TLP: WHITE

APCERT Annual Report 2017

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

CONTENTS

TWNCERT	241
VNCERT	253

Chair's Message 2017

The Asia Pacific Computer Emergency Response Team (APCERT) experienced a period of growth during 2017 with respect to both the scope and reach of our work. We saw our number of Operational Members increase to 30 teams representing 21 economies, and the breadth of our activities increase to encompass two new Working Groups, with an additional three proposed concepts in development. In this respect, as in many others, it was a rewarding year during which we continued to advance our cyber security collaboration in the region.

During 2017, APCERT undertook a series of initiatives to broaden our international collaboration. This included the revision of our membership structure and the creation of new partnership categories. With this approach we are expanding APCERT's breadth of engagement and depth of expertise and collaboration.

In addition to Operational Members, APCERT offers partnership categories for both not-for-profit/government organisations and corporate entities who share APCERT's vision for improved cyber security collaboration across our region and globally. APCERT also established a Liaison Partner category to, amongst other things, encourage developing CERTs in the Asia Pacific region and established CERTs outside the region to engage with the APCERT community. Representatives from six economies attended the APCERT Annual General Meeting and Conference in New Delhi, India at the invitation of the Steering Committee. The Organisation of Islamic Cooperation CERT (OIC-CERT) once again participated in the APCERT Cyber Exercise Drill.

The productive collaboration facilitated by the APCERT community is possible only through the commitment and drive of our Operational Members. They are the reason that collaboration across the region continues to prosper. APCERT is a community that is the sum of its parts, and without the contributions of individual members, APCERT would not continue to develop and grow. I would also like to acknowledge the contributions of APCERT's Supporting Members – now our Corporate Partners – to help us achieve our goals. We also appreciate the support of organisations such as the Asia Pacific Network Information Centre (APNIC) and the Forum of Incident Response Security Teams (FIRST).

The members of the Steering Committee have again demonstrated their dedication and leadership to the APCERT community, working together to achieve positive results, including as convenors of the various APCERT working groups. I thank them for their support and ongoing commitment to the APCERT community and its mission. In particular I thank MOCERT for its contribution over the past two years, and welcome CERT-In to the Steering Committee.

I would also like to thank JPCERT/CC for its unstinting support and contribution as the APCERT Secretariat, with almost all activities and operations of APCERT in some way facilitated or enabled by the Secretariat. JPCERT/CC has provided the Secretariat role since becoming a founding member of APCERT in 2003, and has consistently demonstrated outstanding and ongoing commitment to the community. On behalf of the APCERT community, I offer my appreciation for this valuable support and assistance.

CERT Australia is honoured to have been re-elected as Chair of the APCERT Steering Committee for 2018 and looks forward to working with all APCERT Members and our partners throughout the coming year.

Dr Ewan Ward
Chair, APCERT
CERT Australia

I. About APCERT

1. Objectives and Scope of Activities

The Asia Pacific Computer Emergency Response Team (APCERT) is a coalition of Computer Emergency Response Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs) within the Asia Pacific region. The organisation 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 actualisation.

The formation of CERTs/CSIRTs at the organisational, national and regional levels is essential to the 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);
- Trans-European Research and Education Networking Association (TERENA: www.terena.org) task force (TF-CSIRT: www.terena.nl/tech/task-forces/tf-csirt/);
- Organisation of the Islamic Cooperation – Computer Emergency Response Team (OIC-CERT: www.oic-cert.net);
- 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). The region covers the entire Asia Pacific, comprising of 56 economies. The list of those economies is available at: 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: (www.apcert.org/documents/pdf/OPFW(26Mar2013).pdf).

As of December 2017, APCERT consists of 30 Operational Members from 21 economies across the Asia Pacific region and 3 Corporate Partners. During 2017, BGD e-GOV CIRT (Bangladesh), BtCIRT (Bhutan) and CERT NZ (New Zealand) joined APCERT as an Operational Member. NCSC (New Zealand)'s membership was replaced by CERT NZ.

Operational Members (30 Teams / 21 Economies)

Team	Official Team Name	Economy
AusCERT	Australian Computer Emergency Response Team	Australia
bdCERT	Bangladesh Computer Emergency Response	Bangladesh

	Team	
BGD e-GOV CIRT	Bangladesh e-Government Computer Incident Response Team	Bangladesh
BruCERT	Brunei Computer Emergency Response Team	Negara Brunei Darussalam
BtCIRT	Bhutan Computer Incident Response Team	Bhutan
CCERT	CERNET Computer Emergency Response Team	People's Republic of China
CERT Australia	CERT Australia	Australia
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
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	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	Macao
MonCIRT	Mongolian Cyber Incident Response Team	Mongolia
MyCERT	Malaysian Computer Emergency Response Team	Malaysia
NCSC	New Zealand National Cyber Security Centre *Withdrew membership in September 2017	New Zealand
SingCERT	Singapore Computer Emergency Response Team	Singapore
Sri Lanka CERT|CC	Sri Lanka Computer Emergency Readiness Team Coordination Centre	Sri Lanka

TechCERT	TechCERT	Sri Lanka
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

Corporate Partners (3 Teams) *formerly referred to as Supporting Members

- Bkav Corporation
- Microsoft Corporation
- SecureWorks

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

At the APCERT AGM 2017, CERT Australia was re-elected as Chair of APCERT, and Malaysian Computer Emergency Response Team (MyCERT) as Deputy Chair. JPCERT/CC was re-elected as Secretariat.

The following teams were elected to/remained on the APCERT Steering Committee (SC).

Team	Term	Other positions
CERT Australia	2016 - 2018	Chair
CERT-In *Newly elected at AGM 2017	2017 - 2019	
CNCERT/CC	2016 - 2018	
JPCERT/CC	2015 - 2017	Secretariat
KrCERT/CC	2016 - 2018	
MOCERT *Stepped down at AGM 2017	2015 - 2017	
MyCERT	2015 - 2017	Deputy Chair
TWNCERT	2016 - 2018	

3. Working Groups (WG)

There are currently six (6) Working Groups (WGs) 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 (24): AusCERT, bdCERT, BruCERT, CamCERT, CCERT, CERT-In, CNCERT/CC, GovCERT.HK, HKCERT, ID-SIRTII/CC, KrCERT/CC, LaoCERT, maCERT, mmCERT, MNCERT, MOCERT, MonCIRT, MyCERT, PHCERT, SingCERT, 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 (12): AusCERT, BKIS, HKCERT, ID-CERT, ID-SIRTII/CC, JPCERT/CC, KrCERT/CC, 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 basis 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 (12): AusCERT, BruCERT, CNCERT/CC, HKCERT, ID-CERT, ID-SIRTII/CC, JPCERT/CC, MOCERT, MyCERT, 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 as they relate to the Operational Framework (also known as sub-documents), and supplement these with guidelines or other documents as needed
  - Identify and resolve issues relating to APCERT policies, procedures and governance, including through referring them to the SC or APCERT membership where appropriate, and
  - Undertake other activities related to policy, procedures and governance for APCERT as directed by the SC.
- Convener (1): CERT Australia
- Members (5): HKCERT, JPCERT/CC, KrCERT/CC, MOCERT, 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 (11): CERT-In, CNCERT/CC, HKCERT, ID-SIRTII/CC, JPCERT/CC, KrCERT/CC, MOCERT, 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): MyCERT
- Members (11): BruCERT, GovCERT.HK, HKCERT, ID-CERT, JPCERT/CC, KrCERT/CC, SingCERT, Sri Lanka CERT|CC, TWCERT/CC, Bkav Corporation, SecureWorks

7) Drill WG (formed in 2017)

- Objectives
  - To serve as a permanent Organizing Committee for the annual cyber drills and assist the Lead Organizing CERT
  - To maintain centralized documentation for the drills, their working documents, procedures, handbooks and feedback.
  - To allow continuous improvements.

- Convener (1): ThaiCERT
- Members (10): AusCERT, CERT Australia, CERT-In, HKCERT, JPCERT/CC, SingCERT, Sri Lanka CERT|CC, TechCERT, ThaiCERT, TWCERT/CC

4. APCERT Website

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

II. APCERT Activity Report 2017

1. International Activities and Engagements

APCERT has been dedicated to represent and promote APCERT activities in various international conferences and events. From January to December 2017, APCERT Teams have hosted, participated and/or contributed in the following events:

- **AP* Retreat Meeting (26 February – Ho Chi Minh City, Vietnam)**
  APCERT Chair and Secretariat attended the AP* Retreat Meeting which was held in conjunction with APCIROT 2017 and presented activities of APCERT to the community.

- **APCERT Drill 2017 (16 March)**
  https://www.apcert.org/documents/pdf/APCERTDrill2017PressRelease.pdf
  APCERT Drill 2017, the 13th APCERT Cyber Exercise Drill, was successfully conducted to test the response capabilities of the participating APCERT Teams. Pursuant to the Memorandum of Understanding on collaboration between APCERT and the Organisation of the Islamic Cooperation – Computer Emergency Response Team (OIC-CERT) in September 2011, APCERT invited the participation from OIC-CERT Teams for the third time. 23 teams from 18 economies of APCERT (Australia, Brunei Darussalam, People's Republic of China, Chinese Taipei, Hong Kong, India, Indonesia, Japan, Korea, Lao People's Democratic Republic, Macao, Malaysia, Mongolia, Myanmar, Singapore, Sri Lanka, Thailand and Vietnam), and 4 teams from 4 economies of OIC-CERT (Egypt, Morocco, Nigeria and Pakistan) participated in the Drill. The theme of the drill was "Emergence of a New DDoS Threat".

- **APEC-TEL 55 (2 – 7 April – Mexico City, Mexico)**
  APCERT participated APEC TEL 55 and presented the APCERT's overview and latest activities for a safer cyber space base on the regional framework.

- **29th Annual FIRST Conference (11- 16 June – San Juan, Puerto Rico)**

  https://www.first.org/conference/2017/

  APCERT Teams attended the Annual FIRST Conference in San Juan, Puerto Rico, and shared valuable experience and expertise through various presentations.

- **National CSIRT Meeting (16-17 June – San Juan, Puerto Rico)**

  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) 2017 (11 September)**

  ACID 2017, led and coordinated by SingCERT, entered its 12th 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 2017 (12-15 November – Delhi, India)**

  https://apcert2017.in

  The APCERT Annual General Meeting (AGM) & Conference 2017 was held on 12-15 November, 2017 at Hotel the Ashok in Delhi, India.

  Programme Overview:

12 November (Sun)	AM:	Working Group Meetings
	PM:	APCERT Team Building, Welcome Cocktail
13 November (Mon)	AM:	TSUBAME Workshop
	PM:	Steering Committee Meeting
14 November (Tue)	AM:	APCERT Closed Conference
	PM:	APCERT Annual General Meeting
15 November (Fri)	AM:	Open Conference

- **TSUBAME Workshop 2017 (12 November – Delhi, India)**

  The APCERT TSUBAME Workshop 2017 on Network Traffic Monitoring Project was held on 12 November, in conjunction with APCERT AGM & Conference 2017.

JPCERT/CC enhance the TSUBAME project and the cooperation among its members.

- **APEC-TEL 56 (10-15 December– Bangkok, Thailand)**
  Some APCERT teams participated at APEC TEL 56.

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)**
  Koichiro Komiyama of JPCERT/CC has been serving as a member of FIRST.org Board of Directors since June 2014.

- **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.

2. APCERT SC Meetings

From January to December 2016, SC members held five (5) teleconferences and two (2) face-to-face meeting to discuss APCERT operations and activities.

18 January	Teleconference
25 February	Face-to-face meeting concurrently held at APRICOT 2017 in Ho Chi Minh City, Vietnam

27 April	Teleconference
18 July	Teleconference
13 September	Teleconference
1 November	Teleconference
12 November	Face-to-face meeting at APCERT AGM 2017 in Delhi, India

3. APCERT Training Calls

APCERT held six (5) training call in 2016 to exchange technical expertise, information and ideas.

Date	Title	Presenter
8 February	Digital Forensics	Sri Lanka CERT|CC
19 April	Mobile Vulnerability Check and Case Study	KrCERT/CC
1 August	Cyber Detection, Eradication and Forensic (Cyber D.E.F)	MyCERT
3 October	Cyber threat information sharing	CERT Australia
5 December	Introduction of DDoS Offensive and Defensive Exercise in Taiwan	TWNCERT

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

URL: *www.apcert.org*
Email: *apcert-sec@apcert.org.*

III. Activity Reports from APCERT Members

AusCERT

Australian Computer Emergency Response Team – Australia

1. Highlights of 2017

1.1 Summary of major activities

AusCERT continues to deliver sought after computer security incident handling and early warning information.

1.2 Achievements & milestones

1.2.1 Health Sector ISAC Deployment

During 2017 AusCERT has established an Information Security and Analysis Centre (ISAC) servicing the Health Sector.

1.2.2 Education Sector pilot MISP Implementation

The AusCERT instance of Malware Information Sharing Platform (MISP), for the Education Sector has been successfully piloted in 2017 with the system ready for full use in 2018.

1.2.3 New AusCERT Website

AusCERT has expanded the facilities for the members to control their related interactions with AusCERT services through the website. This provide convenience and value to the AusCERT constituency.

1.2.4 Constituency growth

AusCERT, with a membership-based constituency, has increased the breadth of organisations that it serves.

2. About AusCERT

2.1 Introduction

AusCERT is a leading Cyber Emergency Response Team for Australia and provides information security advice to its members, including the higher education sector. As a not-for-profit security group based at the University of Queensland's (UQ) Information Technology Services (ITS), AusCERT is the single point of contact for dealing with cyber

security incidents affecting or involving member networks. AusCERT helps members prevent, detect, respond to and mitigate cyber and Internet based attacks.

2.2 Establishment

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

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

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

2.3 Resources

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

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

2.4 Constituency

AusCERT is a member-based organization and its constituents consist of private, government and education businesses.

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).

3. Activities & Operations

3.1 Scope and definitions

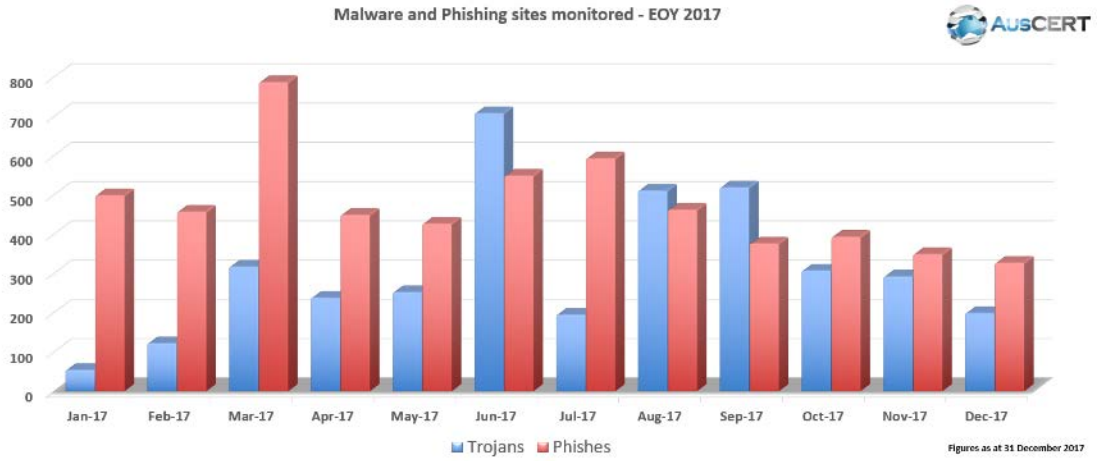
AusCERT monitors and evaluates global cyber network threats and vulnerabilities and remains on-call for members after hours. AusCERT publishes the Security Bulletin Service, drawing on material from a variety of sources, with recommended prevention and mitigation strategies.

Services provided are listed as:

- Incident Management [3.2], https://www.auscert.org.au/services/incident-management-service/
- Early Warning Service [3.3] https://www.auscert.org.au/services/early-warning-service/
- Malicious URL Feed [3.4] https://www.auscert.org.au/services/malicious-url-feed/
- Member security incident notification's (MSINs)[3.5.1] https://www.auscert.org.au/services/security-incident-notifications/
- Phishing take-down [3.6] https://www.auscert.org.au/services/phishing-take-down-service/
- Security Bulletin Service [3.7] https://www.auscert.org.au/services/security-bulletins /
- AusCERT's member only IRC channel
- AusCERT Conference https://conference.auscert.org.au/
- AusCERT Certificate Service https://cs.auscert.org.au/

3.2 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 2017. These tallies are sites that are located around the world in a manner that affects the operation of the constituency that AusCERT is serving.

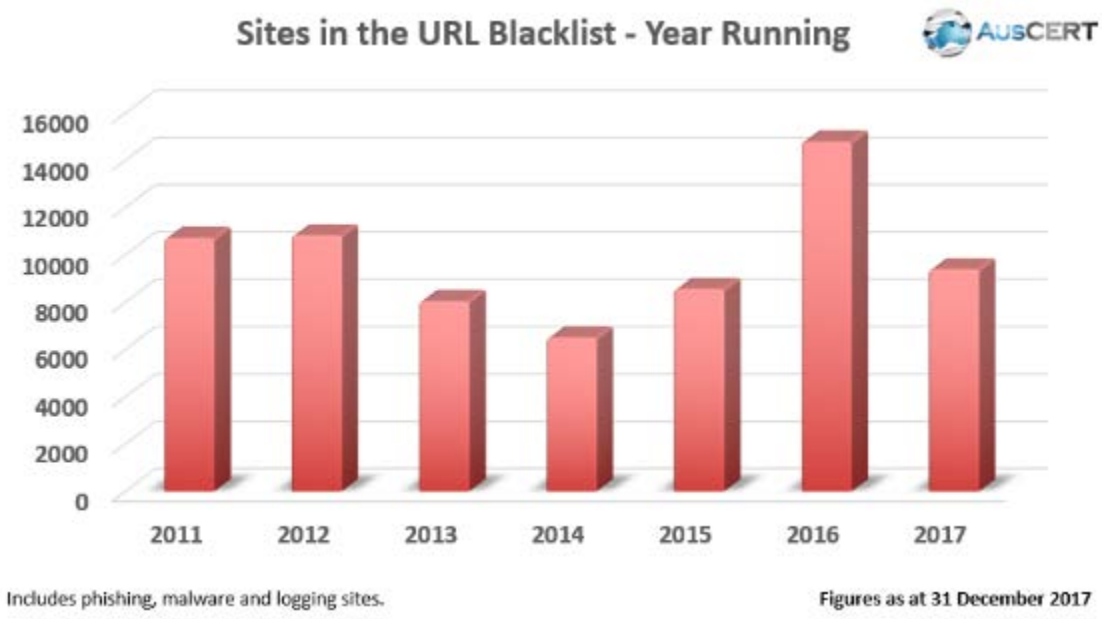
3.3 Early Warning System

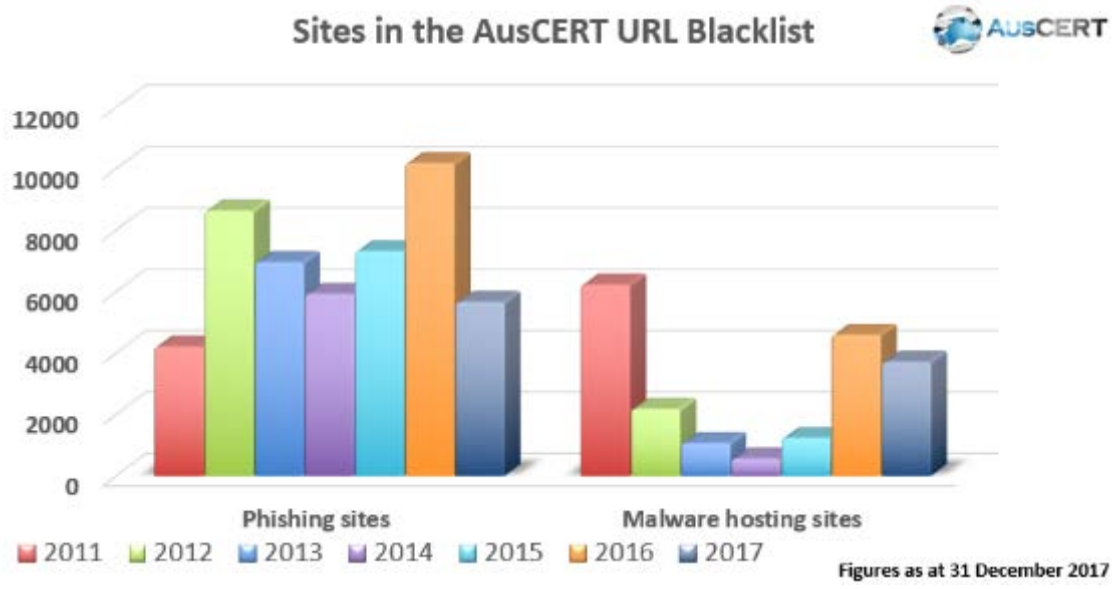
Members can subscribe to receive urgent SMS notifications, when AusCERT's Security Bulletin Service identifies a vulnerability that has reached critical stages. In most circumstances this occurs when AusCERT is aware of active, in-the-wild exploitation of a vulnerability.

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. Throughout the year of 2017 forty-eight (48) bulletins merited the need to elevate them to alerts where constituencies were advised of taking special attention to the information contained in the bulletin released. Of the forty-eight alerts, only a subset was of an importance that required to send accompanying SMS's.

3.4 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.





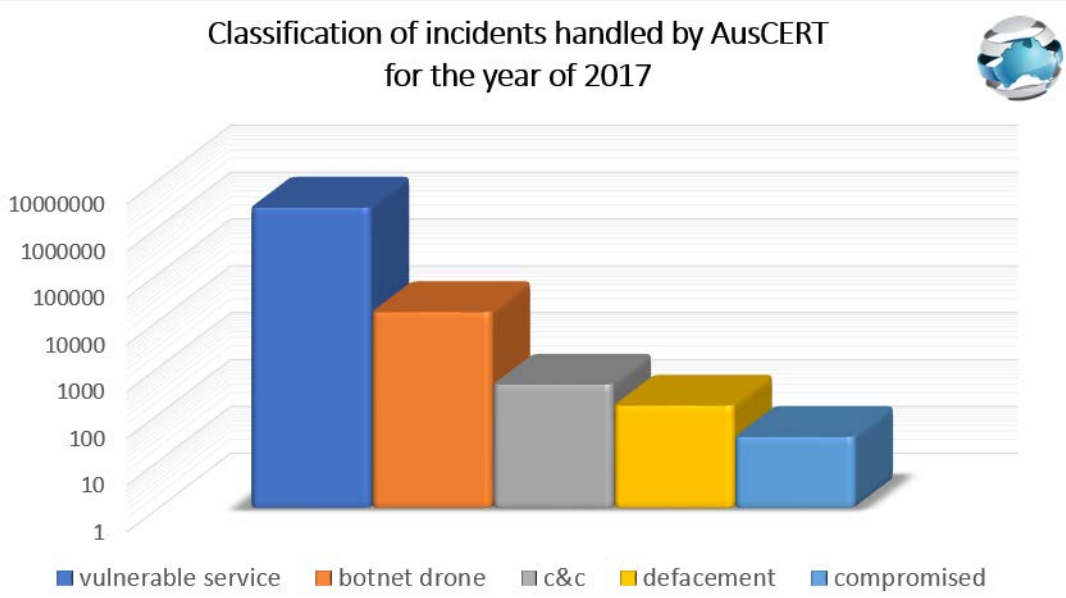
3.5 Notifications

3.5.1 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. We are now, in 2017, able to report on the numbers and types of incidents reported to the Members.

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.

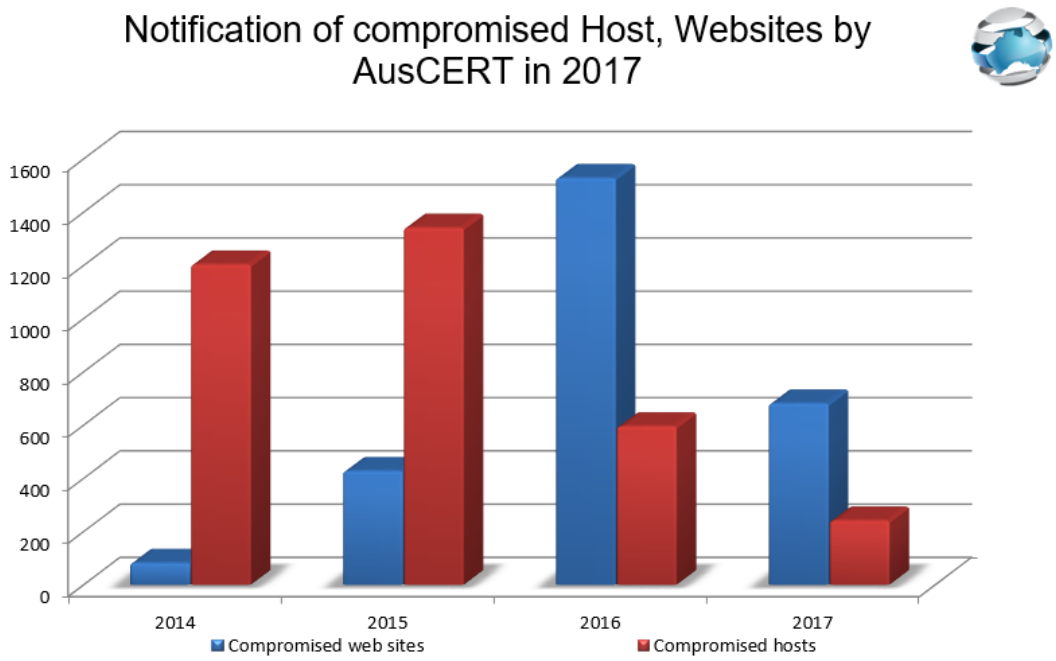


Indicators of Vulnerabilities such as the notification that services that are running by members are vulnerable, were made at a staggering two million, five hundred and eighty-six thousand, two hundred and thirty-two (2,586,232) times.

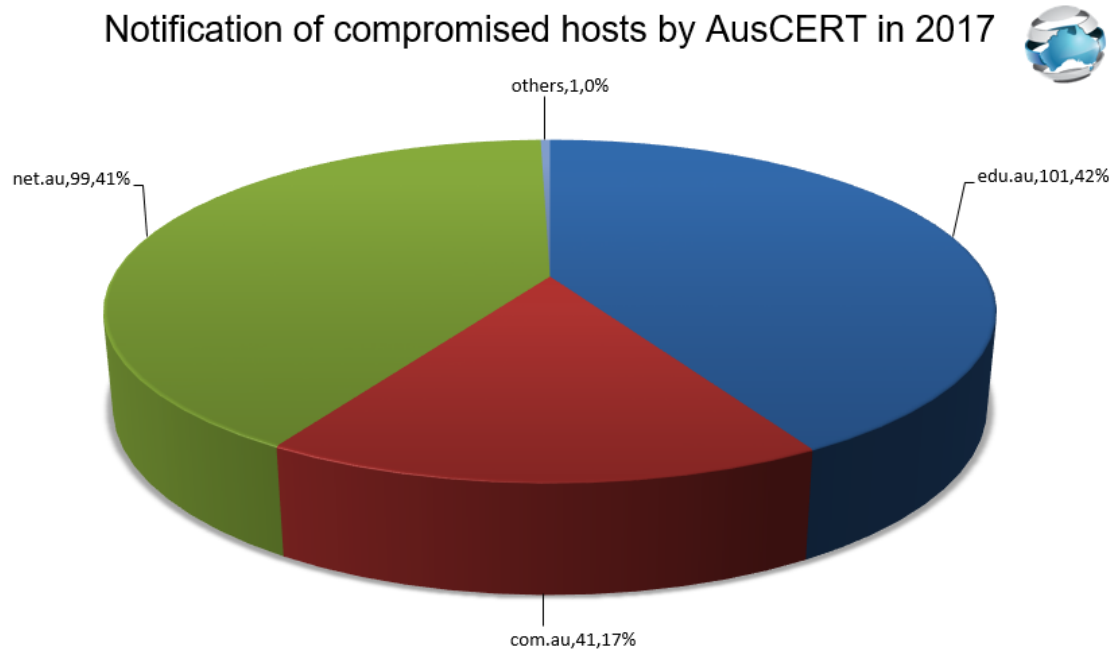
The numbers of other types of notifications are not as many but are just as important. Botnet drones tallied at fifteen thousand two hundred and thirty-two (15,232), Command and Control were found in four hundred and thirty-one (431) unique instances, Defacement at one hundred and fifty-four (154) and compromised hosts at thirty-three (33) instances.

3.5.2 Legacy notification and reporting system.

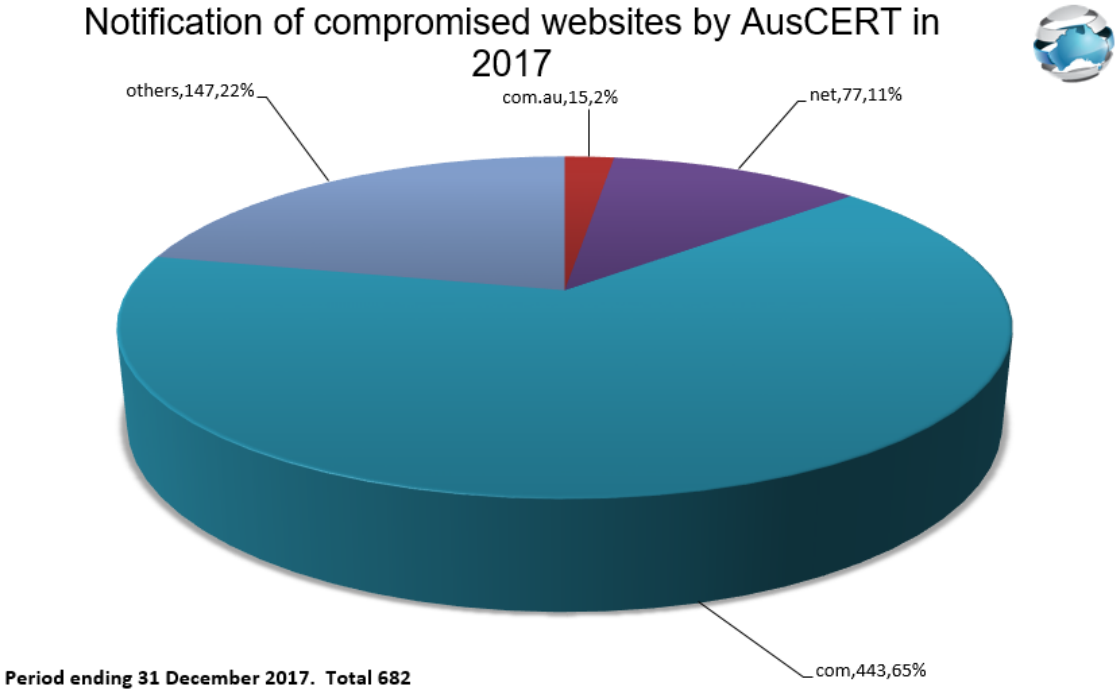
To be able to compare notes of the continued notification of compromised host and websites the following graphs are still provided for reference. These numbers and graphs are provided this year as a bridge to the new system and its reporting capability.



AusCERT email notifications of compromised hosts and web sites in Australia and overseas. **As at 31 December 2017.**



Period ending 31 December 2017. Total 242



3.6 Phishing Takedown

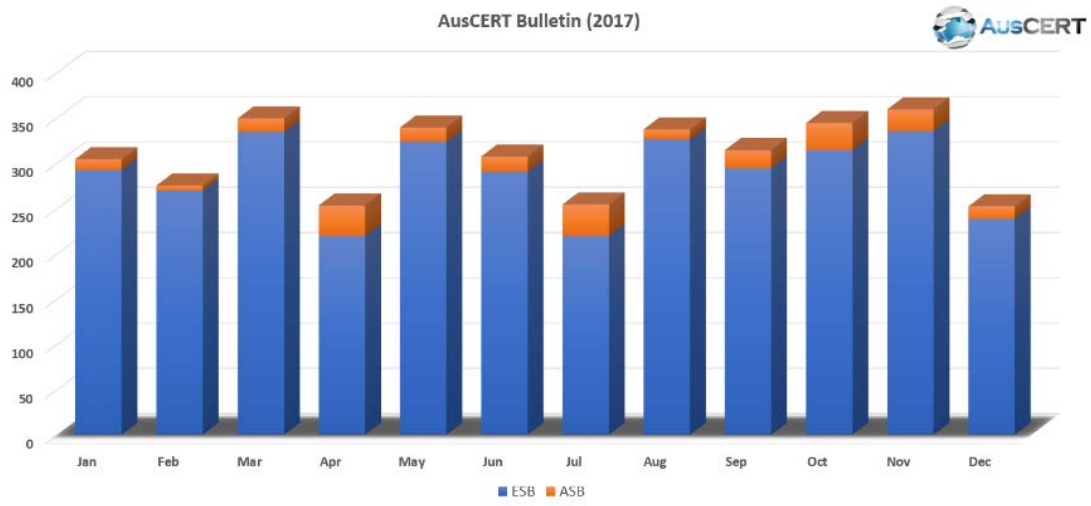
AusCERT Members can utilise AusCERT's considerably large overseas and local contact network for removal of phishing and malware sites. The number of sites that were handled in the year 2017 has already been graphed in the section Malware URL. Specifically, for Phish site, the tally is Five thousand six hundred and sixty-eight (5,668). A subset of these. This service is not limited to taking down phishing sites but also of takedowns of sites that are serving malware. Of those malware sites, three thousand seven hundred and fourteen (3,714) sites have been reported in the calendar year of 2017. This can be seen from the diagram below.

3.7 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 2017, three thousand four hundred and fifty-three (3,453) External Security Bulletins (ESBs) and two hundred and thirty-four (234) 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.



3.8 Publications

3.8.1 Week-In-Review

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

3.8.2 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.

3.8.3 Newsletters

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

3.8.4 Blog Posts

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.

4. Events organized / hosted

4.1 AusCERT Training

This year of 2017 AusCERT has piloted two training courses that are delivered for the constituency. In light of the success of the rolling out of the Risk Management and

Incident Response course, AusCERT is keen to include addition courses into the coming year.

4.2 AusCERT Conference

The AusCERT Conference 2017, took place from 23rd-26th May 2017 in Surfers Paradise Gold Coast, Australia. With the theme of "United We Stand" the conference covered areas such as:

- Mandatory Breach notification laws: and item that is focal as Australia moves to adopt these laws.
- Governance and compliance in Cyber Risk Management;
- Information sharing for better information security response and defence.
- Biometric security their pros and cons and ways to break voice recognition systems
- The use of Artificial Intelligence to combat Cyber threats.

5. International Collaboration

5.1 International partnerships and agreements

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

5.2 Capacity building

5.2.1 APCERT Drill 2017

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 "Emergence of a New DDoS Threat" wherein AusCERT played through the exploitation of devices infected with Mirai malicious code. The drill is extremely valuable as it fosters communication between the CERTs in the region and beyond. In all, 23 CERT teams from APCERT participated, along with 4 teams from the Organisation of Islamic Cooperation – Computer Emergency Response Team

(OIC-CERT). AusCERT operations staff members were kept busy throughout the exercise with tasks that included email analysis, malware analysis and log file analysis.

6. Conclusion

This year of 2017 has been one of growth both in capacity and capability for AusCERT which was reflected by the addition of two (2) more analysts in the year of 2017 on top of the numbers gained in the previous year 2016. The year was a clear demonstration that there are many ways to assist a CERT's constituency in reducing the impact of computer based malicious attacks. AusCERT has been part of that activity in keeping the internet a safe and reliable resource.

BGD e-Gov CIRT

Bangladesh e-Government Computer Incident Response Team - Bangladesh

1. HIGHLIGHTS OF 2017

1.1 Summary of Major Activities

- 684 cyber security incidents registered in our tracking system in 2017.
- Organized 3 cyber security events.
- Arranged 18 cyber security trainings.

1.2 Achievements and milestones

- Publish Mobile Apps for incidents reporting from Mobile Phone;
- Published various cyber security related articles in native language (Bengali).

2. ABOUT CIRT

2.1 Introduction

BGD e-GOV CIRT mission is to support government efforts to develop and amplify ICT programs by establishing incident management capabilities within Bangladesh, which will make these programs more efficient and reliable.

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 5 people are working in BGD e-GOV CIRT and more people will be join soon.

2.4 Constituency

Constituency of BGD e-Gov CIRT are all governmental ministry & institutions of Bangladesh including National Data Center (NDC) located at BCC where host their IT resources and services.

The constituency range and description will be continuously checked and updated to ensure that all ICT resources which should be protected are covered by the designed and implemented incident management services.

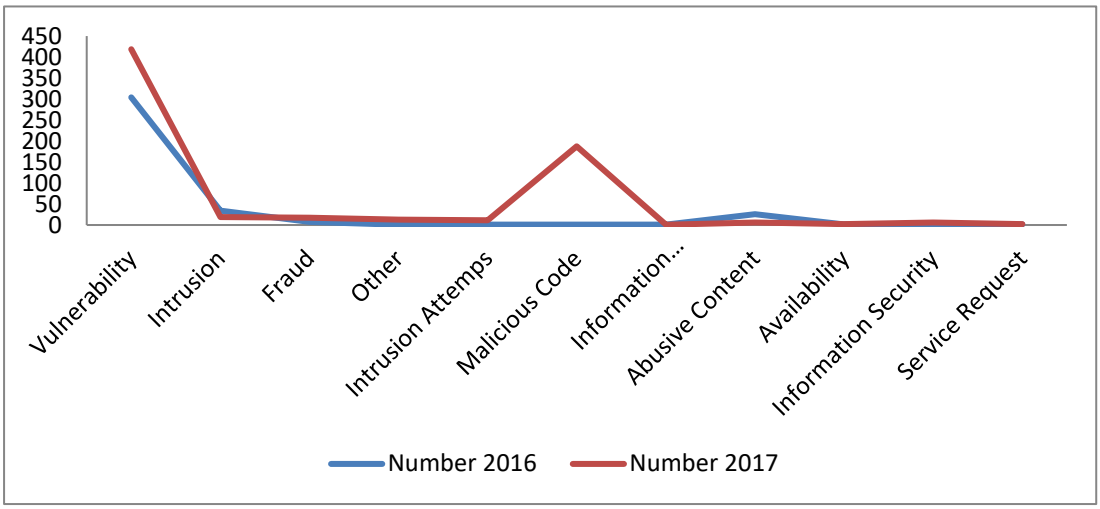
3. ACTIVITIES AND OPERATIONS

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 Incidents handling reports

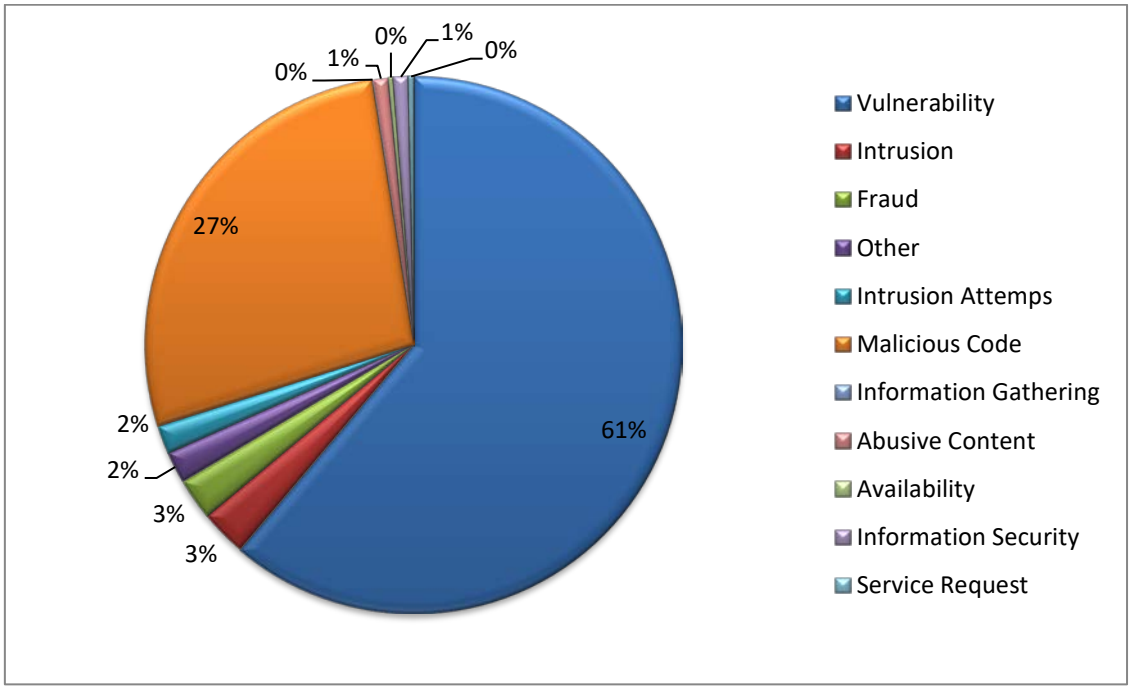
BGD e-GOV CIRT will receive information regarding cyber security incidents, triage incidents and coordinate response. Possible activities related to incident handling include Reporting, Coordination, Incident response support and Incident analysis and evidence collection. Total 684 incidents are reported at 2017 which is more 305 than the year 2016. In addition, the vulnerability, malicious code attack are higher than the previous year.



Number of incident reported at 2017

3.3 Abuse Statistics

BGD e-GOV CIRT received numerous incident reports on different forms of cyber-attack via mail and web portal. Some of the common cyber threats observed in Bangladesh are website defacements, phishing websites and ransomware, including new ransomware variants such as Bad Rabbit, Petya/Petna and WannaCry infections. In 2017 total 684 incidents are reported at BGD e-GOV CIRT.



Incidents Classification

3.4 Publications

- Publications: Published "BGD e-GOV CIRT" annual report of 2016.
- Published "Government of Bangladesh Information Security Manual (GoBISM) v1.5"
- Published article on The Effect of Bitcoin on Cybersecurity by CIRT Team Leader Tawhidur Rahman on Pentest Magazine
- Published article on Crowdsourcing improvement in Cybersecurity and Bangladesh by CIRT Team Leader Tawhidur Rahman on Digitalworld 2017 event magazine.
- Published article on Cybersecurity Framework for Rooppur Nuclear Power Plant Bangladesh by CIRT Team Leader Tawhidur Rahman.
- Published article about Buffer Overflow: Taking control of an operating system by Mohammad Ariful Islam on Pentest Magazine
- Published article about Malware Analysis Infection method & Malicious work by Debashis Pal on Pentest Magazine

3.5 New Services

Currently BGD e-GOV CIRT gives the following services:

- Security assessments
- Configuration and maintenance of security tools, applications, and services

- Intrusion detection
- Security consulting
- Awareness building

BGD e-GOV CIRT will facilitate forensic analysis to its stakeholder after the laboratory established.

4. EVENTS ORGANIZED/HOSTED

4.1 Training

BGD e-GOV CIRT gave training in 18 different Security category. Created 2496 Cyber aware people through conducting different types of trainings and events.

4.2 Drill and Exercises:

- Attend on ”50th TF-CSIRT Meeting & FIRST Regional Symposium for Europe”.
- Attend on ”2017 APISC Security Training Course”.
- Attend on ”29th Annual FIRST Conference in Puerto Rico".
- Participate in “OIC Drill 2017”.
- Attend on “OIC-CERT Annual Conference 2017 in Baku, Azerbaijan”.
- Attend on “APCERT Annual General Meeting & Conference 2017 in New Delhi, India”.
- CERT Game Challenge conducted by comCERT and NRD

4.3 Conferences and Seminars:

- International Cyber Security Conference Bangladesh
- Workshop on Cyber Security Management at Bangladesh Computer Council

5. International Collaborations

5.1 International Partnership and Collaboration

In order to benefit from international cyber security best-practices, established information security standards and have access to global technological information security research, BGD e-GOV CIRT has already obtained membership with various organizations in international CERT community:

- FIRST
- APWG
- TEAM CYMRU

- SHADOWSERVER
- STOP.THINK.CONNECT
- APCERT
- OIC-CERT

BGD e-GOV CIRT has also collaboration with CERT-In to enhance co-operation in national security, strategic and operational studies.

5.2 Capacity Building

5.2.1 Training

- Attend on ”2017 APISC Security Training Course”.

5.2.2 Drills and Exercises

- Participate in “OIC Drill 2017”.

5.2.3 Seminars and Presentations

- Attend on “50th TF-CSIRT Meeting & FIRST Regional Symposium for Europe”.
- Attend on “29th Annual FIRST Conference in Puerto Rico".
- Attend on “OIC-CERT Annual Conference 2017 in Baku, Azerbaijan”.
- Attend on “APCERT Annual General Meeting & Conference 2017 in New Delhi, India”.

5.2.4 Made SOP for Law Enforcement

- BGD E-GOV CIRT has made Standard Operating Procedure for Law Enforcement of Bangladesh.

6. FUTURE PLAN

- CIRT Laboratory will be operational which will enable BGD e-GOV CIRT to analyze malwares, initiate forensic jobs and many other capabilities.
- Sensor Network will operational.
- Cyber Range will be operational.

7. ATTACHMENT (Photos)

1st Cyber Security Conference

International Cybersecurity Conference Hosted in BGD e-GOV CIRT Inaugurate by Honorable Chif Guest Hon'le State Minister of ICT Division Zuanid Ahmed Palak, MP

International Cybersecurity Conference Hosted in BGD e-GOV CIRT Chaired by Honorable Secretary of ICT Division Subir Kishore Choudhury

International Cybersecurity Conference Hosted in BGD e-GOV CIRT

Training on Eancase Forensic Certification

Training on vulnerability assessment and penetration testing for Government officials of Bangladesh in BGD e-GOV CIRT Training LAB

Blue Whale game awareness rising campaign by BGD e-GOV CIRT presented Hon'le State Minster of ICT Zuanid Ahmed Palak, MP

Member of the Board of Directors of FIRST.Org, Inc and Senior Internet Security Specialist of APNIC Mr. Adli Wahid has visited BGD e-GOV CIRT on October 2017

Accounting fraud investigation training for Audtor General of Bangladesh & FAPAD Bangladesh officer

Meeting With Honorable State Minister, ICT on Cyber Security Bangladesh Issues with all Government Ministry stakeholder.

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.

Government Ministries and Departments

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

E-Government National Centre (EGNC)

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

AITI

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

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

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

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

TelBru – BruNet

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

IT environment in Brunei.

DST – simpur

The second largest internet service provider in Brunei.

1.5 BruCERT Contact

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

Telephone: (673) 2458001
Facsimile: (673) 2458002
Email: cert@brucert.org.bn
website: www.brucert.org.bn
www.secureverifyconnect.info

2. BruCERT Operation in 2017

2.1 Incidents response

In 2017, BruCERT had deployed security threat intelligence sensors in strategic network infrastructure to detect any malicious activities in network. Most of the High severity threats are due to malware related activity such as generic malware, malware infection, malicious bot and IRC Bot. There are some hacking attempts due to vulnerability which may perform by worms. The problems may be a rise due to lack of security controls such as no or outdated Antivirus solution, un-patched operating system or using legacy operating system. The security incidents might also be due to no administrative control to machines connected to the network. The statistic of the security incident is shown as Figure 1.

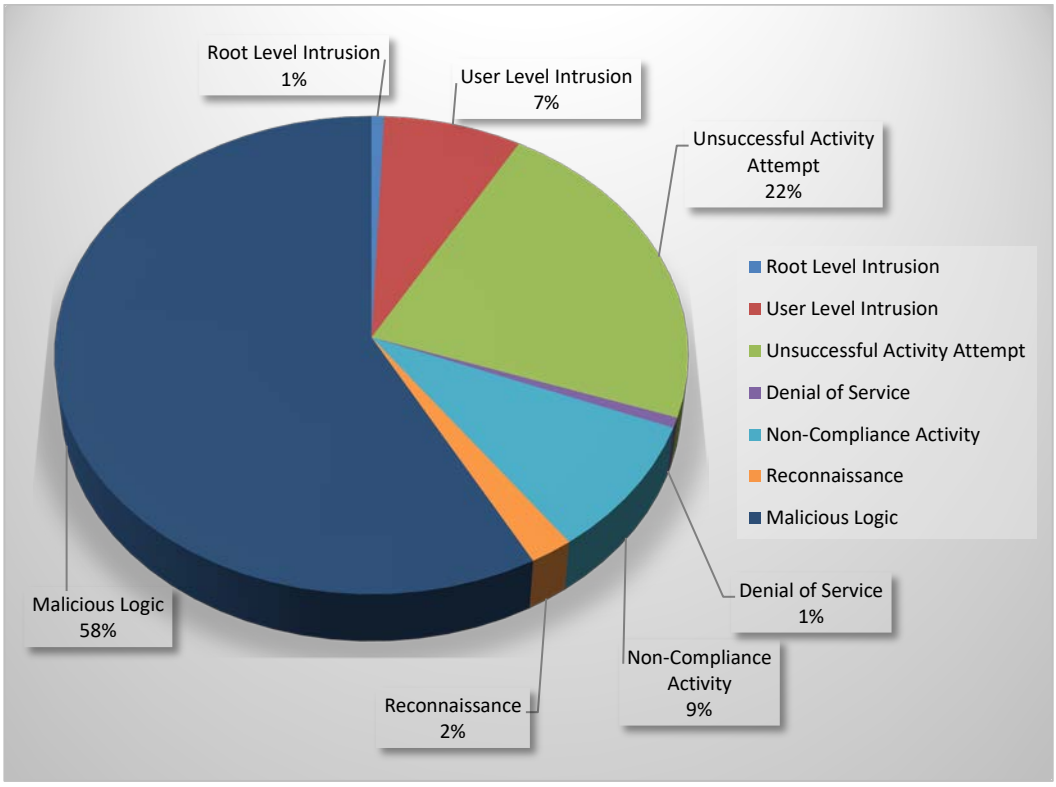


Figure 1

Types of Attack	Count
Root Level Intrusion	142
User Level Intrusion	450
Unsuccessful Activity Attempt	94
Denial of Service	16
Non-Compliance Activity	428
Reconnaissance	198
Malicious Logic	815

Table 1

3. BruCERT Activities in 2017

3.1 Seminars/Conferences/Meetings/Visits

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

- On 6th November 2017 until 9th November 2017 - Two BruCERT delegates attended the OIC-CERT AGM and Annual Conference 2017 which takes place at Baku, Azerbaijan, hosted by Azerbaijan Government CERT.
- On 12th November 2017 until 15th November 2017 - Two BruCERT delegates attended the APCERT AGM and Annual Conference 2017 which takes place at Royal Park Hotel, New Delhi, India, hosted by CERT-IN.

3.2 Awareness Activities

At the start of the year, the Secure Verify Connect campaign highlighted cases of real cyber-crimes – both on our radio show and in our social media. Topics covered included cyber bullying, sextortion, romance scam, online defamation and "booksis" scam.

In April and May, BruCERT focused on bringing awareness to ransomware, and coincidentally the Wannacry ransomware attack happened in May. Topics covered were: Ransomware, downloading ransomware, ransomware phone call, and ransomware prevention. These topics were communicated through our various channels simultaneously: social media, radio, cinema and TV.

In June, BruCERT chose topics that would be relevant to the current Fasting/Hari Raya festive season: unverified messages, online shopping and personal details. These topics were communicated through radio and social media. On 27 June, BruCERT posted an advisory on Petya ransomware on our social media.

In July, continued with the previous month's theme of topics related to Hari Raya festive season – exposing your location, data backup, and personal details. These topics were communicated through radio and social media. In early July BruCERT also released an advisory video on Wannacry & Petya ransomware on RTB. It was aired for 2 weeks with the aim of reaching civil servants.

From August to October, our radio show and social media highlighted cases of real cyber-crimes. BruCERT also highlighted 'Bad Rabbit' ransomware. In November and December, in light of the end of year travel season, BruCERT's rerunning topics related to travel.

Awareness videos

This year, BruCERT released 2 new awareness videos:

- Don't let ransomware hold you hostage
- If your kids can't turn to you, they might turn to someone else online

BruCERT awareness videos are distributed through television (during the local nightly news on RTB), cinema advertising, social media and YouTube.

Awareness website

BruCERT's public awareness website www.secureverifyconnect.info garners an average of 5,200 visits per month. BruCERT plan on refreshing the website in 2018, with a new look and layout.

Events

- **World Backup Day**

March 31, 2017

BruCERT ran a short campaign on social media in support of World Backup Day to bring awareness to the importance of backing up important data. The posts included:

- What is Backup?
- Why backup?
- How should I backup?
- Take the pledge

- **SANS public presentation "One Click Is All It Takes To Bring Down An Organization"**

July 17, 2017

ITPSS hosted a public presentation by Bryce Galbraith of SANS Institute. The event was held at The Core, UBD with 129 people from the public and private sectors. Galbraith also demonstrated examples of spear-phishing techniques and explored ways to fight Advanced Persistent Threats (APT).

- **Cyber Battle: Capture The Flag 2017**

September 3 & 10, 2017

This was the third time ITPSS organized the annual competition. This year, Cyber Battle was supported by Universiti Teknologi Brunei (UTB) as part of their Science and

Technology Week. The qualifying round was held online on 3 Sept, while the final round was hosted at UTB on 10 Sept. The winners of the competition were alert(1), NZN and huroom. The prize presentation was held on the 12 Sept with the Minister of Education, YB Pehin Orang Kaya Indera Pahlawan Dato Seri Setia Awang Haji Suyoi bin Haji Osman as Guest of Honour.

- **GDG DevFest 2017**

November 10, 2017

ITPSS was given 2 slots for speaking at Google Developer Group DevFest 2017. For the first presentation, BruCERT staff presented 'Let's Talk Application Security' which covers how to make applications secure, and avoid exploitations from hackers' perspective. The second presentation was by BruCERT Digital forensic team, explaining various exploitation methods used to steal and spy using Android device.

4. Conclusion

In 2017, BruCERT with the help with its new security intelligence sensor have a better view of how the IT security posture in Brunei Darussalam. The threats are mostly malware related activity such as generic malware, malware infection, malicious bot and IRC Bot. Automatic propagation via open vulnerable services or network shares is also possible which is why it is critically important to enforce strong, secure passwords and to always keep hosts on the network up to date with patches for their OS, browser, and other applications. Users need to be educated or be made aware on how malware can arrive in their systems. Simply clicking on a malicious URL found in an email, web page, or instant message will open the browser to a web page that can automatically install the malware on his system if the browser is vulnerable. Hackers/ attackers typically use social engineering to entice, intimidate, or otherwise trick the victim into running malicious code or clicking on a URL

Even though incidents reported to BruCERT are still far less comparing to other countries but this improvement gives a positive outcome where BruCERT will actively continue to improve its services as a national and government CERT. Hopefully with the ongoing and upcoming initiative such as BruCERT road shows, security awareness to schools and publication of security awareness magazine will better educate the people the importance of Information security and online safety.

BtCIRT

Bhutan Computer Incident Response Team – Bhutan

1. Highlights of 2017

1.1 Summary of major activities

In 2017 BtCIRT has conducted security workshops, published articles and alerts on latest cyber trends, threats, vulnerabilities and best practices. BtCIRT also conducted security awareness program targeting end users, developed security baseline and conducted organisational security assessment of some of the organisations.

1.2 Achievements & milestones:

- BtCIRT has conducted end user cyber security awareness covering all 20 district government offices.
- BtCIRT has conducted Security Assessment for Government Data Centre(GDC) and some other critical infrastructures.
- Developed Security Baseline and conducted Information and Network security workshops involving system owners from various critical organisations.
- BtCIRT has placed sensors at GDC to monitor for threats and vulnerabilities since most of the critical system are hosted there.

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 Communication. BtCIRT's mission is to enhance cyber security in Bhutan by enabling cyber security information coordination and by establishing computer security incident handling capabilities within the country. It is also mandated to proactively monitor government systems for attacks and vulnerabilities.

2.2 Establishment

The BtCIRT's mandate has been approved by the Lhengye Zhungtshog/Cabinet vide Government order number C-2/104/310 dated 20th May 2016. However, the team has commenced its operation a month before i.e April 2016.

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 is extended to national level.

3. Activities & Operations

3.1 Scope and definitions:

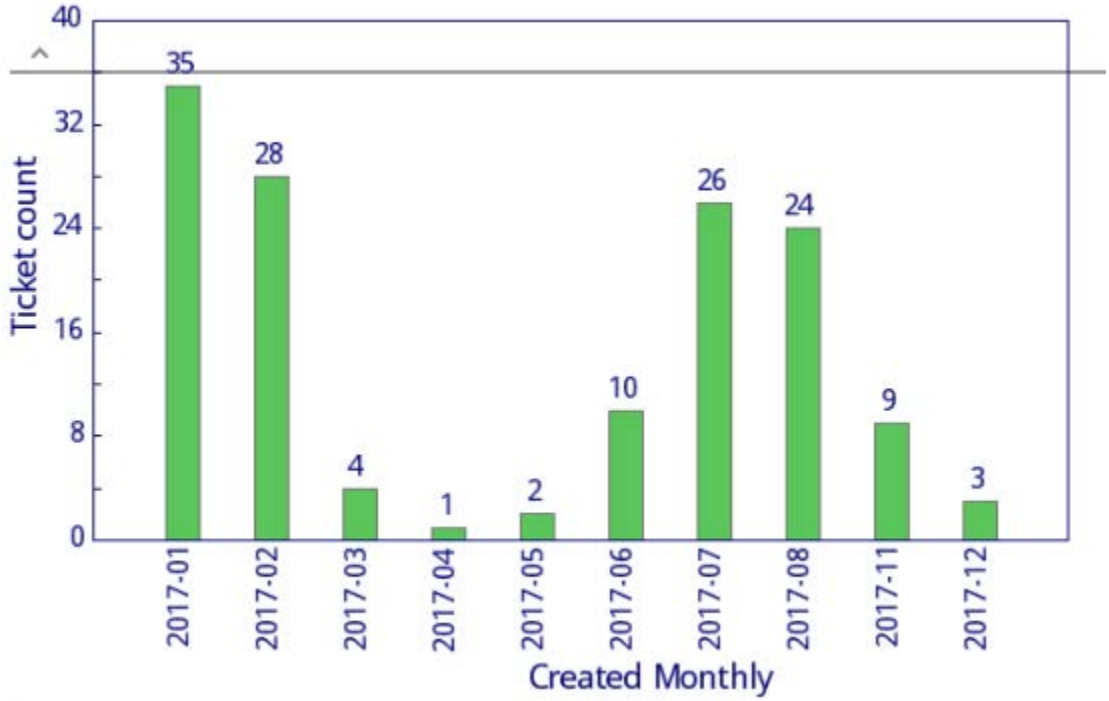
- BtCIRT is mandated to act as central trusted point of national contact in relation to cyber security issues.
- BtCIRT conducts end user awareness at national level and disseminates information on latest threats and vulnerabilities and conducts security workshops related to various cyber security domains.
- BtCIRT actively monitors system hosted in Government Data Centre(GDC) for attacks and vulnerabilities and provides timely report to 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.
- It represents the country in international organisations and forums.

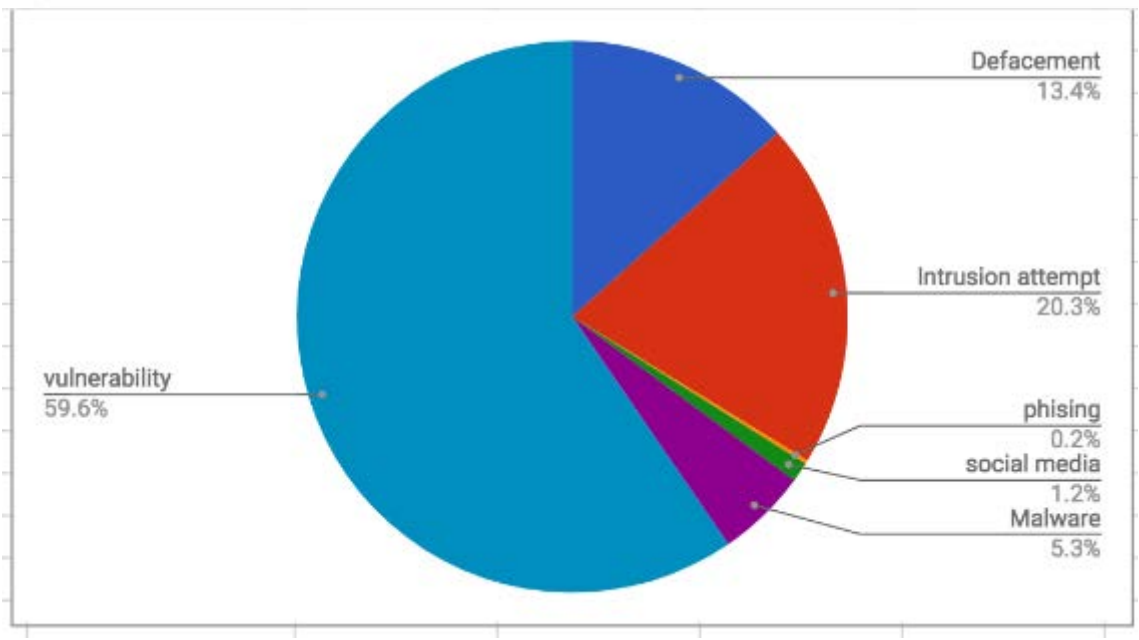
3.2 Incident handling reports:

In 2017 BtCIRT handled 139 incidents of which only 10% was reported by constituents.

3.2.1 General Incident handling statistics:

Following statistics includes Incidents handled monthly and the pie chart represents types of incident handled.

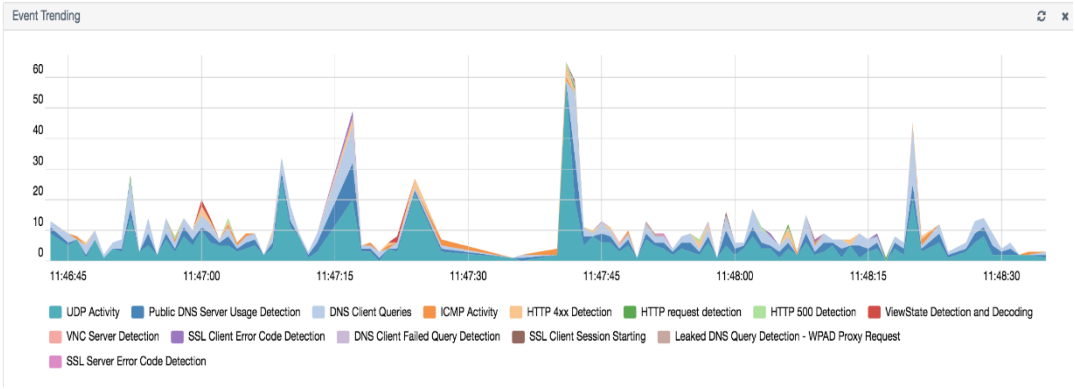




3.2.2 Services to GDC (Government Data Centre)

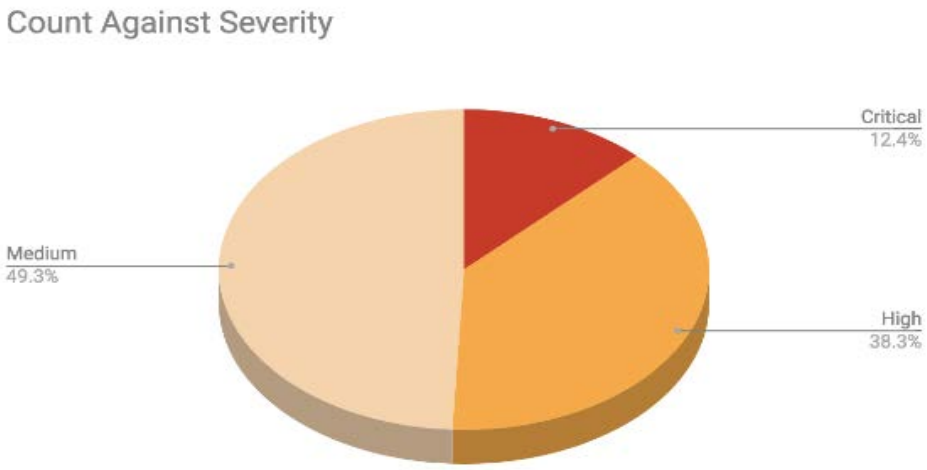
BtCIRT actively monitors Government Data Centre for threats and vulnerabilities in both systems and network and informs GDC team if any issues detected.

Monitor system activity for unusual pattern



Monitor for Vulnerability and attack pattern:

Vulnerabilities are categorized into “Critical”, “Medium”, “High” and “Low” based on how adverse the impact would be if the vulnerability is exploited. Vulnerability of either Critical, high or medium severity were detected in 42 vulnerable systems.

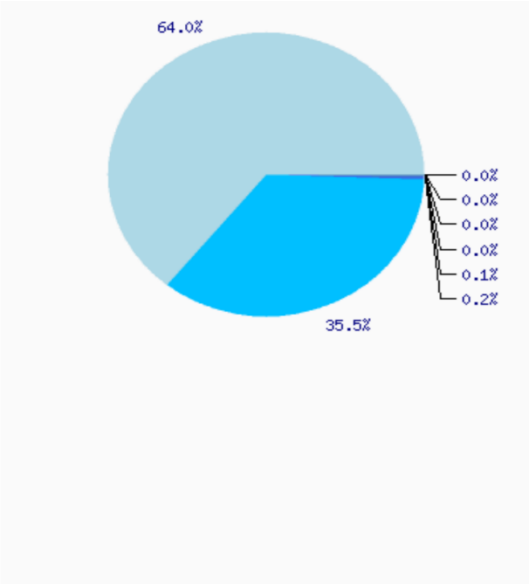


Top Ten critical Vulnerabilities

☐	CRITICAL	PHP < 7.1.0 Multiple Vulnerabilities	Web Servers	13
☐	CRITICAL	OpenSSL 1.0.1 < 1.0.1o / 1.0.2 < 1.0.2c ASN.1 Encoder Negative Zero Value Handling RCE	Web Servers	6
☐	CRITICAL	OpenSSL 1.0.1 < 1.0.1s / 1.0.2 < 1.0.2g RCE	Web Servers	6
☐	CRITICAL	PHP 5.4.x < 5.4.30 / 5.5.x < 5.5.14 Multiple Vulnerabilities	Web Servers	5
☐	CRITICAL	PHP 5.4.x < 5.4.38 / 5.5.x < 5.5.22 / 5.6.x < 5.6.6 Multiple Vulnerabilities (GHOST)	Web Servers	5
☐	CRITICAL	PHP 5.4.x < 5.4.43 / 5.5.x < 5.5.27 / 5.6.x < 5.6.11 Multiple Vulnerabilities (BACKRONYM)	Web Servers	5
☐	CRITICAL	PHP 5.4.x < 5.4.45 / 5.5.x < 5.5.29 / 5.6.x < 5.6.13 Multiple Vulnerabilities	Web Servers	5
☐	CRITICAL	Apache Tomcat 6.0.x < 6.0.45 / 7.0.x < 7.0.68 / 8.0.x < 8.0.32 Multiple Vulnerabilities	Web Servers	3
☐	CRITICAL	Oracle Java SE 6 < Update 115 / 7 < Update 101 / 8 < Update 92 Multiple Vulnerabilities	Web Clients	3
☐	CRITICAL	Oracle Java SE 6 < Update 141 / 7 < Update 131 / 8 < Update 121 Multiple Vulnerabilities	Web Clients	3

Top attacks types

Alarm	Occurrences
Delivery & Attack — Bruteforce Authentication — SSH	4.103
Delivery & Attack — Bruteforce Authentication — Linux/Unix	2.278
Reconnaissance & Probing — Service discovery — Microsoft Remote Desktop	16
Delivery & Attack — Bruteforce Authentication — Microsoft Remote Desktop	6
Reconnaissance & Probing — Service discovery — VNC	2
Reconnaissance & Probing — Service discovery — SSH	1
Delivery & Attack — WebServer Attack - SQL Injection — Attack Pattern Detection	1
Exploitation & Installation — WebServer Attack — XSS	1



3.3 Publications

3.3.1 Security Advisory and Alerts

BtCIRT provides updates on latest threats and vulnerabilities and provides advisories on known threats and best practices via its website, facebook page and email to government system administrations. Users can also subscribe to receive any Alerts or Articles on to their inbox.

4. Events organized / hosted

4.1 Training/Workshops, Drills & exercises

- BtCIRT has conducted 2 Security Workshops in Information and Security related domain with support from Sri Lanka CERT | CC, APNIC and Asi@Connect.
- BtCIRT has also conducted Security Mock drill involving system owners and critical infrastructure operators.
- BtCIRT has also carried out end user security awareness program covering all 20 district government offices.

5. International Collaboration

5.1 International partnerships and agreements

BtCIRT is a member of only 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:

- AusCERT Annual Conference, 23rd- 26th May, 2017, Gold Coast, Australia
- 8th APT Cybersecurity Forum (CSF-8), 24-26 October 2017, Dhaka, Bangladesh

6. Future Plans

6.1 Future Operation

- BtCIRT is planning to strengthen its vulnerability and threat monitoring system and to conduct awareness programs at schools and colleges.
- We are also looking at enforcing international benchmark like CIS as minimal security requirement for all government systems.
- BtCIRT also looks forward to collaborate with more organisations internally and internationally to strengthen its cooperation.

7. Conclusion:

Year 2017 has been challenging and a learning experience for BtCIRT being the second year of its operation. We look forward to take away mistakes made and improve the services we offer in the year 2018 and strengthen national and international collaboration and cooperation.

CCERT

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

1. About CSIRT

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

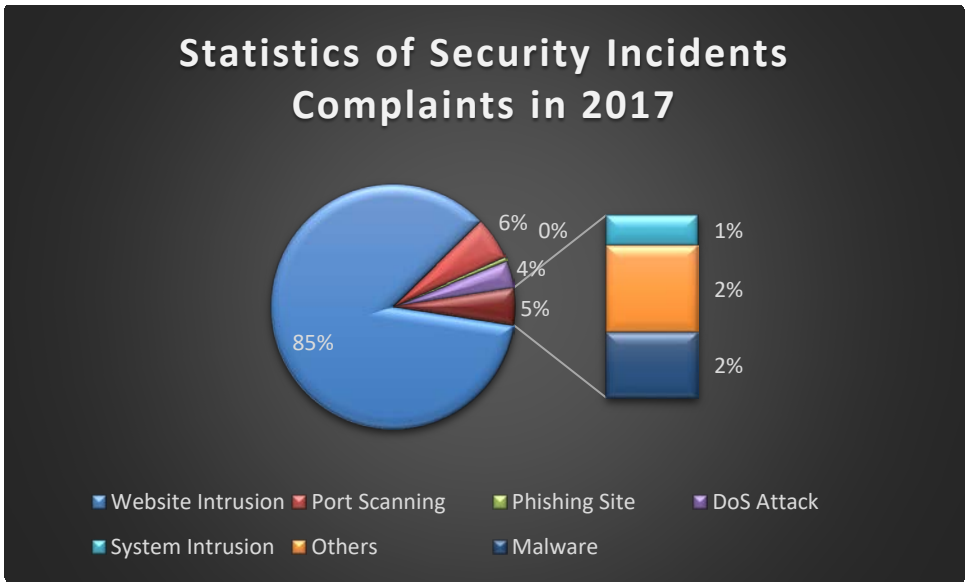
Currently, CCERT mainly deal with security events for CERNET users, which include:

- CERNET Network Monitoring
- Complaint from Other CERT Organizations

- Information Sharing with Other Security Manufacturers

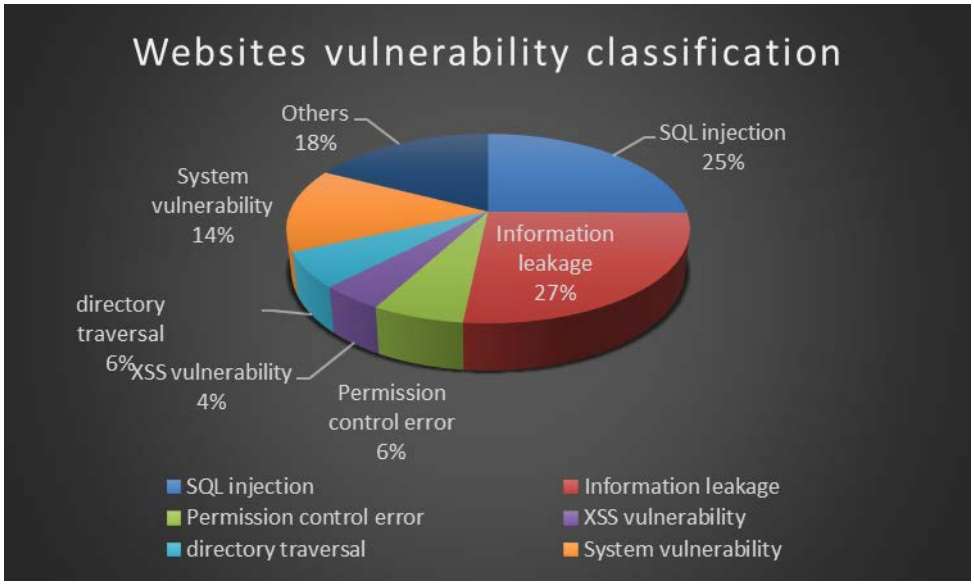
2.2 Incident handling reports

In 2017, CCERT handled 1727 security incident complaints, which include 30 for Malware, 1473 for Website Intrusion, 98 for Port Scanning, 10 for Phishing Site Complaints, 62 for DoS Attack, 14 for System Intrusion and 40 for other network security complaints.



2.3 Abuse statistics

After analyzing the 1473 security events of website attacking, we found all the security vulnerabilities which are used to attack the websites, for more detail please see the following figure:



2.4 Publications

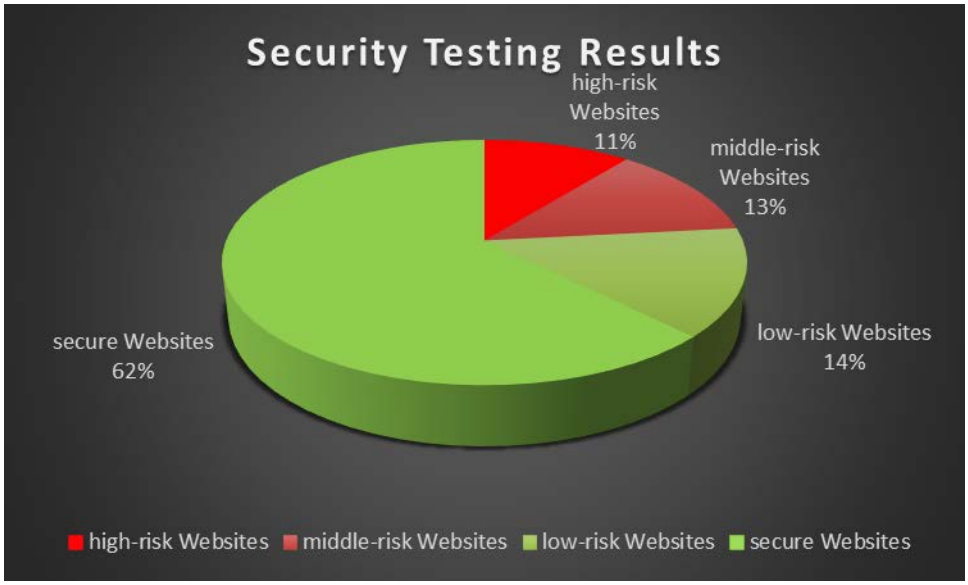
For security bulletins and vulnerability articles published by CCERT, please visit our website https://www.ccert.edu.cn

Published within a specific range :

- Evaluation of the Influence of WannaCry Ransomware on Campus Network
- Work Summary of Comprehensive Management Action of Network Security for China Education and Research Network
- Compendium of Network Security Emergency Response for Education Industry

2.5 Security services

In 2017, CCERT provided security scanning service (free of charge) to 13131 websites, and found that there are about 1416 websites with high-risk vulnerabilities (10.78%), 1647 websites with middle-risk vulnerabilities (12.54%), and 1867 websites with low-risk vulnerabilities (14.22%). No security problems was detected on 8201 websites (62.46%)



3. Events organized / hosted

3.1 Training

Organized 7 trainings, which includes:

- Construction and Positioning of Emergency Response Team
- Sharing of Network and Information Security among Colleges and Universities
- Security Management of Campus Information System
- Governance of Campus Network Security
- Challenges and Countermeasures for Information Security Construction of Colleges and Universities
- Analysis of Big Data and Situation Awareness
- Positioning of Security Services in New Situations

3.2 Conferences and seminars

- Attend the Security Meeting of the Ministry of Education, 8 May, 2017, Qingdao
- Attend the CNCERT Security Annual Meeting, 22 May, 2017, Qingdao
- Attend the Informationization Security Annual Meeting of Colleges and Universities, 9 November 2017, Xiamen
- Attend the 24th annual meeting of CERNET Users, and organize the special forum of classified protection, 22 November, 2017, Jinan

4. Future Plans

4.1 Future projects

- Set up sub-nodes and branch organizations of CCERT relying on the CERNET Hierarchical management organization
- Launch the security monitoring of pure IPv6 protocols in CERNET2

4.2 Future Operation

In 2017, 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 Australia

CERT Australia – Australia

1. Highlights of 2017

1.1 Summary of major activities

Throughout 2017, a key priority and highlight for CERT Australia was working with the APCERT community as Chair of the APCERT Steering Committee. In November 2017, CERT Australia was honoured to be re-elected to the Steering Committee and subsequently as Chair of the Committee for a third term.

1.2 Achievements & milestones

During 2017, the Australian Government continued to implement Australia's *Cyber Security Strategy*. The Strategy included a commitment to increase the capacity of CERT Australia to provide cyber security support to Australian businesses, in particular those providing critical services. The additional capacity is also improving CERT Australia's technical capability to support businesses and to further develop international collaboration.

- A key initiative of the Strategy realised by CERT Australia was the establishment of Joint Cyber Security Centres (JCSC) in Brisbane, Sydney, Melbourne and Perth throughout 2017, with a centre in Adelaide due to be opened in 2018. The JCSC program, managed by CERT Australia, brings together business, academia and government agencies to enhance collaboration on cyber security. The reach of the centres is enhanced by an information sharing portal.

In October 2017, the Australian Government released the *International Cyber Engagement Strategy*. A goal of the Strategy is to achieve a strong and resilient cyber security posture for Australia, the Indo-Pacific and the global community.

- Announced under this Strategy, Australia is working with regional partners in the Pacific to establish the Pacific Cyber Security Operational Network (PaCSON).

2. About CERT Australia

2.1 Introduction

CERT Australia is Australia's national computer emergency response team. It is the national coordination point for the provision of cyber security information and advice for

the Australian community. CERT Australia has a particular focus on Australian private sector organisations identified as Systems of National Interest (SNI) and Critical Infrastructure (CI). It is also the official point of contact in the expanding global community of national CERTs to support more international cooperation on cyber security threats and vulnerabilities.

2.2 Establishment

CERT Australia was formed in 2010 in response to the 2008 Australian Government E-Security Review recommendations that Australia's Computer Emergency Response Team arrangements would benefit from greater coordination.

2.3 Resources

CERT Australia currently employs 82 core staff, a 67% growth from last year. These staffing levels will increase further as CERT Australia develops a 24/7 capability.

2.4 Constituency

CERT Australia seeks to improve cyber security for all Australian internet users by developing information about significant threats and vulnerabilities that may affect Australian systems. CERT Australia is the cyber security coordination point between the Australian Government and the Australian organisations identified as SNI or CI owners and operators.

3. Activities & Operations

3.1 Scope and definitions

CERT Australia undertakes a range of cyber security activities including:

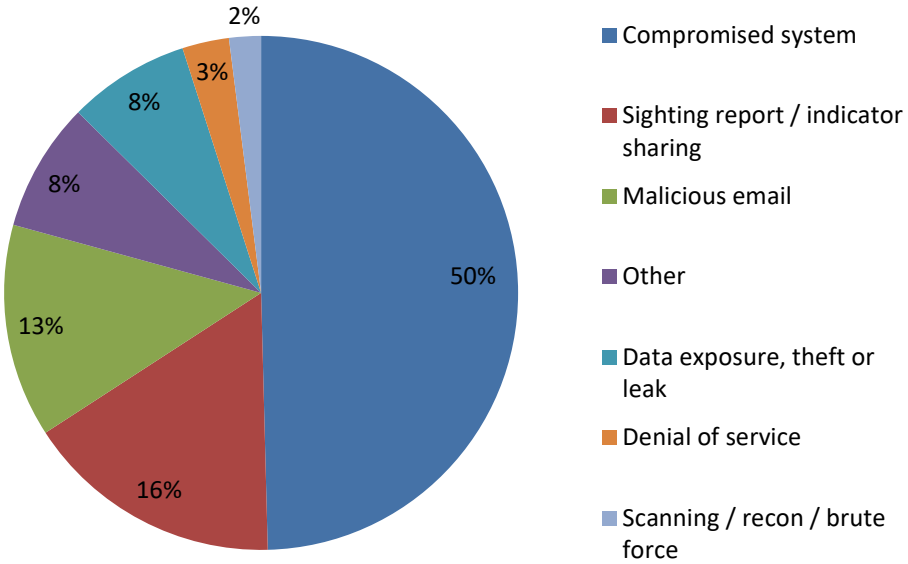
- providing Australians with access to information on cyber threats, vulnerabilities in their systems and information on how to better protect themselves
- promoting greater shared understanding between government and business of the nature and scale of cyber security threats and vulnerabilities within Australia's private sector networks and how these can be mitigated
- providing targeted advice and assistance to enable SNI and CI owners and operators to defend their systems from sophisticated electronic attacks, working in close collaboration with intelligence and law enforcement agencies, via the Australian Cyber Security Centre (ACSC), and

- providing a single Australian point of contact in the expanding global community of national CERTs to support more effective international cooperation.

3.2 Incident handling reports

In 2017, CERT Australia's automated reporting sources identified significantly less incidents. The majority of automated reporting is based on compromised Australian infrastructure (predominantly public-facing websites), details of which are provided to CERT Australia by trusted third parties. These incidents are typically handled in an automated manner through the delivery of an email notification to the owner of the compromised system. The number of these types of incidents has been steadily declining over the past few years, and last year was 4395 down from 10481 in 2016. However, the number of incidents handled directly by CERT Australia incident responders continues to rise, growing from 779 in 2016 to 859 in 2017, an increase of 10%. This means CERT Australia's total number of incidents for 2017 was 5254. Of the 859 incidents manually handled by CERT Australia staff, 342 related to critical infrastructure and major businesses. The chart below gives a breakdown of the incident types for the 859 manually handled incidents.

Figure 1: Incidents by Type, 2017



In addition, CERT Australia led the ACSC's operational response to WanaCry, channeling public messaging through Australia's Stay Smart Online portal as well as using a range of social media platforms.

3.3 Abuse statistics

The ACSC released its third Threat Report in October 2017. The report provided an insight into incidents and malicious activity reported to and handled by the Centre. This report is available at https://www.acsc.gov.au/publications/ACSC_Threat_Report_2017.pdf.

3.4 Publications

CERT Australia publishes cyber security alerts and advisories via its website, secure portal and direct contact with constituents. These alerts and advisories contain up-to-date information on cyber threats and software vulnerabilities and steps that can be taken to improve computer network and system security.

3.5 New services

CERT Australia established a new 24/7 cyber security global monitoring and outreach capability in late 2017, to become fully operational by mid-2018. This will extend the capacity of the Australian Government's cyber security monitoring and incident response, outreach to potentially affected parties, and provision of 24/7 media and crisis communications.

CERT Australia assumed responsibility for the Australian Internet Security Initiative (AISI) on 1 July 2017. The AISI operates as a public-private partnership where Australian internet providers voluntarily work with CERT Australia to help protect their customers from cyber security threats including malware infections and service vulnerabilities.

4. Events organized / hosted

4.1 Drills & exercises

CERT Australia developed, facilitated and participated in a range of cyber security exercises nationally in 2017, including with both government and industry partners.

4.2 Conferences and seminars

CERT Australia supported the annual ACSC Conference, held in Canberra in March 2017. This conference brought together 1,419 cyber security experts from Australia and overseas to discuss the latest trends, mitigations and advances in cyber security.

5. International Collaboration

5.1 International partnerships and agreements

The Australian International Cyber Engagement Strategy, released in 2017, outlined a number of ways in which Australia will enhance international partnerships. Under the Strategy, CERT Australia will strengthen and expand its network of CERT relationships, especially in the Indo-Pacific; and be a prominent contributor to the APCERT community.

5.2 Capacity building

Australia's International Cyber Engagement Strategy outlines a commitment to assisting partners in the Indo-Pacific develop their capacity to address cyber threats, strengthen cyber security and combat cybercrime through the Cyber Cooperation Program (CCP). The CCP was designed to boost the resources behind Australia's cyber capacity building efforts.

5.2.1 Training

CERT Australia conducted one international cyber security training activity online for the APCERT community.

5.2.2 Drills & exercises

CERT Australia participated in five international cyber security exercises in 2017, including the APCERT Drill.

5.2.3 Seminars & presentations

CERT Australia attended the Asia Pacific Regional Internet Conference on Operational Technologies (APRICOT) in Vietnam in February and chaired the APCERT Conference in India in November.

Throughout 2017, CERT Australia also presented at and/or participated in several other international forums including:

- S4 (SCADA Scientific Security Symposium), January - USA

- RSA Security Conference – USA
- International Cyber Security Conference – Saudi Arabia
- Multilateral Network Security Information Exchange – New Zealand
- Policy and Regulation Forum for the Pacific – Fiji
- International ONE Conference; and European Government CERTs Meeting – The Netherlands
- Pacific Islands Law Officers' Network – Tonga
- FIRST Conference; National CSIRTs Meeting ("Second Conference") and Global Forum for Cyber Expertise – Puerto Rico
- ICS Cyber Security – USA
- Cyber Week Conference – Israel
- Blackhat & DefCon – USA
- US ASEAN Cyber Security Workshop – Singapore
- Geek Week; and Cyber Knowledge Data Sharing Conference – Canada
- Meridian Conference – Norway
- Cyber Offensive and Defensive Exercise Taiwan – Taiwan
- FIRST Technical Consortium – Germany
- Other closed events organised by international government organisations and CERTs

6. Future Plans

6.1 Future projects

The Australian Government announced support for the establishment of the PaCSON, as part of the Government's International Cyber Engagement Strategy. Support for the network is aligned with the Government's commitment to work with regional partners in the Pacific. In April-May 2018 Australia will host the PaCSON's inaugural Annual General Meeting and cyber security workshops in Brisbane. It is anticipated that through this engagement members of the PaCSON will strengthen cyber security together.

6.2 Future Operation

CERT Australia will continue to grow as outlined in the Australian Cyber Security Strategy. With this growth, CERT Australia's focus on international partnerships and collaboration will remain a priority. CERT Australia values its ongoing engagement

with the APCERT community and will remain an active and collaborative member in the future.

7. Conclusion

CERT Australia is in the process of expanding its capacity, significantly increasing operations and its ability to engage internationally. APCERT will continue to be a major focus for CERT Australia.

CERT-In

Indian Computer Emergency Response Team – India

1. Highlights of 2017

1.1 Summary of major activities

- CERT-In under the aegis of Ministry of Electronics & Information Technology hosted the Asia Pacific CERT (APCERT) Annual General Meeting and Conference 2017 during 12-15 November 2017 in New Delhi, India.
- CERT-In was elected as an APCERT Steering Committee Member.
- CERT-In to lead two new working groups across APCERT, namely IoT Security and Secure Digital Payments.
- In the year 2017, CERT-In handled **53081** incidents. The types of incidents handled were Website Intrusion & Malware Propagation, Malicious Code, Phishing, Distributed Denial of Service attacks, Website Defacements and Unauthorized Scanning activities. In addition, **53692** spam incidents were also reported to CERT-In. Remedial measures for handling incidents were suggested and implemented in coordination with relevant stakeholders.
- CERT-In is keeping track on latest cyber threats and vulnerabilities. **19** security alerts, **66** advisories and **191** Vulnerability Notes were issued during the year 2017 including **7** Advisories on the secure use of digital payments channels including DOs and DONTs are issued and circulated among various stakeholders.
- Cyber security awareness sessions were conducted for common users regarding security measures to be taken while using digital payment systems under the Government's TV Awareness Campaign and also a Webcast on Wannacry Threats and Countermeasures was carried out.
- CERT-In published key Roles and Responsibilities of Chief Information Security Officers (CISOs) in Ministries/Departments and Organisations managing ICT operations on Ministry of Electronics & IT website.

1.2 Achievements & milestones

- Botnet Cleaning and Malware Analysis Centre (Cyber Swachhta Kendra - www.cyberswachhtakendra.gov.in) has been established by CERT-In for detection of compromised systems in India and to notify, enable cleaning and securing systems of end users to prevent further malware infections. The centre is working

in a public private partnership model in close coordination and collaboration with Internet Service Providers, academia and Industry. The centre was launched on 21st February 2017. The centre is providing detection of malicious programs and free tools to remove the same for common users.

- Indian Computer Emergency Response Team is carrying out cyber security exercises comprising of table top exercises, crisis management plan mock drills and joint cyber security exercises with organizations from key sectors to enable participating organizations to assess their preparedness in dealing with cyber crisis situations. Total 12 such exercises have been conducted in 2017.
- In 2017, CERT-In has signed two MoUs with United States Computer Emergency Readiness Team (US-CERT), Department of Homeland Security, United States of America and The Bangladesh Government Computer Incident Response Team (BGD e-Gov CIRT), Bangladesh Computer Council of Information and Communication Technology Division, Ministry of Posts, Telecommunication and IT, People's Republic of Bangladesh respectively to enable information sharing and collaboration for incident resolution.

2. About CERT-In

2.1 Introduction

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

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

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

2.2 Establishment

CERT-In has been operational since January, 2004.

2.3 Resources

CERT-In has a team of 70 technical members.

2.4 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 in the nature of Advisories, Security Alerts, Vulnerability Notes, 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 2017 is given in the following table:

Activities	Year 2017
Security Incidents handled	53081
Security Alerts issued	19
Advisories Published	66
Vulnerability Notes Published	191
Trainings Organized	22
Indian Website Defacements tracked	29504

Table 1: CERT-In Activities during year 2017

3.3 Abuse statistics

In the year 2017, CERT-In handled **53081** incidents. The types of incidents handled were Website intrusion & Malware propagation, Malicious Code, Phishing, Distributed

Denial of Service attacks, Website Defacements and Unauthorized Scanning activities.

In addition, **53692** spam incidents were also reported to CERT-In.

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

Security Incidents	2017
Phishing	552
Network Scanning / Probing	9383
Virus/ Malicious Code	9750
Website Defacements	29518
Website Intrusion & Malware Propagation	563
Others	3315
Total	53081

Table 2: Breakup of Security Incidents handled

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

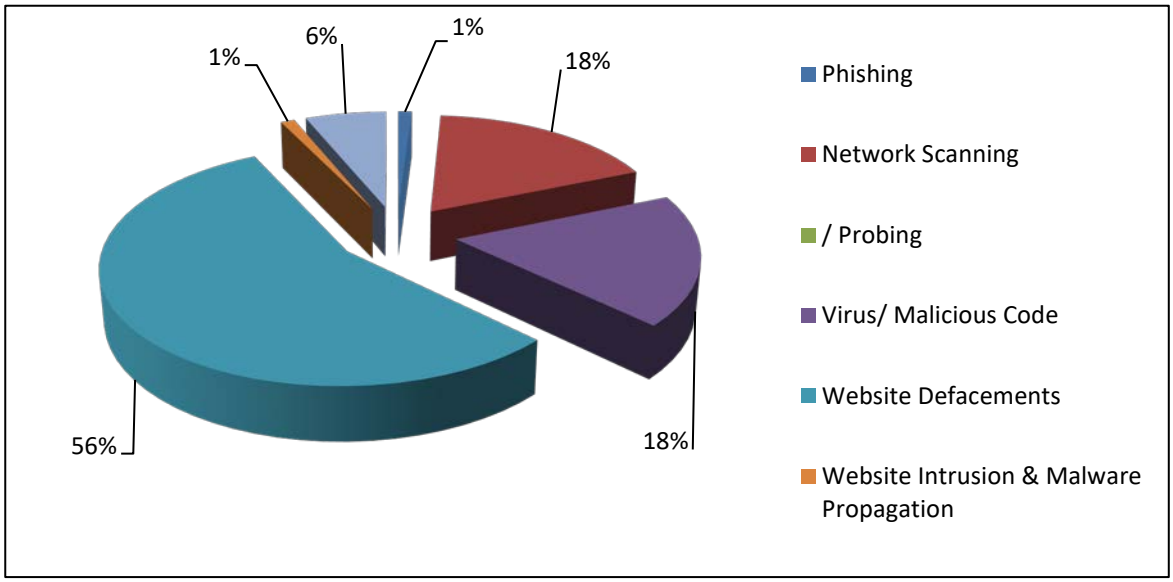


Figure 1: Summary of incidents handled by CERT-In during 2017

3.3.1 Tracking of Indian Website Defacements

CERT-In has been tracking the defacements of Indian websites and suggesting suitable measures to harden the web servers to concerned organizations. A total of **29518** numbers of defacements have been tracked.

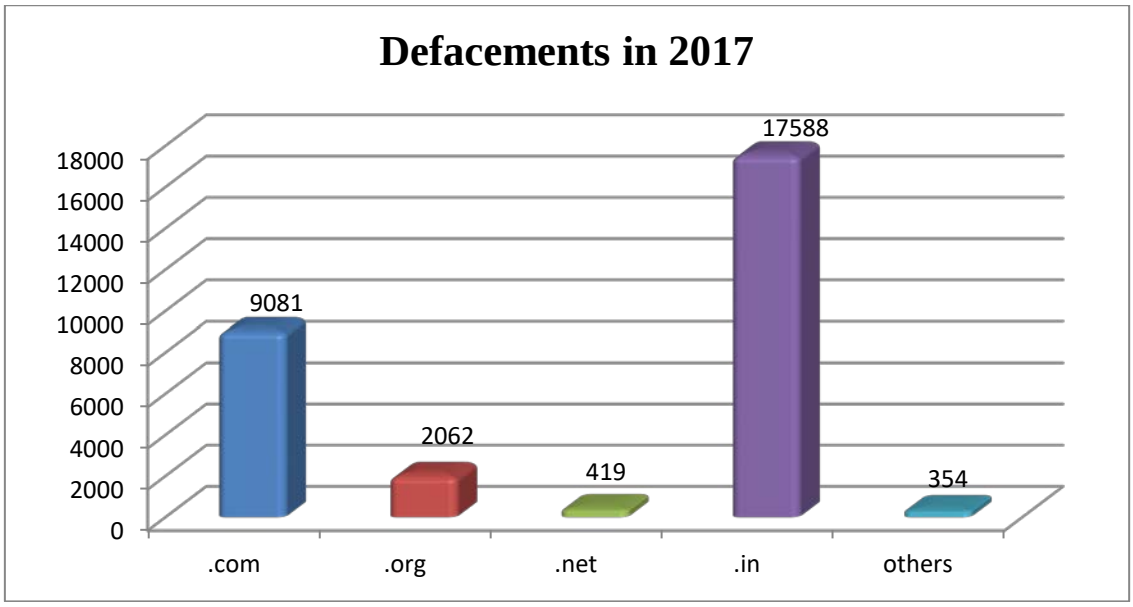


Figure 2: Indian Website Defacements tracked by CERT-In during 2017

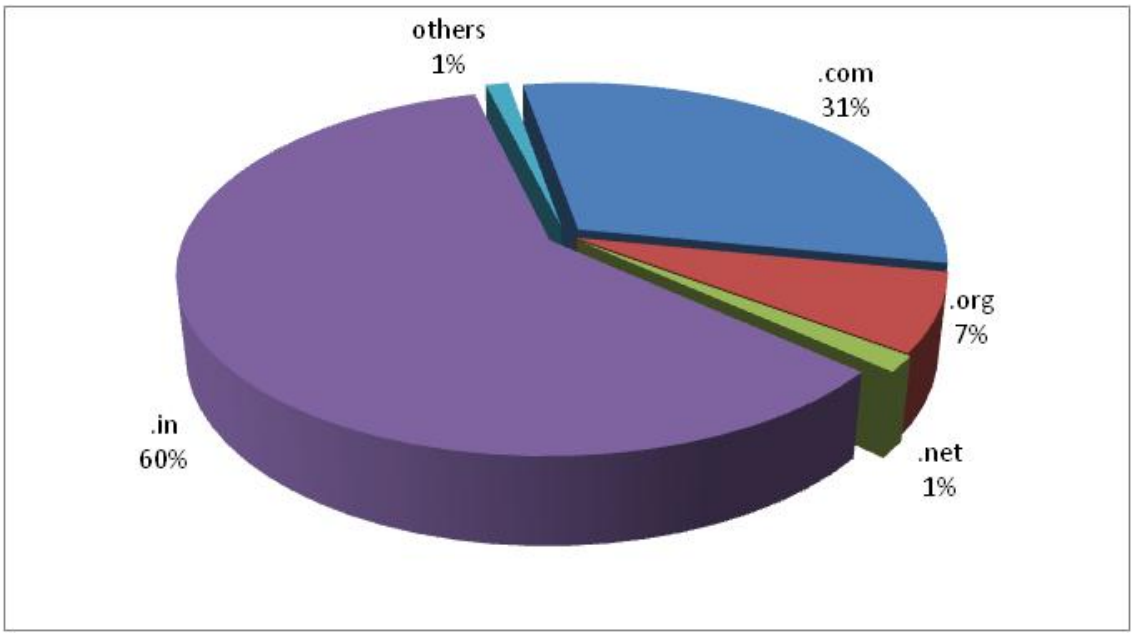


Figure 3: Domain-wise Breakup of Indian Websites Defaced in 2017

3.3.2 Botnet 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 collaboration with Internet Service Providers academia and Industry.

Botnets events processed by Botnet Cleaning and Malware Analysis centre (Cyber Swachhta Kentra) during 2017.

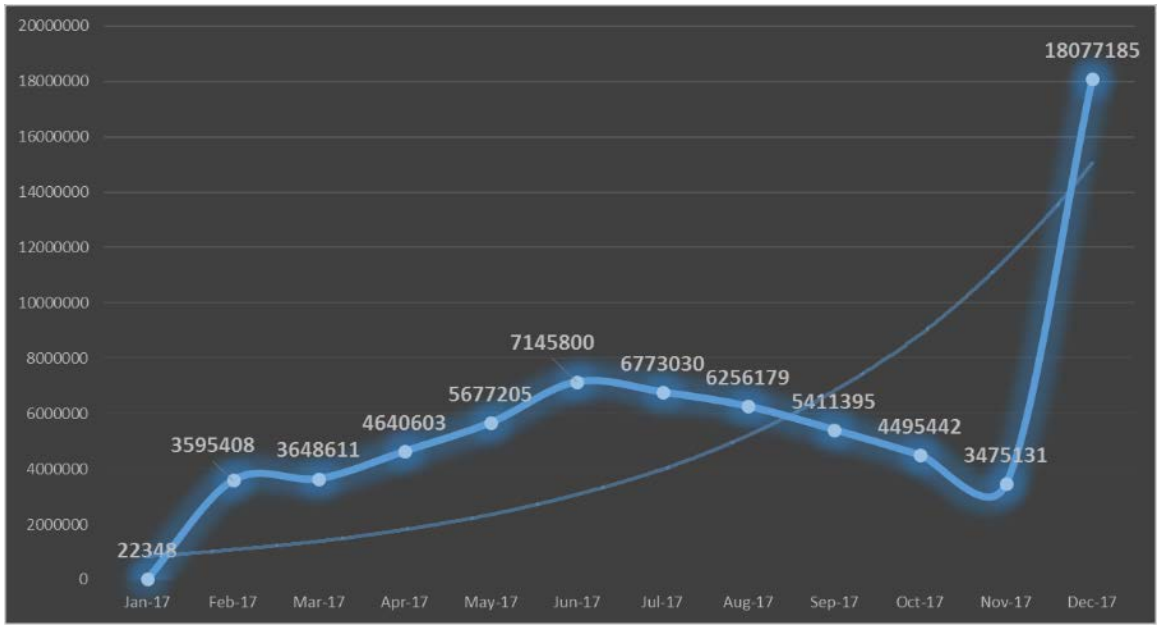


Figure 4: Botnet events tracked by Botnet Cleaning and Malware Analysis Centre

3.3.3 Security Profiling, Assurance framework and Audit Services

- Under Security Assurance Framework, CERT-In has empanelled 67 technical IT security auditors to carry out information security audit, including the vulnerability assessment and penetration test of the networked 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. Services of CERT-In empanelled technical IT security auditors are being used to verify compliance.
- 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 have been conducted.

Services of CERT-In empanelled technical IT security auditors are being used to verify compliance.

- CERT-In has also carried out episodic security audits of key organizations for enhancing their security posture.

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 organisations, 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 2017, CERT-In has conducted 22 trainings on various specialized topics of cyber security. A total of 610 officers including system/Network Administrators, Database Administrators, Application Developers, IT Managers, Chief Information Security Officers (CISOs)/ Chief information officers (CIOs), and IT Security professional have been trained. CERT-In carried out a specific training session only for women IT professionals.

CERT-In has conducted the following training programmes in 2017:

- Workshop on "Cyber Crisis Management Plan" on February 17, 2017
- Workshop on “Embedded Software Safety & Security of National Critical Infrastructure" on February 27, 2017
- Workshop on "Proactive Automated Cloud Security" on February 28, 2017
- Workshop on "Cyber Crisis Management Plan" on March 17, 2017
- Workshop on "Cyber Threats Trends" on March 20, 2017
- Workshop on "Contours of DevOps" on March 23, 2017
- Workshop on "Secure Digital Payments" on March 30, 2017
- Workshop on "Cyber Crisis Management Plan" April 19, 2017
- Workshop on "Endpoint Security & Security of IT Infrastructure" on April 26, 2017
- Workshop on "Cyber Crisis Management Plan" on May 16, 2017
- Workshop on “"Cloud Data Governance & Security" on May 26, 2017
- Workshop on "Cyber Threats and Countermeasures" on May 30, 2017
- ((Exclusively for Women IT Professionals)
- Workshop on "Cyber Crisis Management Plan" on June 22, 2017

- Workshop on "Cyber Security Threats & Mitigations" on July 5, 2017
- Workshop on "Desktop & Mobile Devices Security" on July 11, 2017
- Workshop on "Cloud Security & DDoS Mitigations" on July 13, 2017
- Workshop on "Ransomware & Malware Threats" on July 14, 2017
- Workshop on "Cyber Crisis Management Plan" on August 8, 2017
- Workshop on "Cyber Crisis Management Plan" on August 30, 2017
- Workshop on "Cyber Forensics" on October 11, 2017
- Workshop on "The Hidden Threats & Economics of Cyber Attacks" on October 25, 2017
- Workshop on "Cyber Threats & Cyber Forensics" on November 1, 2017

4.2 Cyber Security Exercises

Cyber security exercises are being conducted by the Government to help the organizations to assess their preparedness to withstand cyber attacks. These exercises have helped tremendously in improving the cyber security posture of the information infrastructure and training of manpower to handle cyber incidents, besides increasing the cyber security awareness among the key sector organizations. CERT-In has conducted 12 exercises in 2017 including 3 joint cyber security exercises conducted with Finance, aviation and shipping sector organizations.

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 utilised 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 organised 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 Understanding (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 2017 CERT-In signed MoUs with United States Computer Emergency Readiness Team (US-CERT), Department of Homeland Security, United States of America and The Bangladesh Government Computer Incident Response Team (BGD e-Gov CIRT), Bangladesh Computer Council of Information and Communication Technology Division, Ministry of Posts, Telecommunication and IT, People's Republic of Bangladesh. 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 participated in APCERT Drill 2017 conducted in March 2017 based on the theme "Emergence of a New DDoS Threat" 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 2017 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 handling incidents of Ransomware.

CERT-In participated in The Organisation of The Islamic Cooperation – Computer Emergency Response Teams (OIC-CERT) drill in September 2017. The theme of the drill was Encountering Cyber Terrorism and Human Trafficking.

5.3 Other international activities

- CERT-In under the aegis of Ministry of Electronics & Information Technology hosted the Asia Pacific CERT (APCERT) Annual General Meeting and Conference 2017 during 12-15 November 2017 in New Delhi India.
- CERT-In participated in the Global Conference on Cyber Space (GCCS) 2017 during 23 – 24 November 2017 in New Delhi.
- CERT-In participated in the FIRST AGM & Conference during 11 – 16 June 2017 at San Juan, Puerto Rico.

6. Future Plans

6.1 Future projects

CERT-In has evolved as the most trusted referral agency in the area of information security in the country. The future plans envisaged are:

- Setting up of mechanisms 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.
- Strengthening of auditor empanelment skill assessment infrastructure.
- Setting up of an automated Threat Information sharing platform.

6.2 Working Groups

- IoT Security Working Group
  - To ensure the secure usage of IoT devices in priority sectors and build trust in secure usage of IoT Ecosystem

- Secure Digital Payments Working Group
  - Build trust in secure usage of digital payments so as to ensure economic 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)

PGP Key Details:

User ID: incident@cert-in.org.in
Key ID: 0x2477855F
Fingerprint: 4A8F 0BA9 61B1 91D8 8708 7E61 42A4 4F23 2477 855F
User ID: info@cert-in.org.in
advisory@cert-in.org.in
Key ID: 0x2D85A787
Fingerprint: D1F0 6048 20A9 56B9 5DAA 02A8 0798 04C3 2D85 A787

CERT NZ

CERT NZ – New Zealand

1. Highlights of 2017

1.1 Summary of major activities

CERT NZ was launched in April 2017, joining New Zealand to the international network of over 100 other CERT-like partner agencies worldwide to get a picture of the cyber threat landscape, both in New Zealand and across the globe. CERT NZ successfully delivered to its establishment functions throughout its first nine months of operation.

1.2 Achievements & milestones

- CERT NZ was launched by the then Communications Minister on 11 April 2017 at a widely attended launch event.
- Its first national cyber security awareness campaign, Cyber Smart Week was run in November 2017 and was well received with wide engagement.
- Its Coordinated Vulnerability Disclosure service was launched allowing coordinated disclosure via the CERT NZ website.
- Produced Quarterly reports for the three quarters CERT NZ was operational, on the threat landscape seen in New Zealand.

2. About CERT NZ

2.1 Introduction

CERT NZ is New Zealand's national computer emergency response team. CERT NZ was set up to improve cyber security in New Zealand, using our broad access to people, information and data to help New Zealand better understand and stay resilient to the threat landscape. It is designed to meet the needs of the whole New Zealand economy; CERT NZ is for all New Zealanders and supports everyday New Zealanders, and all types of businesses and organisations, from small- and medium-sized enterprises through to government agencies and large corporates.

2.2 Establishment

CERT NZ was launched in April 2017 following an announcement in May 2016 that the New Zealand Government would invest in a new organisation to combat cyber security

issue.

2.3 Resources

CERT NZ is a branded business unit within the Ministry of Business, Employment and Innovation. It has 16 FTE, including operations, communications & engagement and governance & reporting staff. CERT NZ also has a contact centre to receive incident reports.

2.4 Constituency

CERT NZ serves all New Zealanders; from individuals and small businesses, all the way through to multi-national organisations and government departments.

3. Activities & Operations

3.1 Scope and definitions

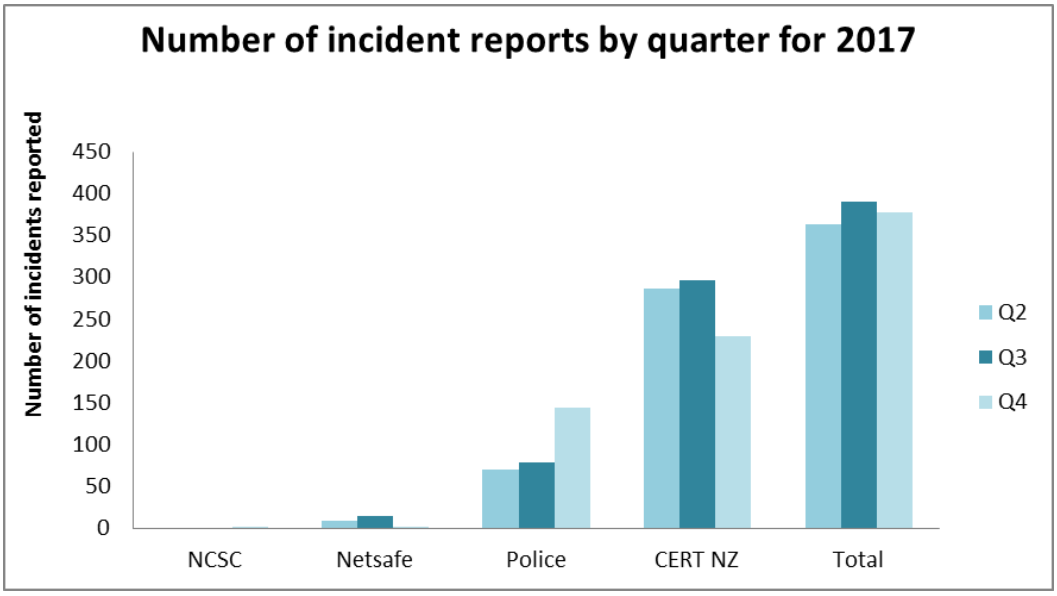
CERT NZ's key services are:

- **Threat identification**: We analyse the international landscape and report on threats.
- **Vulnerability identification**: We analyse data and report on vulnerabilities in New Zealand.
- **Incident reporting**: We triage reported incidents and make referrals.
- **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 help to define the best protections, and raise awareness of cyber security risks, mitigations and impacts.

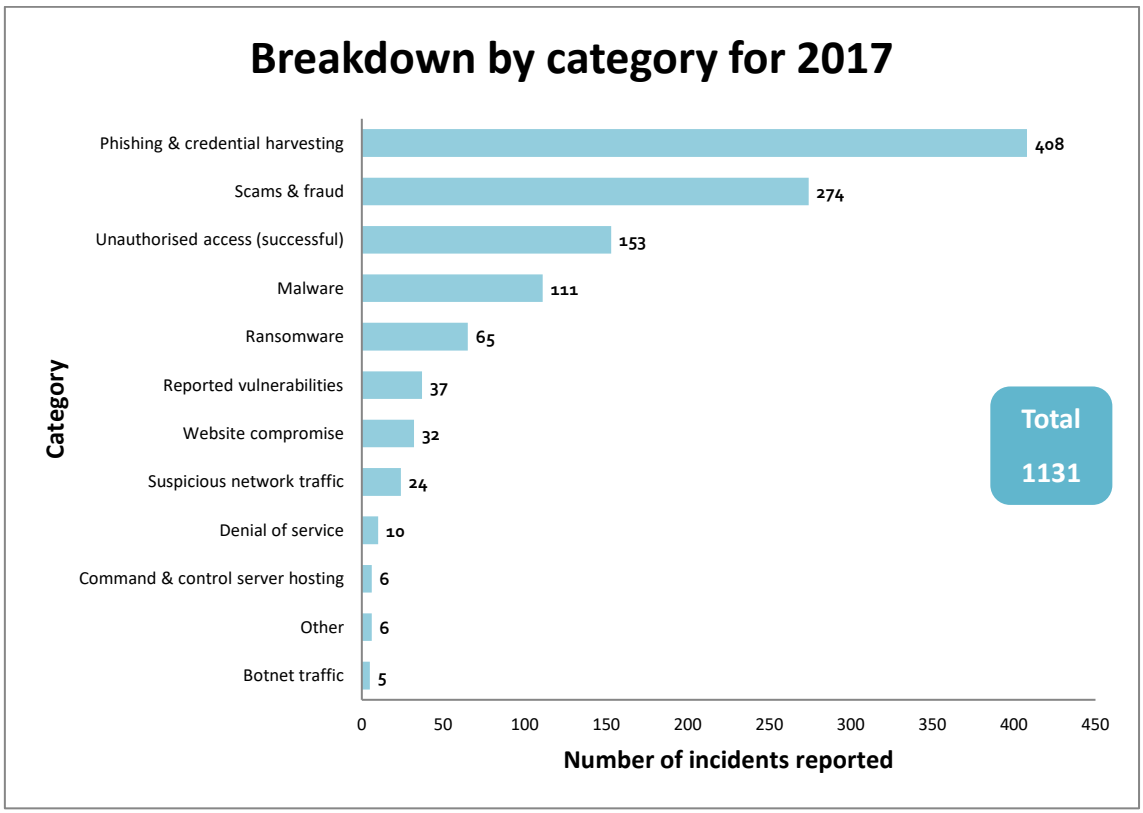
3.2 Incident handling reports

In 2017, CERT NZ received 1131 incident reports through its reporting tool. Of these incident reports, some are referred to partner agencies if it's more appropriate that they investigate it. CERT NZ's partner agencies for referrals[1] are: National Cyber Security Centre (NCSC), Netsafe and NZ Police. The graph below shows the breakdown of incident reports, including referrals, by quarter in 2017 since CERT NZ's launch.

[1] Note the Department of Internal Affairs is also a partner agency of CERT NZ, but not represented in our referrals for 2017.

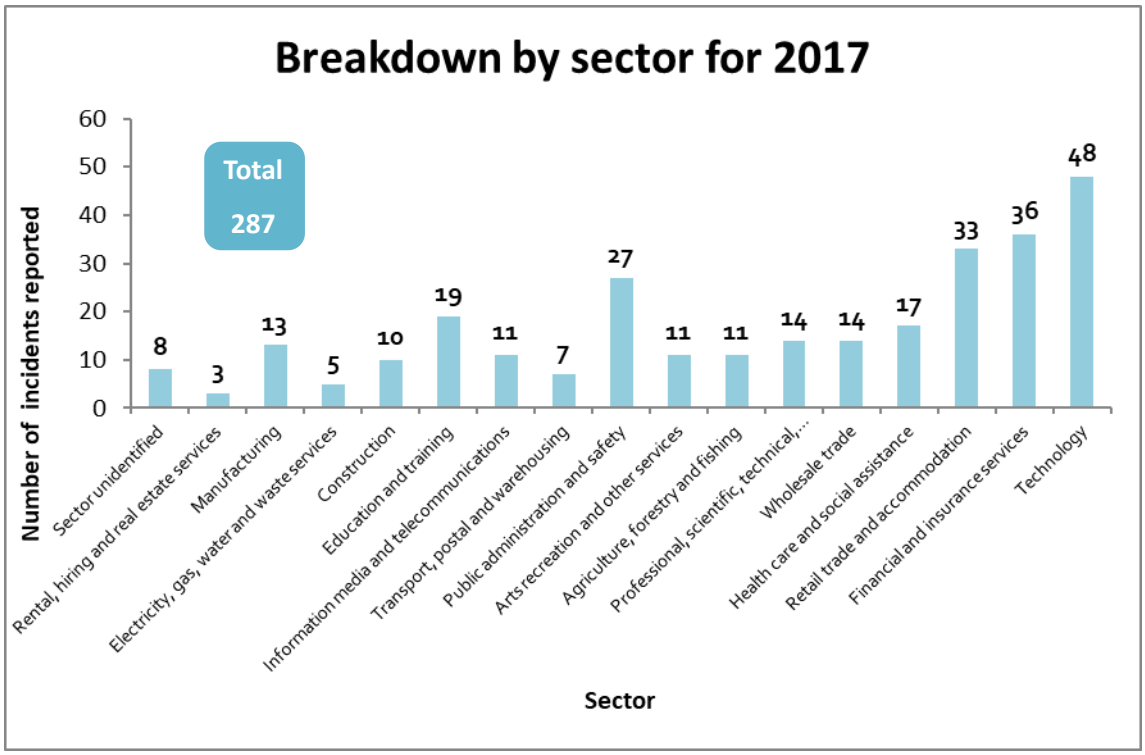


CERT NZ uses categories to record the types of incident reports it receives. The 2017 breakdown by category, including referrals, is presented in the graph below.



From these incident reports, those from organisations and businesses are further broken down by sector[1] in the graph below.

[1] based on Statistics NZ's Standard Industry Output Categories



4. Publications

4.1 Advisories and alerts

CERT NZ publishes two types of public advisories – one for everyday New Zealanders and one for a more technical audience. The former is often used by media and 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 depending on the type of threat, and who the information is targeted at.

Advisories are shared on our website, emailed to subscribers, and shared via social media (Twitter):

- Technical advisories: https://www.cert.govt.nz/it-specialists/advisories/
- Non-technical advisories:

https://www.cert.govt.nz/businesses-and-individuals/recent-threats/

4.2 Quarterly reporting

There is considerable demand for the information CERT NZ has. To meet this demand,

CERT NZ began proactively releasing published reports based on analysis of the incident data received, about the New Zealand threat landscape.

These reports are produced quarterly, and include high level analysis, deep dives into trending issues, case studies and details of the numbers of cases being referred to its partner agencies. This allows others to learn from the incidents reported to CERT NZ, and the information we received from the international CERT community.

By producing high quality & regular content, CERT NZ is meeting its commitment to produce information in an open and transparent way and

Quarterly reports have been well received by the technical community, government agencies and media, as well as lending greater credibility to CERT NZ as we become more established in the New Zealand landscape.

4.3 Quarterly news updates

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

4.4 CERT NZ social media

CERT NZ runs a Twitter account @CERTNZ, and is one of our main channels to share information with New Zealanders.

4.5 CERT NZ Critical Controls

CERT NZ's ten critical controls would mitigate, or better contain, the majority of attacks we've seen, and will be reviewed on an annual basis based on the reports we've received.

4.6 Other publications

CERT NZ has produced a range of resources help keep New Zealanders safe online, such as how to create strong passwords.

5. Events organised / hosted

5.1 Conferences and seminars

CERT NZ ran a successful cyber security awareness campaign, Cyber Smart Week, in November 2017. CERT NZ engaged with partners from across government and the private sector to share cyber security safety messages that gave people the tools to stay safe online.

CERT NZ worked with 64 partner organisations with a combined reach of over 1 million people. CERT NZ created resources that were easily shared, and came with the backing of New Zealand's national authority on cyber security. 100% of participants in the 2017 campaign said they would be likely to participate in future campaign activities.

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).

7. Capacity building

7.1 Training

No formal international training activities were undertaken in 2017.

7.2 Drills & exercises

CERT NZ's focus was on participation in domestic drills & exercises in 2017, and will engage in international exercises in 2018.

7.3 Seminars & presentations

Key presentations in 2017 by CERT NZ are listed below:

- CHCON Christchurch, October 2017.
- B-sides Wellington, November 2017.
- NZ Internet Task Force Conference, November 2017.

8. Future Plans

8.1 CERT NZ will continue to build and expand the delivery of its core services over the next 12 months, and align its work with the updated New Zealand cyber security strategy. Central to its focus is active participation in the international CERT community, to ensure CERT NZ supports the global efforts to improve cyber security.

9. Conclusion

CERT NZ is still very new, but it's growing fast and will continue to deliver and mature in 2018.

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

PGP Key details:

Send PGP encrypted email to: ir@ops.cert.govt.nz

Our PGP fingerprint is: D26F 509F 510D 5618 761D 83FF E2CD 67C3 9AE4 71F2

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 or 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 2002, and became a member of FIRST in Aug the same year. It also took an active part in the establishment of APCERT as a founding member.

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 82990375

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

2. Activities & Operations

2.1 Incident handling

In 2017, CNCERT received a total of about 103.4 thousand incident complaints, a 17.7% decrease from the previous year. And among these incident complaints, 481 were reported by overseas organizations, making a 1.5% rise from the year of 2016. As shown in Figure 2-1, most of the victims were plagued by vulnerabilities (33.9%), phishing (24.3%) and malware (21.8%). Vulnerabilities overtook phishing to be the most complained about category.

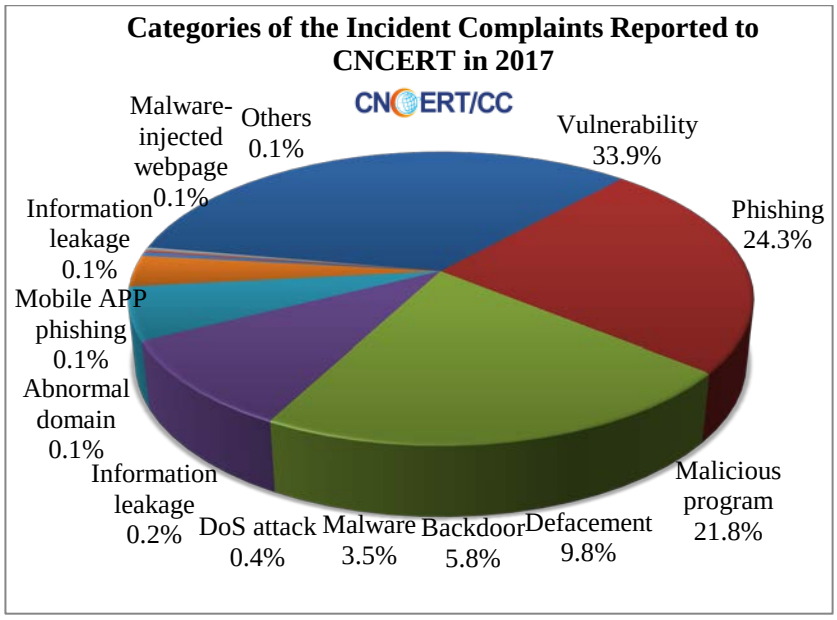


Figure 2-1Categories of the Incident Complaints Reported to CNCERT in 2017

In 2017, CNCERT handled almost 103.6 thousand incidents, a drop of 17.7% compared with that in 2016. As illustrated in Figure 2-2, vulnerabilities (33.9%) dominated the chart about categories of the incidents handled by CNCERT in 2017, followed by phishing (24.3%) and malware (21.7%).

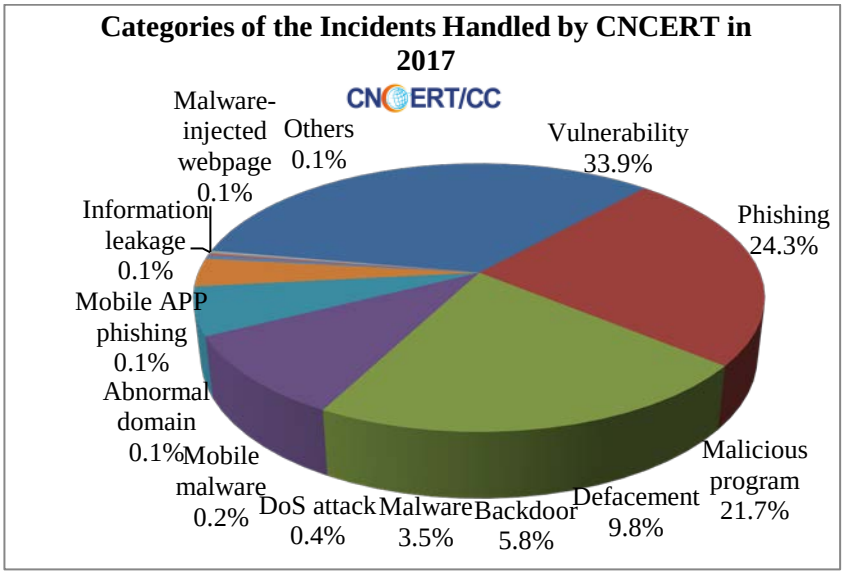


Figure 2-2 Categories of the Incidents Handled by CNCERT in 2017

2.2 Internet Threats

2.2.1 Malware Activities

In mainland China, IPs of the hosts infected with Trojan or Botnet reached about 12.6 million, which decreased by 26.1% compared with that in 2016. We saw more than 47.3 thousand overseas C&C servers which decreased by 1.2% from 2016. 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 and Russia.

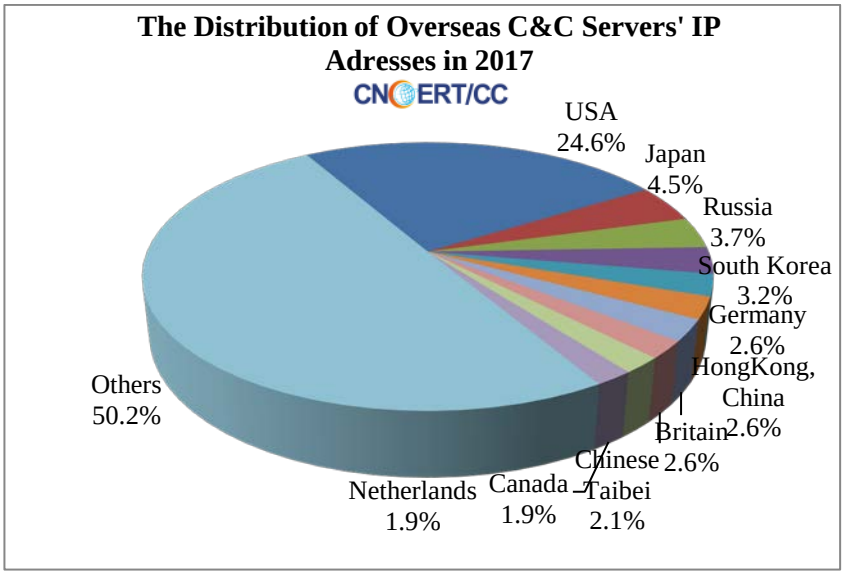


Figure 2-3 Distribution of overseas C&C servers' IP addresses in 2017

By CNCERT's Conficker Sinkhole, over 24.3 million hosts were suspected to be compromised all over the world, among which 3.8 million were located in mainland China. As shown in Figure 2-4, mainland China (15.5%) had the most infection, followed by India (8.3%), and Brazil (5.2%).

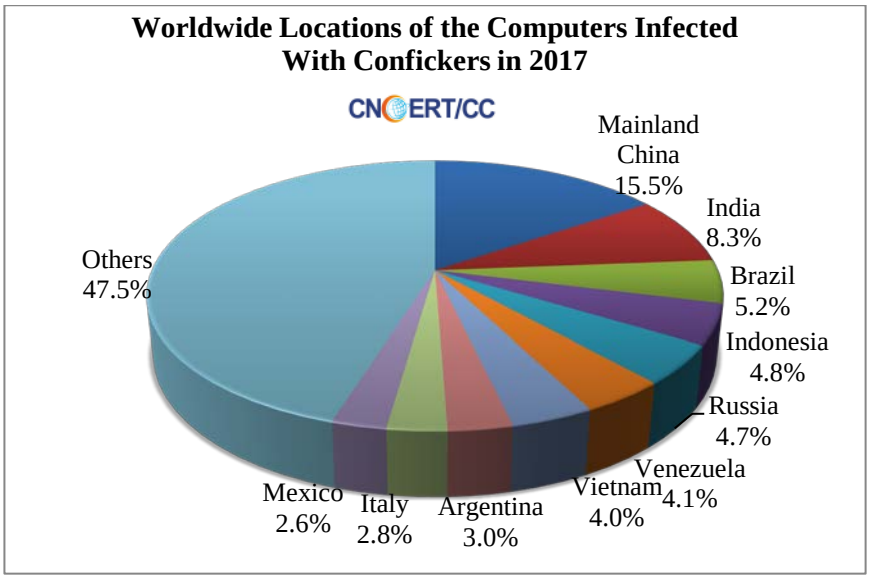


Figure 2-4 Worldwide Locations of the Computers Infected with Conficker in 2017

Malware-hosting websites are the jumping-off places for malware propagation. The malware-hosting websites monitored by CNCERT in 2017 involved about 10.0 thousand domains, 2.7 thousand IP addresses and 79.8 thousand malware download links. Among the 10.0 thousand malicious domains, 49.1% of their TLDs fell into the category of .com. Among the 2.7 thousand malicious IPs, 16.0% were located overseas.

2.3 Website Security

About 20.1 thousand websites in mainland China were defaced, an increase of 20.0% compared with that in 2016, including 618 government sites. Besides, about 29.2 thousand websites in mainland China were detected to be planted with backdoors and secretly controlled, out of which 1,339 were government sites.

In 2017, CNCERT found about 49.5 thousand phishing sites targeting the websites in mainland China. About 5.0 thousand IPs were used to host those fake pages, and 96.4% were out of mainland China. Most of the phishing servers (25.5%) were located in HongKong, China.

CNCERT found almost 21.5 thousand overseas IPs conducting remote control on over

25.5 thousand websites in mainland China. As shown in Figure 2-5, 2,322(10.8%) were located in the U.S., followed with 824 (3.8%) in HongKong, China and 789 (3.7%) in Russia.

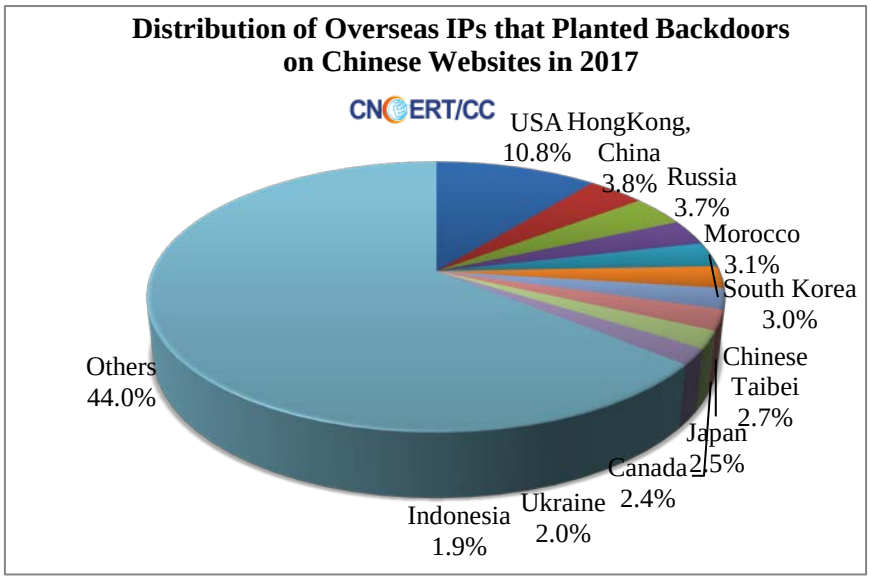


Figure 2-5 Distribution of Overseas IPs that Planted Backdoors on Chinese Websites in 2017

2.4 Mobile threats

In 2017, CNCERT collected about 2.53 million mobile malware samples in total. In terms of the intentions of these mobile malware, rogue behavior took the first place (35.9%), malicious fee deduction (34.3%) secured the second rank, and the next two were those intended for fee consumption and stealing privacy accounting for 10.4% and 7.9% respectively.

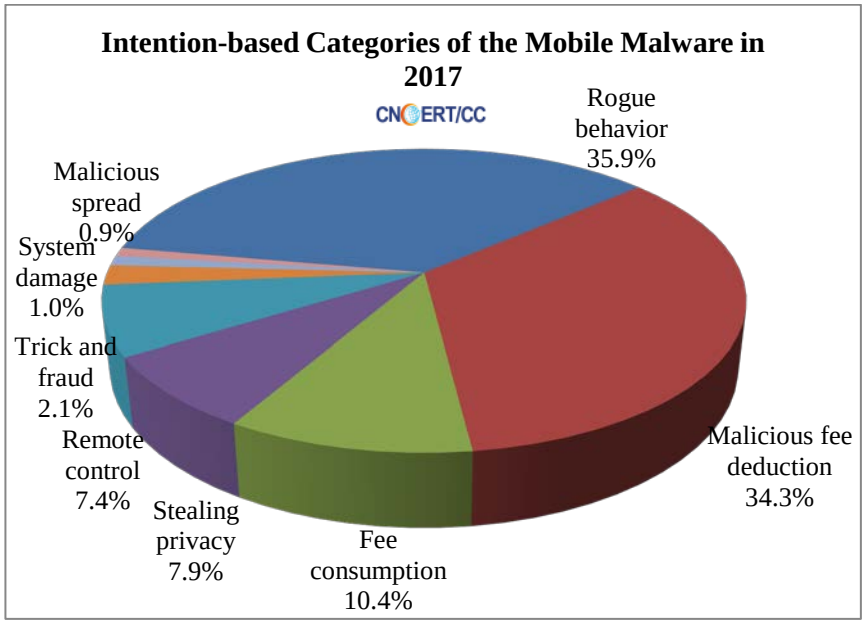


Figure 2-6 Intention-based Categories of the Mobile Malware in 2017

All of these mobile malware identified by CNCERT ran on Android system, recording about 2.53 million (100.0%).

3. Events organized/co-organized

3.1 Conferences

Issuance of "The Review of the 2016 Network Security Situation in China"

CNCERT gave a press conference on the nation's 2016 Network Security Situation in Beijing on 19th April, 2017, introducing the overall picture and highlights of China's network security in 2016. Specialists and representatives from 50 organizations, including government agencies, operation departments of important information systems, telecom operators, domain name registrars, industry associations, Internet companies and security companies, attended this conference. This situation report, which was of distinctive industry characteristics and technical features, outlined the characteristics of China's network security threats in 2016, looked into the potential threats of great concern in 2017 and put forward a number of suggestions.

The 2017 CNCERT Annual Conference in Qingdao, Shandong Province

CNCERT held the 2017 Annual Chinese Conference on Computer and Network Security in Qingdao, Shandong province, from May 22nd to 24th, 2017. The theme of the Conference was "Industry Convergence to Promote Development, Mutual Collaboration to Build Security". Sub-Forums had been set up according to 5 subjects:

Emergency Response, IoT Security, Cybersecurity Artisan, Incident Tracking and International Forum. More than 1,000 representatives from governments, important information systems departments, industries and enterprises, universities, research institutes and other organizations attended the meeting.

The 2nd CNCERT International Cooperation Forum & FIRST Technical Colloquium in Qingdao, Shandong Province

On May 22nd, 2017, the 2nd CNCERT International Cooperation Forum & FIRST Technical Colloquium was held in Qingdao, Shandong province with nearly 200 attendees. The representatives were from government departments for telecom affairs, cybersecurity emergency response organizations and Internet companies in 15 countries and regions, such as Australia, Russia, Korea, Japan, India, Germany and Brazil. This Forum, by inviting both CNCERT international partners and FIRST members, has provided CNCERT, its international partners and cybersecurity enterprises with a profound exchange platform for cybersecurity emergency response affairs to further build trust, promote mutual learning and facilitate comprehensive cybersecurity cooperation.

This one-day event started with CNCERT introducing the implementation and future plan of the Forum, and followed by presentations from FIRST Board member, Ministry of Digital Economy and Society of Thailand, HKCERT, Korea Internet and Security Agency (KISA), (ISC)2, Siemens ProductCERT, CNCERT, Department of Information and Communications Technology (DICT) of the Philippines, Team Cymru, Hebei Unicom, Nanjing Sinovatio Technology and NSFocus on topics of cybersecurity capacity building, cyber crimes, APP security, cybersecurity threats, cybersecurity information sharing, national cybersecurity strategies, financial security, big data threats and cloud security, with best practices and experience being shared among each other.

The China-ASEAN Network Security Emergency Response Capacity Building Seminar in Qingdao, Shandong Province

CNCERT organized the China-ASEAN Network Security Emergency Response Capacity Building Seminar in Qingdao, Shandong province, from May 22nd to 24th, 2017. Delegates from the government departments for telecom affairs and CERTs of Cambodia, Indonesia, Laos, Myanmar, the Philippines, Thailand and Vietnam attended this event. The participants exchanged development, technological and management experience in the field of network security and discussed on how to conduct cooperation

on network security emergency response between China and ASEAN.

4. Drill attended

APCERT Incident Drill 2017

CNCERT participated in the APCERT 2017 Drill as a participant on 22nd March, 2017 and completed it successfully. The theme of the APCERT Drill 2017 was "Emergence of a New DDoS Threat". In this year's drill scenario, the participating teams were tasked to mitigate DDoS incidents triggered by a type of malware which has been widely observed in the Asia Pacific region. This walkthrough is designed to test the participating teams' incident response handling arrangements. 23 CSIRT teams from 18 economies of APCERT took part in the exercise.

ASEAN CERT Incident Drill (ACID) 2017

CNCERT participated in the ASEAN CERT Incident Drill (ACID) 2017 on 11th September and completed it successfully. The theme for ACID 2016 was "The Dangers of Insufficient Authentication and Poor Access Control". According to the scenario, the participants played the "Hacker" and the "Incident Responder" roles. The "Hacker" role was involved in compromising actions and the "Incident Responder" was involved in detection, investigation of various attack and the response procedures.

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 2017

Title	No. of Issues	Description
CNCERT Weekly Reports (Chinese)	53	Emailed to over 400 organizations and individuals and published on CNCERT's Chinese website (http://www.cert.org.cn/)

CNCERT Weekly Reports (English)	53	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)	5	Published on CNCERT's website (http://www.cert.org.cn/)
CNVD Vulnerability Weekly Reports (Chinese)	53	Published on CNCERT's website (http://www.cert.org.cn/)
Articles Analyzing Cybersecurity Threats	36	Published on journals and magazines

EC-CERT

Taiwan E-Commerce Computer Emergency Response Team - Chinese Taipei

1. Highlights of 2017

EC-CERT is committed to supporting and strengthening E-commerce companies' ability to respond to and handle security incidents, and is working with E-commerce Alliances to promote PII and information security activities. EC-CERT has established a basic checklist for E-commerce information security, promoting E-commerce companies to check the completion of security protection and encouraging this industry to strengthen security management.

EC-CERT organizes a seminar inviting hackers to exchange views with CEOs of E-commerce companies face to face. In the past, due to lack of IT professionals and budget, many small scale E-commerce companies couldn't find out security-related loopholes by themselves, by this way, they discussed security breach issue and work out a resolution of the security as well as strengthen transaction security protection.

2. About EC-CERT

2.1 Introduction

EC-CERT stands for "Electronic Commerce - Computer Emergency Response Team", which is supported by Ministry of Economic Affairs of ROC. EC-CERT regularly task composed of information security consulting service and website vulnerability scanning with penetration testing, incident response, issue security information alert, etc., EC-CERT offers services confirmed favor on 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 assistance E-commerce industry enhanced information security, to help deal with information security incidents, avoid being hacked as well as including take promotion of information security and PII protect activities.

2.3 Constituency

EC-CERT aims to enhance E-commerce Company's ability to respond and deal with

security incidents and relative issues. EC-CERT provides security counseling, respectively as E-commerce platforms, logistics providers and service providers, counseling by E-commerce to enhance information security protection in case of external attacks.

3. Activities & Operations

3.1 Scope and definitions

In 2017, EC-CERT planned to come out many E-commerce industry information security reports including web site security online consulting records and step-by-step practical case-solving procedures and recommendations.

3.2 Incident handling reports

EC-CERT provides 32 event visits, handling 27 security incidents, providing 54 security advices, and received 63 computer security incident reports from E-commerce companies.

4. Events organized / hosted

4.1 Conferences and seminars

Information security promotion activities * 2

Participation Asian PKI Union Conference * 3

5. International Collaboration

5.1 Capacity building

5.1.1 Training

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

- Digital Forensics
- Mobile Vulnerability Check and Case Study
- Cyber Detection Eradication and Forensics

5.1.2 Drills & exercises

EC-CERT participated in the APCERT Drill in March 2017. The topic of APCERT online drill is “Emergence of a New DDoS Threat”.

5.2 Other international activities

EC-CERT attended APCERT AGM and Conference 2017 (November, New Delhi, India)

6. Future Plans

EC-CERT aims to create an E-commerce response center 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 fulfill improvement is the key point of EC-CERT in 2018.

7. Conclusion

As long as information technology in progresses, there will always be scams but the key to point is the user awareness and the security management. EC-CERT will continue to work on E-commerce information security in Taiwan.

GovCERT.HK

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

1. Highlights of 2017

1.1 Summary of Major Activities

In 2017, we completed the review of the standing Practice Guide for Information Security Incident Handling with reference to the ISO 27000 standards and promulgated for reference by all our constituents. We also co-organised with the Hong Kong Police Force (HKPF) to run an inter-departmental cyber security drill and walk through the procedures of security events analysis and incident response with our constituents to enhance the overall capability of the Government of the Hong Kong Special Administrative Region (HKSAR Government) in incident management.

In response to the soaring increase of ransomware outbreak during the first half of 2017, we developed dedicated best practices, thematic leaflets, and defensive guidelines for all government users as well as lined up security solutions providers to share with our constituents the latest cyber resilience technologies and best practices to protect information systems from zero day exploit. We also joined with the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) to promote awareness of ransomware and malware attacks through a dedicated "Fight Ransomware Campaign". The "Ransomware Intelligence Portal" was built on social media to share latest risk information and actionable advice with the general public.

To strengthen our capacity in cyber threat monitoring and assessment, we established a cyber risk information sharing platform to centrally manage cyber threat intelligence and actionable advice for the consumption by our constituents. We have reviewed and enforced a cyber threat assessment framework for reference by both internal and outsourced security practitioners so that aligned actions would be derived when pre-defined conditions were met. We also published security alerts and mitigation advice through the Government Computer Emergency Response Team Hong Kong (GovCERT.HK) web portal for reference by the general public.

In February 2017, we hosted a Collaboration Meeting with Japan Computer Emergency Response Team Coordination Center (JPCERT/CC) and HKCERT and invited JPCERT/CC to run a TSUBAME technical workshop to explore collaboration in threat hunting.

1.2 Achievements and Milestones

Cyber Threat Assessment and Incident Management

GovCERT.HK started to publish Weekly IT Security News Bulletins since January 2017 to highlight security information including vulnerabilities, security patches, malicious activities and security incidents that might have impact to government information systems and Internet-based services.

When needed, GovCERT.HK would issue security alerts as early warnings and request government IT users to take appropriate actions accordingly. For easy interpretation on our security alerts, we have reviewed and published the "Cyber Threat Assessment Framework" as a reference tool used to describe, analyse, assess, rate and prioritise various risks by estimating the probability of occurrence and the severity of impact if they occur. The Framework is as follows.

		Threats		
		Low	Medium	High
		☑ Vulnerability reports received from sources ☑ Malicious activities in the cyberspace identified by SIEM ☑ Malware, phishing, web attack (Injection, XSS, DoS/DDoS) requiring user interactions ☑ Only locally exploitable & Privileged access account required	☑ Alerts of targeted attack against the Government received from sources ☑ DDoS/application attack against individual government website/ system/network reported ☑ Remotely exploitable via network & No user interaction required to launch attack ☑ Privilege access elevation enabled	☑ Global outbreak report received from sources ☑ DDoS/application attacks against multiple government websites/ systems/networks reported ☑ Exploit code publicly available & Exploitation reported/observed ☑ Advanced persistent threat with privilege access elevation
Impacts	High ☑ Result in loss of classified data ☑ Affect public-facing website/ e-service ☑ Attack could spread through internal network ☑ Widely reported by local mass media	Security Alert Line-to-Take	High Threat Security Alert Line-to-Take Call for Actions	High Threat Security Alert Line-to-Take Call for Returns
	Medium ☑ Result in loss of data ☑ Affect internal website/e-service ☑ Attack spreads through Internet ☑ Reported internationally but no local media coverage	Security Alert	Security Alert	High Threat Security Alert Call for Actions
	Low ☑ No service interruption ☑ No data loss ☑ Affect individual user/ internal application system ☑ No media coverage	Vulnerabilities & Security Updates	Security Alert	Security Alert

Liaison and Collaboration

We have been proactively participated in the APCERT's activities and worked closely with the CERT community in handling threat information. We also collaborated closely with HKCERT, CNCERT/CC, MOCERT, and JPCERT/CC in different initiatives and projects.

Cyber Threat Intelligence Management

From time to time, we received various cyber threat intelligence from different sources

and gathered threat information from the public domain. To facilitate efficient and effective correlation of threat information and potential impact to the government information systems, we launched the Cyber Risk Information Sharing Platform (CRisP) in April 2017 as an information hub for use by all our constituents.

Riding on the Platform, we were piloting different big data analytics tools to support data collection, correction, and discovery of uncommon usage patterns. We have been piloting the development of different dashboards to facilitate security analysis and formulation of early warnings. The Platform also facilitates closed group discussion and knowledge sharing.

Awareness Building and Public Education

In view of the rising trend of ransomware attacks in 2017, GovCERT.HK developed thematic leaflets to recommend relevant precautionary measures and security controls for our constituents. For the wider community, we also set up thematic web pages at the "Cyber Security Information Portal" (www.cybersecurity.hk, the CSIP portal) on ransomware and posted detailed steps to protect themselves from and defend against ransomware attacks.

GovCERT.HK also devoted much attention to public education and capacity building in different business sectors and age groups. In 2017, we organised 32 school visits to reach out to around 10 000 students, parents and teachers.

2. About GovCERT.HK

2.1 Introduction

GovCERT.HK is a governmental CERT responsible for coordinating incident response for over 80 departmental Information Security Incident Response Teams (ISIRTs) of the HKSAR 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 Computer Emergency Response Team (CERT) community for timely exchange of cyber threat information and coordinated response. GovCERT.HK also works closely with 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 collaborates with the CERT community globally 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 HKSAR Government.

2.3 Resources

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

2.4 Mission and Constituency

Being the governmental CERT, GovCERT.HK will centrally manage incident response within the HKSAR 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 on potential threats and responding to security events with a view to ensure would be well protected.

3. Activities and Operations

3.1 Scope of Services

GovCERT.HK is the computer emergency response team for the HKSAR 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 2017, GovCERT.HK published the following regular security bulletins to raise the awareness among government users and the general public.

- "Security Vulnerabilities and Patches" information would be consolidated on every working day and disseminated to registered subscribers through emails;

- "Security Industry News" would be gathered on every working day and top news with wide impact would be compiled and disseminated to registered subscribers through emails; and
- "Weekly IT Security News Bulletins" would be published on the working day that starts each week to highlight top 2 to 3 security news during the week and summarises vulnerabilities by products for easy reference by security practitioners. These Bulletins would be distributed to registered subscribers through emails and posted at the GovCERT.HK website as public information (www.govcert.gov.hk/en/reports.html#weekly-reports).

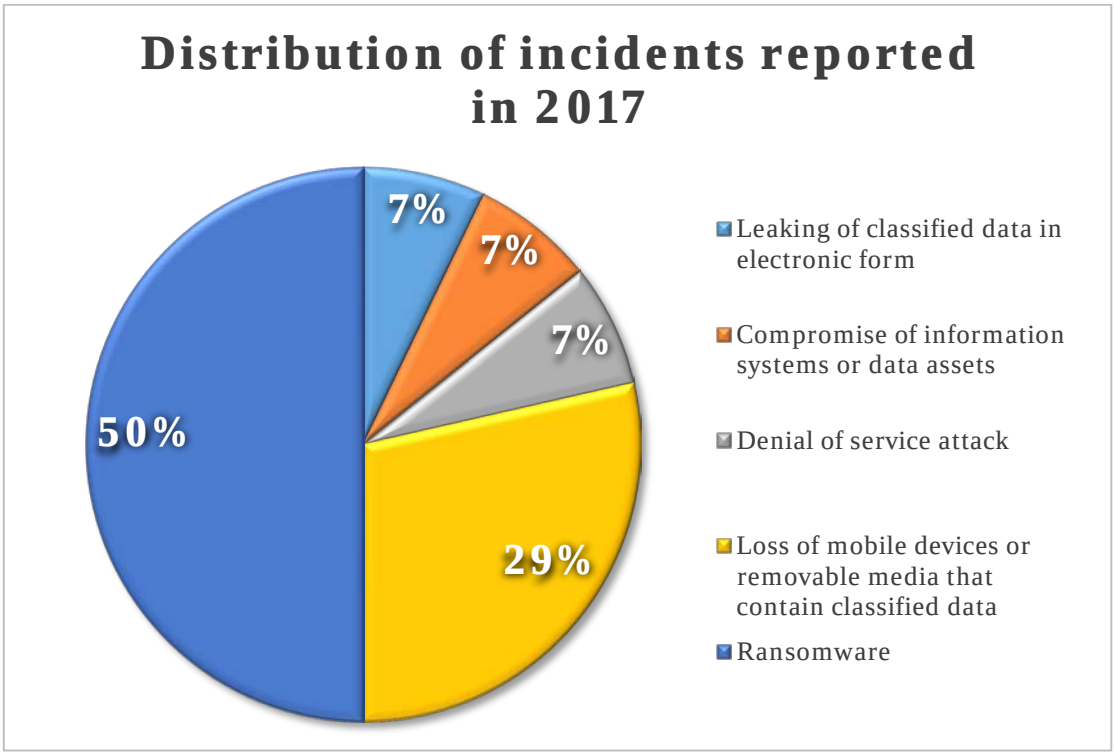
3.3 Alerts and Advisories

In 2017, we published 87 product security alerts associated with computing products widely deployed in government installations. We also released a security advisory for public reference highlighting the risk of the KRACK (Key Reinstallation AttaCKs) vulnerabilities and recommending appropriate measures to protect data confidentiality of Wi-Fi network connections (www.govcert.gov.hk/en/advisories.html).

In 2017, we conducted threat analysis on over 200 security events detected and received from various sources. The threat information was extracted and shared with relevant constituents for appropriate follow-ups.

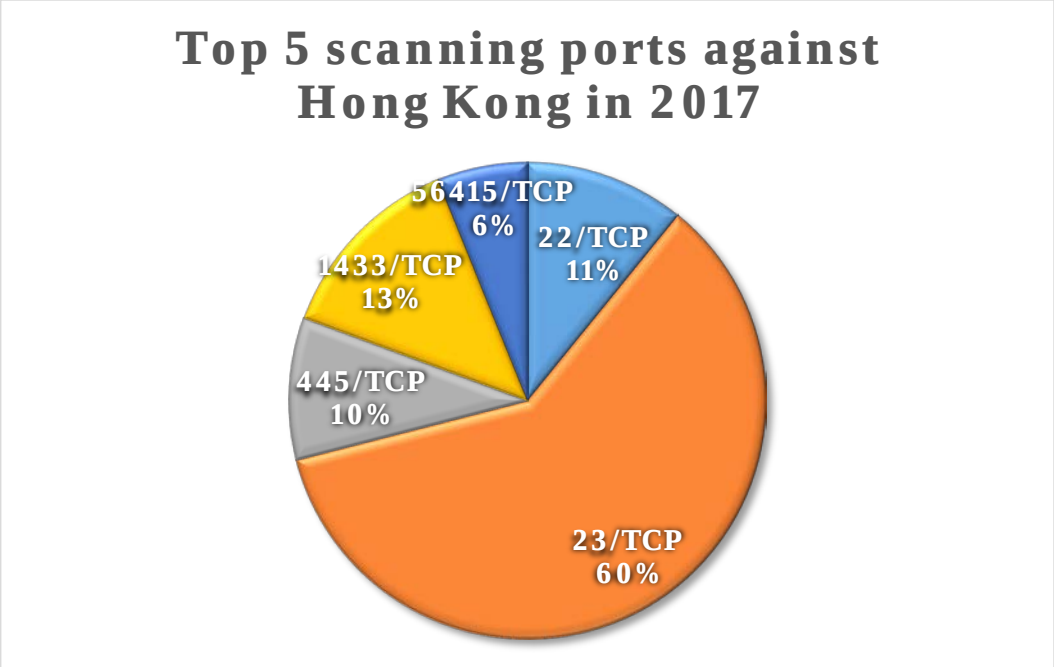
3.4 Incident Handling Reports

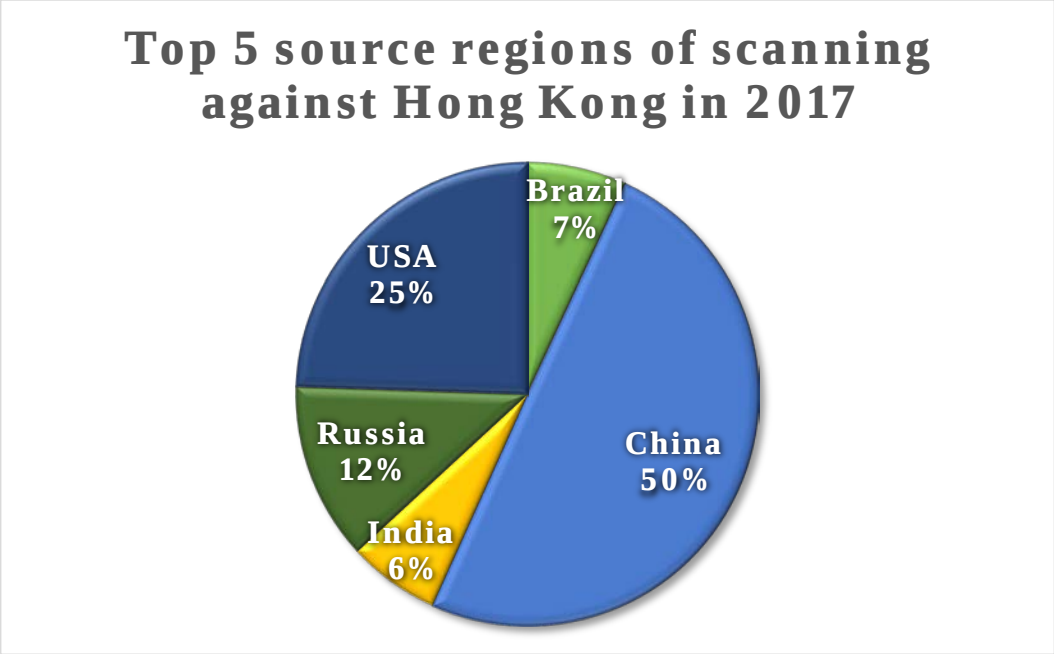
In 2017, GovCERT.HK received and handled various reports of cyber security incidents that were related to the government installations. The following chart shows the distribution of incidents reported in 2017.



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 and the top five source regions of scanning activities detected by the TSUBAME sensors installed in Hong Kong.





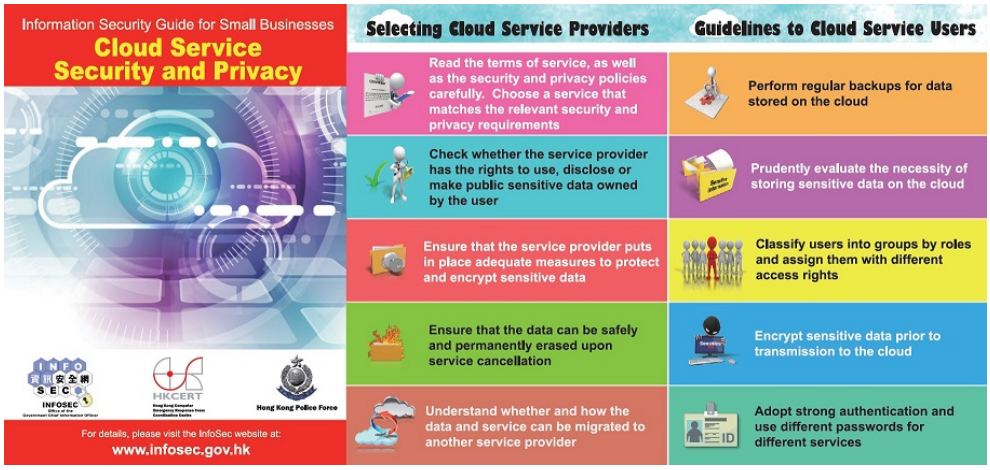
3.6 Publications and Mass Media

To raise public awareness and knowledge on the importance of information security, we have resorted to 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 different theme and offered associated tips having regard to recent security incidents or foreseeable cyber threats. For instance, the radio tips of "Use mobile payment safely" were broadcast in September 2017 to remind the public on security measures in using mobile payment services.
- To provide practical tips and advice for Small and Medium Enterprise (SMEs) and the public to protect from cyber attacks, we developed and shared infographics covering popular security topics such as "Safe Online Shopping" to remind the public to take necessary precautionary actions to stay safe while shopping online.

(www.cybersecurity.hk/en/resources.php#infographics)

- A set of practical guidelines with different themes, including "HTTPS and Website Security", and "Cloud Services Security and Privacy", were produced to educate SMEs to deploying appropriate security measures in their business environment.

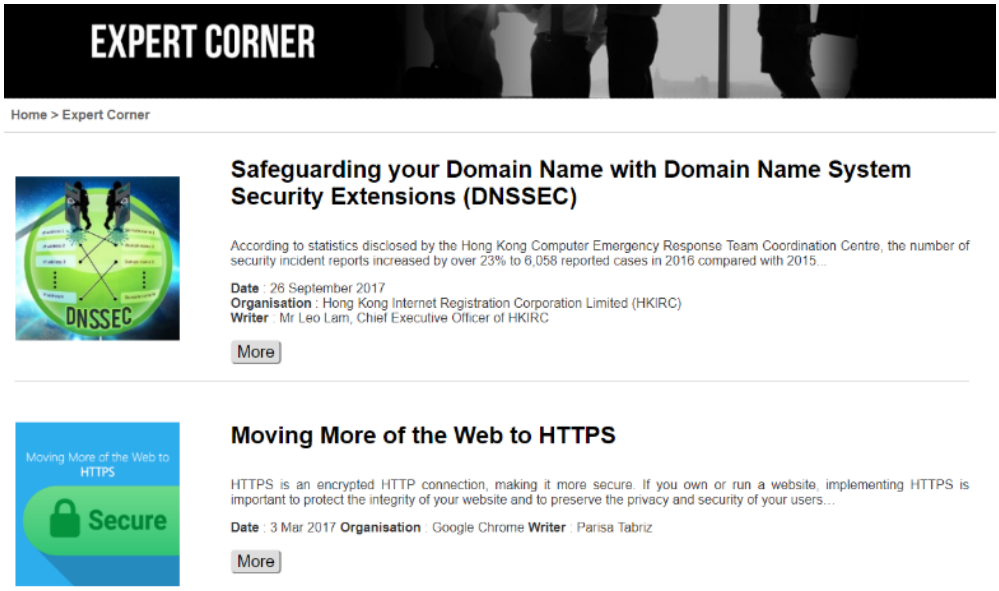


(www.cybersecurity.hk/en/resources.php#leaflets)

- We organised the "Smart Home, Safe Living" 1-Page Comic Drawing Contest with the theme "Smart Home, Safe Living" under the "Build a Secure Cyberspace" promotional campaign from April 2017 to September 2017. The contest has received overwhelming response with some 1 200 entries. A comic booklet and a 2018 calendar, adapted from the winning entries of the contest, were published to remind the public cyber security risks and suggest preventive measures through lively stories and figures.

(www.cybersecurity.hk/en/resources.php#booklet)

- To support and embrace the Domain Name System Security Extensions (DNSSEC) and Hyper Text Transfer Protocol Secure (HTTPS) technologies for better Internet security, adoptions of DNSSEC and HTTPS have been promoted to government websites to safeguard the online environment and strengthen trustworthiness of the websites. We have invited industry experts to contribute and share their insights on these topics and other hot issues at the "Expert Corner" of the CSIP. (www.cybersecurity.hk/en/expert.php)



4. Events Organised/Hosted

GovCERT.HK regularly organises awareness training and solution workshops to share 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 2017, we organised a total of 15 seminars, workshops and solution showcases for government IT staff and users to enhance their awareness of latest security vulnerabilities and update their knowledge in information security technologies.

- Seminars and showcases were conducted for government IT staff and users to raise their security awareness and introduce latest IT security technologies and solutions. The topics included industry best practices, ransomware and security of mobile applications.
- 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.
- Web vulnerability scanning workshops were organised for some 100 government officers to equip them with the necessary skills and knowledge to effectively

identify the potential security weaknesses in web applications and remedy the security risks.

4.2 Drills and Exercises

GovCERT.HK has actively 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.

In addition to conducting thirteen drill exercises involving individual government departments and their respective service contractors, we also conducted the inter-departmental cyber security drill in 2017 with some 40 departments participated to enhance the overall information security incident response capability of the Government. Using a number of simulated scenarios, the participating departments experienced how to respond to cyber security incidents effectively according to the established incident response procedure. In view of the success of this inter-departmental cyber security drill, the drill will be conducted regularly every year.

As the Operational Member of the Asia Pacific Computer Emergency Response Team (APCERT), GovCERT.HK participated in the APCERT Drill with the theme of "Emergence of a New Distributed Denial of Service Threat" in March 2017. GovCERT.HK played the role of Exercise Controller in addition to Player and Observer in the drill.

4.3 Conferences and Seminars

In 2017, GovCERT.HK adopted the slogan "Smart Home, Safe Living" as the key message to government users and the public. The target audience included businesses especially SMEs, organisations, schools and the public.

- Two seminars were organised under the "Build a Secure Cyberspace" promotional campaign in April and September 2017, aiming to promote public awareness of information security and the adoption of security best practices, in particular the risks of Internet-connected devices. The one-day seminar in September 2017

invited industry associations and experts to share insights on a range of security topics, including the most common cyber security threats nowadays, defence against ransomware, the secure use of mobile payment and social media.

- 32 school visits were conducted at primary and secondary schools in 2017, 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.

- To increase cyber security awareness among local primary, secondary and tertiary students on safe use of the Internet and social media, we supported the "Cyber Security Competition" in 2017 organised by the Hong Kong Police Force (HKPF) and the University of Hong Kong. The competition has received overwhelming response with over 7 600 participants. The competition included online quiz, security vulnerability analysis in simulated computers and presentation on topics related to cyber security.
- To promote the development of cyber security technologies and industry in Hong Kong and the Mainland, the second Hong Kong-Mainland Cyber Security Forum with the theme of "Facilitating Data Flow Securely and Orderly, Promoting Economic and Social Development" was held in October 2017. The forum attracted some 150 information security professionals from the Government, research institutions, the academia, professional organisations and the information security industry to exchange views on topics relating to data protection as well as personal data policy and law.
- To commend outstanding IT security professionals for their commitment and contribution in cyber security, we joined the HKPF and HKCERT to co-organise the second "Cyber Security Professionals Awards" (CSPA) in October 2017. Eighty

cyber security managers and practitioners from five different sectors were elected to receiving the awards and merits. The following photo of the hosts and the judges was taken at the Awards Presentation Ceremony.
(www.csprofessionalsawards.net)

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

To raise public awareness, GovCERT.HK collaborated closely with our partners such as HKPF and HKCERT, and security service providers to gather information on security vulnerabilities and promptly issue alerts on malicious cyber activities to the public and private sectors.

In view of the rising trend of ransomware attacks in recent years, GovCERT.HK and HKCERT jointly launched the "Fight Ransomware Campaign" in September 2017. The campaign featured the setting up of a "Ransomware Intelligence Portal" to share with the public the latest intelligence and analysis, security alerts and training information, etc. related to ransomware. As of December 2017, the campaign has conducted a total of four public seminars on ransomware and posted nearly 30 articles through the portal.

GovCERT.HK also plays 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. The IILG mechanism would be activated in support of major events or in response to incident outbreak or natural disasters that would affect the smooth operation of the Internet infrastructure of Hong Kong. In 2017, the IILG collaboration mechanism was activated six times in support of major events.

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 February 2017, GovCERT.HK hosted an International CERTs Collaboration Meeting with JPCERT/CC and HKCERT to share view on collaboration opportunity and invited JPCERT/CC to run a technical workshop on TSUBAME, the Internet threat monitoring system, with a view to support GovCERT.HK's cyber threat monitoring mechanism.

On 7 September 2017, GovCERT.HK signed an agreement with CNCERT/CC to receiving the China National Vulnerability Database information. This enabled

GovCERT.HK to strengthen its capability in vulnerability analysis and management.

GovCERT.HK has participated in the following events in 2017:

- CNCERT/CC Annual Conference
- FIRST Annual Conference
- Annual Technical Meeting for CSIRTs with National Responsibility
- 2017 China Cybersecurity Week
- Hong Kong – Mainland Cyber Security Forum
- Microsoft Digital Crimes Consortium 2017
- Four APCERT on-line training sessions

6. Future Plans

6.1 Upcoming Projects

With the global upsurge in cyber security threats, GovCERT.HK will continue to stay vigilant in defending against potential cyber attacks. GovCERT.HK will explore appropriate tools and facilities to establish a testing centre for providing vulnerability scanning, penetration test, and malware analysis capability to protect government information systems.

6.2 Future Operations

GovCERT.HK will continue to forge closer ties and enhance information exchange with the CERT community, as well as streamline its operations to cope with the increasing security threats and alleged cyber attacks in the region. We will also explore the adoption of community-driven standards and protocols of Structured Threat Information Expression 2.0 (STIX2) and Trusted Automated Exchange of Intelligence Information (TAXII) to support effective threat analysis and exchange of cyber threat information in the long run.

To strengthen Hong Kong's overall capability in defending against and recover from cyber attacks, we will launch an initiative to promote territory-wide cyber security information sharing and collaboration. A pilot partnership programme for cyber security information sharing and collaboration will be launched to promote trusted partnership of local cyber security stakeholders across prominent sectors for sharing cyber threat information and security analysis on emerging cyber risks and vulnerabilities, as well as providing actionable insights to the community.

7. Conclusion

Cyber attacks become increasingly sophisticated and stealthy. GovCERT.HK has been proactively collaborating with local and global CERTs, making timely response and enhancing appropriate defensive measures to the imminent cyber security threats. GovCERT.HK would actively 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 enhance the cyber security resilience capability of the community.

Contact: cert@govcert.gov.hk
Websites: www.govcert.gov.hk
www.cybersecurity.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 organization in Hong Kong, has operated the centre since then.

1.2 Organization 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, three Consultants and six Security Analysts and one Administrative Assistant.

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 2017, HKCERT had handled 6,506 security incidents which was 7% increase of the previous year (see Figure 1).

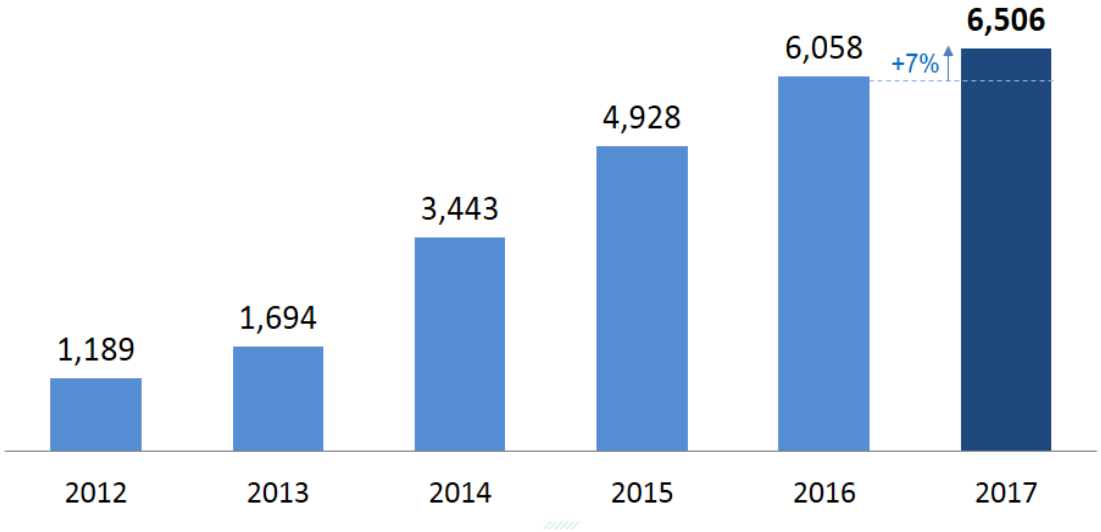


Figure 1. Incident Reports Handled by HKCERT

The increase of the number of incidents was due to the increase of referral cases as a result of closer collaboration with global security researchers and organizations. Referral cases accounted for 91% of the total number of security incidents.

Two major categories of security incidents, Botnet (2,084 cases) and Phishing (1,680 cases) remained at similar level as in the previous year (see Figure 2).

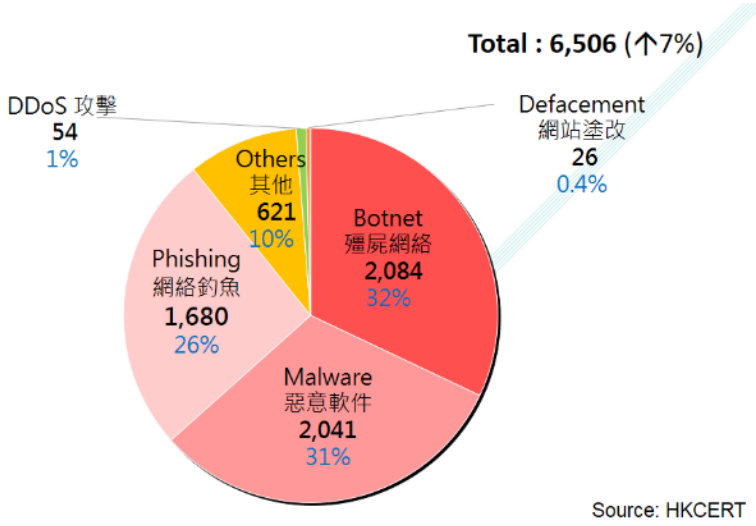


Figure 2. Distribution of Incident Reports in 2017

The number of malware infection incident reports rose sharply by 79% in 2017 (see Figure 3.) These cases were mainly due to WannaCry sinkhole detections and XcodeGhost contaminated mobile apps. Among all malware reports, despite fewer Ransomware incident reports (178 cases) were made to HKCERT last year, there were 1,210 bot-Wannacry cases. These involved large number of computers being infected by the notorious Wannacry ransomware that rocked the world last May, but encryption was yet to be triggered.

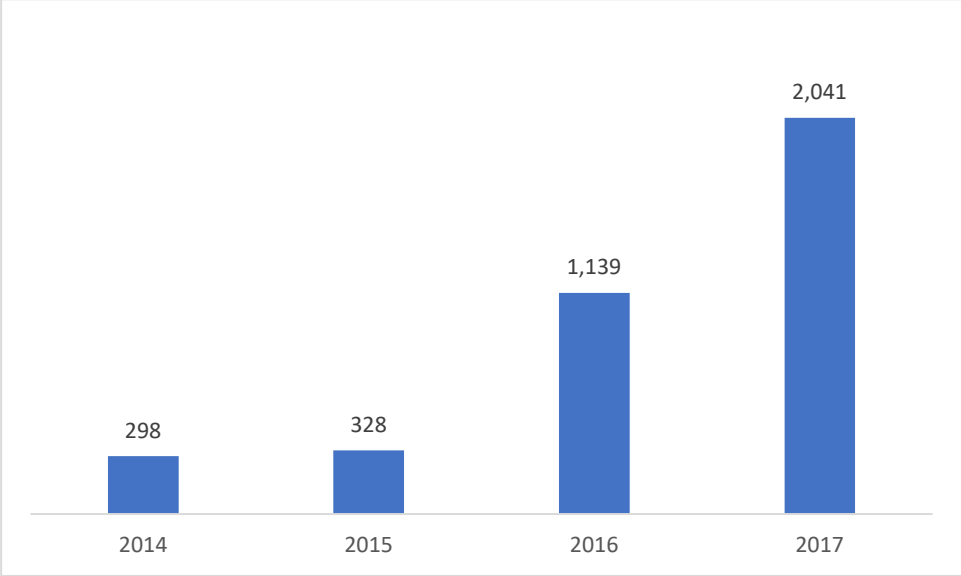


Figure 3. Number of Malware Incident Reports in the past 4 years

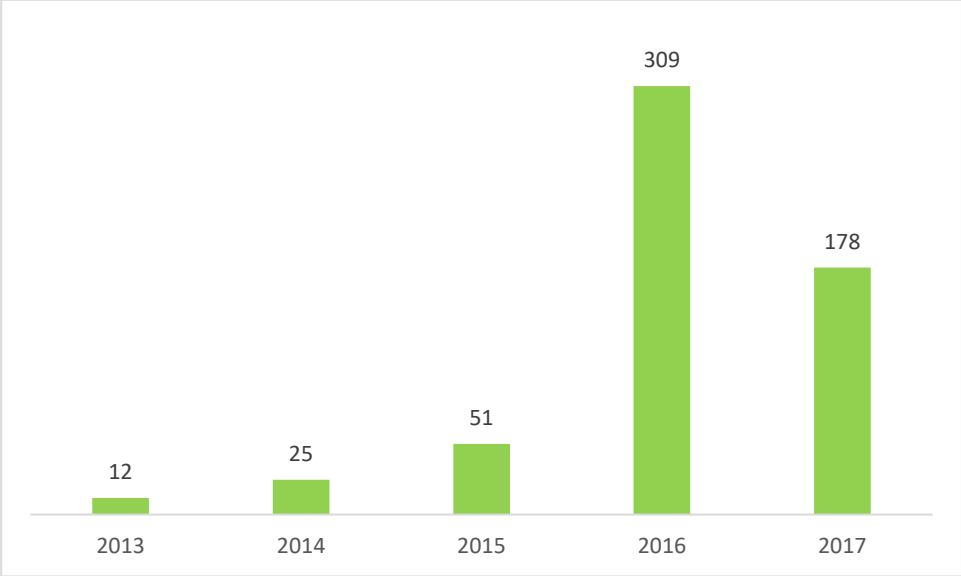


Figure 4. Number of Ransomware Incident Reports in the past 5 years

2.2 Watch and Warning

During the period from January to December of 2017, HKCERT published 250 security bulletins (see Figure 5) on the website. In addition, HKCERT have also published 110 blogs, including security advisories on DDoS extortion, marketing adware, smart device installation, ransomware, IoT Botnet, remote desktop service risk, third party plugins, etc. HKCERT also published the "best security reads of the week" every week to inform the public of good security articles.

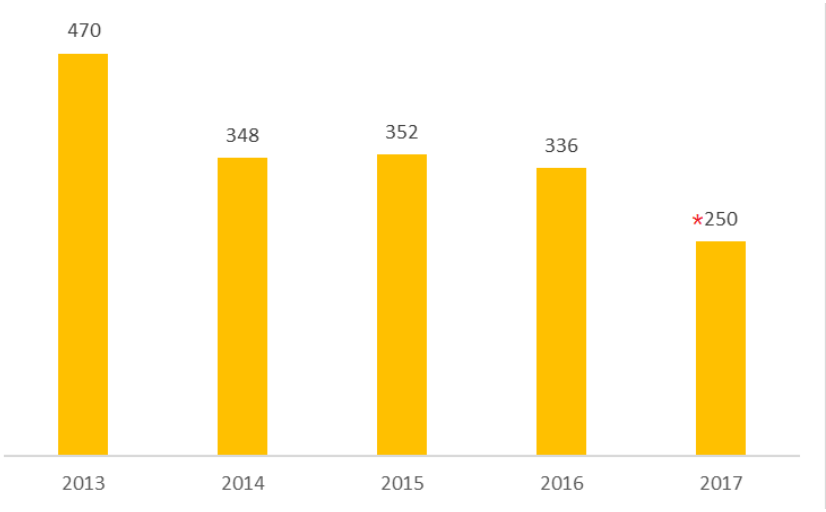


Figure 5. HKCERT Published Security Bulletins

**The drop of Security Bulletins 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 6 showed the trend of bot related security events maintains similar figures (from 4,656 in Q4 2016 to 4,690 in 2017). But the figures have included WannaCry sinkhole which maintains around 2,000. Mirai got significant decrease after 1 year of botnet clean operation.

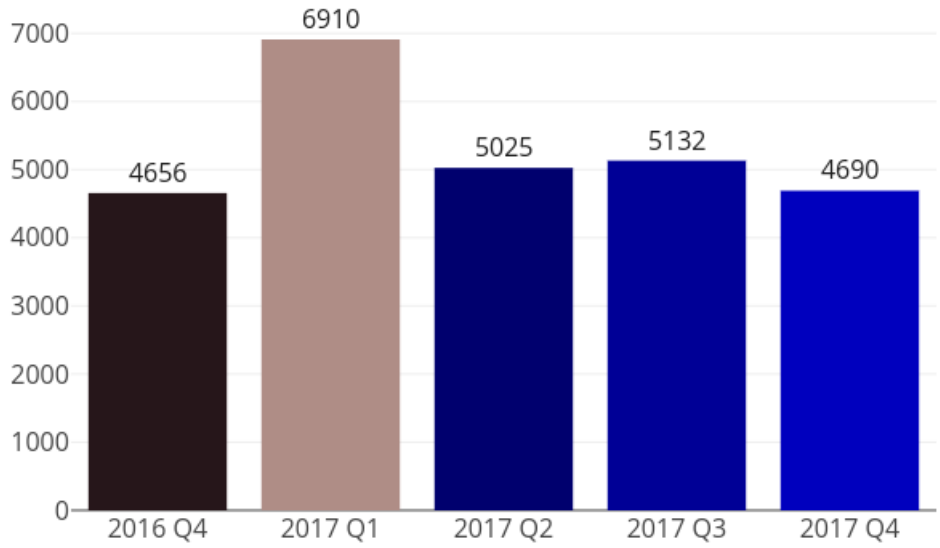


Figure 6. Trend of Bot related security events in the past year

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

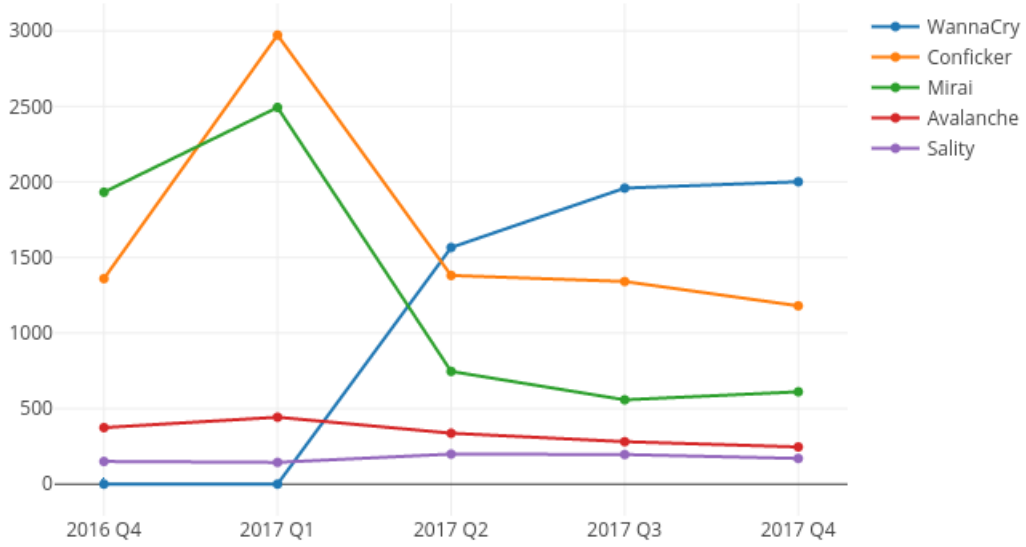


Figure 7. Trend of Top 5 Botnet Families in the past year

(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 Hong Kong Google Play Store's Apps Security Risk Report. The Report is a co-operation with CNCERT/CC. (see https://www.hkcert.org/play-store-srr).

- 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).

- HKCERT had published 50 weekly column articles in a local Chinese newspaper (Hong Kong Economic Times) to raise the cyber security awareness of business executives.
  (see https://hkpc.org/en/corporate-info/media-centre/media-focus#1).

3. Events organized and co-organized

3.1 Seminars, Conference and Meetings

HKCERT jointly organized the "Build a Secure Cyberspace 2016" campaign with the Government and Hong Kong Police Force. The campaign involved public seminars, and a 1-Page Comic Drawing Contest. Two public seminars were organized in April and September 2017.

For the graphic design contest, HKCERT had received about 1,200 applications from Open group, Secondary School group and Primary School group. A professional judge panel selected winners with good attractive drawing (See Figure 8).

Figure 8. Champion entries of Open, Secondary School and Primary School Group (from left to right)

We organized the 2-day Information Security Summit 2017 with other information security organizations and associations in August 2017, 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 2017 to promote the public seminar and the 1-Page Comic Drawing Contest.
- HKCERT was interviewed by the media from time to time to give objective and professional views on information security topics and incidents.

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 New Delhi
- Participated in the FIRST Meeting and National CSIRT Meeting in Puerto Rico
- Participated in the CNCERT Conference in Qingdao
- Participated in the AusCERT Conference in Gold Coast
- Participated in International honeypot initiatives, including joining the Tsubame project of JPCERT/CC and The Honeynet Project.
- 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 organizations 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 organize joint events regularly. In 2017, HKCERT was a co-organizer and a member of the judge panel member in the 2nd Cyber Security Professionals Awards organized by Hong Kong Police Force.
- To combat worsening ransomware cyber attacks, HKCERT and the government GovCERT.hk jointly launched a "Flight Ransomware Campaign" on 5 September 2017 to strengthen the readiness of Hong Kong businesses and general public against ransomware attacks. Riding on the popularity of social media and mobile technologies, the new campaign includes the creation of a Facebook page "Ransomware Intelligence Portal" (www.facebook.com/ransomware.hk) where HKCERT teams up with major international IT and cyber security companies for early sharing of intelligence of global trends and insights about ransomware, security alerts and training information with the public. In addition, the public will have access to free anti-malware software with real-time protection, provided by cyber security partners of the campaign.

- 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. In 2017, HKCERT had worked with ISPs to develop a "Service Provider Interconnection, Routing and Information Security Best Practices" (SPIRITS) guideline. A symposium was also organized with HKISPA in December to promote the best practice guideline. More activities will be expected in 2018 to engage ISPs in Hong Kong.
- HKCERT continued to Maintain the Information Security Advisory and Collaboration (ISAC) Mailing list with the Internet infrastructure organizations, and advised on latest information security issues through the list
- HKCERT also liaised with critical infrastructure sector and had delivered awareness briefings to these organizations for better protecting the security environment of Hong Kong; created the Information Security Advisory and Collaboration (ISAC-CI) Mailing list with the critical infrastructure organizations, and advised on latest information security issues through the list.

5. Other Achievements

5.1 Advisory Group Meeting

HKCERT had held the Advisory Meeting in September of 2017. The meeting provides solicit inputs from the advisors on the development strategy of HKCERT.

5.2 Three Year Strategic Plan

HKCERT prepared its third rolling Three Year Strategic Plan based on inputs from Advisory Group, the Strategy and Service Review Report and the previous CERT Study Tour and discuss with the government. The plan would be updated annually. HKCERT based on this plan to prepare the annual plan and budget to solicit funding support from the government.

5.3 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 publicized the information to the public quarterly and used the information in decision making. HKCERT joined the Cyber Green project initiated by JPCERT/CC to explore development of useful metrics for measuring cyber health.

5.4 Year Ender press briefing

HKCERT organized a year ender press briefing to media in January 2018 to review cyber security 2017, and provided outlook to 2018 to warn the public for better awareness and preparedness. It received very good press coverage.

Figure 9. 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 organizations to build a more secure Hong Kong and Internet.

6.2 Funding

HKCERT had secured Government funding to provide the basic CERT services in 2018/2019. 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

HKCERT is working on enhancing the infrastructure to increase the efficiency of information search and sharing. HKCERT was developing automation tools to enhance the incident response process.

7. Conclusion

In 2017, HKCERT was active in promoting public awareness of ransomwares and their

impact on corporations particular SMEs. The cross border collaboration and intelligence driven response continued to improve the proactiveness and effectiveness of incident response. HKCERT has seen the immense power of collaboration and would invest more to further this success.

With the Internet security facing more crises from financially motivated cyber crimes, Internet of Thing (IoT) attacks, more use of mobile payment apps, more regulation for security and privacy and supply chain attacks, HKCERT expects 2018 would be continuously a challenging year.

JPCERT/CC

Japan Computer Emergency Response Team / Coordination Center – Japan

1. Highlights of 2017

1.1 Summary of major activities

- Joined "No More Ransom" project as a Supporting Partner

On April 2017, JPCERT/CC joined "No More Ransom" project as a Supporting Partner. This is a global initiative launched as a joint effort by Dutch National Police, The European Police (Europol), Intel Security and Kaspersky Lab and aims to disseminate information about the danger of ransomware as well as to provide useful resources such as free decryption tools to help victims recover their data without having to pay ransoms to cybercriminals.

https://www.nomoreransom.org/en/index.html

1.2 Achievements & milestones

- Reappointed as APCERT Steering Committee member and Secretariat

At the APCERT AGM & Conference 2017 in Delhi, JPCERT/CC was re-elected as a member of the Steering Committee (SC) and the Secretariat. JPCERT/CC has been serving the community as a SC member and Secretariat since the establishment of APCERT in 2003.

2. About JPCERT/CC

2.1 Introduction & Establishment

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

2.2 Constituency

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

3. Activities & Operations

3.1 Incident Handling Reports

In 2017, JPCERT/CC received 18,450 computer security incident reports from Japan and overseas.

	1st Qtr	2nd Qtr	3rd Qtr	4th Qtr	Total
Incident Reports	4,095	5,225	4,600	4,530	**18,450**

Figure 1. Incident reports to JPCERT/CC (2016)

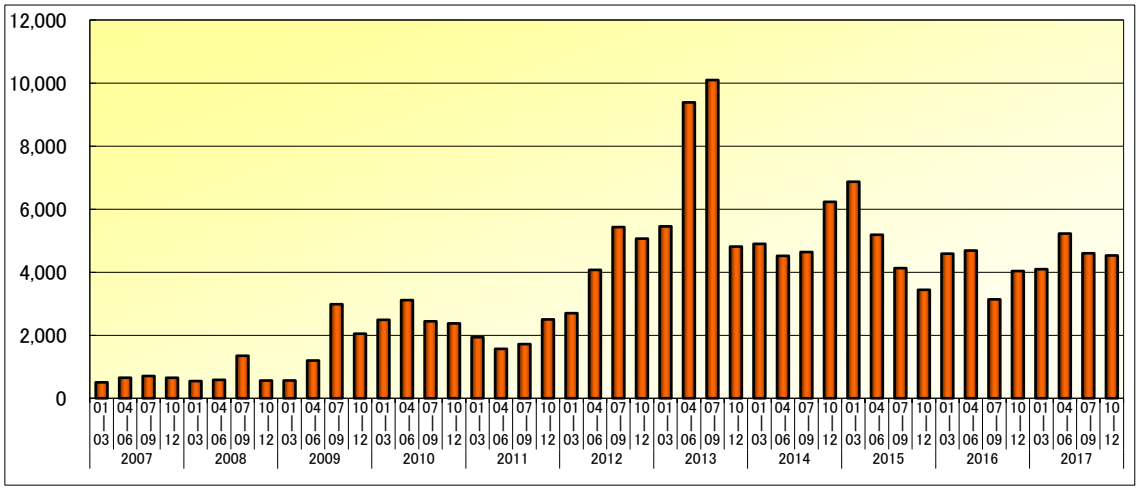


Figure 2. Incident reports to JPCERT/CC (2007-2017)

3.2 Abuse statistics

Incident reports to JPCERT/CC in 2017 were categorised as in Figure 3. About 53% of the reports were on scan, followed by website defacement and phishing.

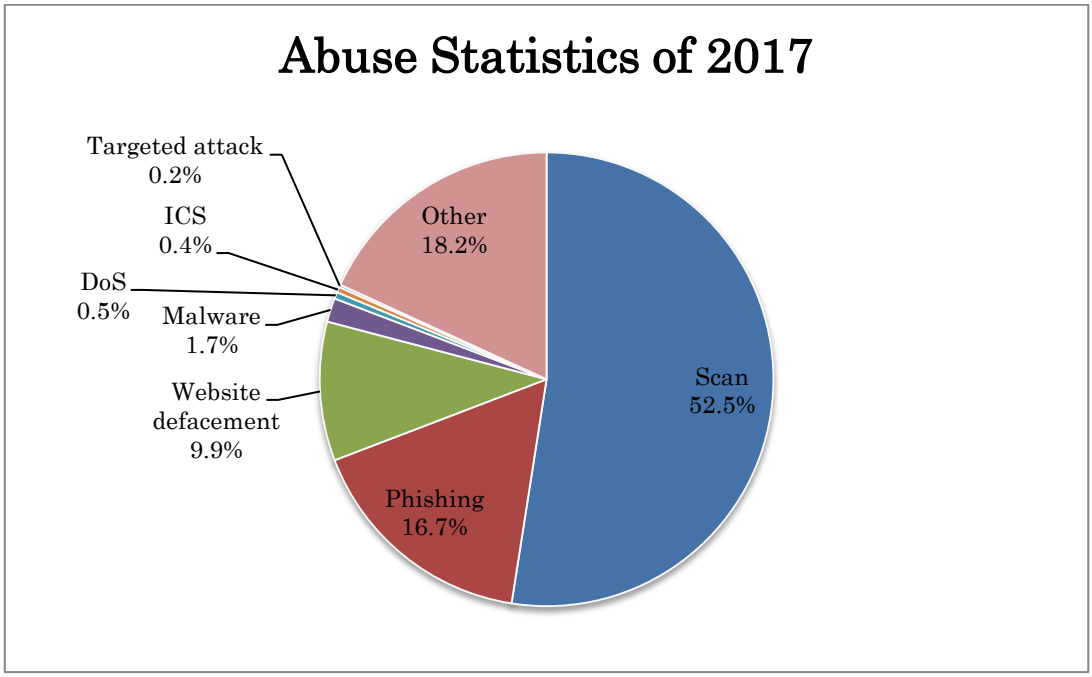


Figure 3. Abuse Statistics of 2017

3.3 Security Alerts, Advisories and Publications

- **Security Alerts**

https://www.jpcert.or.jp/english/at/ (English)

https://www.jpcert.or.jp/at/ (Japanese)

JPCERT/CC publishes security alerts on widespread, emerging information security threats and their solutions. In 2017, 50 security alerts were published.

- **Early Warning Information**

JPCERT/CC publishes early warning information to the Japanese government and organisations providing national critical infrastructure services and products through a dedicated portal site called "WAISE (Watch and Warning Analysis Information for Security Experts)". Early warning information contains reports on threats, threat analysis and their solutions.

- **Japan Vulnerability Notes (JVN)**

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

https://jvn.jp/ (Japanese)

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 (https://www.cert.org/), ICS-CERT (https://ics-cert.us-cert.gov/), CPNI (https://www.cpni.gov.uk/), NCSC-FI (https://www.ncsc.fi/) and NCSC-NL (https://www.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 2017, 302 vulnerabilities coordinated by JPCERT/CC were published on JVN. 195 were cases published with IPA through the Information Security Early Warning Partnership, and 104 were published through partnerships with overseas coordination centers, developers, researchers, etc.

Of the 195 published through the Information Security Early Warning Partnership, 183 were reported to IPA by researchers, security vendors, etc. 12 were reported directly by the software developers. Of the 104 published through global partnerships, 55 were reported and published by CERT/CC, 1 by NCSC-FI, 26 were reported by developers on software they developed, 9 were reported by an overseas researcher, and 13 were published originally by JPCERT/CC through public monitoring activities and based on the information collected via the channels that JPCERT/CC has established privately. In addition, there were 3 issues published as technical alerts based on publicly available information.

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.

In December 2017, a member of JPCERT/CC was elected as a member of the CVE Board, which is a committee to discuss operations for global and smooth handling of CVE, moderated by the MITRE Corporation.

- **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**

http://blog.jpcert.or.jp/ (English)

Since September 2010, JPCERT/CC has been providing security news and technical observations related to Japan, as well as international activities that JPCERT/CC engages in on its English blog. In 2017, 17 articles were published.

- **Quarterly Activity Reports**

https://www.jpcert.or.jp/english/menu_documents.html (English)

https://www.jpcert.or.jp/report/ (Japanese)

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

- **JPCERT/CC on Twitter**

https://twitter.com/jpcert_en (English)

https://twitter.com/jpcert (Japanese)

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

- **Analysis Center**

JPCERT/CC has a team to conduct technical research and artifact analysis, including not only viruses and bots but also tools that can potentially be used with malicious intent. Findings through the analysis are crucial during incident handling, and our Analysis Center is committed to enhance its analysis environment and capability.

- **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.

3.5 Projects

- **CyberGreen Initiative**

http://www.cybergreen.net/

CyberGreen is a global initiative designed to efficiently create a "healthy" cyberspace through cooperation with technical partners such as CSIRTs, ISPs and security vendors across the globe. The initiative provides metrics-based measurement and statistical analysis that can be compared across nations and regions. JPCERT/CC is working with global partners to improve upon the metrics, statistical analysis methods and visualisation.

3.6 Associations and Communities

- **Nippon CSIRT Association**

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

http://www.nca.gr.jp/index.html (Japanese)

The Association is a community for CSIRTs in Japan. JPCERT/CC serves as a member of the Steering Committee and 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 hosted 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 2017, JPCERT/CC renewed MoU's with bdCERT, BruCERT, CERT Australia, CERT.GOV.AZ, ID-SIRTII/CC, MOCERT, MonCIRT, Sri Lanka CERT|CC, ThaiCERT, TWCERT/CC, TWNCERT and VNCERT.

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

https://www.first.org

JPCERT/CC contributes to the international CSIRT community by serving as a member of the Board of Directors of FIRST since 2005. JPCERT/CC also supports CSIRTs who wish to become a member of FIRST.

- **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 2017.

- Web defacement training at Africa Internet Summit (May, Nairobi)
- Network forensics training at FIRST Regional Symposium (September, Taichung)

5.2.2 Drills & Exercises

JPCERT/CC participated in the following drills in 2017 to test our incident response capability:

- APCERT Drill 2017 (22 March)

- ASEAN CERTs Incident Drill (ACID) 2017 (11 September)

5.2.3 Seminars & presentations

In 2017, JPCERT/CC dispatched speakers to the following international cyber security events:

- APRICOT 2017 / FIRST Technical Colloquium (February, Ho Chi Minh City)
- CNCERT/CC Annual Conference (May, Qingdao)
- Annual Meeting of the Global Forum on Cyber Expertise (June, Washington DC)
- 29th Annual FIRST Conference (June, San Juan)
- National CSIRT Meeting (June, San Juan)
- PacSec 2017 (November, Tokyo)
- CODEBLUE 2017 (November, Tokyo)
- Botconf 2017 (December, Montpellier)
- APEC TEL 56 (December, Bangkok)

...and many more

5.3 Other international activities

Below are some of the international events that JPCERT/CC attended in 2017:

- S4x2017 ICS Security Conference (January, Miami)
- RSA Conference US 2017 (February, San Francisco)
- CanSecWest 2017 (March, Vancouver)
- ISO/IEC JTC 1/SC 27 Information Standard Meeting (April, Hamilton) (October, Stockholm)
- APWG eCrime 2017 (June, San Francisco)
- PacNOG (July, Suva)
- Black Hat USA 2017 (July, Las Vegas)
- DEFCON 25 Hacking Conference (July, Las Vegas)
- 2017 APISC Security Training Course (July, Seoul)
- HITCON 2017 (August, Taipei)
- 26th USENIX Security Symposium & Workshop (August, Vancouver)
- The 5th China-Japan-Korea CSIRT Annual Meeting for Cybersecurity Incident Response (September, Seoul)
- OWASP AppSec USA 2017 (September, Orlando)
- ICS Cyber Security Conference (October, Atlanta)

- Virus Bulletin Conference 2017 (October, Madrid)
- APCERT AGM and Conference 2017 (November, Delhi)
- BlueHat v17 (November, Seattle)
- Global Conference on Cyberspace (November, Delhi)

…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

- Pilot Project: Internet Risk Visualisation - Mejiro

JPCERT/CC is working on a pilot project to visualise risks on cyber space based on data provided by multiple sources in comparison to the number of IP addresses assigned to each economy. Towards 2018, JPCERT/CC plans to launch a portal site with visualised map based on risk index, which aims to provide hints for mitigation process.

7. JPCERT/CC Contact Information

URL: https://www.jpcert.or.jp/english/

E-mail: global-cc@jpcert.or.jp

Phone: +81-3-3518-4600

Fax: +81-3-3518-4602

KrCERT/CC

Korea Internet Security Center – Korea

1. Highlights of 2017

1.1 Summary of major activities

In 2017, ransomware represented by WannaCry swept across the world. KrCERT/CC handled with the incidents by analyzing and raised awareness by issuing advisory and press release with instructions that users could easily follow. Furthermore, as the tension has rose by missiles launched by DPRK, KrCERT/CC kept on the alert for any cyberattacks.

1.2 Achievements & milestones

KrCERT/CC provides services like 24/7 monitoring and DDoS sheltering system. It runs system that crawls 3.7 million websites registered in Korea in order to detect hidden malware on domestic websites.

KrCERT/CC also operating two kinds of alliance with domestic and international concerning organizations under the name of "Cyber Threat Intelligence" and "Global Cyber Threat Intelligence" since 2014 and 2016 respectively. It have a meeting with the members on a regular basis for exchanging knowledge about recent threat and technology.

Furthermore, with C-TAS, Cyber Threat Analysis & Sharing System, 198 member organizations share threat information in real time.

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, one planning team, and thirteen teams.

KrCERT/CC carries out various responsive and preventive programs designed to minimize 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 (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 communication 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 KISA (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.

The multiple names of KrCERT/CC occasionally give cause for confusion. In South Korea, it is called KISC, or the Korea Internet Security Center.

2.3 Resources

As of Dec. in 2017, around 160 employees from 3 divisions, 1 center, and 1 planning team work for KrCERT/CC.

2.4 Constituency

KrCERT/CC serves as the focal point to coordinate security incidents in all Korean constituencies. 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 national CERTs/CSIRTs, international organizations and security vendors.

3. Activities & Operations

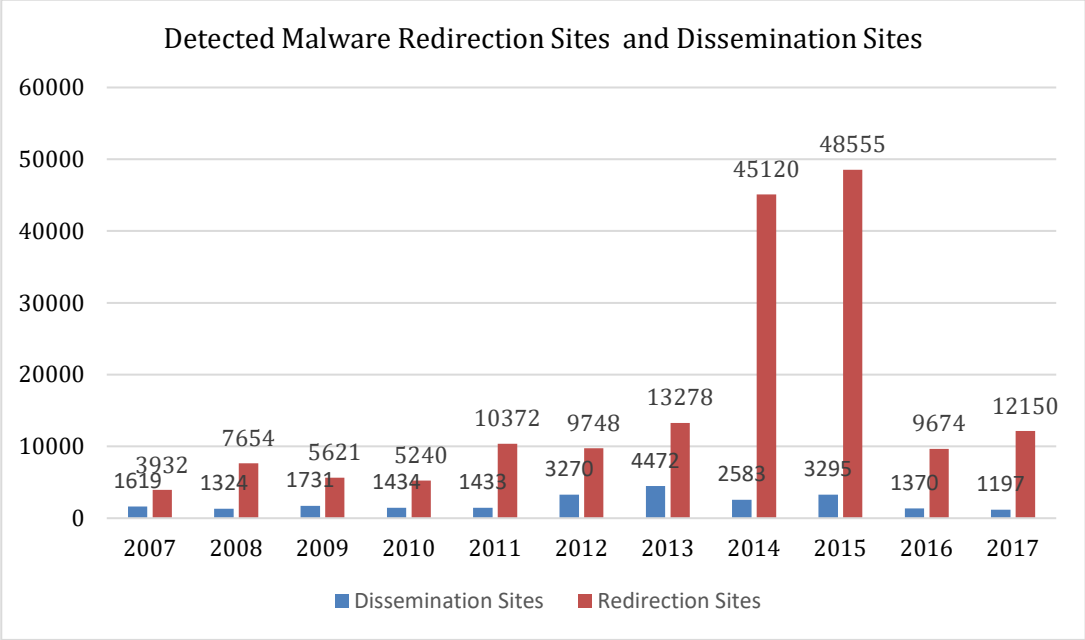
3.1 Scope and definitions

KrCERT/CC works for the safe and reliable cyber space by preventing cyberattacks and enhancing countermeasures. The mission of 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

The number of compromised website distributing hidden malware slightly decreased in 2017 by 12.6% from 1370 to 1197. Meanwhile, the number of redirection sites has increased after a plunge in 2016 by 25.6%.



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 is uploaded on the website.

4. Events organized / hosted

4.1 Training

KrCERT/CC has been organizing the 2017 APISC Training Course, an annual invitation-based security training course on CSIRT establishment and operation 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. 19 participants from 19 countries including the Philippines, Thailand and India participated in the 2017 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. It has cybersecurity consultation program, providing a consultation on the Information Security Management System. In addition, GCCD hosts two types of Cybersecurity seminar. One is an invitation-based training in Korea, which provides general security information. And the other is a joint cybersecurity seminar in a local country. The Join seminar is customized for partner country with their needs.

4.2 Drills & exercises

KrCERT/CC hosted a 2-day domestic cyber threat drill in November 2017 with the Ministry of Science and ICT(MSIT) to check readiness of rapid cyber threat response and an organic cooperative system. 36 companies including ISPs, security vendors, portal service providers, webhard service providers, online shops and critical infrastructure organizations participated in the drill. It enabled participants to check an entire response process from threat detection to incident investigation through these drills. Aside from this, 3 more cyber drills were conducted with relevant agencies.

4.3 Conferences and seminars

KISA hosted the 2nd CAMP Annual Meeting. CAMP Cybersecurity Alliance for Mutual Progress(CAMP), a networking platform to achieve sustainable benefits of secure cyber environment, was initiated by the Korean government in 2016 and in its second year of operation CAMP held a couple of events such as Regional Forums in Africa and Asia and the Annual Meeting in Korea. Among the most important gatherings is the Annual Meeting where all members gather to exchange experiences and information, discuss direction of operations, and organize activities that advance mutual interests. The main theme of the year 2017 was "Cyber Resilience by Security Cooperation" and total 45 cybersecurity related organizations from 34 countries participated in this meeting.

Additionally, in collaboration with the Ministry of Science and ICT, KISA hosts the 6th “Day of Information Security” celebration and “International Conference on Information Security(ICIS)” on July 12.

4.4 Competition

KrCERT/CC hosted the 14th Hacking Defence Contest (HDCON) with the MSIT in November 2017. HDCON is a time-honored domestic contest that started in 2004. Only

10 teams which got through the preliminaries made it to the finals. The 2017 HDCON was a platform to test competency of the participants in incident analysis and forensics in the whole process of incident handling. Accompanied with HDCON, a training session for vulnerability analysis on embedded devices and a seminar for KISA's two profiling cases was held. Furthermore, KrCERT/CC also arranged an event to find a drone vulnerability. The winner of the event got the drone as a prize. KrCERT/CC expects a competition like this would contribute to create the right environment for the participants to not only raising awareness.

5. International Collaboration

5.1 International partnerships and agreements

KrCERT/CC has close relationship with relevant institutions including CERTs internationally. It also hosts several meeting for enhancing cooperation.

5.2 Capacity building

5.2.1 Training

KrCERT/CC participates in APCERT online training on a regular basis.

5.2.2 Drills & exercises

KrCERT/CC joined in the APCERT Drill in March 2017. The drill required the participants to solve virtual incident with 9 injects.

5.2.3 Seminars & presentations

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

- FIRST TC at APROCOT 2017 in February 2017, Ho Chi Minh, Vietnam
- CNCERT/CC International Cooperation Forum, May, Qingdao, China
- CERT-RO Annual Conference, November, Bucharest, Romania
- 2017 APCERT AGM, November, New Delhi, India
- FIRST Technical Symposium, December, Czech, Prague

6. Future Plans

KrCERT/CC pursues further cooperation with both domestic and international organizations. It also tries to make better environment itself by raising awareness and capacity building. For these goals, KrCERT/CC will expand its cooperation and partnership and deepening relationship. And, it will expand its capacity building

program such as APISC.

7. Conclusion

Getting through some global incidents like WannaCry, people has been getting aware of cyber security. Though, many companies still avoid investing into cybersecurity and users have less interest in it. KrCERT/CC will make efforts to raise awareness for making better environment. And it will also keep in mind that it is needed to prevent and respond to incident even in unadmired moment, which will be a stepping stone for the enhanced cyber security in Korea.

LaoCERT

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

1. Highlight of 2017

1.1 Summary of Activities

- Co-organized the seminar with IT GREEN Public Company Limited on Security Analytics to ministry's officers, banks and Telecom enterprises on 16 March 2017 in Vientiane, Laos PDR.
- Co-organized the seminar with APNIC on Cyber Security and Threat Intelligence to ministry's officers, banks and Telecom enterprises on 21-22 August 2017 in Vientiane, Laos PDR.

1.2 Achievements & milestones

- Data Protection Law

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 2017.

2.2 Establishment

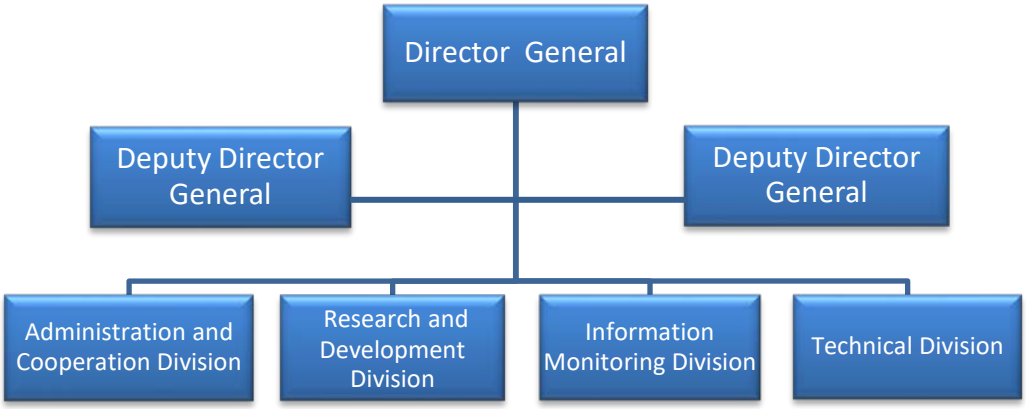
LaoCERT was established in February 2012 by degree 220/MPT as a LaoCERT division under the Lao National Internet Center, Ministry of Post and Telecommunications (MPT), Government of Lao PDR. It was established by following up as ITU-IMPACT recommendations and It has been announcement to become the national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

2.3 Resource

LaoCERT currently contain 31 staffs, 7 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 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.

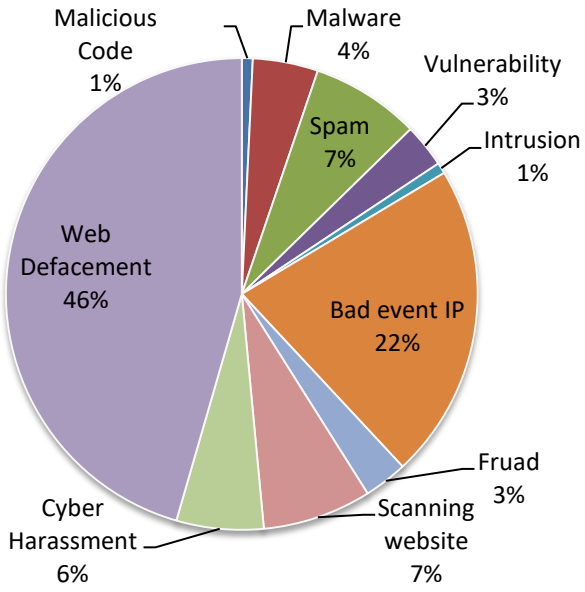
3. Activities & Operations

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.

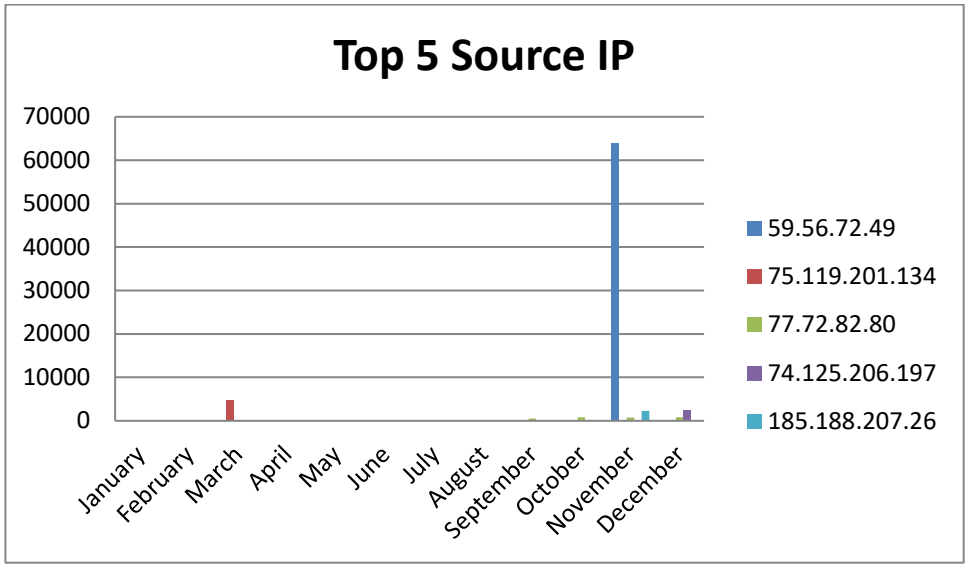
3.2 Incident handling report

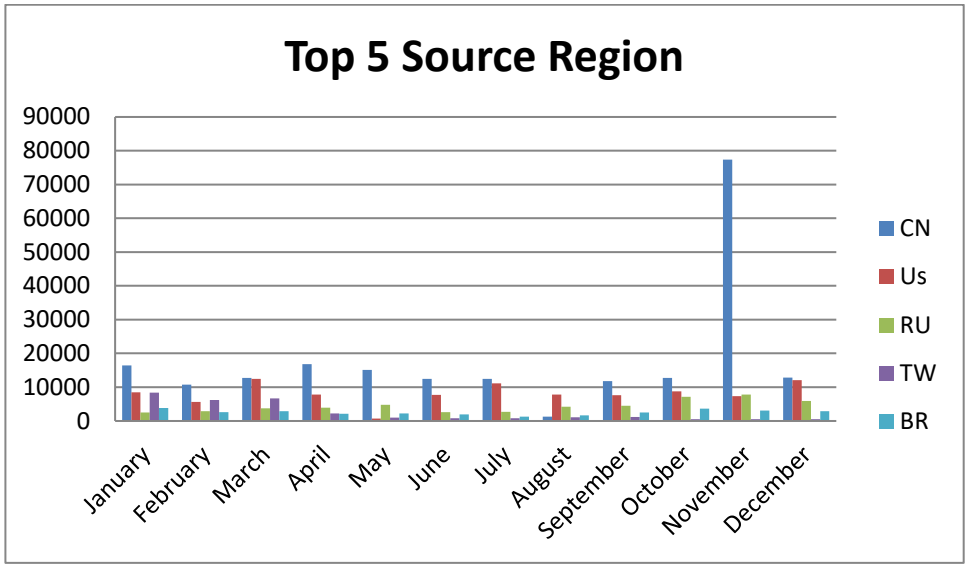
The following graph shows the incidents that happened in 2017.

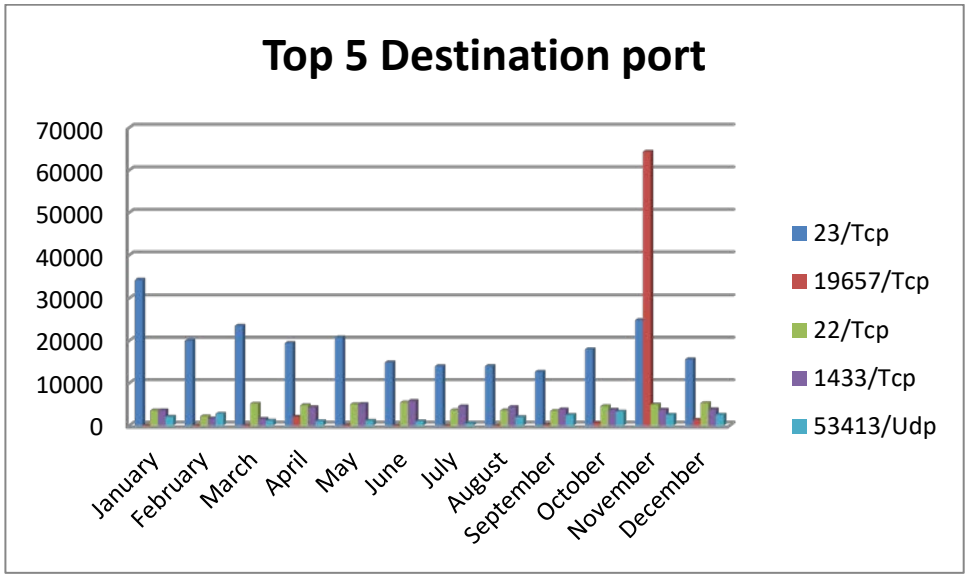


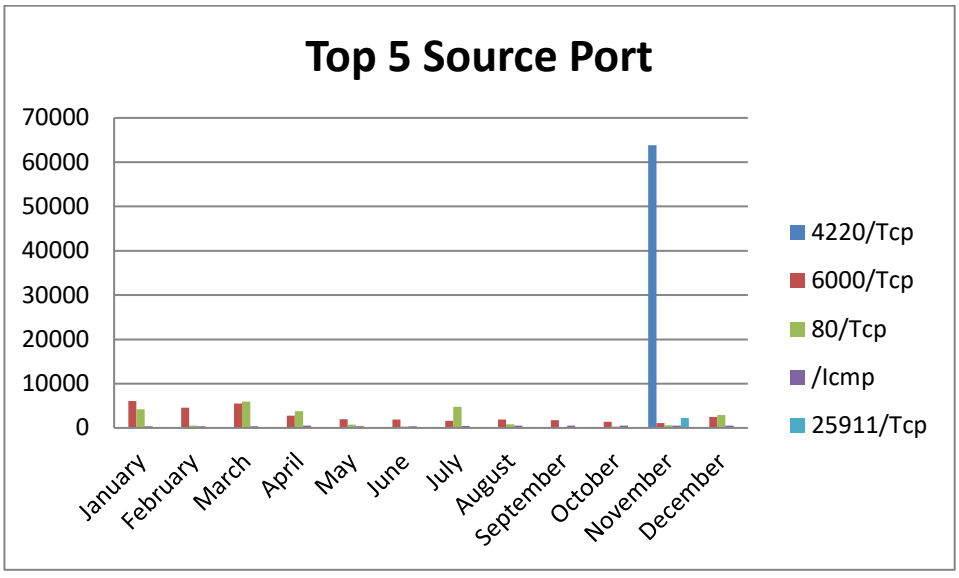
3.3 Abuse Statistics (TSUBAME Sensor)

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 2017.




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
CN
Us
RU
TW
BR


Top 5 Destination port
70000
60000
50000
40000
30000
20000
10000
0
January
February
March
April
May
June
July
August
September
October
November
December
23/Tcp
19657/Tcp
22/Tcp
1433/Tcp
53413/Udp


Top 5 Source Port
70000
60000
50000
40000
30000
20000
10000
0
January
February
March
April
May
June
July
August
September
October
November
December
4220/Tcp
6000/Tcp
80/Tcp
/Icmp
25911/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

- Advisories on social issue of internet using.
- Network Vulnerability Assessment for government agencies and private sectors.

4. Events organized / hosted

4.1 Training

- Co-Organized the Training Course on Data Network Fabric Configuration and Security Analytics Configuration on 25th – 28th, April 2017 in Vientiane, Laos PDR by invite experts from Thailand.

5. International Collaboration

5.1 International partnership and agreement

- MoU signed with VNCERT on 22nd June, 2017.
- MoU signed with CNCERT on 05th December, 2017.

5.2 Capacity Building

5.2.1 Training

- Joint the training course on Improving ICT Policy Promotion Skills Utilizing Standards Overcome Challenges by deployment of ICT Infrastructure Corresponding to the Situation from 18th January – 04th February 2017 in Tokyo, Japan.
- Attended the Training Program on CSMS (Cyber Security Management System) from 14th – 23rd February 2017 in Tokyo, Japan.
- Attended the India-Asean Workshop on Advanced Networking Techniques from 06-24 February 2017 in India.
- Joint the training course on Defense Practice against Cyber Attacks from 19th February – 04th March 2017 in Tokyo, Japan.

- Joint the training course on Service Inspection Gateway (SIG) from 24th – 26th May, 2017 in China.
- Attended the Training Course on Malware Analysis from 29th May - 2nd June 2017 in Hanoi, Vietnam.
- Attended the training course on Cyber Crime Tactical from 12th - 23rd June 2017 in Bangkok, Thailand
- Joint the ASEAN Cyber Wellness of Tutor from 05th -09th July 2017 in Indonesia.
- Joint the Asia-Pacific Information Security Training "APISC" from 31th July – 04th August 2017 in Seoul, South Korea.
- Joint the training on Reducing Cyber Crime through Knowledge and Capacity Building from 07th August- 29th September 2017 in India.
- Attended the APT training course on Cyber Security Technologies Recent Trend of Risks and Countermeasures to them from 07th – 16rd June 2017 in Japan.

5.2.2 Drills and Exercises (Online)

- Participating the APCERT Drill on 22 March 2017.
- Joint the ASEAN–Japan Cyber Exercise on 18th May 2017.
- Joint the ASEAN CERT Incident Drill (ACID) on 11 September 2017.

5.2.3 Seminar and conference

- Joint the 1st ASEAN-Japan Information Security WG on Cyber Exercise, CIIP and Capacity Building Meeting on 06th – 07th February 2017 in Manila, Philippine.
- Joint the 2nd ASEAN-Japan Information Security WG on Cyber Exercise, CIIP and Capacity Building Meeting on 27th – 28th April 2017 in Kuala Lumpur, Malaysia.
- Attended the ASEAN Cyber Norms Workshop on 8th – 9th May 2017 in Singapore.
- Attended the China-ASEAN Network Security Emergency Response Capacity Building Seminar on May 22nd - 24th, 2016 in Qingdao, China.
- Joint the 3rd ASEAN-Japan Information Security Joint Working Group Meeting on 11th – 14th July 2017 in Tokyo, Japan.
- Attended the Countering On-line Extremist Messaging from 18th -22nd July 2017 in Malaysia.
- Attended the International Law Applicable to Cyber Operations from 28th – 31st August 2017 in Singapore.

- Joint the Workshop on International Cyber Security Policy and Diplomacy for CLMV Countries 12th – 13th October 2017 in Hanoi, Vietnam.
- Attended the 10th ASEAN-Japan Information Security Policy Meeting 10th-11th October 2017 in Singapore.
- Joint the Cyber Security Incident Handling for Government agencies ICT Officials from 25th - 27th October 2017 in Philippine.
- Participating the APT seminar on Cybersecurity on Data Driven Society from 24th -26th October 2017 in Bangladesh.
- Attended the 5th Global Conference on Cyber Space from 22-25 November, 2017 in India.

6. Future Plans

- 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 awareness data protection Law.
- Drafting National Cyber Security Policy.
- Studying National Cyber Security Strategy.

7. Conclusion

LaoCERT is a developing team, we are trying a lot to be a developed and matured team by delicately doing Incident Handling, Cybersecurity Researches, efficiently providing technical advisories, trainings, seminars and workshops to constituencies and doing research on Log Data Analysis as much as we can, LaoCERT enhance Public Awareness Activities and promoting International and National Cooperation for CERT Activities. However, some of our plan are not archived in 2017, we endeavor to continue to archive in 2018 by look forward for supporting and helping from other CERTs and International organization related to cyber security.

mmCERT

Myanmar Computer Emergency Response Team – Myanmar

1. Highlights of 2017

1.1 Summary of major activities

- Collaborate with "Crime Investigation Department (CID)" of Myanmar Police Force to solve the cyber crime cases.
- Giving seminars, workshops and sharing the knowledge to the student of "University of Computer Studies, Yangon (UCSY)", Crime Investigation Department (CID) and "Government Technological College (GTC)".

2. About CSIRT

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 since 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

Members of mmCERT include from one ministry: Ministry of Transport and Communication (MOTC). The operation of mmCERT was directly managed by Information Technology and Cyber Security Department and total five members worked for mmCERT last year. The number of members didn't increase in 2017.

2.4 Constituency

mmCERT has been enhancing for disseminating security information and advisories

and providing technical assistance to his constituencies. These are financial, governmental, research and education, internet service provider, vendor and economy.

3. Activities and 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 2017. According to the results on incident analysis by mmCERT, Intrusion and Malicious cases were the most prominent incident cases in 2017.

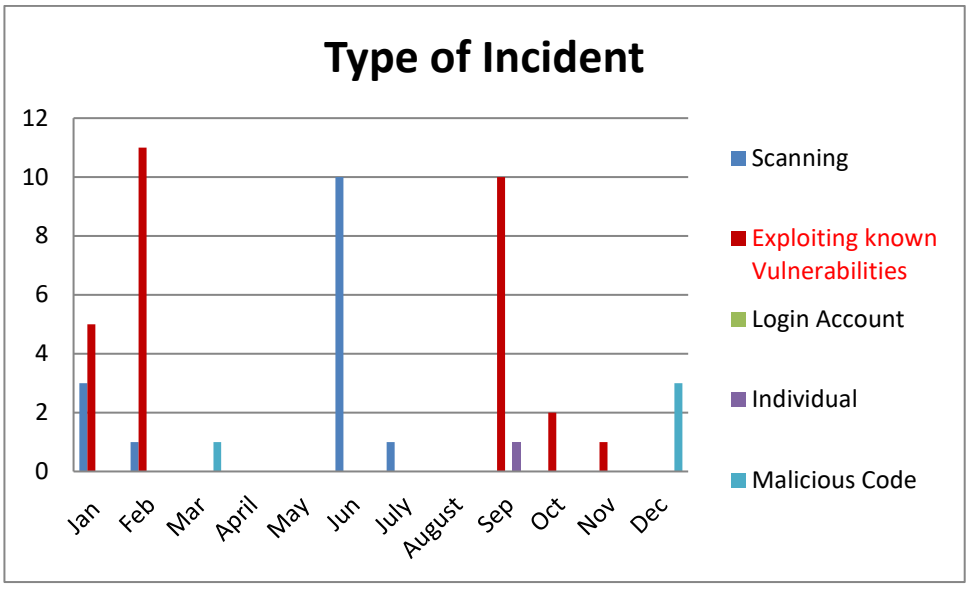


Figure 2 Type of Incident

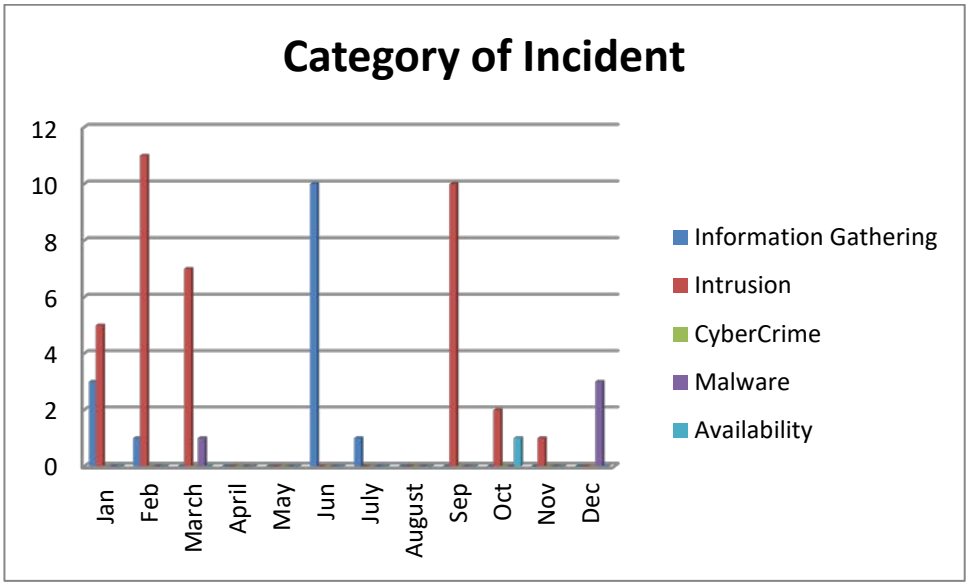


Figure 3 Category of Incident

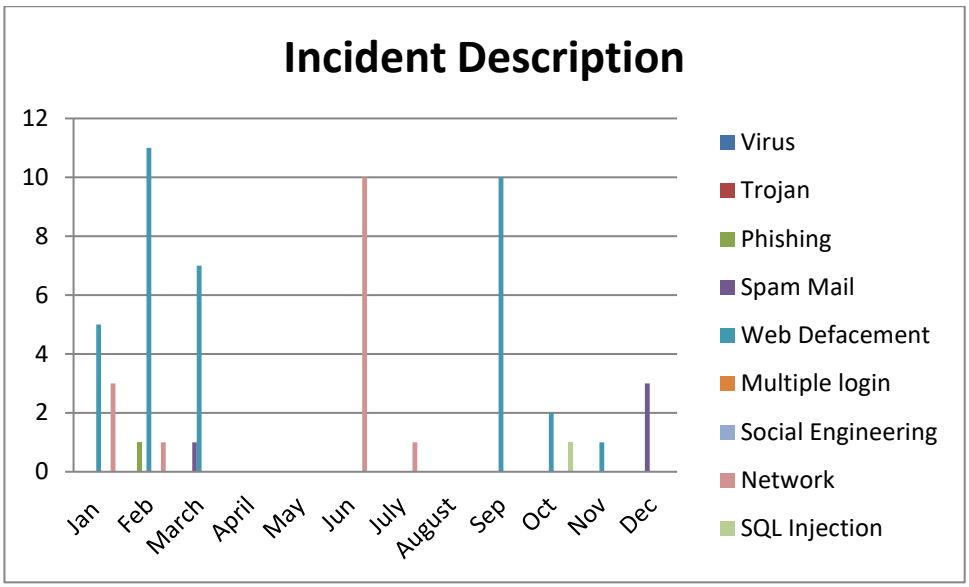


Figure 4 Description

4. Events Organized/Co-organized

4.1 Training

- Attending CEH Training at MCIT, Yangon (May 2-6, 2017)
- Attending the training on Policy and Cyber Security for Safeguarding Public Safety at Naypyitaw (October 30th – 1st November, 2017)
- Attending the training Cyber Security and Digital Forensics at University of Computer Studies Yangon (19th December 2017 to 5th January 2018)

4.2 Conferences and Seminars

- Giving Seminar to Cyber Crime Unit (Myanmar Police Force) at CID, Insein in Yangon on January 1st, 2017.
- Giving Seminar to Cyber Crime Unit (Myanmar Police Force) at CID, Insein in Yangon on May 24th, 2017.
- Participating in JICA-NEC One Day Seminar: Cyber Trend and MINI CYBER EXERCISE at Yangon (1st September 2017)
- Giving Seminar to Cyber Crime Unit (Myanmar Police Force) at CID, Insein in Yangon on Sept 18th, 2017.
- Participating in e-Government Conference & ICT Exhibition 2017 at Naypyitaw (November 7-8, 2017)

5. International Collaboration

5.1 Capacity Building

5.1.1 Training

- Attending Defense Practice Against Cyber Attacks at Tokyo, Japan (February 20 - March 3, 2017)

5.2 Conferences, Seminars and Workshop

- Attending Australian Cyber Security Centre at Canberra, Australia (March 14 - 16, 2017)
- Attending China-ASEAN Network Security Emergency Response Capacity Building Seminar at Qingdao, China (May 22-24 2017)
- Attending ASEAN-JAPAN Workshop on PII Protection and Released Issues at Singapore (27th July, 2017)
- 2017 Seminar on Telecommunication Network Security and Optimization for Developing Countries at Wuhan, China (September 18th to October 17th, 2017)
- Attending Workshop on International Cyber Security Policy and Diplomacy for CLMV Countries at Hanoi, Vietnam (October 12- 13, 2017)

5.2.1 Drill& Exercises

Drill

- Participating in APCERT Drill on March22, 2017. APCERT Drill 2017 Title is "Emergence of the New DDoS Attack"

- Participating in ACID Drill on September11, 2017. ACID Drill 2017 Title is "The Dangers of Insufficient Authentication and poor Access Control"

Cyber exercises

- Participating in ASEAN –JAPAN Cyber Exercise 2017.

6. Future Plans

6.1 Future projects

- Government Security Operation Center
- Government Secure Service Network
- Penetration Testing Labs

7. Conclusion

As being mmCERT is a developing team, we are trying very much for 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.

MNCERT/CC

Mongolia Cyber Emergency Response Team / Coordination Center – Mongolia

1. Highlights of 2017

1.1 Summary of major activities

MNCERT/CC has successfully organized MNSEC 2017 annual event which has covered pretty large scope and allowed the participants to exchange their experience and knowledge.

"Kharuul Zangi 2017" and "Kharuul Zangi U18 2017" cyber security competitions have been held successfully by MNCERT/CC.

1.2 Achievements and milestones

Year 2017 was a full of achievements for MNCERT/CC. One of the main activities was providing its member organizations with security threat news feeds, recommendations, consulting and trainings.

One of the key achievements of this year was continuation of "Kharuul Zangi U18 2017" cyber security competition which was organized among high school senior grade students. 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.

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 appoint 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 – 2

2.4 Constituency

Our constituencies are:

- Internet Service Provider Companies
- Banks
- Mobile Operator Companies
- Universities

- MonCIRT
- General public

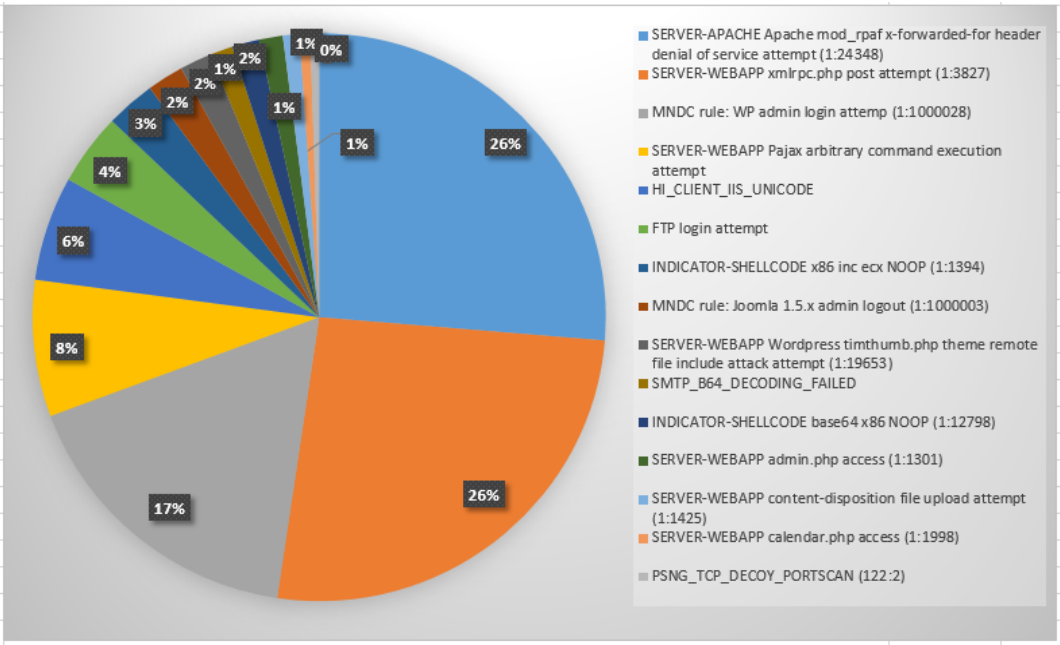
3. Activities & Operations

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 acitivities carried out by MNCERT/CC during the year 2017 is given in the following chart. This chart shows about summary of the critical incidents and attempts that were registered: DoS attempt using vulnerability of Apache server "mod_rpaf" module 26%, attempts to inject malicious code using "xmlrpc.php" module from unauthorized users 26%, attempts to login as an admin to Wordpress web site 17%, attempt to execute malicious code by using Pajax web application 8%, attempts of HI_CLIENT_IIS_UNICODE 6%, attempts to login through FTP 4% and others 13%.



3.3 Publications

- "Practical Recording of All TTY Sessions", Mr.Ganbold Tsagaankhuu, MNCERT/CC advisor.
- "The changing role of states in cyberspace", Mr.Galbaatar Lkhagvasuren, MNCERT/CC board member.

4. Events organized / hosted

4.1 Training

4.1.1 FIRST Fusion and ENISA Webserver Forensics Training

MNCERT/CC, FIRST and APNIC has organized the FIRST FUSION and Webserver Forensics training in Mongolia during 25-27th September 2017 at National IT Park of Mongolia. The training has been instructed by Adli Wahid, a senior internet security specialist of APNIC, Michael Hausding, a security specialist of SWITCH-CERT and Pawel Pawlinski, a security specialist of CERT Polska. The training has covered theoretical and practical aspect of webserver forensics and cyber incident response.
Overall 21 professionals from various industries have been participated in the training. The participant industries include

- Banking sector – 10 people
- Operator company – 4 people
- Government agency – 3 people
- National data center – 2 people
- IT Service company – 2 people

4.1.2 Local Training

On 29th September, MNCERT/CC have conducted two kinds of trainings among security engineers of public and private sectors during MNSEC 2017 event. The training subjects were "Essential security utilities" and "Practical malware analysis", which instructed theoretically and practically by MNCERT/CC security researchers.

4.2 Drills & Exercises

4.2.1 MNCERT/CC Cyber Drill 2017

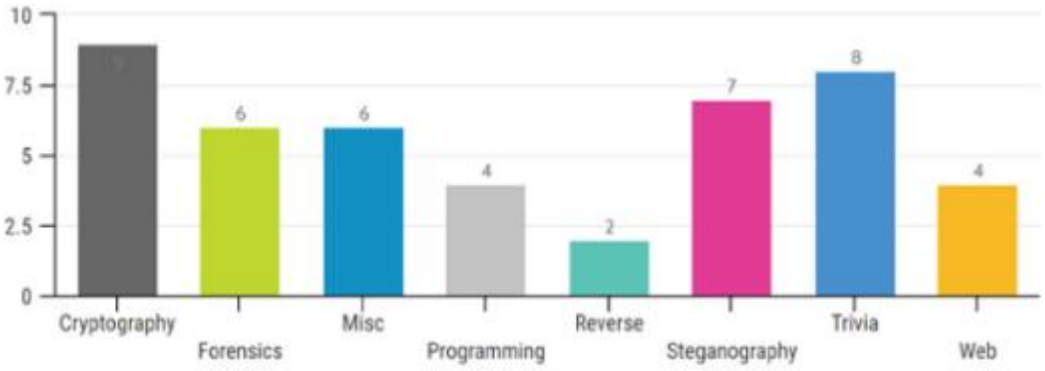
MNCERT/CC has organized the local cyber drill among the member and non-member organizations in 17th May of 2017. The goal of the drill was to practice incident response capability of local organizations. The scenario simulated the infection of ransomware

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 2017" 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 general public. We have successfully organized "Kharuul Zangi 2017" competition between 16th September to 29th September of 2017, in collaboration with Mongolian national data center, National cyber security department, "SafeBit" LLC, National information technology park 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 165 teams of 495 members, 30 teams qualified from the 1st stage. Total of 46 tasks of 8 categories have been given to be completed at 1st stage and 32 tasks have been completed out of them by the competitor teams. Following chart shows the knowledge level of the participants who completed 8 different tasks on the 1st stage.



After the 2nd stage, 10 teams were qualified to final stage. 3rd stage of the competition has been held on 29th September 2017, on MNSEC 2017 event.

Score board of "Kharuul Zangi 2017" contest

4.2.3 "Kharuul Zangi U18 2017" Cyber Security Competition

MNCERT/CC has initiated and organized cyber security competition named "Kharuul Zangi U18 2017" among the high school students under the age of 18 on May 2017. The competition goal is to provide knowledge about possible danger caused by the cybercrime and to increase cyber threat awareness for high school senior grade students.

Totally 164 competitors of 41 teams have challenged for the competition. 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.

4.3 Conferences and seminars

4.3.1 MNSEC 2017 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 the Mongolia and information security is one of them. Therefore, we have organized

MNSEC 2017 event on 28th and 29th September of 2017 at the Corporate Convention Center providing the opportunity to share experience, necessary information, knowledge, technology and new solution within the security community. We have been organizing this event annually since 2012 in Information technology 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 2017 event has been conducted successfully with the great contribution from Team Cymru, APNIC, SWITCH-Cert, CERT Polska, FIRST and Arbor Networks. 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.

This event covered some of the most popular topics in cyber security field, therefore about 224 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.

4.3.2 GOVSEC 2017 event

On 28th April of 2017, Mongolian National Data Center, MNCERT/CC, State Information and Communication Department, Communications and Information Technology Authority, Cabinet Secretariat of Government of Mongolia, Law Enforcement University of Mongolia and National Security Council of Mongolia has jointly organized the "GovSec 2017" event among governmental organizations. The goal of this event was to determine the information security vital issues in introducing the information technology progress to the governmental organizations activities and public services and to provide the participants with possibility to exchange the experiences and ideas of strategic policy and newly developed technologies. The event has covered specifically the manager, IT specialists and security experts in the governmental organizations.

Following presentations were presented on GOVSEC 2017 event on behalf of MNCERT/CC:

- "International and Mongolian case study of attacks towards government", Mr. Enkhsaikhan Pagva, MNCERT/CC board member.
- "Report of MNCERT/CC", Mr. Naranbat Jargalsaikhan, MNCERT/CC executive director.

- "Trend towards cyber security international cooperation", Mr. Galbaatar Lkhagvasuren, MNCERT/CC board member.
- "About activities of Cyber Security Operation Center", Mr. Sandagsuren Ganbat, MNCERT/CC board member.

5. International Collaboration

5.1 International partnerships and agreements

- APCERT
- TEAM CYMRU
- FIRST
- APWG
- FS-ISAC

5.2 Capacity building

5.2.1 Training

- Attended on online webinar trainings organized by TWNCERT.
- Attended on 2017 APISC Security Training Course

5.2.2 Drills & exercises

- Participated in APCERT Drill 2017 on March, 2017

5.2.3 Seminars & presentations

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

- 2017 FS-ISAC APAC SUMMIT on April in Singapore.
- Team Cymru Underground Economy Annual Event on September in Spain.
- Black Hat Asia 2017 on March in Singapore.

6. Future Plans

6.1 Future Operations

MNCERT/CC planned the following activities in 2018.

Events, conferences and drill to participate are as follows:

- APCERT Drill 2018 on March 2018.
- FIRST Annual Conference 2018 on June in Kuala Lumpur, Malaysia.
- APCERT Annual General Meeting 2018 on October in Shanghai, China.

Activities to organize are as follows:

- MNSEC 2018 Cyber Security Event
- "Kharuul Zangi U18 2018" Cyber Security Contest among high school students
- "Kharuul Zangi 2018" Cyber Security Contest among IT specialists.
- Local cyber drill among member organizations.

7. Conclusion

2017 was the year of great success and progress for MNCERT/CC, 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 2018 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 2017

1.1 Summary of Major Activities

During the year 2017 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;
- Conducted workshops to assist the constituency in improving information security for business;
- Maintenance of a website as point of reference for MOCERT services;
- Speech to IT staffs of the constituency at a local event called SAFE-T Summit;
- Assisted in the APCERT Policy Procedure and Governance Working Group;
- Involved in the TSUBAME Working Group;
- Assisted in the APCERT Drill 2017 as OC, Player, Observer and EXCON;
- Article publications in a local magazine called “Macau-ICT”.

1.2 Achievements & Milestones

1.2.1 Presentation

1st Dec 2017 – Speech at SAFE-T Summit

In a local event called SAFE-T Summit 2017, MOCERT delivered a speech titled "Your Enemy in Your House" regarding the security of Windows Powershell and its possible attack vectors.

1.2.2 Memorandum of Understanding (MOU) between MOCERT and JPCERT/CC

The MOU between MOCERT and JPCERT/CC was renewed in June 2017 to continue the goal in establishing and strengthening a strategic collaboration that aims to improve collective information security efforts between MOCERT and JPCERT/CC.

2. About CSIRT

2.1 Introduction

MOCERT (Macau Computer Emergency Response Team) is service that is public facing

from MANETIC (Macau New Technologies Incubation Centre).

This service is funded by MANETIC, an organization that is supported through industry and government 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 Macau.

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 in secondary, tertiary as professional audiences.

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, Macau.

2.3 Workforce Power

The staffing for the MOCERT service is sourced from MANETIC's pool of computer security professional and support staff. As of the year ending 2017 there are two (2) staff providing the service with two (2) 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 Macau with computer security incident handling information, promoting information security

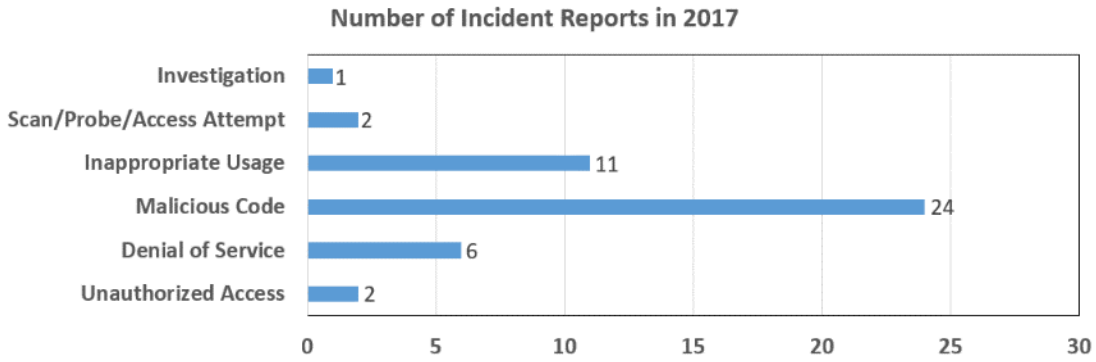
awareness, as well as coordinating on an international and local level, computer security issues, advisories, incident response, and research for the Macau public and local enterprises.

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. Reluctance from reporting issues provides a challenge in addressing the cyber security of Macau.

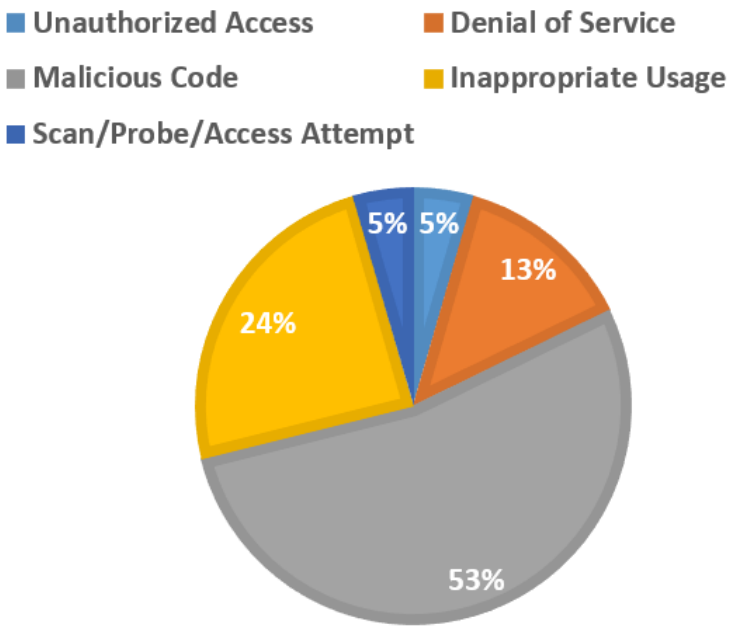
Sources of incidents are from three distinct channels.

1. Reported by Web
2. Reported by E-mail message
3. MOCERT initiated from incident discovery activity.



3.3 Abuse Statistics

The following pie graph denotes the abuse distribution as noted for the year 2017. The numbers are drawn from the incidents handled.



3.4 Publications

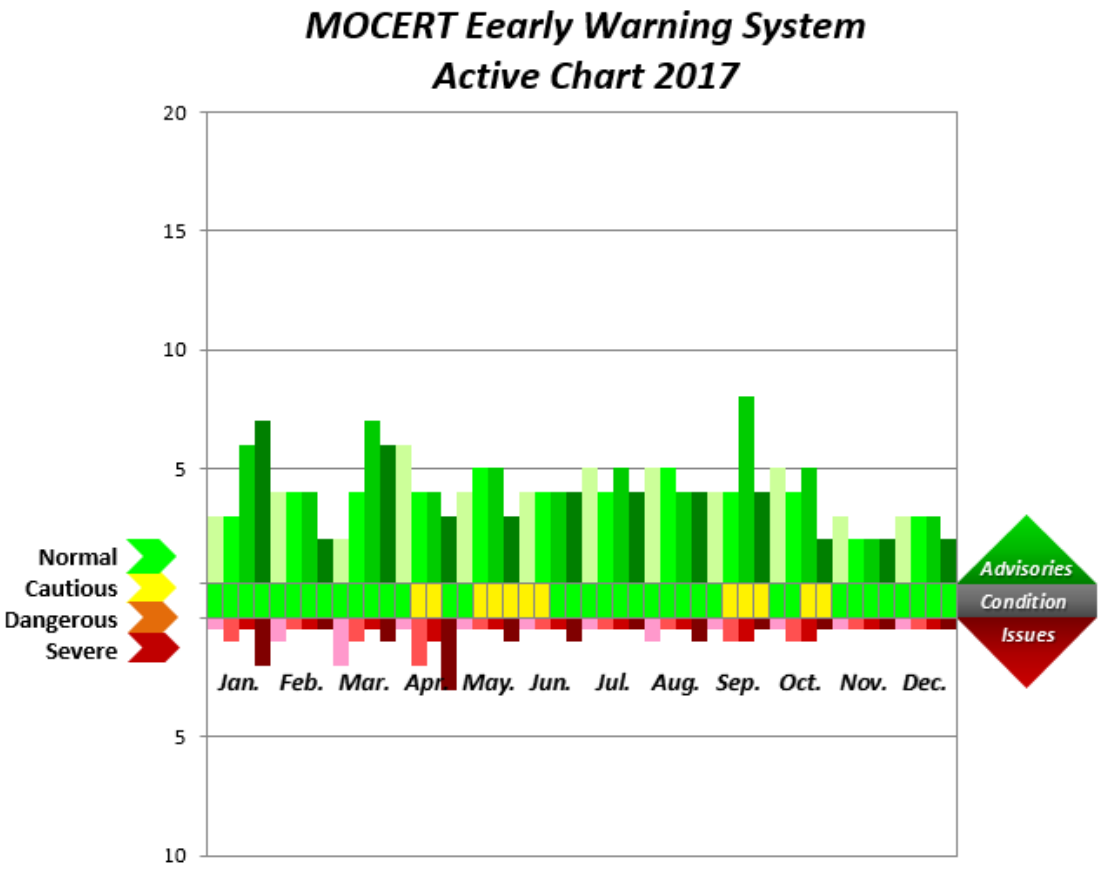
3.4.1 Articles

MOCERT published articles in a local magazine called "Macau-ICT". The magazine is distributed free of charge to the constituency.

- Macau-ICT ISSUE 25
  Title: Infection, Prevention, and the Future of Ransomware
  Link:
  http://www.manetic.org/index2.php?option=com_flippingbook&view=book&id=35:issue-25&catid=3:macau-ict&tmpl=component
- Macau-ICT ISSUE 24
  Title: Introduction to Website Penetration Testing Tool "OWASP MANTRA"
  Link:
  http://www.manetic.org/index2.php?option=com_flippingbook&view=book&id=34:issue-24&catid=3:macau-ict&tmpl=component

3.5 Early Warning Notices

A website collects notifications related to computer security, where all notifications are reviewed by staff to determine the impact to Macau constituency. The notifications are then classified to Issues and Advisories and then posted. The following diagram shows the distribution of the 216 postings in 2017 with 194 postings being Advisories, and 22 Issues.¥



4. Events Organized / Hosted

4.1 Training

Staffs in MOCERT service a 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.

4.2 Conferences and Seminars

MOCERT jointly hosted with the Macau New Technologies Incubator Centre (Manetic) and Macau Association of Systems Engineering (MASE), and co-organized with Public Administration and Civil Service Bureau (SAFP), and supported by Macau Science Centre (MSC), an event "SAFE-T Summit 2017" on the 1st December at Macau Science Center.

This annual event provides an opportunity to link the professionals in Macau. Guests from various organizations shared IT security related real-world cases and solutions to more than 150 audiences. During the summit, MOCERT delivered a speech titled "Your

Enemy in Your House". The speech shared possible attack vectors regarding the security of Powershell.

Through this platform, it is believed that more valuable and forward-looking information security knowledge can be introduced to Macau. Local citizens and all interested parties are also able to learn more about current age of internet from a professional prospective.

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 actively participated in APCERT online training courses held in 2017.

5.2.2 Drills & Exercises

- APCERT Drill

  The involvement in 2017 in the APCERT drill included as a Player, Observer and EXCON. Also MOCERT assisted the Drill Organising Committee in preparing the Drill artifact and designing the Detailed Scenario.

6. Future Plans

6.1 Future Projects and Operation

Future projects will mainly focus on the provision of more IT security consultancy services for the constituency. MOCERT will still provide on-demand training courses, incident handling services, and hold the annual cybersecurity conference for the constituency. Also, MOCERT will keep improving the Early Warning System and continue to collaborate with local and international members on incident handling and information sharing.

7. Conclusion

2017 has been a year where MOCERT provided further vulnerability assessment and penetration testing services for local enterprises.

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 these changes are done progressively in the next few years 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 as allow our financial situation. 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 education 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. Due to absence of any financial support and self-financing we constantly feel shortage of the qualified experts.

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, high schools and other educational organizations.

2. Activities & Operations

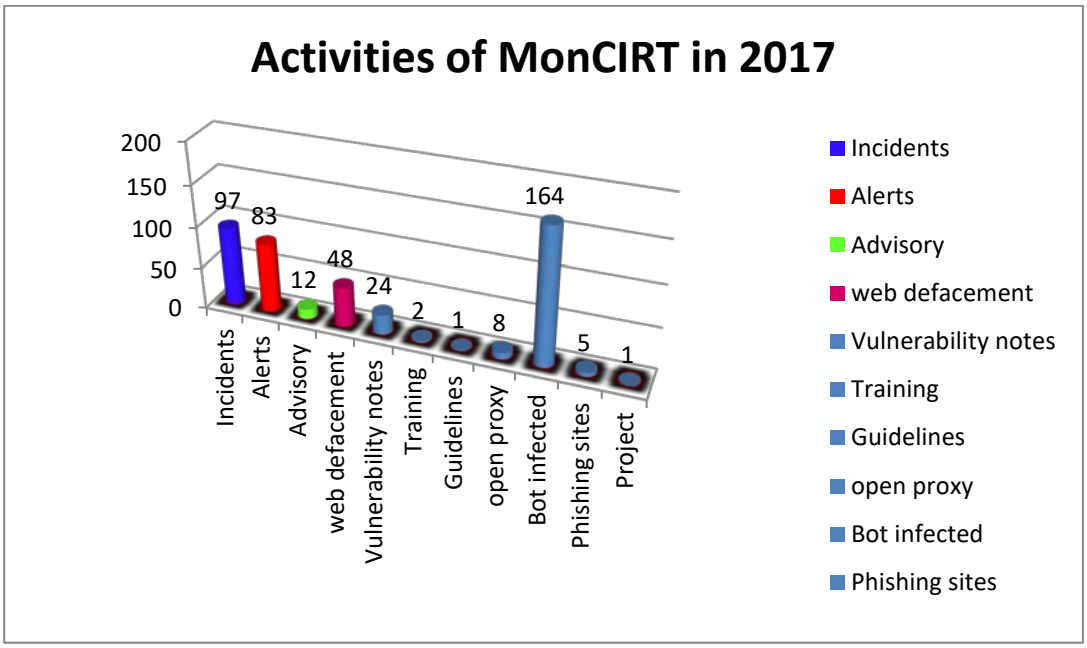
2.1 Summary

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 2017, we are in the midst of this security period. The summary of activities carried out by MonCIRT during the year 2017 is given in the following table:

Activities	Year 2017
Security Incidents handled	94
Security Alerts issued	83
Advisories Published	12
Vulnerability Notes Published	24
Security Guidelines Published	1
Trainings Organized	2
Mongolian Website Defacements tracked and	48

advised	
Open Proxy Servers tracked	8
Bot Infected Systems tracked	164
Phishing (mirror) web sites tracked and removed	5
Projects	1

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



The majority of internet threats in Mongolia in 2017 are delivered from previously unknown sources and not popular web sites that have been hacked for use by cybercriminals. From the sudden spread of WannaCry and Petya/NotPetya, to the swift growth in coinminers, 2017 provided us with another reminder that digital security threats can come from new and unexpected sources. With each passing year, not only has the sheer volume of threats increased, but the threat landscape has become more diverse, with attackers working harder to discover new avenues of attack and cover their tracks while doing so.

Phishing attacks overwhelmingly come from unknown sources hacked by cybercriminals.

From January through December 2017, the MonCIRT received 368 email messages and more than 100 hotline calls reporting computer security incidents or requesting information. More than 100 of these messages, information was related with real

incidents and we provided with recommendations. We received 28 vulnerability reports and handled 94 computer security incidents during this period. We cannot retrieve incident handling statistics from organizations, administrators due to executive's restriction.

We continue to provide advice to computer system administrators, users in the Internet community who report security problems. We established regular dialog with system administrators of organizations and to offer information on state of Internet security to the system administrators, network managers, and others in the Internet community.

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 2017 MonCIRT handled several incidents related with Coin mining attacks explode, Software Supply Chain attack, Ransomware, Mobile malware attack, use of Zero days.

Cyber criminals in Mongolia and neighbor countries who have been firmly focused on ransomware for revenue generation are now starting to explore other opportunities. During the past year, the astronomical rise in crypto currency values inspired many cyber criminals to shift to coin mining as an alternative revenue source. This coin mining gold rush resulted in an 6,200 percent increase in detections of coinminers on endpoint computers in 2017.

With a low barrier of entry—only requiring a couple lines of code to operate—cyber criminals are using coinminers to steal computer processing power and cloud CPU usage from consumers and enterprises to mine crypto currency. While the immediate impact of coin mining is typically performance related—slowing down devices, overheating batteries, and in some cases, rendering devices unusable—there are broader implications, particularly for organizations. Corporate networks are at risk of shutdown from coinminers aggressively propagated across their environment. There

may also be financial implications for organizations who find themselves billed for cloud CPU usage by coinminers.

Despite the EternalBlue exploit wreaking havoc in 2017, the reality is that vulnerabilities are becoming increasingly difficult for attackers to identify and exploit.

As we observed the hijacking software updates provides attackers with an entry point for compromising well-protected targets, or to target a specific region or sector. Few Mongolian entities reported that became victims of Petya/NotPetya (Ransom.Petya). As show our investigation after exploiting organization's accounting software as the point of entry, Petya/NotPetya used a variety of methods, spreading across corporate networks to deploy the attackers' malicious payload. We observed more than 10 cases of infection of WannaCry Trojan-Ransom.Win32.Wanna. Also there was 2-8 cases of infections of Locky Trojan-Ransom.Win32.Locky, Jaff Trojan-Ransom.Win32.Jaff, Spora Trojan-Ransom.Win32.Spora, Purgen/GlobeImposter Trojan-Ransom.Win32.Purgen, Shade Trojan-Ransom.Win32.Shade, CryptoWall Trojan-Ransom.Win32.Cryptodef e.t.c.

In 2017, the ransomware 'market' made a correction with fewer ransomware families and lower ransom demands—signaling that ransomware has become a commodity. Many cyber criminals may have shifted their focus to coin mining as an alternative to cash in while crypto currency values are high.

Some online banking threats have also experienced a renaissance as established ransomware groups have attempted to diversify. Below is shown some malware families most commonly used in 2017 to attack Mongolian banking users:userstacked**

1 Trojan-Spy.Win32.Zbot

2 Trojan.Win32.Nymaim

3 Trojan-Banker.Win32.Gozi

4 SpyEye

5 Trojan.Win32.Neurevt

6 Backdoor.Win32.Shiz 2.4

7 Caphaw 3.0

8 Trickster 2.8

MonCIRT has found that overall targeted attack activity in Mongolia is up by 10 percent in 2017, motivated primarily by intelligence gathering. However, a not-so-insignificant 10 percent of attack groups engage in some form of disruptive activity.

Spearphishing is the number one infection vector in Mongolia. The use of zero days

continues to fall out of favor. In fact, only 20 percent of the 18 targeted attack groups that MonCIRT tracks have been known to use zero-day vulnerabilities at any point in the past.

Threats in the mobile space continue to grow year-over-year. The number of new mobile malware variants increased by 50 percent in 2017, as compared to 2016. And last year, an average of 8000 malicious mobile applications were observed each quarter.

As show internet user's reports the exploits for Adobe Flash Player and Internet Explorer vulnerabilities have been in decline, replaced by Microsoft Office exploits.

We are seeing a substantial growth in attacks targeting Microsoft Office users. The main reason for that was the numerous zero-day vulnerabilities found in Office over the last 12 months. Binary memory corruption vulnerabilities CVE-2017-0261, CVE-2017-0262, CVE-2017-11826 were used in APT attacks. Exploits for three 'logical' vulnerabilities – CVE-2017-0199, CVE-2017-8570, and CVE-2017-8759 – have been the go-to exploit for most spear-phishing attacks this year.

Exploits for Android also showed a 5% increase, accounting for 25% of all exploits. Last year's rapid growth continues, mostly due to an increasing number of exploits that facilitate root privilege escalation on Android mobile devices.

The damage caused by network worms, Trojans and ransomware cryptors being distributed via the Mongolian network with the help of EternalBlue and EternalRomance SMB exploits, as well as the number of users infected, is incalculable.

In the yearly statistics for network attacks blocked by IPS's of organizations, we saw the Intrusion.Win.MS17-010.* verdict become one of the most exploited network vulnerabilities in the space of just a few months.

In 2017, we received reports on 5284 malware attacks launched from web resources located in various countries around the world.

More than 80% of notifications about attacks blocked by antivirus components were received from online resources located in 10 countries as show below: USA 33%, Russia 23%, China 18,5%, Netherlands 11,4%, Germany 8,9%, Ukraine 2,3% and others.

As show our monitoring component the malware delivery networks are now hiding in legitimate sites that are typically allowed by acceptable use policies. As shows below the 10 malicious programs most actively involved in online attacks launched against Mongolian internets users in 2017.

1. Maliciuos URL: 76%
2. Trorjan.Scrict,Generic: 6,4%
3. Trojan-Clicker.HTML.lframe.dg: 1.83%

4. Trojan.JS.Miner.d 1,1%
5. Trojan.JS.Small.ci 1.0%
6. Packed.Multi.MultiPacked.gen: 0,62%
7. Trojan-Downloader.JS.Agent.npe: 0,32%
8. Trojan-Dropped.VBS.Agent.bp: 0,1%
9. Trojan.JS.Agent.dvu: 0,08%
10, Trojan-Downloader.Scrict.Generic: 0,08%

Other scripts perform different malicious activities. For example, Trojan.JS.Small.ci aggressively injects third-party ads into traffic, Trojan.JS.Miner.d is a web miner, Trojan.JS.Agent.sileof is the detection for fraudulent resources that lock browsers with constantly generated fake messages about infections.

MonCIRT identified the most frequently detected threats on Mongolian Internet user computers in 2017. This rating does not include the Adware and Riskware classes of program.unique sers**

1 DangerousObject.Multi.Generic 32.6%
2 HackTool.Win32.KMSAuto.i 8.21%
3. Trojan.Script.Generic 8.17%
4 Trojan.Multi.GenAutorunReg.a 8.1%
5 Trojan.WinLNK.Runner.jo 5.5%
6 Trojan.WinLNK.Agent.gen 4.69%
7 Trojan.WinLNK.StartPage.gena 4.2%
8 Trojan-Downloader.Script.Generic 3.6%
9 Trojan.Win32.AutoRun.gen 3.5%
10 HackTool.Win32.KMSAuto.c 3.3%
11 Virus.Win32.Sality.gen 3.1%
12 Trojan.Multi.Powecod.a 2.9%
13 Trojan.Win32.Starter.yy 2.6%

When we receive a vulnerability report, our vulnerability expert analyze the potential vulnerability and will try to connect with producers via suppliers in Mongolia to inform them of security issues identified in their products.

We observed some attack techniques and exploits as shown below:

- **IoT vulnerabilities** – Several IoT vulnerabilities hit the headlines throughout the past year, with multiple attacks and campaigns targeting them.

- **SMB propagation** – Several SMB vulnerabilities, EternalBlue, EternalRomance and more, which were allegedly discovered and exploited in Mongolia.
- **RTF** – Security flaws in Microsoft Office Rich Text Format (RTF) were widely abused in Mongolia by threat actors throughout 2017.
- **DDE – Marco-less code execution** – Microsoft Dynamic Data (DDE) Exchange is a legitimate feature that has been widely abused into an attack vector as of late 2017.

Another source of vulnerability information comes from incident analysis. Repeated incidents of the same type often point to the existence of a vulnerability and, often, the existence of public information or automated tools for exploiting the vulnerability.

For Mongolia we calculated the number of file antivirus detections users faced during the year. The data includes malicious programs located on user computers or on removable media connected to computers, such as flash drives, camera and phone memory cards, or external hard drives. As show our monitoring and foreign suppliers reports Mongolia is one of the most PC infected countries in the world. 55 of 100 personal computers in Mongolia can be infected with any malware. Top malware which we summarized is as below: Coinhive, RoughTed, Necurs, Locky, GlobeImposter, Andromedia, Fireball, Conficker and others.

2017 was a particularly interesting year in the malicious email distribution market in its various forms, as some distributors were taken down but others once again reared their heads.

Ever since we found Viking Horde, the first widespread Android botnet on Google Play, we have long foreseen that the use of Android botnets for DDoS attacks is just around the corner.

This year, a new mobile botnet called WireX spread in Mongolia through Google Play. It was used to conduct volumetric DDoS attacks at the application layer, shutting down websites. As it is easy to reach a widespread infection by imbedding malicious code in apps on Google Play, mobile botnets are the perfect weapon for mass DDoS attacks, and will continue to trouble us in the future.

2.3 New services

2.3.1 Anti new attacks System

During 2018-2019 MonCIRT plan to deploy “Anti new types of attacks” System (Blockchain attacks, Cloud attacks, IoT attacks, Cross platform attacks, Mobile attacks) together with 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 percents.

2.3.2 Digital Forensics

Our founders Professor Khaltar T and Mr Baasandorj N (SANS certified ethical hacker, forensic analyst) organized training on digital forensic for staffs of law enforcement organizations, experts of Forensic Analyze Center of Mongolia and Law Enforcement University of Mongolia. In addition thanking to the MonCIRT's proposal the Government of Mongolia allocated resource for implementing project "National Digital Forensic Laboratory".

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. One course offering are geared toward educating policymakers, managers, and senior executives who are responsible for the security of information assets and based in MNS ISO/IEC 27001, 27002, 27005, 27033.

Courses offered in 2017 included the following:

- Network security management and configuration
- Handling techniques of Ransomware, Zero day attacks
- Information and Network security risk management.
- Internal Information Security audit and Self evaluation
- Techniques for configuring Next Generation Firewalls and write rules.
- Fundamentals of Incident Handling and Management

In addition MonCIRT organized following workshops:

« Workshop on "Cloud Computing Security" on December 16, 2017

« Workshop on "Next generation firewall" on September 20, 2017
« Workshop on "Social network threats" on June 27-28, 2017

3.2 Drills

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

Cyber Drill V was planned and developed over two years and culminated in the conduct of a four day exercise between 03-06 October 2017. It was conducted as a 'no-fault' exercise, with the strategic level objective being to test and evaluate Mongolia's educational sector's new crisis management arrangements in order to most effectively address an international cyber security event of national significance. Complementary to this, Cyber Drill V participants' objectives included:

- Evaluating universities, organizations' capability to prepare for, protect from, and respond to cyber attacks' potential effects;
- Evaluating strategic decision making and inter-universities coordination of incident response(s) in accordance with policy and procedures;
- Validating information sharing relationships and communications paths for collecting and disseminating cyber incident situational awareness, response and recovery information; and
- Evaluating the means and processes through which sensitive information is shared across boundaries and sectors without compromising proprietary or national security interests.

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. These events included, for example, emails reporting problems and phone calls asking questions. The problems or incidents in the exercise were all simulated – no live systems were involved.

Cyber Drill V 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 first 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:

a. MonCIRT was one of the partner in organization of annual conference of National Military University dedicated to "Mongolian national security issues" and participated in development of "National security conception till 2030". The governing board director of MonCIRT prof Khaltar Togtuun was one of key speaker on this conference.
b. With sponsorship of Security Solution Service LLC and MonPass CA LLC (the first Certification Authority in Mongolia) organized annual "Security Open Day Mongolia 2017" seminar in December 12-13. Within these days it is successfully hold scientific & practical conference, fair and workshop.
c. Prof Khaltar T and Mr Khadkhuu A (executive director) invited and participated in seminars, conferences organized both in Mongolia or abroad and made some presentations on behalf of MonCIRT, for example CodeIB conference in Novosibirsk, Russia, March 30, 2017 and "Kazakhstan Security Systems - 2017" conference in Astana, Kazakhstan, September 26-28, 2017.

4. Achievements

4.1 Presentations

MonCIRT's board director participated and presented in 2 local conferences as key speakers. In these conferences they have presented following presentations:

a. Conducted presentations during the conference dedicated to Mongolian national security issues on themes "National Information Security Conception".
b. Conducted presentations during the Annual "Security Open Day" seminar on themes "Combat with zero day attack", "University information security issues".

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

4.2 Publications

The MonCIRT published 12 advisories and 24 vulnerability notes in 2017 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. On the day of release, we send advisories to a mailing list of CITA mailing list.

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
- Deploying next generation Firewalls e.t.c.

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 2017. We plan to apply for FIRST membership in 2018 and CNCERT/CC visited us for site visit report purpose.

5. International and Domestic Collaboration

5.1 MoU

In addition to being member of APCERT, MonCIRT renewed Memorandum of Understandings with JPCETT/CC.

5.2 Event participation

May 24th – 25th, 2017

“Annual conference of National Military University dedicated to “Mongolian national security issues”. Ulaanbaatar, Mongolia

March 28 – 30th, 2017

CodeIB conference

Novosibirsk, Russia

June 11-16, 2017
29th annual FIRST conference
San Juan, PR

September 26-28, 2017
"Kazakhstan Security Systems - 2017" conference
Astana, Kazakhstan

November 12-15, 2017
APCERT AGM & Conference.
Delhi, India

5.3 International incident coordination

Upon request of some security companies from Europe, USA and UK CERT we handled incidents related to 5 phishing web sites installed illegally in Mongolian web servers.

6. Future Plans

6.1 Future projects

We now working on deployment of own data room, therefore stopped some services such as email system, website e.t.c. Before we used rented hosts.

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 from this year MonPass CA LLC will finance incident handling, awareness building 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 2017 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

MyCERT

Malaysian Computer Emergency Response Team – Malaysia

1. HIGHLIGHTS OF 2017

1.1 Summary of major activities

25 February 2017	Participated in the APCERT Steering Committee Meeting, Ho Chi Minh City, Vietnam.
16 March 2017	Hosted a visit by the Department of Information and Communication Technology (**DICT**) of Philippines for them to understand cyber security requirement and infrastructure.
22 March 2017	Participated in the APCERT Drill 2017.
12-21 April 2017	Conducted internship programme on incident handling for the Bhutan Computer Incident Response Team (**BtCIRT**).
12-16 June 2017	Received the World Summit on the Information Society (**WSIS**) Prize Champion 2017 during the WSIS Forum 2017 in Geneva, Switzerland. A malware research project titled 'Collaborative Information Sharing Model for Malware Threat Analysis: A Case Study for the Organisation of the Islamic Cooperation – Computer Emergency Response Team' has received recognition from WSIS.
1 August 2017	Participated as the trainer for the APCERT online training on "Cyber Detection, Eradication and Forensic (**Cyber D.E.F**)".
14-23 August 2017	Conducted a capacity building training under the Malaysian Technical Cooperation Program (**MTCP**) attended by selected APCERT members titled "Certified Incident Management and Active Defence Training".
19 September 2017	Conducted the OIC-CERT Cyber Drill 2017 with the participation from the APCERT members with the theme "Encountering Cyber Terrorism & Human Trafficking".
9-16 October 2017	Organised the Cyber Security Malaysia - Awards, Conference & Exhibition (**CSM-ACE**) 2017.

13 October 2017	Organised the National ICT Security Discourse: CyberSAFE Challenge Trophy 2017 (**NICTSeD**), Kuala Lumpur.
6-9 November 2017	Conducted the OIC-CERT Annual Conference 2017 with the theme "*Uncovering Future Threats*" in Baku, Azerbaijan.
12-15 November 2017	Participated in the APCERT Annual General Meeting (**AGM**) & Annual Conference 2017, New Delhi, India.

2. ABOUT CYBERSECURITY MALAYSIA

2.1 Introduction

CyberSecurity Malaysia is the national cyber security specialist agency under the Ministry of Science, Technology and Innovation (MOSTI) 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 are:

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

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

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

iv. Cyber Security Strategic Engagement and Research:
   - Government/Multilateral Engagement; and
   - Strategic Research.

2.2 Establishment

CyberSecurity Malaysia started with the formation of the Malaysian Computer Emergency Response Team (**MyCERT**) on 13 January 1997. On 28 December 2005, the Malaysian Cabinet agreed to establish CyberSecurity Malaysia as a technical agency to monitor the National e-Security aspect. On 21 December 2017, a Memorandum of Agreement was signed between MOSTI and the National Security Council for CyberSecurity Malaysia to provide the necessary cyber security services to

the National Cyber Security Agency (**NACSA**). As the cyber security specialist and technical agency, CyberSecurity Malaysia is committed to 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 cyberspace.

2.3 The Malaysian Computer Emergency Response Team

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

MyCERT operates the Cyber999 Help Centre and Malware Research Centre providing technical support for incident handling and malware advisories and research, respectively. More information about MyCERT can be viewed at: https://www.mycert.org.my/en/

2.3.1 Cyber999 Help Centre

MyCERT operates the Cyber999 Help Centre providing an avenue to Internet users and organisations to report or escalate computer security incidents that threatens their personal or organisational security, safety or privacy. Channels for reporting computer abused and grievances to MyCERT's Cyber999 help centre are available at MyCERT's website at:

https://www.mycert.org.my/en/services/report_incidents/cyber999/main/detail/443/index.html

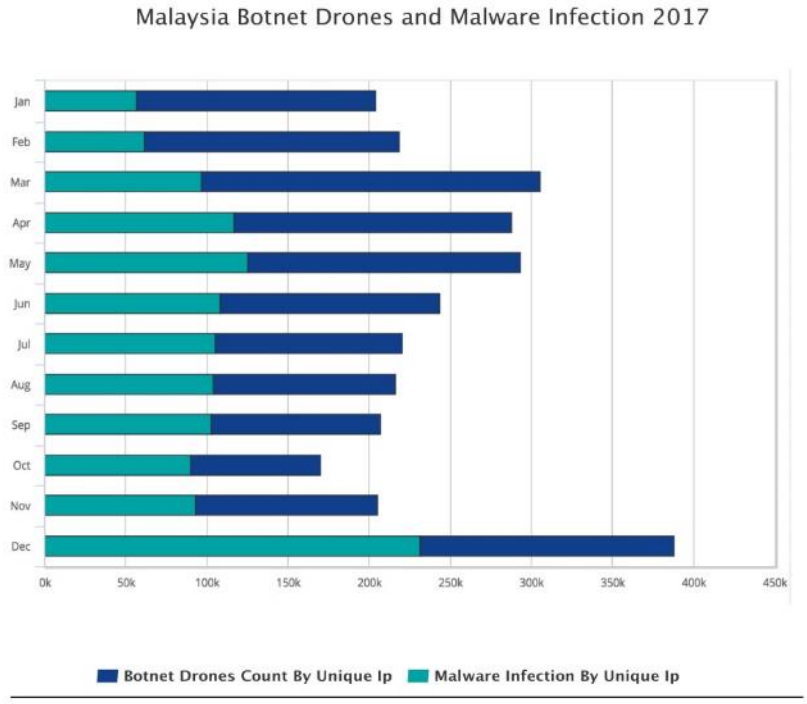
MyCERT, through its Cyber999 help centre, had responded to approximately 7962 incidents, with about 95% incident resolution in 2016. A significant number of incidents reported to MyCERT in 2017 were related to intrusion and fraud cases.

2.3.2 Malware Research Centre

Another valued service provided by MyCERT is the establishment of the Malware Research Centre (**MRC**). The centre has been in operation since December 2009 and functions as a research network for analysing malware and computer security threats. The centre conducts research and development work in mitigating malware threats, produce advisories, monitor threats and collaborate with other malware research

bodies.

The chart below shows the reported Malaysia Botnet Drones and Malware Infection 2017:



	JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC	TOTAL
Botnet Drones Count by Unique IP	147870	157238	208564	170921	168399	135899	115399	111825	104562	80178	112141	156977	1869973
Malware Infections by Unique IP	56237	61270	96800	116858	125018	107877	105242	104125	102614	89726	92931	231356	1290054
TOTAL	204107	218508	305364	287779	293417	220641	220641	215950	207176	169904	205072	388333	2960027

Chart 1: Reported Malaysia Botnet Drones and Malware Infection 2017

2.3.3 Constituency

MyCERT's constituency is the Internet Users in Malaysia. 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, MyCERT will request trusted parties in that particular 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

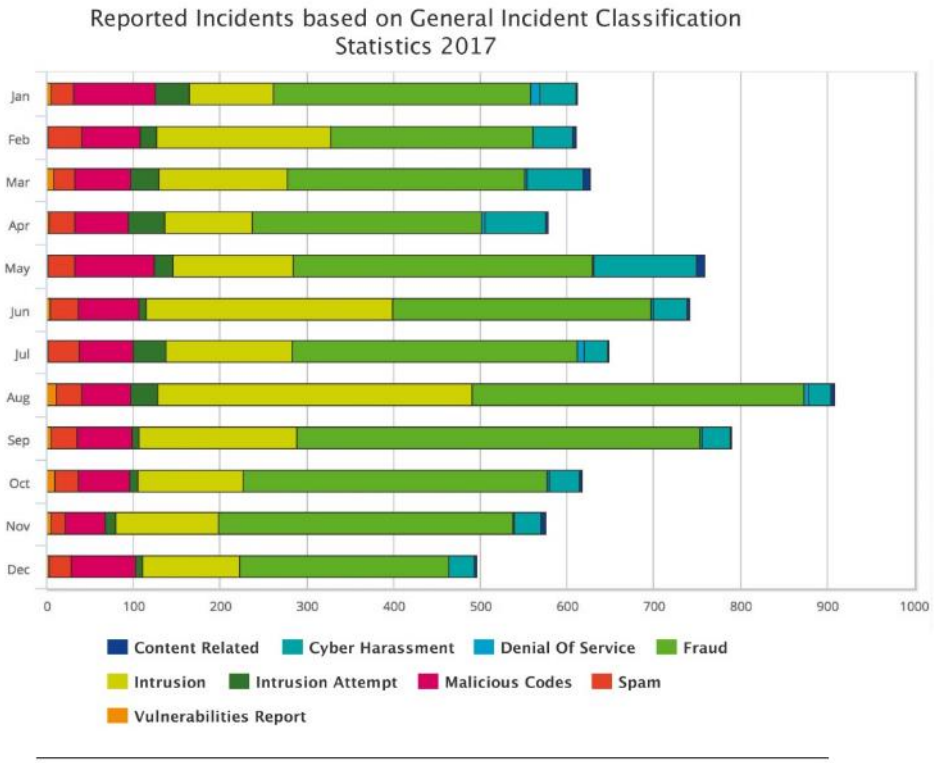
MyCERT receives reports from various parties within its constituency as well as from other constituencies. These include home users, private sectors, government sectors, security teams from abroad (foreign CERTs), Special Interest Groups, as well as through internal proactive monitoring by CyberSecurity Malaysia staff.

MyCERT in 2017 had proactively produced 37 advisories and 11 alerts to inform its constituency on issues relating to computer security. The specific list of the advisories, alerts and summary reports can be viewed at:

https://www.mycert.org.my/en/services/advisories/mycert/2017/main/index.html

There was a decreased in intrusion incident in 2017 as compared to 2016. The majority of the incidents reported to MyCERT were related to fraud. This was followed by intrusion.

The following chart shows the reported incidents managed by MyCERT for 2017:



	JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC	TOTAL
Content Related	2	5	9	2	9	2	1	4	2	2	5	3	46
Cyber Harassment	41	45	64	71	119	39	27	25	32	36	31	30	560
Denial of Service	11	0	3	3	1	3	8	6	2	2	1	0	40
Fraud	296	233	274	265	346	298	329	382	466	351	340	241	3821
Intrusion	98	201	148	101	138	284	146	363	181	121	119	111	2011
Intrusion Attempt	39	19	32	41	22	8	37	31	8	9	11	9	266
Malicious Code	94	68	65	62	92	71	62	56	64	60	46	74	814
Spam	26	38	24	30	31	32	36	30	29	26	17	25	344
Vulnerabilities Report	5	2	8	3	1	4	2	11	6	10	5	3	60
TOTAL	612	611	627	578	759	741	648	908	790	617	575	496	7962

Chart 2: Reported Incidents Handled by MyCERT in 2017

Further information on Cyber999 statistics can be viewed at: https://www.mycert.org.my/statistics/2017.php

4. EVENTS INVOLVEMENT AND ACHIEVEMENTS

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

4.1 Cyber Drills

CyberSecurity Malaysia, through MyCERT, participated in two cross-national Cyber Drills in 2017 namely the APCERT Drill, OIC-CERT Drill and as Executive Controller of the Malaysia National Cyber Drill.

4.2 Trainings

Several workshops or hands-on training were conducted by CyberSecurity Malaysia in 2017 which included:

i. Network Security;
ii. Intrusion Detection Prevention; and
iii. Incident Handling & Network Security.

4.3 Presentations

CyberSecurity Malaysia's representatives had been invited to various talks at international conferences or seminars as speakers. Participation includes the APCERT Malware Mitigation Working Group held during the 2017 APCERT AGM & Conference in Delhi, India, FIRST TF CSIRT in Valencia, Spain, OIC-CERT AGM & Conference in Baku, Azerbaijan and FIRST Conference in San Juan, Puerto Rico, USA.

4.4 Tools developed

In 2017, CyberSecurity Malaysia, through the MyCERT's Malware Research team, has continuously develops tool to support the research and analysis which is the MyCERT Enhanced Multi Analyzer System (MyEMAS). MyEMAS is a comprehensive malware analyzer system combining multiple sandbox technologies and multiple antivirus engines.

4.5 Paper publication

CyberSecurity Malaysia has published 18 international papers to be shared with the security community, which are:

i. *Addressing Cyber Terrorism Threats.* Published in International Cybersecurity Forum
ii. *Factors Influencing User Adoption of Malaysia Cyber Security Clinic (MyCSC) Services*. Published American Scientific Publishers
iii. *Automated Analysis Report Generation Using CSM S-Box Evaluation Tool (CSET).* Published in Malaysian Society for Cryptology Research

iv. *Word Stemming Methods for the Malay Language: A Review.* Published in American Scientific Publishers

v. *A Comparative Analysis Study on Information Security Threat Models: A Propose for Threat Factor Profiling.* Published in Medwell Publications

vi. A Survey of SCADA Testbed Implementation Approaches. Published in Informatics India Ltd

vii. *Cyber Security Situational Awareness Among Students : A Case Study in Malaysia.* Published in World Academy of Science, Engineering and Technology [WASET]

viii. *CCTV Quality Assessment for Forensics Facial Recognition System.* Published in IEEE XPlore Digital Library

ix. *Understanding Cyber Terrorism from Motivational Perspectives: A Qualitative Data Analysis.* Published in Academic Conferences and Publishing International Limited

x. *National Cybersecurity Governance and Implementation of Malaysia for the Critical National Information Infrastructure.* Published in Korea Institute of Science and Technology Evaluation and Planning [KISTEP]

xi. *A New Academic Certificate Authentication Using Leading Edge Technology.* Published in ACM Digital Library

xii. *The Proactive Approach of Digital Forensics Methodology Against Targeted Malware.* Published in World Academy of Science, Engineering and Technology (WASET)

xiii. *A Comparative Study on Result of Speaker Recognition from Various Online Video Evidence.* Published in World Academy of Science, Engineering and Technology (WASET)

xiv. *Randomness Analysis on 3D-AES Block Cipher.* Published in Conference Proceeding / IEEE XPlore Digital Library

xv. *Towards an Enhancement of Organizational Information Security through Threat Factor Profiling Model.* Published in IOP Publishing

xvi. *Forensic Readiness: A Case Study on Digital CCTV Systems Antiforesics.* Published in Elsevier

xvii. *2.5 D Facial Analysis via Bio-Inspired Active Appearance Model and Support Vector Machine for Forensic Application.* Published in The Science and Information Organisation

xviii. *Cyber-related Fraud Incidents in Malaysia. A Seven Years Analysis of MyCERT Data.* published in the International Journal of Information Security and Cybercrime (Vol 6, Issue 2, 2017)

4.6 Social Media

In 2017, CyberSecurity Malaysia received continuous invitation to speak in events with regards to Internet security issues at the local radio and television stations. CyberSecurity Malaysia, through MyCERT, also actively disseminates security concerns through social media such as Facebook and Twitter. As of now, MyCERT Facebook Page has about 50,000 likes and MyCERT Twitter has 1,897 followers.

4.7 Global Cybersecurity Index 2017

Malaysia is ranked third among 193 countries in terms of its commitment to cybersecurity, according to the Global Cybersecurity Index (**GCI**) 2017. The GCI is a survey that measures the commitment of 193 member states to cybersecurity. It assesses a country based on five pillars, namely legal, technical, organisational, capacity building, and cooperation. Launched in 2014, the GCI aims to foster a global culture of cybersecurity.

Chart 3: Top ten most committed, GCI (normalized score)

Country	GCI Score	Legal	Technical	Organizational	Capacity Building	Cooperation
Singapore	0.92	0.95	0.96	0.88	0.97	0.87
United States	0.91	1	0.96	0.92	1	0.73
Malaysia	0.89	0.87	0.96	0.77	1	0.87
Oman	0.87	0.98	0.82	0.85	0.95	0.75
Estonia	0.84	0.99	0.82	0.85	0.94	0.64
Mauritius	0.82	0.85	0.96	0.74	0.91	0.70
Australia	0.82	0.94	0.96	0.86	0.94	0.44
Georgia	0.81	0.91	0.77	0.82	0.90	0.70
France	0.81	0.94	0.96	0.60	1	0.61
Canada	0.81	0.94	0.93	0.71	0.82	0.70

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 Visit

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 collaboration in a two-way knowledge sharing.

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

i. Department of Information and Communications Technology (DICT) Philippines;
ii. State Technical Service Republican Enterprise (STS), Kazakhstan;
iii. Academy Of Information System dan Security Code, Russia; and
iv. R&D Center "Kazakhstan Engineering", Kazakhstan.

5.2 Memorandum of Understanding (MoU)

CyberSecurity Malaysia collaborated, through MoUs, with the following organisations in matters pertaining to cyber security:

i. R&D Center "Kazakhstan Engineering", Kazakhstan;
ii. Garini Technologies Corporation Pte. Ltd., Singapore; and
iii. Thales Communication & Security SAS, France.

5.3 International roles

Amongst the international roles 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 Deputy 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 the service capabilities and encourage local Internet users to report 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 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 in 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 CSM-ACE, which is an annual event to provide 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.

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 computer incidents that were reported to Cyber999 Help Centre in 2017 compared to the previous year. This agency will continuously work with its international allies to generate useful cooperation in safe guarding 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 is an 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.

SingCERT

Singapore Computer Emergency Response Team - Singapore

1. About SingCERT

1.1 Introduction

The Singapore Computer Emergency Response Team (SingCERT) is Singapore's national CERT, serving as a trusted point of contact for cyber incident reporting for the members of the public, private businesses and international CERTs around the world. 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.

1.2 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 transited to the Cyber Security Agency of Singapore (CSA) when it was established on 1 April 2015. CSA is the national body overseeing cybersecurity strategy, operation, education and outreach, technology and industry development for Singapore's critical information infrastructures. It is managed by the Ministry of Communications and Information and reports to the Prime Minister's Office.

1.3 Resources

Specific threat alerts and advisories that affect the constituency are released on the SingCERT website (https://www.csa.gov.sg/singcert) and broadcasted through the SingCERT subscribers mailing list, and CSA's Facebook and Twitter platforms. CSA also maintains a website - GoSafeOnline (https://www.csa.gov.sg/gosafeonline) - to provide cybersecurity trends and tips for individuals and businesses.

1.4 Constituency

SingCERT serves primarily the local constituency comprising end users and private businesses in Singapore.

2. Activities & Operations

2.1 Scope and definitions

SingCERT provides technical assistance and facilitates communication in response to cybersecurity-related incidents affecting our constituency, and collaborates with foreign CERT partners in handling cross border cyber threats. SingCERT also monitors and evaluates global cyber threats and vulnerabilities, and publishes alerts and technical advisories with recommended prevention and mitigation measures. SingCERT does not conduct criminal investigations as it is not an investigative or law enforcement agency.

2.2 Incident handling reports

SingCERT receives incident reports via email and phone, and will assess and follow up with the respective agency or service provider to coordinate and carry out further remediation. In 2017, SingCERT received 4,782 incident reports from its constituency and foreign partners. This is a 133% increase from the 2,045 incidents reported in 2016.

	Jan – Mar	Apr – Jun	Jul – Sep	Oct – Dec	Total
No. of Case Reports	533	1,067	1,511	1,671	**4,782**

Figure 1: Number of Case Reports to SingCERT (2017)

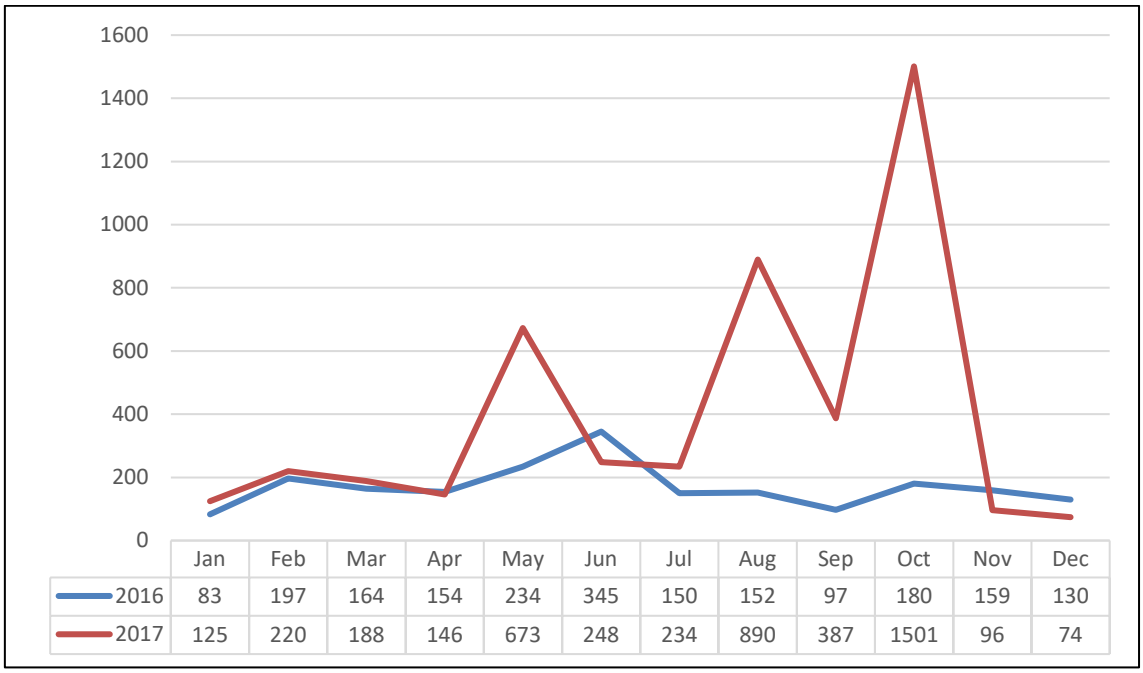


Figure 2: Number of Case Reports to SingCERT (2016-2017)

2.3 Abuse statistics

SingCERT receives numerous incident reports on different forms of cyber-attack. Some of the common cyber threats observed in Singapore are website defacements, phishing websites and ransomware, including new ransomware variants such as Bad Rabbit, Petya/Petna and WannaCry infections. In 2017, 25 ransomware incidents were reported to SingCERT, a 31% increase from the previous year.

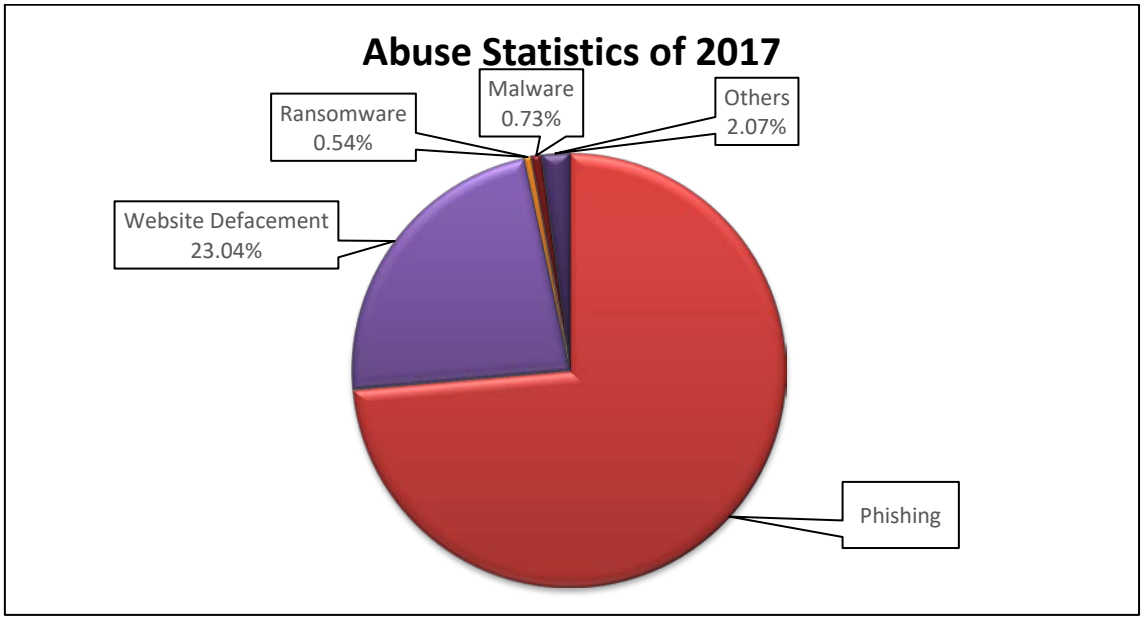


Figure 3: Abuse Statistics of 2017

2.4 Publications

2.4.1 Alerts and Advisories

SingCERT publishes alerts and advisories on widespread, emerging cyber threats with recommended mitigation measures and solutions to raise security awareness about the current cyber landscape. In 2017, 38 alerts and advisories were published on SingCERT's website (https://www.csa.gov.sg/singcert/news/advisories-alerts/) in the following chronological order:

- 8 Feb – Threat Alert: Compromised WordPress Websites due to Outdated WordPress Versions
- 24 Feb – Threat Alert on Cloudflare CloudBleed
- 9 Mar – Apache Struts2 Possible Remote Code Execution
- 15 Apr – Shadow Brokers Leaked New Trove of Hacking Tools
- 13 May – Alert on Wide-Spread "WannaCry" Ransomware Targeting Unpatched Windows Systems

- 14 May – WanaCrypt0r aka WannaCry: What You Need to Know and Actions to Take
- 15 May – Technical Advisory for System Administrators on "WannaCry Ransomware"
- 2 Jun – Educational Platform Edmodo Compromised
- 15 Jun – Fake Mobile Apps
- 23 Jun – Increase in Occurrence of Phishing Emails from 'Logistics' Companies
- 28 Jun – Alert on Global Spread of Ransomware Petya / Petna
- 28 Jun – Technical Advisory on Petya / Petna Ransomware
- 8 Jul – Alert on ISC Bind Vulnerabilities
- 14 Jul – Alert on Apache Struts2 Remote Code Execution Vulnerability
- 9 Aug – Increase in Defacements Affecting Singapore-hosted Websites
- 25 Aug – ShadowPad Backdoor Spreads in Corporate Networks Through Software Update Mechanism
- 6 Sep – Alert on Apache Struts2 Remote Code Execution Vulnerability (S2-052)
- 24 Sep – Alert on Two Apache Tomcat Security Vulnerabilities (CVE-2017-12615 and CVE-2017-12616)
- 30 Sep – Advisory on Multiple Security Vulnerabilities Affecting D-Link DIR-800 Series Routers
- 4 Oct – Alert on Multiple Dnsmasq Vulnerabilities (CVE-2017-14491 to CVE-2017-14496)
- 17 Oct – Alert on Multiple Vulnerabilities Affecting Wi-Fi Protected Access 2 (WPA2) Protocol
- 22 Oct – Alert on Botnet IoT Reaper
- 26 Oct – Advisory on Bad Rabbit Ransomware
- 2 Nov – Advisory on Microsoft Office Dynamic Data Exchange Attacks
- 3 Nov – Alert on Security Vulnerability in Older Versions of WordPress
- 9 Nov – Alert on Browser-based Digital Currency Mining
- 23 Nov – Advisory on Intel Firmware Vulnerabilities
- 23 Nov – Alert on Online Shopping During Festive Season
- 24 Nov – Alert on Microsoft Office Memory Corruption Vulnerability (CVE-2017-11882)
- 30 Nov – Advisory on Exim Internet Mailer Vulnerabilities
- 30 Nov – Alert on Security Flaw Found in macOS High Sierra

- 7 Dec – Alert on Mailsploit to Spoof Email Addresses
- 8 Dec – Securing Your Mobile Devices When Travelling This Holiday Season
- 10 Dec – Alert on Microsoft Malware Protection Engine Critical Vulnerability (CVE-2017-11937)
- 12 Dec – Alert on HP Notebook Keylogger
- 14 Dec – Alert on the Return of Bleichenbacher's Oracle Threat (ROBOT) Attack
- 19 Dec – Alert on Digital Currency Mining Campaign "ZEALOT"
- 29 Dec – Tips to Stay Safe Online in 2018

The following chart shows the increase in alerts and advisories issued by SingCERT in 2017 as compared to 2016:

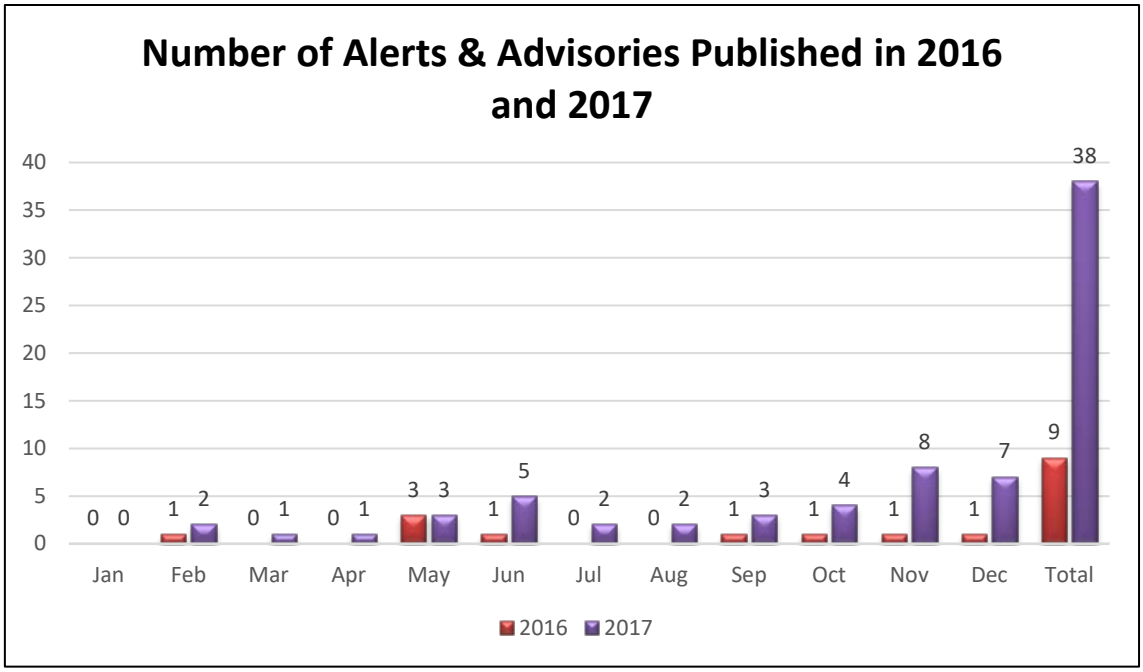


Figure 4: Comparing Number of Alerts and Advisories Published in 2016 and 2017

2.4.2 Singapore Cyber Landscape

The inaugural Singapore Cyber Landscape publication was released on 14 September 2017, highlighting facts and figures on significant cyber threats and incidents in Singapore for 2016. The publication provides an overview of the frequency and scope of cyber-attacks in Singapore, raising awareness of cyber threats among stakeholders, including the general public and businesses so that they can take appropriate actions to defend against such threats. More information about the report, including a downloadable copy is accessible via:

https://www.csa.gov.sg/news/publications/singapore-cyber-landscape-2016.

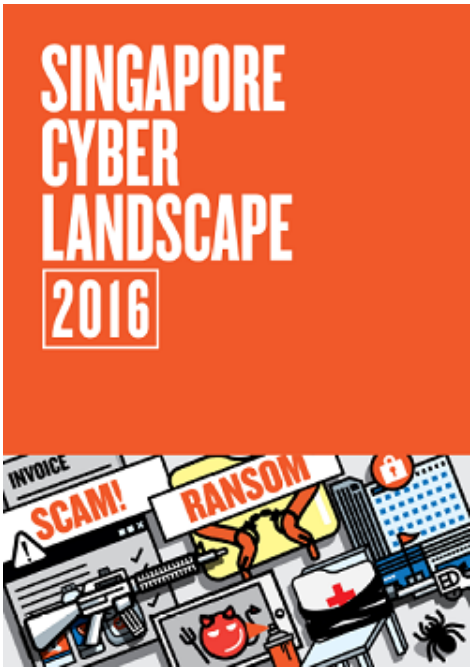


Figure 5: Singapore Cyber Landscape 2016

2.4.3 Cyber Safety Activity Book

CSA released the third issue of a series of Student Activity Books on *Cyber Safety* to raise awareness of the importance of cybersecurity and personal data protection. The activity book is also made available online as a resource for students, teachers and parents and can be accessed at the following link https://www.csa.gov.sg/gosafeonline/resources/activity-book

3. Events organised / hosted

3.1 Drills & exercises

3.1.1 ASEAN CERTs Incident Drill 2017

The 12th ASEAN CERTs Incident Drill (ACID) was conducted successfully by SingCERT on 11 September 2017. A total of 14 CERTs from 12 ASEAN Member States (AMS) and ASEAN Dialogue Partners participated in the drill. The theme "*Dangers of Insufficient Authentication and Poor Access Control*" was selected as it was observed that a large number of cyber threats occurred as a result of compromised systems that arose from poor cyber practices. Participants benefitted from the drill which stressed the importance of having good basic cyber hygiene best practices.

3.2 Conferences and seminars

3.2.1 Singapore International Cyber Week 2017

CSA organised the 2nd Singapore International Cyber Week (SICW) which took place from 18th – 21st September 2017 on the theme "Building a Secure and Resilient Digital Future through Partnership". SICW is Singapore's most established cybersecurity event, providing a platform for cybersecurity experts from around the world to discuss, network, strategise and form partnerships in the cyber security space. More details about the event can be found at https://www.sicw.sg.

3.2.2 National Cybersecurity Awareness Campaign

In 2017, CSA ran a campaign for the public to "Live Savvy with Cybersecurity". CSA also drives awareness efforts through the Cybersecurity Awareness Alliance, a collaboration between public and private sector organizations as well as trade associations, to raise awareness and adoption of cybersecurity measures. Alliance members actively give talks to schools, businesses and the community at various platforms.

4. International Collaboration

4.1 Training

SingCERT participated and benefitted from the following APCERT Training topics that were arranged by TWNCERT:

- "Digital Forensics" presented by Sri Lanka CERT|CC on 8 February 2017.
- "Mobile Vulnerability Check and Case Study" presented by KrCERT/CC on 19 April 2017.
- "Cyber Detection, Eradication and Forensic (Cyber D.E.F)" presented by MyCERT on 1 August 2017.
- "Cyber Threat Information Sharing" presented by CERT Australia on 3 October 2017.
- "Introduction of DDoS Offensive and Defensive Exercise in Taiwan" presented by TWNCERT on 5 December 2017.

4.2 Drills & exercises

4.2.1 APCERT Cyber Security Drill 2017

The annual APCERT Cyber Security Drill was held on 22 March 2017 with the theme "Emergence of a New DDoS Threat", to test the response capabilities of member teams

in responding to DDoS attacks involving compromised IoT devices. As a member of the APCERT Drill Working Group, SingCERT volunteered to be the drill lead and successfully led the group through the planning and conduct of the drill.

4.2.2 ASEAN-Japan Cyber Exercise

In 2017, Singapore co-chaired the ASEAN-Japan Information Security Policy Meeting. CSA was involved as a member of the ASEAN-Japan Cyber Exercise Working Group. The purpose of the working group was to develop an information sharing framework and enhance the cyber cooperation among AMS and Japan not only in an exercise but in business-as-usual and crisis coordination. SingCERT participated in the cyber exercise held on 18 May 2017 with the scenario on DDoS attacks from a certain hacker group.

4.3 Seminars & presentations

4.3.1 APCERT AGM and Conference 2017

SingCERT attended the APCERT AGM and Conference held in New Delhi, India, from 12 to 15 November 2017. This is an annual event where CERTs from the Asia Pacific region gather to exchange information on the latest cybersecurity issues and incident response methodologies. As the lead team of APCERT Drill 2017, SingCERT presented the post-APCERT drill findings at the APCERT AGM.

5. Future Plans

5.1 ACID 2018

Planning and discussions are in progress for the 13th ACID 2018 to determine the theme, scope and details.

5.2 Singapore Cyber Landscape 2017

CSA will be publishing the Singapore Cyber Landscape 2017 to report on the cyber-attacks and trends that occurred in Singapore's cyberspace in 2017.

5.3 Singapore International Cyber Week 2018

Planning and discussions for SICW 2018 has kick started and will be held near 18th to 21st September.

Sri Lanka CERT | CC

Sri Lanka Computer Emergency Readiness Team Coordination Centre – Sri Lanka

1. ABOUT SRI LANKA CERT | CC

1.1 Introduction

The Sri Lanka Computer Emergency Readiness Team | Coordination Centre (Sri Lanka CERT | CC) is the national centre for cyber security in Sri Lanka, mandated to protect the nation's information infrastructure and to coordinate protective measures against, and respond to cyber security threats and vulnerabilities.

1.2 Establishment

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

Sri Lanka CERT 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 and is under the Ministry of Telecommunications and Digital Infrastructure financed by the Government of Sri Lanka.

1.3 Workforce

The Sri Lanka CERT | CC has a total staff strength of fourteen team members consisting of the Chief Executive Officer, Director Operations, Principal Information Security Engineer, Senior Information Security Engineer, Research and Policy Development Specialist, Associate Information Security Engineer, five Information Security Analysts, two Associate Information Security Analysts, an officer in charge of Human Resources and Administrative work and a driver/office assistant. This team is supported by five 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 Facebook and social networks, web mail 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, and intellectual property violations.

This report presents an analysis of the cyber security related data collected by the Sri Lanka CERT|CC during the year of 2017. Based on the said date, following observations can be made;

- Majority of the reported incidents fall in to the category of social media related incidents. Among the social media incidents, Facebook related incidents were the highest.
- Financial frauds targeting local importers and exporters have seen an increase over the past several years. Financial frauds on local importers and exporters have increased more than 100% when compared to 2016.
- There has been an increase in the spread of ransomware and malicious software during the year of 2017, where sensitive data belonging to both individuals as well

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

- A significant number of phishing attacks targeting financial sector organizations were recorded in 2017.
- The number of intellectual property violation incidents shows a decrease in 2017.
- Not a single DoS/DDoS attacks were reported to Sri Lanka CERT during the year 2017.

The above findings lead to the following conclusions:

- Cyber criminals are changing their strategies in order to obtain more financial gains. Social engineering methods are widely adopted and ransomware is becoming a major threat to many organizations and individuals.
- Cyber security has to be recognized as a responsibility not only of organizations but also of every citizen, and each and every citizen has to contribute to ensure a secure online environment.
- Social media related incidents increased exponentially. Therefore, education and awareness among general public is important to ensure secure and ethical usage of social media sites.
- Making the general public, private and public-sector organizations aware of the various types of cyber threats is essential in order to ensure that people gain benefits of the Internet rather than become victims in the cyber world.

2.2 Incident Handling Statistics

Cyber-security related incidents reported to Sri Lanka CERT have increased in the year 2017 compared to previous years. In 2017, a total of 3907 incidents were reported to Sri Lanka CERT. This is a 66.89% increase in comparison to the previous year.

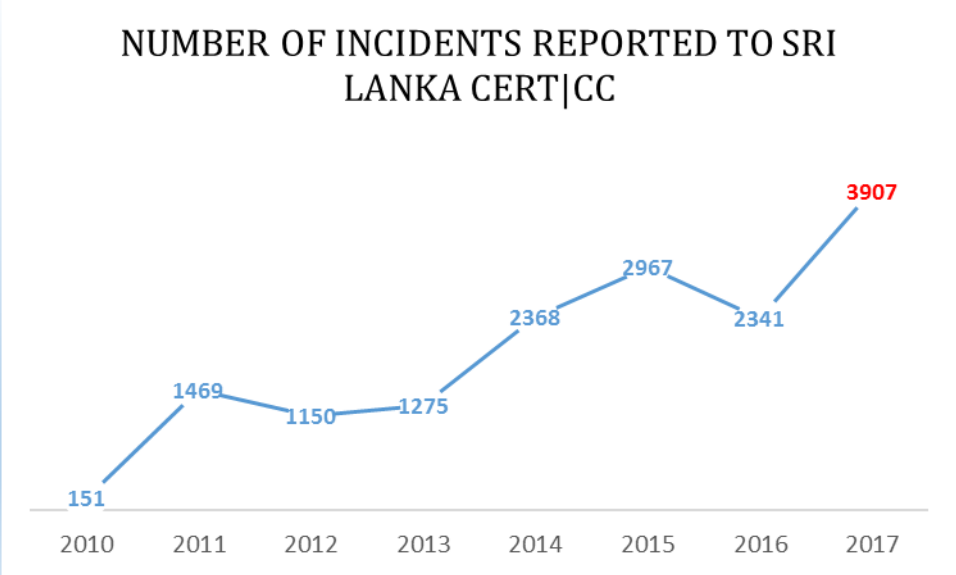


Figure 1. Growth of the number of incidents reported

Type of Incident	Number of Incidents
Phishing	42
Abuse/Hate/Privacy Violation	29
Ransomware	15
Scams	32
Malicious Software issues	24
Financial Frauds	35
Web site Compromise	25
Hate/ Threat emails	14
Intellectual Property violation	06
Unauthorized Access	-
DoS/DDoS	-
Social Media related incidents	3685
Total	3907

Table 1. Types of incidents

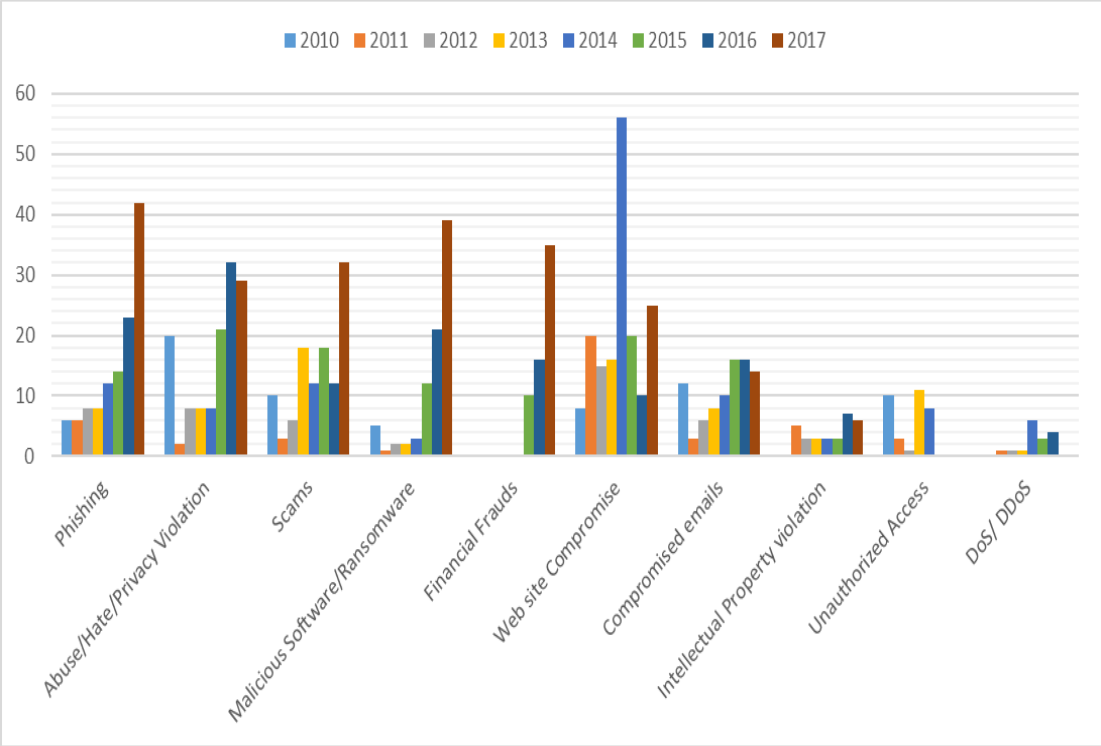


Figure 2. Growth of the types of cyber security incidents

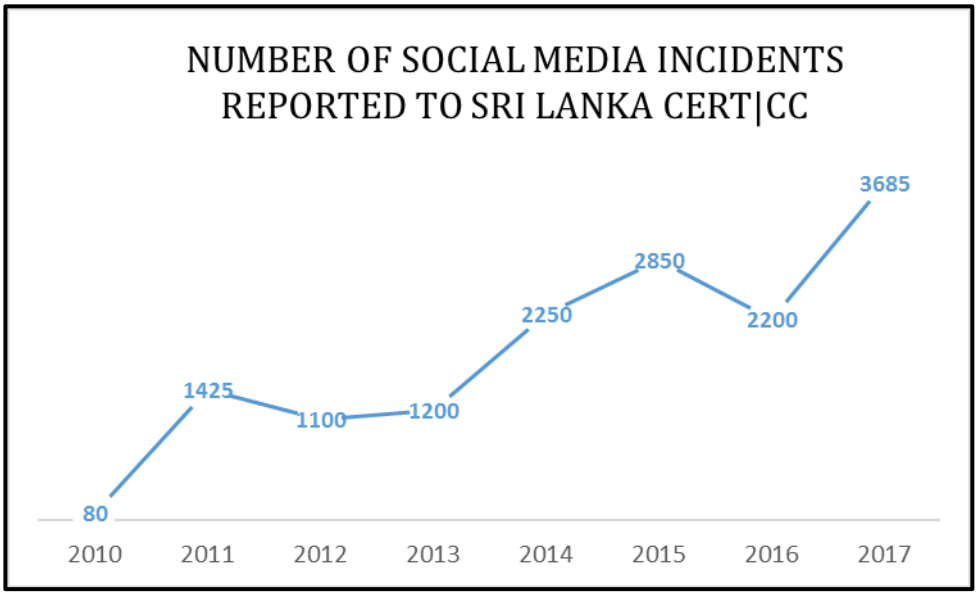


Figure 3. Growth of the social media related incidents

The reported social media related incidents can be categorized as follow.

Social Media Related Incident Types	Number of Incidents
Compromised Accounts	829
Fake Accounts	2018
Phone No Posted	54
Threatening	57
Ransom	1
Email	12
Website	7
Other	241
Porn Video	17
Copyright Violation	7
Photo Abuse	416
Total	3685

Table 2. A classification of the social media related incidents

2.3 Consultancy Services

Sri Lanka CERT|CC continues to provide consultancy services for its constituency (government and non-government).

Typical consultancy services provided during the period include;

- Security assessments for more than 40 government ministries/departments/statutory boards web sites.
- Security assessments for several private organizations.
- VAPT Assessments carried out for requested Networks
- Information Systems Security Review for a major government organization.
- Consultancy for a bank on conducting Security Assessments on their systems.
- Consultancy provided for few organizations which were under ransomware attacks.
- Email Header Analysis and security settings reviews for two private companies.
- Consultancy provided for more than 15 website defacement incidents.

2.4 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.

2.4.1 Awareness Program and Training Sessions

• Participated for Internet security related discussions.
• Approximately 25 Awareness and Training sessions conducted for law enforcement officers including police officers and judges on Internet safety, Social media Security, cybercrime and electronic evidence and related incident handling.
• Newspaper articles
• Information and Cyber Security alerts communicated through Radio and TV Channels
• Posters on Internet Safety – Ministry of Education.
• Carried out awareness sessions in national level events such as "Yowun Puraya".
• Internet Security Awareness sessions carried out in three government schools for teachers, students and parents.
• Conducted two Security Policy Development sessions for Government Officials.
• Conducted training sessions for private companies on their requests.
• Several awareness sessions for Principals and Education Administrative officers on Cyber security and internet safety.
• Eight sessions on "How to be safe on Social Media" for District Child development officers.
• Judges Training Program – Council of Europe (COE) - Special training on cybercrime and electronic evidence for Nepal Judicial Officers
• Nine EDUCSIRT Training programs for school teachers on different topics including Information security, Social Media safety and incident handling
• 1938 Helpline training session on Social Media related incident handling organized by Ministry of Women and Child Affairs
• E-Leadership training program for Senior Local government officials on Information Security and Cybercrime
• Carried out several training sessions for Government CIOs.
• Internet safety and policy development sessions for Officers in Tri Forcers.
• Around 5 awareness and training sessions for SLAS officers.
• Awareness Session for undergraduate students in a local private university.

2.4.2 Awareness through Electronic/Print Media

• Hiru TV - Cybercrime program (complete 20 episodes out of 56)
• Udhayam TV - Awareness program on cyber security
• Newspaper articles
• Information and Cyber Security alerts communicated through Radio and TV Channels
• Posters on Internet Safety – Ministry of Education.

2.4.3 Annual Cyber Security Week 2017

Activities carried out at the Cyber Security Week
• Hacking Challenge
• Cyber Security Quiz for Universities
• Workshops
• 10th Annual National Cyber Security Conference
• Handbook on Security was launched and copies were distributed to conference participants

2.4.4 Council of Europe (COE)/GLACY project

Sri Lanka CERT|CC is engaged with a capacity building programme of the Council of Europe, under a project titled Global Action Against Cybercrime (GLACY) and has been engaged in conducting training programs for law enforcement and officials from Judicial service.

- Participated for a workshop on Criminal Justice statistics on cybercrime and electronic evidence (Ghana)
- Advisory mission on CERT capacities, digital forensics lab and public-private cooperation and a Workshop on cybercrime reporting systems and collection and monitoring of criminal justice statistics on cybercrime and electronic evidence in Nuku'alofa, Tonga, - participated as Council of Europe expert, assess and suggested the CERT operations and way forward. In the workshop importance of criminal justice statistics were presented.
- Global Action On Cybercrime Extended – 3 workshops (Singapore)
- T-CY 17th Plenary meeting, GLACY+ Steering Committee meeting, - Participated with Sri Lankan Delegates (Country coordinator, Judiciary and law enforcement

agents) to present how the TOT programs were effective and how to sustain the training for judiciary and law enforcement in long term.

- Special training on cybercrime and electronic evidence for Nepal judicial officers with trainers from Sri Lanka Judges' Institute in partnership with Nepal Judicial Academy at Kathmandu, Nepal - Participated as resource person to carryout presentations for the course along with Sri Lankan Judges. Trained 25 Nepal Judges during 5day training program.
- Special training on cybercrime and electronic evidence were conducted in Sri Lanka with the support of Council of Europe, Participated as resource person to carryout presentations for the course along with Sri Lankan Judges (1 High court judge, and 3 for Magistrates). 70+ High courts judges and 180+ magistrates from different parts of the country were the participants in these training programs.

2.5 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.

2.6 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 2017. This project was funded by government of Sri Lanka.

2.7 Special Projects

Project Name	Description and Activities
• National Certification Authority (In progress)	• Procurement of Hardware is completed • Procurements of software is completed • Procurement of two data centre locations for production and backup sites are in progress. • Staff trainings are completed. • Implementation is started.
• National Security Operations Center (In progress)	• This is a joint project with ICTA. • Procurement in progress.
• Activities with EduCSIRT (Sector based CSIRT for Educational Sector. Established in collaboration with Ministry of Education)	• Development of Training modules is completed • Completed two trainings for two batches
• Cyber Security Project (Funded by UK High Commission)	• Procurement of Cybercrime investigation resources for Sri Lanka CERT (Encase forensics software and video and image analysis software) • User Trainings for staff on forensics software • Specific foreign trainings on cyber security provided for Sri Lanka CERT • Awareness programmes for government organizations and general public

3. Events organized

3.1 Seminars & Workshops

- Cyber Security Week 2017

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 2017 was held in the month of August 2017, and featured a series of

events including the following;

- Annual National Conference on Cyber Security 2017 – Securing Critical Infrastructure and Environment.
  - Three full-day Workshops for professionals, namely:
    Workshop 1 on "Advanced Web Application Security (Hands on)"
    Workshop 2 on "Incident Response and Internet Security"
    Workshop 3 on "Ethical Hacking and Forensic Computing"

- Hacking Challenge: 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: 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.

- Workshop on Development of the National Cybersecurity Strategy.
  - Two Cyber Security Experts from UK were invited to provide insights for the development of a national cyber security strategy,
  - Task Force members and Stakeholders participated for the workshop and shared their ideas for the strategy.

4. Achievements

4.1 National Cyber security strategy

2016/2017

Sri Lanka CERT|CC commenced work on the first draft of the national cyber security strategy for Sri Lanka in 2016. Stakeholder consultations have been initiated to identify key strategic thrust areas. Following six strategic thrust areas are identified namely;

(1) Establishment of Governance Framework
(2) Enactment and Establishment of Legislation
(3) Policies and Standards, Resilient Digital Government and Infrastructure

(4) Development of Competent Workforce

(5) Raising Awareness and Empowerment of Citizens, and

(6) Development of Public-Private, Local-International Partnerships.

4.2 Research and Policy Development

Sri Lanka CERT strengthened its research arm by recruiting a research team. The team conducted several surveys, such as, Youth's Survey on Social Media Awareness and Public Service Managers Information and Cyber Security Readiness Survey.

4.3 Certification & Membership

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

a) (ISC)2 Colombo Sri Lanka Chapter the local representative organization of International Information Systems Security Certification Consortium.

b) Threat Intelligence from ShadowServer.

5. New services

Sri Lanka CERT is expecting to deliver cyber security managed services during the year of 2018 and has completed the preparatory work during this year.

6. International Collaboration

6.1 Event participation

- Global Cybersecurity Center for Development (GCCD) Training, Korea. Organized by KISA, CAMP
- Cyber Detection, Eradication and Forensic (Cyber D.E.F) Confirmation - APCERT online training Webinar organized by MyCERT.
- Participated for APISC Security Training Course organized by KISA in Soul, Korea.
- APCERT Annual General Meeting and Conference hosted by CERT-In –New Delhi
- Cyber Offence and Defensive Exercise organized by National Information and Communication Security Taskforce Taiwan, R.O.C.
- International visitor leadership program on "Cyber Security". Organized by US Embassy.
- Participated for USTTI training in Washington, DC.

6.2 Other activities

- 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.
- Continuing with network monitoring project "Tsubame" with JPCERT|CC
- Conducted APCERT webinar on "digital forensics and its importance on CERT day to day operations" for the APCERT members
- Conducted Training for Bhutan government officials on Website Security and Network Security (Bhutan).
- Conducted site visit to Bhutan CIRT as the sponsor for membership of APCERT and FIRST and conducted a training program for Bhutan government officers.

6.3 International incident coordination

- APCERT Cyber Security Drill
  - Worked as a member of the organizing committee of APCERT Cyber Security Drill 2017
  - Participated for the drill
- 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 (such as Facebook, Google, Yahoo) to resolve phishing and identity theft incidents.

7. Future Plans

7.1 Future projects

- Development of National Cyber Security Strategy (In progress).
- Development and Implementation of a Security Operations Centre (In progress).
- Establishment of the National Certification Authority (In progress).
- Establishment of sector based CSIRT's (e.g. Telco-CERT).
- Cyber Security Week 2018.

7.2 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.

8. Conclusion

As predicted in Sri Lanka CERT's Annual Report of 2016, a significant growth in financial frauds and ransomware attacks targeting small and medium size businesses were observed in 2017.

During this period, Sri Lanka CERT carried out a large number of information and cyber security training and awareness sessions, and the demand for such programs are increasing. All the events organized by Sri Lanka CERT during the period were very successful, well attended and were high in demand. Sri Lanka CERT will continue to conduct the Annual Cyber Security Week and the Annual National Conference on Cyber Security as we have planned.

Furthermore, Sri Lanka CERT aims to complete the development of the National Information and Cyber Security Strategy during the first quarter of 2018.

Sri Lanka CERT continues to receive requests from other newly established CERTs/CSIRTs to be their sponsor for membership of APCERT and/or FIRST.

Sri Lanka CERT is currently working with UK Foreign and Commonwealth Office and the Council of Europe to enhance the cyber security posture in the country which may have a significant impact to the other nations. During the year 2017 it was able to complete most of the activities that we had planned to achieve this target.

In addition to securing Sri Lanka's cyberspace, Sri Lanka CERT is committed to building a secure information environment in the Asia Pacific region/world with the help of all the CERTs and information security organizations through APCERT/FIRST.

TechCERT

TechCERT – Sri Lanka

1. About TechCERT

1.1 Introduction

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 10thAnniversary on 01stof September 2016.

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 20 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	Qualifications
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)
Kalana Guniyangoda	Lead Security Engineer	MSc. (Moratuwa), BSc. IT (Hons), CHFI
Sashika Suren	Lead Security Engineer	MSc in Info Sec (UCSC), BICT (UCSC), RHCE, RHCSA, MCTS, GDip in Bus Mgmt
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
Viraj Madhawa	Information Security Engineer	BSc(Hons) Eng in Computer Engineering (Peradeniya)
Chathuranga Gunatillake	Information Security Engineer	BEng (Hons) Computer Networks & Security, MBCS, E|NSA, C|EH

Rajith Jayasekara	Information Security Engineer	MBA (Moratuwa), Bsc. Information and Communication Technology
Vidusha Rathnayake	Information Security Engineer	BSc(Hons)in IT Computer Systems & Networking, RHCSA, C|EH
Anuruddha Hewawasam	Information Security Engineer	BSc. Computer Science (UCSC), SSCP, MIEEE
Vishvajith Ihalagama	Information Security Engineer	BSc(Hons) Eng in Computer Engineering (Peradeniya)
Priyankara Bandara	Information Security Engineer	BSc(Hons) Eng in Computer Engineering (Peradeniya)
Asanka Dhananjaya	Information Security Engineer	BSc(Hons) Eng in Computer Engineering (Peradeniya)
Dhushan Chathuranga	Information Security Engineer	BSc(Hons) Eng in Computer Engineering (Peradeniya)
Dilusha Bandara	Information Security Engineer	BSc. Information and Communication Technology, CCNA
Ayodya Balasuriya	Information Security Analyst	BSc. Information Systems (UCSC)
Kushantha Rajaratne	Information Security Engineer	BEng (Hons) Computer Networks and 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

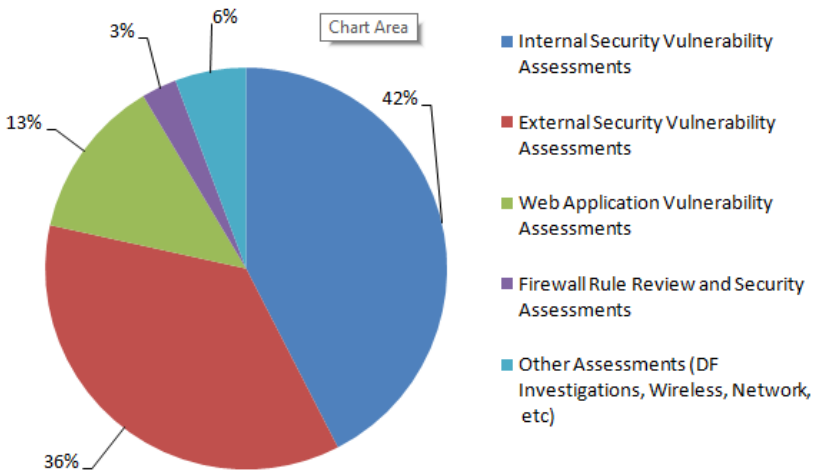
TechCERT Managed Security Services include a range of engineering and consultancy services listed below:

- 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
- 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 Security Assessments Conducted

The details of security assessments conducted by TechCERT during the year 2017 are as follows:

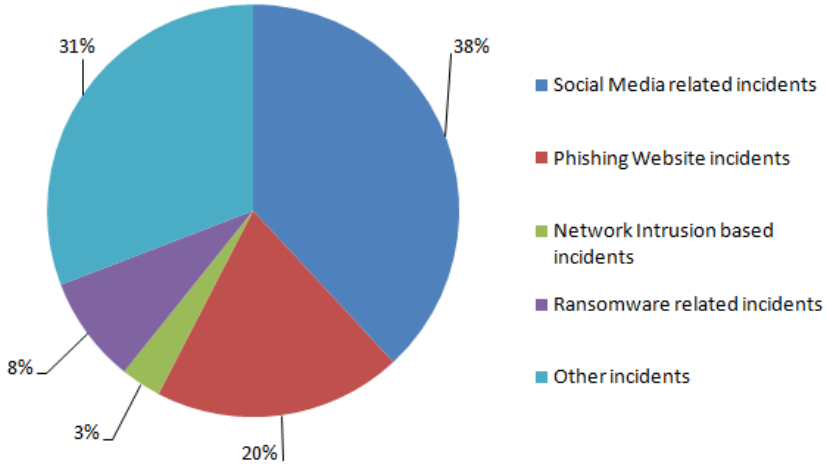
Activity	Count
Internal Security Vulnerability Assessments	2832
External Security Vulnerability Assessments	2403
Web Application Vulnerability Assessments	865
Firewall Rule Review and Security Assessments	189
Other Assessments (DF Investigations, Wireless, Network, etc)	382



2.3 Incident Handling

Throughout the year 2017, TechCERT responded and helped organizations to handle numerous and diverse cyber security incidents and submitted reports pertaining to those incidents. These were reported to us via our hotline, Facebook page, email, clients, Netcraft phishing service, law enforcement units and other security entities.

Activity	Count
Social Media related incidents	168
Phishing Website incidents	86
Network Intrusion based incidents	14
Ransomware related incidents	37
Other incidents	136



3. Alerts and Advisories

TechCERT publishes alerts on various business critical vulnerabilities that are trending at present and relevant solution recommendations through the TechCERT official website https://techcert.lk/en/ throughout the year to spread awareness and knowledge about current security related information among the public.

TechCERT further publishes security facts and best practices on the official Facebook page https://www.facebook.com/techcert.lk/.

4. Events Organized/Hosted

4.1 Organizing Trainings Locally

Over a time frame of several months	Secure Software Development Life Cycle and Best Practices training for Financial Institutes and Telecommunication Companies
8th and 9th February 2018	Two-day workshop on PCI-DSS v3.2 Implementation (CPISI Certification)
23rd March 2017	TechCERT Annual Workshop for Web Application Security and best practices, Ransomware & Cryptocurrency and Security guidance for IOT

4.2 Organizing Trainings Internationally

28th February and 3rd March 2017	"How to secure your TLD Infrastructure" training program in Ho Chi Minh City, Vietnam. Done in partnership with Asia Pacific Top Level Domain (APTLD).

4.3 Cyber Security Drills for Local Organizations

12th June 2017	TechCERT Cyber Security Drill 2017 – Banking Sector
17th June 2017	TechCERT Cyber Security Drill 2017 – Financial Sector
22nd November 2017	TechCERT Cyber Security Drill 2017 – Telecommunication Sector

4.4 APCERT Cyber Security Drill

TechCERT participated in the APCERT Cyber Security Drill as a player. Also TechCERT was in the organizing committee and shouldered the role of EXCON for four teams.

22nd of March 2017	Participated in APCERT Cyber Security Drill 2017

4.5 Conferences and Seminars organized by TechCERT

29th of April 2017	**Seminar – "Stay safe on Internet" and "IoT Security"** Awareness Sessions Conducted for Engineers in Northern Province of Sri Lanka together with IESL (Information Technology and Communications Engineering Section of Sri Lanka)
8th of July 2017	**Seminar – "Stay safe on Internet" and "IoT Security"** Awareness Sessions Conducted for Engineers in Southern Province of Sri Lanka together with IESL (Information Technology and Communications Engineering Section of Sri Lanka)
8th of November 2017	**Seminar – "How to be Proactive Against Cyber Attacks" and "IoT Security"** Awareness Sessions Conducted for Engineering Undergraduates of University of Peradeniya, Sri Lanka together with IESL (Information Technology and Communications Engineering Section of Sri Lanka)
22nd of January 2018	**Seminar – "How to be Proactive Against Cyber Attacks" and "IoT Security"** Awareness Sessions Conducted for Engineering Undergraduates of University of Ruhuna, Sri Lanka together with IESL (Information Technology and

	Communications Engineering Section of Sri Lanka)

5. Future Plans

- In 2018, 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
- Continually enhancing the EagleEye service provided by TechCERT by integrating threat intelligence gathering.
- Further improving and developing the newly formed TechCERT Security Operations Centre (SOC).
- Enhancing the technologies and technical knowledge of the engineers, who work at the DarkLab. DarkLab is a digital forensic investigation laboratory operated at TechCERT.

6. Conclusion

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. As a core part of its mandate to secure the Internet in Sri Lanka, TechCERT also provides information security incident response services and conducts public awareness programs on the safe use of computers and the Internet for the general public. The active involvement in APCERT drill activities has immensely helped TechCERT to successfully conduct cyber drills for Sri Lankan Organizations (Financial Organizations, Banks and Telco & ISPs) for the seventh consecutive year in 2017.

There was a significant increase in phishing attacks and ransomware/hacking incidents in Sri Lanka in 2017 when compared to previous years. 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, The global collaboration and the commitment and dedication of the staff have propelled TechCERT to its present status as a significant player in providing a faster and more efficient service to the clients as well as the public.

ThaiCERT

Thailand Computer Emergency Response Team – Thailand

1. Highlights of 2017

1.1 Summary of major activities

In this year, ThaiCERT focused on supporting public sectors to create sector-based CERTs. We support TB-CERT (Thailand Banking Sector CERT), TCM-CERT (Thailand Capital Market CERT) which were created in this year.

This was also the first time that we organized a 5-day national cybersecurity conference called Thailand Cybersecurity Week 2017 and we hosted the ASEAN-level CTF event called Cyber SEA Game 2017.

To enhance cybersecurity for critical government agencies, ThaiCERT provided training programs consisting of international courses such as such as SANS, CYDER, TRANSITS for key cybersecurity personnel of critical government agencies.

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

3.1.1 Reported Incidents Handled via Triage

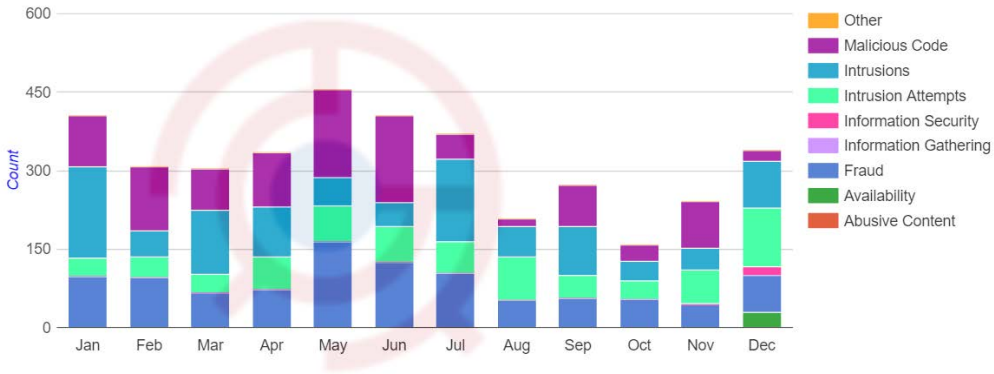


Figure 1: The number of reported incidents in 2017

Via triage, ThaiCERT handled a total of 3,237 reported incident cases (tickets) in 2017, which is a decrease of 5.6% compared to those of 2016 (3,797 cases). The received reports per month varied approximately between 200 to 400 cases, with an average of 270 cases per month.

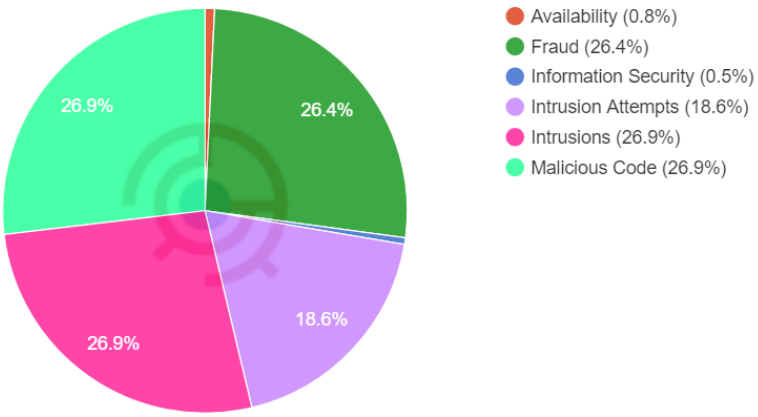


Figure 2: The proportion of reported incidents by incident type in 2017

According to the reported incidents in 2016, classified by the eCSIRT incident classification, Intrusion Attempts dominated with 28.9%, followed by fraud at 26.1%, where all fraud cases were phishing, and intrusions at 17.6%. All such information was handled and notified to the relevant parties through e-mail channels.

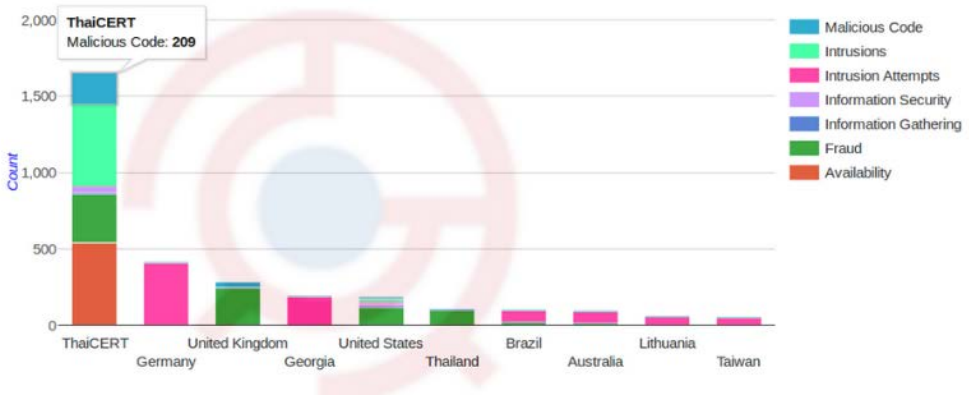


Figure 3: Top 10 incident reporters in 2017

Regarding the incident reporters classified by country, Figure 3 shows that most of the security incidents were reported by the ThaiCERT security watch system, comprising 1655 cases or 51% of all reports. Fraud, Malicious Code and Intrusions incident reports generally came from automatic feeds. The number of incident reports from Germany were in second position (409 cases), followed by the United Kingdom (286 cases).

3.1.2 Reported Incidents Received

ThaiCERT received reports from various channels such as automatic feeds, email and telephone where incident reports were handled via triage and the ISP exchange system. The ISP exchange system provides an information sharing service for ISPs to retrieve incident reports to co-ordinate with their customers. In 2017, ThaiCERT has received incident reports comprising around 2 million unique IPs where the top 3 of incident reports were Botnet (1,995,169 IPs), Open DNS Resolver (237,393 IPs) and Open Proxy Server (21,574 IPs).

3.2 Publications

In 2017, ThaiCERT supported ETDA to publish Cybersecurity Survey 2016 to assess cybersecurity in public and private organizations. ThaiCERT also published 7 infographics to raise awareness, including.

- How to Protect from WannaCry (for Normal User)
- How to Protect from WannaCry (for Administrators)
- Backup Recommendations
- How to Protect and Respond to PETYA (for Normal User)

- How to Protect and Respond to PETYA (for Administrators)
- How to Protect from BlueBorne
- How to Identify Fake News
- For the details, please see https://www.thaicert.or.th/downloads/downloads.html

4. Events organized / hosted

4.1 Training

Co-organized:

- iSEC with Thailand Information Security Association, Jan and Feb 2017

4.2 Drills & exercises

Organized:

- Cybersecurity drill for government agencies, Mar and Dec 2017
- Cyber defense exercise with recurrence (CYDER), Feb 2017
- Drill for capital market sector, Oct 207
- Drill for healthcare sector, Nov 2017

Participated:

- APCERT Drill 2017, Mar 2017
- ASEAN CERT Incident Drill (ACID) 2017, Sep 2017

4.3 Conferences and seminars

Organized:

- Cybersecurity Boot Camp (organized with financial associations and regulators), Oct 2017
- Cyber SEA Game 2017, Nov 2017

Co-organized:

- Advanced Digital Forensics Training, Nov 2017
- Thailand Cybersecurity Week, June 2017

Participated as speaker:

- IoT-Smart City Forum, Bangkok, Thailand, April 2017
- NatCSIRT Conference 2017, San Juan, Puerto Rico, June 2017
- RSA APJ Summit, Singapore, Singapore, July 2017
- APrIGF, Bangkok, Thailand, July 2017
- APISC, Seoul, South Korea, July 2017

- 8th APT Cybersecurity Forum CSF-8, Dhaka, Bangladesh, October 2017
- APEC TEL 56, Bangkok, Thailand, December 2017

Participated:

- RSA Conference 2017, San Francisco, USA, February 2017
- Annual FIRST Conference 2017, San Juan, Puerto Rico, June 2017
- APCERT AGM 2017, New Delhi, India, November 2017

5. Future Plans

- Future projects
- The ASEAN Critical Information Infrastructure Protection Framework
- ASEAN-Japan Cybersecurity Capacity Building Center

TWCERT/CC

Taiwan Computer Emergency Response Team / Coordination Center – Chinese Taipei

1. Highlights of 2017

1.1 Summary of major activities

In 2017, Taiwan Computer Emergency Response Team / Coordination Center (TWCERT/CC) received 4,720 incident reports, collected and published 124 vulnerability alerts.

Also, TWCERT/CC published daily news, monthly reports, incident analysis reports, "CERT/CSIRT Setting up Guide for Enterprises", "Cyber Security Incident Report and Response Guide", "Annual Performance Report " on both official website and Facebook page.

In addition, TWCERT/CC provided new services this year, including MARS, new official website, and Automatic Incident Reporting System.

As for the event part, TWCERT/CC hosted first annual cyber security conference, and co-hosted 10 conferences this year.

Moreover, TWCERT/CC cooperated with multiple resources to exchange cyber security related information, including APWG, AIS, No More Ransom and Stop. Think. Connect. TWCERT/CC also signed MoU with JPCERT/CC and Trend Micro for further cooperation.

1.2 Achievements & milestones

- Developed MARS to detect malicious files and avoid data leakage.
- Cooperated with new resources to exchange cyber security related information.
- Published "CERT/CSIRT Setting up Guide for Enterprises", "Cyber Security Incident Report and Response Guide", "Annual Performance Report ", 12 monthly reports and 6 incident analysis reports.
- Started to host an annual cyber security conference.

2. About TWCERT/CC

2.1 Introduction

Taiwan Computer Emergency Response Team / Coordination Center (TWCERT/CC) is responsible for a safer, stronger cyberspace in Taiwan by responding to major cyber security incidents, analyzing threats, publishing vulnerability information and

exchanging critical cyber security information with trusted partners around the world. The major purposes of TWCERT/CC are to prevent and actively assist the computer and network security incidents in Taiwan, to analyze the system vulnerabilities, to provide computer and network security tools and related documents for the system administrators and the programming guidelines for the developers, and conduct a series of training programs to raise the awareness of network security. TWCERT/CC is constantly reinforcing the organization functions and refining the network security services. With the dedicated devotion and seamless collaboration of the whole team, TWCERT/CC has accomplished several significant gradational goals and missions as follows:

- To assist the handling of the intrusion incidents in the constituency, .tw domain.
- To announce the system vulnerability information.
- To provide security training and education on protection and defending technologies and skills.
- To assess periodically the national-wide security level in the Internet.
- To be the point of contact of Taiwan for international coordination.

2.2 Establishment

In September 1998, National Sun Yat-sen University created TWCERT/CC under the support of National Information and Communication Initiative (NICI) and Taiwan Network Information Center (TWNIC). From January 2010 to July 2014, TWCERT/CC was operated by Taiwan Network Information Center (TWNIC). In August 2014, National Chung-Shan Institute of Science and Technology (NCSIST) took over TWCERT/CC. Since the establishment of Department of Cyber Security of Executive Yuan in June 2016, TWCERT/CC is under the supervision of Department of Cyber Security.

2.3 Organization

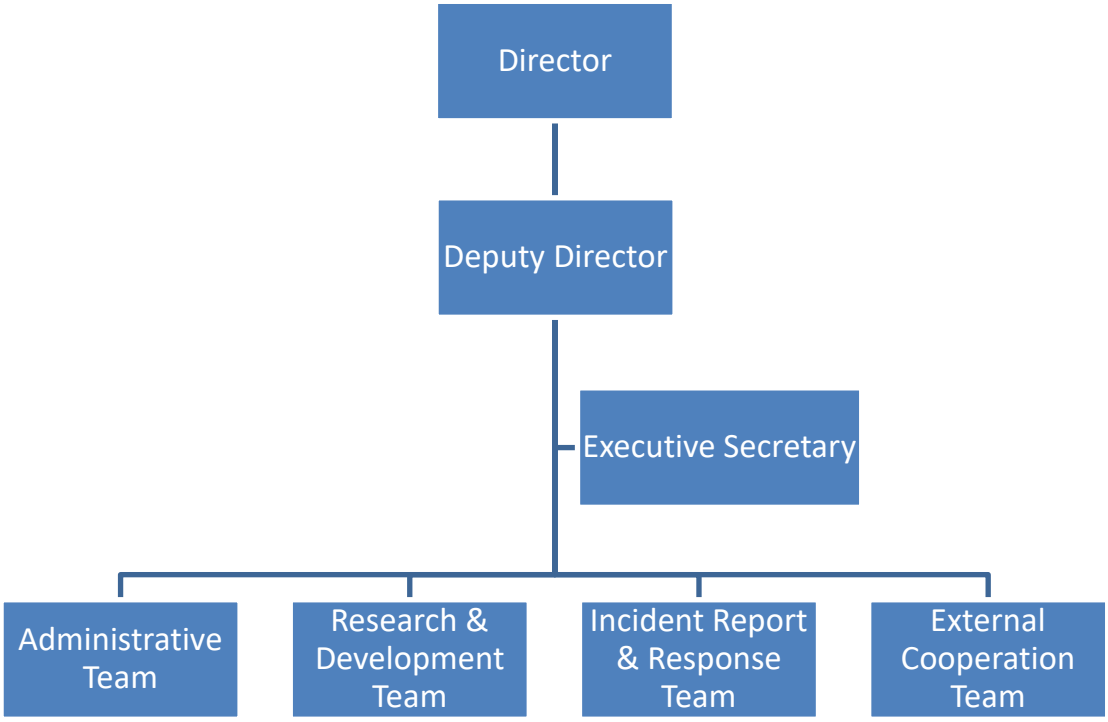


Figure 5. Organization Chart of TWCERT/CC

2.4 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 cyber security capacity, TWCERT/CC leads the promotion of cyber security incident reporting, provision of cyber security educational resources, and cyber security outreaches. Sponsored by the government, TWCERT/CC collaborates and integrates resources with cyber security 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 cyber security collaborative defense system, enhance self-protecting capacity in cyber security industry, cultivate high quality cyber security human resources, and strengthen the public-private partnership on cyber security issues.

3. Activities & Operations

3.1 Incident Report Handling

TWCERT/CC received incident reports from foreign and domestic resources. The resources including CERTs, public and private sectors, cyber security companies, and individual researchers. Nevertheless, we also keep expanding our resources, and find more malicious or hacked domain names/IPs on the internet aggressively.

In order to defend hacker intrusion and stop the spreading of security threats, TWCERT/CC collaborates with partners such as CERTs, government authorities, enterprises, ISPs, cyber security companies, researchers and so on, plays the role as a coordinator between different units to handle the incidents. In 2017, TWCERT/CC received 3,461 incident reports, and the numbers of the reports we received in recent years are shown in table1.

Table 1. Incidents reported to TWCERT/CC in recent years

Year	2010	2011	2012	2013	2014	2015	2016	2017
Total	1,094	6,666	8,126	140,250	15,150	24,116	3,461	4,720

The goals we expect to achieve are as following:

- Prevention: Provide incident advisory and early incident warning for people to avoid similar incidents from happening.
- Handling: Offer an immediate warning when the incident happened. Also, provide technological support to control the damage of the incidents.
- Recovery: Provide technological consultant and support to recover from the damage.

The types of information received by TWCERT/CC in 2017 are shown in Fig. 2.

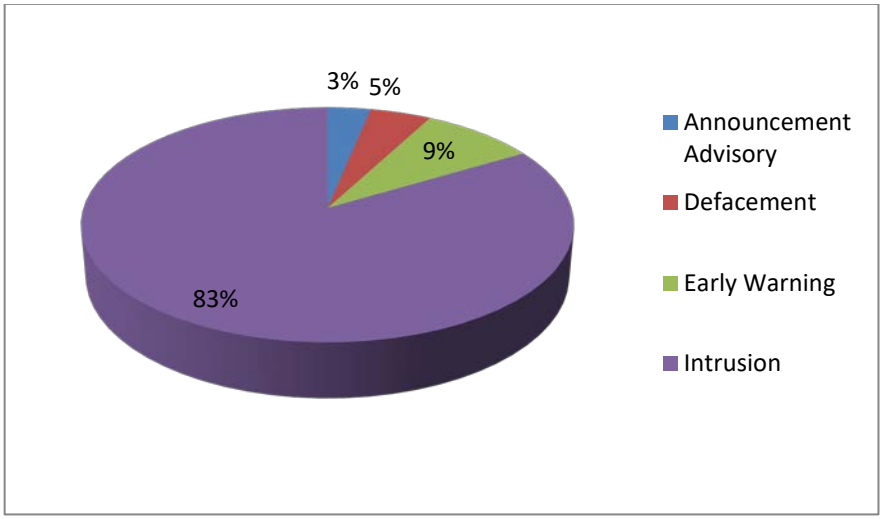


Figure 6. Types of information received by TWCERT/CC in 2017

3.2 Intelligence Monitoring and Warning

- Security Vulnerability Announcement

To promote computer system and network security as well as reduce damage from intrusions, TWCERT/CC is devoted to strengthen its services, release the latest security issues, provide information related to vulnerability patches, cyber security documents and tools for people to use, and actively release reports about the latest attack/defense technologies.

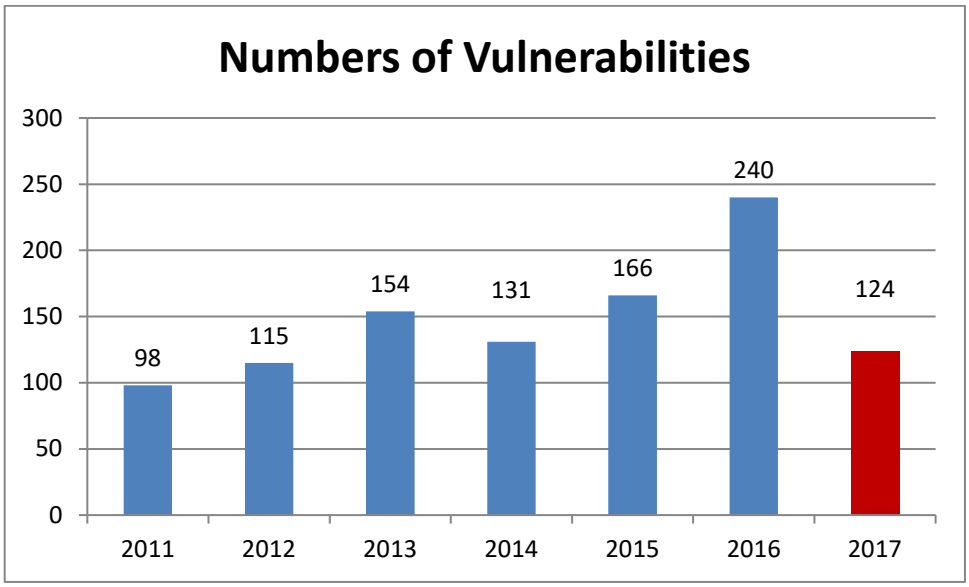


Figure 7. Annual Statistics of Vulnerability by TWCERT/CC

TWCERT/CC maintains a vulnerability database, which is a collection of the information of software vulnerabilities and system weaknesses. The vulnerability database contains 13 categories, and we have collected 124 numbers of vulnerabilities in 2017. We will continuously maintain and update it. The major categories and numbers are shown in Fig. 4 and Table 2.

Table 2. Categories of the Vulnerability in 2017

vulnerability category	number(s)	vulnerability category	number(s)
Denial of service	21	Cross site scripting	5
Gain information	23	Cross-Site Request Forgery	3
Code execution	20	Injection	4
Overflows	8	Directory traversal	1
Memory corruption	6	Http response splitting	2
Gain privilege	26	File inclusion	1
Bypass something	4		

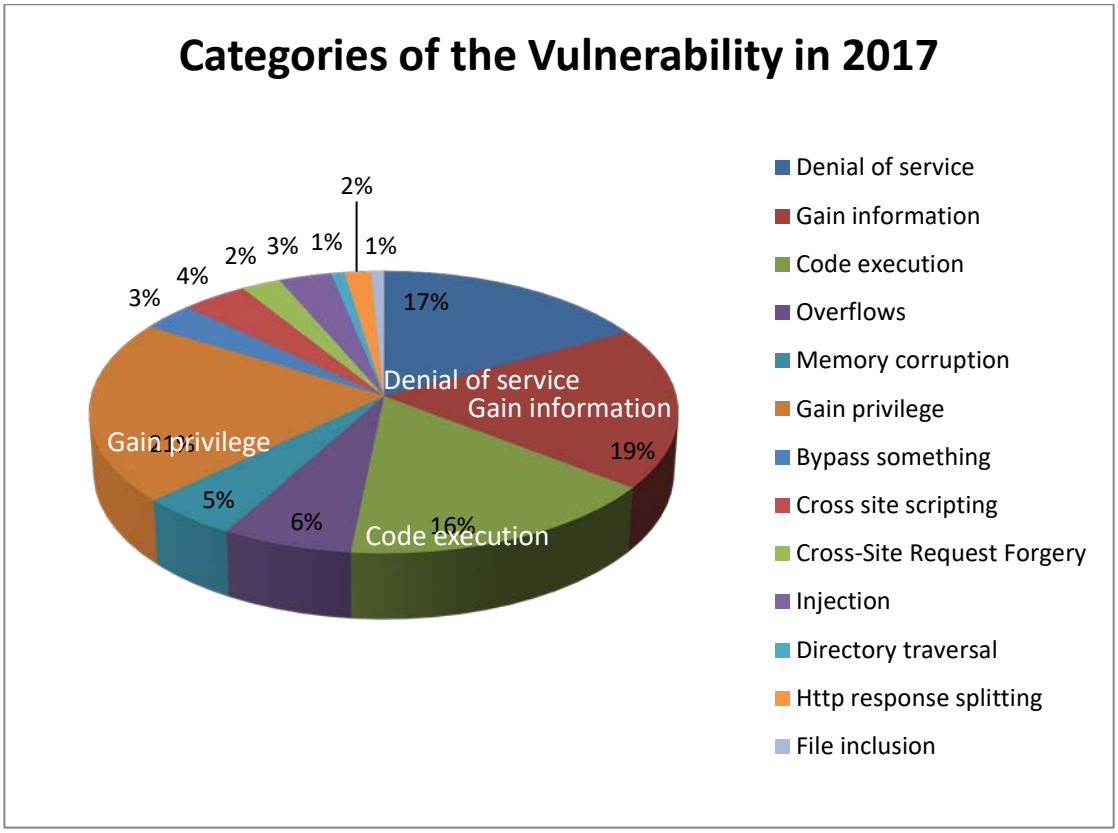


Figure 8. Categories of TWCERT/CC Vulnerability Database

3.3 Publications

TWCERT/CC publish daily news about cybersecurity on its official website and Facebook page, including recent activities of TWCERT/CC, cybersecurity policy threats and trend, incidents and methods of cyberattacks, vulnerabilities of software and hardware, and cybersecurity seminars and activities.

In addition, every month TWCERT/CC integrates cybersecurity news collected and

statistics of incident reporting last month and announces the releases on its official website and cybersecurity newsletters.

As for critical cybersecurity incidents, such as the massive ransomware attacks of WannaCry happened in 2017, TWCERT/CC also published its analysis and countermeasures with important vulnerability updates from Microsoft on its official website and Facebook page.

Also, in 2017, TWCERT/CC started to write an annual performance report, "CERT/CSIRT Setting up Guide for Enterprises" and "Cyber Security Incident Report and Response Guide", and published it on official website and Facebook page.

3.4 Services

- MARS

In order to prevent people in our country from confidential data leakage, TWCERT/CC collaborates with National Center for High-performance Computing (NCHC) and developed Malware Analysis and Report System (MARS). The system provides a web interface for users to upload files and track the detection result of the file they uploaded. After detected the file, system will generate reports and let the users know the risk of the file they uploaded. The system is developing under the supervision of Department of Cyber Security. Currently, only government sectors can access to the system, and the system will be totally opened to people in Taiwan in the future.

- Official Website

In October, TWCERT/CC finished the developing of a brand new website and put it online. The new version of website provides friendlier interface, multiple functions, and bilingual interfaces. After the new website is online, the average page views has tripled than the previous website.

- Automatic Incident Reporting System

In October, in order to help people to have a more convenience way to report the incident, TWCERT/CC developed an Automatic Incident Reporting System and put it online. The system provides web interface and API, and users can choose which one is more suitable for them to use. After the system received the report, the system will send the incident to a ticking system, which is also developed this year, in the backend. The ticking system also helps us to manage the process and status of every incidents we received.

4. Events organized / co-organized / hosted

4.1 Information Security Training & Activity

TWCERT/CC provides a series of security training/education for government agencies and industries to enhance and enrich their knowledge and capability on network and information security. The training course also gives people a channel to exchange information and hands-on practice related to security.

TWCERT/CC hosts/co-host cybersecurity conference and training regularly to raise the security awareness, to enhance security technical skills, and to build an information exchange and communication channel among internet users, administrators, and ISPs.

Table 3. List of TWCERT/CC co-host cyber security conference in 2017

Date	Subject (Conference)
2017/03/15	TWCERT/CC 2.0: From Incident Report to Intelligence Integration and United Defense (Taiwan InfoSec Conference 2017)
2017/04/12	TWCERT/CC 2.0: From Incident Report to Intelligence Integration and United Defense (Secutech 2017)
2017/04/26	Comprehensive Initiation of Civil Cybersecurity Collaborative Defense: Ubiquitous Entrepreneurial Cybersecurity Notifications (Info Security Forum 2017)
2017/04/27	Cybersecurity Intelligence Collection, Analysis, and Forensic Practices (Formulate Internal and External Smart Threat Life Cycle Managements)
2017/05/12	2016 TWCERT/CC Incident Report (Symantec ISTR Media Briefing)
2017/06/04	TWCERT/CC & Cybersecurity (The 12th International Health Information Management Symposium)
2017/06/06	New Thinking of Promoting Civil Cybersecurity Notification- Comprehensive Initiation of Cybersecurity Collaborative Defense (IRCON 2016)
2017/07/11-2017/07/13	CSA Taiwan Summit 2017
2017/10/14	The Dungeons of Hackers (TDOH) Conference 2017
2017/12/19	2018 Internet Threats- Top Ten Necessary Defensive Measures for the Whole Enterprise (2018 Cybersecurity Trend Forum)

4.2 Drill

TWCERT/CC participated in the APCERT Drill in March 22, 2017. The topic of APCERT online drill is “An Evolving Cyber Threat & Financial Fraud”. We simulate an example of real life to make incident response mechanism.

4.3 Conferences and seminars

TWCERT/CC held “Taiwan Cybersecurity Incidents Report and Response Conference 2017- The Innovative Thinking of the Joint Defense in Cybersecurity Field” on September 13, 2017; around 330 people participated the annual cybersecurity conference. In response to several crucial cybersecurity incidents happened in Taiwan during the recent years, the theme of conference was “Cybersecurity Notifications and Responses” so that to bring the participants measures of cybersecurity notifications and responses, access to cybersecurity assistance, and handling procedures and solutions of cybersecurity incidents.

Hung-wei Chien, director of the Department of Cyber Security, also gave a presentation on the subject of “Taiwan’s Cybersecurity Collaborative Defense System”. Mr. Chien said that the key indicators of Taiwan’s cybersecurity development consists of completing basic cybersecurity environment, constructing national cybersecurity collaborative defense system, cultivating high quality cybersecurity intellectuals, and promote self-sufficient capability of cybersecurity industry. The Department of Cybersecurity had established the first “Cybersecurity Service Group” constituted by ten experts with focus on financial institutions, and the total number of Cybersecurity Service Groups is expected to be 4 by 2017. As for cybersecurity risk evaluation, early warning, consistent monitoring, reporting and responding, and improvement assistance should be the four pillars to realize cybersecurity protection centered on risk management. Among the four pillars, reporting and responding is the most critical; only by notifications can cybersecurity incidents be managed and addressed immediately.

Figure 9. Group photo of the guests in 2017 Annual Conference of Taiwan Cybersecurity Notification and Response

5. International Collaboration

In addition to make efforts in security improvement in our domain, TWCERT/CC actively participates in the international security organizations and activities to enhance communication and cooperation with partners. TWCERT/CC plays a role as a coordinator to maintain the global network security. Thus, we exchange and cooperate with international partners, including governments, CERTs, CSIRTs, cyber security companies, researchers and individuals.

Moreover, We participate in international forums, conferences and meetings, and exchange cyber security intelligence with partners.

5.1 International partnerships and agreements

- Forum of Incident Response and Security Teams (FIRST)

The well-known security organization, FIRST, is an important platform for computer emergency teams to exchange information and to collaborate with others on various security issues. It brings together a wide variety of security and incident response teams including especially product security teams from the government, commercial, and academic sectors.

TWCERT/CC joined FIRST in 2001 and became the official contact point of Taiwan. It shares the security information and technologies in many security organizations, such as FIRST, and participates FIRST conferences and technical colloquiums to establish a security joint defense system and enhances incident-handling capability for integrated early-warning mechanism.

- Asia Pacific Computer Emergency Response Team（APCERT)

APCERT, established in 2002, is a regional coordination organization of Asia Pacific with the goal to enhance regional and international cooperation on cybersecurity. APCERT cooperates with CERTs and CSIRTs to maintain a trusted contact network of security experts in the Asia Pacific region, and improve the region's awareness and ability to handle cyber security incidents.

TWCERT/CC jointly develops measures to deal with large-scale security incidents and phishing attack, and exchanges technologies and experiences with APCERT members.

In 2017, TWCERT/CC participated APCERT AGM 2017, and introduced the newly developed system "MARS" to members. Also, we participated in Drill WG and help to design the script for drill 2018.

- Invite Foreign Experts

TWCERT/CC invited many foreign experts from cyber security field and learned from their experience. This year, we had invited experts from Japan and England, and discussed issues such as "How to encourage enterprises in Taiwan to build their own CERT/CSIRT/PSIRT?" With the interaction and cooperation during the meeting and discussion, we learned from the experts' suggestion, and were able to improve our ability and enhance the connection with the world.

- Memorandum of Understanding (MoU)

To further strengthen cooperation and information sharing, TWCERT/CC has been signing a MoU with various security organizations. This year, TWCERT/CC signed MoU with JPCERT/CC and Trend Micro.

- WannaCry Ransomware and FarEATM Hacking Incident in Taiwan

In 2017, WannaCry Ransomware incident happened in May, and Far Eastern International Bank hacking incident happened in October. After the incidents happened, TWCERT/CC published analysis reports and shared it with foreign partners for international joint defense. Also, when foreign partners shared their analysis report with TWCERT/CC, we shared it with authorities and proper partners within our country.

- Cooperate with Anti-Phishing Working Group (APWG)

In 2017, TWCERT/CC started to cooperate with APWG, and connect to the system by

using API. We continuously exchange the information of malicious IPs and phishing websites with the system. If we find any malicious IP or phishing website which locates in our country, we will help to report it to its authorities.

- Connect to Automated Indicator Sharing (AIS)

In 2017, TWCERT/CC started to cooperate with AIS, which was established by US-CERT. We established a TAXII client to connect to the TAXII server of AIS and continuously exchange STIX files with the system. If we find any report, malicious IP or phishing website which related with our country, we will help to share it with proper authorities according to its tlp limitation.

- Become a partner of No More Ransom Project

In 2017, TWCERT/CC started to cooperate with No More Ransom project, which is a project with a goal to mitigate the threat and loss caused by ransomwares, and became a partner with them. We volunteered to translate the content of the website into traditional Chinese, and are now working on it. We believe that it will help people in our country to get away from ransomware's threats.

- Become a partner of STOP.THINK.CONNECT

In 2017, TWCERT/CC started to cooperate with STOP.THINK.CONNECT project, which is a project with a goal to mitigate the threat and loss caused by cyber security issues, and became a partner with them. With authorization, we translate the educational resources of the project, such as videos, into traditional Chinese, and upload them to our official YouTube channel. It can help our people to understand cyber security issues and raise the awareness of it.

5.2 Other international activities

- Participated Cyber Intelligence Asia 2017

In March 2017, TWCERT/CC participated Cyber Intelligence Asia 2017 which was held in Malaysia, and gave a speech with the topic "Cyber Threats Faced in Taiwan".

- Preparation of being a CNA

In 2017, TWCERT/CC contacted The MITRE Corporation, and started to prepare for the application of being a CVE Numbering Authorities (CNA) in Taiwan.

6. Future Plan

The future work of TWCERT/CC will emphasize the harmonic and efficiency of the coordination among different levels and across the nation.

- In 2018, the cybersecurity promotion of TWCERT/CC focuses on small and medium enterprises. Relative activities include publishing cybersecurity e-newsletters, and holding trainings, conferences, and forums.
- Actively collaborate with institutions from Taiwan and abroad to exchange and manage the latest cybersecurity intelligence.
- Encourage people to report spontaneously and help enterprises establish CSIRT/PSIRT.
- Apply for becoming an CVE Numbering Authorities (CNA), setup related process, develop ticketing system, and publish report/response guideline in 2018.
- Use API and standard information sharing format (such as STIX) to connect with more information resources.

7. TWCERT/CC Contact Information

- Website: https://www.twcert.org.tw/
- Facebook: https://www.facebook.com/twcertcc/
- Youtube: https://www.youtube.com/channel/UCciZUJ_GR_LqXdQzdRV3dGw
- E-Mail: twcert@cert.org.tw

TWNCERT

Taiwan National Computer Emergency Response Team – Chinese Taipei

1. Highlights of 2017

1.1 Summary of major activities

TWNCERT aims to support and enhance the government's ability to respond and deal with security incidents. In 2017, TWNCERT received 1,043 reports on cyber security incidents from Taiwan government and published 1,992 security advisories to government sectors as well as provided consulting services.

To raise security awareness, TWNCERT conducted a national large-scale cyber security exercise, named Cyber Offensive and Defensive Exercise (CODE), held a total of 12 national cyber security seminars for the government agencies as well as launched cybersecurity competitions for university students.

In 2017, TWNCERT also attended various international events and delivered presentations on cyber security threats at the FIRST Technical Colloquium and APNIC 44 in Taichung in September, APCERT AGM & Conference in India in November, and APEC TEL 56 in December.

This year, we start to promote the 8 CI sectors in Taiwan which are the energy, water resources, communications and broadcasts, transportation, banking and finance, emergency services and public health care, central government and major metropolitan areas, and high-tech industrial parks to build up the CERT, ISAC and SOC of each CI sector. Three guidelines for the competent authority of different CI sectors with common standards and requirements for CI operators base on our experiences from government sector were also developed in 2017.

1.2 Achievements & milestones

TWNCERT was one of the APCERT Steering Committee members and continued to be the convener of APCERT Training Working Group during the year of 2017, TWNCERT convened 5 APCERT online training programs in 2017, and a total of 22 CERTs member teams had participated in these programs.

2. About CSIRT

2.1 Introduction

As a national CERT, TWNCERT (Taiwan National Computer Emergency Response

Team) acts as the point of contact for the CSIRTs in Taiwan and worldwide for the nation. We aim to enhance the government's 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, which is in charge of cyber security issues 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 120 full-time employees, and the operation funding comes from the Department of Cyber Security.

2.4 Constituency

TWNCERT dedicates to enhance the capability of incident report and response among government authorities and also focuses on other related issues such as national critical information infrastructure protections. Moreover, TWNCERT coordinates information sharing with various organizations such as Financial ISAC, Academic ISAC, National Communications Commission ISAC, major ISPs, major SOCs, law enforcement agencies, other CSIRTs in Taiwan as well as information security industries in Taiwan and worldwide.

3. Activities & Operations

3.1 Scope and definitions

The key missions and responsibilities of TWNCERT are listed below:

- Researching and analyzing national cyber security legislation systems; formulating cyber security regulations and guides for government agencies; gathering cyber security threat information from the Government, academic facilities, and private sectors.

- Developing inter-government agency 2nd tier cyber security monitoring mechanism, researching and analyzing cyber security threats the nation is facing.
- Sharing cyber security information via public-private partnerships, monitoring sensitive government agencies' networks at all time.
- Researching, analyzing and improving national critical incident responses, hosting big scale cyber offensive and defensive exercises, pairing with a security audit, cyber health check and penetration test services, to discover cyber security problems of the Government and critical infrastructures in time.
- Planning cyber security series competitions; enhancing cyber security education effects and raising the public cyber security awareness.
- Developing cybersecurity service systems according to mission needs, researching and proposing resource integration practices of private sectors, the Government, and academic & research facilities; be able to provide effective assists and supports to related agencies to counter when under cyber-attacks or facing threat situations

3.2 Incident handling reports

TWNCERT received 1,043 reports on computer information security incidents from Taiwan government agencies, and more than 1,179 international information security incident reports from overseas in 2017.

Also, TWNCERT established Government Information Sharing and Analysis Center (G-ISAC) in 2009, is the largest information sharing networks in Taiwan. G-ISAC is a public-private partnership which has reduced response time through improved coordination, collaboration capabilities, and efficiencies to enhance cyber security efforts nationally. In 2017, G-ISAC shared a total of 69,717 security incidents and critical information among members including Academic ISAC (A-ISAC), National Communications Commission ISAC (C-ISAC), Financial ISAC (F-ISAC), major SOCs, law enforcement agencies, and CSIRTs in Taiwan.

3.3 Abuse statistics

The top 3 incident categories from government agencies are Website Defacement, Intrusion, and Others.

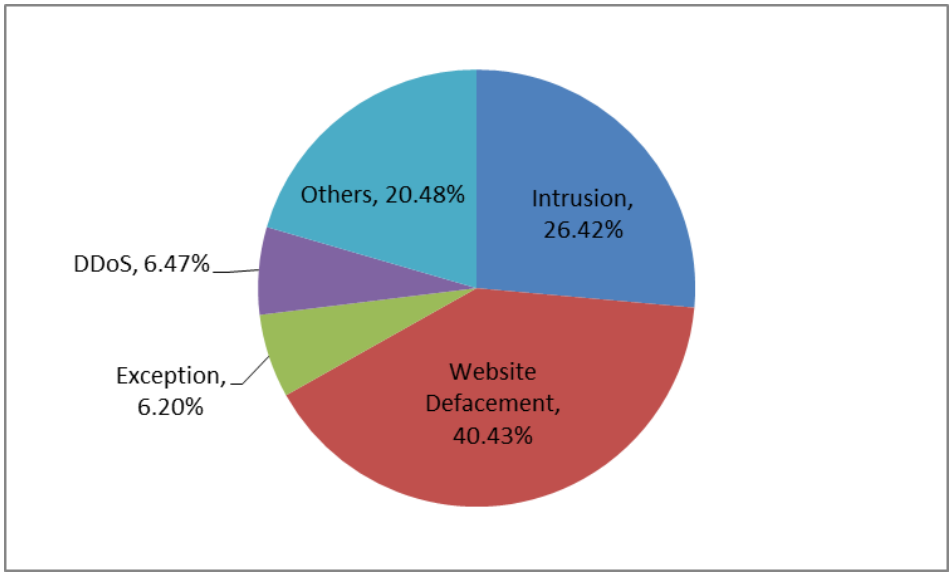


Figure 1 Security incidents from government sectors

The international information security incident reports in 2017 were categorized as in Figure 2. About 41.45% of the incident reports were Malware, followed by Phishing and Attack.

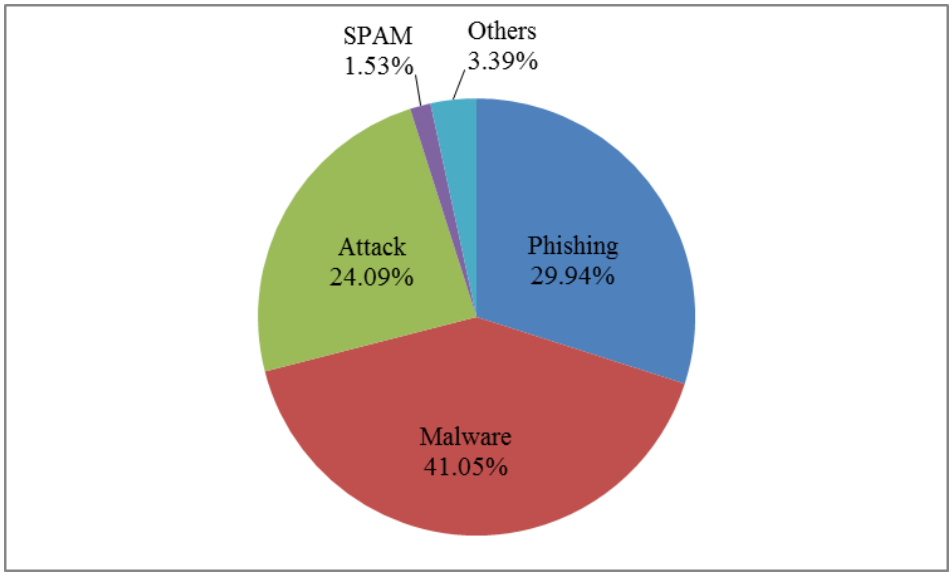


Figure 2 Classification of the international incident reports

Currently, G-ISAC has covered over 99% IPs in Taiwan and has shared thousands of security incidents and critical information each year. G-ISAC members shared a total of 69,717 security information in 2017.

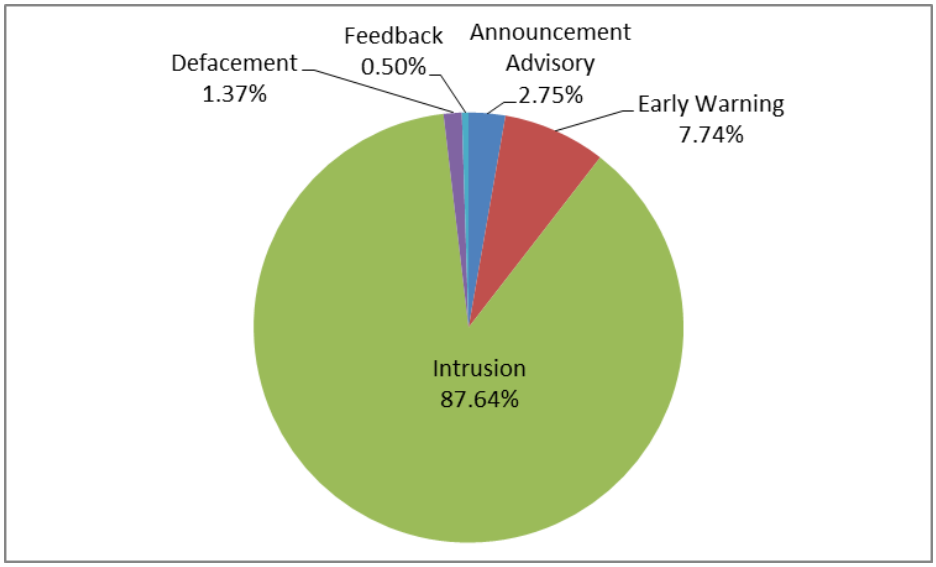


Figure 3 Information sharing distribution of G-ISAC

3.4 Publications

- Government sectors

In 2017, TWNCERT published 1,992 notice advisories to government sectors. The categories were distributed as in Figure 4 and 5.

Month	Emergency	Intrusion	Defacement	Early Warning	Announcement	Total
1	0	4	15	37	12	68
2	0	3	14	43	3	63
3	0	6	27	129	20	182
4	0	22	17	139	11	189
5	0	81	40	61	14	196
6	0	108	14	101	8	231
7	0	111	5	80	11	207
8	0	95	9	94	8	206
9	0	120	7	85	11	223
10	0	97	5	87	11	200
11	0	7	1	125	12	145
12	0	5	5	65	7	82
Total	0	659	159	1,046	128	1,992

Figure 4 Notice advisories to government

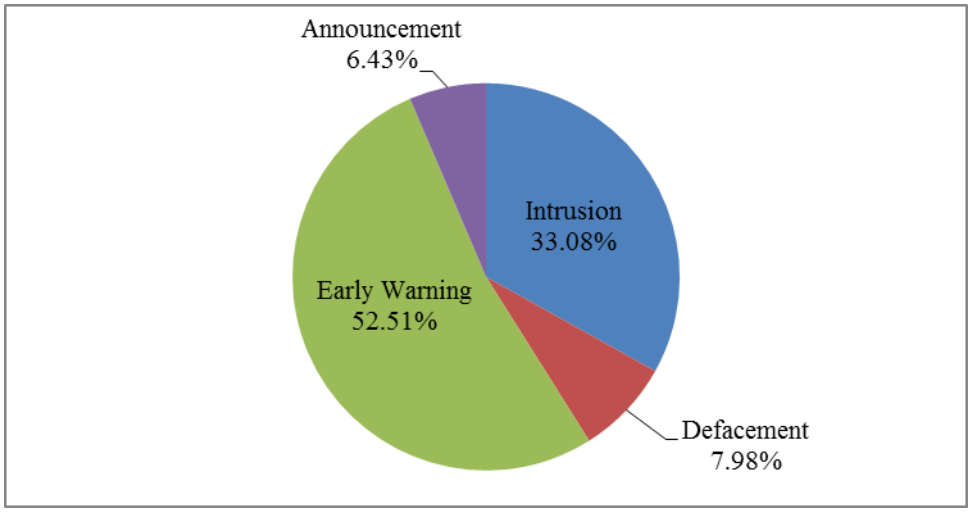


Figure 5 Distribution of government notice advisories

- International incident report sharing

Regarding the international incident report sharing, TWNCERT has reported a total of 3,732 incident reports via G-ISAC to 52 countries shown in figure 6.

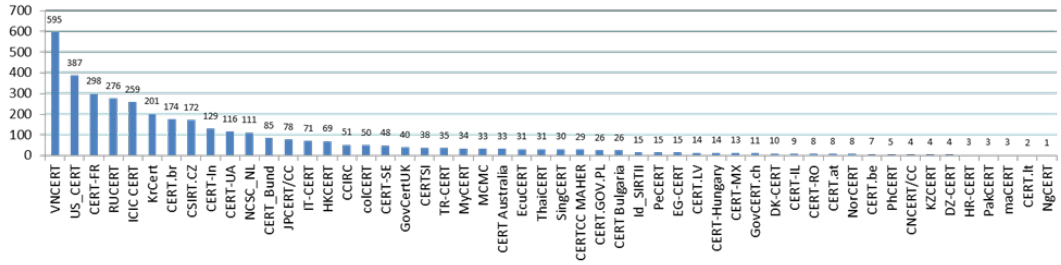


Figure 6 International incident report via G-ISAC

- Website publication

TWNCERT collects and publishes cyber security advisories, news or guidelines via its website. In 2017, TWNCERT published 202 news including cyber security news and bulletins on the website.

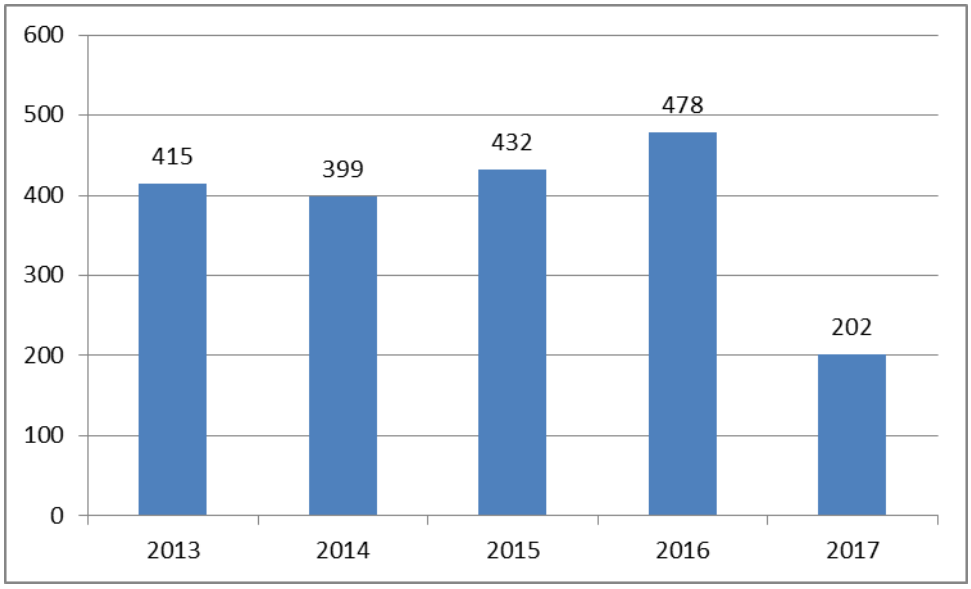


Figure 7 TWNCERT Published news on website

4. Events organized/hosted

4.1 Training

TWNCERT hosts national cyber security workshops and seminars regularly to raise the cyber security awareness among government agencies. In 2017, TWNCERT held 12 national cyber security workshops for government agencies, and a total of 3,290 government technical staffs attended.

Figure 8 Cyber security workshops

4.2 Drills & exercises

- Drill

TWNCERT has conducted a national large-scale cyber security exercise, Cyber Offensive and Defensive Exercise (CODE). This year CODE was mobilized more than 60 government agencies including National Security Bureau, Ministry of National Defense, Office of the President, central and local government agencies to strengthen the preparedness against cybercrimes, technology failures as well as Critical Information Infrastructure (CII) incidents, especially focused on telecommunication and financial sectors. This year delegates from United States, Thailand, South Korean, Japan, Malaysia, Australia, Indonesia, Sri Lanka, UK, EU and Estonia observed the whole event and shared their valuable experiences. This Cyber Offensive and Defensive Exercise is not only a domestic public-private partnership effort, also facilitate international cooperation.

- Cybersecurity competition

To promote cyber security general awareness, TWNCERT launched cyber security series competitions in 2017. It aimed to improve the cyber security awareness among university students. There are more than 3,600 attendees participated.

Figure 9 Cyber security competition

4.3 Conferences and seminars

For G-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 2017, a total of 4 member meetings had been held.

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 organization events, 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
- Anti-Phishing Working Group(APWG)

To further strengthen cooperation, TWNCERT currently has Government Security Program Source Code Agreement with Microsoft, NDA with Fortinet, MOU with JPCERT/CC and Team Cymru for CSIRT Assistance Program.

5.2 Capacity building

5.2.1 Training

As the convener of APCERT Training Working Group, this year TWNCERT continues to coordinate member teams to provide online training sessions every other month. In 2017, a total of 5 APCERT online training programs have been convened, with a total of 22 CERTs, member teams participated. In order to improve the training program, TWNCERT conducted a survey to evaluate the effectiveness of training program and delivered the statistics results at APCERT AGM & Conference in India in November.

Date	Topic	Presentor	Participated Teams
2/8	Digital Forensics	Sri Lanka CERTCC	CNCERT/CC, EC-CERT, GovCERT.HK, JPCERT/CC, KrCERT/CC, LaoCERT, mmCERT, MNCERT/CC, MyCERT, MOCERT, SingCERT, TechCERT, TaiCERT, TWCERT/CC, TWNCERT
4/19	Mobile Vulnerability Check and Case Study	KrCERT/CC	AusCERT, bdCERT, CERT Australia, CERT-INDIA, EC-CERT, GovCERT.HK, JPCERT/CC, KrCERT/CC, LaoCERT, mmCERT, MNCERT/CC, MOCERT, TechCERT, TWCERT/CC, TWNCERT
8/1	Cyber Detection, Eradication and Forensic (Cyber D.E.F): An active cyber defense approach in mitigating operational risk in cyberspace	MyCERT	AusCERT, CERT Australia, CERT-IN, CNCERT, EC-CERT, GovCERT.HK, HKCERT, JPCERT/CC, LaoCERT, MNCERT/CC, MOCERT, mmCERT, SingCERT, Sri Lanka CERT, TechCERT, TWCERT/CC, TWNCERT, VNCERT
10/3	Cyber Threat Information Sharing	CERT Australia	CERT Australia, CERT-IN, VNCERT, AusCERT, HKCERT, JPCERT/CC, GovCERT.HK, bdCERT, MOCERT, TWCERT/CC, TWNCERT
12/5	Introduction of DDoS Offensive and Defensive Exercise in Taiwan	TWNCERT	CERT-In, GovCERT.HK, JPCERT/CC, KrCERT/CC, LaoCERT, mmCERT, MNCERT/CC, MOCERT, SingCERT, Sri Lanka CERT|CC, TechCERT, TWCERT/CC, TWNCERT

Figure 10 APCERT online training programs in 2017

5.2.2 Drills & exercises

TWNCERT participated in APCERT Drill under the theme "Emergence of a New DDoS Threat" on March 22, and solved a set of drill scenario within the given time limit.

Figure 11 APCERT Drill 2017

5.2.3 Seminars & presentations

Below are international events which TWNCERT has participated in 2017.

- APRICOT 2017, February – Vietnam.

- APEC TEL 55, April – Mexico.
- FIRST and National CSIRT conference, June – Puerto Rico.
- Blackhat USA 2017 & Defcon 25, July – Las Vegas.
- APISC 2017, August – South Korea.
- OWASP AppSec USA 2017, September – United States of America.
- FIRST Symposium TC 2017, September – Taiwan, presented "A Case Study of IoT Cyber Security Threats."
- APNIC 44, September – Taiwan, presented "The Present and The Future ISAC in Taiwan."
- APCERT AGM and Conference 2017, November – India, presented "SC Activity Report by TWNCERT," and "Training Working Group Activity and Survey Report."
- Meridian Conference 2017, November – Norway.
- APEC TEL 56, December – Thailand, presented "The overview of Cyber Offensive and Defensive Exercise (CODE) Program 2017 in Taiwan."

6. Future Plans

For 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 APCERT activities such as APCERT Drill. Possible collaboration opportunities with other international organizations will also continue to be a key emphasis to further enhance depth and broadness of the training program.

7. Conclusion

TWNCERT will continuously enhance the collaboration with the 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. About VNCERT

1.1 Introduction and Responsibilities

VNCERT belongs to the Ministry of Information and Communications of Vietnam. It was established in 2005, by the Decision 339/2005/QD-TTg of Vietnam's Prime Minister. The Term 3 of Article 43 (Emergency for network problems) of Decree No. 72/2013/ND-CP dated July 15, 2013 of the Government (on management, provision and use of internet services and online information) regulates:

"Ministries, ministerial agencies, Governmental agencies, telecommunication enterprises, internet service providers, the organizations in charge of national critical information systems protection have to establish computer emergency teams (CERT) to take actions within their competence and cooperate with Vietnam Computer Emergency Response Teams (VNCERT)".

Roles of VNCERT:

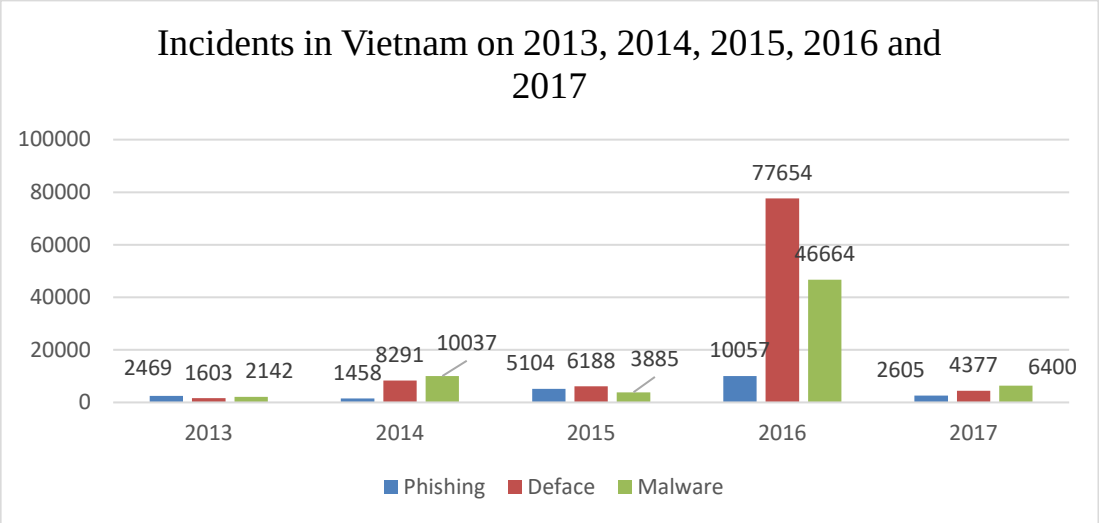
- Being National Coordination Agency for Incident Response nationwide, responsibility for:
- Performing the function of coordinating incident response activities nationwide; Have the right to mobilize and coordinate members of the Vietnam CSIRT Networks and relevant organizations and units to coordinate in preventing, handling and recovering cyber incidents in Vietnam.
- Organizing and administering operations of the Vietnam CSIRT Networks with 165 members (Including: specialized units in charge of incidents response, information security or information technology of ministries, ministerial-level agencies, governmental agencies, provincial-level agencies; telecommunications enterprises and Internet service providers (ISP); organizations and enterprises providing data center services; leasing information space; Units managing and operating the national database; specialized units in information security, information technology of banking, finance, treasury, tax, customs, etc...);
- Monitoring and early warning computer network security problems.
- Building and coordinating to build cyber security technical standard.

- Promoting the formation of local CERTs/CSIRTs in the organizations, enterprises, and agencies in Vietnam.
- VNCERT is the point of contact of Vietnam with the other CERTs in the world.
- Supporting Ministry of Information and Communications of Vietnam with activities in information security state management.
- Implementing and deploying the anti-spam activities.

2. Activities & Operations

2.1 Incident handling reports

In 2017, VNCERT processed 13.382 information security incidents (including 2.605 phishings, 4.377 Defaces and 6.400 Malwares).



Picture 1: Incidents in Vietnam on 2013, 2014, 2015, 2016 and 2017

2.2 Abuse statistics

Security Incidents	2013	2014	2015	2016	2017
Phishing	2.469	1.458	5.104	10.057	2.605
Deface	1.603	8.291	6.188	77.654	4.377
Malware	2.142	10.037	3.885	46.664	6.400
Total	**6.214**	**19.786**	**15.177**	**134.375**	**13.382**

2.3 Incident response coordinating, warning and supporting activities

In 2017 VNCERT had:

- Alerted and required members of national CSIRT network and organization to update 09 vulnerabilities of the Windows Operating System, method exploit of shadow Brokers group (03 weeks before Wannacry campaign)
- Detected and alerted APT attack to Viet Nam.
- Informed and notified about the collection 1.4 Billion Plain-Text Leaked Passwords and required organizations to improve information security solutions.
- Alerted and required organizations block cryptocurrency miners "coinhive" malicious code.

2.4 Anti-spam activities

In 2017, VNCERT received 54.405 advertising text messages (including advertising emails; advertising SMS over Internet)

2.5 Information security legal framework update on

- Law No. 86/2015/QH13 on Cyber information Security 2015, Issue date 19/11/2015, Effective date 01/07/2016.
- Decree No. 85/2016/ND-CP dated July 01, 2016 - on the security of information systems by classification.
- Decision No. 05/2017/QD-TTg dated March 16, 2017 - Regulations on the system of National Cyber Incident Response Plans.
- Circular No 20/2017/TT-BTTTT dated September 12, 2017 - Regulations on coordinating and responding to information security incidents nationwide.
- Circular No. 31/2017/TT-BTTTT dated November 15, 2017 on surveillance of information system security.

3. Events organized / hosted

VNCERT had organized:

- Hosted a training courses on Malware Analysis for LaoCERT in VNCERT.
- Hosted workshop on "Senior level Workshop on International Cyber Security Policy and Diplomacy for CLMV Countries" (CLMV: Cambodia, Laos, Myanmar and Vietnam). Co-organizers by ICT for Peace Foundation and VNCERT.

- Hosted workshop on "The 2nd CAMP Regional Forum" (CAMP: Cybersecurity Alliance for Mutual Progress). Co-organizers by Korea Internet and Security Agency (KISA) and VNCERT. With the participation of delegates from members of CAMP: Vietnam, Korea, Malaysia, Indonesia, Cambodia, Uganda, Kosovo, Mauritius, Mongolia.

4. International Collaboration

- Participated in 03 international drills:
  - APCERT Annual Drill 2017
  - ASEAN-JAPAN Drill 2017
  - ASEAN CERTs Incident Drill 2017
- Negotiated and worked FIRST's delegate about terms and conditions becoming member of FIRST.

5. Future Plans

- To study and draft circular on guiding the organization and operation of incident response teams and job title positions, standards and certificates for members of incident response teams of CSIRT.
- To carry out tasks of the Prime Minister's Decision No. 1622 / QĐ-TTg dated October 25, 2017 approving Project on enhancing the cyber security incident response network and increasing capacity of staffs and specialized units in cyber security incident response to 2020, orientation to 2025.
- To participate international drills.
- To organize national wide drills for Vietnam CSIRT's networks.

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.