2019 : Participated in Forum Group Discussion for draft of Cyber Security and Cyber Resilience Law, Indonesia.
- 11-12 November 2019 : Participated in Seminar "Invitation to be on 7th ASEAN CIO Forum", Thailand.
- 4 December 2019 : Speaker for Indonesian National Institute of Aeronautics and Space.

1.2 Achievements and milestones

Achievement and milestones of Id-SIRTII/CC such as:

- 3-5 September 2019 : Id-SIRTII/CC as a experts and trainer in Capacity Building Program for Cyber Security in Timor Leste.
- 24-27 September 2019 : Participated and Speaker in OIC-CERT Academic Colloquium 2019 in Malaysia.
- 3 September 2019 : Conducted OIC-CERT Online Training Q4 as Capacity Building Program for all member OIC-CERT.
- 16-18 October 2019 : Hosted FIRST Technical Colloquia 2019 in Depok, West Java.
- 5 November 2019 : Conducted OIC-CERT Online Training Q4 as Capacity Building Program for all member OIC-CERT.

Apart from that ID-SIRTII / CC also helped provide cyber security assistance in the successful implementation of general elections and presidential elections 2019 in Indonesia. In 2019, Id-SIRTII/CC also complete of developing a CERT readiness index in order to measure the readiness and maturity of CERT Team in an organization.

2. About Id-SIRTII/CC

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 networks from both inside and outside country, particularly in the security measures 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.

3. Report

3.1 Activities and Operations Monitoring Report

In 2019, Id-SIRTII/CC operations monitoring report can be summarized as follows:

- Received 4,224 complaint reports in total. Most of report coming from local with 3.523 (83,4%) report categorized as verified report, such as website incident, web/application vulnerability, indicator of compromise, phishing and negative content.
- Found 290,381,283 cyber attacks both from local and overseas, which are dominant by malware infection (e.g. malware info stealer) and hacking activity.

3.2 Statistics

Cyber complaint reports to Id-SIRTII/CC in 2019 were categorized as shown in Figure 1. About 81% of the reports were on vulnerability, followed by phishing (9%), website incident (9%), and others (1%).

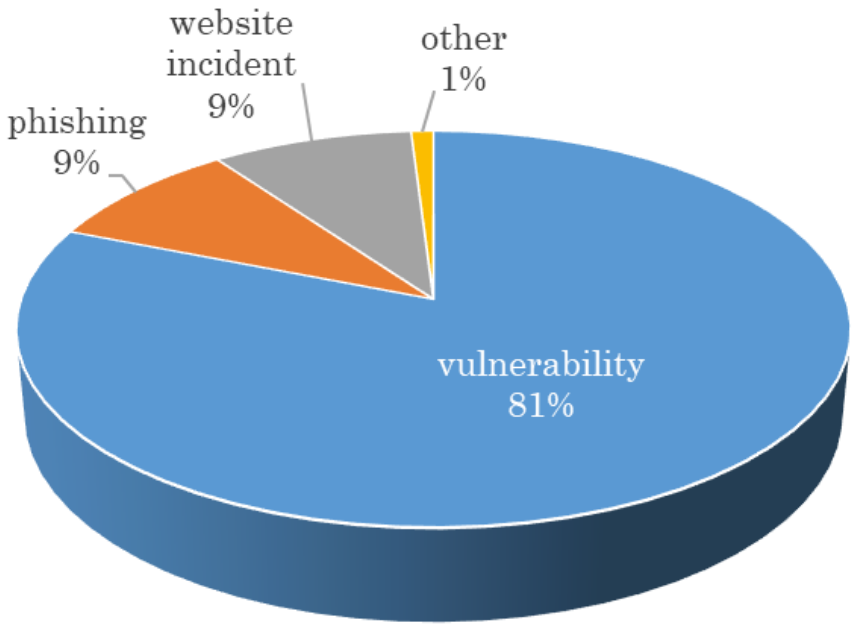


Figure 1. Reports in 2019 Based on Content Category

Based on the sector categories reported as shown in Figure 2, about 52% of the reports were on government sector, followed by national critical infrastructure (25%), digital economic (11%) and others (12%).

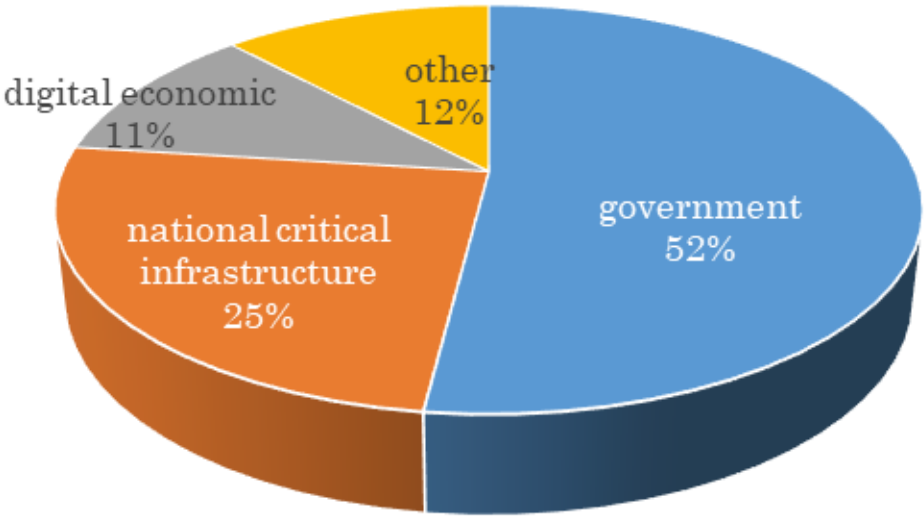


Figure 2. Reports in 2019 Based on Sector Category

In 2019 Id-SIRTII/CC found Cyber Attack Trend in 2019, the highest trend is Malware Attack (39%), followed by Account Hijacking (16,7%), vulnerability (5%). (see in Figure 3).

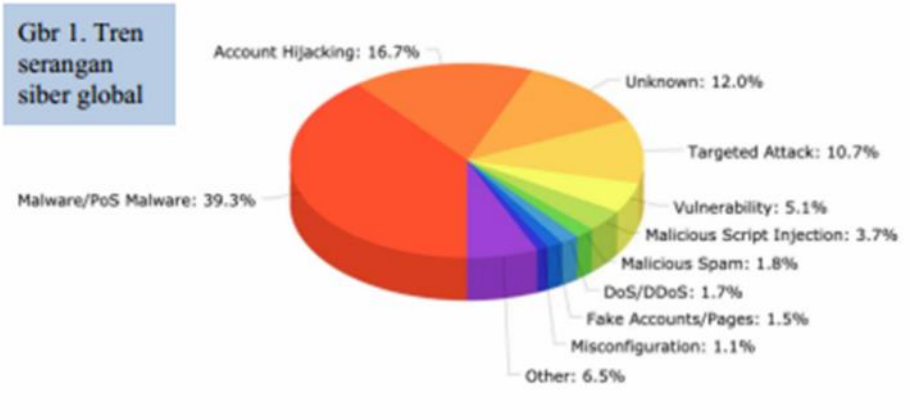


Figure 3. Global Cyber Attack Trend in 2019

Id-SIRTII/CC also found trend of Anonymous users having increase since 2017, 2018 until the end 2019 in Indonesia. Trend of anonymous users in Indonesia shown in Figure 4.

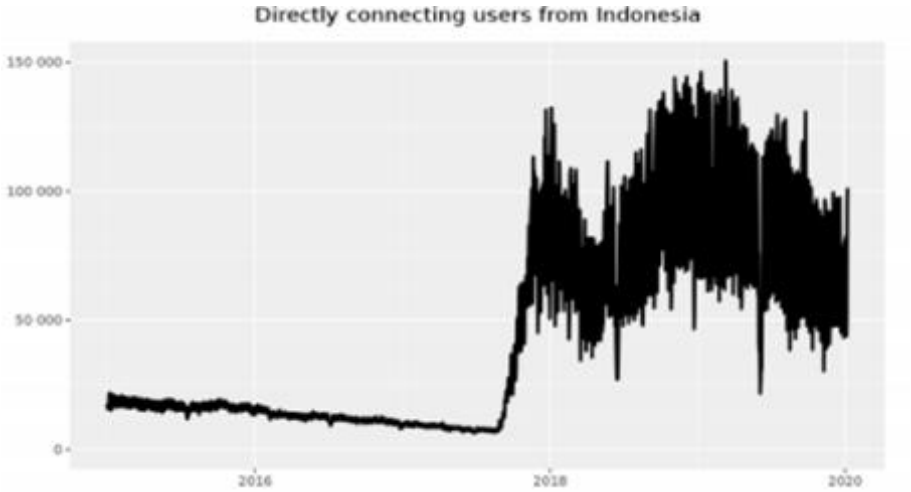


Figure 4. Anonymous Users Trend in 2019

3.3 Publications

Every month Id-SIRTII/CC publish its National Monitoring Monthly Report and every year. Id-SIRTII/CC publish Annual Cyber Security Report for public.

Figure 5. Id-SIRTII/CC Annual Report 2019

4. Events Organized / Hosted

4.1 Conferences and Seminars

In 2019, Id-SIRTII/CC participated on FIRST Technical Colloquia 2019 on 16-18 October 2019, Hotel Margo City Depok, West Java.

4.2 HandsOn Workshop and Training

In 2019, Id-SIRTII/CC also conducted the following events as a part of cybersecurity capacity building program in Indonesia:

- Advance Presistent Threat (APT) workshop.
- IoT workshop.
- Web Application Security Assessment workshop.
- Creating and Managing CSIRT workshop.
- National Cyber Exercise/Table Top Exercise (TTX) to improving cyber resiliency through partnership and coordination.

5. International Collaboration

5.1 International Partnerships and Agreements

Id-SIRTII/CC maintains its partnerships and agreements with other CERT organizations such as JP-CERT/CC, CNCERT, Cybersecurity Malaysia, CERT Australia, LaoCERT, and any other cyber security related entities such as national university and

foreign university, association/community and company/private sector.

5.2 Capacity Building

In 2019, Id-SIRTII/CC participated to the following international cyber security events:

- Id-SIRTII/CC joined as a participant in Asia Pacific Internet Security Conference (APISC) Training Course 2019 in Korea.
- Id-SIRTII/CC joined as a participant in Asean-Japan Cybersecurity Capacity Building Centre (AJCCBC) training in Thailand.
- Id-SIRTII/CC as a experts and trainer in Capacity Building Program for Cyber Security in Timor Leste.
- Id-SIRTII/CC joined as participant in Malaysian Technical Cooperation Programme (MTCP) Course: Certified Cyber Defender OIC-CERT 2019 Associate in Malaysia.
- Id-SIRTII/CC joined as participant in JICA Cyber Security Training Program 2019 in Japan.
- Id-SIRTII/CC joined as participant in ASEAN CTF Event in Australia.
- Id-SIRTII/CC joined as participant in Cyber Bootcamp Programme in Australia.

5.3 Conferences and Presentation

In 2019, Id-SIRTII/CC participated and dispatched speakers to the following international cyber security events:

- Participated in 31th Annual FIRST Conference (Edinburgh).
- Participated as a member in OIC-CERT 11th Annual Conference 2019 (Oman).
- Participated in Asia Pacific Internet Security Conference/APISC (Korea).
- Participated in 14th Annual Technical Meeting for CSIRTs with National Responsibility (Edinburgh).
- Participated in APCERT Annual General Meeting 2019 (Singapore).

6. Future Plans

Since April 2018, Id-SIRTII/CC moved to the New established National Cyber and Crypto Agency (NCCA) and works under the National Cyber Security Operation Center. Based on this NCCA vision, mission and its function, Id-SIRTII/CC has to changes and consolidate its function to match with its main organization.

Plans to be carried out by Id-SIRTII/CC are

- updating Point of Contact Indonesia for APCERT, OIC-CERT, Deputy Chair for OIC-

CERT, member of FIRST and ASEAN Regional Forum on ICT Security.

- Id-SIRTII/CC will also help local government and ministries/agencies in Indonesia to build their own CERT Team in order to improve cybersecurity readiness in facing cybersecurity incident.
- Id-SIRTII/CC will conduct an assessment of incident readiness and maturity of CERT Team in an organization, especially for local government and ministries in Indonesia.

Id-SIRTII/CC Contact Information

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 2019

1.1 Summary of major activities

- "Research on Latin American and Caribbean CSIRT Trends (FY2018)" published
  JPCERT/CC has published the " Research on Latin American and Caribbean CSIRT Trends (FY2018)," which summarizes the results of a research regarding the CSIRTs of Latin American and Caribbean nations as well as organizational structure and other matters concerning cyber security, based on published literature and local interviews.

  Research on Latin American and Caribbean CSIRT Trends (FY2018) (Japanese only)
  https://www.jpcert.or.jp/research/20190307_LACSIRT-survey.pdf

- Developed tools for incident response/investigation
  JPCERT/CC has developed some tools to help incident response and investigation and release them on GitHub. In 2019, MalConfScan and MalConfScan with Cuckoo, which extracts malware's configuration information, were released. These tools are compatible with more than 20 malware families.

  https://github.com/JPCERTCC/MalConfScan
  https://github.com/JPCERTCC/MalConfScan-with-Cuckoo

1.2 Achievements & milestones

- Suguru Yamaguchi, First Board Chairman of JPCERT/CC, inducted into the Internet Hall of Fame
  On September 27, 2019, it was announced that Dr. Suguru Yamaguchi, a founding member of JPCERT/CC and its first Board Chairman, had been inducted into the Internet Hall of Fame. The Internet Hall of Fame is a program whose objective is to recognize individuals who have made extraordinary contributions to the development of the Internet. Dr. Yamaguchi's induction is in recognition of his dedication to research and capacity building on cyber security, contributions to

FIRST, which is an organization in which CSIRTs around the world participate, efforts to enhance collaboration among CSIRTs in Africa and Asia, and leadership in the WIDE Project and AI3. Dr. Yamaguchi passed away in May 2016.

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 organization, 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 2019, JPCERT/CC received 18,070 computer security incident reports from Japan and overseas.

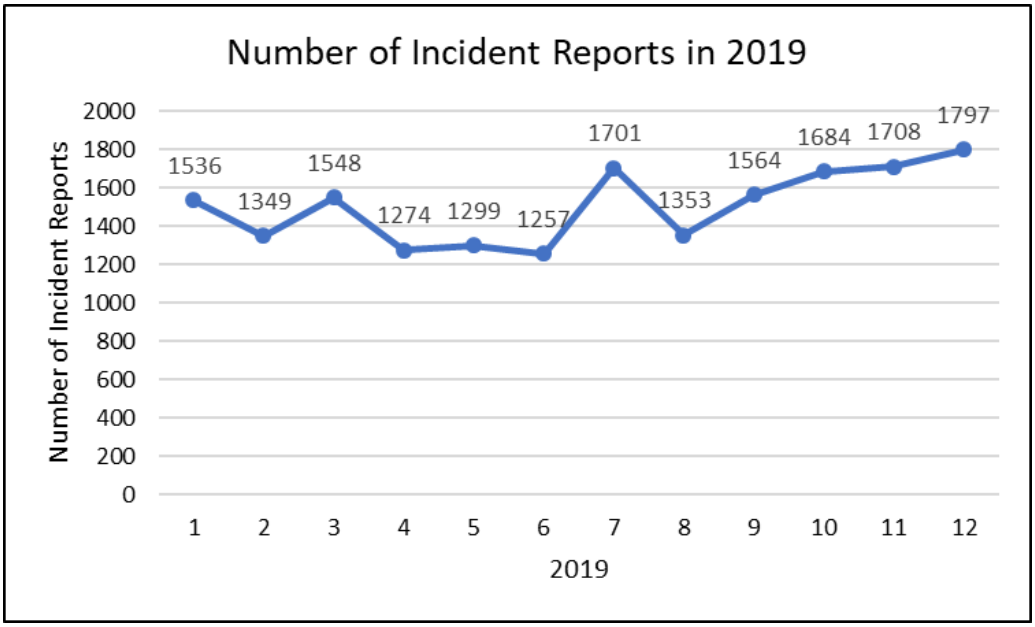


Figure 1: Number of Incident Reports (2019)

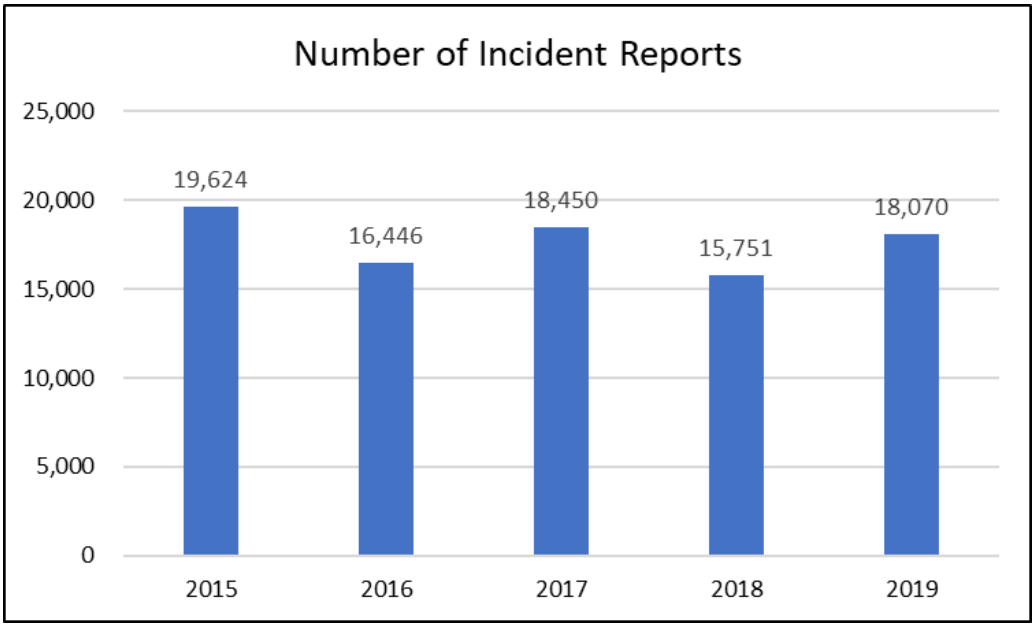


Figure 2. Incident reports to JPCERT/CC (2015-2019)

3.2 Abuse statistics

Incidents reported to JPCERT/CC during the last quarter of 2019 were categorized as in Figure 3. About 70% of the reports were on phishing site, followed by scan and website defacement.

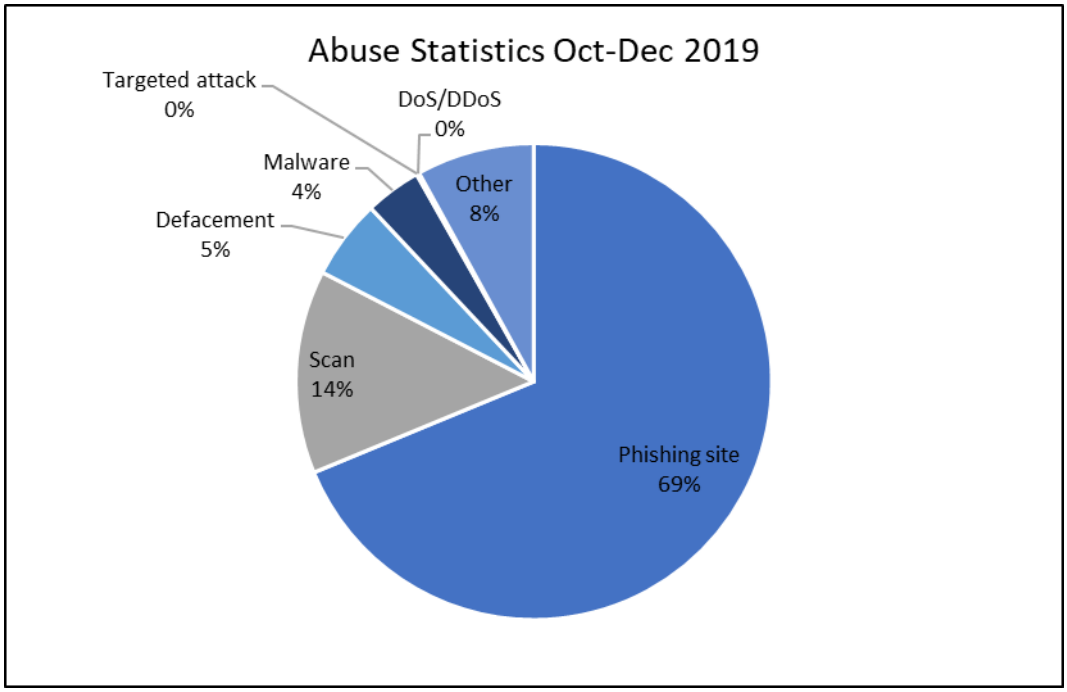


Figure 3. Abuse Statistics of Oct-Dec 2019

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 2019, 46 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 2019, 130 vulnerabilities coordinated by JPCERT/CC were published on JVN. 74 were cases published with IPA through the Information Security Early Warning Partnership, and 56 were published through partnerships with overseas coordination centers, developers, researchers, etc.

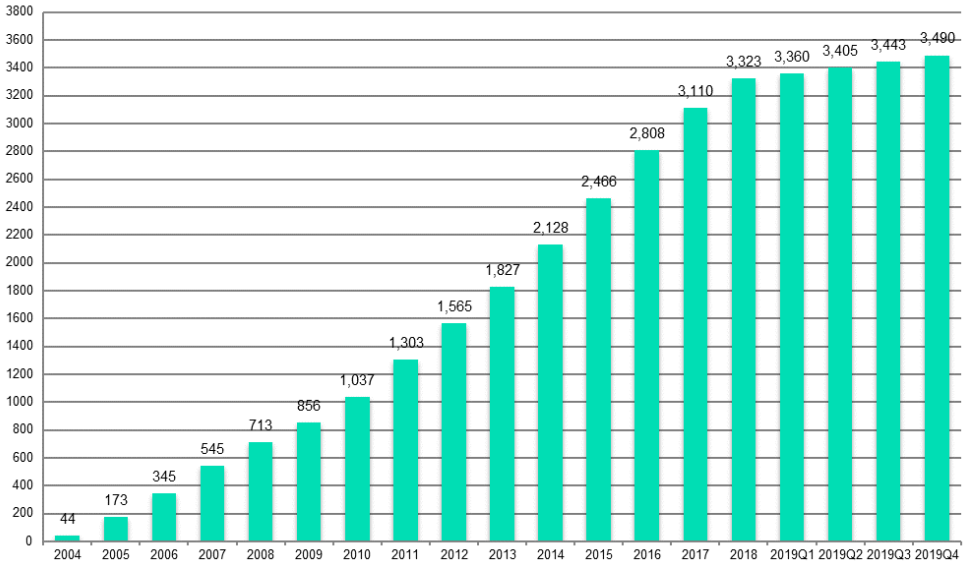


Figure 4: Number of vulnerabilities published on JVN by year

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.

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

  In April 2019, JPCERT/CC published the English version of "Cyber Security First Step for Introducing IIoT to the Factory". This document provides a basic guide to cyber security for introducing IIoT devices to a factory, especially for small and

medium-sized business. Audience of this document are business owners, factory managers, system administrators, and factory engineers.
https://www.jpcert.or.jp/ics/ICS-Security1stStep2018_en.pdf

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

- **Demonstration Test: Internet Risk Visualization – Mejiro**
  https://www.jpcert.or.jp/english/mejiro/
  JPCERT/CC has launched a demonstration test to visualize risks on cyber space based on data provided by multiple sources in comparison to the number of IP addresses assigned to each economy. Users can select a region and specify a period to perform analyses from various angles and obtain a more accurate picture of the situation.

3.5 Associations and Communities

- **Nippon CSIRT Association**
  https://www.nca.gr.jp/en/index.html (English)
  The Association is a community for CSIRTs in Japan. JPCERT/CC serves as a member of the Steering Committee and the Secretariat for the Association.

- **Council of Anti-Phishing Japan**
  https://www.antiphishing.jp/ (Japanese)
  JPCERT/CC serves as the Secretariat for the Council of Anti-Phishing Japan.

4. Events

4.1 Trainings, Seminars and Workshops

JPCERT/CC offers trainings, seminars and workshops for technical staff, system administrators, network managers, etc. JPCERT/CC hosts the 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. In 2019, JPCERT/CC newly signed an MoU with AusCERT and UZ-CERT.

- **FIRST (Forum of Incident Response and Security Teams)**

  https://www.first.org

  JPCERT/CC contributes to the international CSIRT community and served as a member of the Board of Directors of FIRST. JPCERT/CC also supports CSIRTs who wish to become a member of FIRST. In 2019, JPCERT/CC supported PLDT, a telco in the Philippines 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 Training

JPCERT/CC dispatched experts to the following trainings/projects/events in 2019

- ICS security, Mejiro training at Africa Internet Summit (June, Kampala)
- Active Directory log analysis (October, Depok)

5.2.2 Drills & Exercises

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

- APCERT Drill 2019 (31 July)
- ASEAN CERTs Incident Drill (ACID) 2019 (4 September)

5.2.3 Seminars & presentations

In 2019, JPCERT/CC dispatched speakers to the following international cyber security events:

- ICANN APAC and TWNIC Engagement Forum (April, Taipei)
- PHDays 2019 (May, Moscow)
- 31st FIRST Annual Conference (June, Edinburgh)
- National CSIRT meeting (June, Edinburgh)
- Thailand Cybersecurity 2019 (June, Bangkok)
- Asia Pacific School of Internet Governance (July, Bangkok)
- Blackhat USA 2019 (August, Las Vegas)
- Virus Bulletin Conference 2019 (October, London)
- MNSEC2019 (October, Ulaanbaatar)
- Global Forum on Cyber Expertise (October, Addis Ababa)
- World Internet Summit (October, Wuzhen)
- 8th Regional Cyber Security Summit (October, Muscat)
- Internet Governance Forum 2019 (November, Berlin)

...and many more

5.3 Other international activities

Below are some of the international events that JPCERT/CC attended in 2019:

- S4x19 (January, Miami)
- PSIRT Technical Colloquium 2019 (April, Hillsboro)
- Kaspersky Security Analyst Summit 2019 (April, Singapore)
- RSA Conference US 2019 (April, San Francisco)
- ISO/IEC JTC 1/SC 27 Working Group Meeting (April, Tel Aviv) (October, Paris)
- TF-CSIRT MISP training / IHAP(May, Luxemburg)
- DEF CON CHINA 1.0 (May, Beijing)
- Objective by the Sea v2 (June, Monte Carlo)

- M3AAWG 46th General Meeting (June, Budapest)
- RECON MONTREAL 2019 (June, Montreal)
- 28th USENIX Security Symposium & Workshop (August, Santa Clara)
- DEFCON 27 / BsidesLV (August, Las Vegas)
- CppCon2019 (September, Denver)
- M3AAWG 47th General Meeting (October, Montreal)
- Microsoft BlueHat Seattle 2019 (October, Seattle)
- 2019 FIRST Regional Symposium – Small Island Developing States (November, Nadi)
- Zero Nights 2019 (November, St. Petersburg)
- Botconf 2019 (December, Bordeaux)

…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

- **Engagement in cyber norm discussion**

  JPCERT/CC has been involved in several fora of cyber norm discussion (GCSC, IGF, etc). It is JPCERT/CC's plan to continue the engagement from the technical point of view.

- **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

KrCERT/CC

Korea Internet Security Center – Korea

1. Highlights of 2019

1.1 Summary of major activities

KISA, the host organization of KrCERT/CC, established Cyber Security Bigdata Center in December 2018 to respond to sophisticated cyber attacks. And the center started its full function officially since 2019. Also, KISA formed a new division, the Convergence Security Division, to adjust to diversifying cyber environment.

KrCERT/CC conducted a regular cyber drill with specific fields such as the energy and crypto currency service. Besides, KrCERT/CC established a cooperative relation through MoU, hosted cyber security capacity programs, led the cybersecurity alliance, etc. to enhance the level of cyber security with the APCERT members.

1.2 Achievements & milestones

The Cyber Security Bigdata Center collects data from KrCERT/CC's detection and analysis, cooperating with our partners. KrCERT/CC provides the processed data including malicious IPs, malware, C&C servers, distribution sites and etc. KrCERT/CC opens the platform and the data to domestic enterprises to let them improve their defense ability using the data. Also, KrCERT/CC hosted training programs for lecturing how to use the data. KrCERT/CC has endeavored to encourage the private sector to use the big data through all these activities.

KrCERT/CC regularly conducts a cyber drill on response to phishing emails, DDoS, and vulnerabilities of websites. This year, KrCERT/CC conducted the drill with the energy companies, crypto currencies which had been targeted by cyber threats recently. During the drill, which lasted about a month, KrCERT/CC started the drill without a notice in advance on the legitimate running servers of the enterprises. We received good opinions saying that it was a good opportunity to give a favorable reception to make sure the security awareness and investment needs of business executives.

In 2019, KISA established the new division, the Convergence Security Division, which aims to publish the countermeasures of ICT convergence security enhancement, to establish the foundation of ICT convergence security, and to improve the security level

of convergence facilities and devices. The scope of the ICT convergence is wide and there will be great damage to property and life when occurring cyber threats. So, cyber security is necessary to this area. The Convergence Security Division chose 5 essential services, smart factories, autonomous cars, digital healthcare, smart cities, and realistic contents. KrCERT/CC supported publish of 'Strategy of 5G+ Essential Services Convergence Security Enhancement' published by the Information Communication Strategy Committee. Also, KrCERT/CC developed the checklist of vulnerabilities for smart factories and provided the technical specification of the security authentication of autonomous cars. KrCERT/CC certified the IoT products such as digital door-locks, smart chargers, and smarthome applications to guide the users purchase the secure IoT devices.

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, one center with fourteen teams.

KrCERT/CC carries out various responsive and preventive programs designed to minimize cybersecurity damage by enabling a promptly response to incidents and to increase awareness in order to prevent incident.

2.2 Establishment

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

2.3 Resources

As of Dec. in 2019, around 160 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 cybersecurity framework and the 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.

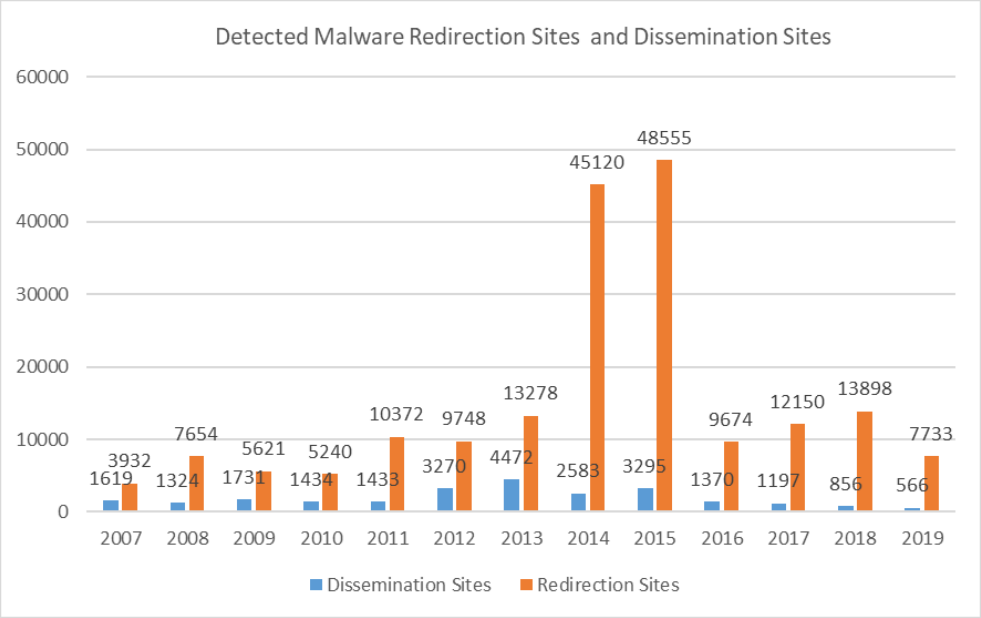
3. Activities & Operations

3.1 Scope and definitions

KrCERT/CC works for the safe and reliable cyber space by preventing cyberattacks and enhancing countermeasures. The mission of it is 1) to guarantee a rapid response to major nationwide Internet incidents to prevent and minimize damages, 2) To cooperate closely with domestic(ISPs, anti-Virus Companies) and foreign partners(FIRST, APCERT, etc.), 3) 7 days/24 hours Monitoring, Early Detection/Response on cyberattacks in the private sector.

3.2 Abuse statistics

Compared with the number of last year, the number of compromised website distributing hidden malware decreased in 2019 by 34% from 856 to 566. The number of redirection sites also decreased by 4% from 13,898 to 7,733.



3.3 Publications

KrCERT/CC semiannually publishes a malware detection report and issues advisory on its websites whenever a major security issue occurs. Also, on a quarterly basis, it uploads a cyber threat trend report on the website. Furthermore, an annual white paper in both Korean and English version is uploaded on the website.

4. Events organized / hosted

4.1 Training

KrCERT/CC held the 2019 APISC Training Course, which is an annual invitation-based security training course on CSIRT establishment and operation that KrCERT/CC has been hosted since 2005. The course opens a door for the participants from different countries mainly in the Asia-Pacific region to build a human network at the working-level which is one of the most important elements in cybersecurity incident response. 13 participants from 13 countries including Thailand, Myanmar, Malaysia, Indonesia participated in the 2019 training course and shared their expertise on cybersecurity structure and CERT operation.

KrCERT/CC also runs GCCD, the Global Cybersecurity Center for Development(GCCD) which was established in June 2015. In 2019, GCCD held seminars in Costa Rica and Laos. At the seminars, experts provided knowledge about CERT/CSIRT operation, information sharing, cyber incident handling experience, and etc.

4.2 Drills & exercises

KrCERT/CC hosted the largest domestic cyber threat drill in May 2019 with the Ministry of Science and ICT(MSIT) to check readiness of rapid cyber threat response and a systematic cooperative system in the private sector. 60 companies, including ISPs, security vendors, portal service providers, and cryptocurrency exchanges, participated in the drill. It includes penetration test for 23 websites conducted by distinguished white hackers in order to find and handle vulnerabilities.

KrCERT/CC also held a cyber drill with the energy sector. As the number of stealing information is growing, this drill focused on responding APT attacks and large volume of DDoS attacks to real websites, with penetration test by professional white hackers.

4.3 Conferences and seminars

In collaboration with the Ministry of Science and ICT, KISA hosts the 8th "Day of Information Security" celebration and "International Conference on Information Security(ICIS)" on July 10. Speakers share their view and experiences about cyber security on Infrastructures, recent cyber threat with technological innovation and so on.

Furthermore, KrCERT/CC holds a meeting on a regular basis with domestic organizations and entities for sharing expertise and know how under the name of "Cyber Threat Intelligence".

5. International Collaboration

5.1 International partnerships and agreements

KrCERT/CC signed the MoU with the members of APCERT, CSA of Singapore and CERT-In of India in November 2019. We expect fruitful cooperation with the APCERT members to improve cyber security level in our region.

Additionally, KISA leads the Cyber security Alliance for Mutual Progress, CAMP. The purpose of CAMP is enhancement of multilateral cyber security cooperation among members. Some of APCERT members also take part in the CAMP. Through CAMP, KrCERT/CC actively shared our knowledge, experiences, etc.

5.2 Capacity building

5.2.1 Training

KrCERT/CC participates in APCERT online training on a regular basis. KrCERT/CC participated in 3 APCERT online training in 2019. Also, KrCERT/CC attended various trainings and conferences such as RSA, Blackhat, etc. for improving the techniques and

knowhow and broaden views for cyber security. KrCERT/CC operates the training program itself. Any members of KrCERT/CC can host trainings regard to any cyber security topics to share knowledge, experiences, the latest trends with all members. Total 29 training programs were hosted by the members of KrCERT/CC. The topics were mostly technique of analysis, detection, recovery.

5.2.2 Drills & exercises

KrCERT/CC joined in the APCERT Drill in July 2019. The drill required the participants to solve virtual incident with 7 injects. Besides KrCERT/CC took part in the drill hosted by TWNCERT as an observer. Also, the other drill KrCERT/CC participated in was 14th ACID(ASEAN CERT Incident Drill) which hosted by CSA(Cyber Security Agency of Singapore). 2019's theme was "Combat Evolving Cyber Threats with Good Cyber Hygiene".

5.2.3 Seminars & presentations

KrCERT/CC took part in the following seminars and conferences:

- FIRST TC at APRICOT 2019 in February 2019, Daejeon, Korea
- FIRST AGM and conference in June, Edinburgh, the U.K.
- 2019 APCERT AGM in October, Singapore

6. Future Plans

KrCERT/CC is operating Malware Information Sharing Platform(MISP) and is planning to discuss with partners for information sharing through MISP since 2020. Also, KrCERT/CC will release the several Korean guidance and the analysis report in English to enhance information sharing with APCERT member and partners.

7. Conclusion

Technology in cyber space is getting evolving and devices are getting more connected. The changes give challenges and require more developed skills for cyber security. KrCERT/CC will improve its capability by embracing new technology and face proactively with challenges. KrCERT/CC will try diverse attempt to safer and securer cyber space and contribute to cyber security in the world.

LaoCERT

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

1. Highlight of 2019

1.1 Summary of Activities

- GCCD-Lao PDR Cyber Security Joint Seminar for the government and private technical authorities on 26 November 2019 in Vientiane Capital, Lao PDR.

1.2 1Achievements & milestones

- Data protection Law.
- Guidelines on the implementation of Prevention and Combating Cyber Crime Law.
- Guidelines a measure on how to protect the website to be secure.

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 2019.

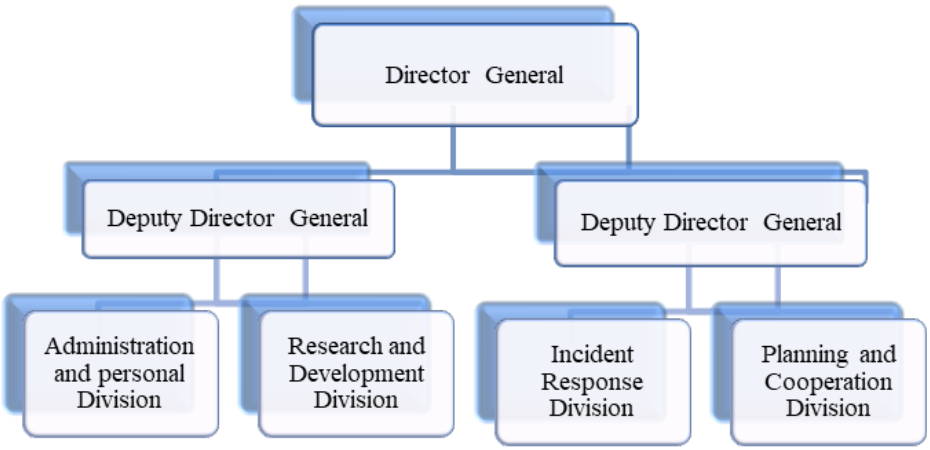
2.2 Establishment

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

- Cellebrite Certified Physical Analyst
- Computer Hacking Forensic Investigator



LaoCERT Organization Charts

2.4 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.

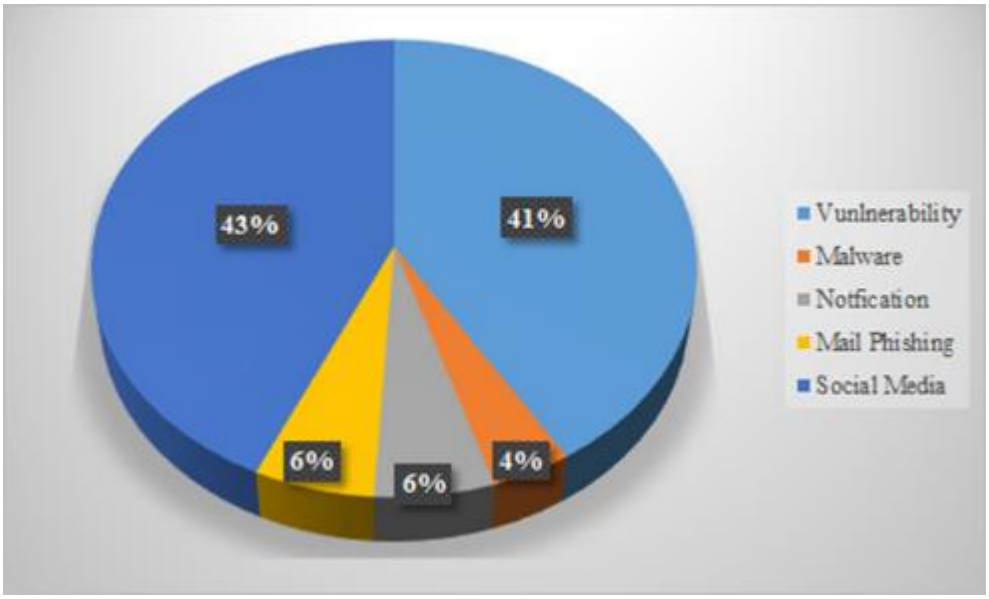
3. Activities & Operations

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.

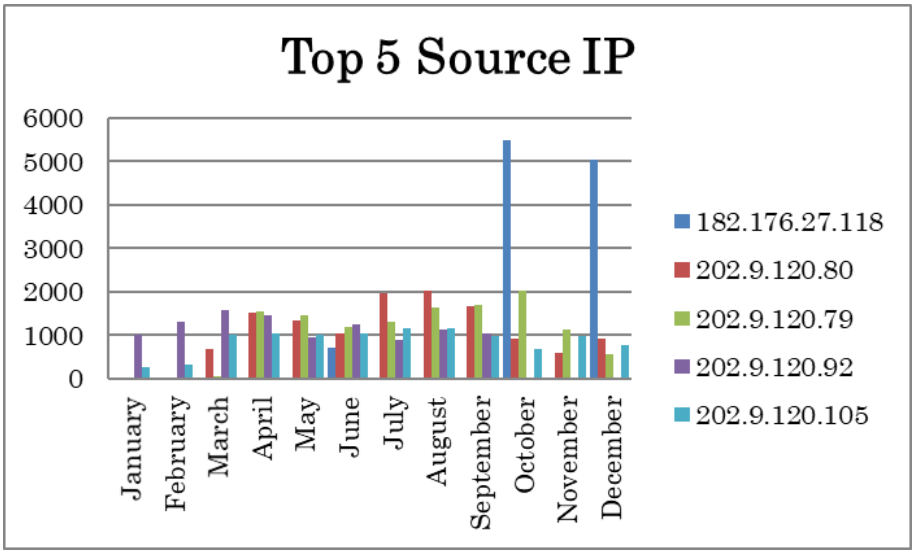
3.2 Incident handling report

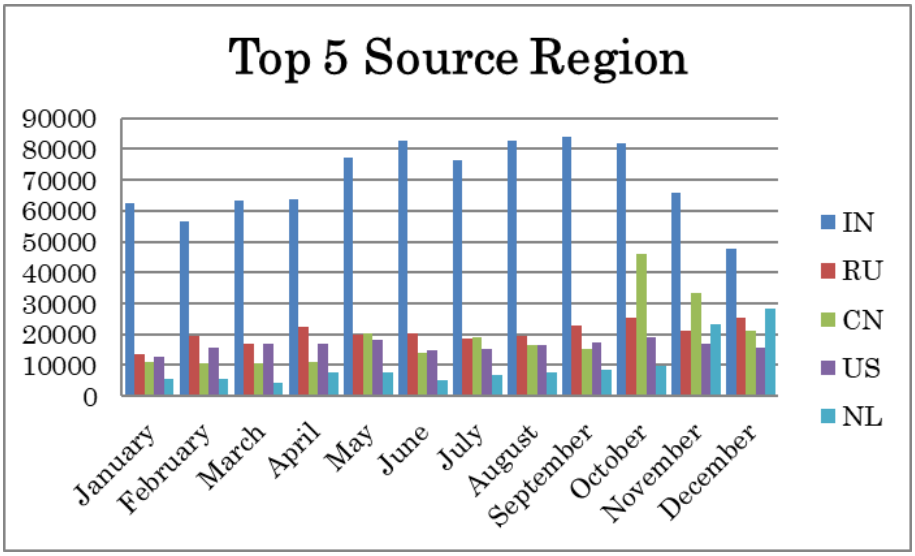
The following graph shows the statistic of incidents that happened in 2019.

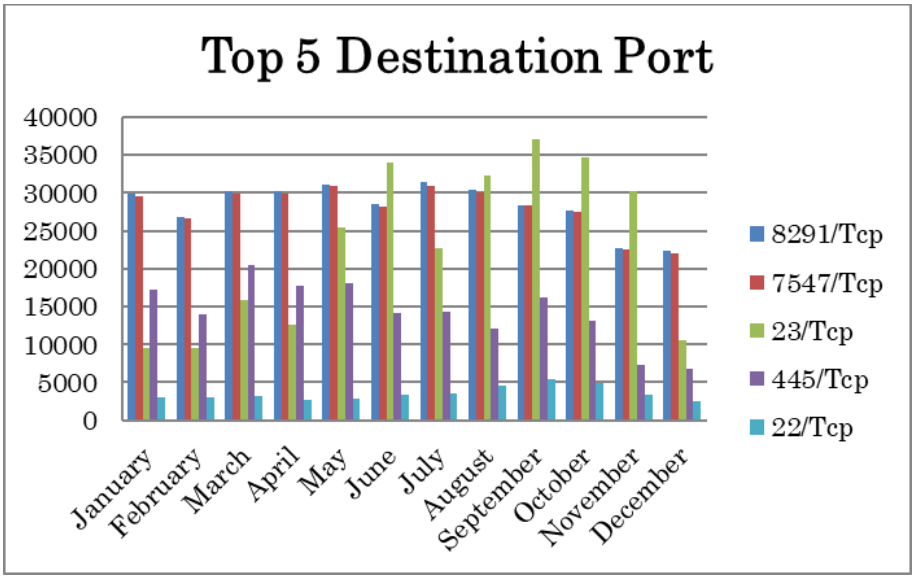


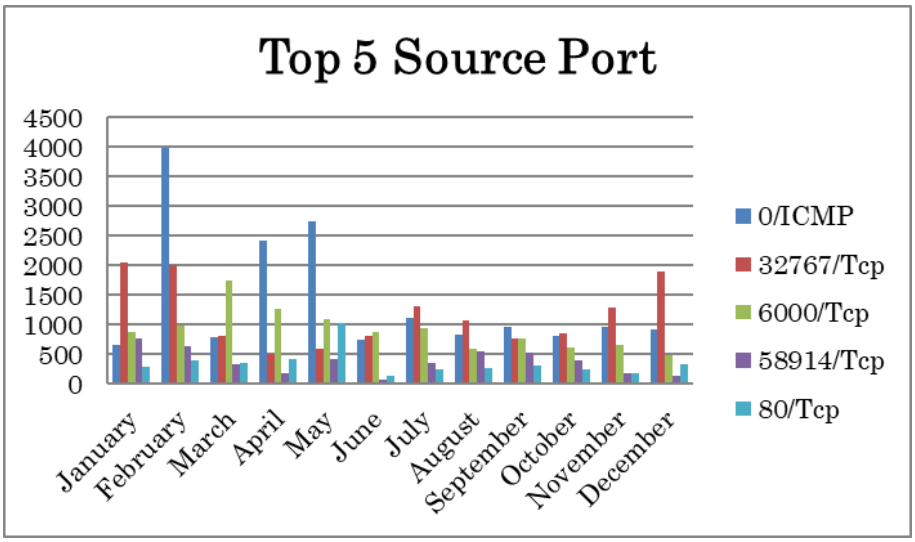
3.3 Abuse Statistics (TSUBAME Sensor)

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 2019.




Top 5 Source Region
90000
80000
70000
60000
50000
40000
30000
20000
10000
0
January
February
March
April
May
June
July
August
September
October
November
December
IN
RU
CN
US
NL


Top 5 Destination Port
40000
35000
30000
25000
20000
15000
10000
5000
0
January
February
March
April
May
June
July
August
September
October
November
December
8291/Tcp
7547/Tcp
23/Tcp
445/Tcp
22/Tcp


Top 5 Source Port
4500
4000
3500
3000
2500
2000
1500
1000
500
0
January
February
March
April
May
June
July
August
September
October
November
December
0/ICMP
32767/Tcp
6000/Tcp
58914/Tcp
80/Tcp

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

- Dissemination and advisories on Cyber Crime Law and social media to provincial throughout the country.
- Create 11 pcs tips poster for using the computer to be secure to public and private sectors.
- Create a pamphlet 5-minute information security company self-assessment in the ASEAN-Japan activities framework.

4. Events organized/hosted

4.1 Training

- Co-Organized the training on Network security and Desktop Exercise Managing a security incident for government official between 18-20 February 2019 in Vientiane capital, Lao PDR.
- Co-Organized the training on HPE Aruba Fundamental Initialization and System Administration and Forcepoint Fundamental Initialization and System Administration for government technical authorities on 31 May 2019 in Vientiane capital, Lao PDR.
- Co-Organized the training on Sangfor IAM Fundamental Initialization and System administration for government official on 30 August 2019 in Vientiane capital, Lao PDR.
- Co-Organized the training on Cryptocurrencies and Darknet Investigation for government technical authorities on 10-12 September 2019 in Vientiane capital, Lao PDR.

4.2 Conferences and seminars

- Co-Organized the Conference on Facebook community standard on 03 September 2019.
- Co-Organized the GCCD-Lao PDR Cyber Security Joint Seminar for the government technical authorities on 26 November 2019 in Vientiane Capital, Lao PDR.

5. International Collaboration

5.1 International partnership and agreement

- MOC signed with the Authorities Information Security (AIS) under the Ministry of Information and Communications of Vietnam on 03 November 2019.

5.2 Capacity Building

5.2.1 Training

The following has shown the statistic for attended the training in 2019:

- Capacity Building in Policy Formation for Enhancement of Measures to Ensure CyberSecurity in ASEAN on 27 January 2018 - 07 February 2019 in Japan.
- Practice Cyber Attack on 17 February – 2 March 2019.
- The 5th Training CYDER and Digital Forensics on 24-30 March 2019 in Bangkok, Thailand.
- The 6th Training of the ASEAN-Japan Cybersecurity Capacity Building Centre on 26 May – 01 June 2016 in Bangkok, Thailand.
- The Asia-Pacific Information Security Training Course 2019 on 08-12 July 2019 in South Korea.
- The 7th Training of the ASEAN-Japan Cybersecurity Capacity Building Centre on 07-13 July 2019 in Bangkok, Thailand.
- The 3rd ASEAN Japan Cybersecurity Working Group on 23-26 July 2019 in Japan.
- The Network Security Monitoring on 26-30 August 2019 in Hanoi.
- The Japan-US joint training on Industrial Control System Cybersecurity on 9-12 September 2019 in Japan.
- The 8th Training of the ASEAN-Japan Cybersecurity Capacity Building Centre on 08-14 September 2019 in Bangkok, Thailand.
- The 9th Training of the ASEAN-Japan Cybersecurity Capacity Building Centre on 10-16 November 2019 in Bangkok, Thailand.
- Jointed in the Singapore Cyber Conquest (SCC) on 01-03 October 2019 in Singapore.

- The UNODC Regional Darknet Training: Intelligence Collection for Law Enforcement on 04-08 November 2019 in Bangkok, Thailand
- Jointed in the ASEAN Students Contest on Information Security 2019 on 29 November 2019 in Hanoi, Vietnam.
- The training on Security Measures for the Era of Artificial Intelligence on 02-10 December 2019 in Nanjing, PR. China.

5.2.2 Drills and Exercises (Online)

The following has shown the statistic for participated Drills and Exercises in 2019:

- The 5G and ICT Applications on17-28 June 2019.
- The APCERT Cyber Security Drill on 31 July 2019.
- The ASEAN CERT Incident Drill (ACID) 2019 on 4th September 2019.
- The APCERT Web Application Penetration Testing Techniques.
- The APCERT Drill on 28-31 June 2019.

5.2.3 Seminar and presentation

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

- The 3rd ARF Open Ended Study Group on Confidence Building Measure to Reduce the Risk Conflict Stemming from the Use of Information Communication Technologies on 29 January 2019 in Singapore.
- The 1st ASEAN Japan Cybersecurity Working Group Meeting on 26-27 February 2019 in Hanoi, Vietnam.
- Cyber Intelligence ASIA Conference and Exhibition on 26-28 February 2019 in Bangkok, Thailand.
- The Cyber Intelligence ASIA Conference and Exhibition on 26-28 February 2019 in Malaysia.
- The CLMV Senior Level Workshop on International Cyber Security Policy and Diplomacy for CLMV Countries on 04-05 April 2019 in Myanmar.
- The 2nd ASEAN Japan Cybersecurity Working Group on 23-24 April 2019 in Kuala Lumpur, Malaysia.
- The workshop Optimising CERT Capabilities on 23-25 April 2019 in Singapore.
- The Regional workshop on "Norms of responsible state behaviour in cyberspace" on 11-12 June 2019, Kuala Lumpur, Malaysia.
- The Network Security Monitoring on 11-12 June 2019 in Malaysia.

- The INTERPOL Pre-operation Meeting on Operation GOLDFISH ALPHA on 12-14 June 2019 in Singapore.
- The ARF Workshop on Principles of Building Security in the Use of ICTs in the National Context on 25-26 June 2019 in Singapore.
- The 2019 Seminar on Cloud Computing and Big Data under Belt and Road Initiative on 08-30 July 2019 in PR. China.
- The UN-Singapore Cybersecurity Programme "UNSCP" Norm Awareness Workshop on 15-16 July 2019 in Singapore.
- The 3rd ASEAN Japan Cybersecurity Working Group on 23-26 July 2019 in Japan.
- The International Law of Cyber Operations on 13-23 August 2019 in Singapore.
- The 2nd Southeast Asai Crptocurrencise Working Group Meeting on 14-16 August 2019 in Singapore.
- The Reginal Workshop Enhancing the capacity of member States to Prevent and Investigate Cyber-Attacks by Terrorist Actors and Mitigate their impact on 03-06 September 2019 in Japan.
- The workshop of Strengthen Information Security in ASEAN: Develop Regional Security Best Practices on 11-13 September 2019 in Indonesia.
- The 4th Annual Meeting of the Cybersecurity Alliance for Mutual Progress (CAMP) on 30 September – 03 October 2019 in Seoul, Korea.
- The 3rd Singapore International Cyber Week and the 3rd ASEAN Ministerial Conference on Cybersecurity on 01-03 October 2019 in Singapore.
- The INTERPOL Pre-Operation Meeting on Operation Goldfish Alpha on 07-11 October 2019 in Singapore.
- The 12th ASEAN-Japan Cybersecurity Policy Meeting on 29-30 October 2019 in Thailand.
- The Dhaka Global Dialogue on 11-13 November 2019 in Bangladesh.
- The Norms of responsible state behavior in cyberspace on 27-28 November 2019 in Hanoi, Vietnam.

6. Future Plans

- Providing a training and seminar on cyber Security to provincial throughout the country.
- Implementing the threat monitoring system.
- Planning for Monitoring Critical National Information Infrastructure (CNII).

- Planning for Establishing Government Threats Monitoring (GTM).
- Develop national critical information infrastructure protection mechanism to enhance the robustness of Laos's national infrastructure.
- Expanding the awareness raising on data protection Law.
- Drafting National Cyber Security Policy.
- Drafting Cyber Security Law.
- Studying and planning to set up the Honeypot, HoneyNet.
- Establishing the project for training of cyber Security to public and private sector and POC in Lao PDR.
- Planning to set up the Network Monitoring System.

7. Conclusion

LaoCERT always keep continue to develop a team together with attempt to improve a skill capabilities of staff and also focused on devoting to Incident Handling, network security emergency response beside that we also strengthen the collaboration with other international cybersecurity organizations in order to enhance awareness raising activities and the related events on cybersecurity to public and private sectors and provide the training, seminars and workshop to promote legislation and Law on cybersecurity throughout the country consistently.

mmCERT

Myanmar Computer Emergency Response Team – Myanmar

1. Highlights of 2019

1.1 Summary of major activities

Facilitated “Myanmar Cyber Security Challenge” competition 2019" in January at Naypyidaw, Myanmar.

- Hosted the “4th Senior Level Workshop on International Cyber Security Policy and Diplomacy for CLMV Countries” jointly organized “ICT4Peace Foundation Switzerland” on 4 & 5 April 2019 at Nay Pyi Taw, Myanmar
- Hosted “Myanmar Cyber Security Challenge (Open Level)” competition jointly organized by University of Information Technology (UIT) on 11th August at Yangon, Myanmar.
- Participated in “2020 and Impact of Social Media” organized by President’s Office
- Held Cyber Security Awareness Seminar in Universities and Ministry.
    - Conducted the Incident Handling Courses
    - Delivered Incident Handling and CSIRT Management Courses
    - Gave the lecture and share the knowledge Crime Investigation Department (CID) under Myanmar Police Force Achievements & milestones

1.2 Achievements & Milestones

- mmCERT conducted the online Zero Day Malware Analysis Course for APCERT members.
- During 2019, mmCERT/cc solved total 144 cases of STOP ransomware infections and thus Cash flowing of USD 141,120 to the ransomware developer was reduced. mmCERT had assisted to STOP ransomware infected cases not only the constituencies but also from other countries such as Philippine, Malaysia, Pakistan, Sri Lanka, Brazil, South Africa, Jordan etc.
- mmCERT developed “Online Retrieve Tool” to claw back STOP ransomware online decryption keys.
- mmCERT shared practical experiences about “STOP” ransomware at international workshops and seminars.

2. About CERT

2.1 Introduction

Myanmar Computer Emergency Response Team (mmCERT) is a national computer emergency response team for handling cyber security incidents in Myanmar and it was a member of APCERT in 2011.

2.2 Establishment

mmCERT was established as a National Computer Emergency Response Team in Myanmar on July 23 2004 and mmCERT/cc (mmCERT coordination center) is strengthening on Dec 15 2010 . The Ministry of Transport and Communication (MOTC) is a leading Ministry of Information Technology and Cyber Security Department Activities in Myanmar and it provides budget to mmCERT/cc since then. In 2016, The Ministry of Communication and Information Technology (MCIT) was changed the name to the Ministry of Transport and Communication (MOTC).

2.3 Resources

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

2.4 Constituency

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

3. Activities & Operations

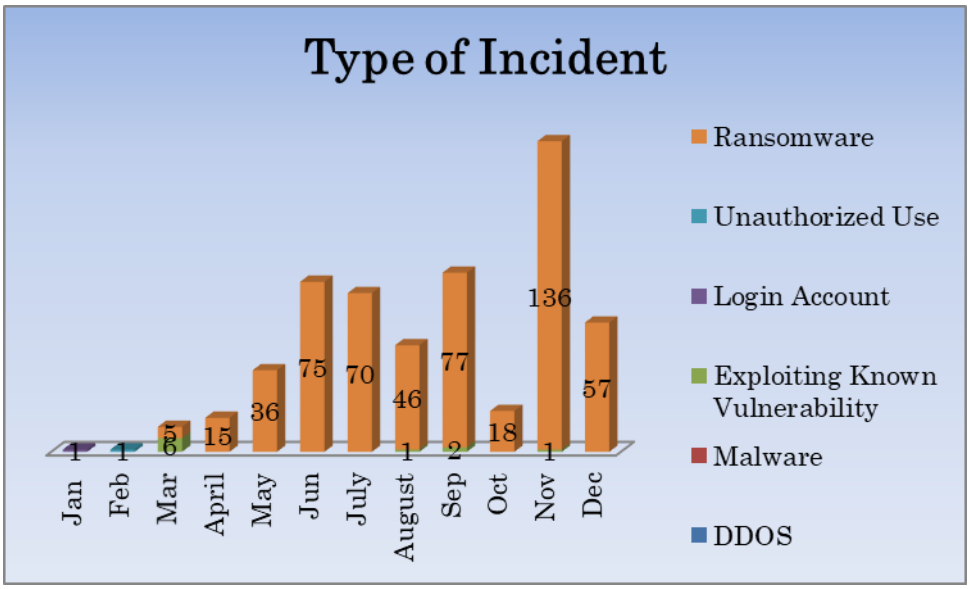
3.1 Scope and definitions

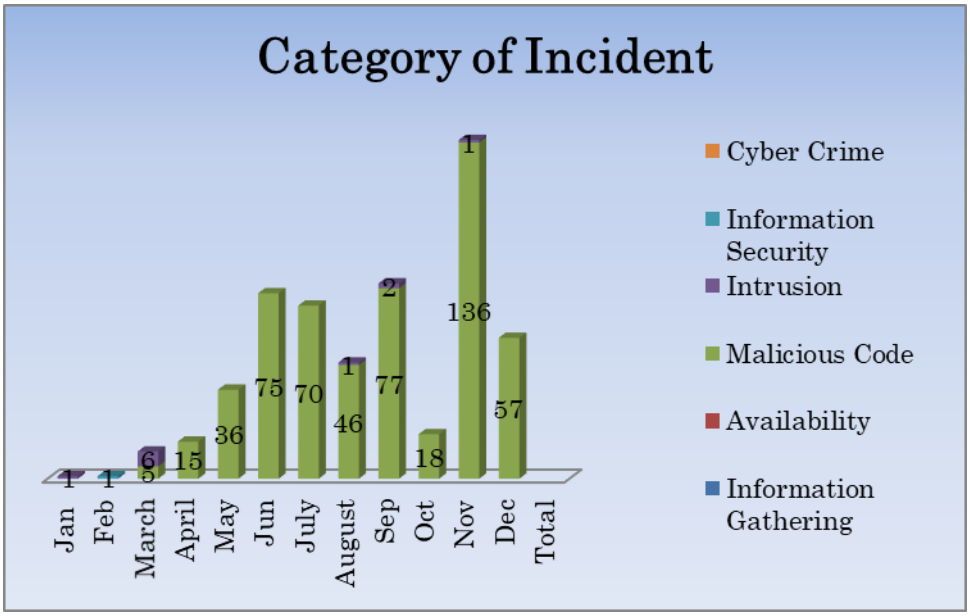
- Create National IT image by cooperating with international CERT teams for cyber security and Cyber crime
- Disseminate Security Information and Advisories

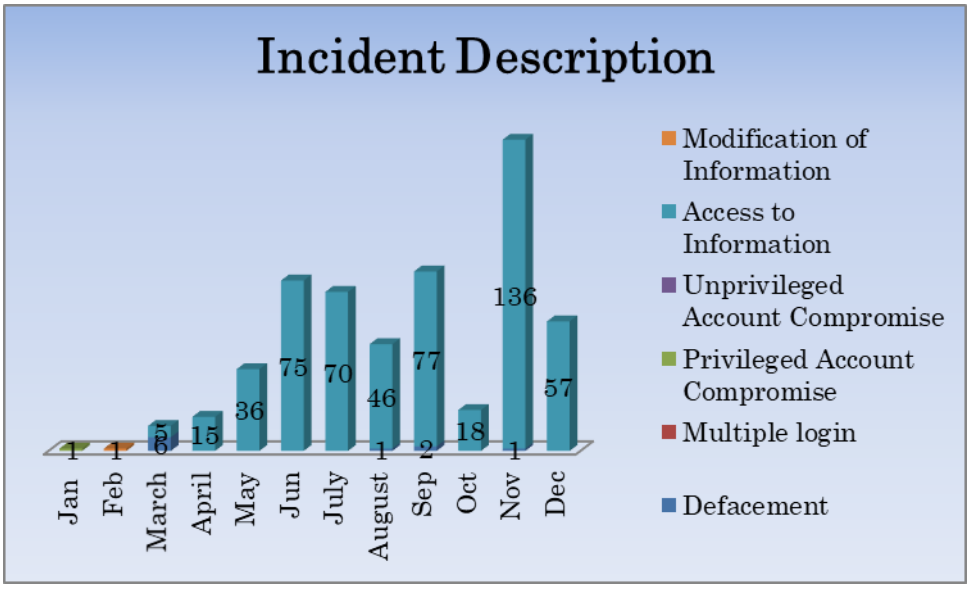
- Provide technical assistance
- Cooperate with law enforcement organizations for cyber crime

3.2 Incident handling reports

The following graph shows the incidents that were solved by mmCERT in 2019. According to the results on incident analysis by mmCERT, Ransomware Attacks were the most prominent incident cases in 2019.







3.3 Publications

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. The updated information about STOP Ransomware, most infecting one in Myanmar, can be known via mmCERT Facebook page. 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.

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 1.3 according to timely changes of encryption method of the developer. 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/

3.3.4 New services

Thorough out this year, mmCERT/cc had been reported many STOP ransomware cases and thus mmCERT mainly responded to STOP ransomware. In July, 2019 mmCERT/cc developed "STOP ransomware Online Key Retrieve Tool" and supported most of victims by performing necessary actions to the infected PC remotely. But this tool has a limitation to Salsala 20 Encryption Method only and later variants of STOP ransomware could not be fixed at this time. 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

mmCERT/cc conducted the Incident Handling Courses at the following universities and organizations:

- University of Computer Studies, Yangon on May 2019
- National Cyber Security Center on May 2019
- University of Computer Studies (Thaton) on 24 ~ 26 August 2019
- Technological University (Mandalay) on 12 ~ 15 November 2019

In order to raise awareness in Incident Responding, mmCERT/cc also provided Incident Handling Course in addition with CSIRT Management Course at the following universities and ministry:

- University of Computer Studies (Meiktila) on 16 ~ 21 September 2019
- Ministry of Information (Nay Pyi Taw) on 4 ~ 8 November 2019
- Technological University (Taunggyi) on 2 ~ 6 December 2019

mmCERT/cc trained the Internship Training Programme for the student of University of Computer Studies (Mandalay) from 13th May to 31st July 2019.

4.2 Drills & exercises

- In Youth All-Round Development Festival-2019 at Magway Division, Myanmar, mmCERT facilitated "Cyber Security Quiz" for basic education school level and university level.
- In order to boost incident response skill and cyber resilience, "Cyber Incident Drill" was also provided during this event.,
- In March 2019, mmCERT jointly hosted with Goldphish Company “Cyber Academy” Workshop in IAC, Naypyidaw. Successively. The online course wais provided in order to harden the knowledge of cyber security and resilience to CIOs and ACIO of government.

4.3 Conferences and seminars

- Hosted the “ 4th Senior Level Workshop on International Cyber Security Policy and Diplomacy for CLMV Countries” jointly organized “ICT4Peace Foundation Switzerland” on 4 & 5 April 2019 at Nay Pyi Taw, Myanmar
- In order to raise cyber awareness, mmCERT held Cyber Security Awareness Seminar at the following Universities:
  - University of Computer Studies (Mandalay) on 14th February 2019
  - Yangon Technological University on 30th July 2019
  - University of Computer Studies (Thaton) on 31st July 2019
  - University of Computer Studies (Hpa An) on 1st August 2019
  - Technological University (Mawlamyine) on 1st August 2019
  - University of Computer Studies (Meiktila) on 5th August 2019
- Developed and facilitated seminars, workshops and sharing the knowledge to the student of “University of Computer Studies, Yangon, Mandalay, Thahton and Meiktila”, Technological University Taunggyi and Mawlamyine and Crime Investigation Department (CID) and “Government Technological College (GTC).”
- Jointly hosted the “Cyber Leadership Awareness Workshop 2019” with ST Engineering (Singapore) & E-Lite Tech (Myanmar) in March 2019
- mmCERT also participated, presented and shared the knowledge about the cyber security status of Myanmar at Myanmar Digital Rights Forum, ICT for Education Forum, MMIX Peering Forum, Beside Myanmar and Myanmar Cyber Security Month.
- Jointly hosted the “Cyber Security Workshop for Myanmar” by Japan Ministry of

Internal Affair and Communications in January and December 2019

- Jointly hosted the "workshop on Protect Networks and Downstream from DDOS Attacks" by Secured Link Company, NEXUS GUARD & Asia Innov8 in September 2019
- Participated and presented at "Workshop on Prosecuting Cyber Crime and Handling Electronics Evidence" organized by U.S DOJ and Myanmar UAGO in November 2019

5. International Collaboration

5.1 International partnerships and agreements

mmCERT plans to be a member of Cybersecurity Alliance for Mutual Progress (CAMP) which serves as a platform where members take collective actions to keep cyberspace secured.

5.2 Capacity building

5.2.1 Training

- Members of mmCERT attended the training "Cyber Security Policy Course" provided by Japan JICA in January 2019.
- Attended Training Program for Defense Practice against Cyber Attacks at Japan in February 2019.
- Attended MOTC Study Tour to Japan organized by Japan Ministry of Internal Affairs and Communications in March 2019
- Attended "Cybersecurity Leadership Program" at Korea in Apirl.
- Attended "Cybersecurity-focused Study Tour" at United States of America in June.
- Pre-operation Meeting for Operation Goldfish Alpha organized by INTERPOL at Singapore in June.
- Attended ASEAN-JAPAN CYBERSECURITY CAPACITY BUILDING (AJCCBC) which provides
- CYDER Course, Network Forensic and Malware Analysis) in May, July, September and November 2019.
- Member of mmCERT attended the APISC Security Training Course at Seoul, Republic of Korea provided by KISA and KrCERT/cc in July 2019
- Member of mmCERT also attended "International Law of Cyber Operations" at Singapore jointly organized by Singapore Cyber Security Agency, Cyber Law

International, Australian Government and Ministry of Foreign Affairs of Netherland in August 2019

- Attended Japan-Us Industrial Control Systems Cybersecurity Training, Japan sponsored by Ministry of Economy, Trade and Industry (METI) and Information-Technology Promotion Agency in September 2019
- Attended Cyber Security Study Tour to Japan jointly organized by Japan Ministry of Internal Affair and Communications and World Bank Group in September 2019.
- Attended China-ASEAN Cybersecurity Industry Exchange Seminar at Nanning, China in October 2019.
- Attended Information Security Workshop organized by APNIC foundation, KDDI Foundation and University of Computer Science at Yangon, Myanmar in October and December 2019.
- 2019 Seminar on Combating Cyber Crime for Myanmar organized by Ministry of Commerce and Yunnan Police College at Kunming, China in October 2019.
- Attended 11th ASEAN-Japan Cyber Security Policy Meeting at Japan in October, 2019.
- Attended Capacity Building on the development of National Cyber Security Policy in the ASEAN countries organized by KOICA at Korea in October, 2019.
- Attended Regional Exercise on Cyber Threat Intelligence Sharing organized by UNODC in December 2019.

5.2.2 Drills & exercises

Drills

- Participating in APCERT Drill on July 31, 2019. APCERT Drill 2019 Title is "Catastrophic Silent Draining in Enterprise Network"
- Participating in ACID Drill on September 4, 2019. ACID Drill 2019 Title is "Combat Evolving Cyber Threats with Good Cyber Hygiene".

Cyber Exercises

- Participating in ASEAN –JAPAN Cyber Exercise on June 20, 2019.

5.2.3 Seminars & presentations

- APCERT AGM and Conference in October at Singapore
- APT Symposium on Cybersecurity in October at Malaysia
- China-ASEAN Cyber security Industry Exchange Seminar on 28 October to 1

November 2019 at China

5.3 Other international activities

- Members of mmCERT participated and ranked fifth position at "ASEAN Capture The Flag (CTF) Event" hosted by AusCERT in June.
- Member of mmCERT attended "4th Annual Meeting of Cybersecurity Alliance for Mutual Progress (CAMP)" in October at Republic of Korea

6. Future Plans

6.1 Future projects

- Government Secure Service Network
- Penetration Testing Labs
- Forensic Lab

6.2 Future Operation

As 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, Computer and Technological Universities' Students effective Capacity Building to our Technical Team members, 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

As government agencies in Myanmar are transiting to Digitalization and E-government platform, it is important to give secure and reliable services to all of Myanmar citizens. 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 (09:30-16:30) Working hour
- 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 2019

1.1 Summary of major activities

MNCERT/CC has successfully organized its annual event and competitions. MNSEC 2019 cyber security event has covered pretty large scope of participants and allowed them to exchange their experience and knowledge.

"Kharuul Zangi 2019" and "Kharuul Zangi U18 2019" cyber security competitions have been held successfully by MNCERT/CC.

1.2 Achievements and milestones

Year 2019 was full of achievements for MNCERT/CC. One of the main activities was providing its member organizations with security threat news feeds, recommendations, consulting and training.

One of the key achievements of this year was continuation of "Kharuul Zangi U18 2019" cyber security competition which was organized among high school senior grade students. Prizes for winners have been expanded with NEST academy programming course vouchers. Goal of the competition is to provide the knowledge of possible danger caused by cybercrime and appropriate knowledge about internet usage and to enhance cyber threat awareness for high school students.

Key achievements continued to MNSEC 2019 event which has been organized with new features such as four types of villages named packet hacking, hardware hacking, redteam and blueteam villages, electronic badges and registration fee.

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 seven members and consultant team with three members on November 2015. In 2016, two members have been added to the steering committee which became totally 9 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.

Human resource:

- Board Chairman – 1
- Chief Executive Officer – 1
- Officer – 2
- Incident Handler – 2
- Analysts – 2
- Legal advisor – 1
- Consultant – 3

2.4 Constituency

Our constituencies are:

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

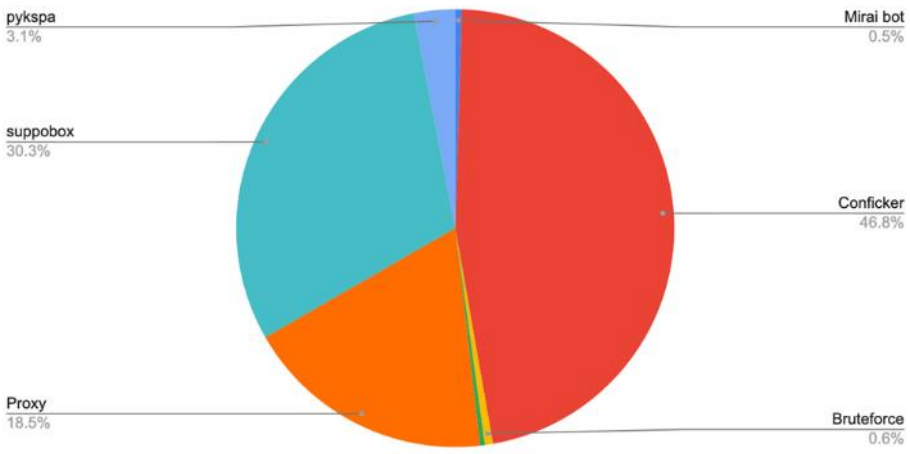
3. Activities & Operations

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 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 of general public.

3.2 Abuse statistics

The summary of malware types faced to Mongolia during the year 2019 is given in the following chart. This chart shows about summary of the malware, bot and vulnerability that were registered outbound traffic from Mongolia: Conficker bot is 46,8%, suppobox malware is 30,3%, Proxy vulnerability is 18,5%, pykspa worm is 3,1%, brute force attack is 0.6% and Mirai bot is 0,5%.



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 NIST Cybersecurity Framework, MISP (Malware Information Sharing Platform), Cyber Threat Intelligence and DevSecOps. After the training, participants discuss any 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 MNCERT/CC Cyber Drill 2019

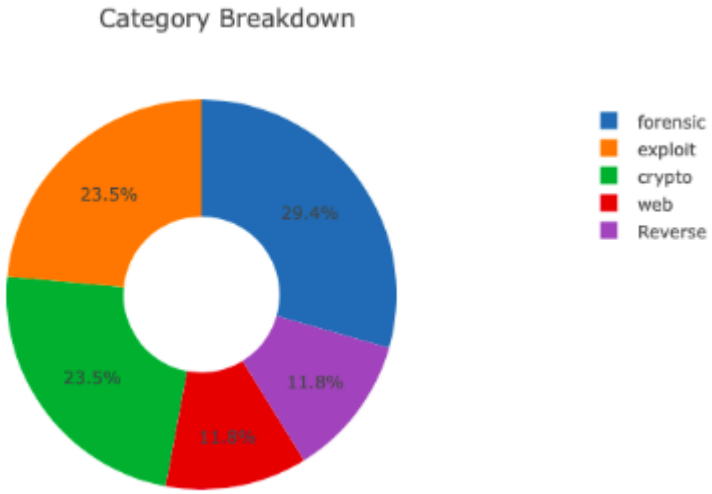
MNCERT/CC has organized the local cyber drill among the member and non-member organizations in 19th September of 2019. The goal of the drill was to practice incident response capability of local organizations. The scenario simulated the infection of malware and was held with 6 stages. Throughout the exercise, the participating organizations activated and tested their incident handling arrangement. This drill included the need for participants to interact locally with MNCERT/CC.

4.2.2 Kharuul Zangi 2019" 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, engineers and general public. We have successfully organized "Kharuul Zangi 2019" competition between 22th September to 04th October of 2019, in collaboration with Golomt Bank, "SafeBit" LLC and "MSTRide" LLC.

1st stage was designed to be completed online while the 2nd and 3rd stages had to be completed onsite using the network and systems designed by the organizers. Out of 170 teams of 398 members, 30 teams qualified from the 1st stage. Total of 20 tasks of 5 categories have been given to be completed at 1st stage and 18 tasks have been completed out of them by the competitor teams.

At 2nd stage, 27 teams have participated the contest and the organizing team of competition prepared 15 tasks of 5 types at this stage. The tasks are shown in the following chart.



After the 2nd stage, 10 teams were qualified to final stage. 3rd stage of the competition has been held on 04th October 2019, at MNSEC 2019 event. Topic of the 3rd stage was StarWars Version Code.

4.2.3 "Kharuul Zangi U18 2019" Cyber Security Competition

MNCERT/CC has initiated and organized cyber security competition named "Kharuul Zangi U18" among the high school students under the age of 18 on April 2019. The competition goal is to provide knowledge of possible danger caused by the cyber crime and to increase cyber threat awareness for high school senior grade students.

Totally 273 competitors of 91 teams have challenged for the competition. Teams increased by 37 than the previous year. 1st stage of the competition had been held onsite while the final 2nd stage had been onsite. High school senior grade students had great interests to this kind of competition and had informed to be more prepared for next Kharuul Zangi U18. One of the achievements of this year was that girls-only team has participated and went to the final round.

4.3 Conferences and seminars

4.3.1 MNSEC 2019 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 your 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 2019 event on 04th October of 2019 at the Shangri-La Ulaanbaatar hotel ballroom providing the opportunity to share experience, necessary information, knowledge, technology and new solutions within the security community. We have been organizing this event annually since 2012 in IT and cyber security field of Mongolia. The goal of this event is to improve cyber security in alliance with government agencies and private sectors by discussing current issues and solutions regarding Mongolian cyber environment.

MNSEC 2019 event has been conducted successfully with the great contribution from JPCERT/CC, APNIC, Team Cymru and CIRCL. Experts from above organizations and CSIRTs have been invited to the event and made great presentations about cyber espionage in Asia and Mongolia with case study.

MNCERT/CC team have a special thanks to these organizations and experts that continuously support us namely Adli Wahid from APNIC, Irek Parafjanczuk from Team Cymru, Yasutaka Ishii from JPCERT/CC and Steve Clement from CIRCL.

This event covered some of the most popular topics in cyber security field such as Use of ML and AI in black hat hacking, Observations from a Honeypot in Mongolia, Red Teaming and Adversary Emulation, Analysis of email threats targeting Mongolian bank sector, State of SOAR, Threat Hunting with GRR and Car hacking technique and its trend. Therefore about 250 representatives, engineers and technical specialists have participated and shared their knowledge & experience. Participation included from sectors such as financial institutions, universities, government agencies, mobile operators and internet service providers.

5. International Collaboration

5.1 International partnerships and agreements

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

This year our membership is expanded to NCFTA (National Cyber Forensics and Training Alliance) which provides Internet Fraud Alert (IFA) and Malware and Cyber

Threat (MCT) information. We inform stolen account credentials and BIN numbers for the intended organizations and banks based on IFA and MCT information.

5.2 Capacity building

5.2.1 Seminars & presentations

MNCERT/CC attended to the following international seminars and meetings:

- International Visitor Leadership Program in the USA.
- FIRST CTI Symposium in London, UK.
- Underground Economy Conference in Strasbourg, France.

6. Future Plans

6.1 Future Operations

MNCERT/CC planned the following activities in 2020.

Events, conferences and drill to participate are as follows:

- APCERT Annual General Meeting 2020 on September in Sri-Lanka.

Local activities to organize are as follows:

- MNSEC 2020 Cyber Security Event
- "Kharuul Zangi U18 2020" Cyber Security Contest among high school students
- "Kharuul Zangi 2020" Cyber Security Contest among IT specialists.
- Local cyber drill among member organizations.
- Local training for our constituency

7. Conclusion

2019 was the year of strengthening our activity for members and public, especially for the local cooperation, the number of our members increased and the cooperation and services for them have improved.

We are looking forward the year 2020 to be a more progressive year in both local and international stage and greater collaboration with APCERT and other international organizations.

MOCERT

Macau Computer Emergency Response Team Coordination Centre – Macao

1. Highlights of 2019

1.1 Summary of Major Activities

During the year 2019 MOCERT has provided the following activities in addition to the base Incident Response and Early Waning through

- Publication of industry specific notification of potential information security issues;
- Publication of broadly affecting issues that affect web servers of Macau origin be they government, industry or other;
- Maintenance of a website as point of reference for MOCERT services;
- Participated in the APCERT Drill 2019 as Player and Observer;

1.2 Achievements & milestones

MOCERT has launched a Cyber Threat Intelligence (MOCERT-CTI) System which is able to automatically collect threat intelligence from open-sources and trusted parties. This MOCERT-CTI, along with another integrated Incident Response Management system, will be beneficial to MOCERT's constituencies to deal with incidents handling tasks more effectively.

2. About CSIRT

2.1 Introduction

MOCERT (Macau Computer Emergency Response Team) is a non-profit service funded by MANETIC (Macau New Technologies Incubation Centre), an organization that is supported through industry sourced funding.

The mode of operation provides for an environment for MOCERT to be self-determined, and agile to changes required for an evolution of the service that is required to be provided as the computer security landscape changes in Macao.

MOCERT's core services are an evolving set of computer security issue collection, analysis and notification that encompasses public and industry specific advisories; Provision of a computer incident reporting facility that assist in security issues reactively, as they are reported, or proactively, from collected network evidence in the regional ASN; Provision of behavioral changes campaigns through educational activities for public.

2.2 Establishment

MOCERT started operations in late 2009 and it was in the validation of the services at the end of 2009 that MANETIC formally established and launched MOCERT as a public facing service on the 8th February 2010. Since then, and in a short time, the services have evolved in a manner that is appropriate to the size of the constituency it serves, Macao.

2.3 Resources

The staffing for the MOCERT service is sourced from MANETIC's pool of computer security professional and support staff. As of the year ending 2019 there are two (2) staff providing the service with eight (8) additional support staff.

2.4 Constituency

The constituency of Macau Computer Emergency Response Team Coordination Centre (MOCERT) shall be the internet users of Macao be they from government, businesses, or home users.

3. Activities & Operations

3.1 Scope and definitions

Macau Computer Emergency Response Team Coordination Centre (MOCERT) is managed by Macau New Technologies Incubator Centre in providing Macao with computer security incident handling information, promoting information security awareness, as well as coordinating on an international and local level, computer security issues, advisories, incident response, and research for the Macau public and local enterprises.

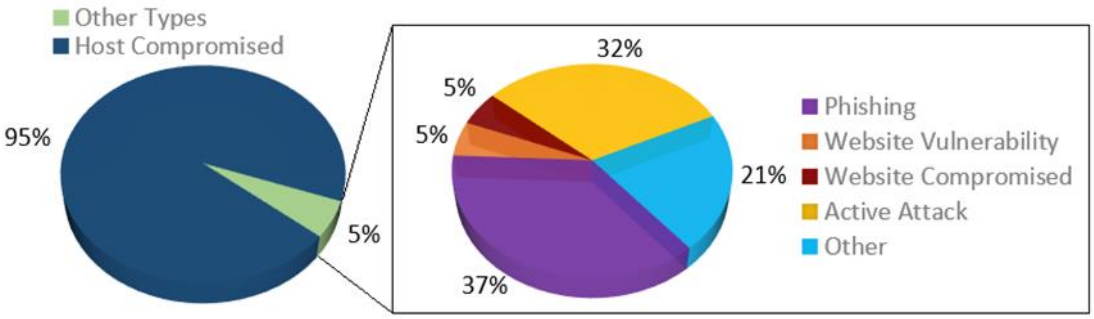
3.2 Incident handling reports

Incident reports are increasing as there is an increase in the natural reports being submitted, but also the increase is due to the addition of a service that proactively warns website owners of security issues. Sources of incidents are from three distinct channels.

i. Reported by Web
ii. Reported by E-mail message
iii. MOCERT initiated from incident discovery activity.

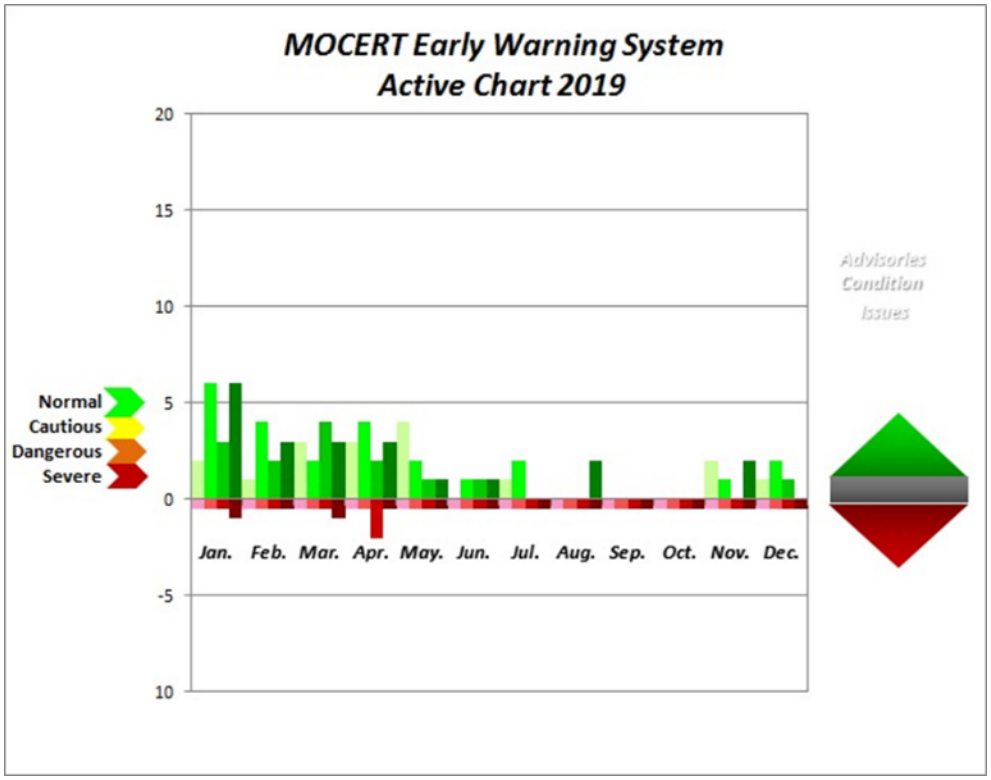
3.3 Abuse Statistics

The following pie graph denotes the abuse distribution as noted for the year 2019. The numbers are drawn from the incidents handled.



3.4 Early Warning Notices

A website collects notifications related to computer security, where all notifications are reviewed by staff to determine the impact to Macao constituency. The notifications are then classified to Issues and Advisories and then posted. The following diagram shows the distribution of the 97 postings in 2019 with 92 postings being Advisories, and 5 Issues.



4. Events organized / hosted

4.1 Training

Staffs in MOCERT service provided on the job training of incidents along with formal attendance to courses and seminars that first show the need for computer security, followed by personnel certification is practical.

5. International Collaboration

5.1 International partnerships and agreements

MOCERT maintains and promotes international partnership and agreements that promote a clean and safe internet.

5.2 Capacity Building

5.2.1 APCERT Online Training

MOCERT participated in APCERT online training courses held in 2019.

5.2.2 Drills & exercises

- APCERT Drill

The involvement in 2019 in the APCERT drill included as a Player and Observer.

6. Future Plans

6.1 Future projects and operation

Future projects mainly focus on the improvement of MOCERT's Threat Information Sharing Platform and provision of IT security consultancy services for the constituency. MOCERT will provide on demand training courses, incident handling services, and hold cybersecurity events for the constituency. Also, MOCERT will continue to collaborate with local and international members on incident handling and information sharing.

7. Conclusion

2019 has been a year where MOCERT launched a cyber threat information sharing platform. The major challenges up ahead are collaborating with local enterprises and organizations to provide solutions that meet their IT security requirements as further security consultancy services are sought. The changes envisaged will be beneficial to MOCERT's constituencies as the platform is progressively being improved to promote a clean and safe Internet.

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/

1.1.1 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.

1.1.2 Workforce

MonCIRT currently has a total of 6 constant staffs such as: executive director-1, experts 3, the bookkeeper 1, system administrator-1. Most of our staffs works part-time.

1.1.3 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.

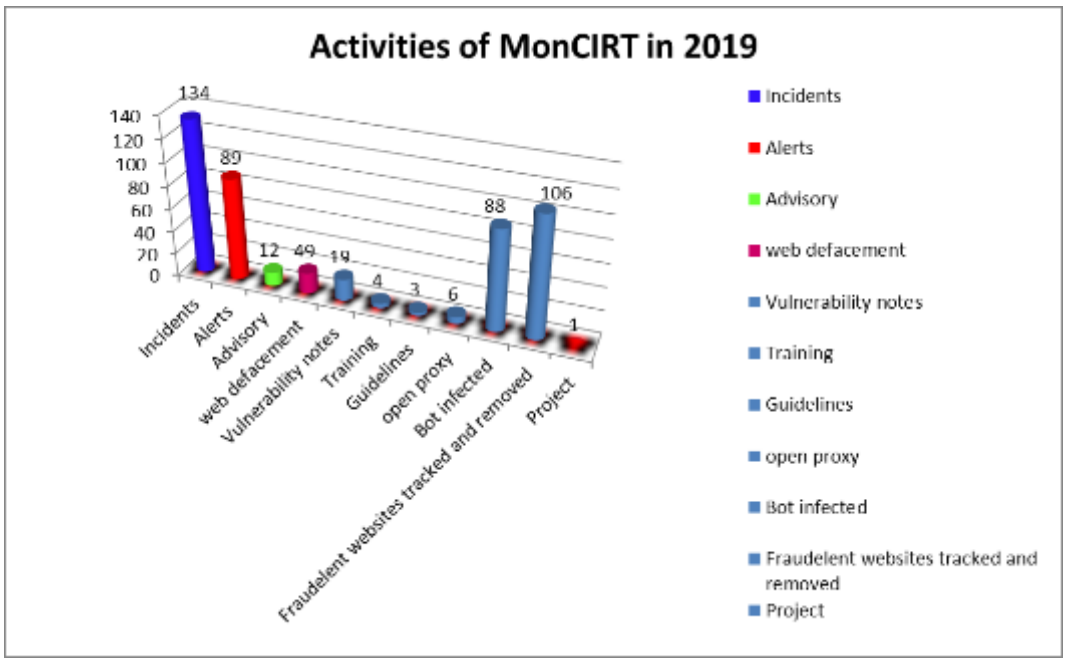
2. Activities & Operations

2.1 Summary

Innovation breeds opportunity in any areas. Web and mobility innovations focus on ease of use, availability, and building large user audiences, but they breed opportunity for cybercrime. Security typically comes later, after a period of breaches and security issues put the issue front and center. Through 2018, we are in the midst of this security period. The summary of activities carried out by MonCIRT during the year 2018 is given in the following table:

Activities	Year 2019
Security Incidents handled	134
Security Alerts issued	89
Advisories Published	12
Vulnerability Notes Published	19
Security Guidelines Published	3
Trainings Organized	4
Mongolian Website Defacements tracked and advised	49
Fraudulent Website (phishing site) hosted within Mongolia tracked and removed	106
Open Proxy Servers tracked	6
Bot Infected Systems tracked	88
Projects	1

The following chart depicts the distribution of various types of activities of the MonCIRT.



2.2 Incident trends

MonCIRT working to create organization's trust to us as reliable security center which can share sensitive information about security compromises and network vulnerabilities. Our connection with the Security Solution, Service & Consulting (SSSC) LLC and Communication, Information Technology School of Mongolian University of Science and Technology contributes to our ability to be neutral, enabling us to work with commercial competitors and government agencies without bias. As a result of connection with SSSC' s monitoring system, IPS and TSUBAME system and sharing of attack data we able to obtain a broad view of incident and vulnerability trends and characteristics.

During the year 2019 MonCIRT handled several incidents related with DDoS, Mobile malware attack, Weaponized Artificial Intelligence attack, Phishing, and identity theft. The number of cybersecurity incidents threatening to Mongolian educational institutes and business organizations is climbing at an alarming rate. Cybercriminals are growing more sophisticated in both the type of attacks they attempt and their ability to carry them out.

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.

2019 was a watershed year for integrity, data breaches, with hacks targeting the systems

and servers of universities and business companies like National University of Mongolia, National Agricultural University, University of Trade and Industry, Redd LLC, Uncovermongolia LLC, Ini LLC, Gangandeever LLC, Tavilga LLC etc. and other entertainment resources. MonCIRT observed that more than 100 fraudulent sites installed remotely, 10000 records were compromised in just those incidents. With more than 48000 personal data records compromised overall, 2019 became a record-breaking year.

In 2019, main trend of breaches was integrity loss and the number rose 35 percent from 2018, and the number rose 45 percent from 2018 to 2019.

Data breaches will continue to escalate, especially now that organized crime groups are turning to cybercrime. Here's a list of some of the biggest internet threats faced Mongolian Internet users in 2018.

Advanced Persistent Threats

Advanced persistent threats (APT) are especially worrisome for IT teams because, like the name implies, these attacks persist, stealthily, for months and even years. They move laterally through the IT infrastructure and steal data while avoiding detection.

Many APT solutions 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."

Weaponized Artificial Intelligence

Cybercriminals are using AI for nefarious purposes. As we observed there was about 20 cases that bad actors tried to use AI in 2019. There have been several attempts that a spear phishing Twitter campaign used AI for automation and to increase success rates. As we see cybercriminals innovate, it won't be long before they adapt machine learning to create ever more effective new threats.

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 2019 the 68 organizations and educational institutes became a victims of phishing attacks like email attachments or links, web-based drive-by or download (multiple responses were permitted).

Scammers are not missing a beat. Often masquerading as trusted companies, they bait

users into disclosing sensitive personal information. These techniques are also used to insert malware and bots into corporate networks — therefore we organized 4 trainings in organizations on how to avoid phishing attacks.
We teach IT specialists of companies on new technology that can protect companies - remote browser isolation. It can insulate endpoints from web-borne threats because it executes all the code remotely, in a safe environment, so it never reaches the end user's device or computer.

Mobile Malware

For 2019 about 280 students of universities and colleges, more than 350 employees of companies had faced an attempted mobile malware attack. We expect the number of mobile malware attacks to continue to increase in 2020. Most of that malware comes from third parties, but it has also been found embedded in apps sold through app stores. The number of mobile malware variants is also growing. The lineup includes Trojans, ransomware and keyloggers. Attackers don't always exploit vulnerabilities to infect mobile devices — oftentimes, unsuspecting users give access permission to the malicious apps, like embedded adware, when they install what they think is a legitimate app.
As we see the third-party app stores host most mobile malware.

Ransomware

We haven't seen the end of the evolution of ransomware yet. In 2019 there was 6 cases of ransomware attacks at different government and local government servers, systems. Cloud providers such as Mobicom cloud, Unitel cloud, iTools cloud are an enticing target because they store massive amounts of data and have large numbers of customers. However, because big providers make for tough adversaries, hackers looking for lower-hanging fruit are more likely to attack smaller services.

IoT Botnets

In 2019, we received report that few internet connected TV-smart boards of 3 universities cracked.
While organizations are very enthusiastic about adopting IoT technologies, many are not aware of the exposure created by vulnerabilities in the IoT ecosystem. And because they often lack visibility into their own ecosystems, it would be easy for them to lose track of data that flows through their corporate networks and not even realize that they'd been hacked.

Identity theft

Nearly 690 Mongolians have been affected by identity theft, according to a 2019 online survey organized by us.

Publicly available numbers from Cyber crime department of Mongolian Policy tell a similar story.

Coin mining

Types of cyber attacks vary from year to year. Lately, crypto mining is in vogue in Mongolia since 2016. In 2019 is observed that crypto mining and related cybercrimes is declined. Overall coin-mining activity declined 40 percent in 2019 in Mongolia.

In 2019 we observed just 4 cryptojacking attempts that Coin miners tried to add computers to their arsenal.

2.3 New services

2.3.1 Anti-new attacks System

We finished and deployed "Anti new types of attacks" System (Blockchain attacks, Cloud attacks, IoT attacks, Cross platform attacks, Mobile attacks) together with Communication and Information Technology school of Mongolian University of Science and Technology. We expected that thanks to this system the number of network attacks to educational networks will decrease about 50 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. Experts from industry are delivering lectures in these workshops apart from MonCIRT staffs.

The MonCIRT offers different training courses. These courses derive from the practical work of the MonCIRT staffs, providing introductory and advanced training for technical staff and the management of network security management, configuration, incident response and are centered around broader Internet security issues and security practices. Courses offered in 2019 included the following:

- *Prevent from deploying fraudulent web sites on your servers.*

- *Struggle with mobile attacks*
- *Network security controls according to ISO 27001:2013.*
- *Fundamentals of Incident Handling and Management*

In addition, MonCIRT organized following workshops:

« Prevent Cyber crime " on September 19, 2019

3.2 Drills

In 2017 MonCIRT organized local network security drill-VII involving all state universities and 14 private universities, institutes.

Cyber Drill VII was planned and culminated in the conduct of a three days exercise between November 08-10, 2019. 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 an 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 VII 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 order to create awareness and build Network Security skills within the constituency MonCIRT conducted the following conferences, seminars, workshops successfully:

i. MonCIRT was one of the partner in organization of annual conference of National Military University dedicated to "Mongolian national security issues". The governing board director of MonCIRT prof Khaltar Togtuun was one of key speaker on this conference.

ii. MonCIRT organized seminars among police investigators on "methodology of investigating cyber crime". Lead instructor is Prof Khaltar T

iii. MonCIRT representatives invited and participated in seminars, conferences organized both in Mongolia or abroad and made some presentations on behalf of MonCIRT, for example "Information security of business and government agencies" conference in Moscow, Russia, March 20, 2019 organized by CNews,

"IT&Security Forum 2019" conference in Kazan, Russia, June 25-26, 2019 and IDC Roadshow, Ulaanbaatar, April 18, 2019.

4. Achievements

4.1 Presentations

MonCIRT's board director participated and presented in Information security conferences in Mongolia and Russia as key speakers. In these conferences they have presented following presentations:

i. Conducted presentation during the IDC Roadshow conference organized by IDC on theme "IT strategy and Information Security".
ii. Conducted presentation during the "IT & Security Forum 2019" conference in Kazan on theme "Conduct comprehensive IT security audit according to ISO 27001 and COBIT".

In addition, Lectures and presentations have been made by members of MonCIRT in various workshops and seminars conducted in the country.

4.2 4.2 Publications

The MonCIRT published 10 advisories and 15 vulnerability notes in 2019 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 available in the repository of MonCIRT and include the following:

- *Network security practices*
- *Overview of network security*
- *Computer Network Security Alternatives*
- *Network security measures etc.*

Other Security Information

The MonCIRT captures lessons learned from handling incidents and vulnerability reports and makes them available to users of the Internet through a social pages and

web site archive of security information.

4.3 Certification & Membership

No Certification and Memberships obtained in 2019.

5. International and Domestic Collaboration

5.1 MoU

No any Memorandum of Understandings signed in 2019.

5.2 International incident coordination

Upon request of some security teams and departments of companies from Europe, USA we handled incidents related to 103 phishing web sites installed illegally in Mongolian web servers.

6. Future Plans

6.1 Future projects

No future projects planned in 2020.

6.2 Future plan

We plan to reorganize board structure, management staffs and expand our operation, establish new services aimed on Business sector's networks, public networks. Following are the future plans:

- Development and implementation of own Intrusion prevention & alert system

7. Conclusion

For MonCIRTs' constant and developing activity it is necessary financial support. Therefore, we signed MOU with MonPass CA LLC and in 2019 MonPass CA LLC financed most of expenses of MonCIRT.

Due to constant financial difficulty MonCIRT gives the basic attention on the new financing strategy, proactive and quality management 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 an real general private sector oriented CSIRT and in future.

All the events organized by MonCIRT during the year 2019 were very successful. We will

continue to conduct the Annual "Security Open Day" and will organize National Conference on Cyber Security under name "MonSec" while finding new ways to reach an even wider audience.

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).

Nisora tower, 207. Tokyo street. Bayanzurkh district. Ulaanbaatar, Mongolia and

Incident Response Help Desk

Phone: +976-70113151

Fax : +976-70113151

SingCERT

Singapore Computer Emergency Response Team- Singapore

1. Highlights of 2019

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.

SingCERT hosted the 17th APCERT Annual General Meeting (AGM) and Conference in Singapore, themed "Fostering a Safer Cyberspace through Partnerships and Collaboration". This was in conjunction with the Singapore International Cyber Week (SICW), Singapore's most established annual cybersecurity event. The theme complements APCERT's efforts in bringing together CERTs/CSIRTs, industries and academia to discuss cyber-related issues and capacity building so as to create a safer and more secure cyberspace.

Against the backdrop of the rising trend in cyber incidents, CSA launched two initiatives aimed at promoting awareness of cybersecurity threats as well as the adoption of good cyber hygiene practices;

i. **3rd Edition of Singapore Cyber Landscape**
Highlights facts and figures on significant cyber threats and incidents in Singapore for 2018.

ii. **Cybersecurity Awareness Campaign – "Go Safe Online C.A.F.E"**
Encourage the adoption of good cybersecurity habits in fun and engaging ways.

In 2019, SingCERT also launched a newly revamped website with an accompanying new logo that is more in keeping with the times.

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. 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 Infocomm Development Authority of Singapore (IDA), in collaboration with the Centre for Internet Research, National University of Singapore (NUS). SingCERT subsumed into the Cyber Security Agency of Singapore (CSA) when it was established on 1st April 2015.

CSA is the national body overseeing cybersecurity strategy, operation, 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 that affects its constituency on its website (https://www.csa.gov.sg/singcert). These are broadcasted through the SingCERT subscribers' mailing list, CSA's Facebook and Twitter platforms.

CSA also maintains a website - GoSafeOnline (https://www.csa.gov.sg/gosafeonline) - to provide cybersecurity trends and tips for individuals and businesses.

2.4 Constituency

SingCERT serves the local constituency comprising members of the public and private businesses in Singapore.

2.5 Redesign of logo and website

In 2019, SingCERT redesigned its logo to reflect the lineage with CSA and improved its website's user friendliness.

SingCERT's Logo:

Figure 1 : SingCERT's logo

The red and blue colours are inspired by CSA's primary colours and represents SingCERT's lineage with CSA. The shield represents SingCERT's role to protect and is wrapped with red banners, which represent the shield warding off cyber attacks. The design of the shield is artistically framed to create the letter 'S' which stands for Singapore/SingCERT. Overall, the logo represents SingCERT, a part of CSA, being a protector to safeguard Singapore's cyberspace.

SingCERT's Website:

Figure 2 : SingCERT's website

Figure 3 : SingCERT's website

The revamped SingCERT website is designed to improve user experience and make the website:

i. Easy to navigate;
ii. More visually appealing with the latest graphical technologies.

The website allows displays in all screen resolutions and is compatible with popular browsers like Firefox, Safari and Google Chrome.

The website serves as resources to its constituency and is accessible at https://www.csa.gov.sg/singcert.

3. Activities & Operations

3.1 Scope and definitions

SingCERT provides technical assistance and facilitates communications in response to cybersecurity related incidents. It 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 email and phone, and will assess the threat and advise individuals, respective agency(s) or service provider(s) on remediation measures.

In 2019, SingCERT handled 3,598 incidents. Although this is a reduction in numbers from 2018, it is due to the review of procedures in SingCERT's classification of incident reports.

Number of Incident Reports	Jan–Mar	Apr – Jun	Jul – Sep	Oct – Dec	Total
2019	665	650	1299	984	**3,598**

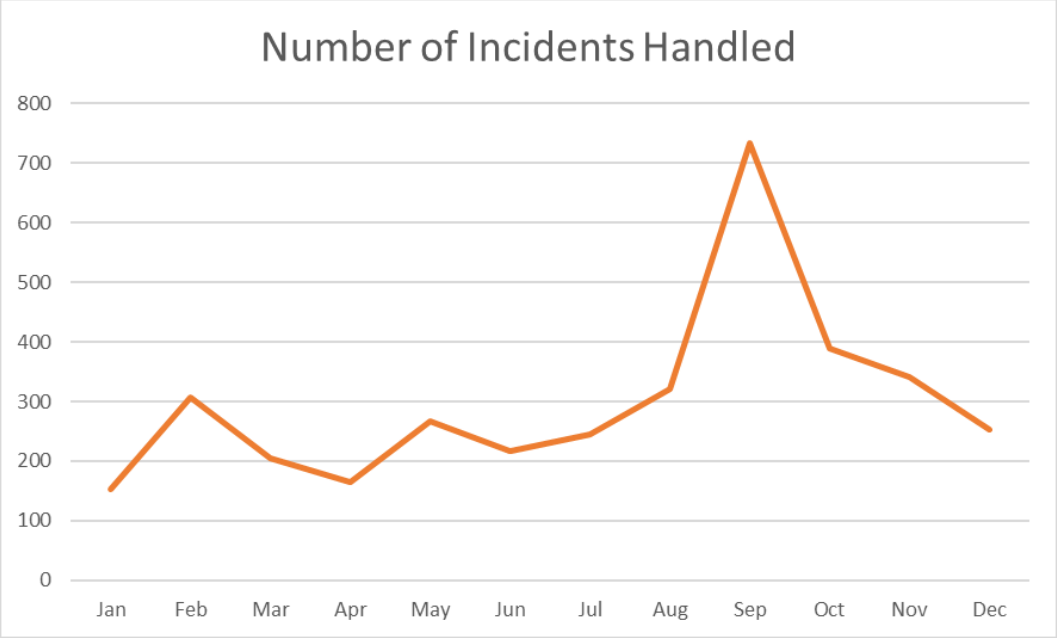


Figure 4: Number of Incidents handled by SingCERT (2019)

3.3 Abuse statistics

SingCERT receives numerous incident reports on different forms of cyber incidents. Among the most common cyber incidents handled by SingCERT are phishing, malware, and leaked information.

Phishing has emerged as the top threat in Singapore, and this has been the trend for the past few years. The phishing threats have also evolved to be more convincing and complicated.

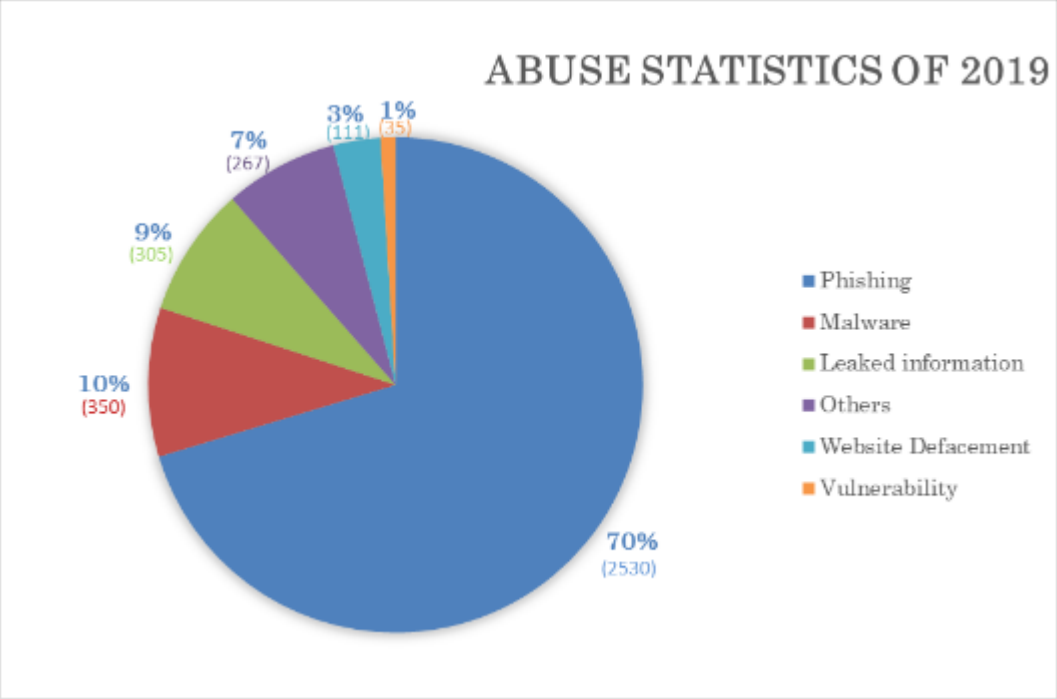


Figure 5: Abuse Statistics (2019)

3.4 Publications

3.4.1 Alerts and Advisories

SingCERT publishes alerts and advisories on emerging cyber threats to raise security awareness about the current cyber landscape.

The following chart shows the number of alerts and advisories published by SingCERT in 2018 and 2019 on a monthly basis.

	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Total
2018	8	3	2	9	4	5	6	2	8	8	5	3	63
2019	6	6	7	6	7	5	5	3	6	3	3	2	59

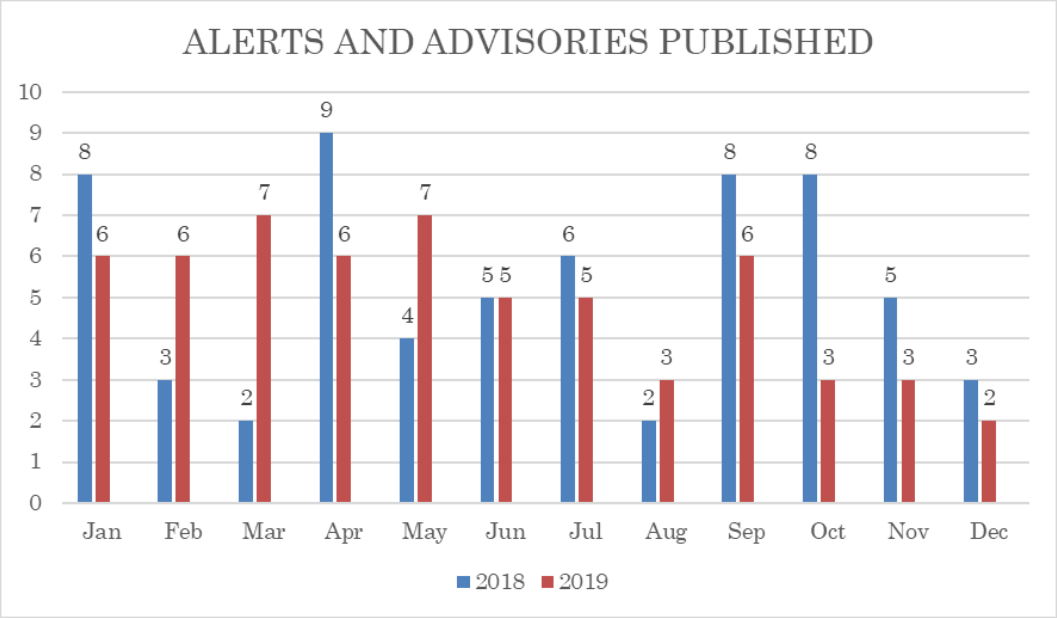


Figure 6: Comparing the Number of Alerts and Advisories Published (2018 to 2019)

A total of 59 alerts and advisories were published on SingCERT's websites https://www.csa.gov.sg/singcert/alerts and https://www.csa.gov.sg/singcert/advisories respectively. Of these alerts and advisories, a significant proportion (44 of 59) were released to address critical patches released by software vendors to fix the vulnerabilities. The list of alerts and advisories are tabulated below:

Date	Title
03 Jan	Advisory on E-mail Extortion Scam
10 Jan	Alert on Microsoft January 2019 Patch Tuesday
16 Jan	Alert on Oracle Critical Patch Update Advisory for Administrators
18 Jan	Advisory on Vulnerability for Android ES File Explorer Application (CVE-2019-6447)
24 Jan	Alert on Linux Advanced Package Tool (APT) Remote Code Execution Vulnerability (CVE-2019-3462)
24 Jan	Advisory on Mitigating DNS Records Tampering
01 Feb	Alert on DNS Flag Day
13 Feb	Alert on Microsoft February 2019 Patch Tuesday
15 Feb	Alert on Vulnerability in runc container runtime (CVE-2019-5736)
20 Feb	Alert on a Critical Remote Code Execution Vulnerability in WordPress
21 Feb	Alert on Critical Remote Code Execution Vulnerability (CVE-2019-6340) in Drupal
21 Feb	Alert on Vulnerability in Microsoft Internet Information Services
07 Mar	Alert on Critical Vulnerability (CVE-2019-5786) in Google Chrome
14 Mar	Alert on Critical Vulnerabilities Affecting Microsoft Products
16 Mar	Alert on Cross-Site Request Forgery (CSRF) to Remote Code Execution Exploitation in WordPress

21 Mar	Alert on Credential Stuffing and Password Spraying Attacks
22 Mar	Alert on Microsoft Windows 7 End-of-life
30 Mar	Alert on Critical SQL Injection Vulnerability in Magento software
31 Mar	Alert on Multiple Critical Vulnerabilities in VMware Products
03 Apr	Alert on Critical Remote Code Execution Vulnerabilities (CVE-2019-2027 and CVE-2019-2028) in Android Devices
04 Apr	Alert on Privilege Escalation Vulnerability (CVE-2019-0211) affecting Apache Web Server
10 Apr	Microsoft April 2019 Patch Tuesday
12 Apr	Remote Code Execution Vulnerability (CVE-2019-0232) in Apache Tomcat
18 Apr	Oracle Critical Patch Update (April 2019) for Administrators
23 Apr	Object Prototype Pollution Vulnerability (CVE-2019-11358) in jQuery
03 May	Exploits Targeting Unsecured SAP Systems Observed
14 May	Alert on Exploit Targeting WhatsApp Vulnerability Discovered (CVE-2019-3568)
15 May	Microsoft Remote Desktop Services Remote Code Execution Vulnerability (CVE-2019-0708)
15 May	Multiple Vulnerabilities Affecting Intel Central Processing Units (CPUs)
15 May	Advisory on Remote Code Execution Vulnerability (CVE-2019-11815) in Linux Operating System
16 May	Microsoft May 2019 Patch Tuesday
17 May	Critical Cisco PI, EPN and Webex Vulnerabilities (CVE-2019-1821, CVE-2019-1822, CVE-2019-1923, CVE-2019-1771, CVE-2019-1772, CVE-2019-1773)
08 Jun	Critical Vulnerability (CVE-2019-10149) in Exim Mail Server
12 Jun	Microsoft June 2019 Patch Tuesday
19 Jun	Alert on Multiple Linux Vulnerabilities
27 Jun	Alert on New Silex Malware on IoT Devices
28 Jun	Magento Commerce and Open Source Security Update
02 Jul	Microsoft Office's Excel Attack Vector
05 Jul	High-Severity Vulnerabilities in Cisco Products
10 Jul	Microsoft July 2019 Patch Tuesday
19 Jul	High-Severity Vulnerability in Iomega and LenovoEMC Products
23 Jul	Critical RCE Vulnerability (CVE-2019-1579) in Palo Alto Gateway
13 Aug	Alert on WordPress Auto-Update Policy
14 Aug	Microsoft August 2019 Patch Tuesday
30 Aug	Critical Vulnerability CVE-2019-5869 in Google Chrome
07 Sep	Over-The-Air Provisioning Phishing Attacks Against Android Devices
07 Sep	Critical Vulnerability (CVE-2019-15846) in Exim Mail Server
11 Sep	Microsoft September 2019 Patch Tuesday
24 Sep	Microsoft Out-Of-Band Security Updates (CVE-2019-1367 and CVE-2019-1255)
28 Sep	New Variant of Technical Support Scams – Scammers claim to investigate cybersecurity issue
30 Sep	High-Severity Vulnerabilities in Cisco Products
01 Oct	Critical Vulnerability CVE-2019-16928 in Exim Mail Server
09 Oct	Microsoft October 2019 Patch Tuesday
31 Oct	xHelper Malware Targeting Android Devices
08 Nov	Critical Cisco Webex Vulnerabilities CVE-2019-15283
13 Nov	Microsoft November 2019 Patch Tuesday

20 Nov	Compromise of Official Monero Website
11 Dec	Microsoft December 2019 Patch Tuesday
20 Dec	Emotet Malware Campaign

3.4.2 Singapore Cyber Landscape

The 3rd edition of the Singapore Cyber Landscape publication was released on 18th June 2019, highlighting facts and figures on significant cyber threats and incidents in 2018. 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 prevent such threats. More information about the report, including a downloadable copy, is available via https://www.csa.gov.sg/news/publications/singapore-cyber-landscape-2018

Figure 7: Singapore Cyber Landscape 2018

3.4.3 National Cybersecurity Awareness Campaign

CSA launched the 3rd cybersecurity awareness campaign to bring awareness to the community and provide avenues for members of the pubic to pick up cybersecurity tips.

Cybersecurity Awareness Campaign – "Go Safe Online C.A.F.E"

This campaign "Go Safe Online C.A.F.E (Cybersecurity Awareness for Everyone)" was launched on 4th Sep 2019, which builds on the momentum from 2018 and continues to encourage 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

A series of roadshows were organised to encourage the adoption of cybersecurity habits in fun and engaging ways. The event features interactive activities for visitors to get hands-on practice of key cybersecurity habits that help them stay safe online. These activities include:

i. 'Block the Viruses' – to educate players on the impact of malware infection in devices,
ii. 'Spot Signs of Phishing' – to educate players on how to identify real versus phishing emails or websites, and
iii. 'Password Journey' – to educate players on how to create a strong and memorable password.

4. Events organised & hosted

4.1 Drills & Exercises

4.1.1 ASEAN CERT Incident Drill 2019

The ASEAN CERT Incident Drill (ACID) is an annual drill that Singapore has been hosting since 2006. The drill serves to strengthen cybersecurity preparedness and cooperation within the region.

On 4th September 2019, SingCERT successfully conducted the 14th iteration of ACID. More than 100 participants from ten ASEAN Member States (AMS) and five Key Dialogue Partners participated in the drill. The participants were put through a series of scenario injects that are designed based on the prevalent cybersecurity threats. The theme "Combat Evolving Cyber Threats with Good Cyber Hygiene" was chosen due to the increasing prevalence of cyber incidents involving the breach of sensitive information such as users' credentials. Leaked credentials are a staple data source for threat actors to carry out malicious activities such as credential stuffing attacks. Successful attacks enable the threat actor to impersonate the user and monetise the unauthorised access through selling the stolen information or incorporating the information for subsequent

social engineering attacks, in the form of spear phishing and business email compromise fraud.

4.1.2 Government Bug Bounty Programme

The Singapore Government Bug Bounty Programme (GBBP) is an ongoing initiative to build a secure and resilient Smart Nation. The GBBP had succeeded in the discovery of vulnerabilities that would otherwise be undetected. In 2019, two GBBPs were conducted during the period of 8th to 18th July and 18th November to 8th December 2019. The programme gathered ethical hackers globally to look for security weaknesses in the Government systems.

This programme was organised in partnership with HackerOne – the world's largest community of cybersecurity researchers and white hat hackers. By bringing together a community of cyber defenders who share the common goal of developing a safe and resilient cyberspace, the GBBP aims to build a shared sense of collective ownership over the cybersecurity of Government systems and websites, which is vital to achieve Singapore's Smart Nation goals.

4.2 Conferences and seminars

4.2.1 APCERT Annual General Meeting (AGM) and Conference 2019

SingCERT hosted the 17th APCERT Annual General Meeting (AGM) and Conference in Singapore, from 29th September to 2nd October 2019 with the theme "Fostering a Safer Cyberspace through Partnerships and Collaboration". The theme complements APCERT's efforts to bring together CERTs/CSIRTs, industry and academia to discuss cyber-related issues, and capacity building in the region so as to create a safer and more secure cyberspace. The conference was attended by 100 participants from the APCERT community.

As part of the APCERT AGM and Conference programme, SingCERT organised a visit for the participants to visit Gardens by the Bay, for the participants to see a part of Singapore during their time here. The Conference was also held in conjunction with the Singapore International Cyber Week 2019, to allow the APCERT members the opportunity to attend the region's most established cybersecurity event.

4.2.2 Singapore International Cyber Week 2019

The Singapore International Cyber Week (SICW) is Singapore's most established annual

cybersecurity event, providing a platform for cybersecurity experts from around the world to discuss, network, strategise and form partnerships in the cyberspace.

The 4th SICW was held from 1st to 3rd October 2019, with the theme "Partnerships for Trust and Confidence". It emphasises the importance of close collaborations amongst governments, industry and various stakeholders, to ensure a trusted and secure cyberspace as an enabler for economic growth. SICW 2019 successfully concluded with a record 10,000 participants from the region and beyond, as well as 170 speakers, 300 exhibitors and sponsors. Details about the event can be found at https://www.sicw.sg.

4.2.3 Cybersecurity Awareness Alliance

CSA drives awareness efforts through the Cybersecurity Awareness Alliance, a collaboration between public and private sector organisations as well as trade associations, to raise awareness and adoption of cybersecurity measures. Alliance members actively engaged schools, businesses and the community at various platforms to share about cybersecurity and awareness.

5. International Collaboration

5.1 Training

SingCERT participated and benefitted from the following APCERT trainings arranged by TWNCERT:

Date	**Title**	**Presented by**
09 Apr	Web Application Penetration Testing Techniques	VNCERT
04 Jun	Web Penetration Testing 101	TWNCERT
06Aug	Digital Forensics (Storage Media & Mobile Phones)	CERT-IN
10 Dec	Zero Day Malware - Static Analysis	mmCERT

5.2 Drills & exercises

5.2.1 Asia Pacific Computer Response Team (APCERT) Cyber Security Drill 2019

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 31st July 2019 with the theme "Catastrophic Silent Draining in Enterprise Network". 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 participated in

the planning and execution of the drill and was also part of the Exercise Controller Team conducting the drill.

5.2.2 ASEAN-Japan Cyber Exercise

The ASEAN-Japan Cyber Exercise seeks to validate and improve information sharing mechanism 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 Cyber Exercise held on 20th June 2019 which aims to enhance the coordination of cyber incidents between countries.

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 2019 Annual Technical Meeting for CSIRTs with National Responsibility (NatCSIRT 2019) provides a forum for National CSIRTs to share information, tools, and strategies that address problems unique to CSIRTs that are responsible for a nation or an economy. It is also beneficial to both newly established and matured National CSIRTs as a platform for networking and collaboration. Details about the organisation can be found at https://www.first.org.

As a member of FIRST, SingCERT attended the FIRST Conference and Technical Meeting for National CSIRTs held in Edinburgh, Scotland, from 16th to 22nd June 2019.

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 2020:

S/n	Description	Category
1	Singapore Cyber Landscape 2019	Publications
2	5th Singapore International Cyber Week (SICW)	Events Organising & Hosting
3	15th 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. It is mandated with the task of protecting Sri Lanka's Information and Information Systems infrastructure. Its services range from responding to and investigating information security breaches, to preventing security breaches by way of awareness creation, security assessments and security capability building.

1.2 ESTABLISHMENT

As the national CERT, Sri Lanka CERT | CC acts as the central hub for cyber security of the nation. It is the single trusted source of advice on the latest threats and vulnerabilities affecting computer systems and networks, and a source of expertise to assist the nation and member organizations, in responding to and recovering from Cyber-attacks.

Sri Lanka CERT was established on 1st of July 2006 as a subsidiary of Information and Communication Technology Agency of Sri Lanka (ICTA). ICTA is the Government Agency responsible for the development of IT Infrastructure and Policy in Sri Lanka.

Sri Lanka CERT presently serves under the Ministry of Defence.

1.3 WORKFORCE

Sri Lanka CERT | CC has a total staff strength of seventeen (17) team members consisting of a Chief Executive Officer, Chief Operating Officer, Head of Research, Policy & Projects, Information Security Engineers, Associate Information Security Engineers, Information Security Analysts, Associate Information Security Analysts, Head of Human Resources and Administration and a driver/office assistant. This team is supported by five (05) undergraduate interns.

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 Certified Ethical Hacker (CEH) and Certified Hacking Forensics Investigator (CHFI), 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 entire cyber community of Sri Lanka (private and 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. Based on the 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.

This report presents an analysis of the cyber security related data collected by the Sri Lanka CERT|CC during the year of 2019. As a summary following observations can be made;

iv. Number of reported cases related to personal information misuse has been increased during the year 2019.
v. Financial frauds targeting local importers and exporters have seen a decrease during the year 2019 compared to 2018.
vi. There has been an increase in the spread of ransomware and malicious software during the year of 2019, where sensitive data belonging to both individuals as

well as corporate businesses have been made unavailable through encrypting, erasing or modifying data.

vii. A significant number of web site compromises targeting government and private sector organizations were recorded in 2019.

viii. Majority of the reported incidents fall into the category of social media related incidents. Among the social media incidents, Facebook related incidents were the highest.

In addition, Sri Lanka CERT was able to provide digital forensics services as follows;

i. Appearing in courts as expert witness for the digital forensics investigations conducted by CERT

ii. Number of forensic work carried out/involved in was more than 24 for the year

iii. Most of them are for the CID (Criminal Investigation Department), CCB (Counterfeit Currency Bureau), FCID (Financial Crimes Investigation Division), Others for some other police stations around the country.

Cyber-security related incidents reported to Sri Lanka CERT have increased in the year 2019 compared to previous year. In 2019, a total of 3566 incidents were reported to Sri Lanka CERT while it was 2598 during the year 2018. The increase is due to the significant number of cases reported for website compromise and privacy related issues.

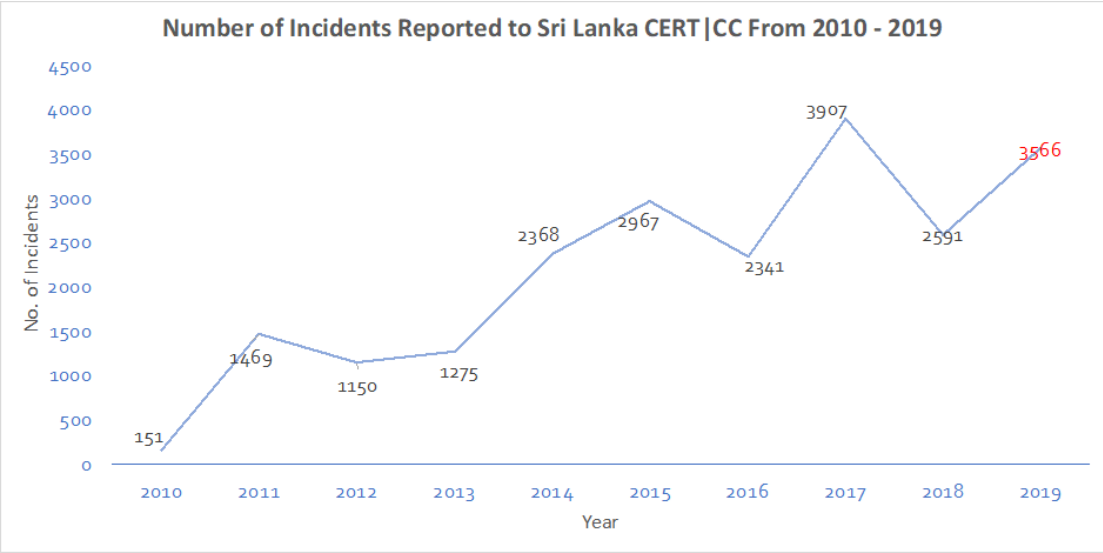


Figure 1. Growth of the number of incidents reported

Incident Type	No of Incidents
File Recovery	1
DDOS	2
Ransomware	11
Abuse/Hate/Privacy violation	307
Malicious Software issues	3
Phone Hacking	1
Scams	5
Phishing	5
Website Compromise	175
Financial/Email frauds	28
Intellectual property violation	1
Server Compromised	2
Social media	2662
Other	363
Total	**3566**

Table 1. Types of incidents

Incident Type	Year									
	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
Phishing	6	6	8	8	12	14	23	42	12	5
Abuse/Hate/Privacy Violation	20	2	8	9	8	21	32	29	11	307
Scams	10	3	6	18	12	18	12	32	7	5
Malicious Software/Ransomware	5	1	2	2	3	12	21	39	19	14
Financial Frauds	-	-	-	-	-	10	16	35	21	7
Web site Compromise	8	20	15	16	56	20	10	25	9	175
Compromised emails	12	3	6	8	10	16	16	14		21
Intellectual Property violation	-	5	3	3	3	3	7	6	6	1
Unauthorized Access	10	3	1	11	8	-	-	0	-	
DoS/ DDoS	-	1	1	1	6	3	4	0	1	2
Social Media Incidents	80	1425	1100	1200	2250	2850	2200	3685	2505	2662
Phone Hacking	-	-	-	-	-	-	-	-	-	1
Server Compromised	-	-	-	-	-	-	-	-	-	2
Other	-	-	-	-	-	-	-	-	-	364
Total	151	1469	1150	1275	2368	2967	2341	3907	2591	3566

Figure 2. Growth of the types of cyber security incidents

2.2 CONSULTANCY SERVICES

Sri Lanka CERT|CC continues to provide consultancy services to government and non-government agencies.

Typical consultancy services provided during the period include;

i. Development of Cybersecurity Curriculum for National Police Academy
ii. TEC member of Procurement of VAPT service provider for Bank of Ceylon (BoC)
iii. Police Criminal Records Division (CRD) fingerprint committee for the

Automated Fingerprint Identification System (AFIS)

iv. TEC member of Procurement of ATP solution for BoC
v. TEC member of Procurement web development service for Tea Board
vi. TEC member of Procurement of Reserve Management System (RMS) for CBSL
vii. Member of Procurement Committee of e-Passport
viii. TEC member of Procurement of email solution for Bank of Ceylon
ix. TEC member of Procurement of Privileged Access Management (PAM) solution for Bank of Ceylon
x. TEC member of Procurement of ATM AV for BoC
xi. Security assessments for 18 government department web sites
xii. Technical Expert of the President commission on Ester Sunday terrorist attack

2.3 TRAINING / EDUCATION SERVICES

Sri Lanka CERT|CC continues to conduct and facilitate training programs and education sessions targeting various audiences. This includes Chief Innovation Officers (CIOs), System Administrators, Banking and Telecom Sector Staff, Law enforcement authority staff, Tri-forces, Students, Engineers and the General Public.

a. Awareness Program and Training Sessions

i. Cyber security awareness session for schools (1 session)
ii. Digital forensics training for National Police Academy (3 sessions)
iii. Cyber security workshop for SIS officers
iv. Training sessions for SLAS officers at SLIDA (12 sessions)
v. Cyber Security session for NVQ level 4 students
vi. Information security lecture for Bio informatics Postgraduate/MSc doctors
vii. Training for school IT Tamil teachers via EduCSIRT program (3-day session)
viii. Session on Email security and document protection for STF officers
ix. Cyber Security workshop for OCDS officers
x. Cyber security training for National Police Academy

b. Awareness through Electronic/Print Media

xi. Newspaper articles
Provided information for 2 articles
xii. TV programs
01 live session
03 video cuts

xiii. Radio programs

17 Voice cuts and one live session

c. Annual Cyber Security Week 2019

Since 2008, Sri Lanka CERT|CC has been conducting an annual security awareness programme titled Cyber Security Week (CSW). This international event attracted the attention of the local as well as regional information security professionals. Cyber Security Week 2019 was held in the months of October 2019, and featured a series of events including the following;

- Hacking Challenge, 8th October 2019 at Lavender Room, BMICH
  Hacking Challenge is a contest for IT Professionals to attack or defend an actual network within a given timeframe. The participants were Technical Security Professionals, Network Administrators, System Administrators and students following information security post-graduate courses.

- Cyber Security Quiz: 7th October 2019 at Lavender Room, BMICH
  This competition is open only to students of Sri Lankan Universities and other tertiary education institutions. The objective of the quiz is to assess the knowledge and to identify and reward the aspiring young information security professionals.

- 12th Annual National Cyber Security Conference – 15th October 2019 at Hilton Colombo,
  - This year's theme was "Cyber Security…United we stand, divided we fall"
  - More than 400 participants
  - Conducted the awarding ceremony for the winners of Hacking Challenge and
  - Quiz
  - Chief Guest was Hon. Minister of Digital Infrastructure and Information Technology
  - Keynote address was delivered by Dr. Henry Pearson, Cyber Security Ambassador, UK

- Workshops – 9th, 10th & 11th October 2019 at DLC, SLIDA

- Securing Internet identifiers and incident Response (Hands On)-by ICANN
- Threat detection and Response-Made simple and effective-by CISCO
- Threat hunting Techniques and Methods (Hands on)- By Estonian Experts

- Supporting events
  - Workshop on IT risk assessment for banks
  - Workshop on IT risk assessment for ISPs

2.4 PUBLICATIONS

Website

The Sri Lanka CERT|CC website publishes security related awareness bulletins for the public through News Alerts, Glossaries, Case Studies, Statistics and FAQs.

E-mails

Sri Lanka CERT|CC disseminates security related information through e-mails to its subscribers.

Newsletters

Sri Lanka CERT|CC continues to publish and circulate The Cyber Guardian e-newsletter to a large number of students, through the SchoolNet- the network connecting secondary schools in Sri Lanka.

Newspapers/media

Sri Lanka CERT|CC 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 themselves against these attacks.

2.5 OPERATIONAL SUPPORT PROJECTS

It was able to conduct a project to acquire cyber security investigation/assessment resources and enhance the capabilities of staff during the year 2019. This project was funded by government of Sri Lanka.

2.6 NATIONAL PROJECTS

Project Name	Project Status
1. Establish the National Cyber Security Operations Centre (NCSOC) to monitor threats digital government application and critical infrastructure.	Procurement started
2. Establish Root Certification Authority to provide digital certifications to the certification service provides	Ready for commissioning
3. National Surveys to assess cyber security landscape of Sri Lanka a. Critical Information Infrastructure Readiness Survey b. Public Employees Cyber Security Readiness Survey c. National Survey on Citizen Perceptions of Cyber Security (Department of Census and Statistics) d. Supply and Demand Assessment of Cyber Security Professionals	Surveys in progress
4. Development of Information Security Manual for Government Organizations and development Baseline Security Standards	Work in progress

3. ACHIEVEMENTS

3.1 NATIONAL CYBER SECURITY STRATEGY

The government of Sri Lanka ensured its commitment to keep the nation safe, secure and prosperous, by introducing Sri Lanka's first Information and Cyber Security Strategy which will be implemented over period of five years from 2019 to 2023. Sri Lanka CERT developed the National Information and Cyber Security Strategy of Sri Lanka with the support of stakeholders and obtained the cabinet approval for the strategy on 16th October 2018.

Sri Lanka CERT is in the process of the implementation of the National Information and Cyber Security Strategy and have initiated several projects during the year 2019.

3.2 RESEARCH AND POLICY DEVELOPMENT

Research and policy development team of Sri Lanka CERT was involved in drafting the Cyber Security Act during the year 2019. The process is ongoing for the enactment of the act through the parliament of Sri Lanka.

3.3 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

3.4 TRAINING FOR STAFF

Sri Lanka CERT was able to provide following local training and conference participation for its staff

i. Discussion with NI-CO team on "CERT maturity model of ENISA"
ii. Discussion with world bank team on “Cybersecurity capacity maturity model”
iii. CISCO security workshop for CERT staff
iv. Cyber Maturity Model (CMM) workshop with Oxford university
v. Participation at ISC2 Sri Lanka chapter meetings

4. INTERNATIONAL COLLABORATION

4.1 EVENT PARTICIPATION

i. FIRST Symposium and TF-CSIRT meeting (Estonia)
ii. CYBERUK 2019 (UK)
iii. HR training (India)
iv. First Annual General Meeting & Conference and NatCSIRT Meeting 2019 (Scotland)
v. International visitors leadership program (Germany)
vi. Japan -US Industrial Control System Training (Japan)
vii. APCERT Annual General Meeting & Conference (Singapore)
viii. nCSIRT workshop (Singapore)
ix. ITU Asia-Pacific & CIS Inter-Regional Cyber Drill (Malaysia)
x. nCSIRT workshop (UK)
xi. CAMP 4th AGM (Korea) -Sri Lanka is in the operations committee

4.2 APCERT

i. Became a member of the APCERT Steering Committee from 2019
ii. APCERT steering committee meetings
iii. Continuing with network monitoring project "Tsubame" with JPCERT|CC
iv. APCERT working group teleconferences- Secure Digital payments
v. APCERT online trainings (3 trainings)
vi. APCERT cyber drill 2019 working group discussions
vii. OIC-CERT cyber drill 2019
viii. APCERT AGM Program Committee Meetings
ix. APCERT AGM and Conference (Singapore)

- Member of the program committee of AGM
- Presented at the Public Conference on "National Information and Cyber Security Strategy"
- Contributed to several APCERT working groups.
- Made new contacts with cyber security related organizations.

4.3 OTHER ACTIVITIES

i. Reporting of malicious IP address details received from International counterparts to local ISPs. The International counterparts consists of CERT Bund - Germany, Microsoft, Shadow Server and APCERT Data Exchanger.
ii. Continuing with network monitoring project "Tsubame" with JPCERT|CC
iii. Ministerial delegation to Finland and Estonia
iv. NatCSIRT teleconferences
v. ICANN GAC meeting (Japan)
vi. Government delegation to Estonia for e-Governance conference and discussions
vii. Government delegation to Portugal for a Cyber Security Study Tour

4.4 INTERNATIONAL INCIDENT COORDINATION

i. APCERT Cyber Security Drill
- Worked as a member of the organizing committee of APCERT Cyber Security Drill 2019
- Participated for the drill

ii. Engagements with CERTs in the Asia Pacific region. Sri Lanka CERT has regular operational engagements with CERTs/Information security

organizations in other regions of the world and commercial establishments and solution providers to resolve phishing and identity theft incidents.

5. FUTURE PLANS

5.1 FUTURE PROJECTS

i. Development of National Vocational Qualification (NVQ) Standards for Cyber Security
ii. Information and Cyber Security Skills Framework for government employees.
iii. Development of a Web Portal to increase citizens' (business, government organizations) awareness on cyber security
iv. Train 2200 government employees with information and cyber security
v. Upgrading Education Sector CERT (EduCERT) with physical premises
vi. Development of e-Learning Modules on Information and Cyber Security
vii. Improving the Information and Cyber Security Readiness of the Government Organizations Maintaining Critical Information Infrastructure (10 organizations)
viii. Development and Implementation of a Security Operations Centre (in progress).
ix. Establishment of sector based CSIRT's (e.g. Telco-CERT).
x. APCERT AGM 2020 with Cyber Security Week.
xi. Cyber Security project with European Union (Cyber4Dev) to implement the provisions of the National Information and Cyber Security Strategy.

5.2 FUTURE OPERATIONS

This section details the changes anticipated in Sri Lanka CERT with regard to staff, equipment and capabilities:

- Sri Lanka CERT shall recruit undergraduate students on internships basis to enhance the information security capabilities of the younger generation.
- Sri Lanka CERT shall continue to operate as a skilled small group of professionals.
- Sri Lanka CERT shall continue to invest on developing the capacity of the staff.

6. CONCLUSION

During the period, Sri Lanka CERT has observed that number of web sites which were compromised has been increased. The main reason for such compromises were due to obsolete Content Management Systems used by those web sites.

It was also observed that financial frauds happening through email compromise is very common as in the previous year and CERT was able to make the public, small business establishments and large corporates aware of such threats in order to stop them from becoming victims.

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 conduct a program called Cyber Resilience for Development (Cyber4Dev) which is jointly funded by the Foreign and Commonwealth Office of UK, Dutch Ministry of Foreign Affairs, and Estonian Information System Authority.

It is expected to operationalize a few national level Information Security related projects during the year 2020 to support the implementation of the National Information and Cyber Security Strategy of Sri Lanka.

Sri Lanka CERT became a member of the steering committee of APCERT in 2019 and expects to contribute to the enhancement of cyber security and improve the collaboration in the region with the support of all the APCERT members.

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 general public and Sri Lankan organizations keep their computer systems and networks secure. TechCERT celebrated their 13th Anniversary on 01st of September 2019.

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. In order 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	Engineering Manager	MBA (Colombo), MSc. (Moratuwa), BSc. Eng (Moratuwa), C|EH, AMIE (SL), MCS (SL)
Kasun Chathuranga	Lead Security Engineer	MSc. (Moratuwa), BSc. Eng (Moratuwa), RHCE, RHCSA, AMIE(SL), MIEEE
Nalinda Herath	Lead Security Engineer	MSc. (Moratuwa), BSc. Eng (Moratuwa), C|EH, CPISI, ITIL, CCNA (Security), AMIE(SL), ISO/IEC 27001 Lead Auditor
Kalana Guniyangoda	Lead Security Engineer	MSc. (Moratuwa), BSc. IT (Hons), GCFA, C|HFI
Sashika Suren	Lead Security Engineer	MSc in InfoSec (UCSC), BICT (UCSC), RHCE, RHCSA, MCTS, GDip in Bus Mgmt, Red Hat Certified Ansible Automation Specialists, Certified Payment Card Industry Security Implementer (CPISI)

Geethika Wijerathne	Manager Projects & Administration	MSc in Information System Management (Colombo), PMP
Mishra De Silva	Senior Account Manager	MBA (Colombo), BBA (U.S.A), AS (U.S.A), MSLIM
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) Engin 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) Engin Computer Engineering (Peradeniya)
Dushan Chathuranga	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	Associate 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
Madhuri Prabodhika	Associate Information Security Engineer	BSc(Hons) Computer Science (Peradeniya), C|EH
Hirushan Thilanka	Information Security Analyst	BSc. Information Systems (UCSC)
Radeesha Bandara	Information Security Engineer	Bsc. Computer Systems and Networking(Curtin), RHCSA, CCNA security
Pubudu Ranasinghe	Associate Information Security Analyst	BSc. (Hons) in Information Technology(Cyber Security)

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 general public.

2. Activities & Operations

2.1 Services 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 a information security leader in Sri Lanka, TechCERT also the member of Emergency Cyber Security Coordination Center after it has been initiated.

And also, 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)

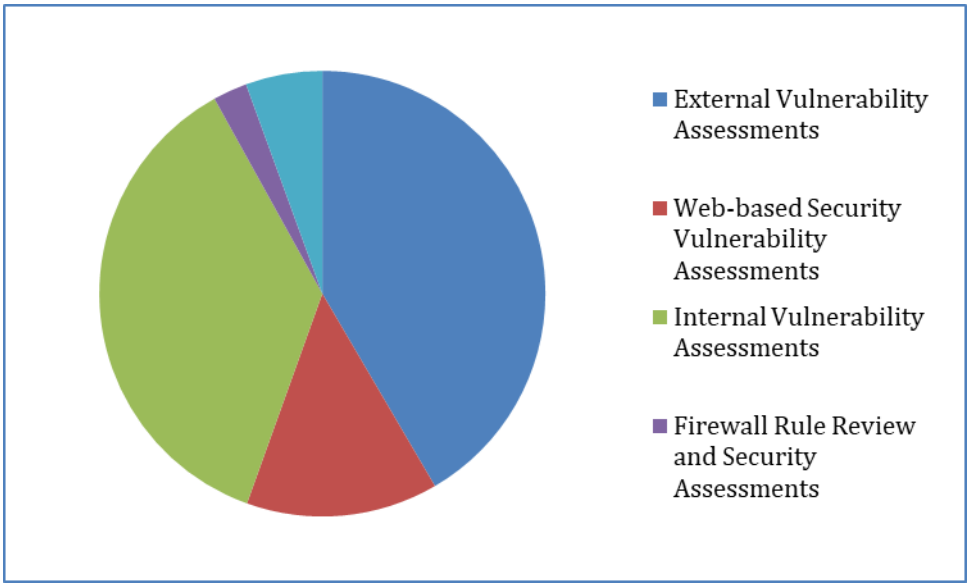
2.2 TechCERT Activities and Operations

The details of activities and operations conducted by TechCERT during the year 2019 are as follows:

2.2.1 Security Assessments

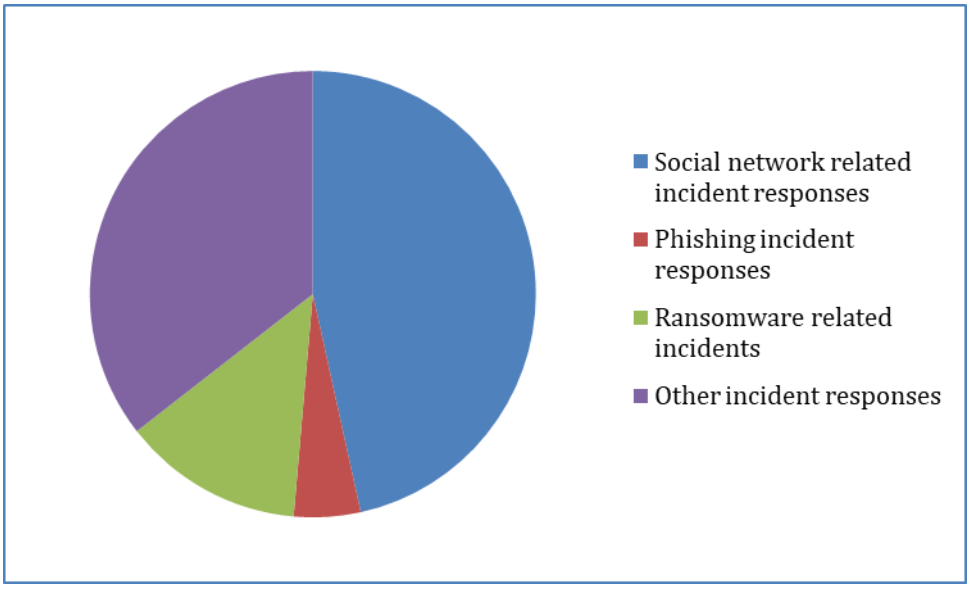
Activity Type	Count
External Vulnerability Assessments	2967

Web-based Security Vulnerability Assessments	993
Internal Vulnerability Assessments	2602
Firewall Rule Review and Security Assessments	177
Other Assessments (DF investigations, Wireless, Network, etc.)	397



2.2.2 Incident Report

Types of Incident Response	**Count**
Social network related incident responses	135
Phishing incident responses	14
Ransomware related incidents	38
Other incident responses	103



3. Events Organized by TechCERT

3.1 Organizing Training Seminars, Workshops and Demonstrations

21st November 2019	Workshop - Critical Security Controls for Effective Cyber Defence and Security Automation

3.2 Participation in Conferences, Workshops and Training Programs

- Dileepa Lathsara, Chief Operating Officer of TechCERT participated in the, International Visitor Leadership Program (IVLP) in the U.S. on "Advancing an Open, Reliable a Secure Digital Economy" from January 4th - 25th 2020
- Chathuranga Gunathilaka, Senior Security Engineer of TechCERT participated in the, APCERT Annual General Meeting & Conference in Singapore from 29th September - 2nd October 2019.
- Sashika Suren, Lead Security Engineer of TechCERT, participated in the, Apricot Conference, included "Network monitoring and management workshop" from February 18th to 28th 2019 in Daejeon, South Korea.
- Madhuri Prabodhika, Associate Information Security Engineer of TechCERT, participated in the, SL CERT Cyber Security Week, "Android Mobile Application Security - Hands on" workshop held on November 05th 2018.
- Hirushan Thilanka, Information Security Analyst of TechCERT, participated in the (ISC)2 Colombo Sri Lanka Chapter, "RED TEAM INSIGHTS FROM DOWN UNDER" held on October 24th, 2019

- Asanka Dhananjaya, Information Security Engineer of TechCERT, participated in the workshop organized by Tufin, "Unveiling Enhanced Capabilities for Managing Next Generation Firewall Policies" held on September 30th, 2019 in Sri Lanka.

3.3 Cyber Security Drills

31st July 2019	**APCERT Cyber Security Drill 2019** TechCERT actively participated in the APCERT Drill 2019 as the leader of the Organizing Committee and a member of EXCON team.
3rd October 2019	**Cyber Security Drill for Sri Lankan Banking Sector** TechCERT conducted a Cyber security drill for the Banking Sector in Sri Lanka on the Theme "Countering Application Security Threats".
07th August 2019	**Cyber Security Drill for Sri Lankan Finance & Insurance Organizations** TechCERT conducted a Cyber security drill for the Banking Sector in Sri Lanka on the Theme "Countering Application Security Threats".
20th November 2019	**Cyber Security Drill For Sri Lankan Telcos And ISP's** TechCERT conducted a Cyber security drill for the Banking Sector in Sri Lanka on the Theme "Countering Application Security Threats".

4. Future Plans

- In 2020, 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 2020.

5. Conclusionss

TechCERT has been 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.

With the experience gained by participating in and taking part in organizing the APCERT drill activities; TechCERT was able to conduct cyber drills for the Sri Lankan Organizations (Financial Organizations, Banks and Telco & ISPs) for the fifth consecutive year.

There was a significant increase in phishing attacks and website defacement/hacking incidents in Sri Lanka in 2019, when compared to previous year. TechCERT was able to successfully respond to most of the incidents reported and assist the relevant authorities to mitigate the threats with minimum effect. TechCERT is confident of its ability and readiness to successfully assist its constituency in computer emergencies by providing pro-active response. In achieving the organizational objectives, TechCERT shall continue to increase its staff strength, 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

ThaiCERT

Thailand Computer Emergency Response Team – Thailand

1. Highlights of 2019

1.1 Summary of major activities

In May 2019, The Cybersecurity Act, B.E. 2562 (2019) was published. Under the Cybersecurity Act, CII organization will be identified and need to follow upcoming cybersecurity measure. Under this law, national CSIRT will be established and National Cyber Security Committee (NCSC) is high body headed by the prime minister to oversee policy.

In aspect of capacity buildings, we organized Thailand Cybersecurity 2019 which is cybersecurity seminar to empower critical organizations to stay ahead of growing cyber threats. More than 3000 people was participated in the event. We partnered with RSAC to organize Bangkok RSA Unplugged 2019 under the event.

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

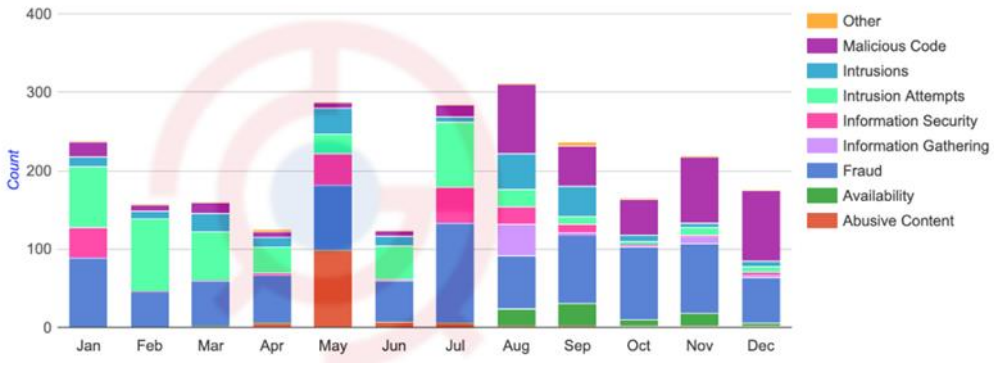


Figure 1: The number of reported incidents in 2019

Via triage, ThaiCERT handled a total of 2,470 reported incident cases (tickets) in 2019, which are slightly decreased from those of 2018 (2,520 cases). The received reports per month are around 200 cases.

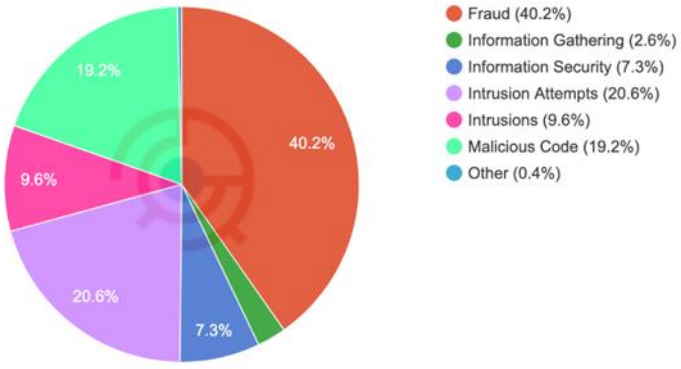


Figure 2: The proportion of reported incidents by incident type in 2019

According to the reported incidents in 2019, classified by the eCSIRT incident classification, Fraud dominated with 40.2%, where all cases were mostly phishing websites, followed by Intrusion Attempts at 20.6% and Information Security at 7.3%. All such information was handled and notified to the relevant parties through e-mail channels.

3.2 Publications

In 2019, ThaiCERT published A Threat Actor Encyclopedia, ThaiCERT Annual Report 2017-2018 and Cyber Threat Alerts & Articles 2018. For the details, please see https://www.thaicert.or.th/downloads/downloads.html

4. Events organized/hosted

4.1 Training

Organized:

- AJCCBC Trainings, Jan Mar May Jul Sep and Nov 2019

4.2 Drills, exercises

Participated

- APCERT Drill 2019, Jul 2019
- ASEAN CERT Incident Drill (ACID) 2019, Sep 2019

4.3 Conferences and seminars

Organized:

- Thailand CTF 2019, Sep 2019
- Cyber SEA Game 2019, Nov 2019

Co-organized:

- Fundamentals of Incident Handling, with CMKL academy
- Advanced Incident Handling, with CMKL academy

Participated:

- RSA Conference 2019, San Francisco, USA, April 2019
- Annual FIRST Conference 2019, Edinburgh, Scotland, June 2019
- APCERT AGM 2019, Singapore, September 2019

5. Future Plans

- Thailand Cybersecurity 2020 Event
- SOC Reservice

TWCERT/CC

Taiwan Computer Emergency Response Team / Coordination Center – Chinese Taipei

1. Highlights of 2019

1.1 Summary of Major Activities

In 2019, the Taiwan Computer Emergency Response Team / Coordination Center (TWCERT/CC) shared nearly 12 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 3,994 subscribers, 34 hacked incidents intelligence, 53 vulnerabilities news, as well as information of 55 seminars, campaigns and contests, to raise awareness and reveal the importance of incident reporting to public.

As a Numbering Authority of the Common Vulnerabilities and Exposures (CVE®), we assigned 27 CVE IDs this year, and issued Taiwan Vulnerabilities Annual Report 2019. 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.

About the cybersecurity activities, TWCERT/CC joined 15 domestic and international cybersecurity conferences and seminars, an international drill, and hosted the 2019 Conference of Taiwan Cyber Security Notification and Response and Working Meeting of Taiwan CERT/CSIRT Alliance for two times. 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 globe.

As for TWCERT/CC's services, in addition to the Anti-Phishing Notification Window service and the Automatic Incident Reporting System, TWCERT/CC released the Virus Check system to public on July and have totally received about three thousand files, 7 of them were malicious files that never seen.

1.2 Achievements & Milestones

- Shared nearly 12 million incident reports separated in 11 categories; intrusion and botnet are the top two common types of attacks of cybersecurity in 2019.
- Issued 12 monthly e-newsletters, 34 hacked incidents intelligence, 53 vulnerabilities news, as well as information of 55 seminars and campaigns.
- According to more than twelve hundred vulnerabilities collected in the Taiwan Vulnerabilities Annual Report 2019, SQL-injection, Cross-Site Scripting (XSS) and broken access control are the top three most common types of vulnerabilities in 2019.
- As a Number Authority of Common Vulnerabilities and Exposures , 27 CVE IDs were assigned in 2019.
- Participated in 6 international and assisted 9 domestic cybersecurity conferences and seminars, hosted the 2019 Conference of Taiwan Cyber Security Notification and Response and 2 regular meetings of Taiwan CERT/CSIRT.
- Optimized the Virus Check system and released to public. This year we discovered 7 new malicious files regarding Trojan, backdoor and hack tools, and reported phishing websites from 263 offshore and 109 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 2019, 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 2019, TWCERT/CC shared about twelve million cyber intelligence, the monthly numbers and types of incident reports shared are shown respectively in Figure 1 and Figure 2.

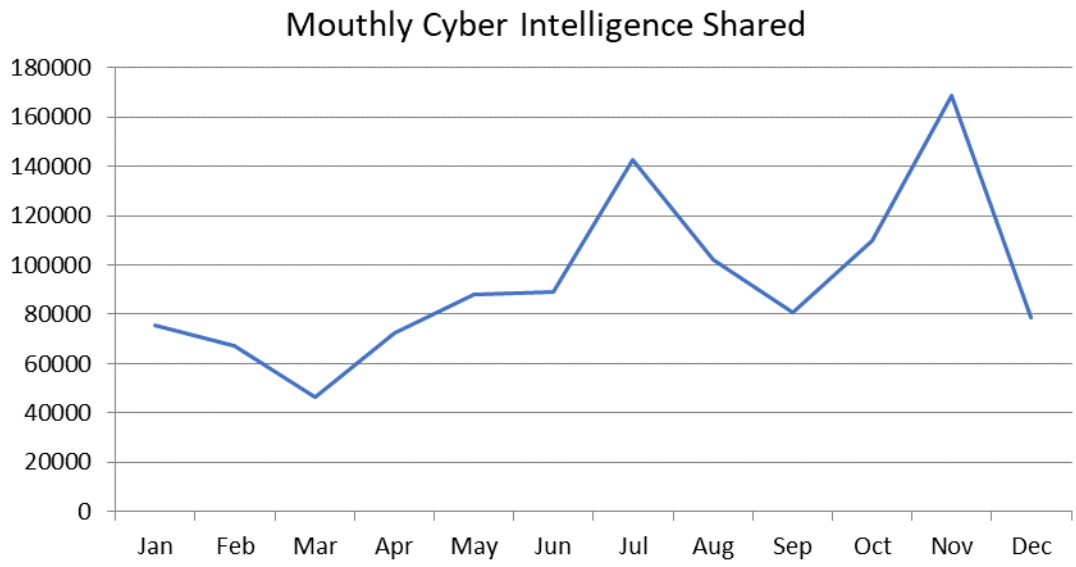


Figure1. Numbers of cyber intelligence TWCERT/CC shared in 2019

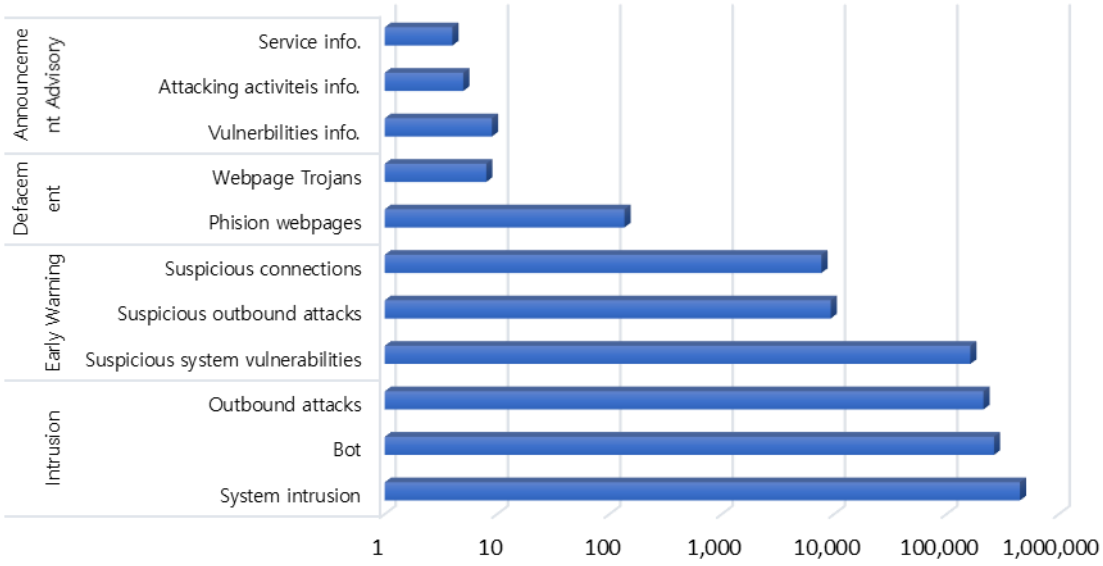


Figure2. Types of cyber intelligence TWCERT/CC shared in 2019

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 2019, TWCERT/CC issued 12 monthly e-newsletters. Furthermore, 34 hacked incidents intelligence, 53 vulnerabilities news, as well as information of 55 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 2019, TWCERT/CC collected nearly 1,300 vulnerabilities intelligence separated in 22 categories.

i. 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.

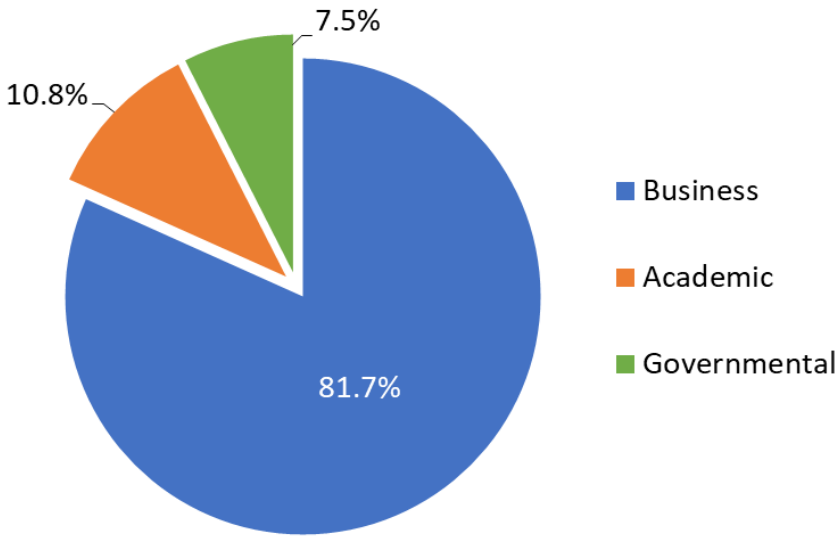


Figure 3. Source Statistics of Vulnerabilities

ii. Categorization Statistics of Vulnerabilities by TWCERT/CC

Vulnerabilities categorization is shown in Figure 4. SQL Injection, Cross Site Scripting(XSS), Arbitrary File Download, Sensitive Data Exposure and Broken Authentication(and weak password) are top 5 of vulnerabilities collected.

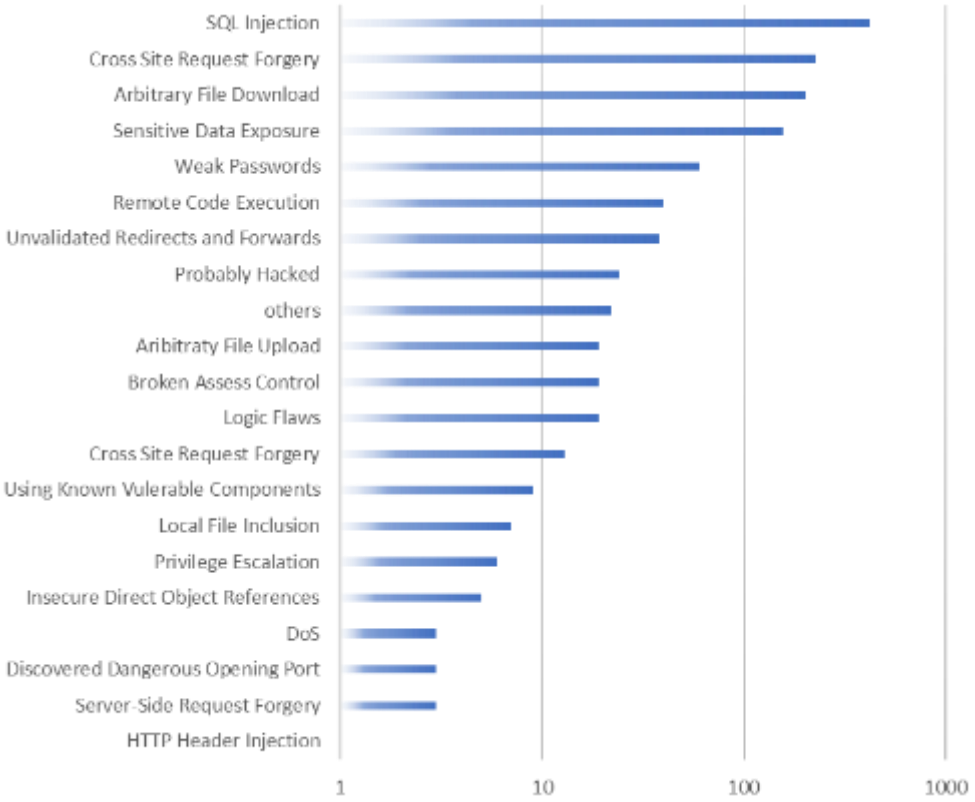


Figure 4. Categorization Statistics of Vulnerabilities

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 2019, 27 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
Netcom products	7	CVE-2019-9882, CVE-2019-9883, CVE-2019-13411, CVE-2019-13412, CVE-2019-15064, CVE-2019-15065, CVE-2019-15066
IOT devices	11	CVE-2019-11060, CVE-2019-11061, CVE-2019-11063, CVE-2019-11064, CVE-2019-13405, CVE-2019-13406, CVE-2019-13407, CVE-2019-13408, CVE-2019-15067, CVE-2019-15068, CVE-2019-15069
Software service systems	9	CVE-2019-9884, CVE-2019-9885, CVE-2019-9886, CVE-2019-11062, CVE-2019-13409, CVE-2019-13410, CVE-2019-15071, CVE-2019-15072, CVE-2019-15073

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, Trend Micro 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.

Cybersecurity Advocacy

In order to raise users' awareness of cybersecurity, disseminate advanced security knowledge and provide a variety of services, TWCERT/CC has been evolving the official website ceaselessly. This year, some major features has been developed or revised:

i. Reviewed and renovated the structure, provides a more intuitive website framework and surfing experience;

ii. Facilitated with varied functions and tools, meanwhile contents and services were enriched, which improves the immediacy and interactivity of service to end users;

iii. Dedicating in being in line with Web Accessibility Protocol 2.0, AA standard is expected in near future and more people are to be reached;

iv. Enabled a simplified reporting instrument, which requires less details to be inputted and raises people's approaching to submit incident reports.

Figure 5. TWCERT/CC official website

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 seven times: presentation of 2019 Symantec Internet Security Threat Report, Info Security 2019, InfoSec Taiwan 2019, TiEA Information Security Lecture, TTU Cyberspace2019, HITCON Defense 2019, 2019 CYBERSEC 101, and propagating the cruciality of incident reporting and responding to public.

4.2 Conferences and Seminars

TWCERT/CC has been propagating information security and importance of incident reporting, aiming to penetrate some critical knowledge to the masses and build up a solid concept about cyber security in people's mind. On October 8th, 2019, TWCERT/CC officiated the 2019 Conference of Taiwan Cyber Security Notification and Response, in order to disseminate to enterprises and people the key concept of cybersecurity, and to raise the awareness of incident reporting as facing a cyberspace with threats aggravating. During the Conference, commissioner of National Communications Commission, Mr. Teng Wei-Chung, Director General of National Security Council ICT Security office, MG. Liao Shu-Huang, Director General of Department of Cyber Security, Mr. Jyan Hong-Wei, representative from AusCert, Mr. Geoffroy Thonon, representative from American Institute in Taiwan, Mr. Engen Ryan, researcher from Trend Micro Inc., Mr. Fang Jia-Ching, expertise form IBM, Mr. Lee Chen-ta, presented the Conference and gave speeches and keynotes to share their experiences in security incidents, responding and protecting techniques before, during, and after an incident, and working experiences in domestic ISACs, to improve the public understanding of cybersecurity and awareness to incident reporting.

This year, 420 participants attended the Conference, and 33% of them were from the industry of information services, followed by 10.4% from government officials and 10% from financial industry. According to a post conference survey, 83% of them highly evaluated the Conference, meanwhile, 96% of the people engaged considered the issues discussed to be helpful to their businesses or works, and 75% of them spook highly to the stands presented in the campaign. 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 2019 Conference of Taiwan Cyber Security Notification and Response

Apart from the Conference, TWCERT/CC acts as a coordination team for business enterprises in information security technologies and endeavor in raising their awareness of cybersecurity. Thus, in 2019, consultants from industries, the police and partner CERTs were invited to help draw up a standard operating procedure of TWCERT/CC, which provides a high-efficient communication channel as assisting and coordinating Taiwanese enterprises to respond to information security incidents.

In the year 2019, TWCERT/CC also hosted two regular Taiwan CERT/CSIRT meetings, 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.

Bridging between international cybersecurity organizations and domestic incidents response teams, TWCERT/CC has been dedicated to help these members from Taiwan CERT/CSIRT Alliance apply for international organizations and improve their global communications. This year, two Alliance members succeeded with the aim from TWCERT/CC. QNAP, a Taiwanese network storage device manufactory, made it to join the FIRST. And TWCSIRT, an incident response team of National Center of High-Performance Computing, also became a member of APCERT. In the future, TWCERT/CC and its members will continue devoting in assistance and coordination with Taiwanese enterprises, to help them fortify and to connect them with the world of cybersecurity

5.2 APCERT Cyber Drill

In order to get experienced in incidents handling, and further bring some feedbacks from problems faced or ideas got, TWCERT/CC and its members have participated in APCERT Cyber Drill 2019, which helped consolidate the standard operating procedures in incident reporting and assisting, and improve their efficiency and effectiveness.

On July 31st, 2019, roles of a player and an observer were acted by two TWCERT/CC members, performed a drill which simulated a bank's internal staff training platform to be intruded via a CVE-2018-7600 referred vulnerability by attackers, who then gain access to its database and send phishing emails according to stolen employees' information, aim for a mining malware installed in users' device as long as the phishing email have been clicked.

5.3 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 six international conventions, and shared its working results to professionals from CERTs/ CSIRTs around the world at FIRST 2019 Conference and FIRST Technical Colloquia in APNIC 48. In the future, 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 2019

Date	Conference/Seminar
2019/Mar/22	IETF 104 Prague Conference
2019/May/20	The CNA Summit
2019/Jun/12	2019 First Conference
2019/Sep/10	APNIC 48 FIRST Technical Colloquia
2019/Sep /23	APCERT Conference 2019
2019/Nov/17	IETF 106 Prague Conference

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:

i. Publish prompt vulnerability information and cybersecurity incidents, monthly cybersecurity e-newsletter, and annual report;
ii. Release trends, policies, threats about cybersecurity from time to time;
iii. Collect and release the latest information of conferences, seminars, and trainings relative to cybersecurity;
iv. 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 2019

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 2019, TWNCERT published more than two thousand cyber security advisories for government agencies. Also, TWNCERT provided consulting and training services for government agencies and critical infrastructure sectors.

To increase cyber security capability and promote cooperation, TWNCERT conducted a national large-scale cyber security exercise, named Cyber Offensive and Defensive Exercise. Besides, TWNCERT launched cyber security competitions for university students to nurture cyber security talents as well as created a cyber security protection game for raising cyber security awareness. Moreover, TWNCERT held 24 cyber security protection and eight Government Configuration Baseline trainings for government agencies.

In 2019, TWNCERT participated in various international events and delivered presentations on cyber security threats, detection techniques, and information sharing mechanisms at the Digital Crimes Consortium 2019 in Portugal, National CSIRT Meeting in Scotland, Underground Economy Conference 2019 in France, APCERT AGM & Conference 2019 in Singapore, APCERT training program, etc.

1.2 Achievements & milestones

TWNCERT conducted the Cyber Offensive and Defensive Exercise (CODE 2019) in November. The invited participants were from thirteen foreign countries along with domestic public and private sectors in Taiwan. This year's exercise was performed in a unique way, it's a live action exercise. Red teams and blue teams act against each other with four scenarios on the simulated environment in the financial services field.

Beyond receiving incident reports from communities, TWNCERT has become more proactive to reach cyber security information from various sources and retrieve actionable intelligence, e.g. validated phishing pages, vulnerable services for N-ISAC members and government agencies.

As the convener of APCERT Training Working Group, TWNCERT has convened five

online training sessions and one training workshop. Year around, a total of twenty-eight APCERT member teams participated in these programs.

2. About TWNCERT

2.1 Introduction

As a national CERT, TWNCERT acts as the point of contact for the CSIRTs in CI sectors in Taiwan and worldwide for the nation. We aim to enhance the government and CI sectors' ability to respond and deal with cyber security incidents, 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

TWNCERT received around seven hundred reports on cyber security incidents from Taiwan government agencies, and about one thousand and three hundred international cyber security incident reports from overseas in 2019.

Additionally, around one hundred and twenty thousand cyber security incidents and critical information were shared among N-ISAC members, including CI sector ISACs, major MSSPs, law enforcement agencies, and CSIRTs in Taiwan.

3.3 Abuse statistics

- **Government agencies**

  Intrusion and Defacement most reported incident categories from government agencies.

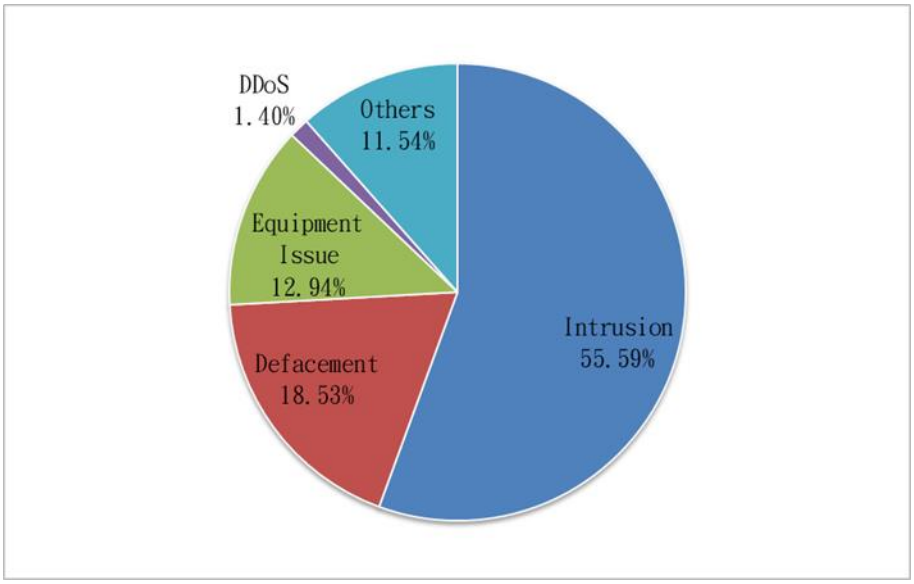


Figure 1 Security incidents from government agencies

- **International incident report**

  The international cyber security incident reports in 2019 were categorized as in Figure 2. About 57.47% of the incident reports were Malware, followed by Phishing and Attack.

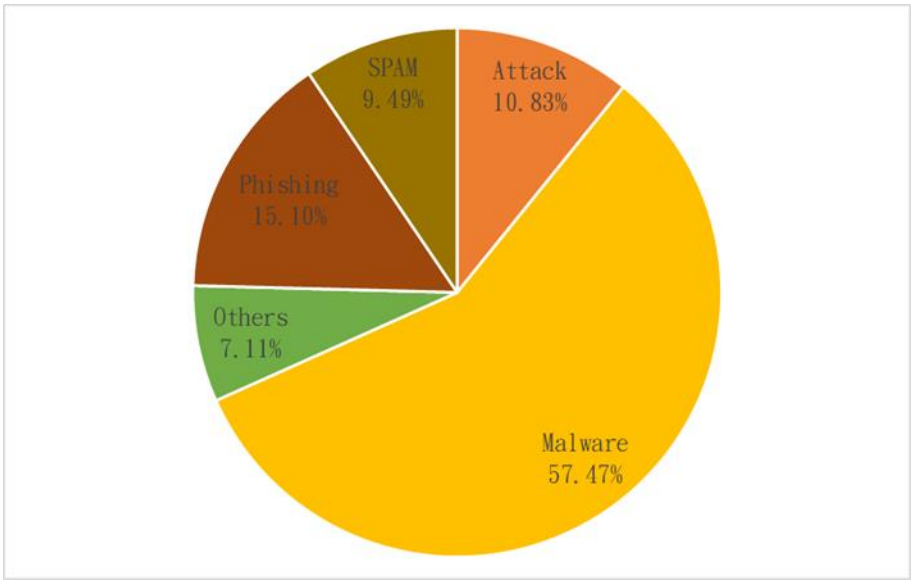


Figure 2 Classification of the international incident reports

- **N-ISAC information sharing**

  N-ISAC members shared thousands of cyber security incidents and critical information, around one hundred and twenty thousand cyber security information in 2019.

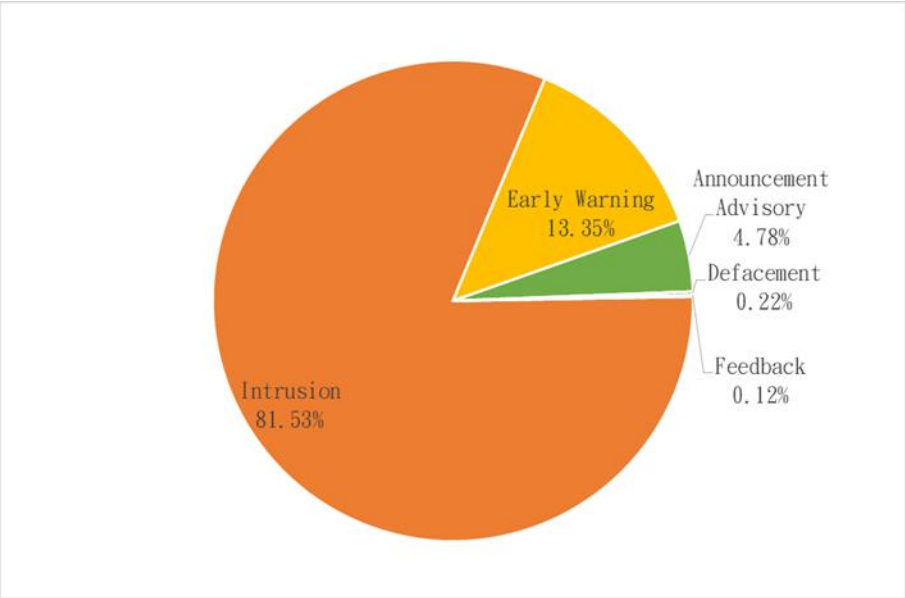


Figure 3 Information sharing distribution of N-ISAC

3.4 Publications

- **Website publication**

  TWNCERT collects and publishes cyber security advisories, news or guidelines on the website. In 2019, TWNCERT published around ninety articles including cyber security news and security alerts on the website.

- **Government agencies**

  In 2019, TWNCERT published more than two thousand notice advisories to government agencies. The categories were distributed as in Figure 4.

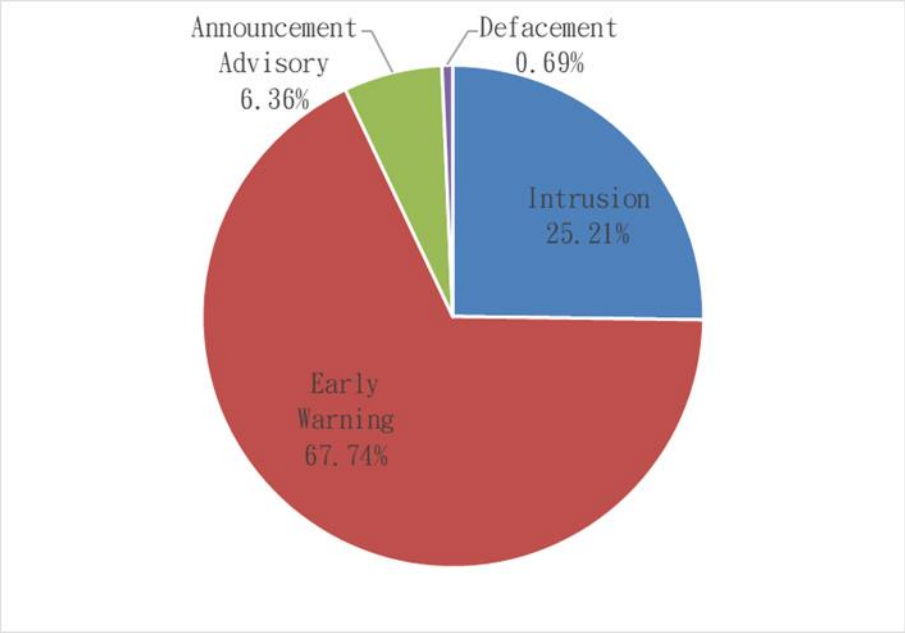


Figure 4 Distribution of government notice advisories

- **International incident report sharing**

  Regarding the international incident report sharing, TWNCERT has reported a total of 3,052 reports containing 14,282 suspicious IP addresses to 55 countries shown in figure 5.

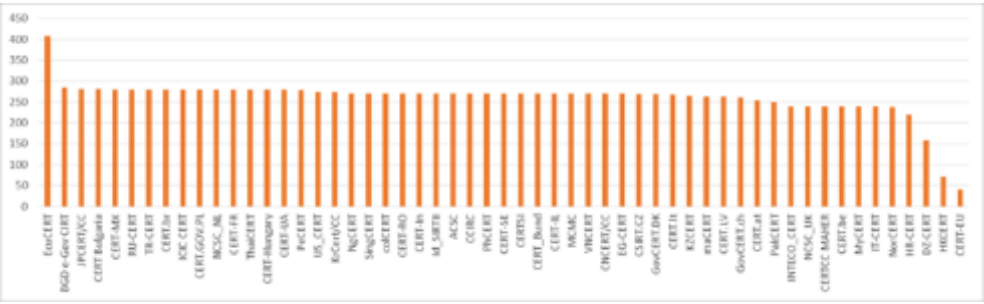


Figure 5 International incident reports

4. Events organized/hosted

4.1 Training

TWNCERT developed eight courses to improve cyber security protection among government agencies. In 2019, TWNCERT held twenty-four cyber security protection trainings for around seven hundred government staffs.

In order to strengthen the computer network and system security among government

agencies, TWNCERT held eight Government Configuration Baseline (GCB) trainings to more than two hundred fifty government technical staffs in 2019.

4.2 Drills & exercises

- **Drill**

  TWNCERT conducted a national large-scale cyber security exercise, Cyber Offensive and Defensive Exercise (CODE 2019) in November. More than fifty five organizations were invited to participate in CODE 2019. The invited participants were from thirteen foreign countries along with domestic public and private sectors in Taiwan. This year's exercise was performed in a unique way, it's a live action exercise. Red teams and blue teams act against each other with four scenarios on the simulated environment of the financial field.

Figure 6 Cyber Offensive and Defensive Exercise (CODE 2019)

- **Cyber security competition and cyber security protection game**

  To nurture cyber security talents and to promote cyber security general awareness, TWNCERT launched cyber security competition and cyber security protection game in 2019. There are more than ten thousand attendees participated.

Figure 7 Cyber Security Competition and Cyber Security Protection Game

4.3 Conferences and seminars

For N-ISAC members, TWNCERT held quarterly meetings among members, not only discuss issues and problems found during each quarter but also improve information sharing efficiency and effectiveness. In 2019, a total of four member meetings had been held. The fourth meeting in December was the N-ISAC annual meeting. The experts from FS-ISAC, Thailand TB-CERT, Japan F-ISAC, and domestic public and private sectors in Taiwan were invited to share valuable insights and experiences with N-ISAC members.

Figure 8 N-ISAC Members Meeting

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 five 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 and one training workshop. Year around, a total of twenty-eight APCERT member teams had participated in these programs. To improve the training program, TWNCERT conducted a survey to evaluate the effectiveness of the training program and delivered the statistics results at the APCERT AGM & Conference in September.

Date	Topic	Presenter	Participation Team
2019/2/12	Digital Forensic Analysis with Free and Open Source Tools	TechCERT	BtCIRT, CNCERT/CC, GovCERT.HK, HKCERT, JPCERT/CC, KrCERT/CC, LaoCERT, MOCERT, Sri Lanka CERT|CC, TechCERT, ThaiCERT, EC-CERT, TWCERT/CC, TWNCERT
2019/4/9	Web Application Penetration Testing Techniques	VNCERT	ACSC, bdCERT, CERT-In, CNCERT/CC, GovCERT.HK, JPCERT/CC, KrCERT/CC, LaoCERT, mmCERT, MOCERT, SingCERT, VNCERT, EC-CERT, TWCERT/CC, TWNCERT
2019/6/4	Web Penetration Testing 101	TWNCERT	CNCERT/CC, GovCERT.HK, JPCERT/CC, KrCERT/CC, LaoCERT, mmCERT, SingCERT, Sri Lanka CERT|CC, EC-CERT, TWNCERT, Panasonic PSIRT
2019/8/6	Digital Forensics (Storage Media & Mobile Phones)	CERT-In	BtCIRT, CERT-In, CNCERT/CC, GovCERT.HK, HKCERT, ID-SIRTII/CC, JPCERT/CC, mmCERT, MOCERT, SingCERT, TechCERT, EC-CERT, TWCERT/CC, TWNCERT, FINCSIRT
2019/9/30	Honeypots & Honeynet	APNIC	APCERT AGM Training Workshop
2019/12/10	Zero Day Malware – Static Analysis	mmCERT	AusCERT, bdCERT, CERT-In, CNCERT/CC, GovCERT.HK, HKCERT, JPCERT/CC, KrCERT/CC, mmCERT, SingCERT, Sri Lanka CERT|CC, EC-CERT, TWNCERT, FSI-CERT

Figure 9 APCERT training programs

5.2.2 Drills & exercises

TWNCERT participated in APCERT Drill under the theme "Catastrophic Silent Draining in Enterprise Network" on July 31st and solved a set of drill scenarios within the given time limit.

Figure 10 APCERT Drill 2019

5.2.3 Seminars & presentations

Below is the list of international events that TWNCERT participated in 2019.

- APEC TEL 59 Conference
- Black Hat Asia 2019
- Digital Crimes Consortium 2019
- FIRST 2019 Conference
- Black Hat USA 2019 & DEF CON 27
- Underground Economy Conference 2019
- APCERT AGM & Conference 2019
- Meridian 2019
- APEC TEL 60 Conference
- Industrial Control Systems (ICS) Cyber Security Conference
- ICANN 2019 Conference

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 2019

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 continued to deploy the annual activities like drills, workshops, training and complete the responsibility of incident response coordination.

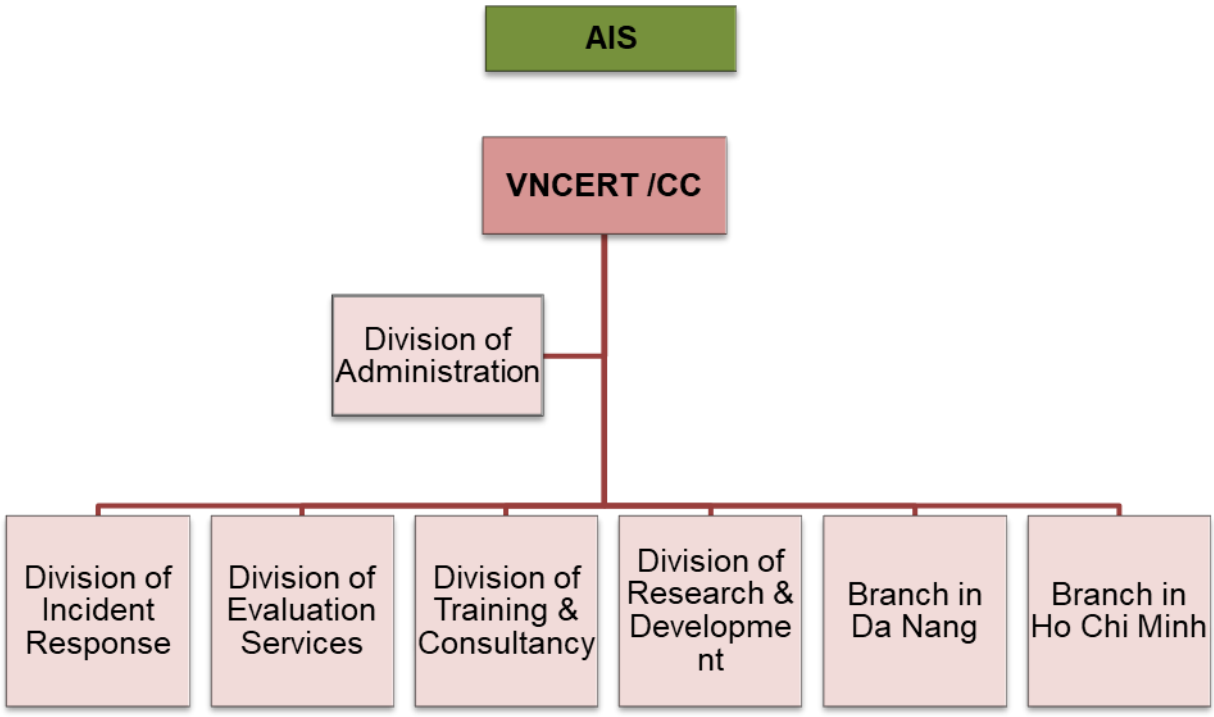
2. About VNCERT/CC

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 40 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 174 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)



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 130 members (including information technology centers of Ministries, ministerial agencies, governmental agencies, telecommunication enterprise, Internet service providers, 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 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	2019
Phishing	3,167
Deface	1,432
Malware	577
Total	**5,176**

Statistics of incidents by VNCERT

4. Events organized / hosted

4.1 Training

VNCERT had organized:

- 1 training courses on Network Security Monitoring for LaoCERT in Hanoi
- 5 internal training courses for staffs of VNCERT/CC
- 5 training courses for technicians at provinces
- 8 training courses for members of VNCSIRTs Network.

4.2 Drill & exercises

5 other information security exercises and training courses for different government agencies.

4.3 Conference & seminars

VNCERT cooperated with other organizations to organize annual events such as "Security World 2019", "National Information Security Day 2019" and organized 5 other conferences for CSIRTs Network members and information security departments from all over the country.

5. International Collaboration

5.1 International partnerships and agreements

No new agreements on 2019

5.2 Capacity building

5.2.1 Training

- Provided 01 training course for LaoCERT

- Nominated 10 delegations to attend the training coursed abroad

5.2.2 Drills & exercises

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

5.2.3 Seminars & presentations

Attended FIRST conference, NatCSIRT meeting, ASEAN-Japan meetings, CAMP meeting and other regional workshops in ASEAN.

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.

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 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

FSI-CERT

Financial Security Institute – Computer Emergency Response Team - Korea

1. Highlights of 2019

1.1 Summary of major activities

During 2019, FSI-CERT traced and analyzed various cyber threat data of financial institutions and published two intelligence reports.

- THE Incident Response MATRIX FOR MALWARE ATTACK
- TA505 Threat Group Profiling

FSI has contributed to strengthening incident response activities in the financial sector, such as preventing infringement of financial companies and the spread of damage, by carrying out digital forensic analysis to prevent incidents of servers and PCs that are likely to be breached.

By conducting a bug bounty program for the first time in the Korean financial sector, we have strengthened the stability of financial companies' services through preliminary analysis and response to potential vulnerabilities of financial security softwares.

Through collection, analysis and prompt information sharing of malwares affecting financial companies, we have contributed to the prevention of security incidents, avoiding the spread of damage.

We have also conducted incident response training for financial companies to strengthen their capabilities and check their incident response systems through actual practice such as blind(unannounced) training.

In order to reinforce our DDoS response system, we established a defense system capable of handling Tera-scale DDoS attacks by connecting with Cloud DDoS Scrubbing Centers.

And, FSI-CERT joined APCERT as a Liaison Partner to share information on security incidents in the Asia-Pacific region and strengthen cooperation.

1.2 Achievements

- 2nd, Jan. Full-scale implementation of the Financial Security Regtech System
- 10 th, Mar. 2019 General Meeting of the Financial Security Forum
- 11 th, Apr. Initiation of the 2019 Computer Emergency Response Training
- 1st.Jun. First bug-bounty program in financial sector
- 3rd, Jun. Opening of the 2nd FSI Education & Event Series for Threat Analysis (FIESTA)
- 20th.Jun. 2019 Financial Security Advisory Committee
- 3rd.Jul. Designated as ISMS-P integrated certification institution in financial sector
- 10th.Jul. College Student Financial Security Camp 2019
- 21st.Oct. Initiation of Fintech Security Check Service
- 22nd. Oct. joined APCERT Liaison Partner
- 7th.Nov. 2019 Financial Information Security Conference(FISCON)
- 6th.Nov. Intelligence Report Publication "THE Incident Response MATRIX FOR MALWARE ATTACK"
- 6th.Dec. Certification Program Launched - 2nd CFSE(Certified Financial Security Expert)
- 13th.Dec. Intelligence Report Publication "TA505 Threat Group Profiling"

2. About FSI-CERT

2.1 Introduction

FSI-CERT is a financial security-specialized organization founded by laws and regulations of the Government.

Through information sharing of incidents, notification of intrusion attempts, analysis of the incidents' cause, prompt response and prevention measures, we have established and operated an incident response system in the financial sector.

In case of incidents resulting from cyber-attacks, we analyze the cause of the incident through digital forensics, etc. and provide initial response along with prevention measures to hold back further damage or incidents.

We protect the financial industry from various cyber threats through threat monitoring, computer emergency response, vulnerability analysis and assessment.

2.2 Establishment

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

2.3 Resources

As of Dec., in 2019, around 200 employees from 7 divisions and 2 centers, work for FSI.

2.4 Constituency

FSI-CERT serves for the security of Korea's financial constituencies.
We are responsible for handling security issues in the financial industry through cyber threat detection, cyberattack response, and vulnerability analysis.

2.5 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

3. Activities & Operations

3.1 Scope and definitions

- Incident Response
  - Incident analysis and response
  - Collection, analysis, and response to malware
  - Computer Emergency Response Training
  - Threat intelligence sharing
  - Operation of DDOS attack emergency Response Center
  - Publication of Intelligence reports

- Integrated Security Monitoring of financial sector
  - Establishing and operating Integrated Security Monitoring Systems
  - Cyber threat information Sharing
  - Detecting and analysing intrusion attempts
  - Development and Application of the New Detection Technique

- Vulnerability Analysis and Assessment
  - Analysis and assessment of vulnerabilities of electronic financial facilities
  - Business evaluation of information technology sector
  - Stability Assessment of Cloud Service Providers
  - Analysis of security vulnerabilities and Establishment of assessment standards

3.2 Incident Response

3.2.1 Incident analysis and response

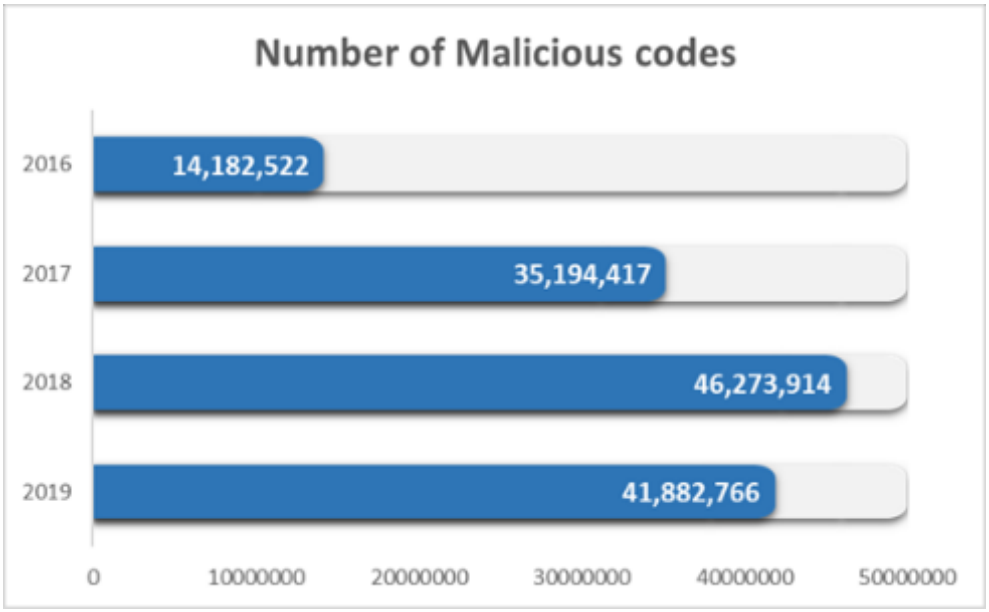
In the event of a cyber-attack against the financial sector, our forensic investigators get on the scene immediately to gather evidence and analyze the cause of the accident through digital-forensics. We also establish measures to prevent damage propagation and enhance cyber threat response capabilities of related financial organizations by conducting incident prevention digital forensic analysis on PCs that are likely to be targeted.

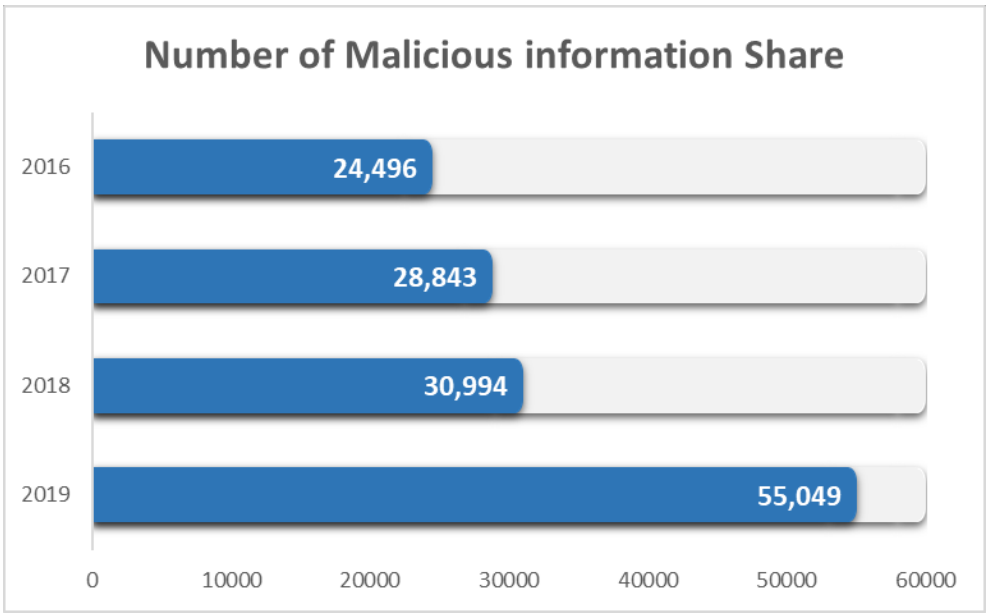
3.2.2 Collection, analysis, and response to malicious code information

We collect and analyze malwares distributed to intrude financial companies, share recent information security trends and perform the leading role for establishing and implementing the corresponding actions.

We systematically manage the vast amount of malware analysis results by using our

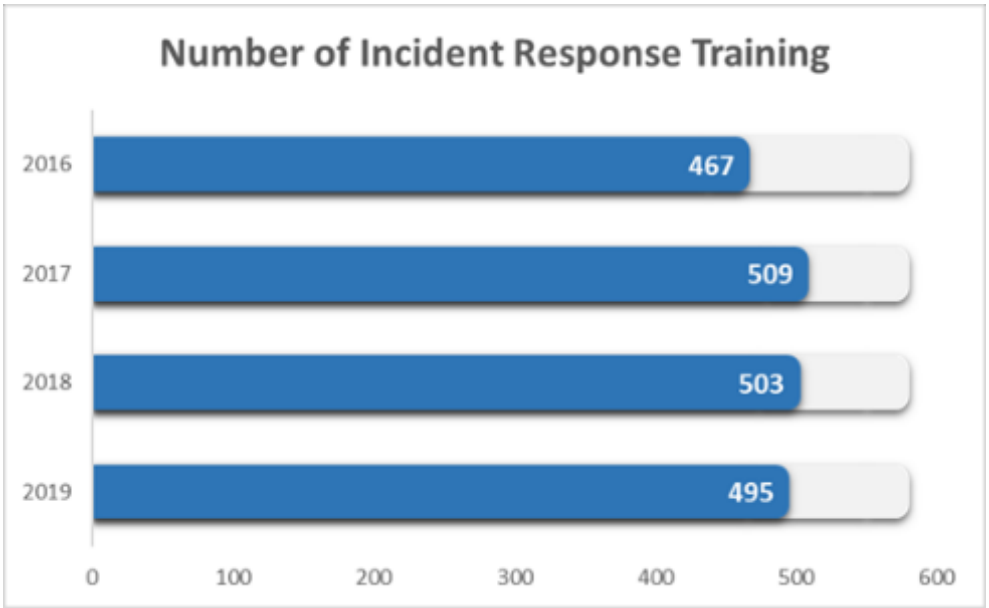
malware analysis system and provide information from correlation analysis.





3.2.3 Incident Response Training

DDoS attack response training, Server hacking response training, APT attack response training, etc. are conducted blindly to check the incident response system of financial companies.



3.2.4 Operation of DDOS Attack Emergency Response Center

If a large scaled DDoS Attack occurs which cannot be handled by financial companies, we aid them by filtering and sending back only valid traffic to the financial companies.

3.3 Integrated Security Monitoring

FSI-CERT operates a Financial sector Information Sharing and Analysis Center (ISAC) and uses a big data-based security monitoring system to detect cyber threats against the entire financial sector 24/7. Self-developed intrusion detection rules detect and analyze electronic intrusion attempts targeting financial companies quickly and efficiently.

Establishing and operating integrated Security Systems

- Security monitoring 24/7 in the financial sector
- Provide vulnerabilities and intrusion information, as well as the countermeasures
- Operation of analysis and response system

Detecting and analyzing intrusion attempts

- Intrusion Detection & Analysis
- Phishing / pharming site Detection & Reporting
- Monitoring availability of services
- Following the latest security trends

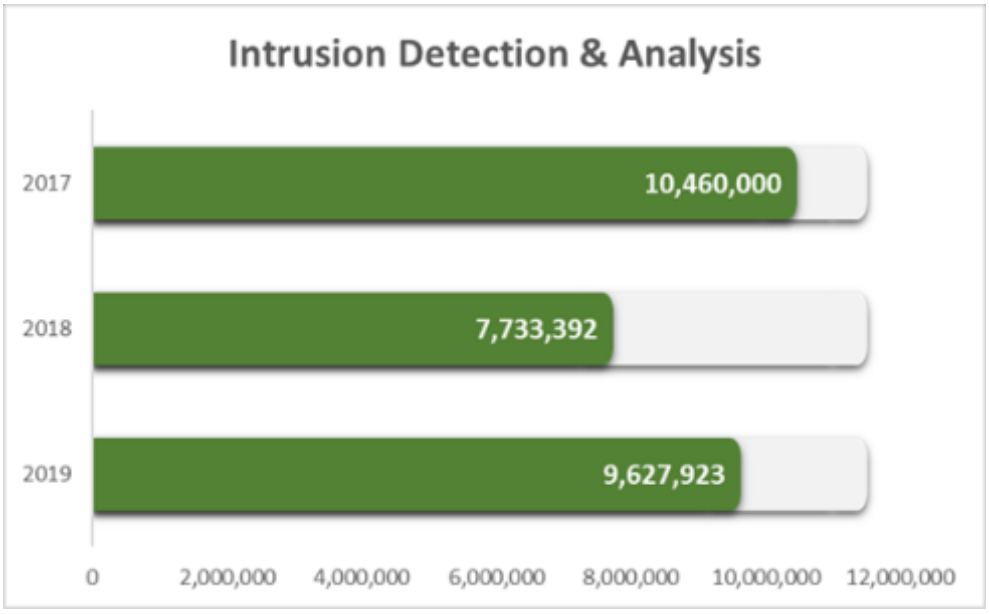
Serve as an integrated security operation center of the financial sector

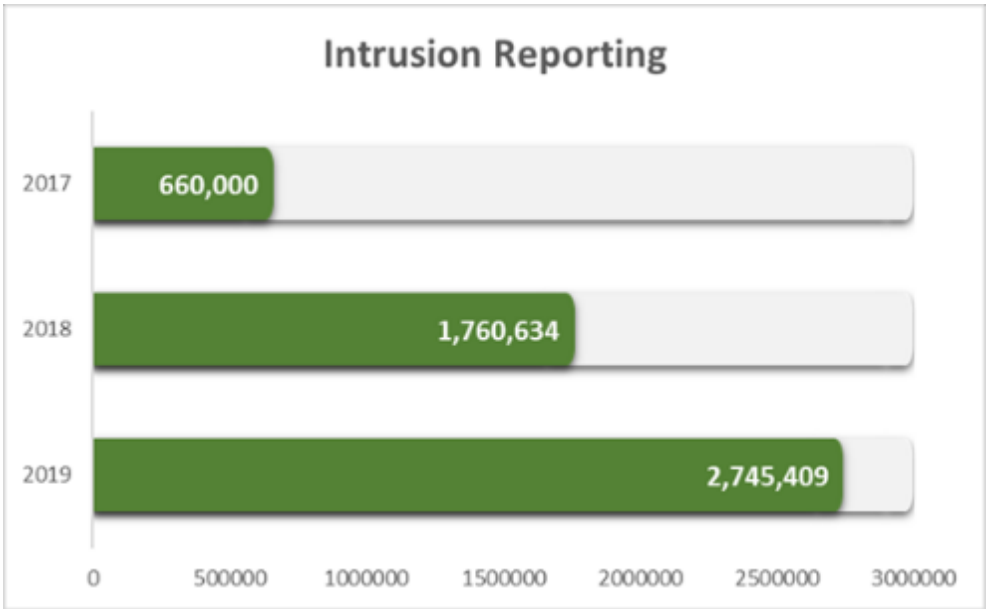
Cyber threat information Sharing

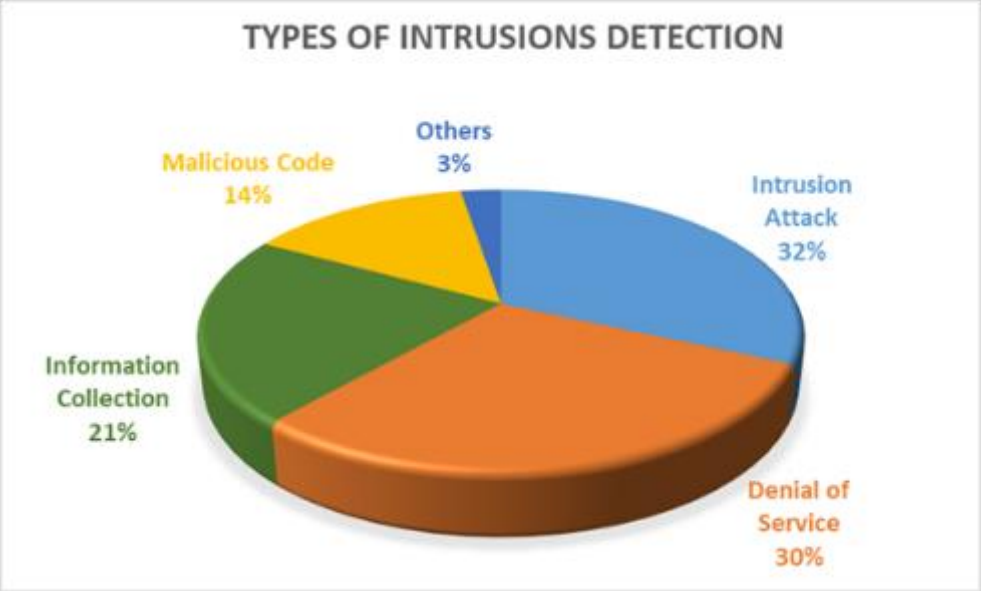
- Notification of intrusion attempts
- Intrusion intelligence sharing
- Fraud information sharing

Developing security attempts

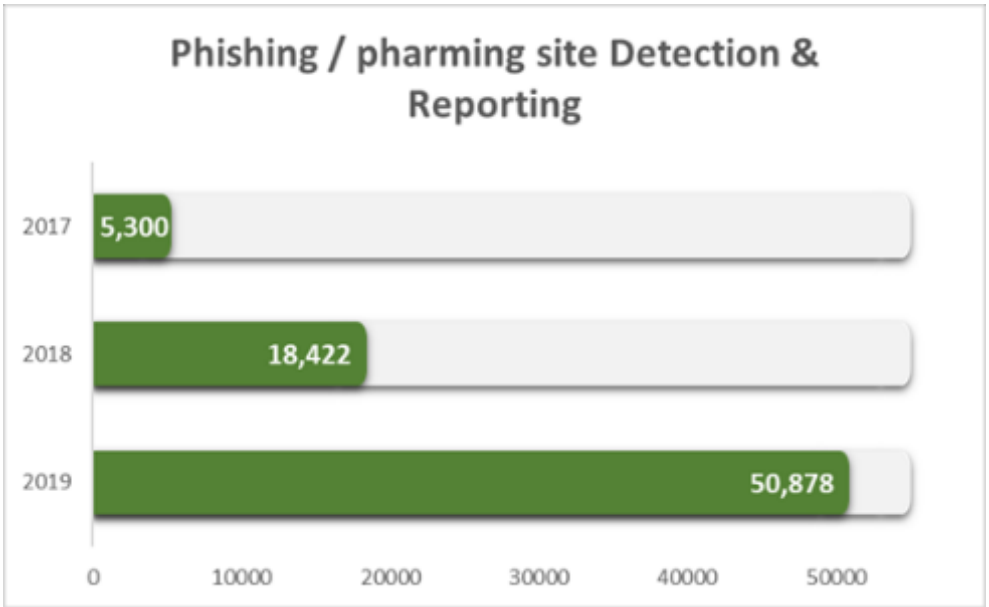
- Intrusion detection rule development
- Advanced cyber threat detection
- Latest phishing / pharming site detection techniques







With our self-developed phishing detection system, we also protect the valuable assets of consumers by detecting phishing sites that impersonate financial companies and malicious apps that are abused for voice phishing crimes.



3.4 Vulnerability Analysis and Assessment

We have provided comprehensive inspections and vulnerability checks on electronic financial infrastructure such as public homepages to help find and mitigate potential vulnerabilities in financial companies' systems.

We also support the autonomous security system of financial companies and have improved our evaluation method and inspection tools for inspecting vulnerabilities on our own and provided technology support and education to prevent incidents and provide a safe financial service.

Inspection areas : Information security management systems, Servers, Network, Information security systems, Web Applications, Mobile Applications, HTS(Home Trading System) Applications, Penetration Testing

3.5 Financial Security Education

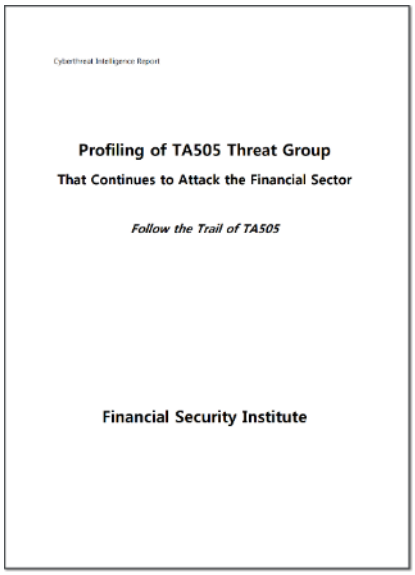
FSI enhances security capabilities by providing specialized education for executives and employees of financial companies.

FSI provides cyber education and customized off-line education reflecting the latest issues and demands in the financial security of executives, department heads and staff of financial companies.

In particular, in order to enable trainees to proactively respond to electronic financial breaches, hands-on training programs based on the latest hacking scenario at the Hacking Defense Training Center are provided.

4. Publications

FSI-CERT analyzes various cyber threat data for the financial sector and uploads monthly financial security trend reports on the website, Also, we select a research project every year, publishing cyber threat intelligence reports as a result.



- THE Incident Response MATRIX FOR MALWARE ATTACK

Based on actual cyber incidents' data that were investigated for 5 years from the foundation of FSI, we propose a matrix model based on malware attacks that can be used for response.

- TA505 Threat Group Profiling

Profiling analysis of the recent attacks on domestic users and financial institutions.

5. Events Organized / Hosted

- Financial Security Forum 2019
- Bug bounty program for financial sector
- Financial Security Advisory Committee 2019
- Seminar with CEOs on Information Security Day

- College Student Financial Security Camp 2019
- FIESTA 2019 (FSI Inner Education & Event Series for Threat Analysis)
- FISCON 2019 (Financial Information Security Conference)

6. Conferences and Presentation

In 2019, FSI-CERT dispatched speakers to the following international events:

- Black Hat ASIA 2019, hosted UBM(Singapore, March)
- HITB SecConf 2019, hosted HITB(Hack in the box)(Amsterdam, May)
- Financial Security Seminar by Central Bank of Egypt (May 2019)
- The State Bank of Vietnam Workshop, hosted by the Asian Development Bank (Hanoi, September)
- Virus Bulletin 2019, hosted VB(London, Oct)
- Bank of Thailand Seminar, hosted by the Asian Development Bank (Bangkok, December)

7. Future Plans

7.1 Future projects

FSI-CERT is celebrating its fifth anniversary and will be preparing for the next five years. For the past five years, we have worked to create a safe electronic financial environment. In the future, we will focus on new technologies such as AI, IoT, bigdata and Cloud security to proactively respond to security threats that may arise in the rapidly changing financial environment.

7.2 Future Operation

By upgrading existing systems such as our Security monitoring system, Malware analysis system, Phishing detection system and developing additional inspection tools, we will provide faster and more efficient services.

8. Conclusion

In this rapidly changing financial environment in which IT and financial converge vigorously leading to innovative financial services such as FinTech and Bigdata, bilateral online platform-based financial services have experienced widespread expansion and the paradigm of governmental regulation has changed from pre-planned regulation to autonomous self-regulation. FSI-CERT exerts continuous efforts to ensure an effective

and proactive response to computer emergencies and provide vital security services to financial institutions in order to protect the information asset and property of financial users.

Disclaimer on Publications

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

APCERT ANNUAL REPORT 2019

TLP: WHITE

APCERT
Asia Pacific Computer Emergency Response Team