APCERT
Asia Pacific Computer Emergency Response Team

TLP: WHITE

APCERT Annual Report 2016

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

CONTENTS

Chair’s Message 2016

2016 was a year for consolidation for APCERT, an opportunity to focus on increased information sharing, training and capacity building within APCERT and to build stronger partnerships both within the Asia Pacific region and beyond the region. It was also a rewarding year for the APCERT community, with effective collaboration both within the region, as well as outreach on a global level. This international collaboration has continued to increase the profile of APCERT.

APCERT’s partnership with the Organisation of Islamic Cooperation CERT (OIC-CERT) continued to develop in 2016. APCERT was pleased to again welcome OIC-CERT participation in its Annual Drill and OIC-CERT representatives to its Annual General Meeting (AGM) and Conference in Tokyo, Japan, in October 2016. Equally, APCERT was honoured to be represented at the OIC-CERT Annual Conference in Jeddah, Kingdom of Saudi Arabia in December 2016, and to present to the Conference on the Asia Pacific cyber security threat environment and APCERT activities.

The partnership between APCERT and APNIC continued to develop throughout 2016, with face-to-face meetings between APNIC and the Steering Committee in the margins of the Asia Pacific Regional Internet Conference on Operational Technologies (APRICOT) in Auckland, New Zealand, in February 2016 and at the 2016 APCERT AGM & Conference. APNIC and APCERT also collaborated with the Forum for Incident Response Security Teams (FIRST) to support a FIRST Technical Colloquium, also in the margins of APRICOT.

I would also like to take this opportunity to recognise JPCERT/CC’s outstanding and ongoing commitment and contribution to APCERT and the international CERT community more broadly. In October 2016, JPCERT/CC celebrated its 20th anniversary, marking it as one of the oldest national CSIRTs in the world. JPCERT/CC was a founding member of APCERT, has been a constant member of the Steering Committee, serving as Chair from 2011-2015, and has provided the Secretariat for APCERT since its foundation. Beyond APCERT, JPCERT/CC has long been an active contributor to the global CERT community and has a strong track record in both collaboration and capacity building. On behalf of the APCERT community, I offer my sincere congratulations to JPCERT/CC.

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.

I also 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.

As always, recognition must also be given to APCERT's Operational Members, who have ensured 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.

CERT Australia is honoured to have been re-elected as Chair of the APCERT Steering Committee 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 2016, APCERT consists of 28 Operational Members from 20 economies across the Asia Pacific region and 3 Supporting Members.

Operational Members (28 Teams / 20 Economies)

Team	Official Team Name	Economy
AusCERT	Australian Computer Emergency Response Team	Australia
bdCERT	Bangladesh Computer Emergency Response Team	Bangladesh
BruCERT	Brunei Computer Emergency Response Team	Negara Brunei Darussalam

CCERT	CERNET Computer Emergency Response Team	People's Republic of China
CERT Australia	CERT Australia	Australia
CERT-In	Indian Computer Emergency Response Team	India
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	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

Supporting Members (3 Teams)

- Bkav Corporation
- Microsoft Corporation
- SecureWorks

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

At the APCERT AGM 2016, CERT Australia was re-elected as Chair of APCERT, and Malaysian Computer Emergency Response Team (MyCERT) as Deputy Chair.

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

Team	Term	Other positions
CERT Australia	2016 - 2018	Chair
CNCERT/CC	2016 - 2018	
JPCERT/CC	2015 - 2017	Secretariat
KrCERT/CC	2016 - 2018	
MOCERT	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 meets 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

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 2016

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 2016, APCERT Teams have hosted, participated and/or contributed in the following events:

- **APCERT Drill 2016 (16 March)**

  https://www.apcert.org/documents/pdf/APCERTDrill2016PressRelease.pdf

  APCERT Drill 2016, the 12th 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. 26 teams from 20 economies of APCERT (Australia, Bangladesh, Brunei Darussalam, People's Republic of China, Chinese Taipei, Hong Kong, India, Indonesia, Japan, Korea, Lao People's Democratic Republic, Macao, Malaysia, Mongolia, Myanmar, New Zealand, Singapore, Sri Lanka, Thailand and Vietnam), and 6 teams from 6 economies of OIC-CERT (Egypt, Morocco, Nigeria, Oman, Pakistan and Tunisia) participated in the Drill. The theme of the drill was "An Evolving Cyber Threat and Financial Fraud".

- **APEC-TEL 53 (12-17 June - Tacna, Peru)**

  CNCERT/CC represented APCERT at APEC TEL 53, and presented the APCERT's overview and latest activities for a safer cyber space base on the regional framework.

- **28th Annual FIRST Conference (12-17 June - Seoul, Korea)**

  https://www.first.org/conference/2016

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

- National CSIRT Meeting (17-18 June - Seoul, Korea)

  APCERT teams attended the National CSIRT Meeting, hosted by CERT/CC and exchanged various activity updates as well as recent projects and research.

- APCERT Annual General Meeting (AGM) & Conference 2016 (24-27 October - Tokyo, Japan)

  https://www.apcert.org/apcert2016/

  The APCERT Annual General Meeting (AGM) & Conference 2016 was held on 24-27 October, 2016 at Royal Park Hotel in Tokyo, Japan.

  Programme Overview:

24 October (Mon)	AM:	Working Group Meetings
	PM:	APCERT Team Building, Welcome Cocktail
25 October (Tue)	AM:	TSUBAME/Cyber Green Workshop
	PM:	Steering Committee Meeting
26 October (Wed)	AM:	APCERT Closed Conference
	PM:	APCERT Annual General Meeting
27 October (Thu)	AM:	Open Conference

- TSUBAME Workshop 2016 (25 October - Tokyo, Japan)

  The APCERT TSUBAME Workshop 2016 on Network Traffic Monitoring Project was held on 26 October, in conjunction with APCERT AGM & Conference 2016. JPCERT/CC enhance the TSUBAME project and the cooperation among its members.

- ASEAN CERT Incident Drill (ACID) 2016 (27 September)

  ACID 2016, led and coordinated by SingCERT, entered its 11th 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.

- APEC-TEL 54 (30 October – 4 November - Kyoto, Japan)

  TWNCERT represented APCERT at APEC TEL 54, and presented the APCERT's overview and latest activities for a safer cyber space base on the regional framework.

- **The OIC-CERT 8th Annual General Meeting and Annual Conference 2016 (11-14 December - Jeddah, Saudi Arabia)**
  https://www.oic-cert.org/event2016/index.html
  As APCERT Chair team, CERT Australia represented APCERT. An introduction of APCERT members and main activities were given at the presentation session.

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.

20 January	Teleconference
22-23 February	Face-to-face meeting concurrently held at APRICOT 2016 in Auckland, New Zealand
19 April	Teleconference
24 June	Teleconference
18 August	Teleconference
20 September	Teleconference
25 October	Face-to-face meeting at APCERT AGM 2016 in Tokyo, Japan

3. APCERT Training Calls

APCERT held six (6) training call in 2016 to exchange technical expertise, information and ideas.

Date	Title	Presenter
3 February	Introduction to Network Forensics and Analysis	TWNCERT
6 April	Internet of Things (IoT) Trend	ID-SIRTII/CC
1 June	A Presentation on How to Help Organizations Conduct Effective Exercises	SecureWorks
3 August	Tactical against malicious scanning network	HKCERT
5 October	The Growing Threat of Ransomware in Malaysia	MyCERT
7 December	How Microsoft Safeguards Your Data in the Cloud	Microsoft

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 2016

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 SOC Deployment

During 2016 AusCERT has established a Security Operations Center (SOC) servicing a section of its constituency.

1.2.2 Flying Squad on handling Australia's largest PII leakage.

AusCERT's Flying Squad was called in to handle Australia's largest private information leak. This was testament to the high level of service that AusCERT offers its constituency in handling time critical and sensitive incident handling events.

1.2.3 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:

- Security Bulletins (3.2)
- Incident Management (3.3)
- Early Warning (3.4)
- Malicious URL Feed (3.5)
- Phishing Take Down (3.6)
- AusCERT's member only IRC channel
- AusCERT Conference
- AusCERT Certificate Service

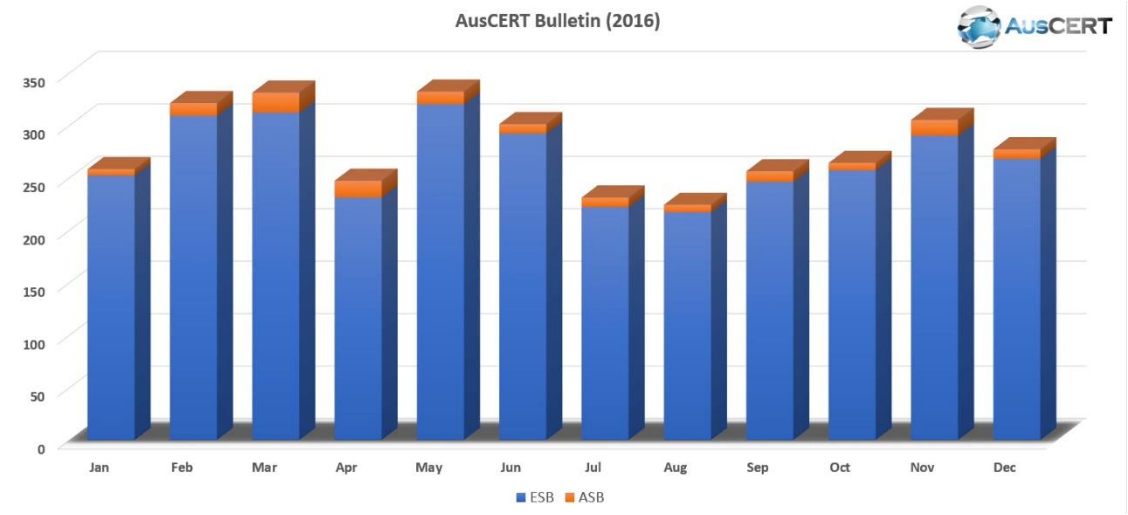
Full details on AusCERT's operations, services and activities can be found here: https://www.auscert.org.au/services

3.2 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.

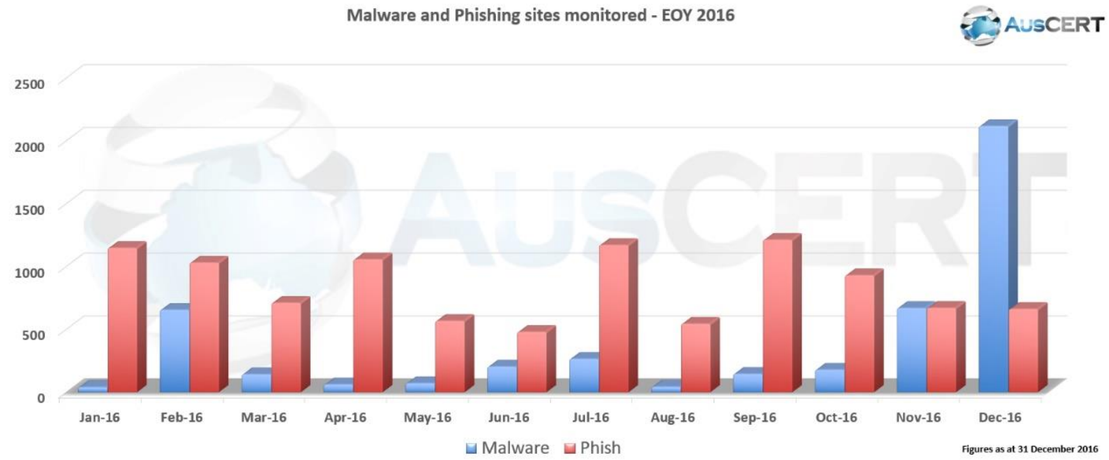
During 2016, three thousand and ninety-one (3,091) External Security Bulletins (ESBs) and one hundred and twenty-two (122) AusCERT Security Bulletins (ASBs) were published.

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.



3.3 Incident handling reports

AusCERT's Incident Management Service (sometimes referred to as incident response) includes incident coordination and incident handling, both of which are standard inclusions as part of AusCERT's 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 2016. These tallies are sites that are located around the world in a manner that affects the operation of the constituency that AusCERT is serving.

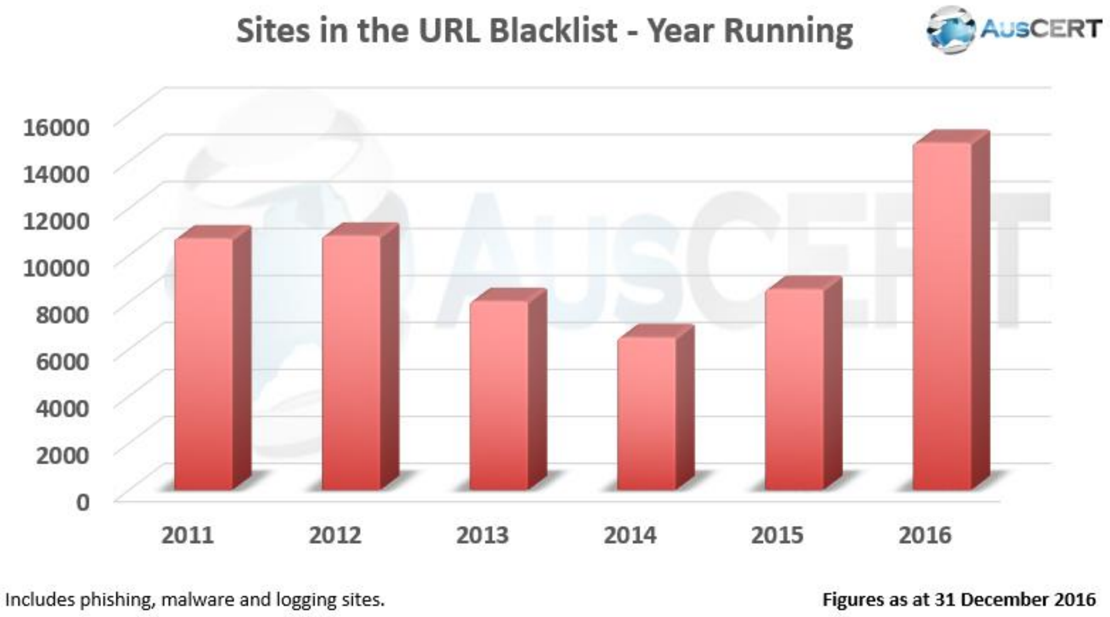
3.4 Early Warning System

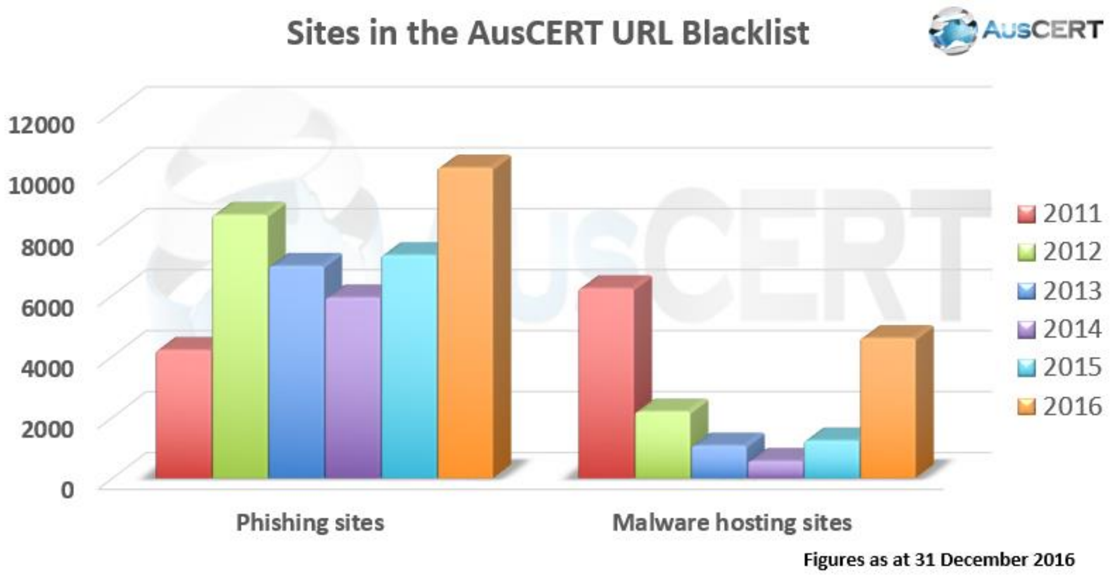
Members can subscribe to receive urgent SMS notifications, when AusCERT's Security Bulletin Service identifies a vulnerability that has reached critical stages. In most circumstances this occurs when AusCERT is aware of active, in-the-wild exploitation of a vulnerability.

Alerts are sent along with Bulletins, but are given special importance. Throughout the year of 2016 ninety-three (93) 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.

3.5 Malicious URL List.

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.



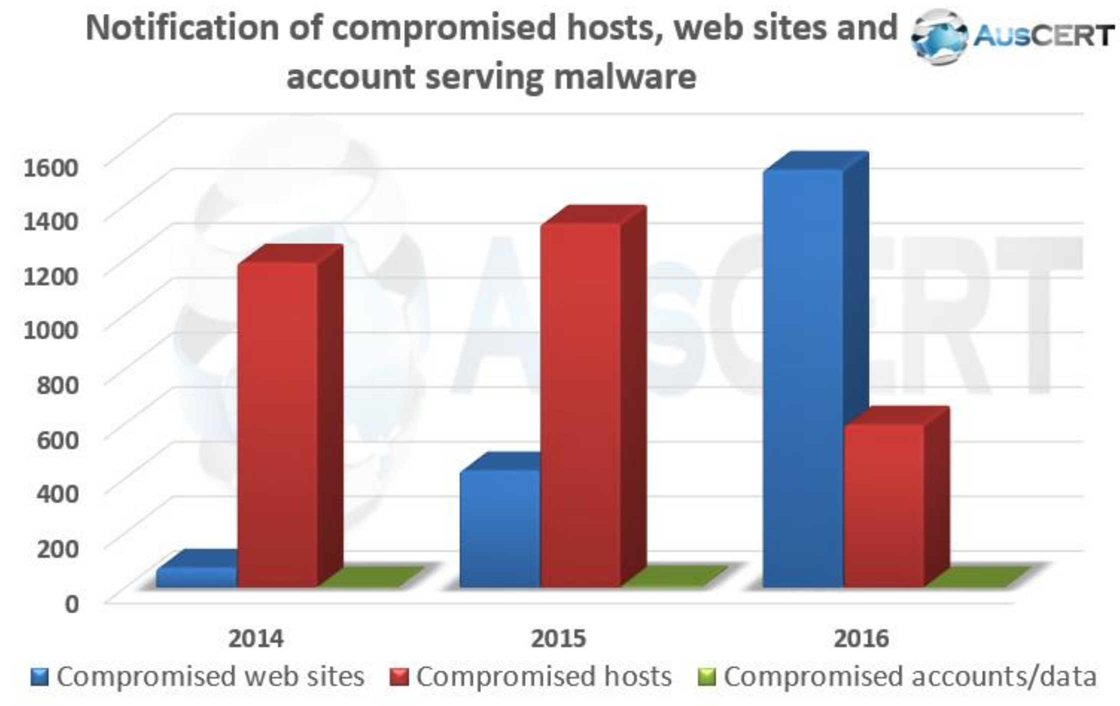


3.6 Phishing Takedown

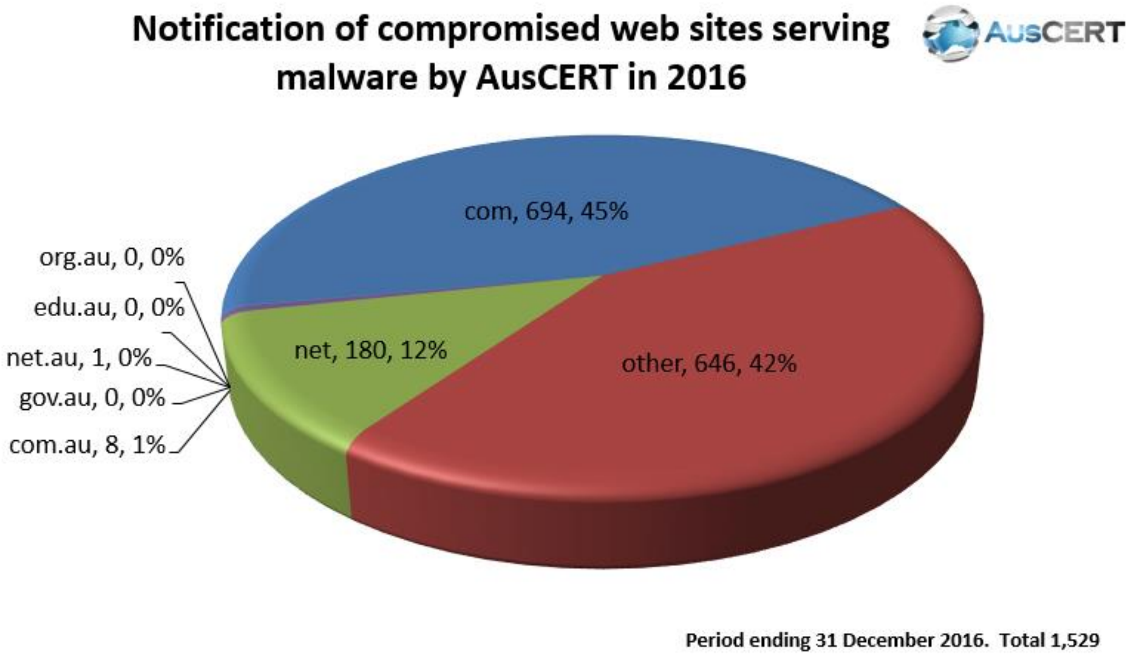
AusCERT Members can utilise AusCERT's considerably large overseas and local contact network for removal of phishing and malware sites. The number of sites that were handled in the year 2016 has already been graphed in the section Malware URL. Specifically, for Phish site, an increased number of phish sites were handled as compared to the previous year. The tally for 2016 was Ten thousand one hundred and eighty-four (10,184) a thirty-nine percent (39%) increase from 2015's tally of seven thousand three hundred and seventeen (7,317).

3.7 Abuse statistics

As for websites that have been compromised and serve malware, three thousand seven hundred and ninety-four (3,794) sites have been reported in the calendar year of 2016.

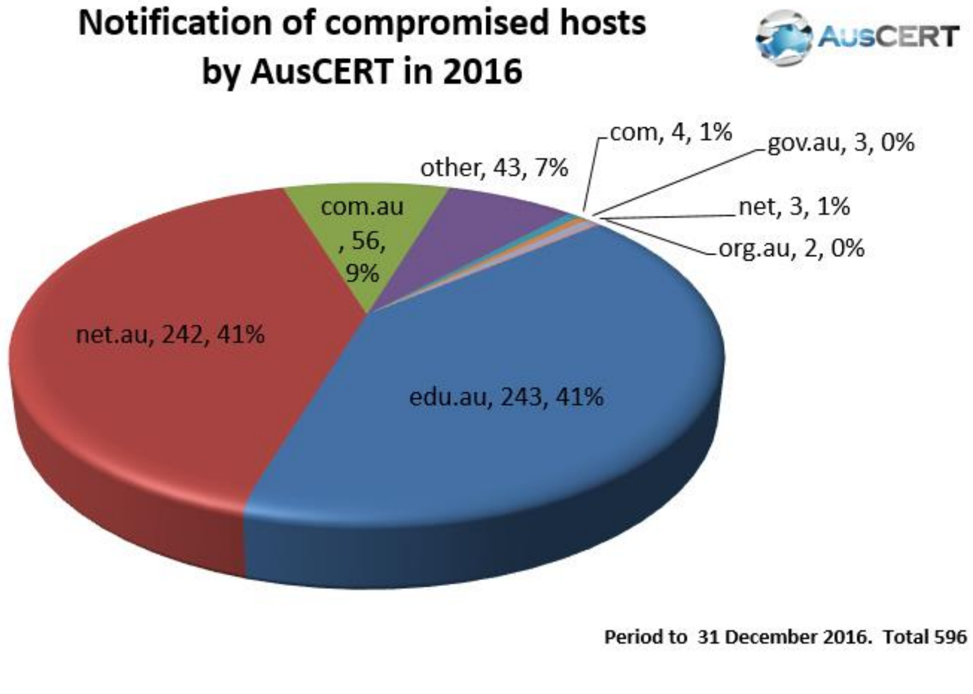


AusCERT email notifications of compromised hosts and web sites in Australia and overseas. **As at 31 December 2016.**



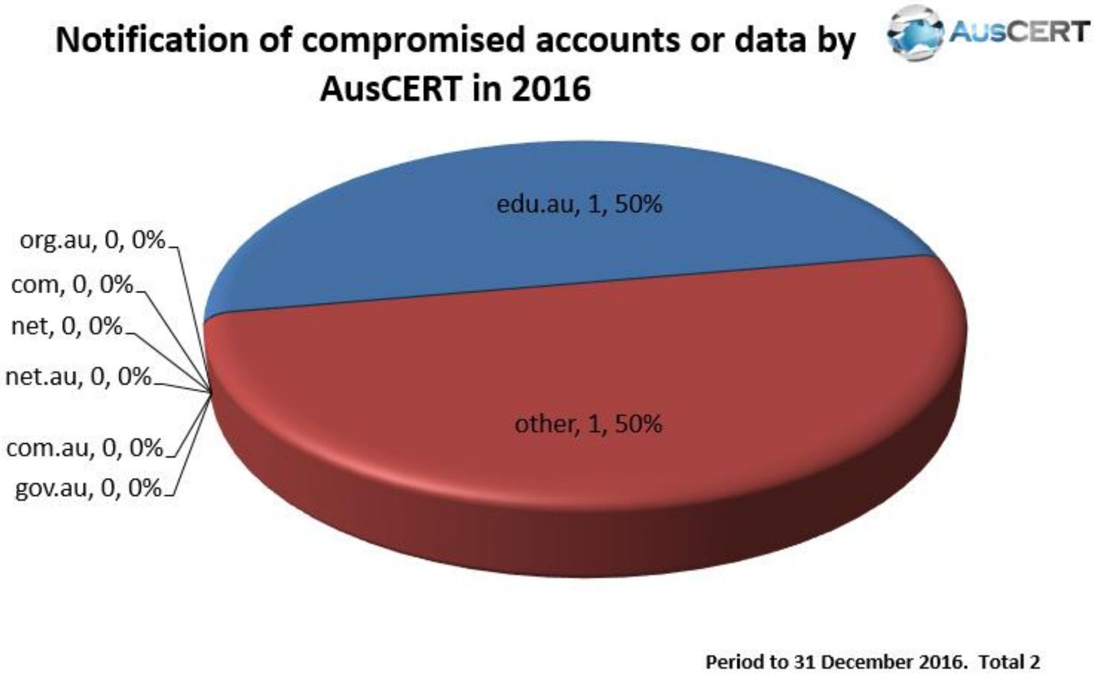
Notification of compromised web sites serving malware by AusCERT in 2016

Period ending 31 December 2016. Total 1,529



Notification of compromised hosts by AusCERT in 2016

Period to 31 December 2016. Total 596



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. Two publications were issued out in the year of 2016, for the month of February and the month of July.

4. Events organized / hosted

4.1 AusCERT Conference

The AusCERT Conference, took place from 23rd-27th May 2016 in Surfers Paradise Gold Coast, Australia. The conference covered areas such as:

- Growing concern surrounding interconnectivity of devices and systems; their ability to be remotely accessed or controlled;
- Do individuals and companies care about the ability of these devices being exploited and misused resulting in adverse consequences?
- What are the privacy concerns about ubiquitous, interconnected devices?
- Should we be concerned or embrace the personalised service delivered by ubiquitous devices from the personal data they collect?

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 2016

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 "An Evolving Cyber Threat and Financial Fraud" wherein AusCERT played through several scenarios of financial fraud. The drill is extremely valuable as it fosters communication between all of the CERTs in the region and beyond. In all, 26 CERT teams from APCERT participated, along with teams from 6 economies of 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 2016 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 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.

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 2015

2.1 Incidents response

In 2015, BruCERT receives quite a high numbers of security incidents reports from both the public and the private sector. There were an increasing number of incidents that had been reported to BruCERT, which show positive feedbacks from the Brunei community. There was also a decreasing number of website that had been defaced in Brunei. This might due to the increasing awareness of the government and the public sector regarding the importance of Information security to maintain their website. Most of the defacement are due to lack of security controls being placed and install security patches on the victims' sides. The statistic of the security incident is shown as Figure 1.

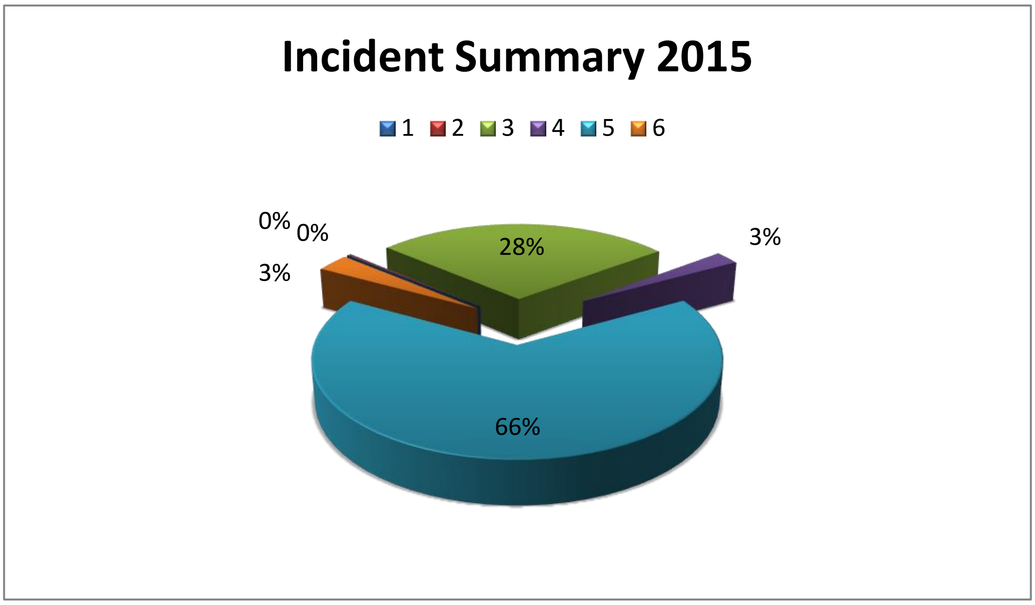


Figure 1

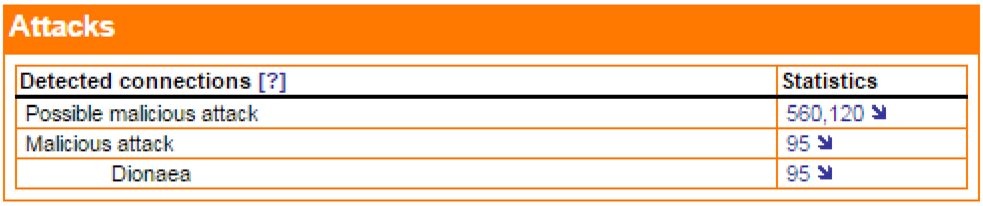
Types of Attack	Count
Malicious Website	1
Cyber Harassment	2
Spam	542
Scam	9
Malicious Software	832
Website defacement	8

2.2 Summary of BruCERT Honey Pot Project

In this section, BruCERT had deployed the Honey Pot project initiative with TelBru. With this Honey Pot, BruCERT can have a better understanding, what is the current security landscape of Brunei cyber space.

Summary of honeypot activities

This data shows the overall activities from the honeypot starting from January 2015 until December 2015.

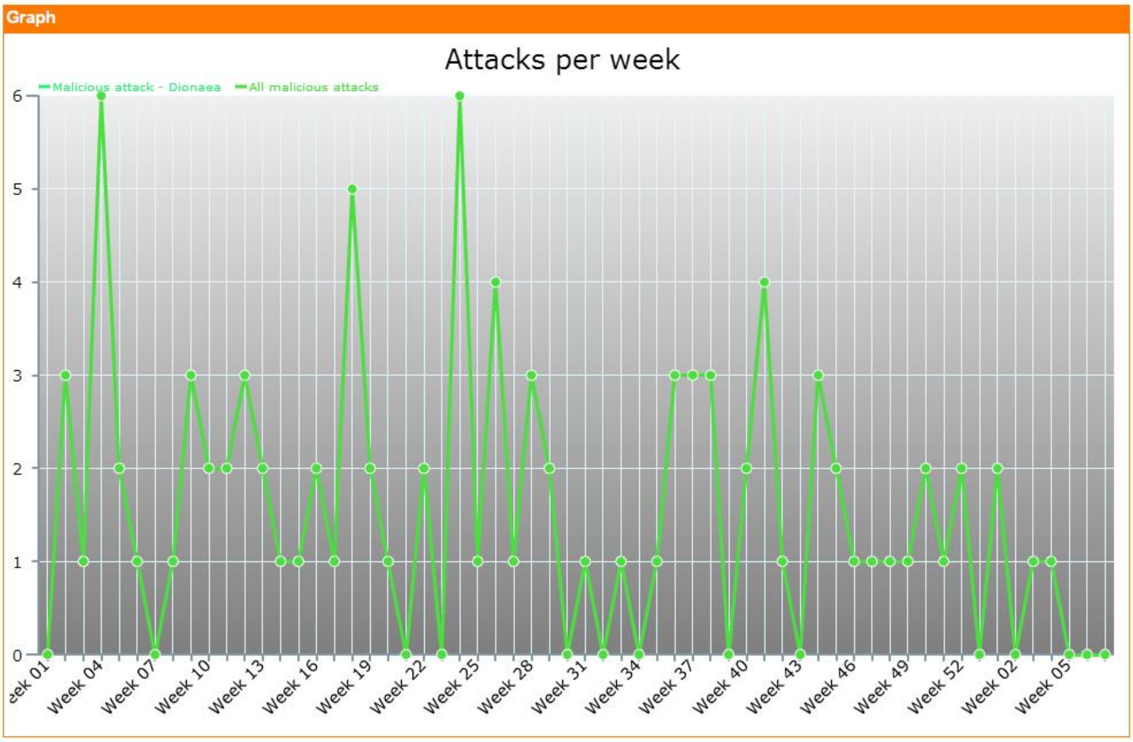


Attacks

Detected connections [?]	Statistics
Possible malicious attack	560,120 ↘
Malicious attack	95 ↘
Dionaea	95 ↘

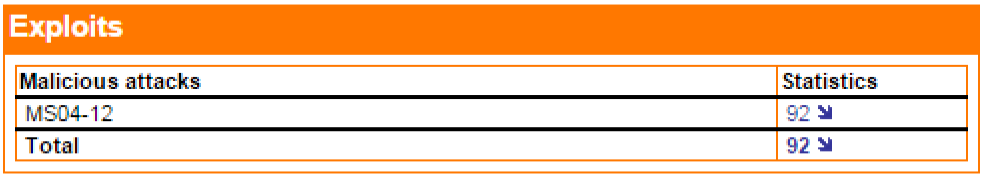
Total Malicious attack

Daily data on malicious attack from attacker origins, to the honeypot.



Exploits targeted by malware

Exploits used by the malware and the total number of times it has been used.

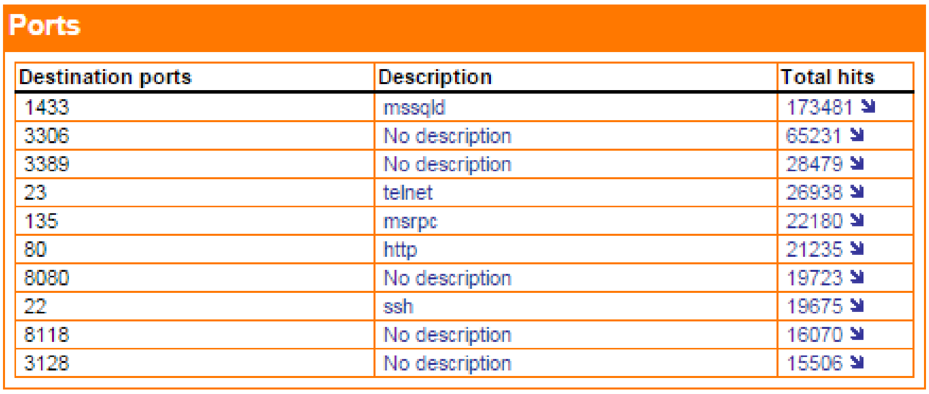


Exploits

Malicious attacks	Statistics
MS04-12	92
Total	92

Most attacked Port

Most attacked port and total number of hits.



Ports

Destination ports	Description	Total hits
1433	mssqld	173481
3306	No description	65231
3389	No description	28479
23	telnet	26938
135	msrpc	22180
80	http	21235
8080	No description	19723
22	ssh	19675
8118	No description	16070
3128	No description	15506

Destination ports	Descriptions	vulnerabilities
3306	MySQL database system	MySQL Authentication bypass
1433	MSSQL (Microsoft SQL Server database management system) Monitor	Exploit buffer overflows, hijack existing sessions and to misuse privileges once authenticated
135	MSRPC	CVE-2003-352 CVE-2003-528 CVE-2003-533 CVE-2003-717 CVE-2003-813 Buffer overflow in certain DCOm interface allows remote attackers to execute arbitrary code via malformed message.
3389	Microsoft Terminal Server (RDP)	CVE-2012-0173 Vulnerabilities provides attackers with remote access via Remote Desktop Protocol (RDP).
5000	"Universal Plug and Play(UPNP) is a technology pioneered and developed by Microsoft	CVE-2013-6987 CVE-2013-6955

3. BruCERT Activities in 2015

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 September 2015 until 10th September 2015 - Four BruCERT delegates attended the APCERT and OIC-CERT AGM and Annual Conference 2015 which takes place at Kuala Lumpur, Malaysia, hosted by MY-CERT.

3.2 Awareness Activities

- **Cyber Battle: Capture The Flag (CTF)**
  October 4 & 11, 2015

BruCERT organized CTF with the support of AiTi. The event was open to citizens and permanent residents of Brunei Darussalam (aged 30 years old and below). Publicity for the event included a press conference, newspaper ads, social media posts, and online contests through Facebook and Instagram.

14 teams had registered for the competition. An elimination round was held on the October 4 at ITPSS to determine the top 10 teams who would compete in the actual event. The final of the competition was held a week later on 11th October 2015. The top 2 teams from the competition were selected to represent Brunei at Cyber SEA Games 2015 that was held in Jakarta in November.

- **TechXpo 2015: BruCERT Carnival**
  October 22-25, 2015

BruCERT joined the 4-day TechXpo 2015, organized by D'Sunlit at the ICC. The objective of our participation in the expo was to spread IT security awareness to the public. Prior to the roadshow, we started advertising the upcoming carnival through social media, providing teasers on what can be expected from our booth.

We came up with a newly designed booth with a carnival theme, with a few different activities. The vibrant look and feel of the booth, in addition to the fun activities and prizes were successful in attracting visitors. A quick survey showed that 90% of visitors enjoyed their visit to the BruCERT Carnival.

The activities on offer were Password Challenge, Social Media Checkup, Dumpster Diving, and Think Before You Post.

4. Conclusion

In 2015, BruCERT observed an improvement in IT security response in both the public and government agencies comparing to the previous years. 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.

This report also concludes the honeypot finding for the month January to December 2015. The honeypot continuously detecting massive possible malicious attack or attempt of compromise on MySQL database system services (port 3306) and (MSSQL, Microsoft SQL Server database management system) server (port 1433). Port 23 and 22 were still being constantly scanned for is vulnerabilities followed by port 8080, 135, and also port 3128.

CCERT

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

1. Introduction

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

The main tasks of CCERT include:

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

2. Summary for 2016

2.1 Handling security incident complaints from CERNET users

In 2016, CCERT handled 1438 security incident complaints, which include 321 for Spams, 883 for Website Intrusion, 127 for Port Scanning, 18 for Phishing Site Complaints, 24 for DoS Attack, 29 for System Intrusion and 36 for other network security complaints.

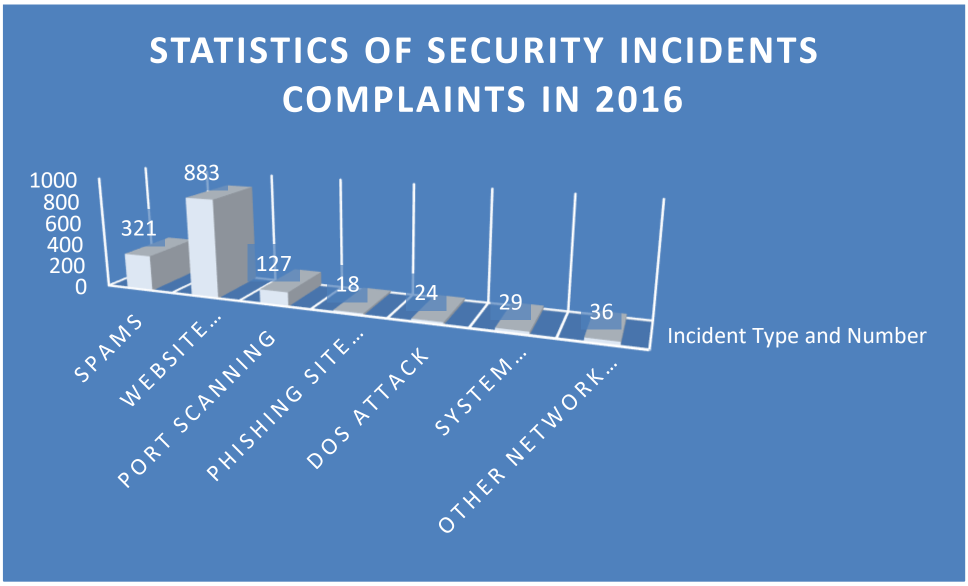


Figure 1

Compared to 2016, the number of security incidents reported to CCERT in 2016 is decreased significantly. We think the main reason for such decrease is that China has been paying more attention to network information security. More and more administration departments and organizations set up their own network security teams, that is, most of the information security incidents are directly forwarded to the users involved instead of CCERT acting as information distributor. Looking at the security incidents in 2016, the number of website information security incidents is still the highest one, while the proportion of spam is being lowered year by year, which might be due to the change in information communication approach, i.e. the instant message and social software are gradually taking part of the role of e-mail software.

2.2 Security Monitoring and Information Publication

In 2016, CCERT carried on the analysis and evaluation of the security situation, and sent large-scale alarm messages the users for 6 times. One thing to be emphasized is that we made a comprehensive technical analysis on the emergency Shadow Brokers event in the middle of 2016, and sent alerts to users and vendors who might be impacted, and continuously follow up this case for consequence assessment.

2.3 Technical Consultation and Security Service

In 2016, CCERT provided security scanning service (free of charge) to 11349 websites, and found that there are about 995 websites with high-risk vulnerabilities (8.77%), 899 websites with middle-risk vulnerabilities (7.92%), and 1172 websites with low-risk vulnerabilities (10.33%). No security problems was detected on 8281 websites (72.98%)

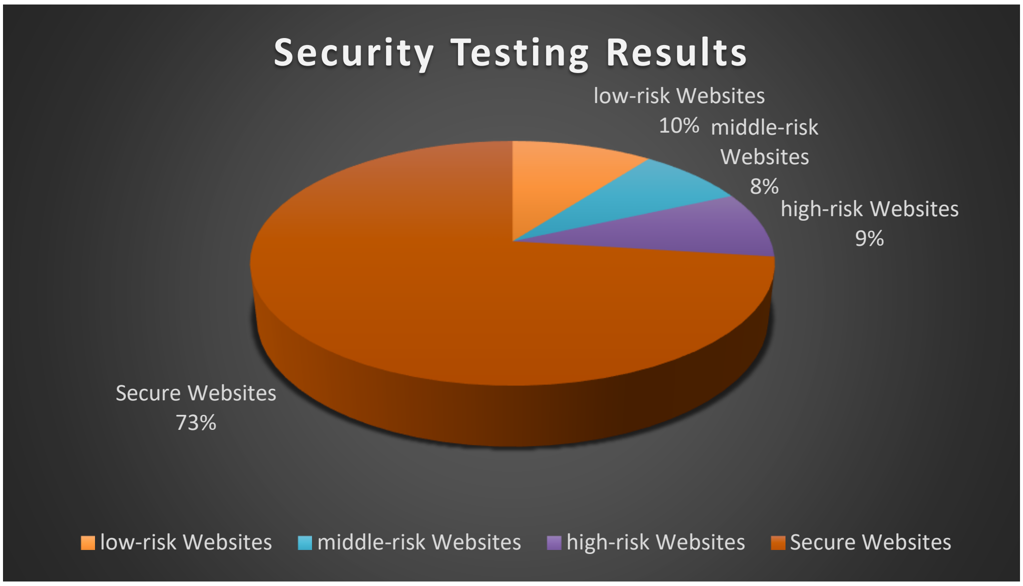


Figure 2

Attribute to the Chinese government's focus on network information security, the security of China's domestic website has been considerably improved, and the proportion of website with high-risk vulnerabilities decreased significantly in comparison with 2015.

2.4 Security training and activities

CCERT held 23 training workshops with totally 3018 participants in 2016, in which the security topics include:

- Security analysis on the department website systems in colleges and universities
- Security consideration in construction and maintenance of campus wireless networks
- HOWTO for big data platform of campus security
- Security of web system
- Interpretation of Network Security Act
- Information security authentication system
- Principle and testing technology of web application security vulnerability
- The CTF challenge start-up training for university security management and operations

- Analysis of the CTF competition questions for university security management and operations

3. Future plan for 2017

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 2016

1.1 Summary of major activities

Working with the APCERT community throughout 2016 as Chair of the APCERT Steering Committee was a key priority and highlight for CERT Australia. In October 2016, CERT Australia was honoured to be re-elected to the Steering Committee and subsequently as Chair of the Committee for a second term.

1.2 Achievements & milestones

In April 2016, the Australian Government released *Australia's Cyber Security Strategy; Enabling innovation, growth & prosperity.* 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.

2. About CSIRT

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 49 core staff, a significant growth from 23 last year.

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 2016, CERT Australia had 11,260 cyber incidents reported, a decrease of approximately 28 per cent from 2015. The reduction in incidents is largely due to the smaller number of notifications received from third parties relating to compromised websites. The incidents handled by CERT in 2016 required a range of responses depending on their nature. Significantly, 439 of these incidents specifically affected the CI and other SNI (an increase of almost 42% from the previous year).

3.3 Abuse statistics

The Australian Cyber Security Centre (ACSC) has released its second Threat Report in

October 2016. The report provides 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_2016.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

Under the Australian Government's Cyber Security Strategy, CERT Australia has been given the lead to deliver a new national awareness raising program covering education and awareness for cyber risks across the private and public sectors. Under the Strategy CERT Australia is also responsible for exercising Australia's national Cyber Incident Management Arrangements.

In 2016, CERT Australia significantly increased the number of domestic and international partners able to access STIX-formatted threat information via its TAXII services. CERT Australia also released an open source software tool (the 'cti-toolkit') which enables partners to easily download and process STIX-formatted threat material into a variety of different formats to facilitate its use in their own environments.

4. Events organized / hosted

4.1 Drills & exercises

CERT Australia was involved in 14 different cyber security exercises throughout 2016, of these seven were international exercises, four were with business and industry partners and 3 were for government or law enforcement.

4.2 Conferences and seminars

CERT Australia supported the Annual ACSC Conference, held in Canberra in April 2016. This conference brought together 1,130 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 Cyber Strategy has outlined a number of ways in which Australia will fulfill global responsibility. In November 2016, Australia announced the appointment of Dr Tobias Feakin as Australia's inaugural Ambassador for Cyber Affairs.

The Australian Government is working on an international cyber engagement strategy that will facilitate further international partnerships.

5.2 Capacity building

Australia's cyber security strategy commits to building cyber capacity in the Indo-Pacific region and elsewhere, including through public-private partnerships. This will include sharing techniques to combat cybercrime, and enable close collaboration between national CERTs.

5.2.1 Training

There were no formal international training activities undertaken in 2016.

5.2.2 Drills & exercises

CERT Australia participated in seven international exercises in 2016.

5.2.3 Seminars & presentations

CERT Australia presented at the Asia Pacific Regional Internet Conference on Operational Technologies (APRICOT) in Auckland, New Zealand in February and chaired the APCERT Conference in Tokyo, Japan in October.

Throughout 2016, CERT Australia also presented at and/or participated in several other international forums including:

- S4 (SCADA Scientific Security Symposium), January - USA
- International Watch and Warning Network (IWWN) Annual Meeting, June –New Zealand
- FIRST conference, June – Republic of Korea
- Blackhat & DefCon, August – USA
- New Zealand Internet Task Force 2015 Conference, November – New Zealand
- Kiwicon, November – New Zealand
- Other closed events organised by international government organisations and CERTs

6. Future Plans

6.1 Future projects

The Australian Government announced the launch of the Joint Cyber Security Centres (JCSC), as part of the Government's Cyber Security Strategy. The JC will be centralized information sharing centres that provide up-to date information about the nature and number of cyber threats. A pilot will be located in Brisbane and will be officially launched in February 2017 before being rolled out across Australia.

6.2 Future Operation

CERT Australia will continue to grow as outlined in the Australian Cyber Security Strategy, with a focus on International partnerships and Collaboration. CERT Australia will continue to value the ongoing engagement with the APCERT community and this will be a continued focus for CERT Australia in the future.

7. Conclusion

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

CERT-In

Indian Computer Emergency Response Team – India

1. Highlights of 2016

1.1 Summary of major activities

a) CERT-In operationalized the Botnet Cleaning and Malware Analysis Centre for common users.

b) In the year 2016, CERT-In handled 50362 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, 57262 spam incidents were also reported to CERT-In. Remedial measures for handling incidents were suggested and implemented in coordination with relevant stakeholders.

c) CERT-In is keeping track on latest cyber threats and vulnerabilities. 12 security alerts, 79 advisories and 325 Vulnerability Notes were issued during the year 2016. In addition, 19 Advisories on the use of digital payments channels including DOs and DONTs are issued and circulated among various stakeholders.

d) Cyber security awareness sessions have been conducted for common users regarding security measures to be taken while using digital payment systems under the Government's TV Awareness Campaign.

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 close coordination and collaboration with Internet Service Providers academia and Industry. Website of the centre was operationalised in December 2016. 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 mock drills with organizations from key sectors to enable participating organizations to assess their preparedness in dealing with cyber crisis situations. 11 such mock drills have been conducted so far.

- In 2016, CERT-In signed MoUs with CERT-UK, Information Security Centre Uzbekistan and Cyber Security Department Vietnam 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 designate d 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. The constituency of CERT-In is the Indian cyber community. CERT-In works closely with the Chief Information Security Officers (CISOs) and System Administrators of various sectoral and organisational networks of its constituency.

2.3 Resources

CERT-In has a team of 50 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 and Operations of CERT-In

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 2016 is given in the following table:

Activities	Year 2016
Security Incidents handled	50362
Security Alerts issued	12
Advisories Published	98
Vulnerability Notes Published	325
Trainings Organized	11
Indian Website Defacements tracked	31664
Bot Infected Systems tracked	10020947

Table 1. CERT-In Activities during year 2016

3.3 Abuse Statistics

In the year 2016, CERT-In handled 50362 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, 57262 spam incidents were also reported to CERT-In.

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

Security Incidents	2016
Phishing	757
Network Scanning / Probing	416
Virus/ Malicious Code	13371
Website Defacements	31664
Website Intrusion & Malware Propagation	1483
Others	2671
Total	50362

Table 2. Breakup of Security Incidents handled

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

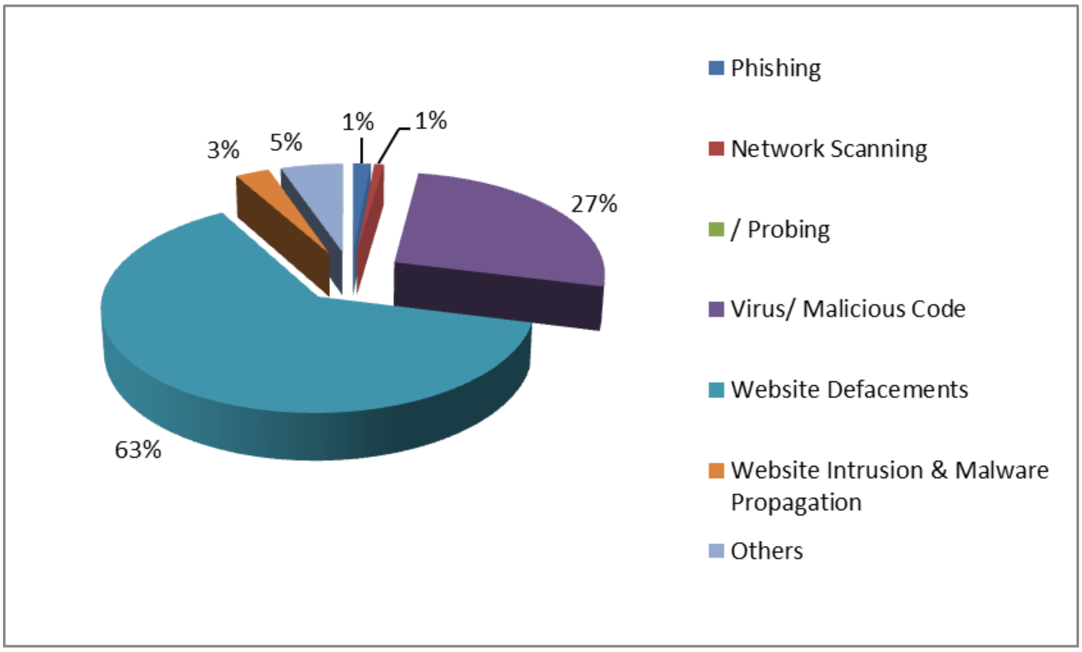


Figure 1. Summary of incidents handled by CERT-In during 2016

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 31664 numbers of defacements have been tracked.

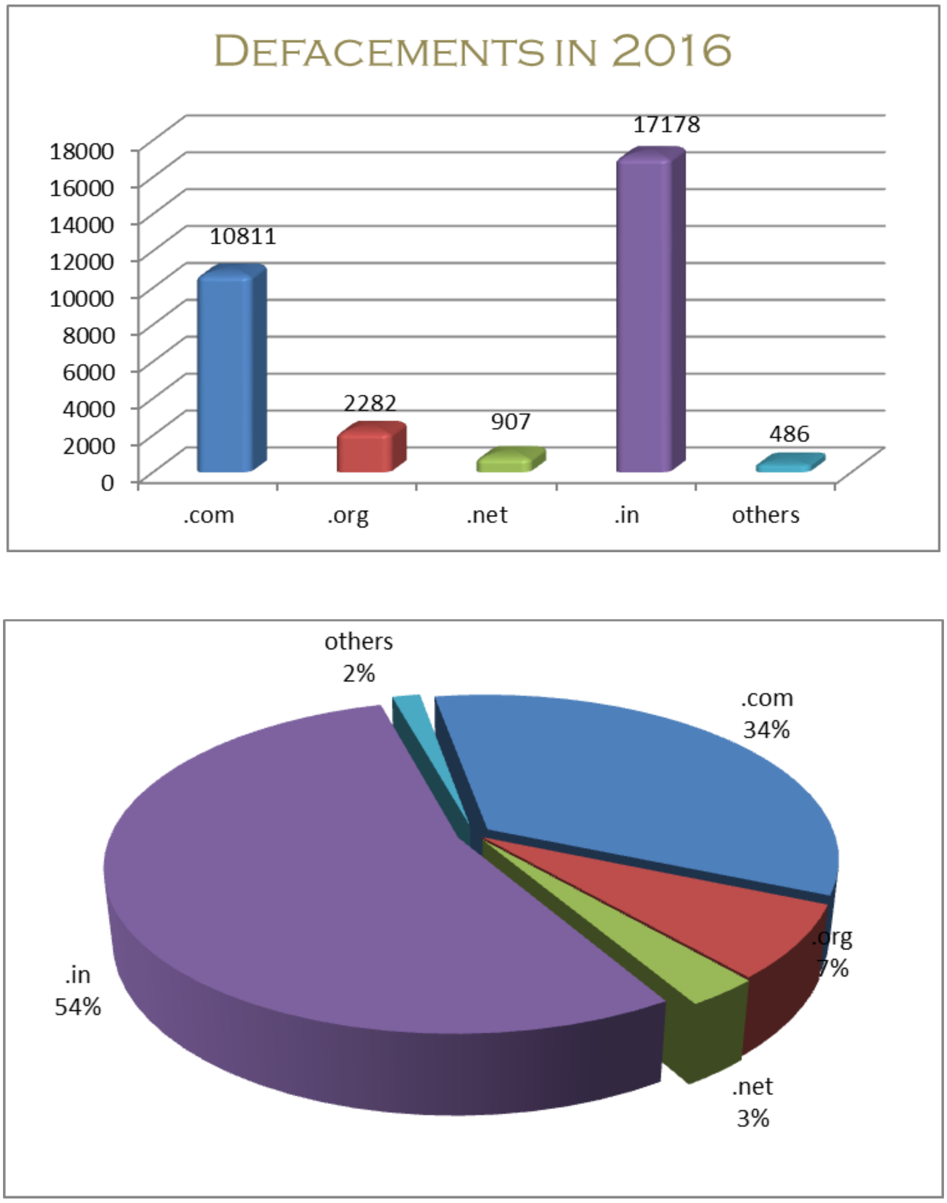
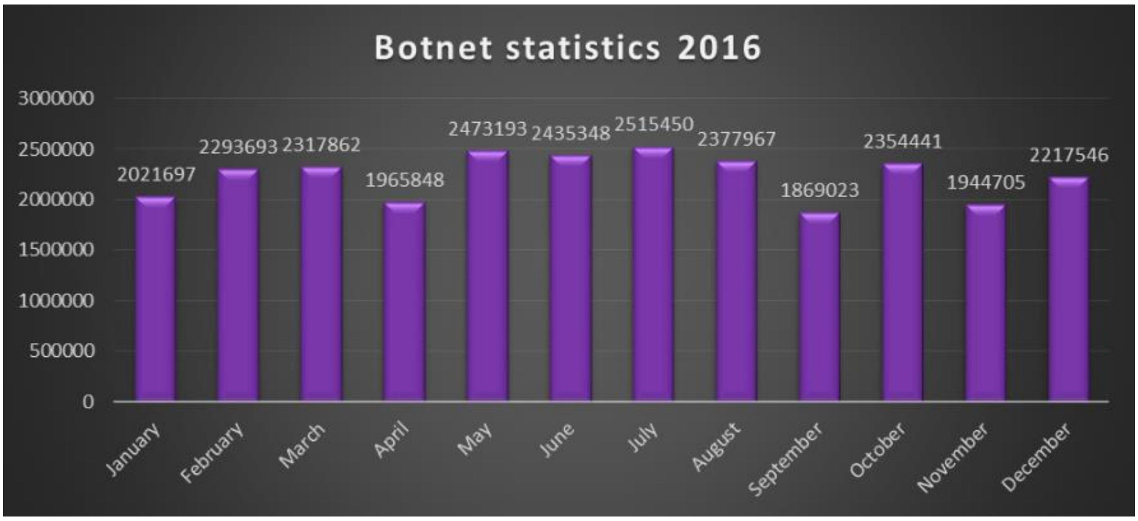


Figure 2: Domain-wise Breakup of Indian Websites Defaced in 2016

3.3.2 Botnet Tracking and Mitigation

CERT-In is tracking Bots and Botnets involving Indian systems. After tracking the IP addresses of systems that are part of Botnet, actions are being taken to notify concerned users in coordination with the Internet Service Providers and advise them to clean the respective systems and prevent malicious activities. Figure 4 shows the number of Bot infected systems tracked in 2016.



3.4 Services

3.4.1 Security Profiling, Assurance framework and Audit Services

- Under Security Assurance Framework, CERT-In has empanelled 32 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 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 IT security auditors are being used to verify compliance.
- CERT-In has also carried out episodic security audits of key organizations for enhancing their security posture.

3.4.2 Network Traffic Scanning for early warning

CERT-In has set up a facility to gather useful network information from different IT networks across the country for meaningful analysis to detect and predict possibilities of cyber attacks. At present, some organizations are voluntarily providing network traffic information to CERT-In for proactive scanning of their networks. This facility is meant only to scan the network traffic data header information and no content data is captured or scanned. CERT-In is analyzing this network traffic information for providing immediate alerts and tailored advisories to the participating organizations.

4. Events organized/ co-organized

4.1 Education and Training

To create awareness and to enable users to implement best practices, CERT-In is organizing workshops and training programmes 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 CERT-In staff.

CERT-In has conducted the following training programmes during 2016:

- Workshop on "IPv6 Security" on December 16, 2016
- Workshop on "Secure Coding Practices" on November 18, 2016
- Workshop on "Cyber Security Threats & Cyber Forensics" on October 26, 2016
- Workshop on "Endpoint Security & Secure IT Infrastructure" on October 14, 2016
- Workshop on "Advanced Targeted Attacks" on July 29, 2016
- Workshop on "Cyber Attack Trends and Mitigations" on June 30, 2016
- Workshop on "Cyber Security Threats and Countermeasures" on May 31, 2016
- Workshop on "DDoS Attacks & Mitigation" on February 29, 2016
- Workshop on "Encrypted Traffic & Hidden Threats" on February 25, 2016
- Workshop on "Emerging Cyber Security Threats and Challenges" on January 29, 2016
- Workshop on "Cyber Crisis Management Plan, Compliance & Auditing" on January 22, 2016

4.2 Drills and exercises

Cyber Security Mock Drills are being conducted by the Government to help the organisations to assess their preparedness to withstand cyber attacks. These drills 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. Till date CERT-In has conducted 11 Cyber security drills of different complexities with participation from more than 110 organizations covering various sectors of Indian economy i.e. Defence, Paramilitary forces, Space, Atomic Energy, Telecommunications(ISPs), Finance, Power, Oil & Natural Gas, Transportation(Railways & Civil Aviation) , IT/ ITeS/ BPO sectors and Data Centres from Government/Public/ Private. Joint Cyber Security Drill by CERT-In & RBI was successfully conducted on September 30, 2016 for various banks to enable them to assess their emergency incident response preparedness.

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 crimes and cyber attacks as well as collaborating for providing swift response to such incidents. In 2016 CERT-In has been signed MoUs with CERT-UK, Information Security Centre Uzbekistan and Cyber Security Department Vietnam. 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 2016 conducted on 16 March 2016 based on the theme “Evolving threat and financial fraud” to test the response capability of leading Computer Security Incident Response Teams (CSIRT) from the Asia Pacific economies.

ASEAN CERTs Incident Response Drill (ACID), 2016 was conducted with the objectives of Strengthening cyber security preparedness of ASEAN member states and Dialogue partners in handling cyber incidents and reinforce regional coordination drills to test incident response capabilities. The theme of the drill held in September 2016 was handling incidents of Ransomware, in which CERT-In participated.

6. Future Plans

6.1 Future Projects

CERT-In has been 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.
- Promotion of R&D activities in the areas of malware prevention.
- Implementation of a crisis management framework to enable organisations to respond to cyber incidents and assess the preparedness of organisations to withstand cyber attacks

*****

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

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 2002. 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 nation's cybersecurity posture, and protect critical infrastructure cybersecurity. CNCERT leads efforts to prevent, detect, warn and coordinate the cybersecurity threats and incidents, according 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 2016, CNCERT received a total of about 125.7 thousand incident complaints, a 1.0%

decrease from the previous year. And among these incident complaints, 474 were reported by overseas organizations, making a 14.0% drop from the year of 2015. As shown in Figure 2-1, most of the victims were plagued by phishing (42.3%), vulnerability (24.6%) and malicious program (12.0%). Phishing overtook vulnerability to be the most frequent incident complained about.

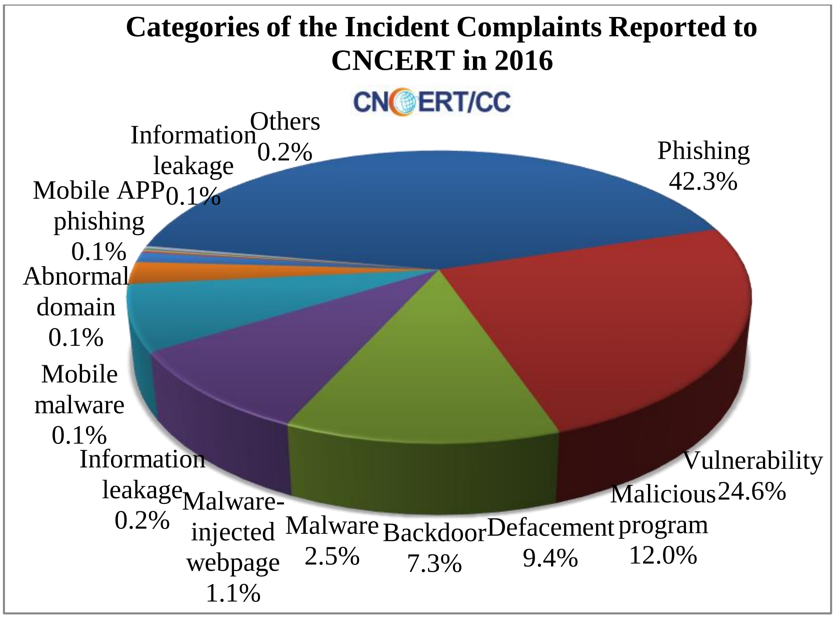


Figure 2-1Categories of the Incident Reported to CNCERT in 2016

In 2016, CNCERT handled almost 125.9 thousand incidents, a slight rise of 0.1% compare with that in 2015. As illustrated in Figure 2-2, phishing (42.3%) dominated the categories of the incidents handled by CNCERT in 2016, followed by vulnerability (24.7%) and malicious program (12.0%).

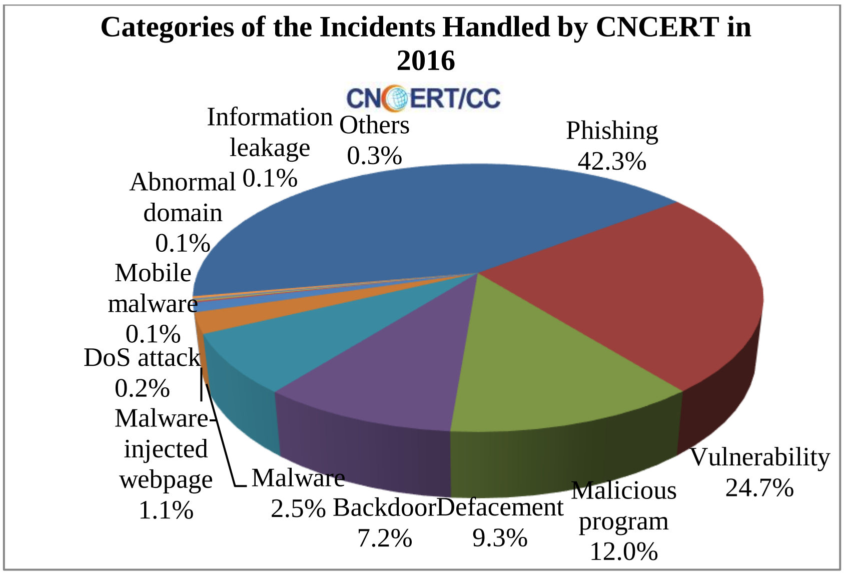


Figure 2-2 Categories of the Incidents Handled by CNCERT in 2016

2.2 Internet Threats

2.2.1 Malware Activities

In mainland China, IPs of the hosts infected with Trojan or Botnet reached about 17.0 million, which decreased by 14.1% compared with that in 2015. We saw more than 48.0 thousand oversea C&C servers which decreased 25.4% from 2015. As shown in Figure 2-3, the US hosted the largest number of oversea C&C servers' IPs of Trojan or Botnet, followed by Hongkong, China and Japan.

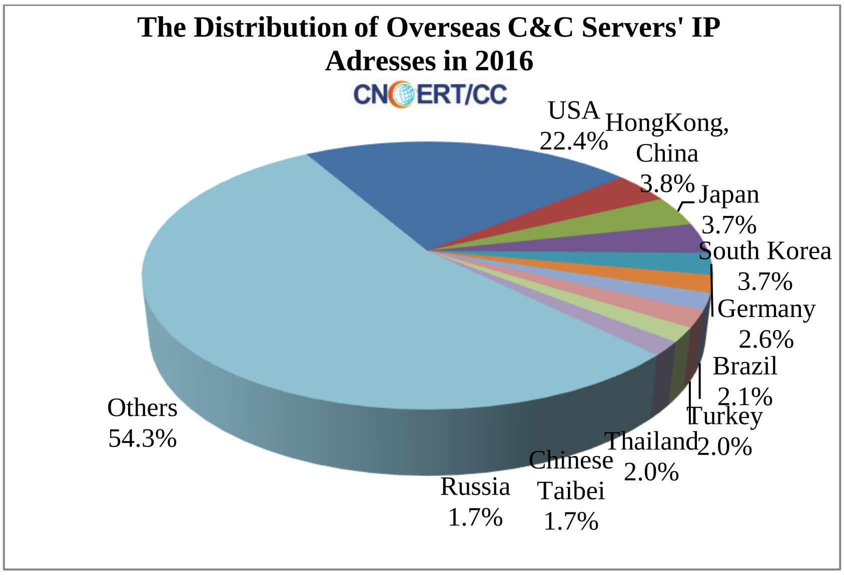


Figure 2-3 Distribution of overseas C&C server's IP addresses in 2016

By CNCERT's Conficker Sinkhole, over 38.5 million hosts were suspected to be infected all over the world. And 5.6 million compromised hosts were located in mainland China. As shown in Figure 2-4, mainland China (14.5%) had the most infection, followed by India (9.3%), and Brazil (5.8%).

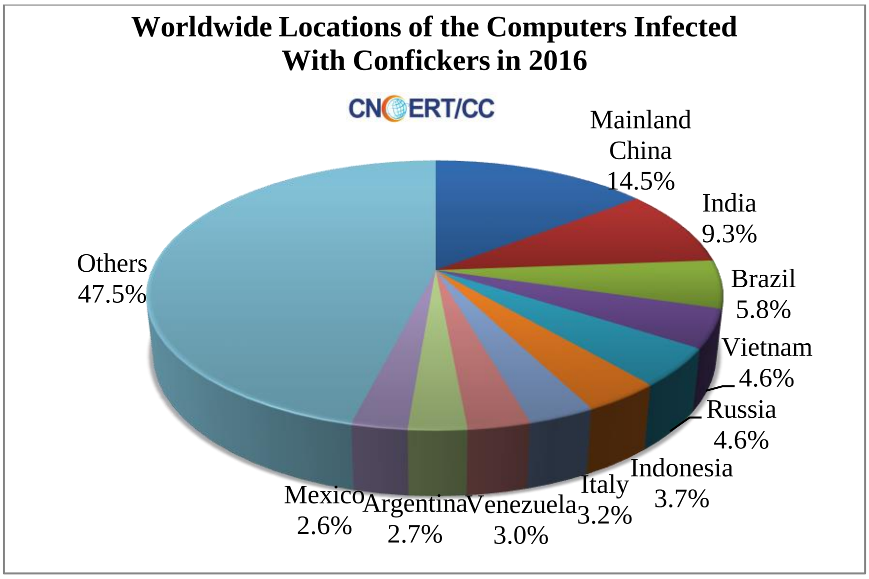


Figure 2-4 Worldwide Locations of the Computers Infected with Confickers in 2016

The malware-hosting websites is the jumping-off place for malware propagation. The malware-hosting websites monitored by CNCERT in 2016 involved about 0.8 thousand domains, about 4.1 thousand IP addresses and about 122 thousand malware download links. Among the 0.8 thousand malicious domains, 68.9% of their TLDs fell into the category of .com. Among the 4.1 thousand malicious IPs, 10.6% were located overseas.

2.3 Website Security

About 16.8 thousand websites in mainland China were defaced, a decrease of 31.7% compare with that in 2015, including 467 government sites. Besides, about 82.1 thousand websites in mainland China were detected to be planted with backdoors and secretly controlled, including 2,361 government sites.

In 2016, CNCERT found about 178.0 thousand phishing sites targeting the websites in mainland China. About 20.1 thousand IPs were used to host those fake pages. About 85.4% were out of mainland China. Most of the phishing servers (25.4%) were located in China HongKong.

CNCERT found almost 33.0 thousand overseas IPs conducted remote control on over

68.3 thousand websites in mainland China. As shown in Figure 2-5, 4618 (14.0%) were located in the US, followed with 2115 (6.4%) in Hongkong, China and 1255 (3.8%) in South Korea.

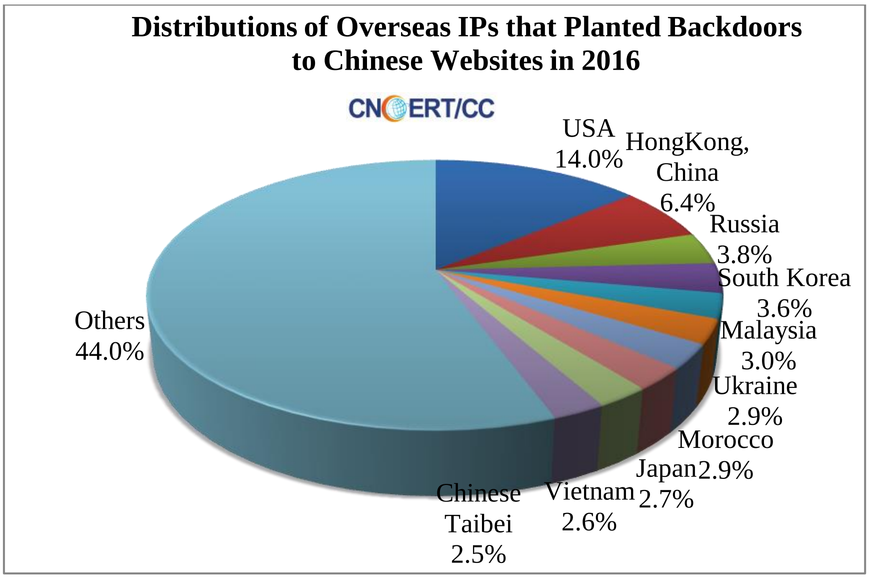


Figure 2-5 Distribution of Overseas IPs that Planted Backdoors to Chinese Websites in 2016

2.4 Mobile threats

In 2016, CNCERT collected about 2.05 million mobile malware samples in total. In terms of intentions of these mobile malware, rogue behavior took the first place (71.8%), fee consumption (25.3%) stood the second place. And followed it were those intended for malicious fee deduction and stealing privacy accounting for 1.4% and 0.8% respectively.

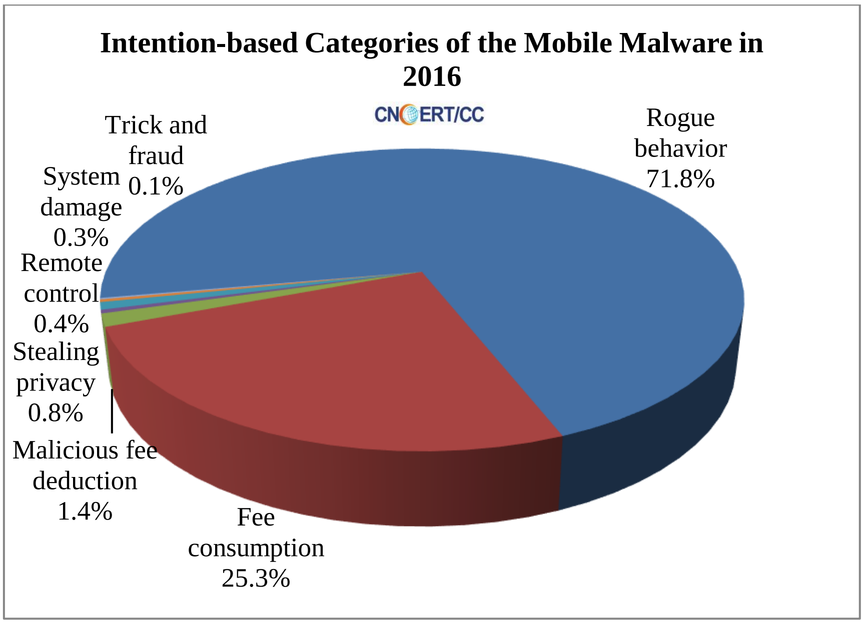


Figure 2-6 Intention-based Categories of the Mobile Malware in 2016

The majority of these mobile malware identified by CNCERT ran on Android platform, recording about 0.95 million (99.9%).

3. Events organized/co-organized

3.1 Conferences

The issue of "A Review of Network Security Situation in 2015"

CNCERT gave a press conference on 2015's Network Security Situation in Beijing on 21st April, 2016, introducing the overall picture and main features of China's network security in 2015. Specialists and representatives from 53 organizations including governmental agencies, operation departments of important information system, telecom operators, domain registrars, Industry Associations, Internet companies and security companies attended this conference. This situation report, which was with distinctive industry characteristics and technical features, outlined the characteristics for China's Internet network security threats in 2015, looked into the threats of much concern in 2016 and made a number of suggestions.

The hold of 2016 CNCERT Annual Conference in Chengdu, Sichuan Province

CNCERT held 2016 Annual Chinese Conference on Computer and Network Security in Chengdu Sichuan from May 25th to 26th, 2016. The theme of the conference is "Gather Cyber Talents, Build Secure Ecosystem". Sub-Forums had been set up according to the 6 subjects: Network Security Threat Intelligence, Network Security Personnel Training, Vulnerability Security and Value Priorities, Mobile Internet Security Ecology, Data Security and CNCERT-CIE Network Security Forum. More than 900 representatives from governments, important information systems departments, industries and enterprises, universities, research institutes and other organizations attended the meeting.

The hold of the fourth China-Japan-Korea Annual Meeting for Cyber Security Incident Response

The operational level delegates of the national CERTs/CSIRTs (Computer Emergency Response Teams / Computer Security Incident Response Teams) of China, Japan and Korea, gathered in Kunming City of China to hold the fourth China-Japan-Korea Annual Meeting for Cyber Security Incident Response from August 31st to September 1st, 2016. Key achievements of this year's meeting were: agreed on basic principles of the next three years' Cooperative Framework and Possible Activities for Cyber Security Enhancement in the MOU; understood and shared current vulnerability coordination activities (including domestic vulnerability handling processes) and related issues in each country; concluded to seek further opportunities to discuss cyber security technical issues of common concern, in an effort to enhance mutual collaboration.

The hold of The China-ASEAN Network Security Emergency Response Capacity Building Seminar in Chengdu

CNCERT organized the China-ASEAN Network Security Emergency Response Capacity Building Seminar in Chengdu, China from May 24 to 26, 2016. Delegates from the telecom department of government and CERTs of Cambodia, Indonesia, Laos, Malaysia, Myanmar, the Philippines, Thailand, Vietnam, and Singapore attended this conference. The participants exchanged development, technology and management experience in the field of network security and discussed how to conduct cooperation on network security emergency responding between China and ASEAN.

4. **Drill attended**

APCERT Incident Drill 2016

CNCERT participated in the APCERT 2016 Drill as a participant on 16 March 2016 and completed it successfully. The theme of the APCERT Drill 2016 was "An Evolving Cyber Threat and Financial Fraud". The scenario, for this year, simulated a contemporary cyber threat with financial motivation that targets to defraud individual and financial institutions. This walkthrough is designed to test the participating teams' incident response handling arrangements. 26 CSIRT teams from 20 economies of APCERT took part in the exercise.

ASEAN CERT Incident Drill (ACID) 2016

CNCERT participated in the ASEAN CERT Incident Drill (ACID) 2016 on September 27th and completed it successfully. The theme for ACID 2016 was "Ransomware and Cyber Forensics". 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 the other released information, were reprinted and quoted by massive authoritative media and thesis home and abroad.

Figure 4-1 lists of CNCERT's publications throughout 2016

Name	Issues	Description
Weekly Report of CNCERT (Chinese)	52	Emailed to over 400 organizations and individuals and published on CNCERT's Chinese-version website (http://www.cert.org.cn/)
Weekly Report of CNCERT (English)	52	Emailed to relevant organizations and individuals and published on CNCERT's English-version website (http://www.cert.org.cn/english_web/documents.htm)
CNCERT Monthly Report (Chinese)	12	Issued to over 400 organizations and individuals on regular basis and published on CNCERT's website (http://www.cert.org.cn/)

Annual Report (Chinese)	1	Published on CNCERT's website (http://www.cert.org.cn/)
CNVD Vulnerability Weekly Report (Chinese)	52	Published on CNCERT's website (http://www.cert.org.cn/)
Articles Analyzing Cybersecurity Threat	36	Published on journals and magazines.

EC-CERT

Taiwan E-Commerce Computer Emergency Response Team - Chinese Taipei

1. Highlights of 2016

EC-CERT dedicates to support and enhance E-commerce Company's ability to respond and deal with security incidents, and work with E-commerce Alliances to promote PII and information security activity. In 2016, EC-CERT developed a basic checklist for E-commerce information security, and has established SOPs for E-commerce.

EC-CERT organizes a seminar letting hackers to exchange views with CEOs of E-commerce companies face to face. In the past, due to lack of IT professionals, 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 is response for information security consulting service and website vulnerability scanning with penetration testing, incident response, post security information alert, etc., EC-CERT offers those services in order to prevent 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 activities.

2.3 Constituency

EC-CERT aims to enhance E-commerce Company's ability to respond and deal with security incidents and other related 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 2016, EC-CERT gathered the 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 33 event visits, handling 25 security incidents, providing 61 security advice to E-commerce companies.

4. Events organized / hosted

4.1 Training

In 2016, EC-CERT holds a series of training, including E-commerce information managements and personal information protection courses, a total of 64 companies, 84 people attended.

4.2 Conferences and seminars

Information security promotion activities * 2

E-commerce PII information security protection Reference Guide Meeting * 2

Participation Asian PKI Union Conference * 2

5. International Collaboration

5.1 Capacity building

5.1.1 Training

EC-CERT Attended Network Security Packet Analysis course and training programs of APCERT.

5.1.2 Drills & exercises

EC-CERT participated in APCERT Drill 2016 to evaluate the capability of incident report and response.

5.2 Other international activities

EC-CERT was invited to attend a Workshop on Electronic Commerce and security issues related to Electronic Commerce at Nov/1-7/2016, Czech Republic.

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 lead to frequent increases in consumer fraud cases, how to help E-commerce industry conduct prevention work, deal with detail during progress and fulfill improvement is the key point of EC-CERT in 2017.

7. Conclusion

As long as technology progresses, there will always be scams but the key to making improvements is awareness and commitment on the part of senior management to take responsibility and action. EC-CERT will continue to support Taiwan's e-commerce information security work.

GovCERT.HK

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

1. Highlights of 2016

1.1 Summary of Major Activities

Since its establishment in April 2015, the Government Computer Emergency Response Team Hong Kong, GovCERT.HK, has effectively fulfilled its responsibilities to centrally coordinate incident responses for over 80 departmental Information Security Incident Response Teams (ISIRTs) of the Government of the Hong Kong Special Administrative Region (HKSAR Government) as well as to bolster cyber security capabilities of the territory through proactive collaboration with the industry, critical Internet infrastructures, and the Computer Emergency Response Team (CERT) community for rapid exchange of threat information and coordinated response.

1.2 Achievements and Milestones

To promote the development of cyber security technologies and industry, we organised the first Hong Kong – Mainland Cyber Security Forum in April 2016 for cyber security professionals to share views on emerging cyber risks and counter measures associated with FinTech, cloud computing, and Internet security.

To address the increasing cyber security threats, we are progressively strengthening our capabilities in collating vulnerability information that would have impact on government installations and information and communications technology (ICT) users, assisting the government ISIRTs in contingency planning and incident response communications for both cyber attacks and data breach events.

Inspired by the Information Sharing Working Group and the TSUBAME Working Group, we were developing a cyber risk information sharing platform for internal use to facilitate speedier dissemination of cyber threat intelligence from GovCERT.HK to over 80 government ISIRTs. We would also pilot the use of big data analytics technology to collect and analyse cyber threat intelligence to formulate targeted cyber threat alerts and actionable advice for our stakeholders so that they can take early precautions and reinforce Hong Kong's cyber security together.

2. About GovCERT.HK

2.1 Introduction

GovCERT.HK is a governmental CERT responsible for coordinating incident response for the HKSAR Government.

Locally, GovCERT.HK works closely with the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) on sharing threat information and organising public awareness activities. GovCERT.HK focuses on government-related matters while HKCERT provides services related to incident response to all ICT users across the territory, covering public and private sectors as well as individuals.

Globally, GovCERT.HK collaborates with the CERT community in sharing incident information and threat intelligence; participating in training events, workshops and forums; 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 different 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 enable government departments to understand the associated risks of information and cyber security, acquire necessary skills and take appropriate actions to protect government information infrastructure and data assets.

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; providing timely security advice; coordinating cyber security drills; promoting public awareness and capabilities; and engaging global CERT community with a view to enhancing information and cyber security in the region.

3.2 Incident Handling Reports

In 2016, GovCERT.HK has received and handled various types of information and cyber security incidents that are related to the installations of the HKSAR Government. The issues varied from vulnerable websites, malware infection, web defacement, distributed denial-of-service (DDoS) attacks, fraudulent emails to unauthorised access and loss of computing devices.

3.3 Alerts and Advisories

In 2016, we have published 85 product security alerts associated with computing products widely used in government installations, and one security advisory recommending system administrators to review security configuration of all versions of Microsoft Windows operating systems as well as to mitigate potential risks associated with the Windows PowerShell automation tools.

We have also issued 20 security reminders to government departments requesting them to take effective and prompt responsive measures against potential attacks and high-risk malware infection, in particular ransomware. We also reminded all users to regularly use anti-malware software to scan their computer systems and perform data backup, and store the backup copy offline.

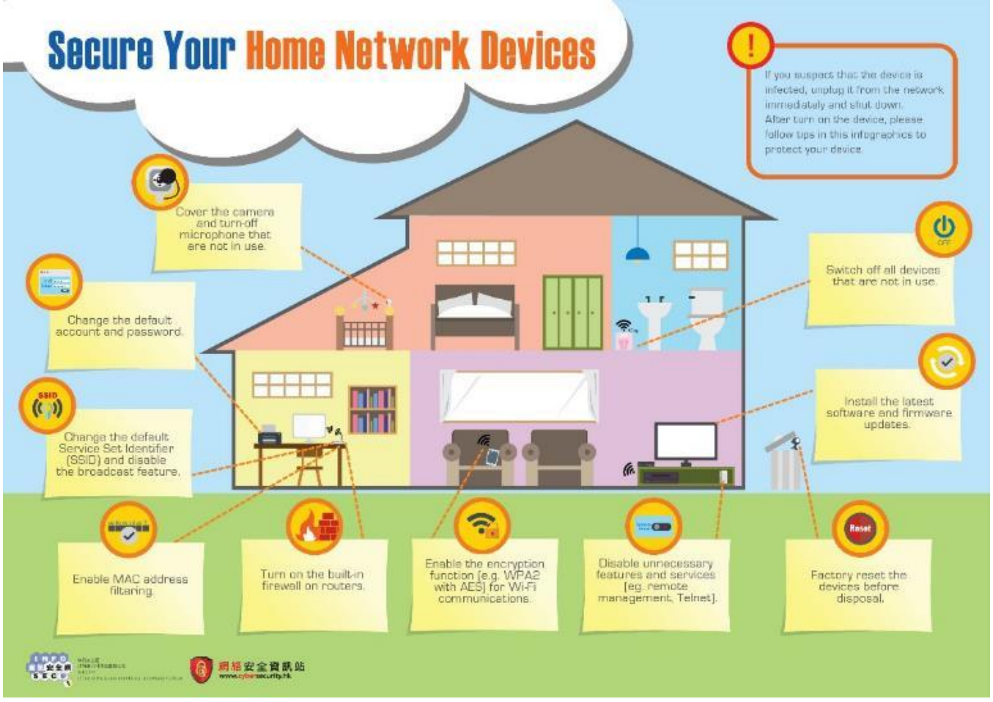
3.4 Publications and Mass Media

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.

- Radio episodes entitled “e-World Smart Tips” were broadcast to help the public understand more about information security in various aspects and raise their awareness of information security. The radio episode in each week featured a different theme and offered associated tips having regard to recent security incidents or foreseeable cyber threats. For instance, the radio tips of “Be a Good

Netizen" were broadcast in September 2016 to disseminate messages of safe and ethical use of the Internet.

- To provide practical tips and advice for Small and Medium Enterprise (SMEs) and the general public to protect from cyber attacks, we have developed and shared infographics covering popular security topics such as "Secure Your Home Network Devices" to remind the public to take necessary precatory actions for protecting their networking and computing devices.



Secure Your Home Network Devices

If you suspect that the device is infected, unplug it from the network immediately and shut down. After turn on the device, please follow tips in this infographics to protect your device.

Cover the camera and turn-off microphone that are not in use.

Change the default account and password.

Change the default Service Set Identifier (SSID) and disable the broadcast feature.

Switch off all devices that are not in use.

Install the latest software and firmware updates.

Enable MAC address filtering.

Turn on the built-in firewall on routers.

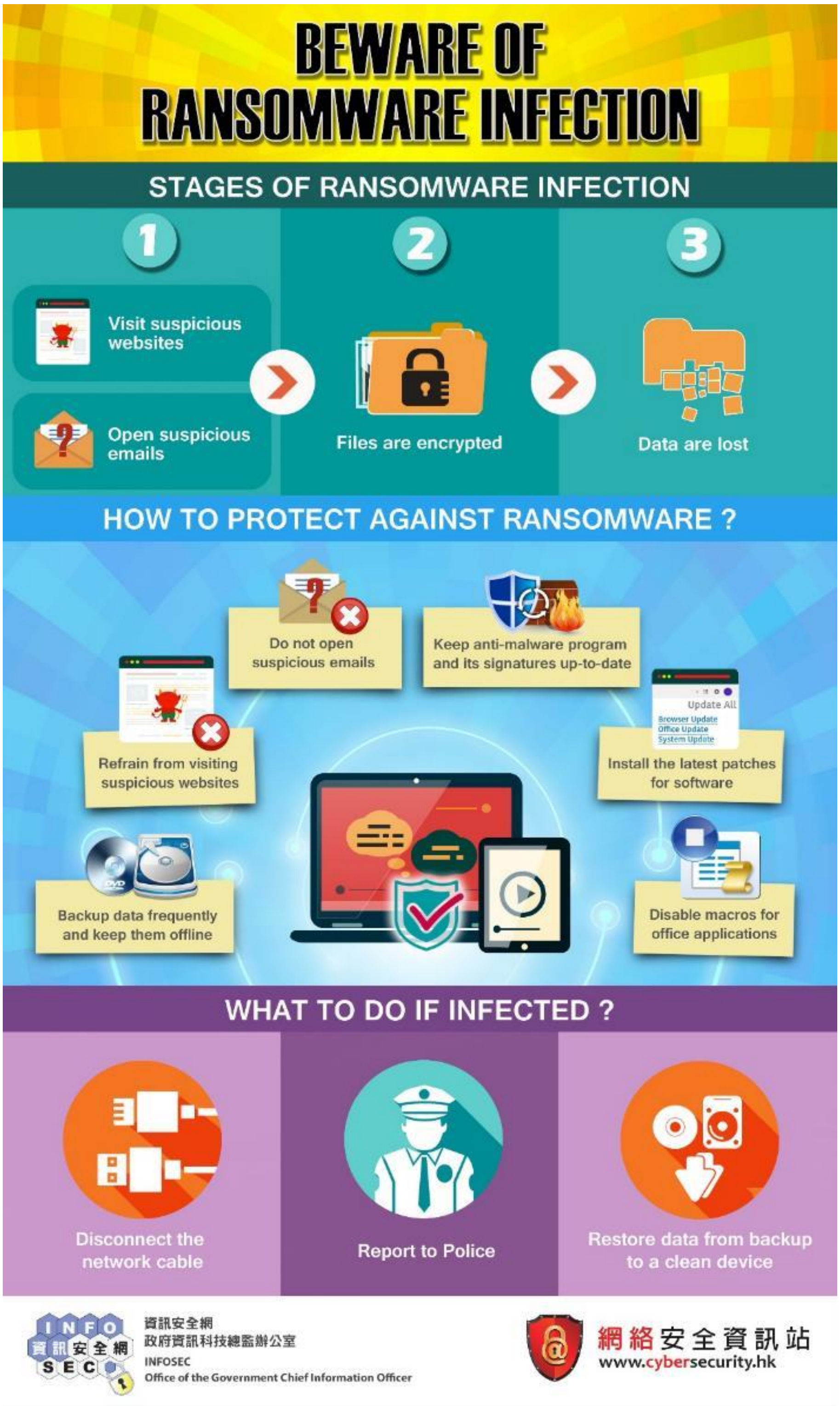
Enable the encryption function [e.g. WPA2 with AES] for Wi-Fi communications.

Disable unnecessary features and services [eg. remote management, Telnet].

Factory reset the devices before disposal.

網絡安全資訊站
www.cybersecurity.hk

- In view of the rising reports of ransomware infection and data loss incidents, we have designed a poster titled "Beware of Ransomware Infection" to advise our stakeholders the importance of data protection and ways to protect themselves against ransomware. The poster was posted in public libraries, government premises and disseminated to schools and SMEs for awareness promotion.



BEWARE OF RANSOMWARE INFECTION

STAGES OF RANSOMWARE INFECTION

1
Visit suspicious websites
Open suspicious emails

2
Files are encrypted

3
Data are lost

HOW TO PROTECT AGAINST RANSOMWARE ?

Do not open suspicious emails

Keep anti-malware program and its signatures up-to-date

Refrain from visiting suspicious websites

Install the latest patches for software

Backup data frequently and keep them offline

Disable macros for office applications

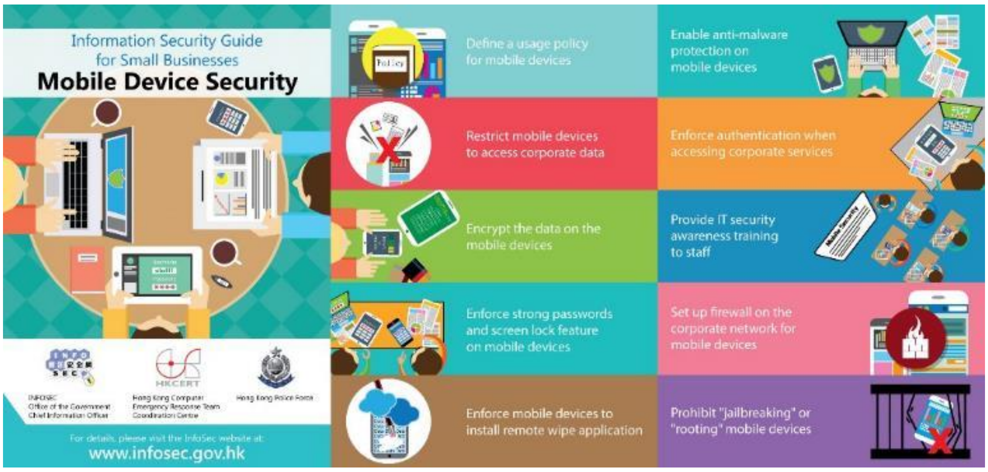
WHAT TO DO IF INFECTED ?

Disconnect the network cable

Report to Police

Restore data from backup to a clean device

- A set of practical guidelines with different themes, including “Mobile Device Security”, “Beware of Phishing” and “Defense Against Malware”, were produced to educate SMEs to deploying appropriate security measures in their business environment.



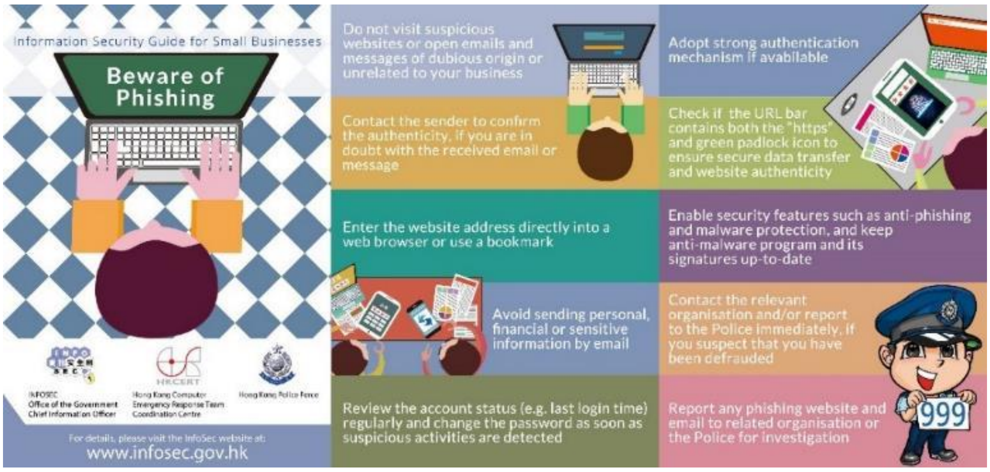
Information Security Guide for Small Businesses

Mobile Device Security

- Define a usage policy for mobile devices
- Enable anti-malware protection on mobile devices
- Restrict mobile devices to access corporate data
- Enforce authentication when accessing corporate services
- Encrypt the data on the mobile devices
- Provide IT security awareness training to staff
- Enforce strong passwords and screen lock feature on mobile devices
- Set up firewall on the corporate network for mobile devices
- Enforce mobile devices to install remote wipe application
- Prohibit "jailbreaking" or "rooting" mobile devices

INFOSEC Office of the Government Chief Information Officer · HKCERT Hong Kong Computer Emergency Response Team Coordination Centre · Hong Kong Police Force

For details, please visit the InfoSec website at: www.infosec.gov.hk



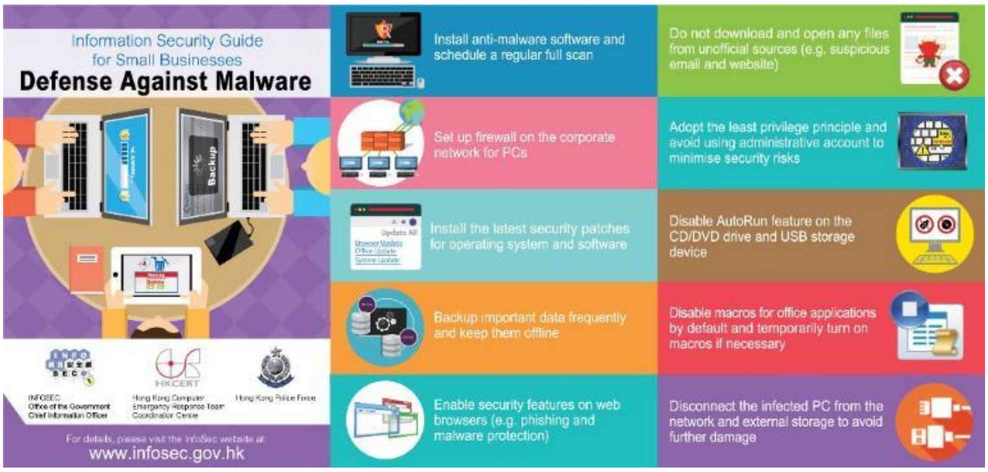
Information Security Guide for Small Businesses

Beware of Phishing

- Do not visit suspicious websites or open emails and messages of dubious origin or unrelated to your business
- Adopt strong authentication mechanism if avabilable
- Contact the sender to confirm the authenticity, if you are in doubt with the received email or message
- Check if the URL bar contains both the "https" and green padlock icon to ensure secure data transfer and website authenticity
- Enter the website address directly into a web browser or use a bookmark
- Enable security features such as anti-phishing and malware protection, and keep anti-malware program and its signatures up-to-date
- Avoid sending personal, financial or sensitive information by email
- Contact the relevant organisation and/or report to the Police immediately, if you suspect that you have been defrauded
- Review the account status (e.g. last login time) regularly and change the password as soon as suspicious activities are detected
- Report any phishing website and email to related organisation or the Police for investigation

INFOSEC Office of the Government Chief Information Officer · HKCERT Hong Kong Computer Emergency Response Team Coordination Centre · Hong Kong Police Force

For details, please visit the InfoSec website at: www.infosec.gov.hk



Information Security Guide for Small Businesses

Defense Against Malware

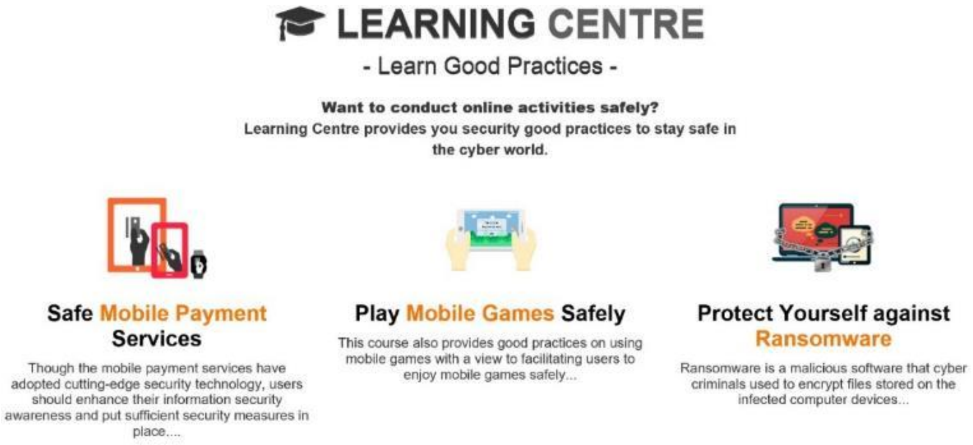
- Install anti-malware software and schedule a regular full scan
- Do not download and open any files from unofficial sources (e.g. suspicious email and website)
- Set up firewall on the corporate network for PCs
- Adopt the least privilege principle and avoid using administrative account to minimise security risks
- Install the latest security patches for operating system and software
- Disable AutoRun feature on the CD/DVD drive and USB storage device
- Backup important data frequently and keep them offline
- Disable macros for office applications by default and temporarily turn on macros if necessary
- Enable security features on web browsers (e.g. phishing and malware protection)
- Disconnect the infected PC from the network and external storage to avoid further damage

INFOSEC Office of the Government Chief Information Officer · HKCERT Hong Kong Computer Emergency Response Team Coordination Centre · Hong Kong Police Force

For details, please visit the InfoSec website at: www.infosec.gov.hk

- Various learning modules were launched on our thematic website in response to high-impact security events. In the light of the surge in ransomware infection cases in 2016, we have developed a learning module on “Protect Yourself against Ransomware”. Other training modules like “Play Mobile Games Safely” and “Safe

Mobile Payment Services" were also produced to provide users with good practices to stay safe in the cyber world.



LEARNING CENTRE

- Learn Good Practices -

Want to conduct online activities safely?
Learning Centre provides you security good practices to stay safe in the cyber world.

Safe Mobile Payment Services
Though the mobile payment services have adopted cutting-edge security technology, users should enhance their information security awareness and put sufficient security measures in place....

Play Mobile Games Safely
This course also provides good practices on using mobile games with a view to facilitating users to enjoy mobile games safely...

Protect Yourself against Ransomware
Ransomware is a malicious software that cyber criminals used to encrypt files stored on the infected computer devices...

- To actively reach out to the general public, social media like YouTube and Twitter, as well as newspapers, were used to share tips and best practices on information security and attract public to participate in our security seminars and events.

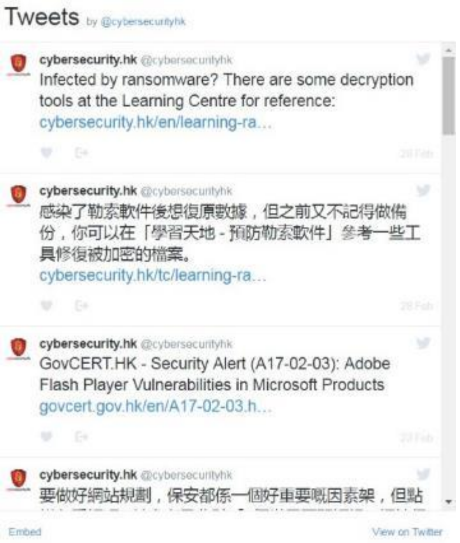
Ransomware

Take Precautions Against Cyber Attacks (Scene 3)
Duration: 0:15
Tips

Ransomware
Duration: 2:34
Tips

Take Precautions Against Cyber Attacks (TV API)
Duration: 0:30
Tips

Pre
Aga
A
(S
Dura



Tweets by @cybersecurityhk

cybersecurity.hk @cybersecurityhk
Infected by ransomware? There are some decryption tools at the Learning Centre for reference: cybersecurity.hk/en/learning-ra...

cybersecurity.hk @cybersecurityhk
感染了勒索軟件後想復原數據，但之前又不記得做備份，你可以在「學習天地 - 預防勒索軟件」參考一些工具修復被加密的檔案。
cybersecurity.hk/tc/learning-ra...

cybersecurity.hk @cybersecurityhk
GovCERT.HK - Security Alert (A17-02-03): Adobe Flash Player Vulnerabilities in Microsoft Products
govcert.gov.hk/en/A17-02-03.h...

cybersecurity.hk @cybersecurityhk
要做好網站規劃，保安都係一個好重要嘅因素架，但點

Embed
View on Twitter

4. Events Organised/Hosted

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

4.1 Training

In 2016, we have organised a total of 14 seminars, workshops and solution showcases for government IT staff and users to enhance their awareness of the 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 the latest IT security technologies and solutions. The topics included industry best practices, mobile and cyber security, data protection, end-point protection and big data analytics.
- 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 the standing incident response procedures with a view to enhancing the overall incident response capabilities.

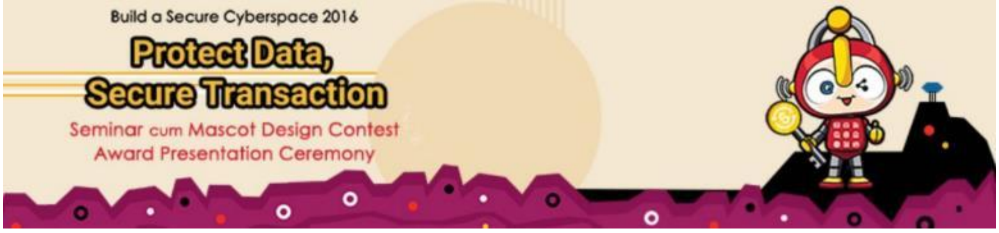
In 2016, we conducted eight drill exercises involving different government departments and their respective service contractors. We also conducted an inter-departmental cyber security drill with the participation of some 30 departments to enhance the overall information security incident response capabilities of the Government.

As the Operational member of APCERT, GovCERT.HK participated in the APCERT Drill with the theme of "An Evolving Cyber Threat and Financial Fraud" in March 2016.

4.3 Conferences and Seminars

In 2016, GovCERT.HK adopted the slogan "Protect Data, Secure Transaction" as the key message to government users and the general public. The target audience included businesses especially SMEs, organisations, schools and the general public.

- Two seminars were organised under the "Build a Secure Cyberspace" campaign in May and November 2016, aiming to promote public awareness of information security and the adoption of security best practices. The one-day seminar in November 2016 invited industry associations and experts to share insights on a range of security topics, including the most common cyber security threats nowadays, associated security advice, security challenges faced by website administrators, points-to-note for secure mobile payment and the safe use of public Wi-Fi.
- The Cyber Security Programme was specifically organised this year. The Programme featured a series of activities for public participation, including the "Protect Your Precious Assets in Cyberspace" seminar. Representatives from the Government, industry associations and solution providers spoke on the best practices of information security with regard to a number of hot topics, including online privacy and security measures for mobile platforms.
- 34 seminars were conducted at primary and secondary schools in 2016, reaching out to nearly 11 000 students and teachers for raising their awareness of cyber security and strengthening their knowledge of protecting personal information.
- A mascot design contest with the theme "Protect Data, Secure Transaction" was organised from April 2016 to July 2016. The contest has received overwhelming response with over 2 000 entries. These entries have clearly conveyed the salient points of protecting computing devices from cyber security traps, and accurately highlighted the importance of data protection and online transaction security.


Build a Secure Cyberspace 2016
Protect Data,
Secure Transaction
Seminar cum Mascot Design Contest
Award Presentation Ceremony

- To commend outstanding IT managers and practitioners for their contributions to the industry, the Cyber Security Professionals Awards (CSPA) was organised in

September 2016. This event was the first of its kind in Hong Kong to encourage cyber security personnel to exchange experience and insights with the objective of enhancing the industry's capabilities of cyber security protection. The awards presentation ceremony was successfully held in January 2017.
[http://www.csprofessionalsawards.net/]

- To promote the development of cyber security technologies and industry in both Hong Kong and the Mainland, the first Hong Kong-Mainland Cyber Security Forum were held in April 2016. The forum attracted some 200 information security professionals from the Government, research institutions, the academia, professional organisations and the information security industry.

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 with 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.

GovCERT.HK also steered the Internet Infrastructure Liaison Group (IILG) to closely monitor the Internet operation status with a view to alerting related parties to abnormal activities. IILG is comprised of members from Internet infrastructures, including the Hong Kong Internet Exchange and the Hong Kong Internet Registration Corporation Limited, major Internet service providers and stakeholders.

5.2 International Collaboration

To foster the Government's 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.

GovCERT.HK has participated in the following events in 2016:

- CNCERT Annual Conference in May 2016
- FIRST Annual Conference 2016 in June 2016
- NatCSIRT Annual Technical Meeting in June 2016
- 2016 China Cybersecurity Week in September 2016
- APCERT Annual General Meeting and Conference 2016 in October 2016
- Five APCERT on-line training sessions from April to December 2016

6. Future Plans

6.1 Upcoming Projects

Apart from public awareness training and promotion initiatives, GovCERT.HK will support the Inter-university Capture the Flag Contest and work with local universities and the industry to organise a cyber security contest to promote awareness of information security and proper cyber etiquette.

To carry forward the success of the inter-departmental cyber security drill 2016, GovCERT.HK will continue to organise the drill on an even larger scale to enable prompt and efficient response to cyber security incidents.

6.2 Future Operation

GovCERT.HK will continue to forge closer ties and enhance information exchange with the CERT community, as well as streamline and enhance its operations appropriately to cope with the increasing security threats and alleged cyber attacks in the region.

In addition to the events and conferences attended in 2016, GovCERT.HK will also join the Microsoft Digital Crime Consortium to network with the global cyber security communities for knowledge and experience sharing, and to enhance the collaboration with the security industry.

7. Conclusion

GovCERT.HK has made substantial strides towards collaboration and operations with local and global CERTs to meet the ever-increasing challenges on cyber security and yielded well-recognised results in safeguarding the Government and the public against cyber security threats. GovCERT.HK will continue to take forward the cyber security initiatives by joining hands with the industry, professional organisations and various stakeholders to maintain a secure, stable and trustworthy cyber world for people from all walks of life.

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 2016, HKCERT had handled 6,058 security incidents which was 23% increase of the previous year (see Figure 1).

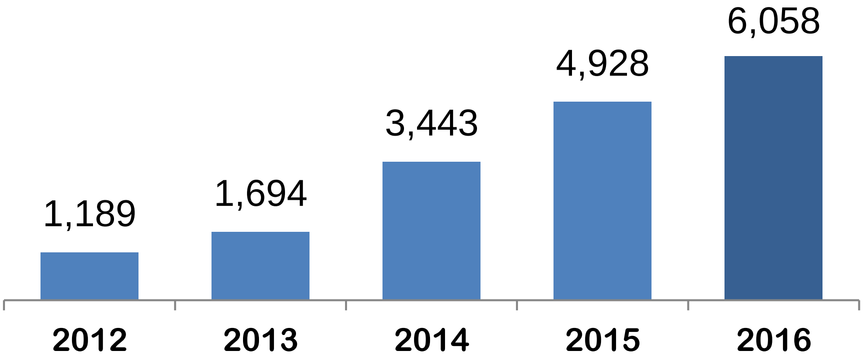


Figure 1. Incident Reports Handled by HKCERT

The huge 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 89% of the total number of security incidents.

Two major categories of security incidents, Botnet (2,018 cases) and Phishing (1,957 cases) remained at similar level as in the previous year (see Figure 2).

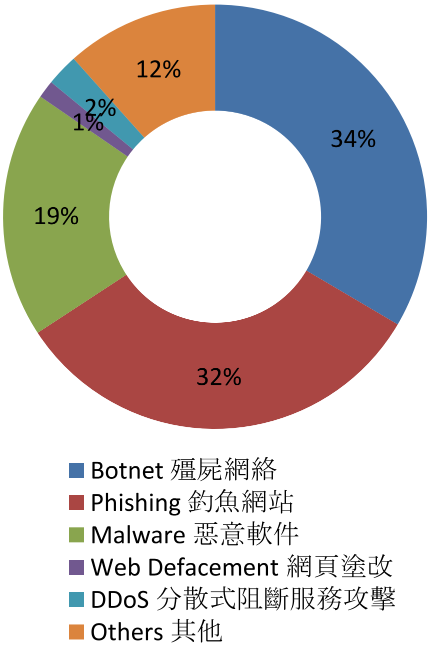


Figure 2. Distribution of Incident Reports in 2016

The number of malware infection incident reports rose sharply by 247% in 2016 (see Figure 3.) These cases were mainly due to XcodeGhost contaminated mobile app and ransomware. Ransomware case had grown rapidly by 506% (see Figure 4) with Locky, CryptXXX and Zepto as the most prominent ones.

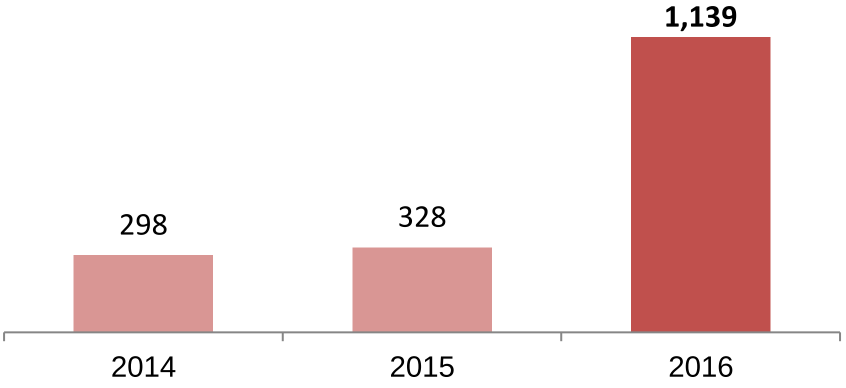


Figure 3. Number of Malware Incident Reports in the past 3 years

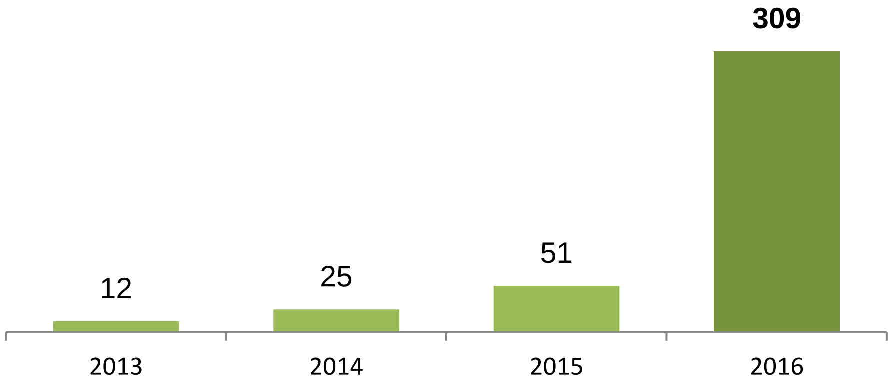


Figure 4. Number of Ransomware Incident Reports in the past 4 years

2.2 Watch and Warning

During the period from January to December of 2016, HKCERT published 336 security bulletins (see Figure 5) on the website. In addition, HKCERT have also published 101 blogs, including security advisories on SSL/TLS Protocols Security, phishing scam, banking Trojan, ransomware, vulnerabilities on Android devices, DDoS by IoT devices and data leakage. HKCERT also published the "best security reads of the week" every week to inform the public of good security articles.

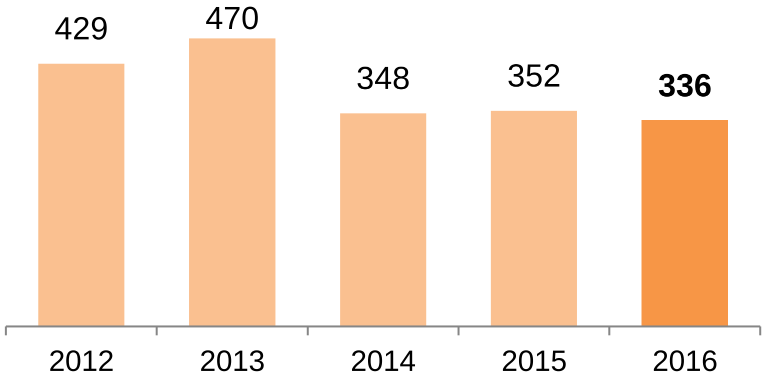


Figure 5. HKCERT Published Security Bulletins

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 slightly decreasing from 5,626 in Q4 2015 to below 5,000 in 2016. Figure 7 showed the trend of top 5 botnet families in the past year. The overall decreasing trend of botnet families, except a new botnet family Mirai in Q4 1016, reflected the effectiveness of the botnet takedown operation.

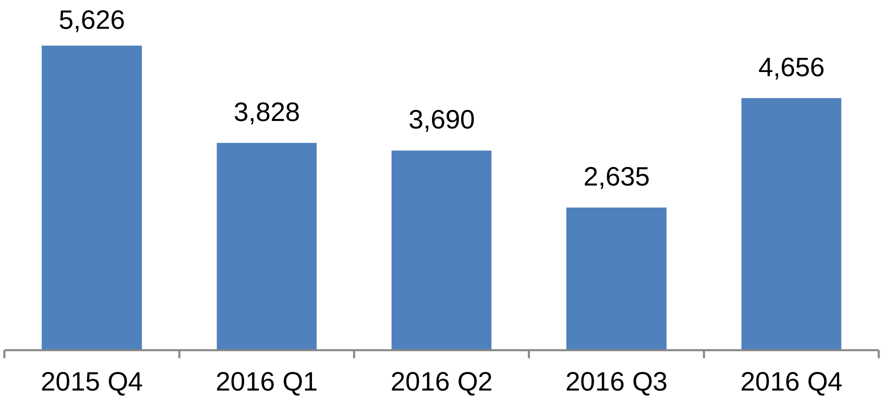


Figure 6. Trend of Bot related security events in the past year

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

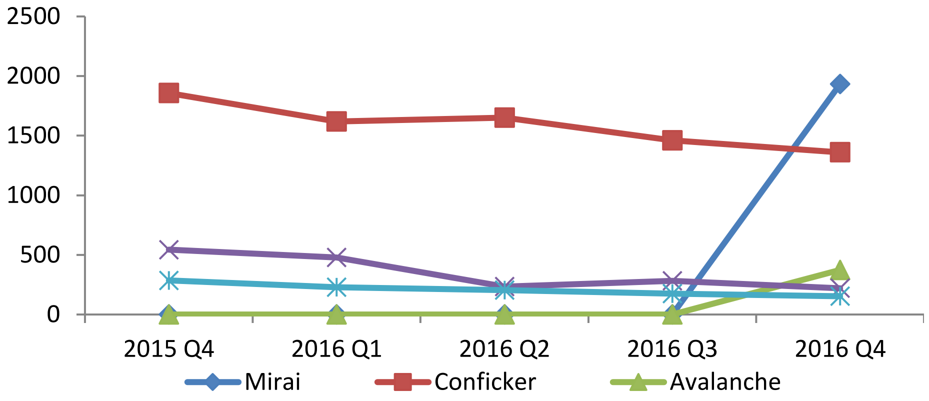


Figure 7. Trend of Top 5 Botnet Families in the past year

(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).

香港地區 Google Play 商店
應用程式保安風險報告
CNCERT/CC
国家互联网应急中心
HKCERT
Hong Kong Google Play Store's Apps Security Risk Report

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

- HKCERT had published the statistics of incident reports 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 mascot design contest. Two public seminars were organized in May and November 2016.

For the graphic design contest, HKCERT had received over 2,000 applications from Open group, Secondary School group and Primary School group. A professional judge panel selected winners with good attractive designs (See Figure 8).

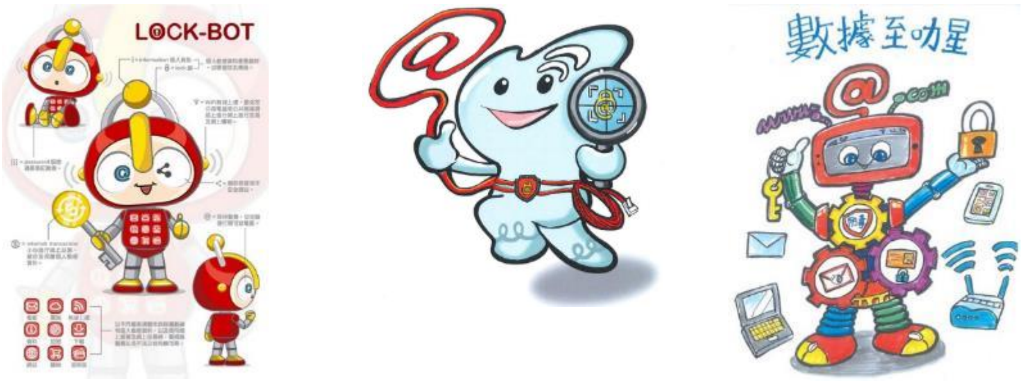
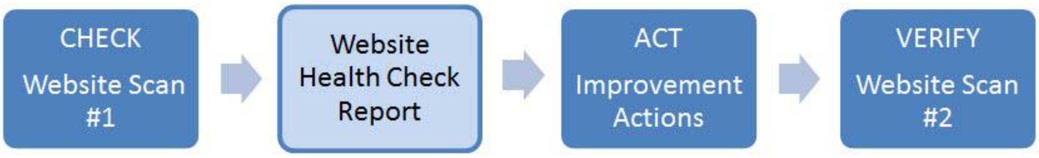


Figure 8. Champion entries of Open, Secondary School and Primary School Group (from left to right)

We organized the 2-day Information Security Summit 2016 with other information security organizations and associations in September 2016, inviting local and international speakers to provide insights and updates to local corporate users.

We organized a SME Free Web Security Health Check Pilot Scheme to promote SMEs to secure their website using the "Check-Act-Verify" approach. Free website scanning and advisory was provided to SMEs joining the scheme. A public seminar was organized to debrief the findings of SME website security status in the scheme.



3.2 Speeches and Presentations

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

3.3 Media promotion, briefings and responses

- HKCERT published an advertorial in November 2016 to promote the public seminar and the mascot design 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 Japan and delivered a talk on DSMS.
- Participated in the FIRST AGM and Conference in Seoul; participated in the Annual Meeting for CSIRTs with National Responsibility in Seoul.
- Participated in the APCERT Drill (March 2016) and acted as member of the Organizing Committee and the Exercise Control team. The theme of the drill this year was "An Evolving Cyber Threat and Financial Fraud". The drill was a great success with 26 APCERT teams from 20 economies, and 6 economies of OIC-CERT participating.
- Participated in the CNCERT Annual Conference 2016 in ChengDu.
- Participated in International honeypot initiatives, including joining the Tsubame project of JPCERT/CC and The Honeynet Project.
- Participated in the Digital Crime Consortium Conference in Vienna, Austria
- Represented APCERT in the Advisory Council of DotAsia Organization

HKCERT signed an MOU with CNCERT to further collaboration in incident response, information exchange and project cooperation.

HKCERT promotes to other CERTs to use the IFAS system (the IFAS.io initiative) developed by HKCERT. The IFAS.io initiative got some pilot users. These pilot users also contributed to IFAS by providing feedback to the system. One CERT pilot user even produced a patch for the installation script.

HKCERT promotes the Decision Support and Monitoring System (DSMS) to other CERTs.

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:

- 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 2016, HKCERT was a coorganizer and a member of the judge panel member in the first Cyber Security Professionals Awards organized by Hong Kong Police Force.
- Continued to work with police, ISPs and domain registries on closing down bulletproof hosting, phishing sites and botnet command and control centres in Hong Kong. HKCERT is still working closely with HKIRC on pre-empting the risks caused by Conficker worm generating pseudo-random domains with ".hk". In 2016, HKCERT had worked with ISPs to clean up Citadel, ZeroAccess, GameoverZeus, Pushdo, Ramnit and XcodeGhost botnet machines in Hong Kong. In 2016 September, HKCERT organized a Cyber Security Symposium "Challenges to Cyber Resilience for Internet Infrastructure Providers".
- Maintained the Information Security Advisory and Collaboration (ISAC) Mailing list with the Internet infrastructure organizations, and advised on latest information security issues through the list
- 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 August of 2016. 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 2017 to review cyber security 2016, and provided outlook to 2017 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 2017/2018. 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 2016, HKCERT was active in global botnet takedown operations and the cyber threat intelligence development. The cross border collaboration and intelligence driven response had improved the proactiveness and effectiveness of incident response. HKCERT also champion the sharing of IFAS with overseas CERTs. HKCERT has seen the immense power of collaboration and would invest more to further this success.

With the Internet security facing more crises from crime-as-a-service, ransomware, phishing, IoT attacks and new security challenges arising from adoption of emerging technologies like cloud computing, mobile payment and Internet of things, HKCERT would expect a more challenging year 2016.

JPCERT/CC

Japan Computer Emergency Response Team / Coordination Center – Japan

1. Highlights of 2016

1.1 Summary of major activities

- Hosting APCERT Annual General Meeting and Conference 2016 (October)

  JPCERT/CC hosted the APCERT Annual General Meeting and Conference 2016 which was held on 24-27 October 2016 in Tokyo, Japan. Besides serving as a member of the Steering Committee and Secretariat of APCERT, JPCERT/CC had the pleasure to actively engage in the event as the host from the planning phase to the actual logistics. The four-day event attracted about 150 people from 30 economies, not only APCERT members but also from partner organisations that APCERT is engaged with.

1.2 Achievements & milestones

- Celebration of JPCERT/CC 20th Anniversary

  In October 2016, JPCERT/CC celebrated its 20th anniversary since its establishment. JPCERT/CC officially started its operation in October 1996, and today it is one of the oldest CSIRTs in the world. In retrospect of the history of the organisation, a symposium was held on 28 October, inviting various partner organisations especially in the local communities.
- AfricaCERT Meritorious Service Award for JPCERT/CC

  In June 2016, AfricaCERT Meritorious Service Award was given to JPCERT/CC, Dr. Suguru Yamaguchi (posthumously) and Koichiro Komiyama. The award was given in acknowledgement for pioneering and contributing through activities to support the African CSIRT community and its human resource development in Africa since 2010.

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 hasbeen 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 focus on technical staff of enterprises in particular. 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 2016, JPCERT/CC received 16,446 computer security incident reports from Japan and overseas.

	1st Qtr	2nd Qtr	3rd Qtr	4th Qtr	Total
Incident Reports	4,587	4,686	3,137	4,036	**16,446**

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

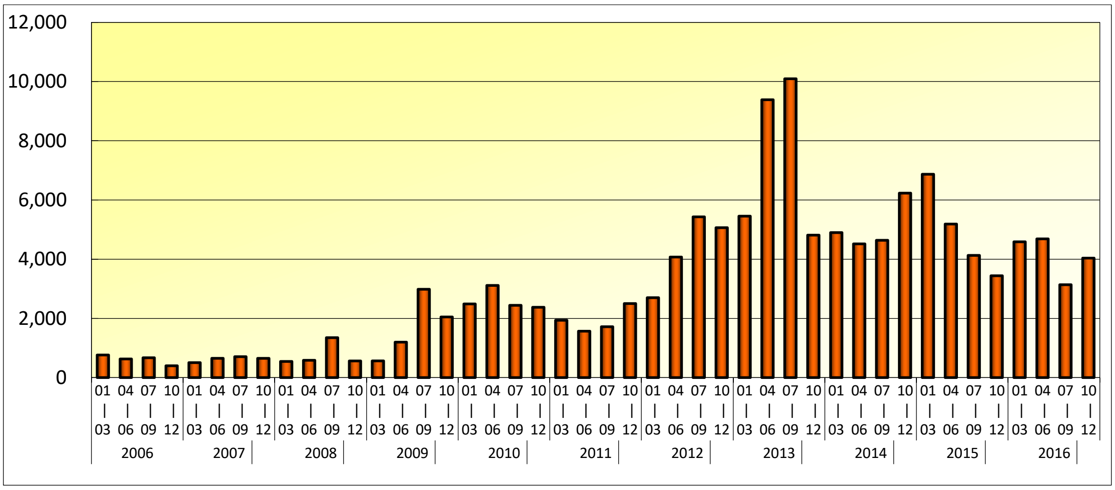


Figure 2. Incident reports to JPCERT/CC (2006-2016)

3.2 Abuse statistics

Incident reports to JPCERT/CC in 2016 were categorised as in Figure 3. About 43% of the reports were on scan, followed by website defacement and phishing.

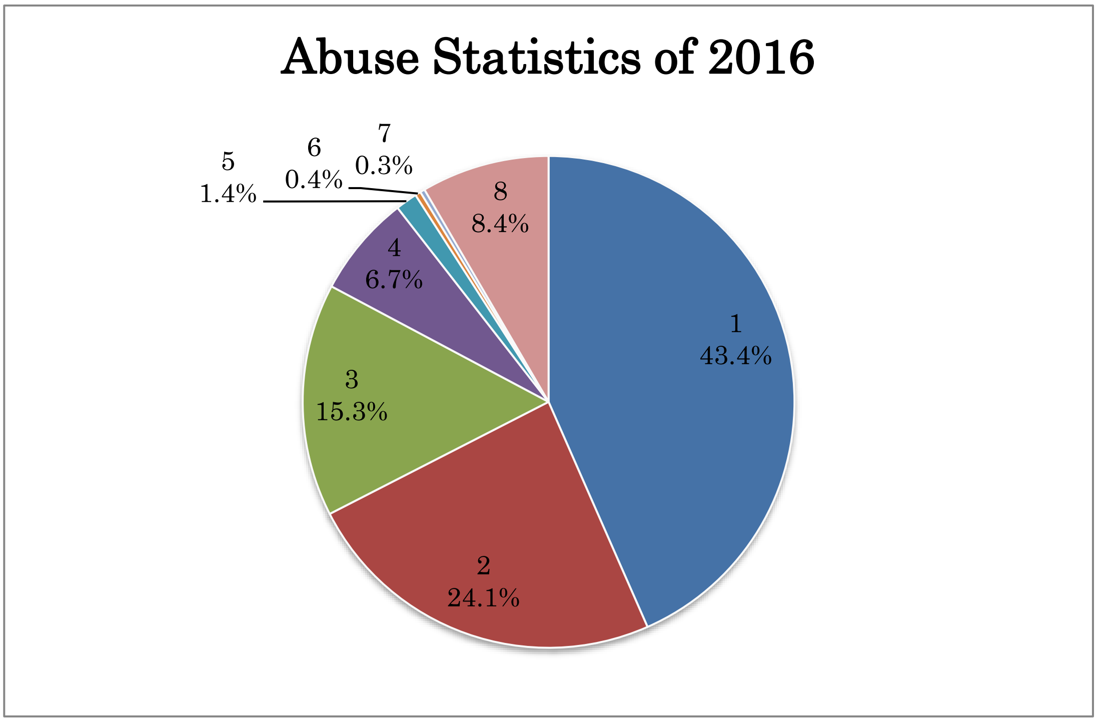


Figure 3. Abuse Statistics of 2016

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 2016, 51 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". 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 used in Japan. JVN is jointly operated by JPCERT/CC and the Information-technology Promotion Agency (IPA) and provides the descriptions, solutions, and developers' statements on each vulnerability (including information on affected products, workarounds and solutions, such as updates/patches).

  For global software products, JPCERT/CC conducts vulnerability handling operations cooperatively 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 susceptible products. Once solutions become publicly available, JPCERT/CC publishes advisories for the reported issues on JVN.

  In 2016, 342 vulnerabilities coordinated by JPCERT/CC were published on JVN. 190 were cases published with IPA through the Information Security Early Warning Partnership, and 152 were published through partnerships with overseas coordination centers or developers.

  Of the 190 published through the Information Security Early Warning Partnership, 138 were reported to IPA by researchers, security vendors, etc. 52 were reported by developers on software developed by themselves. Of the 152 published through global partnerships, 105 were reported and published by CERT/CC, 1 by ICS-CERT, 24 were reported by developers on software they developed, and 2 were reported by an overseas researcher. In addition, there were 18 issues published as 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 2016, a member of JPCERT/CC was nominated 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 2016, 18 articles were published.

- **Quarterly Activity Reports**

  https://www.jpcert.or.jp/english/doc/reports.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 the industrial control system (ICS) security in Japan, and since January 2013, JPCERT/CC's incident handling service was extended to 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. In 2016, the tool was 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 researches and artifact analyses, including not only viruses and bots but also tools that can potentially be used with malicious intent. Findings through the analyses are crucial in the course of 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 analyse Internet traffic data, in order to better understand the Internet threats mainly in the Asia Pacific region. It deploys sensors widely in the region, collecting and sharing the data with all participating teams. The TSUBAME project aims to establish a common platform to promote collaboration among CSIRTs mainly in the Asia Pacific region. TSUBAME Working Group is active in APCERT and observation results are exchanged among the teams.

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 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 staffs, system administrators, network managers, etc. As one of the key events in 2016, 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 2016, JPCERT/CC newly signed an MoU with SI-CERT (Slovenia) and CERT-MU (Mauritius) respectively.

- **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 2016.

- TSUBAME Training for LaoCERT (February, Vientiane)

- CSIRT training for Indonesia, Cambodia, Laos, Myanmar, Vietnam and Timor-Leste, as part of JICA's (Japan International Corporation Agency) Project for Strengthening Capacity Building in Information Security (March/October, Bali/Jakarta)
- Malware Analysis training and CyberGreen Workshop for AfricaCERT, Africa Internet Summit (June, Gaborone)
- CSIRT training for ASEAN CIIP officials as part of HIDA's (Overseas Human Resources and Industry Development Association) Training Program (August, Ho Chi Minh)
- Malware Analysis training at FIRST Regional Symposium for Arab and African Regions (October, Sharm el-Sheikh)
- Network Forensics and Malware Analysis training for AfricaCERT, AFRINIC (November, Mauritius)

5.2.2 Drills & Exercises

JPCERT/CC participated in the following drills in 2016 to test our incident response capability:

- APCERT Drill 2016 (16 March)
- ASEAN CERTs Incident Drill (ACID) 2016 (27 September)

5.2.3 Seminars & presentations

In 2016, JPCERT/CC dispatched speakers to the following international cyber security events:

- Prague 2016 FIRST Technical Colloquium with TF-CSIRT (January, Prague)
- Raleigh 2016 FIRST Technical Colloquium (February, Raleigh)
- APRICOT 2016 / Auckland 2016 FIRST Technical Colloquium (February, Auckland)
- Munich 2016 FIRST Technical Colloquium for Threat Intelligence (February, Munich)
- Asia Regional Forum CBM Workshop (March, Kuala Lumpur)
- CNCERT/CC Annual Conference (May, Chengdu)
- Annual Meeting of the Global Forum on Cyber Expertise (June, Washington DC)
- 28th Annual FIRST Conference (June, Seoul)
- National CSIRT Meeting (June, Seoul)
- IRCON 2016 (July, Taipei)

- CODEBALI 2016 (September, Bali)
- MNSEC-2016 (September, Ulaanbaatar)
- APEC TEL 54 (November, Kyoto)
- Sri Lanka Cyber Security Week (November, Colombo)
- Borderless Cyber Asia 2016 (November, Tokyo)
- Hong Kong International Computer Conference 2016 (November, Hong Kong)
- Internet Governance Forum 2016 (December, Jalisco)
- OIC-CERT Annual Conference (December, Jeddah)

...and many more

5.3 Other international activities

Below are some of the international events that JPCERT/CC joined in 2016:

- S4x16 ICS Security Conference (January, Miami)
- RSA Conference US 2016 (February, San Francisco)
- APRICOT 2016 (February, Auckland)
- CanSecWest 2016 (March, Vancouver)
- ISO/IEC JTC 1/SC 27 Information Standard Meeting (April, Tampa)
- 28th TRANSITS I Training Workshop (April, Egmont aan Zee)
- APWG eCrime 2016 (June, Toronto)
- OWASP AppSec EU 2016 (June, Rome)
- Black Hat USA 2016 (August, Las Vegas)
- DEFCON 24 Hacking Conference (August, Las Vegas)
- 25th USENIX Security Symposium (August, Austin)
- The 4th China-Japan-Korea CSIRT Annual Meeting for Cybersecurity Incident Response (August, Kunming)
- Virus Bulletin Conference 2016 (October, Denver)
- 2016 APISC Security Training Course (October, Seoul)
- ISO/IEC JTC 1/SC 27 Information Standard Meeting (October, Abu Dhabi)
- APCERT AGM and Conference 2016 (October, Tokyo)
- ICS Cyber Security Conference (October, Atlanta)
- Black Hat Europe 2016 (November, London)
- BlueHat v16 (November, Seattle)
- CNA Summit (November, Rockville)
- Botconf 2016 (November, Lyon)

- HITCON 2016 (December, Taipei)

  …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

- Use of STIX/TAXII

  JPCERT/CC is positively considering the use of STIX/TAXII in terms of information exchange, especially with overseas CSIRTs. JPCERT/CC has been making efforts to prepare its internal environment for smooth and effective use of STIX/TAXII.

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 2016

1.1 Summary of Major Activities

Although there were no significant incidents in 2016, all cybersecurity entities in South Korea have been maintaining the tension at work since the nuclear bomb test of North Korea in early 2016. KrCERT/CC has reinforced its monitoring activities to be ready for unexpected surge of cyber threats in the private sector. In addition to that, we respond to pharming, ransomware, vulnerabilities, hacking and other incidents which persistently emerge.

> * Pharming: A cyber attack intended to redirect a website's traffic to another, fake site. Pharming can be conducted either by changing the hosts file on a victim's computer or by exploitation of a vulnerability in DNS server software. (Source: Wikipedia)

1.2 Achievements & Milestones

A website is one of the most common path of malware dissemination. Since 2006, KrCERT/CC has been operating a service that detects hidden malicious codes on a website. We expanded coverage of the service in 2016 to crawl 3.4 million domestic websites.

KrCERT/CC has been operating two kinds of alliance with domestic and international security vendors under the name of "Cyber Threat Intelligence" and "Global Cyber Threat Intelligence" since 2014 and 2016 respectively. We have a monthly meeting with the two alliances at the working-level and published the "2017 Cyber Security & Threat Predictions."

Furthermore, KrCERT/CC conducts the APISC Security Training Course in a bid to solidify trust through mutual exchanges among other CERTs. 24 teams participated in the program to share their procedures and technical know-how as well as had a chance to enhance a human network. Also, KrCERT/CC successfully hosted the 28th FIRST Annual Conference in Seoul last June.

2. About CSIRT

2.1 Introduction

The Korea Computer Emergency Response Team/Coordination Center (KrCERT/CC) is Korea's national CSIRT in 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 (a former KISA). Since its foundation, it has responded to and handled numerous security issues and tasks. The first major incident was the Internet Crisis caused by so-called 'slammer worm' in 2003. At that time, KrCERT/CC had difficulties in communication efficiently with the 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 (a 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

Currently, around 150 employees from 3 divisions and 1 center work for KrCERT/CC.

2.4 Constituency

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

3. Activities & Operations

3.1 Scope and Definition

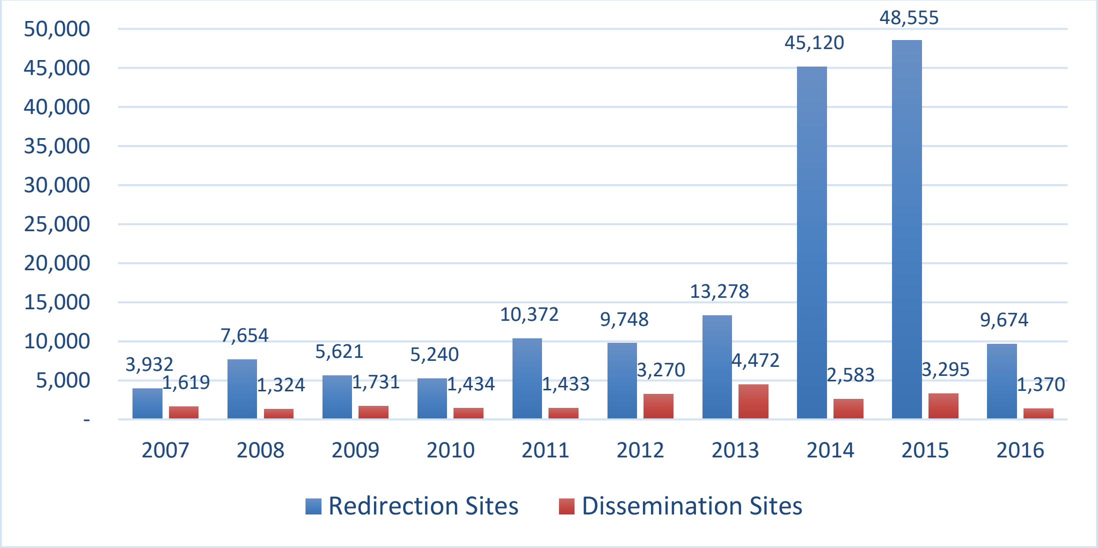
Key roles of KrCERT/CC include response to Internet security incidents related to users and operators as well as raising awareness and international cooperation.

3.2 Abuse Statistics

3.2.1 Malware via Compromised Websites

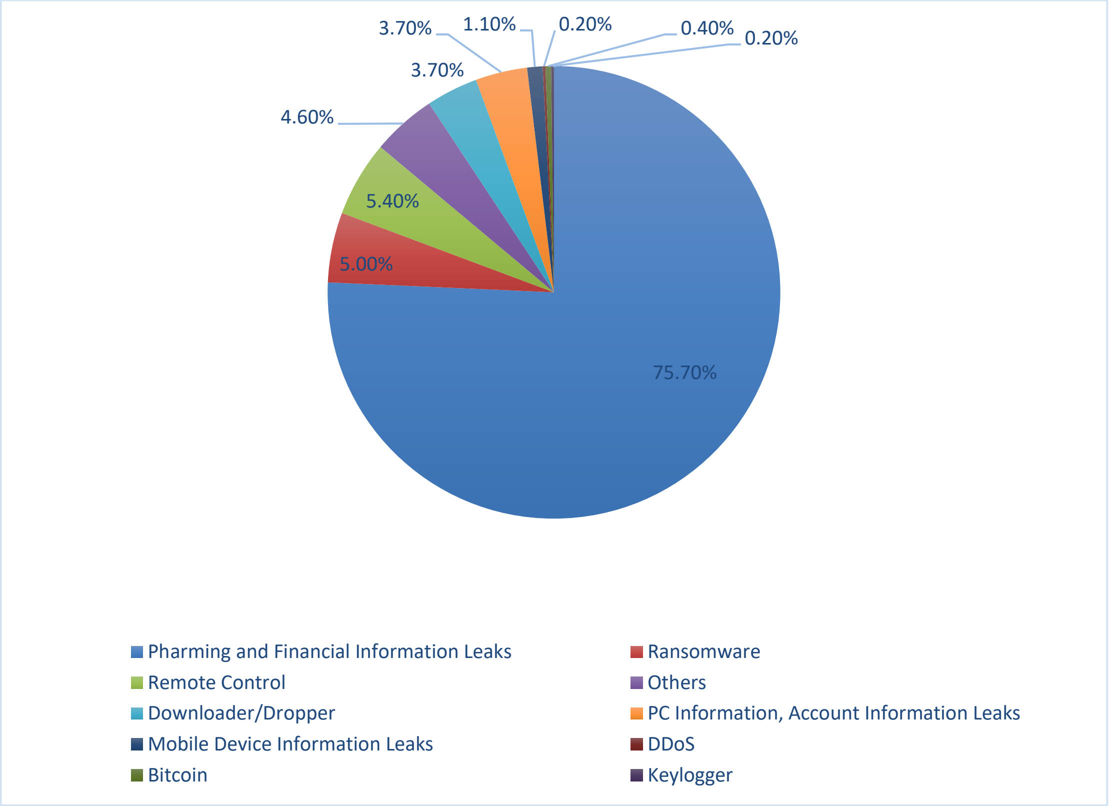
Distribution of hidden malware on websites is on the rise, but a number of sites that directly pass malware decreased by 58.4% over the previous year (3,295 cases → 1,370 cases) and a number of redirection sites that link to the dissemination sites also showed dramatic decrease by 77.8% (43,555 cases → 9,674 cases) compared to the last year.

Detected Malware Redirection Sites and Dissemination Sites



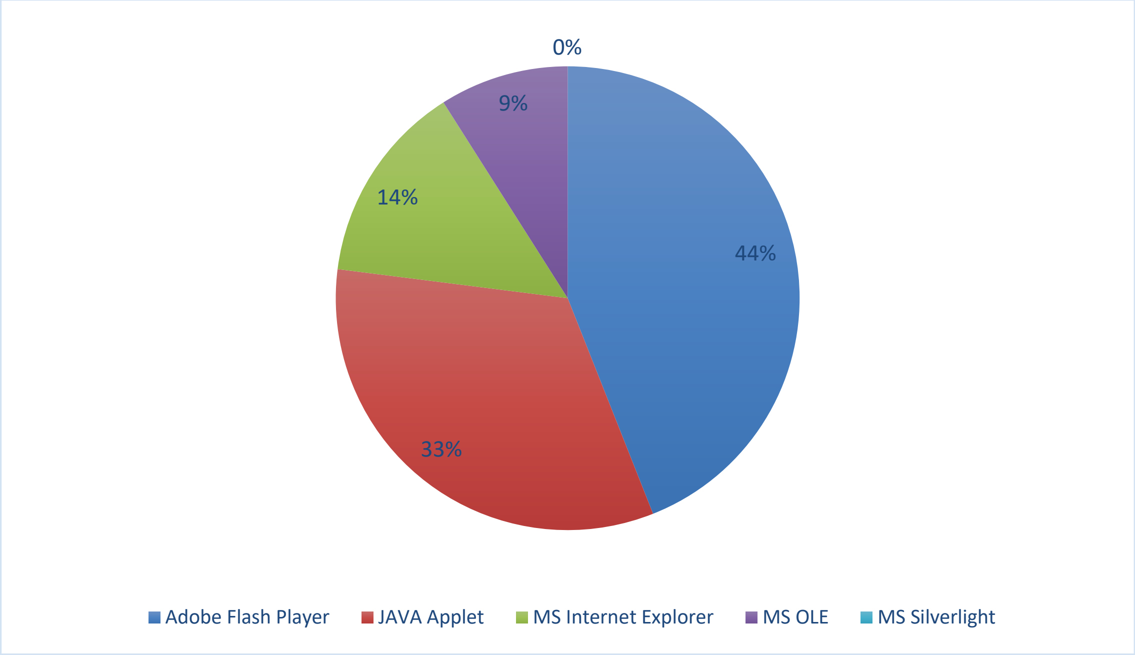
Pharming and information leakage accounted for the largest proportion of malware distributed from websites followed by ransomware and remote control.

Malwares Types in 2016



These types of malware typically exploit vulnerabilities of software installed on the users' PCs. The most commonly used type of software was Adobe Flash Player, followed by Java applet and MS Internet Explorer.

Software Vulnerabilities in 2016



3.2.2 Phishing/Pharming Sites

Sharp increase in pharming sites which started from the end of 2012 seemed somewhat decreased in 2015, but confirmed to be on the rise again in 2016.

Pharming is a financial fraud that causes actual financial loss by infecting a PC with malicious codes. A victim of the infected PC is tricked to access to a fake financial website that misrepresents a normal website which will cause account information leakage like security codes. Phishing sites have also been rising along with the pharming sites. Phishing is a security incident that causes leakage of personal information or account information by clicking a malicious link through e-mails.

KrCERT/CC received about 5,054 reports on phishing and pharming sites from the Financial Supervisory Service and the Financial Security Institute in 2016. The figure increased by two folds and six folds, compared to those of the year 2015 and 2014 respectively. Social issues of Korea are believed to be misused for rampant phishing and pharming incidents.

<Number of Reports on Phishing/Pharming Sites>

Year	2014	2015	2016	Total
Phishing site	875	469	749	2,093
Pharming site	6	1,640	4,305	5,951

3.2.3 Publications

KrCERT/CC publishes a monthly malware detection report in Korean and posts a security announcement on its home page whenever a major vulnerability is found. Also, a quarterly cyber threat trend report is uploaded on the website.

4. Events

4.1 Training

KrCERT/CC has been organizing an annual invitation-based security training course on CSIRT establishment and operation for countries mainly in the Asia-Pacific region since 2005. The course opens a door for the participants from different countries to build a human network at the working-level which is one of the most important elements in cybersecurity incident response. 24 participants from 23 countries including Cambodia, Thailand and India participated in the 2016 training course and shared their knowhow on cybersecurity structure and CERT establishment.

4.2 Drills & Exercises

KrCERT/CC hosted a 2-day domestic cyber threat drill in December 2016 with the Ministry of Science, ICT and Future Planning (MSIP) to check readiness of rapid cyber threat response and an organic cooperative system. 38 companies including ISPs, security vendors, portal service providers, webhard service providers, online shops and defense industry companies participated in the drill. KrCERT/CC also organized an onsite investigation exercise with the Police Office during the drill. We were able to check entire response process from threat detection to incident investigation through these drills as a preparation for cyber attacks like APT and DDoS. Aside from this, 3 more cyber drills were conducted with relevant agencies.

4.3 Conferences and Seminars

KrCERT/CC successfully played a role of the local host for the 28th FIRST Annual Conference in Seoul in June under the theme of "Getting to the Soul of Incident

Response." According to the official counting, 645 experts from 63 countries attended the conference. KrCERT/CC had a valuable experience and a chance to meet various organizations from relevant agencies to experts through the conference.

4.4 Competition

KrCERT/CC hosted the 13th Hacking Defence Contest (HDCON) with the MSIP in October 2016. HDCON is the time-honored domestic contest that started in 2004. About 918 participants from 396 teams signed up for the preliminary round and only 10 teams out of them made it to the finals. As can be seen from the keyword, Actionable, the 2016 HDCON was a platform to test competency of the participants in incident analysis and forensics at the restructured incident sites. Problems were especially related to file recovery, network packet analysis, reverse engineering, web hacking and mobile. One thing to note about is that the teams had to solve the problems in a way that as if they are security managers of an imaginary victim company in its marketing room to address security incidents. KrCERT/CC expects a competition like this would contribute to create the right environment for the participants to not only research on future attack methods but also defense methods.

5. International Collaboration

5.1 International Partnerships and Agreements

KrCERT/CC formed official relationships with relevant agencies including CSIRTs from in and outside of the region and hosts a meeting for information sharing.

5.2 Capacity Building

5.2.1 Drills & Exercises

KrCERT/CC participated in the joint drill organized by APCERT in March 2016 to crack the given task within the 4 hours of time limit and check harmonious incident response among coordination, analysis and response teams of the organization.

5.2.2 Seminars & Presentations

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

FIRST TC at APRICOT 2016, February 2016, Auckland, New Zealand
CNCERT/CC International Cooperation Forum, May 2016, Chengdu, China
CERT-RO Annual Conference, October 2016, Bucharest, Romania

6. Future Plans

6.1 Future Operation

Ransomware and pharming with evolving techniques are likely to keep happening as threats to daily lives of Koreans. KrCERT/CC will quickly detect and respond to such incidents with automated methods through continuous research on attack techniques and enhanced systems. Above all, the utmost important factor is close cooperation and information sharing with partners. Thus, KrCERT/CC will strive to strengthen our capacity to detect as many cyber threats as possible in advance through a stronger information sharing system for safer cyber space.

7. Conclusion

Although there were no major incidents broke out in 2016, possible cyber attacks from in and outside of Korea still exist due to unique geological circumstance that we are put into. The best way to respond to security incidents is prevention. KrCERT/CC will always bear this in mind to raise awareness and strengthen cooperation with other agencies for rapid and effective incident response in the future.

LaoCERT

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

1. Highlight of 2016

1.1 Summary of Activities

- Co-Organized with ICT for Peace Foundation to host The Workshop on International Cyber Security Policy and Diplomacy for CLMV Countries on 31st October – 01st November 2016 in Vientiane, Lao PDR.
- Co-organized with Portcullis Technology, Singapore to organize the Seminar on New Paradigm in Cyber Protection on 15th December 2016 in Vientiane, Laos PDR. By invited experts from Vietnam, Cambodia, Malaysia and Singapore to share experience with representative of Ministries, Banks, ISPs and related organization from Laos on cyber security.
- Organized the seminar on cyber security cooperation to Ministries, Banks, ISPs and related organizations in Laos.

1.2 Achievements & milestones

- Announcement to become National CERT of Lao PDR in 2016.

2. About LaoCERT

2.1 Introduction

Lao Computer Emergency response team (LaoCERT) is the national CERT of Lao PDR, it was established in 2012 as a LaoCERT division under the Lao National Internet Center, Ministry of Post and Telecommunications and it worked very hard to develop on capacity building for its staffs in the field of cyber security with other CERTs organizations in the region.

As working for 4 year passed, it has been announcement to become the national CERT equivalent department in 2016 under to the Ministry of Post and Telecommunications directly and it 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 2016.

2.2 Establishment

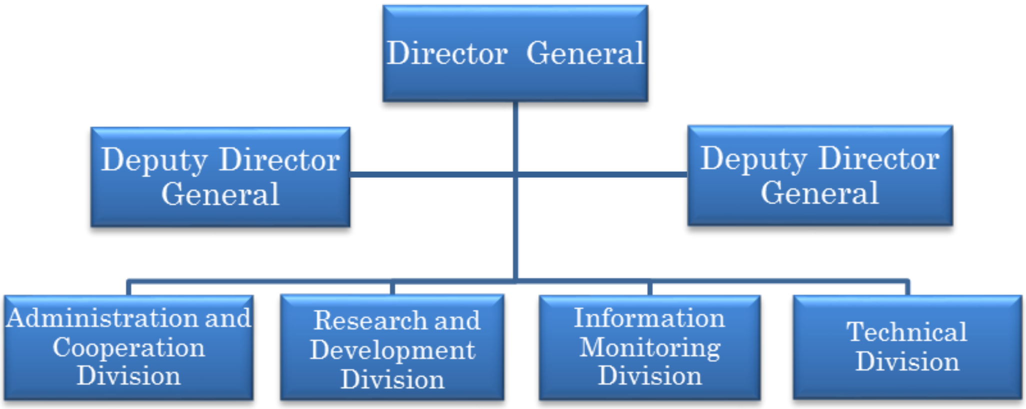
LaoCERT was established in February 2012 by degree 220/MPT and under the Ministry of Post and Telecommunications (MPT), Government of Lao PDR. It was established by following up as ITU-IMPACT recommendations.

2.3 Resource

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

- Cellebrite Certified Physical Analyst
- Computer Hacking Forensic Investigator

LaoCERT Organization Charts


Director General
Deputy Director General
Deputy Director General
Administration and Cooperation Division
Research and Development Division
Information Monitoring Division
Technical Division

2.4 Constituency

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

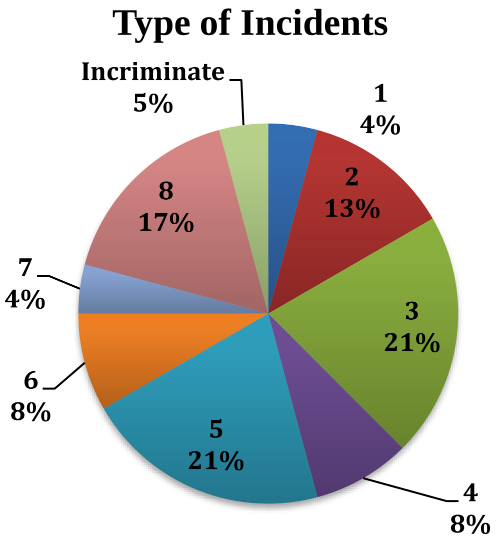
3. Activities & Operations

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.

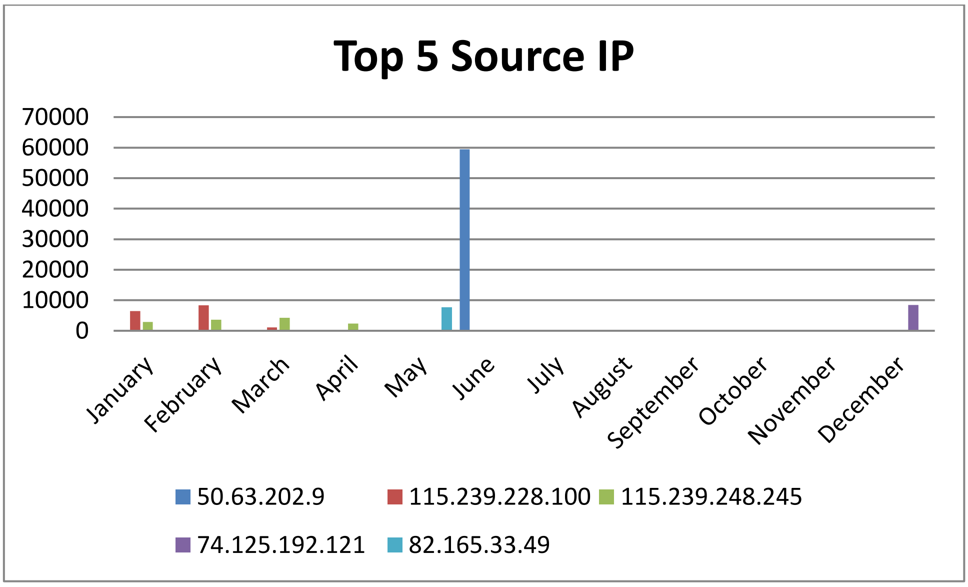
3.2 Incident handling report

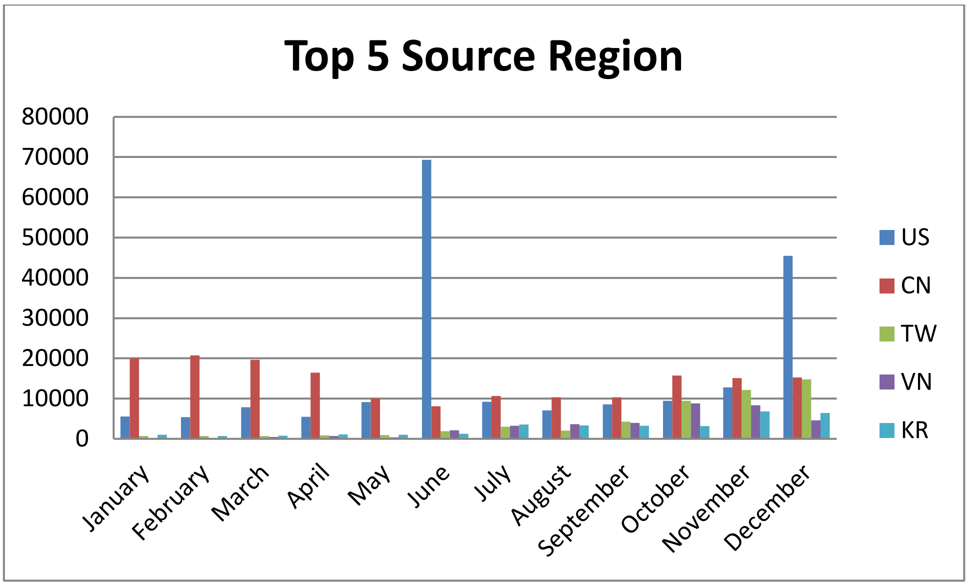
The following graph shows the incidents that happened in 2016.

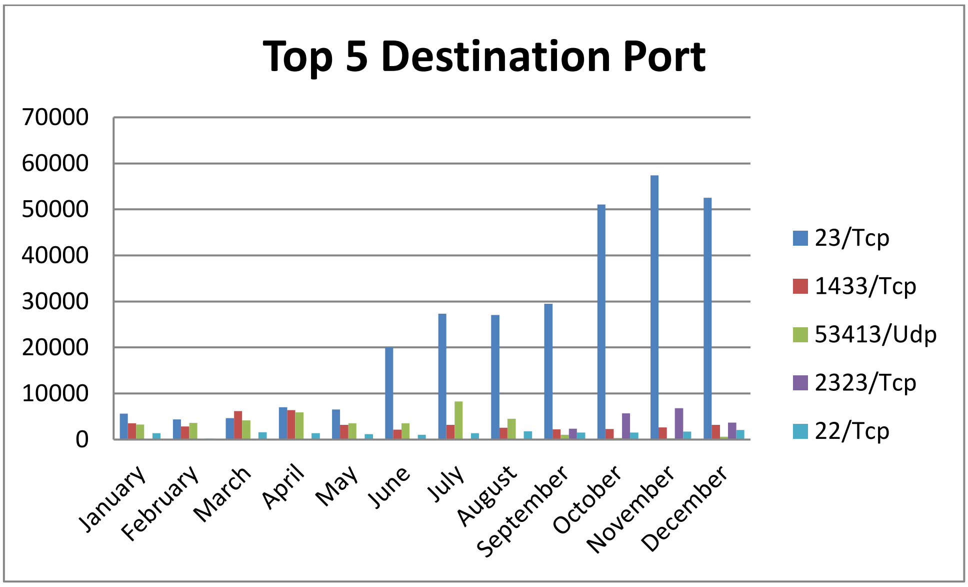


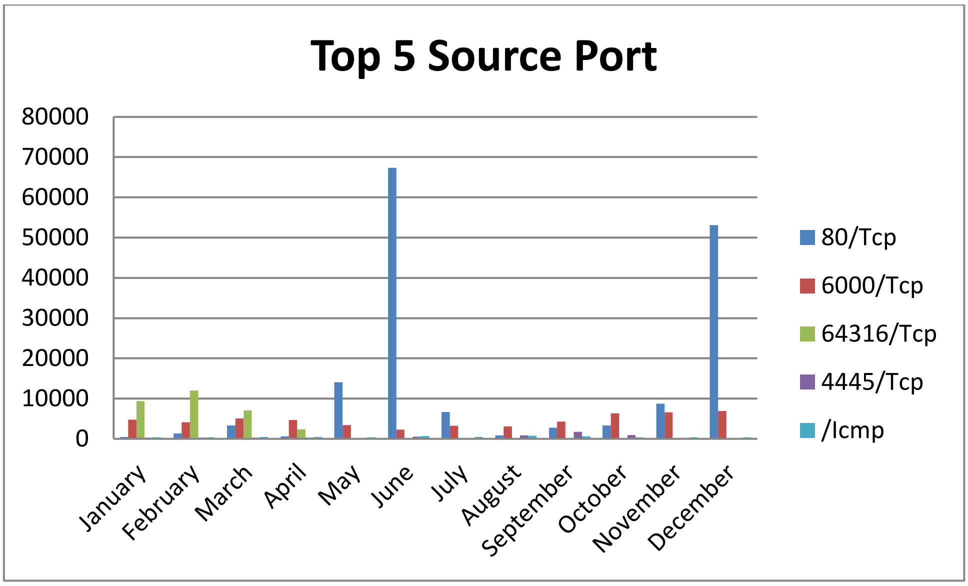
3.3 Abuse Statistics (TSUBAME Sensor)

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 2016.




Top 5 Source Region
80000
70000
60000
50000
40000
30000
20000
10000
0
January
February
March
April
May
June
July
August
September
October
November
December
US
CN
TW
VN
KR


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
1433/Tcp
53413/Udp
2323/Tcp
22/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

- Organize the TSUBAME Advanced Training course on 01st - 05th February 2016 in Vientiane, Laos PDR by invite experts from JPCERT/CC and ThaiCERT.

5. International Collaboration

5.1 International partnership and agreement

- MoM signed with VNCERT on 06th January, 2016.
- Successful to use the CERT's mark from CARNEGIE MELLON UNIVERSITY on 6th of June 2016.

5.2 Capacity Building

5.2.1 Training

- The Training Program on Enhancing Information Security for ASEAN: Focusing on ISMS and ICS (Industrial Control System) Security from 16th – 25th February 2016 in Tokyo, Japan.
- The Computer Network Intrusion Training Course from 25th -29th April, 2016 in Bangkok, Thailand.
- The 5th Training for Information Security Staff from 30th May - 10th June 2016 in Jakarta, Indonesia.
- The 4th Information Security Training on 3rd - 4th March, 2016 in Bali, Indonesia.
- Attending the National Information Security Policy Course and Cybersecurity Allience for Mutual Progress (CAMP) from July 11th - 15th, 2016 in Seoul, Korea.
- The Effective Incident Management and Active Defense Training from 1th – 10th August 2016 in Kuala Lumpur, Malaysia.
- The 6th Training for Information Security Staff from 26th September - 7th October 2016 in Indonesia.
- The APISC Security Training Course from 17th - 22nd October 2016 in Seoul, Korea.
- The Counteraction to Computer Terrorism on 30th October – 12th November, 2016 in Moscow, Russia.
- The Training on Information Security Staff Network Monitoring System from 21st November - 2nd December 2016 in Indonesia.
- The Singapore-United States Training Programme: Workshop on Cybercrime on 3th - 6th May, 2016 in Singapore.

5.2.2 Drills and Exercises (Online)

- Participating the APCERT Drill on March 16, 2016.
- Participating the ASEAN CERT Incident Drill (ACID 2016) on 27 September, 2016.

5.2.3 Seminar and conference

- Joint the 1st ASEAN-Japan WG for Cyber Exercise, CIIP and Capacity Building Meeting on 24 - 25 February 2016 in Brunei.
- Attending the China-ASEAN Network Security Emergency Response Capacity Building Seminar on May 23rd - 27th, 2016 in Chengdu, Sichuan, China.

- Participating the 3rd ASEAN-Japan Information Security Joint Working Group and the 2nd ASEAN-Japan Information Security Joint Working Group Meeting on 26th - 29th July 2016 in Bangkok, Thailand.
- Participating the the 9th ASEAN-Japan Information Security Policy Meeting from 18th - 21th October, 2016 in Tokyo, Japan.
- The Octopus Conference on Cooperation against Cybercrime on 16th - 18th November, 2016 in Strasbourg, France.

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 the Law on preventing and combating cybercrimes to public and private sectors.
- Drafting legislation under Cyber Crime Law
- Drafting National Cyber Security Strategy.
- Drafting of National cyber security policies and data protection Law.
- Implementing Lao Anti-virus.

7. Conclusion

With the legislation and work plans that mention in this report related to the training on human resource capacity building, Threat Monitoring System, Management Online System, Lao Anti-virus Project, Data Protection Law and National Cyber Security Strategy, LaoCERT expect to achieve all work plans in 2017. However the collaboration with other CERTs is very important and we are still need of supporting on human resources capacity building and budget to develop our team. Finally, LaoCERT would like to thank you to APCERT as well as CERTs organization for all kind cooperation and support.

mmCERT

Myanmar Computer Emergency Response Team – Myanmar

1. Highlights of 2016

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)" and "Government Technological College (GTC)".
- Host "Base Capture the Flag (Base CTF)" competition with "Myanmar Computer Professional Association (MCPA)" and private security teams.

1.2 Achievements & milestones

mmCERT's Technical member got the excellent in the project of "New Contribution" of "Professional Networking Training"

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 in 2011.

2.2 Establishment

mmCERT was established as a National Computer Emergency Response Team in Myanmar on July 23 2004 and mmCERT/cc (mmCERT coordination center) is strengthening on Dec 15 2010. The Ministry of Communication and Information Technology (MCIT) is a leading Ministry of National Cyber Security 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/cc include from two ministries: MOTC and Ministry of Science and Technology (MOST). The operation of mmCERT/cc was directly managed by Information Technology and Cyber Security Department and total five members worked for mmCERT/cc last year. The number of members didn't increase in 2016.

2.4 Constituency

mmCERT/cc 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 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 2016. According to the results on incident analysis by mmCERT/cc, Intrusion and Malicious cases were the most prominent incident cases in 2016.

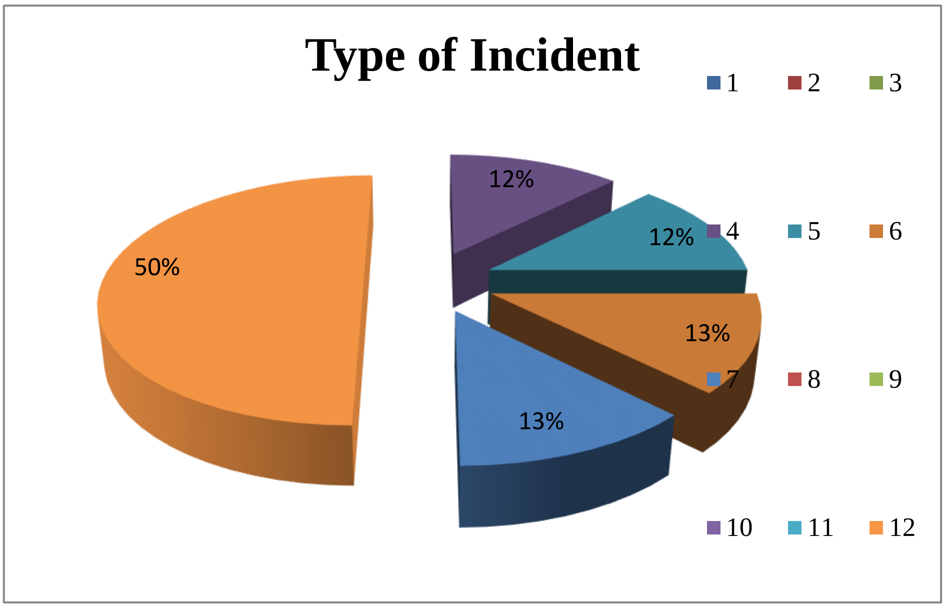


Figure 1 Type of Incident

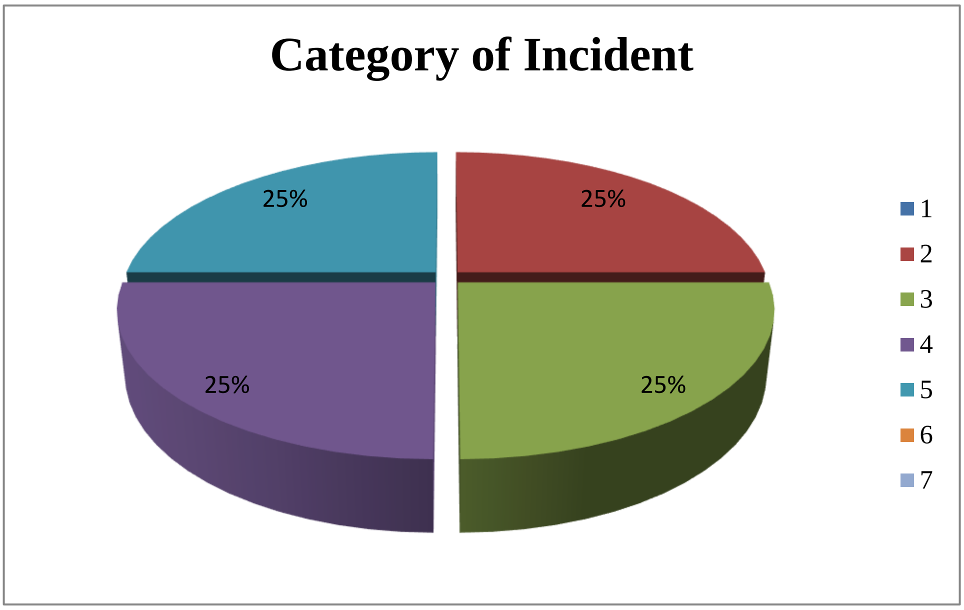


Figure 2 Category of Incident

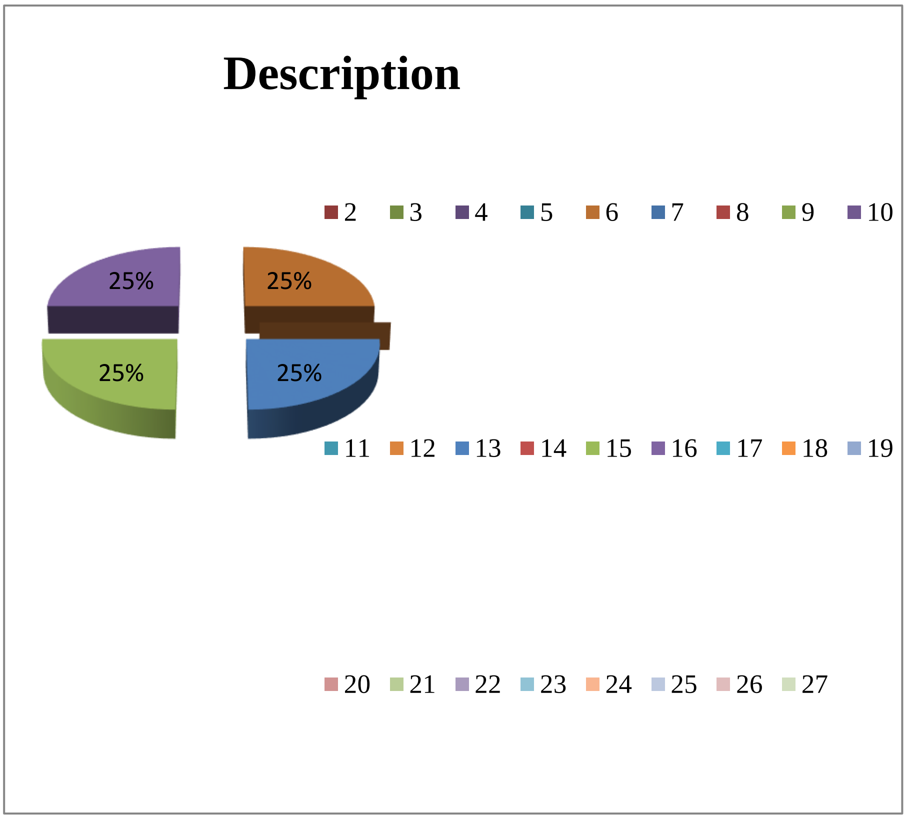


Figure 3 Description

3.3 Abuse Statistics

The following graph shows the Top Destination Port, Top Source Region and Top source IP address statistics obtained from TSUBAME Sensor in 2016.

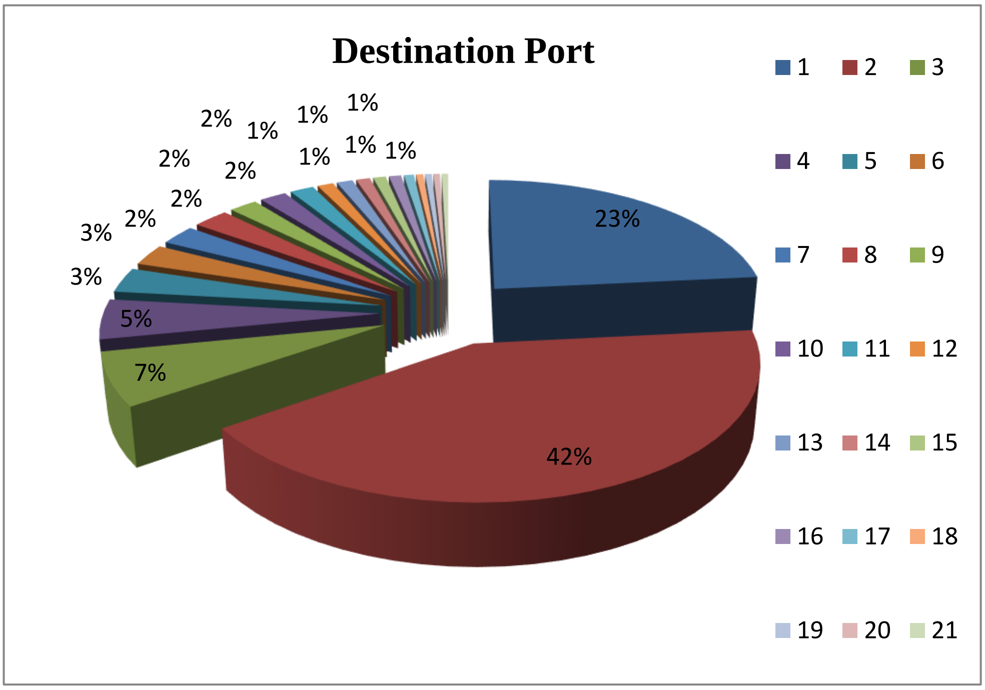


Figure 4 Destination Port

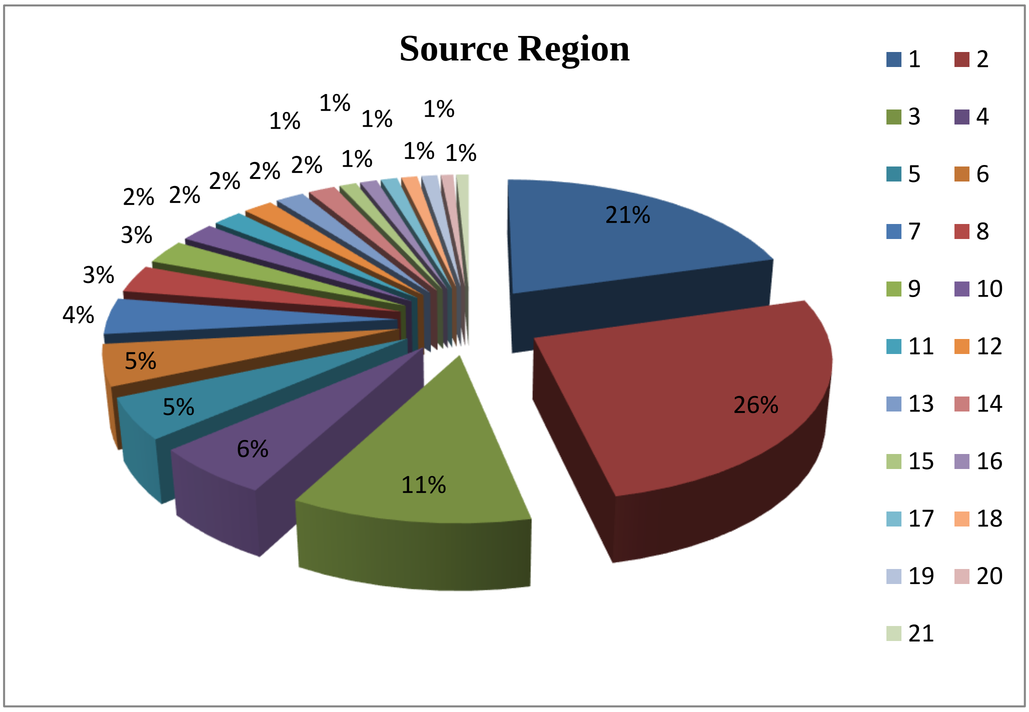


Figure 5 Source Region

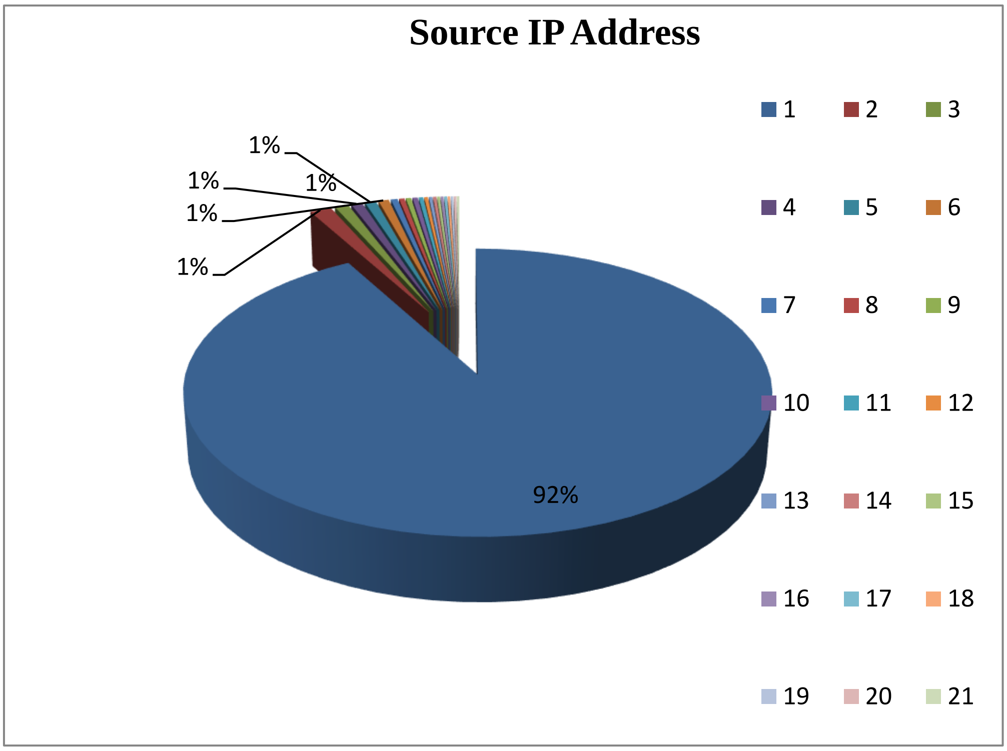


Figure 6 Source IP Address

The following graphs show the Top 5 Destination Ports and Top 5SourcesRegion statistics per month in 2016.

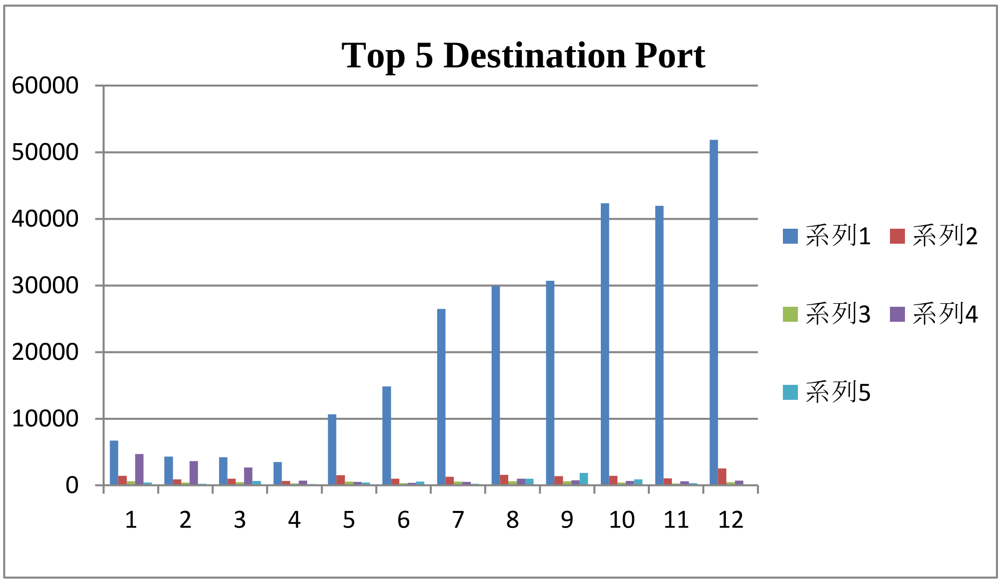


Figure 7 Top5 Destination Port

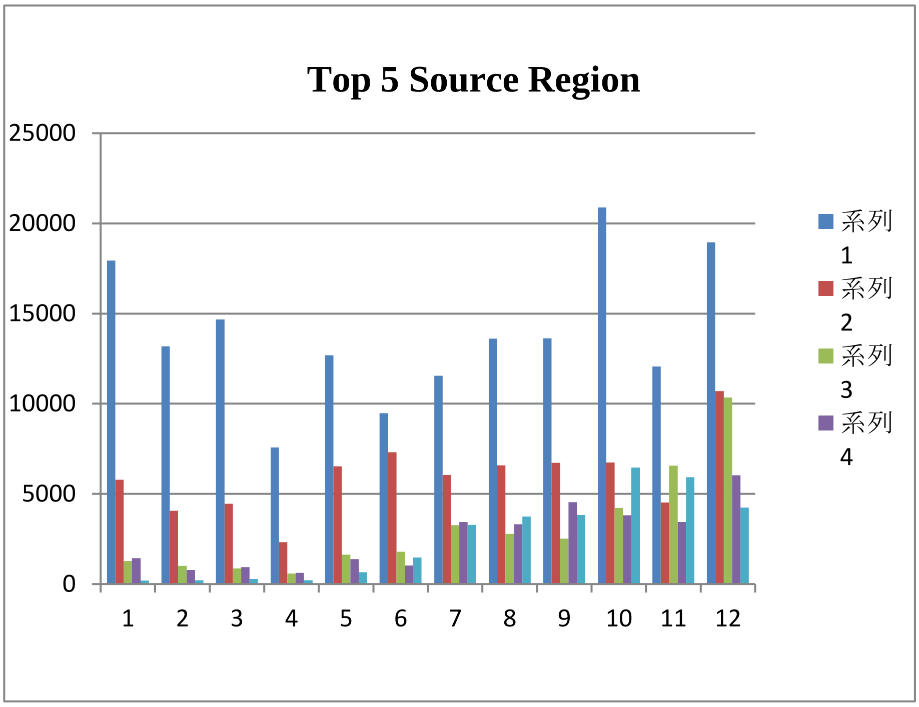


Figure 8 Top5 Source Region

4. Events Organized/Co-organized

4.1 Training

- Giving training to the staffs of the Ministry of Transport and Communication (MOTC) at NayPyiTaw on September 19-23, 2016.
- Attending the Incident Handling training hosted by ASEAN-JAPAN Cyber SEA Game at Myanmar Computer Professional Association (MCPA) on March 28th 2016.
- Attending the Professional Communication English training on February 2016.
- Attending the Professional Diploma in Network Engineering at ICTTI on 9th May 2016 to 11st Oct 2016.

4.2 Drill and exercises

4.3 Conferences and Seminars

- Giving Seminar to Cyber Crime Unit (Myanmar Police Force) at CID, Insein in Yangon on April 26th, 2016.
- Giving Seminar to Cyber Crime Unit (Myanmar Police Force) at CID, Insein in Yangon on August 30th, 2016.
- Giving Seminar to West Yangon Technological University Students at mmCERT in Yangon on October 3-7, 2016.

5. International Collaboration

5.1 Capacity Building

5.1.1 Training

- Attending to "NCSC Staff Training" at Japan (June 20 - 30, 2016)
- Attending to "the 6th ASEAN-JAPAN Information Security Staff Training" at Indonesia (September 26 - October 7, 2016)

5.1.2 Drill & Exercises

5.1.2.1 Drill

- Participating in APCERT Drill on March 16, 2016. APCERT Drill 2016 Title is "An Evolving Cyber Threat and Financial Fraud"
- Participating in ACID Drill on September 27, 2016. ACID Drill 2016 Title is "Ransomware and Cyber Forensics"

5.1.2.2 Cyber exercises

- Participating in ASEAN –JAPAN Cyber Exercise 2016 on May 25, 2016.

5.1.3 Seminar & presentations

- Attending to "CERT Meeting" at China (May 24 - 27, 2016)
- Attending to "28th the FIRST Conference" at Korea (June 12 - 17, 2016)
- Attending to ""The 2nd ASEAN-Japan Information Security Joint Working Group Meeting and The 3rd ASEAN-Japan Information Security Working" at Thailand (July 26 - 29, 2016)
- Attending to "Workshop on Cyber Security" at Singapore (August 16 - 18, 2016)
- Attending to "the 9th ASEAN-JAPAN Information Security Policy Meeting" at Japan (October 18 - 21, 2016)

6. 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 2016

1.1 Summary of major activities

MNCERT/CC has successfully organized MNSEC 2016 annual event which has covered pretty large scope and allowed the participants to exchange their experience and knowledge. Furthermore, we have organized successfully two more events named "Enterprise TECH" and "InfoSec Mongolia 2016" jointly with MOSA and JCI Progress.

Moreover, "Kharuul Zangi 2016" and newly initiated "Kharuul Zangi U18 2016" cyber security competitions have been held successfully by MNCERT/CC.

MNCERT/CC has handled and solved the incidents not only locally but in collaboration with international CSIRTs and cyber security organizations by coordinating them.

Furthermore, one of the main activities was providing its member organizations with security threat news feeds, recommendations, consulting and trainings.

1.2 Achievements and milestones

Year 2016 was a full of achievements for MNCERT/CC. We have joined international cyber security organizations and communities such as FIRST, APWG and FS-ISAC. It allows us to get up-to-date feeds of cyber threats, incidents and vulnerabilities with recommended actions as well as gave the opportunity to implement the project Stop.Think.Connect which was initiated by APWG and was spread through a lot of countries.

Furthermore, joining FS-ISAC as a trial member, we were able to get incidents, threats and vulnerabilities occurred in banking and financial sector and to provide the local banks and financial organizations with up-to-date information and instructions. This is a great contribution to cyber security of the banking sector. In the future, we are looking for getting a full membership of FS-ISAC.

One of the key achievements of this year was initiation of "Kharuul Zangi U18 2016" 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 Incident handling reports

- Valid credit card information which is Mongolian local bank customers' is leaked in Deepnet and social network. MNCERT/CC has discovered that and reported to banks that have to concern those cards.
- In 2016, MNCERT/CC received some DDoS reports that are related to Mongolia from other CERTs. Based on detail information on that reports, MNCERT/CC has notified owners who have to concern their devices and provided some information on how to protect their device.
- According to the notice from Security Operations Center, MarkMonitor, a fraudulent phishing website which has been hosted on a network in our jurisdiction

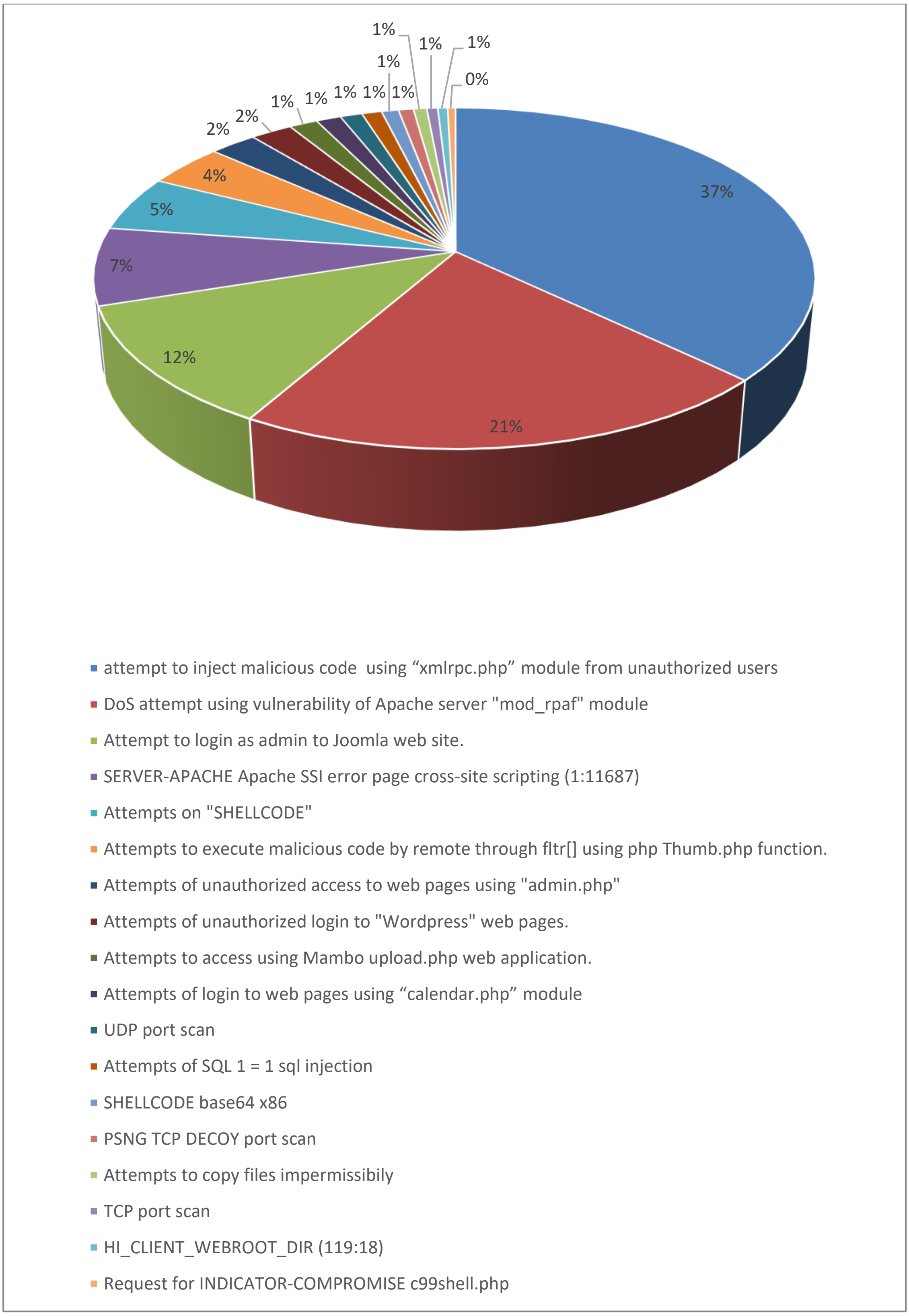
had attempted to steal account information from customers of Western Union and Verizon. MNCERT/CC has taken measurements to remove phishing URLs.

- In 2016, mails with malware file (.docx) attachment have been broadcasted through governmental organizations' electronic mail system. We have detected and determined the cause of this matter and delivered the appropriate recommendations to the governmental organizations. The malware attached with this email was designed to exploit a vulnerability to the system.

Malicious email broadcast was caused from losing one of user's own password. When inspecting the malicious email broadcast process from the server side, it has been sent with the normal email transfer process.

3.3 Abuse statistics

The summary of acitivities carried out by MNCERT/CC during the year 2016 is given in the following chart. This chart shows about summary of the critical incidents and attempts that were registered: attempts to inject malicious code using "xmlrpc.php" module from unauthorized users 37%, DoS attempt using vulnerability of Apache server "mod_rpaf" module 21%, attempts to login as an admin to Joomla web site 12%, SERVER-APACHE Apache SSI error page cross-site scripting 7%, attempts on "SHELLCODE" 5%, attempts to execute malicious code by remote through fltr[] using php Thumb.php function 2% and others 16%.


1%
1%
1%
1%
0%
1%
1%
1%
1%
1%
2%
2%
4%
5%
7%
12%
21%
37%
▪ attempt to inject malicious code using “xmlrpc.php” module from unauthorized users
▪ DoS attempt using vulnerability of Apache server "mod_rpaf" module
▪ Attempt to login as admin to Joomla web site.
▪ SERVER-APACHE Apache SSI error page cross-site scripting (1:11687)
▪ Attempts on "SHELLCODE"
▪ Attempts to execute malicious code by remote through fltr[] using php Thumb.php function.
▪ Attempts of unauthorized access to web pages using "admin.php"
▪ Attempts of unauthorized login to "Wordpress" web pages.
▪ Attempts to access using Mambo upload.php web application.
▪ Attempts of login to web pages using “calendar.php” module
▪ UDP port scan
▪ Attempts of SQL 1 = 1 sql injection
▪ SHELLCODE base64 x86
▪ PSNG TCP DECOY port scan
▪ Attempts to copy files impermissibily
▪ TCP port scan
▪ HI_CLIENT_WEBROOT_DIR (119:18)
▪ Request for INDICATOR-COMPROMISE c99shell.php

3.4 Publications

- "Internet usage in Mongolia" – Mr.Chinzorig Ganzorig, MNCERT/CC board member, http://mncert.org/blog/post/chinzorig-mnsec-2016# (in Mongolian)
- "My security depends on your security" – Mr.Otgonpurev Mendsaikhan, MNCERT/CC board member, http://mncert.org/blog/post/my-security (in Mongolian)
- "Information security" – Mr.Tsenguunjav Dansran, MNCERT/CC security analyst, http://mncert.org/blog/post/information-security (in Mongolian)
- "Misunderstandings about cyber security" – Mr.Otgonpurev Mendsaikhan, MNCERT/CC board member, http://mncert.org/blog/post/is-about (in Mongolian)

4. Events organized / hosted

4.1 Training

4.1.1 FIRST CSIRT Training

MNCERT/CC and FIRST has organized the very first CSIRT training in Mongolia during 26-27th Sep 2016 at National IT Park of Mongolia. The training has been instructed by Michael Hausding, a security specialist of SWITCH-CERT. The training consisted of 6 modules in which both the practical and theoretical aspects of CSIRT have been covered.

Overall 16 professionals from various industries have been participated in the training. The participant industries include

- Banking sector – 5 people
- Operator company – 4 people
- Government agency – 2 people
- Law enforcement – 2 people
- National data center – 2 people
- Security vendor – 1 person

4.1.2 Local Training

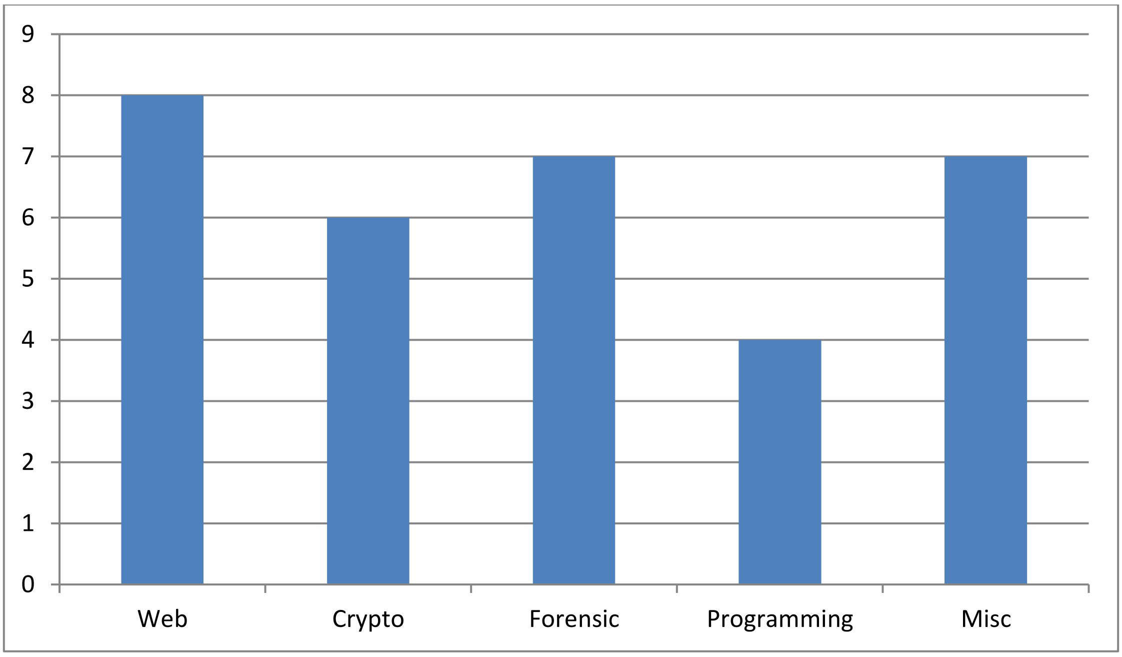
On 29th September, MNCERT/CC have conducted two kind of trainings among security engineers of public and private sectors during MNSEC-2016 event. The training subjects were "Metasploit" and "Open source log management", which instructed theoretically and practically by MNCERT/CC security researchers.

4.2 Drills & Exercises

4.2.1 "Kharuul Zangi 2016" 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. MNCERT/CC has successfully organized "Kharuul Zangi 2016" competition between 16th September to 29th September of 2016, in collaboration with Mongolian national data center, National cyber security department, Communications regulatory commission of Mongolia, "SafeBit" LLC, National information technology park and "MSTRide" LLC.

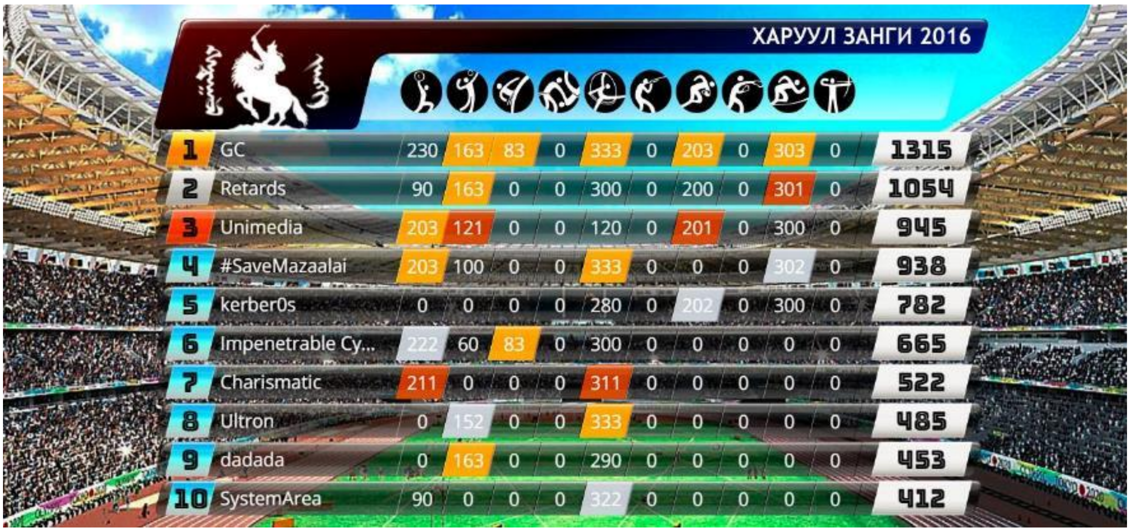
1st stage was designed to be completed online while the 2nd and 3rd stages had to be completed onsite using the network and systems designed by the organizers. Out of 174 teams of 522 members, 30 teams qualified from the 1st stage. Total of 32 tasks of 5 categories have been given to be completed at 1st stage and 22 tasks have been completed out of them by the competitor teams. Following chart shows the knowledge level of the participants who completed 5 different tasks on the 1st stage.



- **Forensic** –Make incident analyse based on the given data.
- **Web** – Compromise the system using website service
- **Crypto** –Encrypting and decrypting the data.
- **Programming** – Automated software development.
- **Misc** - Other types

On the 2nd stage, 28 tasks of advanced level were given to competitors and all the possibility to contact with other teams or to find information resources have been closed by blocking the communication channels such as public web portals, social network, instant messaging services, messengers as well as cell phone, bluetooth and wifi networks. This environmental setup has brought the biggest challenge and 10 teams were qualified to 3rd stage.

3rd stage of the competition has been held on 29th September 2016, on MNSEC-2016 event. During this stage, cameras were fixed by focusing the computer screens of competitor teams and the performance was shown on the screen for audience in real time which was interesting to the participants of MNSEC-2016.



ХАРУУЛ ЗАНГИ 2016

1	GC	230	163	83	0	333	0	203	0	303	0	1315
2	Retards	90	163	0	0	300	0	200	0	301	0	1054
3	Unimedia	203	121	0	0	120	0	201	0	300	0	945
4	#SaveMazaalai	203	100	0	0	333	0	0	0	302	0	938
5	kerber0s	0	0	0	0	280	0	202	0	300	0	782
6	Impenetrable Cy...	222	60	83	0	300	0	0	0	0	0	665
7	Charismatic	211	0	0	0	311	0	0	0	0	0	522
8	Ultron	0	152	0	0	333	0	0	0	0	0	485
9	dadada	0	163	0	0	290	0	0	0	0	0	453
10	SystemArea	90	0	0	0	322	0	0	0	0	0	412

Score board of "Kharuul Zangi 2016" contest

4.2.2 "Kharuul Zangi U18 2016" Cyber Security Competition

MNCERT/CC has initiated and organized cyber security competition named "Kharuul Zangi U18 2016" among the high school students under the age of 18 on May 2016. 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 160 competitors of 40 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. In the further, "Kharuul Zangi U18" annual competition will be held traditionally.

4.3 Conferences and seminars

4.3.1 MNSEC-2016 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-2016" event on 28th and 29th September of 2016 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-2016 event has been conducted successfully with the great contribution from JPCERT/CC, Team Cymru, APNIC, Switch-Cert and Palo Alto UNIT 42. 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 120 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 "Enterprise Tech" event

On 26th February of 2016, MNCERT/CC and Mongolian Software Industry Association (MOSA) has jointly organized the "Enterprise Tech" event among top 100 economic entity including banks, financial and governmental organizations. The goal of this event was to introduce to economic entities how the enterprise technology appropriate usage can influence on reducing the company activity expenses, improving control and enhancing the productivity.

The event has covered the wide range of scope and has discussed about enterprise system development trends, urgent issue faced in Mongolia and its solution ways up-to-date as well as to introduce soft infrastructure platform, information security, mobile communication solutions and the roles of enterprise system consulting companies to business runners.

4.3.3 "InfoSec Mongolia 2016" event

"InfoSec Mongolia 2016" event has been held in conjunction with MNCERT/CC, ASCO, JCI Progress and IT sector organizations on 2nd March, 2016 in Ulaanbaatar.

The event collected the cyber security staffs and experts from the local and overseas as well as exchanging the experiences and ideas of strategic policy and newly developed technologies. Event were significant to expand and deepen the further cooperation among the cyber security experts of private and public sectors.

5. International Collaboration

5.1 International partnerships and agreements

Newly established memberships in 2016:

- MNCERT/CC has joined the APWG (Anti-Phishing Working Group) on January, 2016.
- MNCERT/CC has joined the FS-ISAC (Financial Services - Information Sharing and Analysis Center) as a trial member on August, 2016.
- MNCERT/CC has joined the FIRST as a full member on September, 2016.

5.2 Capacity building

5.2.1 Training

- "Introduction to network forensics and analysis" online training organized by TWNCERT on February, 2016
- "Internet of things (IoT) trend" online training presented by ID-SIRTII/CC on April, 2016
- "Tactical against malicious scanning network" online training presented by HKCERT on August, 2016
- "The growing threat of ransomware in Malaysia" online training presented by MyCERT on October, 2016
- "How Microsoft safeguards your data in the cloud" online training presented by Microsoft Corporation on December, 2016

5.2.2 Drills & exercises

MNCERT/CC participated to the following Drilling exercise:

- APCERT Drill 2016 on March, 2016

5.2.3 Seminars & presentations

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

- APCERT Annual General Meeting and Annual Conference 2016, on October 2016 in Tokyo, Japan.
- "2016 APISC Security Training Course" organized by KrCERT/CC and KISA, 17th to 22nd of October 2016 in Seoul, Korea
- Team Cymru Annual Event UE16 on April in Doha, Qatar

6. Future Plans

6.1 Future Operations

MNCERT/CC planned the following activities in 2017.

Events, conferences and drill to participate are as follows:

- APCERT Drill 2017 on March 2017.
- FIRST Annual Conference 2017 on June in San Juan, Mexico
- APCERT Annual General Meeting 2017 on October in Delhi, India

Activities to organize are as follows:

- Organizing MNSEC-2017 Cyber Security Event
- Organizing GOVSEC-2017 Cyber Security Event among Governmental organizations
- Organizing "Kharuul Zangi U18 2017" Cyber Security Contest among high schools students
- Organizing "Kharuul Zangi 2017" Cyber Security Contest among IT specialists.
- Local cyber drill among member organizations.

7. Conclusion

2016 was the year of great success and progress for MNCERT/CC. We've restructured our organization and reformed our board with new members.

We have extended our international partnership by joining "FIRST" as a full member and "FS-ISAC". More local organizations have joined to MNCERT/CC cyber security services including banking and financial organizations. Moreover, the membership to

“APWG” gave us the opportunity to implement a project named “Stop.Think.Connect” and distribute the cyber security knowledge and awareness to general public.

All in all, we are looking forward the year 2017 to be a more progressive year in both local and international stage and greater collaboration with APCERT.

MOCERT

Macau Computer Emergency Response Team Coordination Centre – Macao

1. Highlights of 2016

1.1 Summary of Major Activities

During the year 2016 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;
- Assisted in the delivery of a course in cyber security topics at high schools;
- Actively taking part in the cyber security community through conferences;
- Speech to IT staffs of the constituency at a local event called SAFE-T Summit;
- Assisted in the APCERT Membership Working Group;
- Assisted in the APCERT Policy Procedure and Governance Working Group;
- Involved in the TSUBAME Working Group;
- Assisted in the APCERT Drill 2016 as OC, Player, Observer and EXCON;
- Article publications in a local magazine called "Macau-ICT".

1.2 Achievements & Milestones

1.2.1 Memorandum of Understanding (MOU) between MOCERT and CNCERT/CC

In order to cope with the challenges of network security on information infrastructures of both mainland China and Macao S.A.R. MOCERT and CNCERT/CC have signed a MOU to reinforce the cooperation on network security and emergency response in 2016.

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 2016 there are three (3) 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

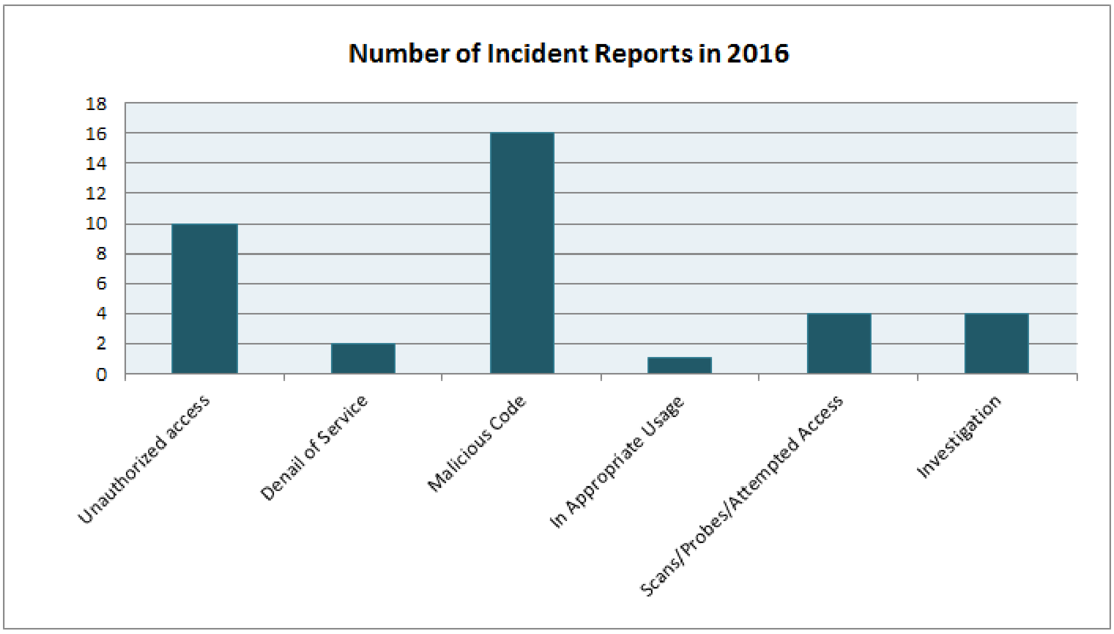
Macau Computer Emergency Response Team Coordination Centre (MOCERT) is managed by Macau New Technologies Incubator Centre in providing Macau with computer security incident handling information, promoting information security awareness, as well as coordinating on an international and local level, computer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

3.2 Incident Handling Reports

Incident reports are increasing rapidly 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.

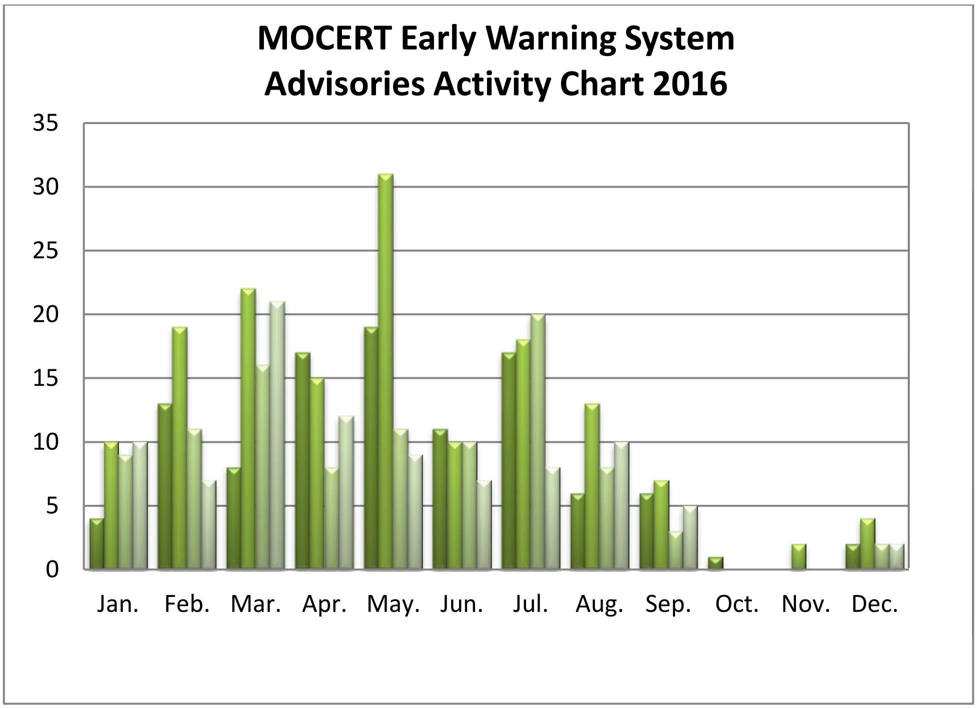
Sources of incidents are from three distinct channels.

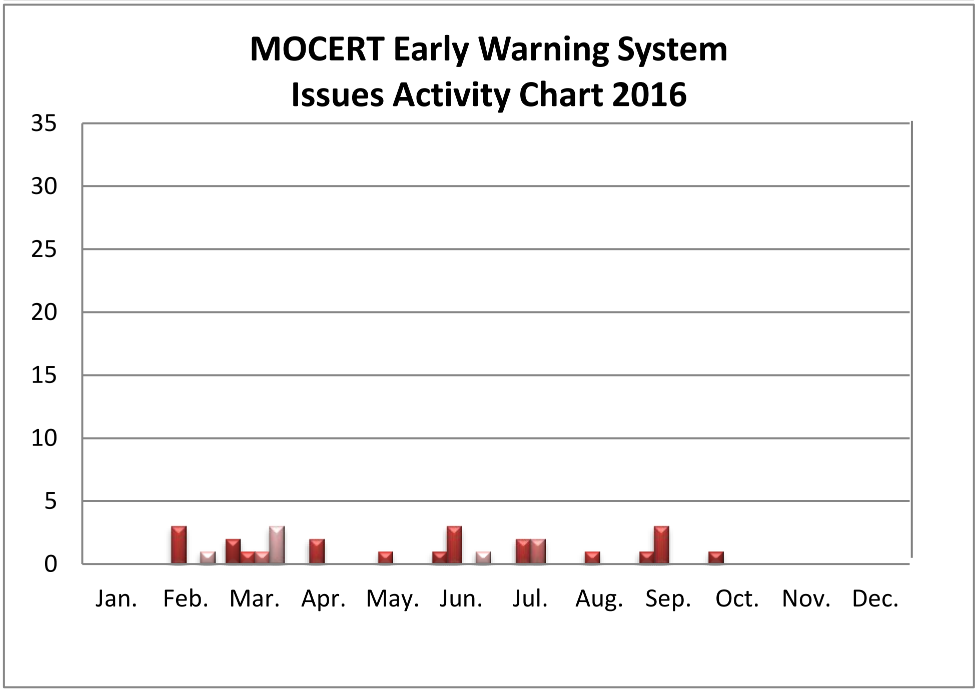
1. Reported by Web
2. Reported by Phone message
3. MOCERT initiated from incident discovery activity.



Early Warning Notices - A website collects notifications related to computer security, where all notifications are reviewed by staff to determine the impact to Macao constituency.

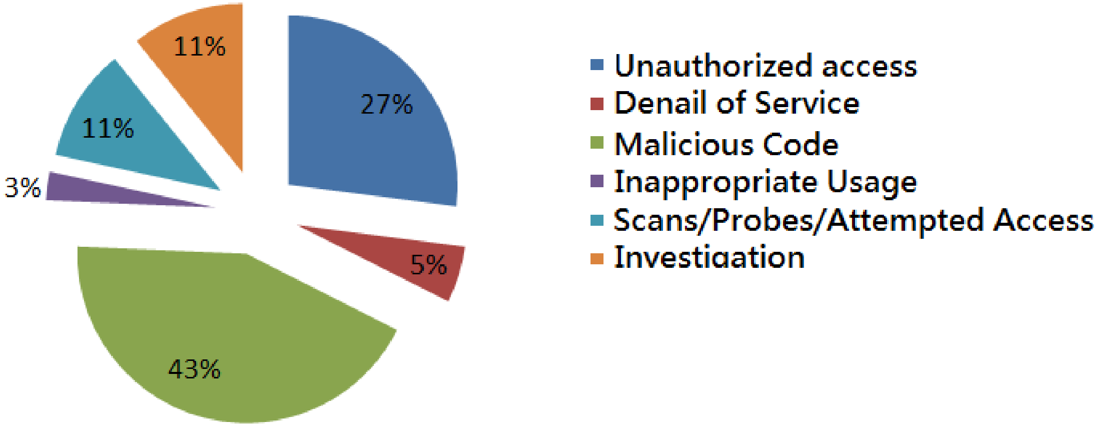
The notifications are then classified to Issues and Advisories and then posted. The following diagram shows the distribution of the 473 postings in 2016 with 444 postings being Advisories, and 29 Issues.





3.3 Abuse Statistics

The following pie graph denotes the abuse distribution as noted for the year 2016. The numbers are drawn from the incidents handled.



3.4 Publications

3.4.1 Leaflet

The four (4) leaflet publications that were previously made continue to be distributed during the multitude of events being organized and co-organized by MOCERT.

3.4.2 Articles

MOCERT published articles in a local magazine called “Macau-ICT” .The magazine is distributed free of charge to the constituency of MOCERT as well as that of MANETIC.

- **Macau-ICT ISSUE 23**

  Title:

  1. Soft System Perspective of Information Security Risk Management

  2. Introduction to “DirBuster”

  Link:

  http://www.manetic.org/index2.php?option=com_flippingbook&view=book&id=32:issue-23&catid=3:macau-ict&tmpl=component

- **Macau-ICT ISSUE 22**
  Title: Introduction to "Temper Data"
  Link:
  http://www.manetic.org/index2.php?option=com_flippingbook&view=book&id=31:issue-22&catid=3:macau-ict&tmpl=component
- **Macau-ICT ISSUE 21**
  Title: OWASP ZAP Account Authentication and Management
  Link:
  http://www.manetic.org/index2.php?option=com_flippingbook&view=book&id=29:issue-21&catid=3:macau-ict&tmpl=component

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 supported a local event called SAFT-T Summit jointly organized by Macau New Technologies Incubator Centre and Macau Association of Systems Engineering, and co-organized by Public Administration and Civil Services Bureau on 17th November 2016. MOCERT delivered a speech with regard to current trend and threat in the IoT industry.

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 Drills & Exercises

5.2.1.1 APCERT Drill

The involvement in 2016 in the APCERT drill included as a Player, Observer and EXCON. Also MOCERT assisted the Drill Organising Committee in designing the

Detailed Scenario. The event continues to be instrumental in reshaping some of the services provided by MOCERT for 2016.

5.2.2 Seminars & Presentations

MOCERT attended APCERT AGM and Conference in Tokyo.

6. Future Plans

6.1 Future Projects and Operation

Future projects include expand the services of penetration testing, IT auditing, and information security training for the constituency. Staff of MOCERT will learn and sharpen their skills through training to assist the constituency in assessing information security risk and against cyber-attacks. MOCERT will collaborate with IT staff of the constituency in regard to their demands for improving information security through conducting series of on-demand training courses.

MOCERT also plan to develop the Early Warning System for the constituency and make it more effective in the future.

7. Conclusion

2016 has been a year where our services adjusted and improved as requests from the constituencies increased.

The major challenges up ahead are restructuring the team to expand service in capacity and functionality as further penetration testing and automated vulnerability scanning is 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 aimed to securing Mongolian Education and Business sector's cyber space. MonCIRT provides Incident Prevention and Response services as well as Security Quality Management Services as allow our financial situation. MonCIRT 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
- Consult to business entities in handling of cyber security incidents
- Issue guidelines, advisories, vulnerability notes and white papers on information security practices, procedures, prevention, response and reporting of cyber incidents
- Improve information security awareness, literacy, provide comprehensive trainings.
- 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 all business entities, personals.

The MonCIRT helps constitutes to 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/ (Now under construction)

1.1.1 Establishment

MonCIRT was established in 2006 as NGO. From 2006 till 2013 MonCIRT operate as sole national CSIRT of Mongolia. After establishment of MNCERT/CC (with MonCIRT's full support) and National Cyber Security Department in 2011 MonCIRT acts as the focal point for cyber security for the nation, especially educational and business sector.

1.1.2 Workforce

MonCIRT currently has a total of 8 constant staffs such as: head-1, executive director-1, experts 4, the bookkeeper 1, system administrator-1.

1.1.3 Constituency

Currently MonCIRT's constituency encompasses the Educational and Business Sector of Mongolia. Our constituency consist of business companies, educational institutes, private sector organizations, NGO and general Internet users. From 2015 we began to cooperate closely with Mongolian Chamber of Trade and Industry, Erdemnet ISP (Special ISP for educational sector), Chief Information Officers and system administrators of business sector.

In addition, MonCIRT acts as a focal point in Mongolia for cooperation and coordination with relevant bodies outside Mongolia. We also promoting latest international best practices and standards to our constituency and providing 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 & Operations

2.1 Activities

The summary of activities carried out by MonCIRT during the year 2016 is given in the following table:

Activities	Year 2016
Security Incidents handled (failure, email attack, malware, improper usage, attrition e.t.c)	468
Security Alerts issued	198
Advisories Published	21
Vulnerability Notes Published	45
Security Guidelines Published	1

Trainings Organized	2
Mongolian Website Defacements tracked and advised	162
Open Proxy Servers tracked	2
Bot Infected Systems tracked	352
Phishing (mirror) web sites tracked and removed	3
Projects	1

This part of the report describes the statistics of team activities and security incident reports handled by MonCIRT, both from external and internal sources. In 2016 MonCIRT handled 468 incidents which was 3 times decrease of the previous year which related with parliament election, new political situation and decrease of reporting activities of constituency. The major category of security incidents was phishing (214 cases) and Botnet. The phishing cases decreased 2 times.

From January through December 2016, the MonCIRT received 642 email messages and more than 280 hotline calls reporting computer security incidents or requesting information. About 58% of these messages, information was related with real incidents and we provided with recommendations, advises and. We cannot fully retrieve incident handling statistics from organizations, administrators due to executive’s restriction.

The majority of web threats in Mongolia in 2016 are delivered from popular web sites that have been hacked for use by cybercrime. The once obscure link farm for search engine poisoning now resides within popular web sites. The exception for link farms is now a rogue domain or remote web location. Phishing attacks overwhelmingly come from popular and trusted web sites hacked by cybercrime.

We received 16 vulnerability reports and handled 37 serious security incidents during this period.

We continue to provide advice to system administrators in the Internet community who report security problems. From 2015 operates our regular chat system with administrators of organizations.

In 2016, MonCIRT reported about 28.371 IPs of large botnets (Conficker, Downadup, Sality etc.) and sent 216 botnet warnings to universities, companies and supported them.

Abuse statistics in last two year

Security Incidents	2015	2016
Phishing	464	504
Deface	291	162
Malware	4.231	3.426
Other	240	378
Total	**5.226**	**4.470**

2.2 Watch and Warning

Three of our experts acts as watch and monitoring officers and regularly receive cyber security advisories, alerts, notes from different sources including APCERT mailing list, JPCERT/CC analyse note, monthly report, weekly reports of CNCERT, publications@us-sert.gov . Once serious alerts, vulnerabilities, threats appears we publish them on web site, social and news portals on Mongolian language,

During reported period we published 198 alerts, advisories, notes on web sites, portals like news.mn, cybersafety.mn, dorgio.mn, ikon.mn, medee.mn, time.mn e.t.c.

2.3 Malware and the web vulnerabilities

In 2016, MonCIRT focus on handling the security incident of Website defacements and Intrusion. By analyzing the 314 mn domain website Intrusion incidents handled in 2016, we find the following causes which result in the above website intrusion:

1. SQL Injection Vulnerability
2. Weak Password Account Vulnerability
3. Permission Control Vulnerability
4. Cross Site Scripting Vulnerability
5. System Vulnerabilities existed in website servers
6. Information Leakage in Website

In which is the largest number of Intrusion incidents is SQL injection and followed by the access control vulnerability, while the Information Leakage vulnerability is becoming another serious threat.

From 2015 operates MonCIRT's real time chat system with administrators and this system helped us to collect more information on faced threats. In addition, our "System

Admins" facebook page (https://www.facebook.com/Монголын-Систем-Администраторуудын-Холбоо-1413925735581985/) help us to collect more information on cyber security and allow to discuss threats trends interactively.

MonCIRT working closely with Mon Pass CA, the certification authority in Mongolia and support digital certificates usage in Mongolia, .

Most vulnerable web sites have the domain gov.mn and we reported to the National Security Council and Cyber Security Department.

The relative volume of the various alerts can help to describe how attacks are established and launched. They also frequently provide hints about how methods have evolved. Based on this, the main focus in 2016 may have been the subversion of systems, with larger coordinated attacks being executed across fairly broad swaths of the Internet.

Because of usage of security suites increasing the number of malware attack reported was decreased. As show our survey in Mongolia widely uses Kaspersky Internet Security, Bitdefender Internet security and Eset Nod.

2.4 Incident trends

Based on our experience the MNCERT/CC start to handle incidents. As a result of connection with NDC's monitoring system, our sensors 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 2016 MonCIRT handled several incidents of intrusions into websites using SQL and Cross Site Scripting, PHP injection and injecting Java script to redirect visitors to malicious websites. By exploiting vulnerabilities in web applications trusted websites are infected with links to malicious websites serving content that contains client side exploits. Most of incidents handled was web site defacements. We tracked and advised in 162 defacement cases from which 21 is handled by our team.

As show our monitoring, the malware delivery networks are now hiding in legitimate sites that are typically allowed by acceptable use policies. As shows below the leading categories for hosting malware (versus delivery) for the 2016 in Mongolian Internet segment.

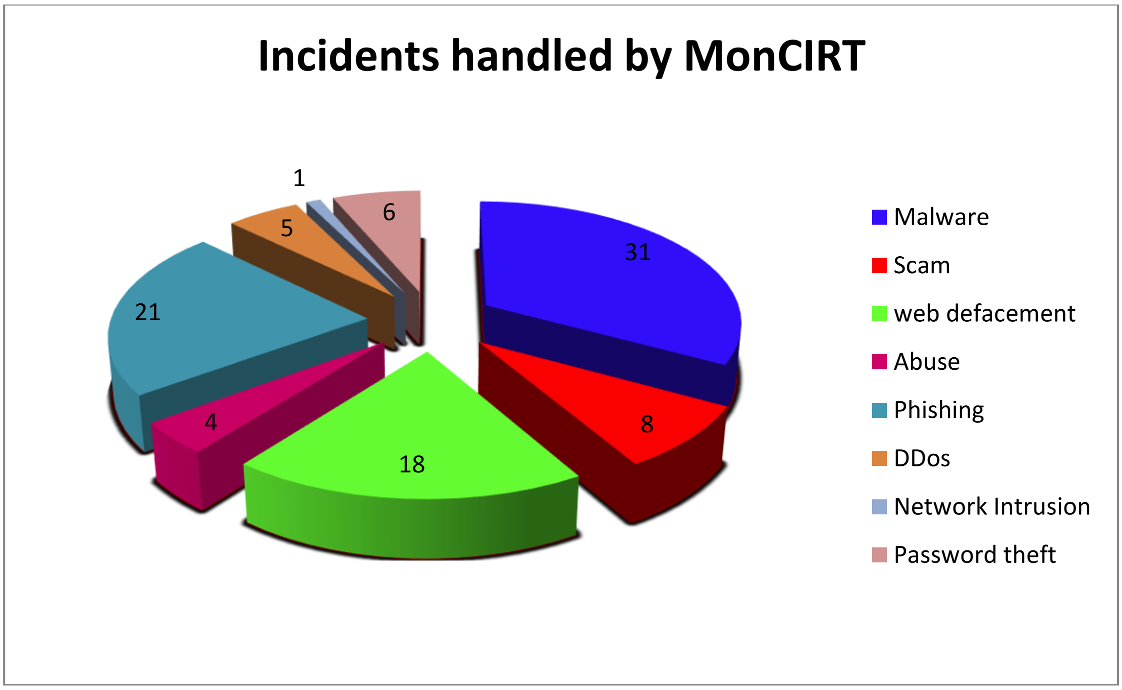
1. Online Storage
2. Software Downloads
3. Pornography

4. Open/Mixed Content
5. Computers/Internet
6. Placeholders
7. Phishing
8. Hacking
9. Online Games

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.

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.

The following chart depicts the distribution of various types of incidents handled by MonCIRT



2.5 Security Monitoring and Information Distribution

In 2016 MonCIRT implemented security monitoring activities and found that, most of the large scale DoS attacks in the business and educational network are still DNS Reflection Attacks, after analyzing the attacking sources we found that, not only the DNS servers configured with recursive query service are used for DNS Reflection

Attacks, but also some personal wireless routers with open source system are used for NS Reflection Attacks, and based on these intrusion incidents, we published the security configuration guide for users with these wireless routers.

2.6 Anti-spam activities

In 2016, MonCIRT received 3.423 complaints on spam messages (including 1295 spam SMS on mobile phones) and advised how to deal with such a messages.

2.7 New services

MonCIRT now works on establishment of impact analysis service for our constituency. In addition we plan to offer Cyber security requirements development service.

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 programmes on focused topics for targeted audience such as CISOs, financial and banking sector officers, System Administrators etc. Experts from industry are delivering lectures in these workshops apart from MonCIRT staff.

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 2016 included the following:

- Network security management and configuration
- Information Security for Managers
- Fundamentals of Incident Handling and Management

MonCIRT organized following workshop:

« Workshop on "New Cyber threats" on August 24, 2016

In addition we participated in organizing of ethical hacking contest “Kharuul Zangi 2016”.

3.2 Drills

In 2016 MonCIRT cannot organize local network security drill, participate in APCERT drill due to financial limitation, new parliament election and the new Government.

4. Achievements

4.1 Presentations

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

- Presentation on Annual "ICTPA Open Day" and ICTPA expo 2016 conference on themes "Emerging cyber threats".

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

4.2 Certification & Membership

No Certification and Memberships obtained in 2016:

5. International and Domestic Collaboration

5.1 MoU

We signed MOU with RUCERT.

5.2 Event participation

June 12–17, 2016 — Seoul, Korea. 28th Annual FIRST Conference on Computer Security Incident Handling

May 26-27, 2016 – Kazan, Russia. IT&Security forum.

5.3 International incident coordination

Upon request of some security companies from Europe, USCERT and UK CERT we handled incidents related to 4 phishing web sites installed illegally in Mongolian web servers.

6. Future Plans

6.1 Future projects

We now working on development of all necessary documents, handbooks of NDC CERT. In addition our experts will train staffs of NDC CERT. This project started in April 2012 and continue.

6.2 Future plan

We plan to deploy the incident monitoring mechanism in Mongolia and impact analysis service for our constituency.

7. Conclusion

For MonCIRTs' constant and developing activity we ask for financial support from MonPass CA, the Certification Authority of Mongolia and SSSC LLC. Despite difficulties in financing MonCIRT handled many incidents related with Business organizations and MonCIRT's awareness campaigns was successful. The awareness and knowledge of the public on information security have increased considerably thanking these awareness campaigns.

MonCIRT now gives the basic attention on the new financing strategy, paid membership mechanism.

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 educational and private sector oriented CSIRT.

MonCIRT shall continue to participate in regional events such as the Annual APCERT events, join to FIRST. In relation with this we invite APCERT operational members to visit us and prepare site visit report for FIRST. We kindly ask APCERT to promote this and call CNCERT, KRCERT/CC, JPCERT/CC (close to Mongolia) to visit us.

Contact Information

Postal Address: Mongolian Cyber Incident Response Team (MonCIRT).
Tokyo street 3-12. Bayanzurkh District. Ulaanbaatar, Mongolia, 13381
.

Incident Response Help Desk

Phone: +976-70113151
Fax : +976-70153286

MyCERT

Malaysian Computer Emergency Response Team – Malaysia

1. HIGHLIGHTS OF 2016

1.1 Summary of major activities

21-24 February 2016	Participate in the APCERT Steering Committee Meeting and APCERT Security Day in Auckland, New Zealand.
16 March 2016	Participate in the APCERT Drill 2016.
2-6 May 2016	Receive the World Summit on the Information Society (**WSIS**) Prizes 2016 during the WSIS Forum 2016, Geneva, Switzerland.
17-20 May 2016	Deployment of a Malware Collection Point (**MCP**) at Brunei Computer Emergency Response Team (**BruCERT**).
26 July 2016	Conduct the OIC-CERT Cyber Drill 2016.
1-10 August 2016	Conduct a capacity building training under the Malaysian Technical Cooperation Program (**MTCP**).
15 August 2016	Signing Ceremony of a Memorandum of Understanding (MoU) between CyberSecurity Malaysia and the Academy of Informational Systems (**AIS**) from the Russian Federation.
8 September 2016	The official launching of Cyber Range Malaysia, at the International Islamic University Malaysia (**IIUM**), Kuala Lumpur.
27-30 September 2016	Participate in the Organization of the Islamic Cooperation – Computer Emergency Response Team (**OIC-CERT**) Technical Workshop in conjunction with CodeBali International and the FIRST Technical Colloquium Conference.
17-19 October 2016	Organise the Cyber Security Malaysia- Awards, Conference & Exhibition (**CSM-ACE**) 2016 and MoU signing ceremony with Kaspersky Lab.
17 October 2016	Host a visit by the Defense Space Agency (**DSA**) of Nigeria.

19 October 2016	Organise the National ICT Security Discourse: CyberSAFE Challenge Trophy 2016 (**NICTSeD**), Kuala Lumpur.
21 October 2016	Host a visit by CERT-UK.
21-26 October 2016	Participate in the APCERT Annual General Meeting (**AGM**) & Annual Conference 2016, Tokyo, Japan.
2 November 2016	Signing Ceremony of a MoU between CyberSecurity Malaysia and the Korea Internet & Security Agency (**KISA**) from the Republic of Korea.
11-14 December 2016	Conduct the OIC-CERT 8th AGM & Annual Conference 2016 in Jeddah, Kingdom of Saudi Arabia.

2. ABOUT CYBERSECURITY MALAYSIA

2.1 Introduction

CyberSecurity Malaysia is the national cyber security specialist agency under the purview of the Ministry of Science, Technology and Innovation with a vision of being a globally recognised National Cyber Security and Specialist Centre by the year 2020.

CyberSecurity Malaysia's main roles can be summarised as follows:

i. To assist the National Security Council of Malaysia (NSC) in the implementation of the National Cyber Security Policy (NCSP);

ii. To provide Cyber Security Emergency Services and act as the national technical coordination centre;

iii. To conduct Cyber Threat Research & Risk Assessment;

iv. To provide Cyber Security Quality Management Services; and

v. To build capability in the field of cyber security (training) and to create awareness and a culture of cyber security (outreach).

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:

- Strategic Engagement
- Research

2.2 Establishment

CyberSecurity Malaysia started with the formation of Malaysian Computer Emergency Response Team (**MyCERT**) on 13 January 1997 as a unit under MIMOS Berhad, an agency under the Ministry of Science, Technology and Innovation Malaysia. On 28 December 2005, the Cabinet of Minister meeting, through the Joint Cabinet Notes by the Ministry of Finance (MoF) and Ministry of Science, Technology and Innovation No. H609/2005, agreed to establish a National ICT Security and Emergency Response Centre (now known as CyberSecurity Malaysia) as a National Body to monitor the National e-Security aspect, separated from MIMOS to become a government agency and incorporated as a Company Limited-by-Guarantee, under the supervision of Ministry of Science, Technology and Innovation of Malaysia.

The Malaysian Government gazetted the role of CyberSecurity Malaysia by the Order of the Ministers of Federal Government Vol. 53, No.13, dated 22 June 2009 (revised and gazetted on 26 June 2013 [P.U. (A) 184] by identifying CyberSecurity Malaysia as an agency that provides specialised cybersecurity services and continuously identifies possible areas that may be detrimental to national security and public safety.

2.3 The Malaysian Computer Emergency Response Team

The Malaysia Computer Emergency Response Team (**MyCERT**) is the 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, respectively providing technical support for incident handling and malware advisories and research. More information about MyCERT can be viewed at: https://www.mycert.org.my/en/

2.4 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

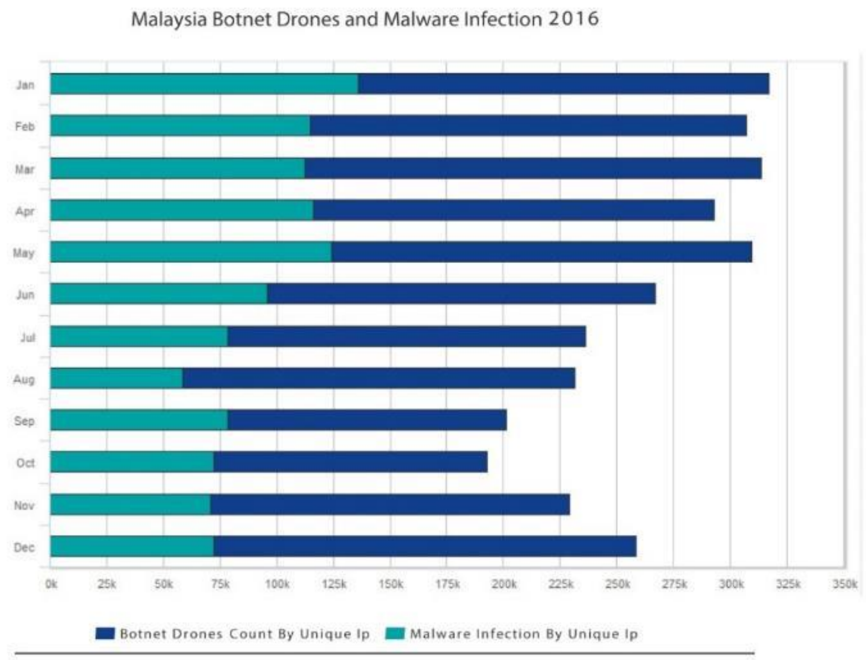
MyCERT, through its Cyber999 help centre, had responded to approximately 8334 incidents, with about 94% incident resolution in 2016. A significant number of incidents reported to MyCERT in 2016 were related to intrusion and fraud cases.

2.5 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.

MRC successfully launched several initiatives in 2016 that were essential to the centre's establishment. In extending the Lebahnet 2.0 project capabilities, the MRC team has enhanced a Multi Analyzer System called MyEMAS. This system allows the team to analyse all collected malware sample onto the Big Data platform. This will centralised the information which can be shared among malware researchers.

The chart below shows the reported Malaysia Botnet Drones and Malware Infection 2016:



	JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC	TOTAL
Botnet Drones Count by Unique IP	180894	192286	201281	176745	185467	171109	157850	172749	122859	120299	158292	186445	2026276
Malware Infections by Unique IP	136105	114793	112446	116097	124100	95781	78239	58460	78485	72492	71022	72036	1130056
TOTAL	316999	307079	313727	292842	309567	266890	236089	231209	201344	192791	229314	258481	3156332

Chart 1: Reported Malaysia Botnet Drones and Malware Infection 2016

2.6 Constituency

MyCERT's constituency is the Malaysia's Internet Users. 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 the 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.

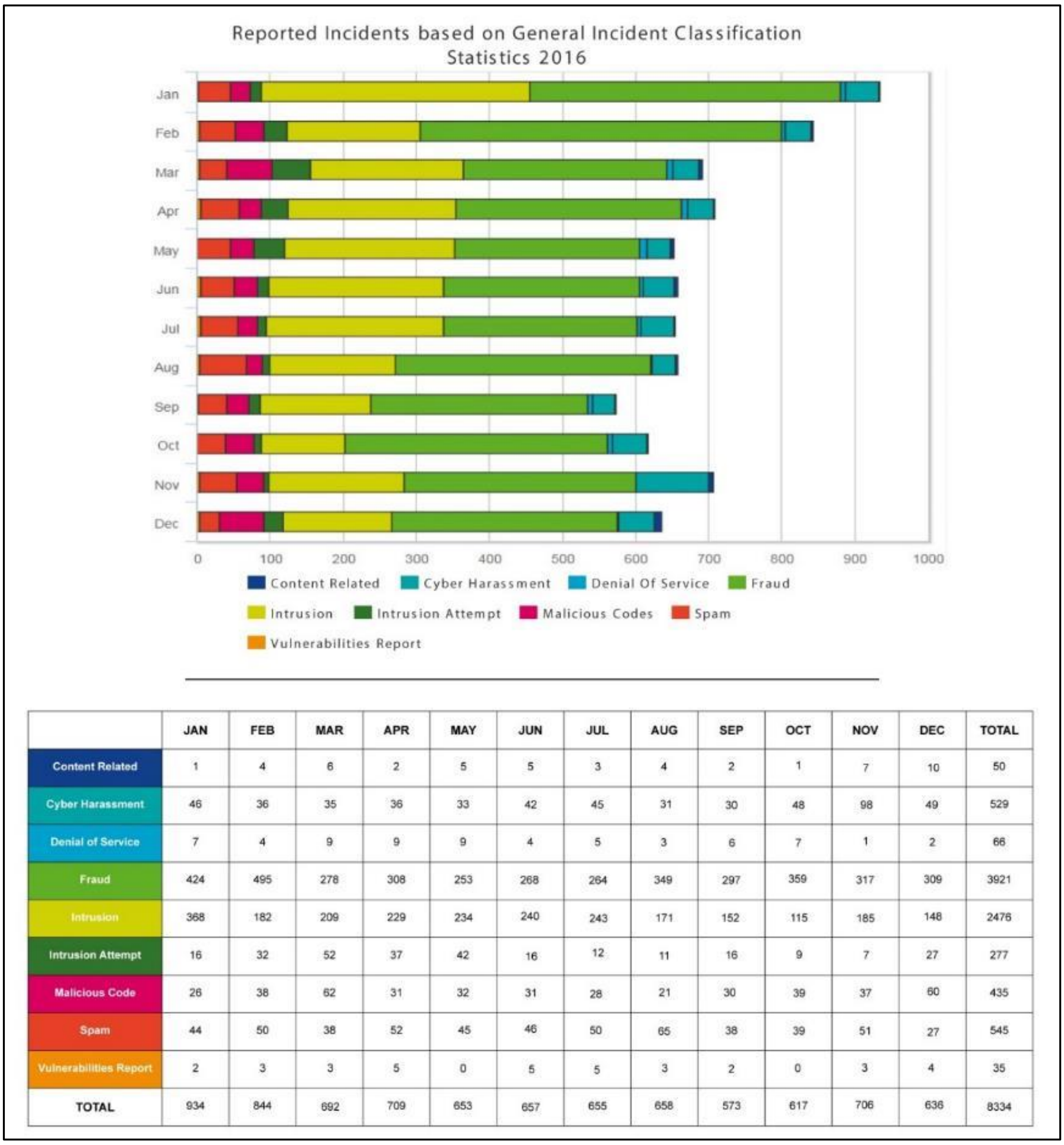
MyCERT in 2016 had proactively produced 77 advisories and 12 alerts to inform its constituency on issues relating to computer security. The specific list of the advisories, alerts and summary reports can be viewed at:

https://www.mycert.org.my/en/services/advisories/mycert/2016/main/index.html.

There was an increased in Intrusion incident in 2016 compared to 2015. Majority of the intrusions reported to MyCERT were related to web defacements, which were mainly due to unpatched servers and applications. This was followed by accounts being compromised mainly through social network accounts being hacked (Facebook, Instagram).

MyCERT also observed an increased in fraud incidents. Incidents that are commonly reported were related to phishing, online scam, impersonation, email spoofing, and counterfeit online transactions. Cyber harassment incidents also increased, especially in relation to Cyber Bullying (such as fake profile, cyber blackmail scam, and humiliation among others) and Cyber Stalking (such as threatening, slurs, and unsolicited sexual photos).

The following chart shows the reported incidents managed by MyCERT for 2016:



	JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC	TOTAL
Content Related	1	4	6	2	5	5	3	4	2	1	7	10	50
Cyber Harassment	46	36	35	36	33	42	45	31	30	48	98	49	529
Denial of Service	7	4	9	9	9	4	5	3	6	7	1	2	66
Fraud	424	495	278	308	253	268	264	349	297	359	317	309	3921
Intrusion	368	182	209	229	234	240	243	171	152	115	185	148	2476
Intrusion Attempt	16	32	52	37	42	16	12	11	16	9	7	27	277
Malicious Code	26	38	62	31	32	31	28	21	30	39	37	60	435
Spam	44	50	38	52	45	46	50	65	38	39	51	27	545
Vulnerabilities Report	2	3	3	5	0	5	5	3	2	0	3	4	35
TOTAL	934	844	692	709	653	657	655	658	573	617	706	636	8334

Chart 2: Reported Incidents Handled by MyCERT in 2016

Further information on Cyber999 statistics can be viewed at: https://www.mycert.org.my/statistics/2016.php.

4. EVENTS INVOLVEMENT AND ACHIEVEMENTS

MyCERT actively participated in IT security events such as trainings, seminars, conferences and meetings. MyCERT members have contributed their competencies in the following events:

4.1 Cyber Drills

As in previous years, MyCERT was immensely involved in co-organising an international drill called OIC-CERT Cyber Drill 2016. The objective of the drill is to test on the procedures and incident handling practices of participating organisations. There were 5 participating teams from 5 countries that took part in the cyber drill.

Apart from the OIC-CERT Cyber Drill, MyCERT had also participated in two cross-national Cyber Drills namely the APCERT Drill 2016 and ASEAN CERT Incident Drill (ACID) 2016.

4.2 Trainings

Several workshops or hands-on training were conducted by MyCERT in 2016 which included:

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

4.3 Presentations

MyCERT representatives had been invited to various talks at international conferences or seminars as speakers. The team had participated in the APCERT Malware Mitigation Working Group held during the 2016 APCERT AGM & Conference in Tokyo, Japan.

Other events that MyCERT participated were:

i. The Honeynet Project Annual Workshop 2016, San Antonio, Texas, USA.
ii. OIC-CERT AGM & Conference, OIC, Jeddah, Kingdom of Saudi Arabia.
iii. ASEAN Regional Forum (**ARF**) Conference, Kuala Lumpur Malaysia.
iv. Amsterdam 2016 FIRST Technical Colloquium, CISCO, Amsterdam.
v. China- ASEAN Network Security Emergency Response Capacity Building Seminar, Chengdu, China.
vi. IEEE Symposium on Computer Applications and Industrial Electronics, Penang Malaysia.
vii. NatCSIRT Meeting, Seoul, Korea.
viii. FIRST Technical Colloquium (TC), Bali, Indonesia.
ix. Critical Infrastructure Protection & Resilience ASIA, Bangkok, Thailand.
x. China-ASEAN Cyberspace Security Summit Forum, China.

xi. International Conference on CyberLaw, CyberCrime & CyberSecurity, New Delhi, India.

xii. 2nd International Conference on Electronic and Software Science 2016, Takamatsu, Japan

Apart from international security events, MyCERT personel have given presentations in more than 20 local events throughout 2016 as a part of MyCERT's contribution towards providing cyber security awareness at the national level.

4.4 Tools developed

In finding approaches to anticipate malware infection, MyCERT's MRC team continuously develops tools to support their research. The year 2016 saw the development of LebahNet 2.0 with the following features:

i. LebahPi - a lebahnet sensor based on Rasberry Pi that will support to capture threat information.

ii. Drown Checker Portal - a tool that assists the public user to identify the vulnerability of SSL Drown in their public server.

4.5 Paper Publication

MyCERT has published 17 international papers to be shared with the security community, which are:

i. *Observing the Presence of Mobile Malwares using Low-Interaction Honeypot*, 2016 IEEE Symposium on Computer Applications & Industrial Electronics. Published and indexed in IEEE Xplore: http://ieeexplore.ieee.org/document/7575048/

ii. *Exploitation of Android Mobile Malware in Phishing Modus Operandi: A Malaysia Case Study, The Second International Conference on Electronics and Software Science 2016.* Published and indexed in ResearchBib: http://paper.researchbib.com/?action=viewList&isbn=978-1-941968-40-6&pid=58

iii. *Elements in the Cyber Security Framework for Protecting the Critical Information Infrastructure Against Cyber Threats.* Published in Information-iii: http://www.information-iii.org/abs_e2.html#No7(A)-2016

iv. *Strengthening User Authentication for Better Protection of Mobile Application Systems.* Published in Jatit:

http://www.jatit.org/volumes/Vol85No3/17Vol85No3.pdf

v. *Securing Sensor to Cloud Ecosystem Using Internet of Things (IoT) Security Framework.* Published in ACM: http://dl.acm.org/citation.cfm?id=2896387

vi. *Test Input Generation for Detecting SQL Injection Vulnerability in Web Application.* Published in Medwelljournals: https://www.medwelljournals.com/archivedetails.php?jid=1816-9503&issueno=54

vii. *Mapping 2D to 3D Forensic Facial Recognition via Bio-Inspired Active Appearance Model.* Published in Jurnalteknologi: http://www.jurnalteknologi.utm.my/index.php/jurnalteknologi/article/view/6939

viii. *Development of Cyber Security Awareness Strategy Using Focus Group Discussion.* Published in IEEEXPLORE: http://ieeexplore.ieee.org/document/7556109/

ix. *Enhanced Affixation Word Stemmer with Stemming Error Reducer to Solve Affixation Stemming Errors.* Published in UTM: http://journal.utem.edu.my/index.php/jtec/issue/view/98

x. *CSM S-Box Evaluation Tool (CSET): Tool to Evaluate the Strength of an S-Box.* Published in Institute for Mathematical Research: http://www.mscr.org.my/V6%281%29/IJCR_6%281%29_47-63.pdf

xi. *Malay Word Stemmer to Stem Standard and Slang Word Patterns on Social Media.* Published in Springer: http://hepd.pnpi.spb.ru/CSD/CSDPublications/LNCS9714.pdf

xii. *Rules and Results for SSL/TLS Nonintrusive Proxy Based on JSON Data.* Published in IEEEXPLORE: http://ieeexplore.ieee.org/document/7740366/

xiii. *Word Stemming Challenges in Malay Texts: A Literature Review.* Published in IEEEXPLORE: http://ieeexplore.ieee.org/document/7571887/

xiv. *CyberSecurity Malaysia: Towards Becoming a National Certification Body for Information Security Management Systems Internal Auditors.* Published in World Academy of Science, Engineering and Technology: http://waset.org/publications/10005256/cybersecurity-malaysia-towards-becoming-a-national-certification-body-for-information-security-management-systems-internal-auditors

xv. *Forensics Readiness: A Case Study on Digital CCTV Systems Antiforensics.* Published in Syngress: https://www.safaribooksonline.com/library/view/contemporary-digital-forensic/9780128054482/B9780128053034000101.xhtml

xvi. *On the Reproducibility and Repeatability of Likelihood Ratio in Forensics: A Case Study Using Face Biometrics.* Published in University of Surrey: http://personal.ee.surrey.ac.uk/Personal/Norman.Poh/data/norman_BTAS2016_LLRconf.pdf

xvii. *Research Framework for SCADA Center of Excellence (COE).* Published in IJCIT : http://www.ijcit.com/index.php

4.6 Social Media

In 2016, MyCERT personnels were invited continuously to speak with regards to Internet security issues at the local radio and television stations. MyCERT also actively disseminate security concerns through social media such as Facebook and twitter. As of now, MyCERT Facebook Page has about 1,986 likes and MyCERT Twitter has 1,212 followers.

5. INTERNATIONAL COLLABORATION

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

5.1 Working 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. Global Cyber Security Capacity Centre (**GCSCC**), Oxford Martin School, University of Oxford;

ii. Academy of Informational Systems (AIS), The Russian Federation;

iii. The Ministry of Interior, Republic of Korea;

iv. Korea Internet & Security Agency (KISA), Republic of Korea;

v. Defense Space Agency (DSA), Nigeria; and

vi. National Cyber Security Agency (NCSA), United Kingdom.

5.2 Memorandum of Understanding (MoU)

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

i. Information Technology Promotion Agency, Japan;
ii. National Agency for Computer Security (**NACS**), Republic of Tunisia;
iii. National Computer Network Emergency Response Technical Team Coordination Centre of China (**CNCERT/CC**), China;
iv. CERT Australia, Australia;
v. Wing Marketing & Trading Co. Ltd., Hong Kong;
vi. King Saud University, Saudi Arabia;
vii. Traffic Observation and Management Ltd, Ireland;
viii. Decision Group Inc., Singapore;
ix. Military College of Signals – National University of Science & Technology (**MCS-NUST**), Rawalpindi, Pakistan;
x. Indonesia Security Incident Response Team on Internet Infrastructure/ Coordination Centre (**ID-SIRTII/CC**), Indonesia;
xi. State Technical Service Republican Enterprise founded on the right of economic competence of the Agency of the Republic of Kazakhstan on Communication and Information, Kazakhstan;
xii. Direction Generale de la Securite des Systemes d'information "DGSSI", Morocco;
xiii. Alliacom, France;
xiv. IT Protective Security Services Sdn. Bhd. (**ITPSS**), Brunei;
xv. Thailand Computer Emergency Response Team (**ThaiCERT**), Thailand;
xvi. The Indian Computer Emergency Response Team (**CERT-In**), the Republic of India;
xvii. Academy of Informational Systems, Russia;
xviii. Korea Internet & Security Agency of the Republic Of Korea; and
xix. Cybercrime Investigation and Coordinating Centre, Department of Information and Communications Technology, Republic of the Philippines.

5.3 New Partnerships and Existing Cooperation

Amongst the potential partnership and existing cooperation in the area of cyber security 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; and

ii. The Convenor for the APCERT Malware Mitigation Working Group – MyCERT has been given the thrust by the APCERT members to lead the WG in 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 report or data on malware attacks and focus on the impact analysis and remedial action.

6. FUTURE PLANS

Since the establishment of CyberSecurity Malaysia, MyCERT as a department in particular, 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 information 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 information 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 computer 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 2015 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 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.

NCSC

New Zealand National Cyber Security Centre – New Zealand

1. About the New Zealand National Cyber Security Centre (NCSC)

1.1 Introduction

The New Zealand National Cyber Security Centre (NCSC) provides enhanced services to government agencies and critical infrastructure providers to assist them to defend against cyber-borne threats. The Centre was a key element of the New Zealand Cyber Security Strategy that was released in December 2015.

The NCSC is hosted within the GCSB which has a legislative mandate (Section 8A of the Government Communications Security Bureau Act 2003) to ensure the protection, security, and integrity of communications, and information infrastructures of importance to the Government of New Zealand; and to do everything that is necessary or desirable to protect the security and integrity of the communications and information infrastructures including identifying and responding to threats or potential threats to those communications and information infrastructures.

GCSB also has functions and powers under the network security provisions of part three of the Telecommunications Interception Capability and Security Act (TICSA) to assess proposed changes to telecommunications networks for potential risks to national security.

The core NCSC cyber mission is ensuring New Zealand's most important information systems are impenetrable to cyber-borne threats. We achieve this by working closely with a wide range of organisations of national significance – e.g. to government departments, key economic generators, niche exporters, research institutions and operators of critical national infrastructure.

NCSC assists these entities protect their own networks from the types of threats which are typically beyond the capability of commercially available tools. In addition to this cyber security role we also provide a range of information assurance services and security guidance as part of suite of government protective security requirements framework. This work is undertaken collaboratively across government and the security sector, to develop and promote information security standards.

1.1.1 Establishment

The NCSC was formally established in June 2011 and became operational in September

2011. The NCSC's responsibilities include:

- Incident coordination and response for our customers;
- Engagement with public and private sector customers to develop and improve awareness of cyber security threats;
- The provision of national information assurance guidelines through the New Zealand Information Security Manual (NZISM);
- Administering the network security provisions of the Telecommunications Intercept Capability and Security Act (TICSA);
- Liaison with the international community and global partners to promote greater cooperation around cyber security; and
- Work in coordination with other organisations acting in the domestic cyber security space (e.g. the soon to be established CERT New Zealand, Connect Smart www.connectsmart.govt.nz, New Zealand Police, the department of Internal Affairs, New Zealand Internet Task Force, Netsafe etc)

1.1.2 Workforce

The NCSC comprises of a skilled team of cyber security professionals with technical, policy and incident coordination backgrounds. Over the 2015-16 year the NCSC has continued to grow its capacity and capability in a number of areas, including within the engagement area and with its policy support to wider Government initiatives with an information security element.

1.1.3 NCSC Customers

The NCSC's customers are drawn from a broad cross section of significant New Zealand organisations. Sectors represented include government departments, key economic generators, niche exporters, research institutions and operators of critical national infrastructure.

2.

2.1 Incident handling reports

The National Cyber Security Centre (NCSC) recorded 338 cyber incidents in the year from June 2015 to June 2016, compared with 190 in the previous year, the nature of the threats are becoming more complex and the sources of them more diverse.

There is a growing range of international threat actors, targeting New Zealand organisations for financial gain or as a means of advancing their own position.

NCSC assesses that New Zealand organisations, both public and private, have information which is attractive to others - whether intellectual property for a new technology innovation, customer data, business and strategies or government positions. In part the increase in recorded incidents reflects increased detection of threat activity by our cyber defensive capabilities. NCSC expects that this trend will continue as we develop our relationships with our customers and make our cyber defensive capabilities available to them.

2.2 Additional activities

In addition to receiving incident reports, the NCSC:

- Issued cyber threat and incident advisories to customer and partners.
- Facilitates Security Information Exchanges (SIE) to critical infrastructure sector based groups including Government, Control Systems, University's, Networks, Finance, and Crown Research industries. Typically each SIE meets 3-4 times a year.
- Regulatory Authority for the Telecommunications Interception Capability Security Act.
- Coordinated and hosted industry engagement forums.
- Provides cyber briefings to key organisations, sector groups, information security forums and industry.

2.3 Project CORTEX

As part of the NCSC's cyber security function work is undertaken across government and the private sector to implement capabilities (CORTEX) to protect nationally significant organisations from advanced cyber threats and to deny cyber threat actors the ability to effect New Zealand's national security.

CORTEX focuses on countering advanced malware that is typically beyond the defensive capabilities of commercially available tools.

It helps protect against theft of intellectual property, loss of customer data, destruction or dissemination of private communications, holding data for 'ransom' and damage to IT networks and services.

3.

3.1 International Collaboration

The NCSC has undertaken a review of its international engagement arrangements with the establishment of CERT NZ. Notably, CERT NZ will take the lead role in representing New Zealand within the ACERT network. CERT NZ is expected to formally take up the representative role once it is operational in April 2017.

3.1.1 Future International Collaboration

New Zealand Government agencies are working together to determine where New Zealand can best contribute to international networks and with the likes of regional capacity building.

3.2 Industry Engagement

The NCSC continues to coordinate and organise a range of industry and government forums throughout the last year. There have also been a number of board level presentations to a number of industries to raise security awareness of risks and to encourage best practice.

3.3 The New Zealand Information Security Manual (NZISM)

The NCSC has released several new versions of the NZISM following ongoing:

- identification of emerging areas of risk;
- Significant research and development
- Consultation with NCSC customers

Work continues to better integrate the NZISM with the Protective Security Requirements (PSR), which is a framework outlining the Government's expectations for managing personnel, physical and information security. The PSR assists government agencies to manage business risks and assure continuity of service delivery.

4. Presentations/conferences

The NCSC is hosting the MNSIE conference in New Zealand in 2017 and intends to attend the ACSC conference in Australia in 2017.

4.1 Publications

The NCSC continues to publish a number of security alerts and advisories via its website and through direct exchanges with customers and partners where appropriate. The NCSC cyber threat report for the period June 2015 to June 2016 is also due to be released soon.

5. Future projects

- Development of a close working relationship with CERT NZ from its launch in 2017.
- Development of sector specific exercises

6. Establishment of CERT NZ

The New Zealand Government is in the process of establishing CERT New Zealand, which is due to be stood up in April 2017. CERT NZ will help ensure New Zealanders and organisations across the broad spectrum of the New Zealand economy are able to access information and advice to assist prevent and mitigate cyber threats.

While CERT NZ will have primary responsibility for general cyber threat reporting and response, the NCSC will continue to play a key role in response to significant cyber events, particularly those which may impact on nationally significant systems and information. CERT NZ will pick up responsibility for liaising with the APCERT network.

7. Conclusion

The NCSC has continued to build its expertise and capability to support and protect New Zealand's critical national infrastructure from the public and private sectors from cyber threats. Relationships with these customers are becoming increasingly productive as NCSC's aperture increases, our consequential understanding of the threats increases, and NCSC calibrates its support to meet customer needs.

The development of CERT NZ presents as an exciting chapter in the New Zealand response to cyber security threats as it will enable a more comprehensive response to the range of threats. NCSC will continue to support New Zealand involvement and cooperation with international networks such as APCERT, through CERT NZ and wish all APCERT members well.

SingCERT

Singapore Computer Emergency Response Team - Singapore

1. Highlights of 2016

1.1 Summary of major activities

1.1.1

A Partnership was forged with CyberGreen Institute for the Cyber Security Agency of Singapore (CSA) to be the cornerstone sponsor for the CyberGreen Initiative. Under CSA, SingCERT works closely with CyberGreen to enhance the development of a risk-based common metrics for assessing cyber risks and vulnerable servers across the world's networks. This is part of the larger effort to make the cyberspace clean and resilient to cyber-attacks.

1.1.2

The 11th ASEAN Cyber Incident Drill (ACID) was successfully conducted on 27 September 2016, with participants from the ASEAN member states and their dialogue partners providing positive feedback on the conduct of the annual drill.

1.2 Achievements & milestones

1.2.1

Participated in the AP-CERT Pre-Drill Comms Test and actual AP-CERT Drill on 16 March 2016.

1.2.2

Attended the AP-CERT Annual General Meeting (AGM) and Conference in Tokyo from 24 to 27 October 2016 and also presented SingCERT's perspective on its use case on the CyberGreen initiative during the CyberGreen Workshop.

2. About SingCERT

2.1 Introduction

The Singapore Computer Emergency Response Team (SingCERT) serves as a one-stop for cybersecurity incident response in Singapore. Besides providing assistance to its constituency in incident resolution and coordination, SingCERT also broadcast specific threat advisories through its website (https://www.csa.gov.sg/singcert) and promotes cyber hygiene best practices through various initiatives such as GoSafeOnline (https://www.csa.gov.sg/gosafeonline).

2.2 Establishment

SingCERT was set up in 1997 and came under the ambit of the Cyber Security Agency of Singapore (CSA) when it was formed on 1 April 2015. It aims to facilitate the detection, resolution and prevention of cybersecurity-related incidents within the Singapore cyberspace.

2.3 Resources

Specific threat alerts and advisories that affects the constituency will be released on the SingCERT website.

2.4 Constituency

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

3. Activities & Operations

3.1 Scope and definitions

SingCERT's focus is on providing technical assistance and coordinating responses to cybersecurity-related incidents affecting our constituency, as well as on collaborations with other foreign CERT partners in handling cross-border cybersecurity-related incidents.

3.2 Incident handling reports

SingCERT receives incident reports from the constituency via email and phone, and will assess and follow up with the respective agency or service provider to coordinate and carry out further remediation.

3.3 Abuse statistics

In 2016, SingCERT received a significant increase in the number of ransomware reports as compared to the previous year. The ransomware attacks illustrated a new attack vector to hold victims to ransom by encrypting their files

3.4 Publications – SingCERT Advisories (Details available on SingCERT website)

- Gooligan Malware on 1 Dec 2016
- Tech Support Scam on 17 Nov 2016
- Enhancing the Security of Internet-Connected Devices on 26 October 2016
- Shadow Brokers Leaked Tools targeting Popular Network Devices on 1 September 2016
- Kaspersky Report on Compromised RDP Servers – "The xDedic Marketplace" on 18 June 2016
- Unsecured Virtual Network Computing (VNC) Configurations on 23 May 2016
- Software Vulnerability in Symantec's Antivirus Engine on 19 May 2016
- Ransomware on 6 may 2016
- Software Vulnerability Discovered by CISCO in their ASA Software on 11 February 2016

4. Events organized / hosted

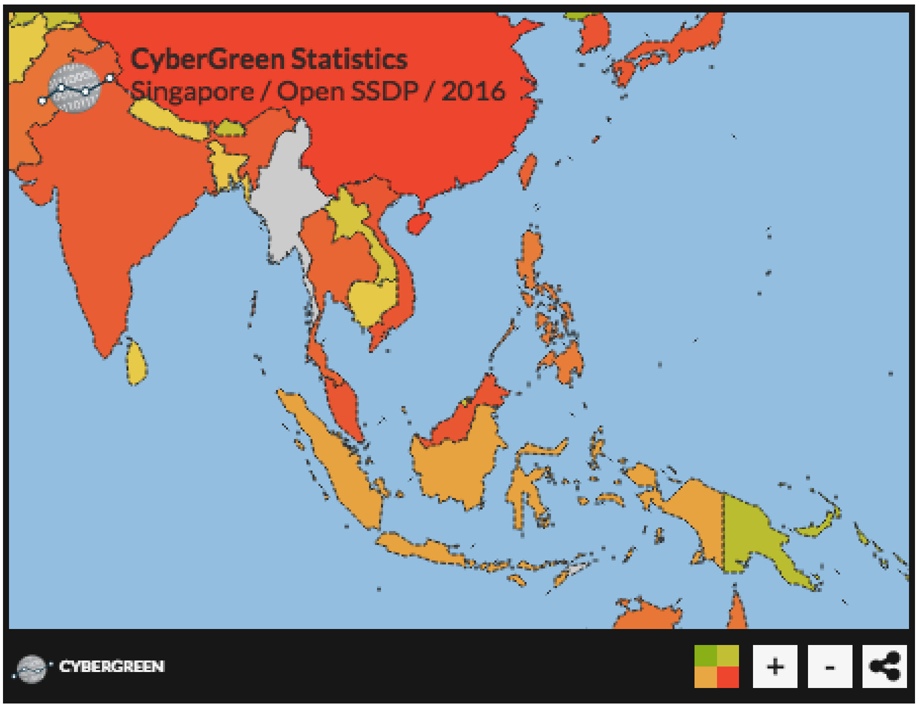
4.1 Drills & exercises

SingCERT conducted the 11th ASEAN Cyber Incident Drill (ACID) 2016 on 27 September 2016.

5. International Collaboration

5.1 International partnerships and agreements

CSA/SingCERT signed up a collaboration agreement with CyberGreen as one of its cornerstone sponsor on 10 October 2016. As part of this collaboration, a CyberGreen ASEAN Portal was also launched during the Singapore International Cyber Week (SICW) as an online platform to provide ASEAN Member States a regional view on the cyber health state and the necessary resources needed to enhance regional remediation efforts collectively.



CyberGreen ASEAN Regional View

5.2 Capacity building

5.2.1 Training

SingCERT participated and benefited from the following APCERT Training topics that were arranged by TWCERT:

a. "Internet of Things (IoT) Trend" that was presented by ID-SIRTII/CC on 6 April 2016.

b. "How to Help Organisations Conduct Effective Exercises" that was presented by Dell SecureWorks on 1 June 2016.

c. "Tactical Against Malicious Scanning Network" that was presented by HKCERT on 3 August 2016.

d. "The Growing Threat of Ransomware in Malaysia" that was presented by MyCERT on 5 October 2016.

e. "How Microsoft Safeguards Your Data in the Cloud" that was presented by Microsoft Corporation on 7 December 2016.

5.2.2 Drills & exercises

The 11th ASEAN Cyber Incident Drill (ACID) 2016 was conducted successfully with participants benefitting from the drill on 27 September 2016. The theme "Ransomware and Cyber Forensics" was selected as ransomware was the prevailing cyber threat and emerged as a new attack vector affecting many constituencies globally. A total of 15 CERTs from 10 ASEAN Member States and ASEAN Dialogue Partners attended the Drill.

6. Future Plans

6.1 Future projects

SingCERT will be organising the 12th ACID in September 2017. Planning and discussion are in progress to determine the theme, scope and details.

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 focal point for cyber security for the nation. It is the single trusted source of advice for 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 July 2006 as Sri Lanka's National CERT, by the ICT Agency of Sri Lanka (ICTA). ICTA is the Government Agency responsible for the development of IT Infrastructure and Policy in Sri Lanka. Sri Lanka CERT is registered as a Private Limited Liability Company, and is a fully owned subsidiary of ICTA, which in turn is fully owned by the Government of Sri Lanka.

Sri Lanka CERT|CC is presently under the purview of Ministry of Telecommunications and Digital Infrastructure and is fully financed by the state budget.

1.3 Workforce

The Sri Lanka CERT|CC has a total staff strength of fifteen team members consisting of Chief Executive Officer, Manager Operations, Principal Information Security Engineer, Senior Information Security Engineer, Research and Policy Development Specialist, Associate Information Security Engineer, four Information Security Analysts, Associate Information Security Analyst and an officer in charge of HR and Administrative work. This team is supported by three 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 whole of the 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 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

As the national point of contact for matters relating to cyber security incidents, Sri Lanka CERT|CC receives numerous reports from domestic and/or international partners about various cyber security incidents/vulnerabilities that affected/may affect our national cyber-space. Following are some of the different types of incidents reported during 2016 (1st of January – 31st of December);

- Ransomware and financial frauds
- Scams
- Malicious software
- Compromised unique IP’s extracted from the information collected by automated systems
- Vulnerabilities on applications, operating systems and firmware etc.
- Phishing incidents and various other scams associated with this
- Content related matters such as privacy violations

- Cyber-attacks on various systems and applications

This annual report analyzes the cyber security incident information collected / managed by Sri Lanka CERT|CC in 2016, in order to obtain an overall view of the nature and dynamics of these types of events relevant to the evaluation of the risks targeting the ICT systems in Sri Lanka.

Based on the collected data, the following have been observed;

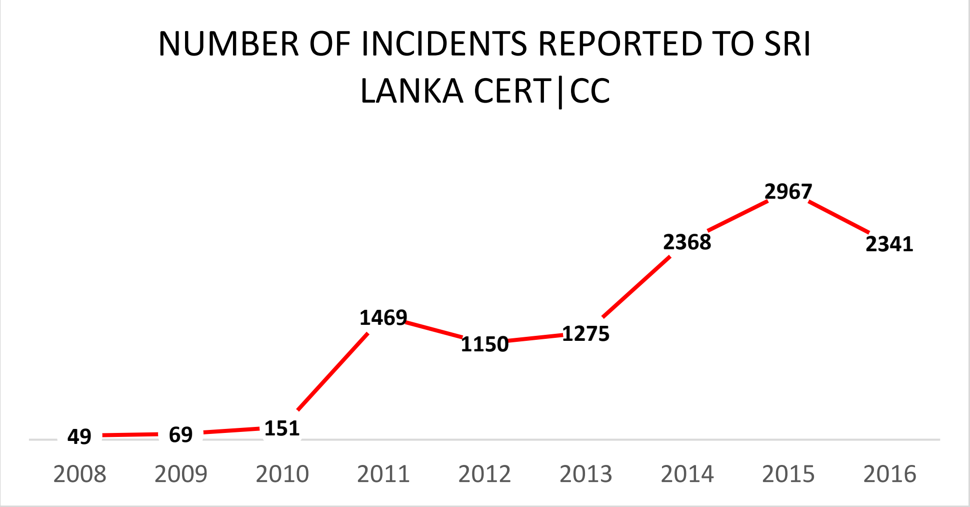
- Financial frauds targeting local importers/exporters are increasing
- There has been an increase in the spread of ransomware during the year, where sensitive data belonging to both individuals as well as corporate businesses have been made unavailable by encrypting data in those computers.
- There is an increase in the phishing attacks targeting financial sector organizations including banks
- The number of social media related incidents have decreased during the year compared to the previous year
- There is an increase in the Internet abusing cases reported to Sri Lanka CERT

The above findings lead to the following conclusions:

- Cyber criminals are changing their strategies in order to obtain more financial gains
- The need to educate the general public on ethical use of the Internet is more apparent in order to benefit the society as a whole
- Cyber security has to be recognized as an integral part of every citizen and each and every citizen has a responsibility to contribute to ensuring a secure online environment.
- Making the general public, private and public sector organizations aware about various types of cyber threats is a vital part of ensuring that people will gain the true benefits of the Internet rather than be a victim in the cyber world.

2.2 Incident Handling Statistics

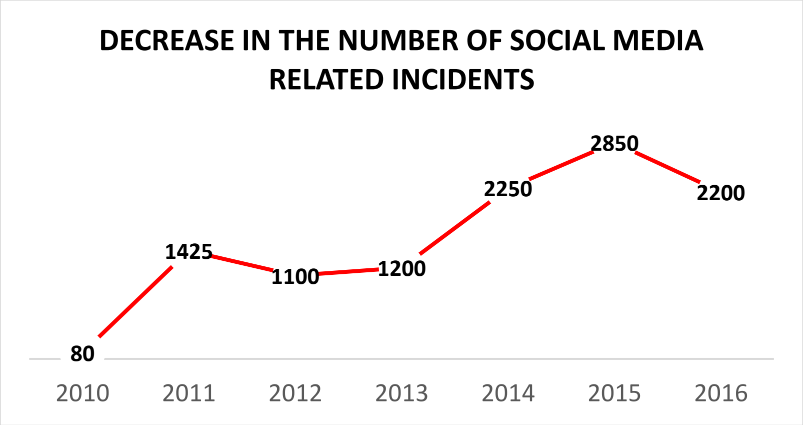
Incidents reported to Sri Lanka CERT have decreased in the year 2016 compared to the previous year. In 2016 2,341 incidents were reported while it was 2,967 in the year 2015. This represents a 20% decrease in reported incidents compared to the year 2015.



Graph 1: Total number of reported incidents

It was observed that the number of reported cases related to social media have also decreased considerably in the year 2016.

The reason for this may be the result of extensive capacity building activities that have been undertaken by Sri Lanka CERT in recent years, through the establishment of the Cyber Crime Division of the Sri Lanka Police as well as the establishment of sector based CSIRTs. In addition to this, Sri Lanka CERT was able to train and establish an incident response team at the National Child Protection Authority (under the Ministry of Women & Children's Affairs). Hence the reported incidents may have been distributed among such establishments, and these statistics are not available with us at this present moment.

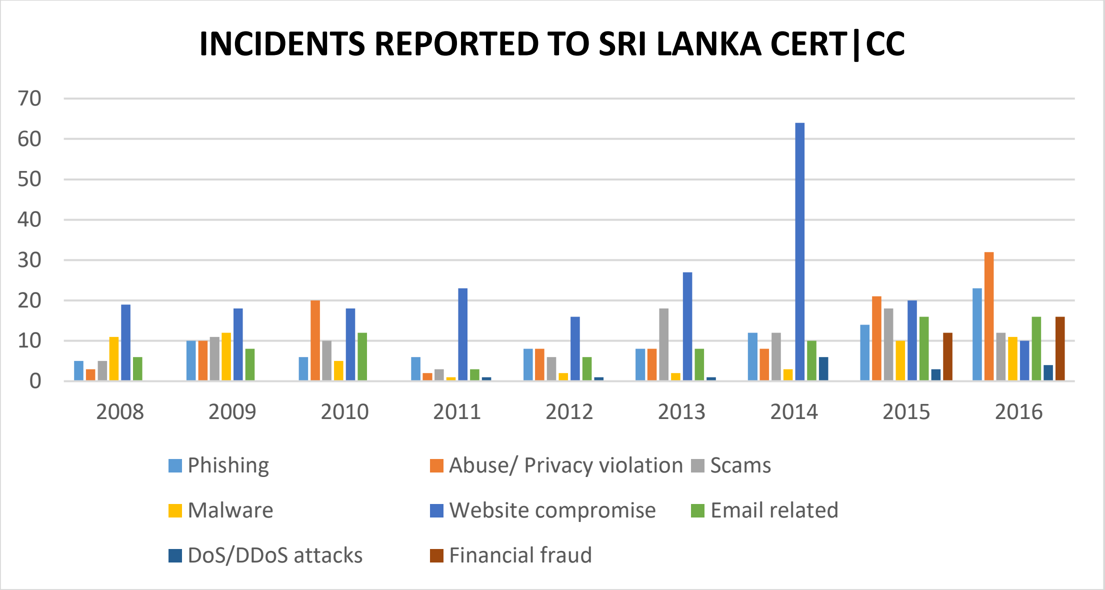


Graph 2: Total number of social media related incidents

The following table depicts the distribution of various types of incidents reported to Sri Lanka CERT during 2016. All the incidents reported to Sri Lanka CERT have been resolved satisfactorily.

Type of Incident	Year 2016
Phishing	23
Abuse/Hate/Privacy violation (via mail)	32
Ransomware	10
Scams	12
Financial Frauds	16
Malicious Software issues	11
Web site Compromise	10
Compromised/hate/threat Email	16
Intellectual property violation	7
DoS/DDoS	4
Social Media related incidents	2200
Total	**2341**

Table 1: Number of reported incidents in year 2016



Graph3: Types of incidents reported to Sri Lanka CERT|CC from 2008- 2016

From Graph 3 it is evident that ransomware attacks and financial frauds are on the increase.

2.3 Consultancy services

Sri Lanka CERT|CC continues to provide consultancy services in response to requests made, particularly by government departments.

Typical consultancy services provided during the year 2016 include;

- Representing Technical Evaluation Committees (TEC's) for both Government and other State Owned Enterprises (SOE's) in order to assist them to procure information security solutions/systems.
- Application security and server hardening for a number of government and private sector organizations.
- Application and network security vulnerability assessments for e-Government applications.
- Carrying out technical forensic investigations for the Criminal Investigations Division (CID) of Sri Lanka Police;
    - Credit Card fraud investigations prosecuted under the Payment Devices Frauds Act, 2006, where Sri Lanka CERT serves on the panel of experts through a special gazette notification.
    - Investigating ATM and Credit Card skimming cases.

  - Investigation of Money Laundering cases.
- Carrying out technical forensic investigations for Private sector organizations.
- Assisting several government organizations and private sector organizations to develop an Information Security Policy for their organizations.
- Assisting government and private sector institutions to secure their operational environment and secure their applications by performing information security policy formulation workshops, network architecture reviews, consulting on secure network and system design and system hardening.

2.4 Training / Education services

In order to fulfil its mandate to create awareness and build information security skills within the constituency; Sri Lanka CERT|CC continues to conduct and facilitate training programs and education sessions targeting various audiences. This includes CIOs, Engineers, System Administrators, Banking and Telecom Sector Staff, Lawyers, Judges, Attorney Generals Department staff, Students, and the General Public.

During the year 2016 Sri Lanka CERT|CC conducted a number of awareness, training and education programs successfully which includes;

- Presentations at SLIDA for government officers (5 Nos)
- Presentations at Bar Association (3 Nos)
- Training programs for the National Police Academy (6 Nos)
- Presentation for the Tri-forces legal officers at the Air Force Headquarters
- Presentation at TRC for Police Officers (4 Nos)
- One day workshop for CID officers
- Awareness programs at SOS Villages covering all locations in the country i.e Piliyandala, Galle, Jaffna, Monaragala, Nuwaraeliya and Anuradhapura
- Awareness programs at Youn Puraya Event (Sigiriya)- ICTA stall (3 days)
- Organising a Software Development Security & CSSLP Certification Awareness Session
- Organising Awareness Sessions on Mobile Technology and Investigations for Judges and Police officers
- Infotel 2016 (provided a Sri Lanka CERT stall for 3 days)
- Presentation on How Internet Turned Against Women - University of Kelaniya
- Internet Safety Awareness- NCC/Emmanuel Memorial Church

- Leadership Training programme for adolescents on prevention of drug abuse and cyber related Crimes- Church of Ceylon Youth Movement, Colombo North Area
- Leadership Training programme for adolescents on prevention of drug abuse and cyber related Crimes- Church of Ceylon Youth Movement, Colombo North Area
- Presentation on 'Challenges & Opportunities in Social Commerce at (ISC)2 Colombo Chapter Monthly meeting
- Presentation at Safer Internet day conference highlighting safer Internet usage for Children
- Wireshark workshop for law enforcement officers
- Awareness Programme on Information Security for Government Organization CIO's

Electronic/Print Media

- Hiru TV cybercrime program contributed to 50 episodes
- Derana TV 24x7 Biz News (1 hr program)
- RanOne FM Live radio program on Safe use of mobile phones
- Regular newspaper articles related to Cyber Security and Cyber Crime
- Announcement of security alerts on Print Media as well as Radio and TV

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 judiciary during the year 2016 and will continue for the next year as well.

2.5 Publications

Website

The Sri Lanka CERT|CC website publishes security related awareness bulletins for the public via News Alerts and a Knowledge Base. Glossaries, Case Studies, Statistics and FAQs are among some of the other published items.

E-mails

Sri Lanka CERT disseminates security related information via e-mail alerts to its subscribers. Similarly, the Cyber Guardian e-newsletter that was initiated in mid-2010 is distributed to a large number of students by the Ministry of Education, 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

Sri Lanka CERT continues to maintain a sensor for the JPCERT/CC hosted TSUBAME Internet Scan Data Acquisition System project.

3. Events organized / co-organized

3.1 Seminars & Workshops

- Cyber Security Week 2016

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 2016 was held in the month of November 2016, and featured a series of events including the following;

- Annual National Conference on Cyber Security 2016.
- Three full-day Workshops for professionals, namely:

    - Technical workshop on “Practical Network Security and Incident Response”
    - Technical workshop on “Penetration Testing-Hands on”
    - Technical workshop on “Cyber Security for Corporate Executives”

- 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.

- Information 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.

All of these events were well attended and the feedbacks received were very positive.

- APNIC 42
  - Sri Lanka CERT was the local host for this international conference
  - According to the APNIC post-conference report it was one of the most successful conferences to date, attracting 332 delegates from 39 economies, representing 133 Member organizations.
  - Sri Lanka CERT staff also presented during the conference (2 presentations)

Organized a FIRST Technical Colloquium for the first time in Sri Lanka along with APNIC 42

4. Achievements

4.1 National Cyber security strategy

Sri Lanka CERT|CC commenced work on the first draft of the national cyber security strategy for Sri Lanka during the year 2016. Stakeholder consultations have been initiated in order to discuss this in detail with the relevant stakeholders during the year 2017 before finalising it. Expecting to complete this and have it adapted during the year 2017.

4.2 RESEARCH AND POLICY DEVELOPMENT

The initiation of the research arm of Sri Lanka CERT will add more value to our services in the future. This team was able to conduct several research activities during the year 2016 which helped us to understand the current cyber security posture in Sri Lanka.

4.3 Certification & Membership

Sri Lanka CERT continues to enjoy the benefits of membership to the following professional security organizations;

a. Microsoft SCP (Security Cooperation Program).
b. Collaborative agreement with ITU Subsidiary "IMPACT", where Sri Lanka CERT benefits from receiving threat intelligence from the region and is also part of the global incident response teams.
c. International Information Systems Security Certification Consortium, Inc., (ISC)².
d. Threat Intelligence from ShadowServer.

5. New services

5.1 Setting up sector based CSIRTs

Sri Lanka CERT|CC initiated the setting up of sector-based Computer Security Incident Response Teams (CSIRTs) in 2010. Typical sectors are Banking, Telecom, Defence and Education.

The rationale for sector based CSIRT's is to ensure that Sri Lanka CERT|CC remains a small, focused national body that functions only as an incident escalation and coordination point and ensures national readiness to tackle large scale incidents effectively.

FINCSIRT

Bank CSIRT continued to be in operation during the year 2016 and has successfully resolved a number of security incidents reported by its members during the year. Bank CSIRTs core objectives however remained the same i.e. sharing threat intelligence anonymously using an information sharing platform, and adhering to a baseline information security standard based on ISO 2700. Accordingly, Bank CSIRT continues to protect its constituency from various security threats by taking proactive measures. In addition to its initial services, Bank CSIRT introduced a basic Security Operations Centre (SOC) as an additional paid service to the member banks during the year 2015, which has now expanded its services to other member banks during the year 2016.

The Bank CSIRT expanded its role in the year 2016 to cover whole financial sector organizations and was renamed as FINCSIRT.

Edu-CSIRT

Sector based CSIRT for the educational sector was established in collaboration with Ministry of Education. A handbook was developed for training the teachers and have conducted several training programs for the IT teachers during the year 2016. During 2016 Edu-CSIRT was able to train 100 teachers from all parts of the country and they expect to continue with this program to reach up to 1,000 teachers. They will convey the information security and the safe use of the Internet messages back to the school environment. In the event of an incident Edu-CSIRT will be the first responder and they are sufficiently competent to handle it.

5.2 National Certification Authority

The Electronic Transactions Act no. 19 of 2006 creates a foundation for the existence of a national certificate authority. ICTA has been designated as the National Certification Authority.

As a fully own subsidiary of ICTA, Sri Lanka CERT|CC was designated to function as the implementation body for the National Certificate Authority (NCA) of Sri Lanka. The process of setting up the NCA using the provisions granted under the above Act is on-going.

Sri Lanka CERT|CC has completed most of the hardware and software procurements and configurations.

Since there were implementation delays due to unexpected procurements, NCA is expected to start the operations during the year 2017.

6. International Collaboration

6.1 Event participation

- "Underground Economy" conference in Doha, Qatar
- AusCERT conference in Gold Coast, Australia
  - Delivered a presentation on "The psychological impact of Online versus offline victimization and victim support "
- Participated at the FIRST AGM and conference in Seoul, South Korea.
  - Contributed for the FIRST cyber security training materials
  - Chaired a session in the main conference having three speakers from NCSC-FI, USCERT, JPCERT|CC

- Participated at the NatCSIRT meeting which discuss issues related to National CERTs
- Delivered a presentation at the NatCSIRT meeting on "Role of National CSIRTs for bridging the gap"
- Chaired a session at the NatCSIRT meeting having three speakers from NISC (Japan), NCSC (Netherlands), CERT.LV (Latvia)
- Moderated a panel discussion at the NatCSIRT meeting

- Participated at the APCERT conference in Tokyo, Japan
  - Delivered a presentation on "Human Centered IT Security Research for a Cleaner and Greener Cyber Space "
  - Contributed for the working group activities
- Cybersecurity Alliance for Mutual Progress (CAMP) training and inauguration meeting in South Korea

6.2 Other activities

- Continuing with network monitoring project "Tsubame" with JPCERT|CC
- Contributed for Internet Governance Forum (IGF) activities
- Submitted news article for APNIC blog
- Trained 5 members of BtCIRT (Bhutan) staff in Sri Lanka
- Visited Bangladesh eGOV CIRT and provided the sponsor report to APCERT

6.3 International incident coordination

- Reporting of malicious IP address details received from International security organizations/CERTs to Local ISPs
- APCERT Cyber Security Drill
  - Worked as a member of the organizing committee of APCERT Cyber Security Drill 2016
  - There were 8 teams from 7 countries in the organizing committee.
  - Participated as a drill player and exercise controller
  - 26 CSIRT teams from 20 economies participated for the drill.
- In addition to the 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

The following projects are either in the conceptual stage or just being initiated, and are intended to serve the constituency directly;

Development of National Cyber Security strategy (Ongoing).

Development and Implementation of a Security Operations Centre (On-going).

Establishment of the National Certification Authority (ongoing).

Establishment of sector based CSIRT's.

Cyber Security Week 2017.

8. Framework

8.1 Future Operations

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

Continue to recruit undergraduate placement students on internships on an annual basis to enhance the information security capabilities of the younger generation.

Continue to operate as a small focused group of professionals, but building sufficient skills nationally to combat and prevent cyber-crime.

Keep the staff up-to date on cyber security threats and technical knowhow by providing adequate training.

9. Conclusion

During 2016, majority of the incidents reported to Sri Lanka CERT were related to social networking sites and various malicious activities such as account hijacking and fake account creation. These were typically motivated by revenge, extortion or malicious software distribution. Ethical use of Internet should be promoted to avoid this kind of incidents.

However, it was observed that there are significant number of financial frauds and ransomware attacks targeting businessmen and organizations. It is expected that this motive change in the cyber-attacks will continue in the year 2017 as well.

All the events organized by Sri Lanka CERT during the year 2016 were very successful, well attended and were high in demand. We will continue to conduct the Annual Cyber Security Week and the Annual National Conference on Cyber Security in the coming years as well.

Sri Lanka CERT|CC shall continue to participate in regional events such as the Annual APCERT cyber security drill and also welcomes opportunities to collaborate with its sister CERTs in incident coordination and resolution.

In the year 2016 Sri Lanka CERT was able to support Bt-CIRT in Bhutan by providing training for 5 members of their team. They have also invited Sri Lank CERT to be their sponsor for both APCERT and FIRST membership.

We were able to support BGD eGOV CIRT of Bangladesh by sponsoring their application for APCERT membership.

Sri Lanka CERT also co-sponsored MCI-CERT of Iran to help them obtain full membership of FIRST in collaboration with MyCERT, Malaysia.

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.

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 to TechCERT

TechCERT, Sri Lanka's first and largest Computer Emergency Readiness Team (CERT) helps general public and Sri Lankan organizations keep their computer systems and networks secure. TechCERT celebrated their 10th Anniversary on 01st of 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 TechCERT Team

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.):

Qualification	Number of Qualified Employees
PhD	3
MEng/MSc.MPhil	11
MBA	1
BSc Eng/BSc/BIT/BEng	19
CISSP	1
C|HFI	2
Certified ISMS Auditor (ISO27001)	2

CCNA/ CCNA Security	3
Chartered Engineers	1
MCTS	1
CISE	1
C|EH	6
ITIL v3	1
PMP	1
CPISI	4
RHCSA/RHCSE	6
ENSA	1

1.3 Constituency

TechCERT's constituency comprises its member organizations, selected governmental organizations and the general public of Sri Lanka. In accordance with the mandate of TechCERT, it provides effective response to malicious cyber threats, widespread security vulnerabilities identify and respond to cyber security incidents and conduct training and awareness to encourage best practices in information security among the Sri Lankan Internet community.

2. Activities & Operations

2.1 Services Provided

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

- Network surveying, penetration tests and vulnerability assessments
- Emergency response and damage control for computer security incidents
- Vulnerability research and verification and white-hat exploitations
- Wireless network security assessment and reconfiguration
- Firewall and router security assessments
- Web application security assessment and remediation
- Verification of compliance with physical and environment security standards
- Organizational IT operations analysis and advisory services on IT security Policies with respect to ISO 27001:2013 standard
- Host discovery assessment

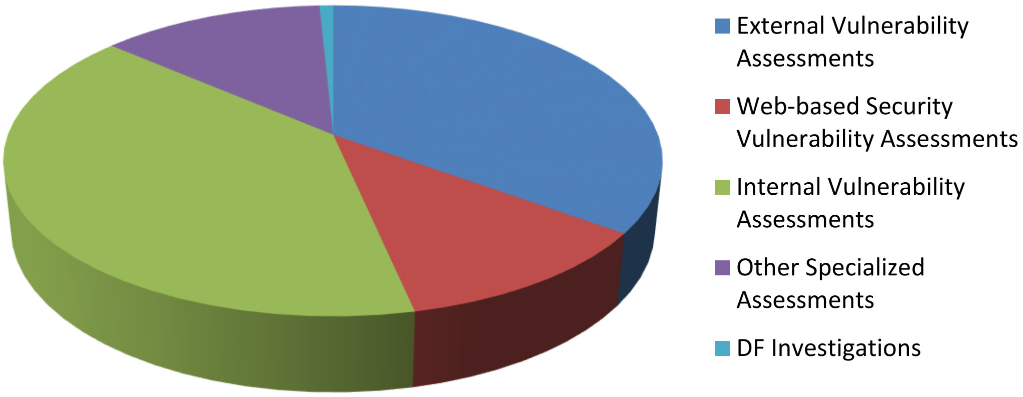
- Providing PCI-DSS certification to Sri Lankan clients in collaboration with QSA company
- Business IT risk assessment and advisory services on BCP and DRP
- Evolving a security strategy against malware and other attacks
- Consultancy for PKI implementation, certificate authority (CA) planning, setting up, CA operations and support services
- Software security functionality audit and code reviews
- Digital forensic investigation services for private and public sector organizations
- IT security information dissemination
- Phishing early warning system management and operations
- Other Pro-active IT security services

2.2 TechCERT Activities and Operations

The details of activities and operations conducted by TechCERT during the year 2016 are as follows:

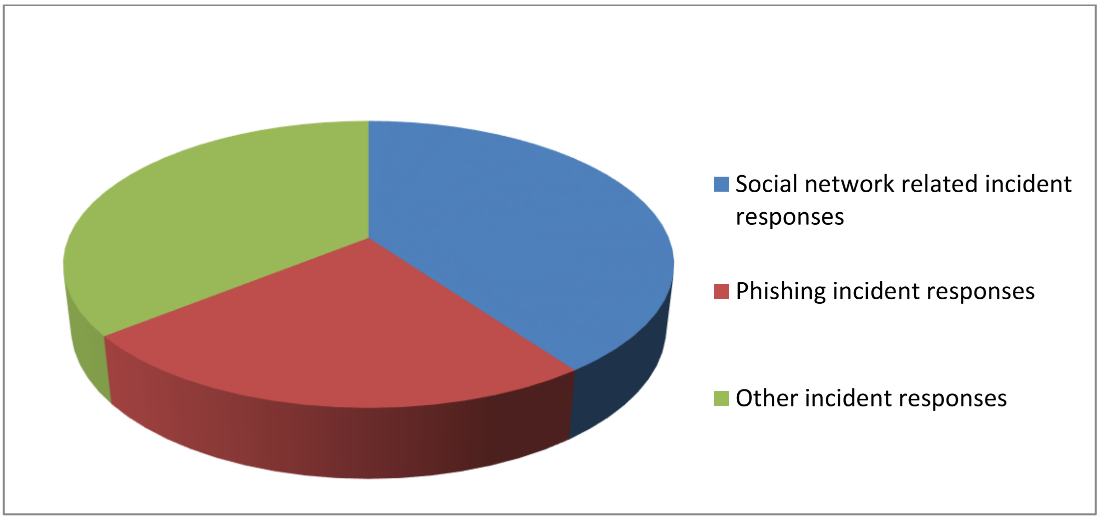
2.2.1 Security Assessments

Activity Type	**Count**
External Vulnerability Assessments	2296
Web-based Security Vulnerability Assessments	760
Internal Vulnerability Assessments	2602
Other Specialized Assessments	843
DF Investigations	52



2.2.2 Incident Response

Types Of Incident Response	Count
Social network related incident responses	62
Phishing incident responses	92
Other incident responses	103



3. Events Organized by TechCERT

3.1 Organizing Training Seminars, Workshops and Demonstrations

25th and 26th of May 2016	**Workshop – Certified Payment Card Industry Security Implementer** "Certified Payment Card Industry Security Implementer (CPISI)" workshop conducted by SISA, India in collaboration with TechCERT
26th of January 2017	**Workshop – Cyber Security Awareness Workshop** Security awareness training for the staff members of a leading finance organization in Sri Lanka
7th July 2016 (Runuhu Chapter) 22nd July 2016 (Wayamba Chapter) 30th August 2016 (Rajarata Chapter)	**Seminar – "Stay safe on Internet" and "How to Avoid Cyber Attacks"** IESL provincial seminar series was conducted.

3.2 School Training Programs on "Safe Internet Browsing and E-mail Security"

Program Name	Date	Audience	Venue
Information Security Awareness Training	12th March 2016	Teachers	Ananda College, Puttalama, Sri Lanka
Information Security Awareness Session	17th April 2016	Teachers & Students	Ananda College, Puttalama, Sri Lanka
Information Security Awareness Workshop	19th June 2016	Teachers	Maliyadeva College, Kurunegala, Sri Lanka

3.3 Participation in Conferences, Workshops and Trainings Programs

- Dileepa Lathsara, Chief Operating Officer of TechCERT participated in the, 28th Annual FIRST Conference, "Getting Back to the Roots" held in Seoul, South Korea
- Dileepa Lathsara, Chief Operating Officer of TechCERT participated in the 9th

Annual National Conference on Cyber Security organized by SLCERT|CC & ICTA Sri Lanka held on 02nd November 2016.

- Kushan Sharma, Engineering Manager of TechCERT and Kasun Chathuranga Lead Engineer of TechCERT participated in APCERT annual general conference, which was held on 24 – 27 October 2016 in Tokyo, Japan
- Harshana Porawagama, Engineering Manager of TechCERT & Nalinda Herath, Lead Engineer of TechCERT participated in the SISA Summit on 05th February 2016 in Mumbai, India.

3.4 Cyber Security Drills

24th March 2016	**APCERT Cyber Security Drill 2016** TechCERT actively participated in the APCERT Drill 2016 as the leader of the Organizing Committee and a member of EXCON team.
18th May 2016	**Cyber Security Drill for Sri Lankan Finance & Insurance Organizations** TechCERT conducted a cyber-security drill for the Banking Sector in Sri Lanka on the Theme "An Evolving Cyber Threat & Financial Fraud".
3rd August 2016	**Cyber Security Drill for Sri Lankan Banking Sector** TechCERT conducted a cyber-security drill for the Banking Sector in Sri Lanka on the Theme "An Evolving Cyber Threat & Financial Fraud".
17th November 2016	**Cyber Security Drill For Sri Lankan Telcos And ISP's** TechCERT conducted a cyber-security drill for the Banking Sector in Sri Lanka on the Theme "An Evolving Cyber Threat & Financial Fraud".

4. Achievements

4.1 Technological Achievements

EagleEye service provided by TechCERT is a web application security monitoring service. Under this service, the clients will be notified of an ongoing attack to their website with the guidance to mitigate the attack.

4.2 Publications

- 53 articles were published in the TechCERT official website https://techcert.lk/en/ during the year 2016 in order to enhance the basic security knowledge of the general public.
- MSD Fernando, Hamid Jahankhani, Mathews Z Nkhoma "Cases of Network Administrator Threats", Journal Paper, ERU Symposium 2017, University of Moratuwa, Sri Lanka
- Prasad Thushara Peiris, M Shantha D Fernando, Gihan V Dias, "Web traffic Analysis for Content Prioritization", Journal Paper, ERU Symposium 2016, University of Moratuwa, Sri Lanka
- Madhuka Udantha, Surangika Ranathunga, Gihan Dias, "An Episode-based Approach to Identify Website User Access Patterns", Journal Paper, ERU Symposium 2016, University of Moratuwa, Sri Lanka

5. Future Plans

- In 2017, 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.
- Develop a system to automate the detection and containment of Security Information Leakages.
- Enhancing the technologies and technical knowledge of the engineers, who work at the DarkLab. DarkLab is a c digital forensic investigation laboratory operated at TechCERT.

6. Conclusion

TechCERT achieved a remarkable milestone in the year 2016 by celebrating its 10th

Anniversary being a leading information security and engineering consultancy services provider. 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 the Sri Lankan Organizations (Financial Organizations, Banks and Telco & ISPs) for the sixth consecutive year in 2016.

There was a significant increase in phishing attacks and website defacement/hacking incidents in Sri Lanka in 2016, 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. Introduction

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.

1.1 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.

1.2 Staffing

ThaiCERT technical staffs consist of 1 specialist and 17 engineers who are responsible for incident response, threat analysis and digital forensics.

2. Activities & Operations

2.1 Incident Statistics

Reported Incidents Handled via Triage

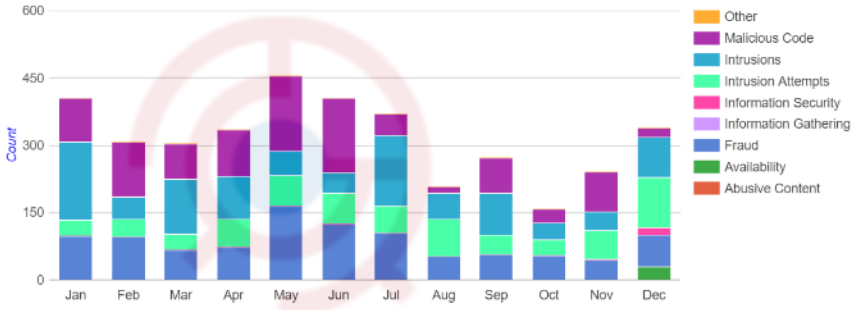


Figure 1: The number of reported incidents in 2016

Via triage, ThaiCERT handled a total of 3,797 reported incident cases (tickets) in 2016, which is a decrease of 13.1% compared to those of 2015 (4,371 cases). The received reports per month varied approximately between 200 to 500 cases, with an average of 316 cases per month.

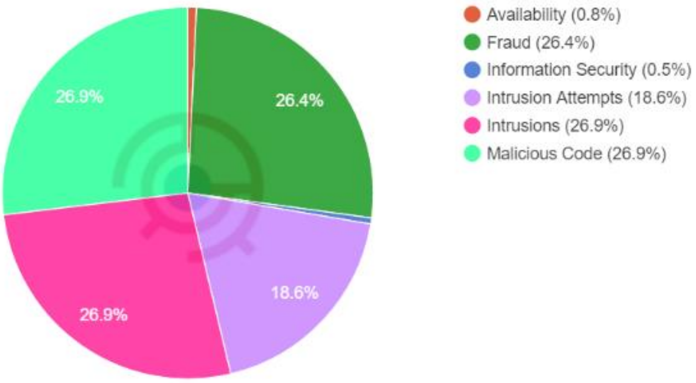


Figure 2: The proportion of reported incidents by incident type in 2016

According to the reported incidents in 2016, classified by the eCSIRT incident classification[1], malicious code (mostly malware URLs) dominated with 26.9%, followed by fraud at 26.4%, where all fraud cases were phishing, and intrusions at 26.9%. All such information was handled and notified to the relevant parties through e-mail channels.

[1] http://www.ecsirt.net/cec/service/documents/wp4-clearinghouse-policy-v12.html#HEAD6

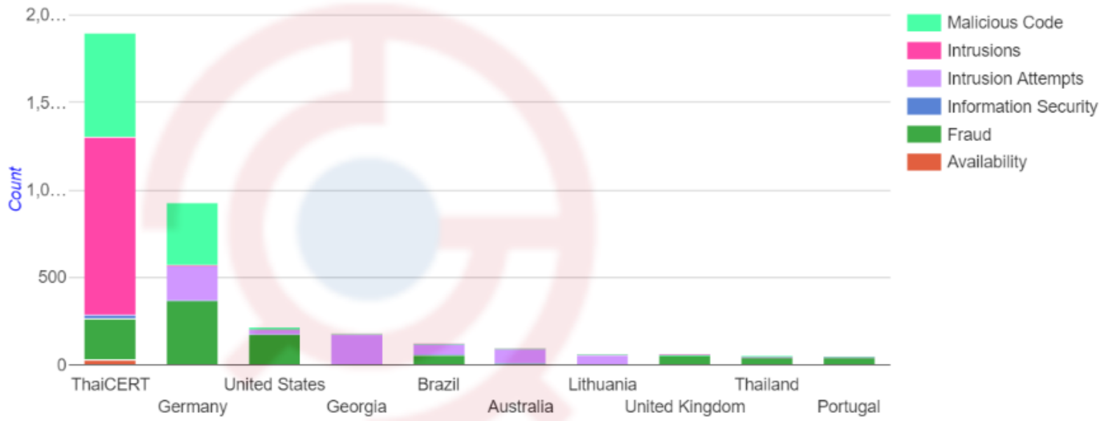


Figure 3: Top 10 incident reporters in 2016

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 1,899 cases or 50% of all reports. The source of Fraud, Malicious Code and Intrusions incident reports generally came from automatic feeds. The number of incident reports from Germany were in second position (927 cases), while number of incident reports from the United States (216 cases) slightly decreased.

2.2 Reported Incidents Received

Type of Incidents		Number of reported unique IPs
Abusive Content	Abusive Content	0
Malicious Code	Malware	1,221,637
	Malware URL	444
Information Gathering	Scanning	238
Information Security	Data Leakage	32
Intrusion Attempts	Brute Force	1,135
Intrusion	Web Defacement	288
Availability	Open DNS Resolver	148,637
	DDoS	14
Fraud	Web Phishing	309
Others	Open Proxy Server	15,315

Figure 4: Reported Incidents Received in 2015 counted by unique IPs

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 2016, ThaiCERT has received incident reports comprising 1.8 million unique IPs where the top 3 of incident reports were Malware (1,221,637 IPs), Open DNS Resolver (148,637 IPs) and Open Proxy Server (15,315 IPs).

2.3 Training

Co-organized:

- Invited to be a trainer of incident response training co-organized by JPCERT/CC and LaoCERT, Lao PDR, Feb 2016
- iSEC with Thailand Information Security Association, Nov 2016

2.4 Drill

Organized:

- Cybersecurity drill for government agencies under ThaiCERT Government Threat Monitoring project, Feb 2016
- Cyber Defense Exercise with Recurrence, Dec 2016

Participated:

- APCERT Drill 2016, Mar 2016
- ASEAN CERT Incident Drill (ACID) 2016, Sep 2016

2.5 Meetings and Seminars

Co-organized:

- Incident Handling 101 with JNSA, Mar 2016
- (ISC)^2 Security Congress APAC 2016 with (ISC)^2, Jul 2016
- CSIRT Promotion Seminar with NTT-EAST, Nov 2016

Participated:

- RSA Conference 2016, San Francisco, USA, Feb 2016
- APCERT AGM 2016, Tokyo, Japan, Mar 2016
- Annual FIRST Conference, Seoul, Korea, Jun 2016

2.6 MoU

- Microsoft under Government Security Program, Oct 2016
- KrCERT/CC KISA, Apr 2016
- 18 critical associations and government agencies, Sep 2016

3. Certifications

ThaiCERT technical staff currently holds the following professional information security.

certificates:

- CompTIA Security+
- GIAC GCUX/GSEC/GCIA/GPEN/GCIH/GWAPT/GXPN/GCFE/GCFA/GREM
- Certified Ethical Hacker (CEH)
- AccessData ACE/AME
- EnCase Certified Examiner (EnCE)
- Certified Forensic Computer Examiner (CFCE)
- Certified Information Systems Security Professional (CISSP)
- ISMS Lead Auditor
- Certified Information Systems Auditor (CISA)

TWCERT/CC

Taiwan Computer Emergency Response Team / Coordination Center – Chinese Taipei

1. About TWCERT/CC

1.1 Introduction

Taiwan Computer Emergency Response Team / Coordination Center (TWCERT/CC) is a security organization for computer intrusion handling, security-related resource and tools providing, latest vulnerability information publishing, and security education popularizing. In addition to play a coordination role in Taiwan security domain (.tw), TWCERT/CC actively participates in international network security organizations and actions to strengthen communication and coordination with CERTs. Expect to provide users with a safe and convenient internet environment under cooperating with domestic and international security organizations.

1.2 Establishment

TWCERT/CC formally established since 1998. 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.

The main purpose of TWCERT/CC is to provide assistance to handle the incidents regarding information and network security. By raising the security awareness in our network community and developing security technologies to improve the liability of the network environment. Our missions are:

- Speed up the circulation of network security information to enhance the safety of domestic information and networks.
- Research and develop the computer network detecting and defending skills to strengthen the network safety.
- Facilitate the foundation of each organization's emergency response team, promote the national wide network security, and reconcile the combination and interchange on security information.
- Encourage and coordinate the exchanges and cooperation between each international emergency response institution to maintain the global network security.

1.3 Organization

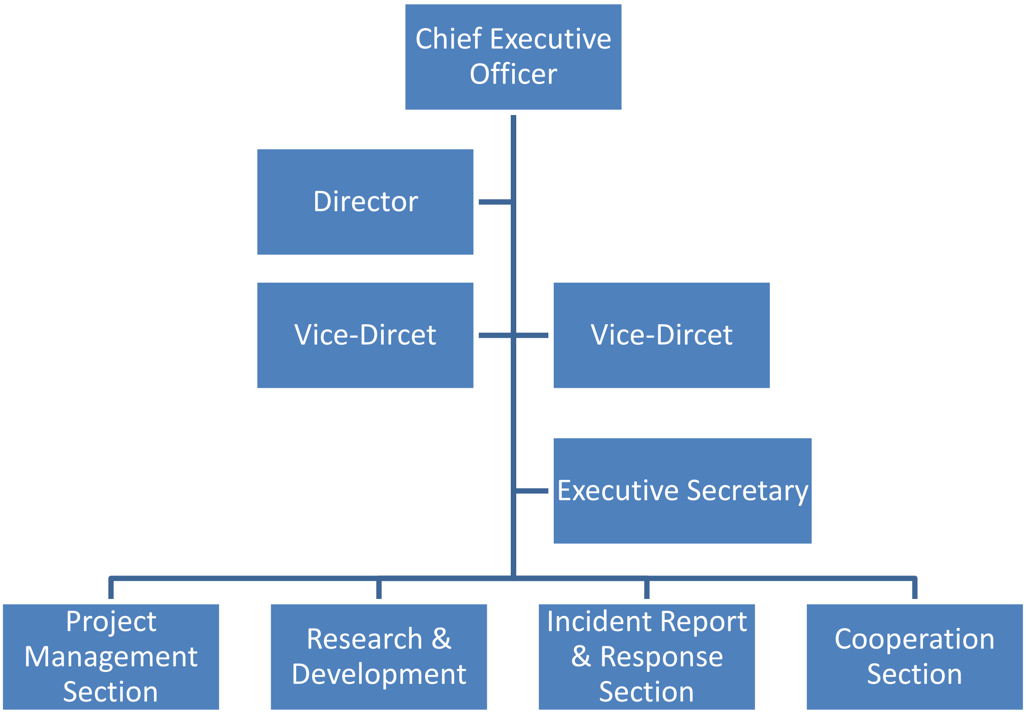


Figure 9.Organization of TWCERT/CC

2. Activities & Operations

2.1 Incident Report Handling

Frequent incidents show that it is great urgent to improve system and network security. To defend hacker intrusion and stop up security threats spreading, TWCERT/CC works hard for safeguarding security and plays the contact agent for sharing the experiences on dealing Taiwan's network security incidents with other CERTs. In 2016, TWCERT/CC received 3,461 computer security incident reports.

Year	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016
Total	788	660	1087	679	1094	6666	8,126	140,250	15,150	24,116	3,461

Table 1. Incident reports to TWCERT/CC (2016)

Expect to achieve the following goals:

- Possible incidents prevention: provide an incident response channel and the prevent mechanism for the victims to avoid analogous events happening.
- Real-time incidents handling: offer an immediate warning and defense force to effectively restrain and control incidents extending.
- Recovery support: provide technological consultant and support to recovery operation and reduce damage.

The incident reports to TWCERT/CC in 2016 have categorized as in Fig. 2.

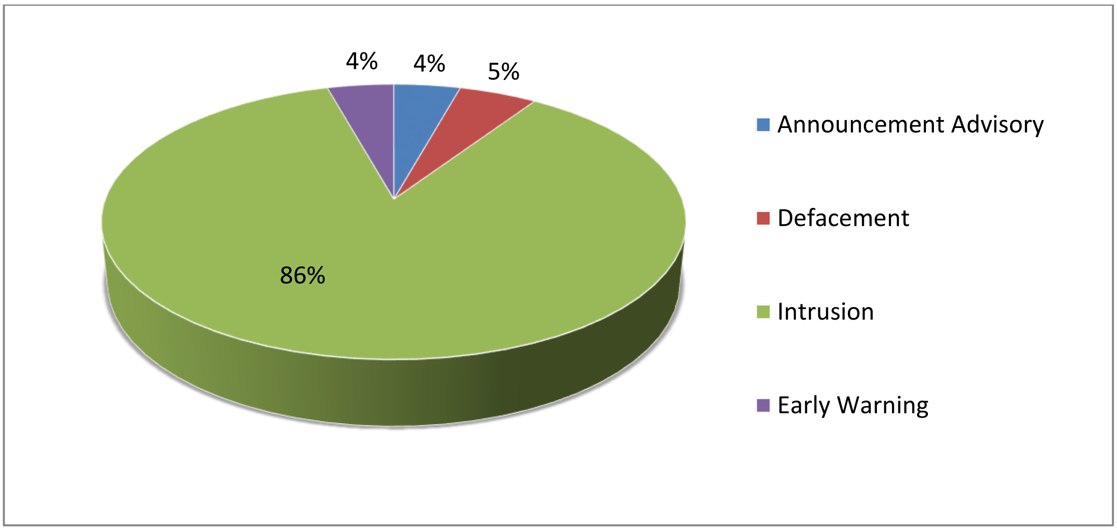


Figure 10. Distribution of incident response

2.2 Intelligence Monitoring and Warning

- Security Vulnerability Announcement

  To promote system and network security and reduce damage from intrusion, TWCERT/CC is devoted to strengthen services, to publish latest security issues, to provide security documents/tools, vulnerability patch information and security related documents download, and actively research attack/defense technologies.

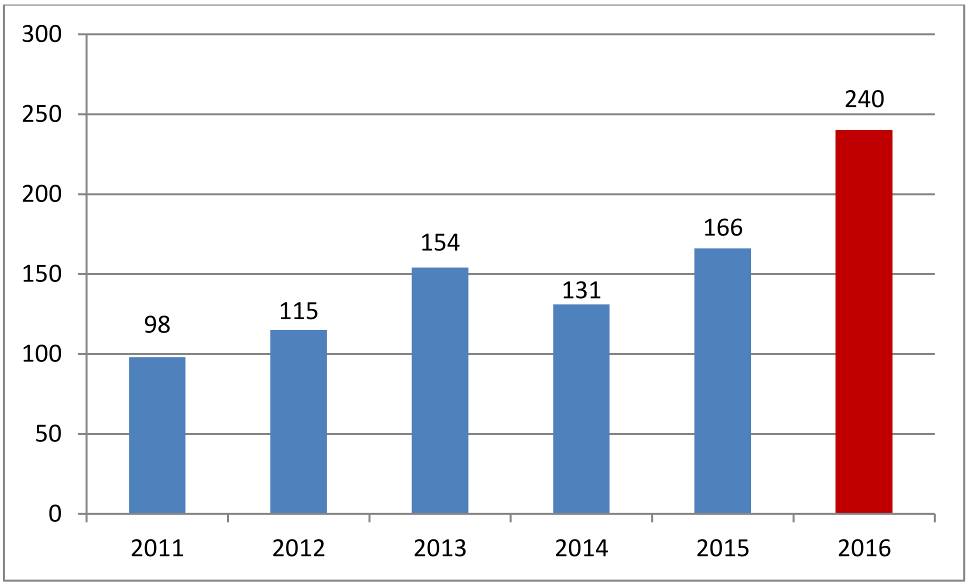


Figure 11. Annual Statistics of Vulnerability by TWCERT/CC

The major purpose of the establishment of the localized Vulnerability Database is to collect the information of software vulnerabilities and system weaknesses. The vulnerability database contains 14 categories, we have collected 240 numbers of vulnerabilities in 2016. We will continuously invest manpower to maintain and update. The major categories are shown in Fig. 4 and Table 2.

vulnerability category	number(s)	vulnerability category	number(s)
Denial of service	28	Cross site scripting	18
Gain information	29	Cross-Site Request Forgery	4
Code execution	66	Others	3
Overflows	20	Injection	7
Memory corruption	1	Directory traversal	2
Gain privilege	34	Http response splitting	0
Bypass something	25	File inclusion	3

Table 2. Categories of the Vulnerability in 2016

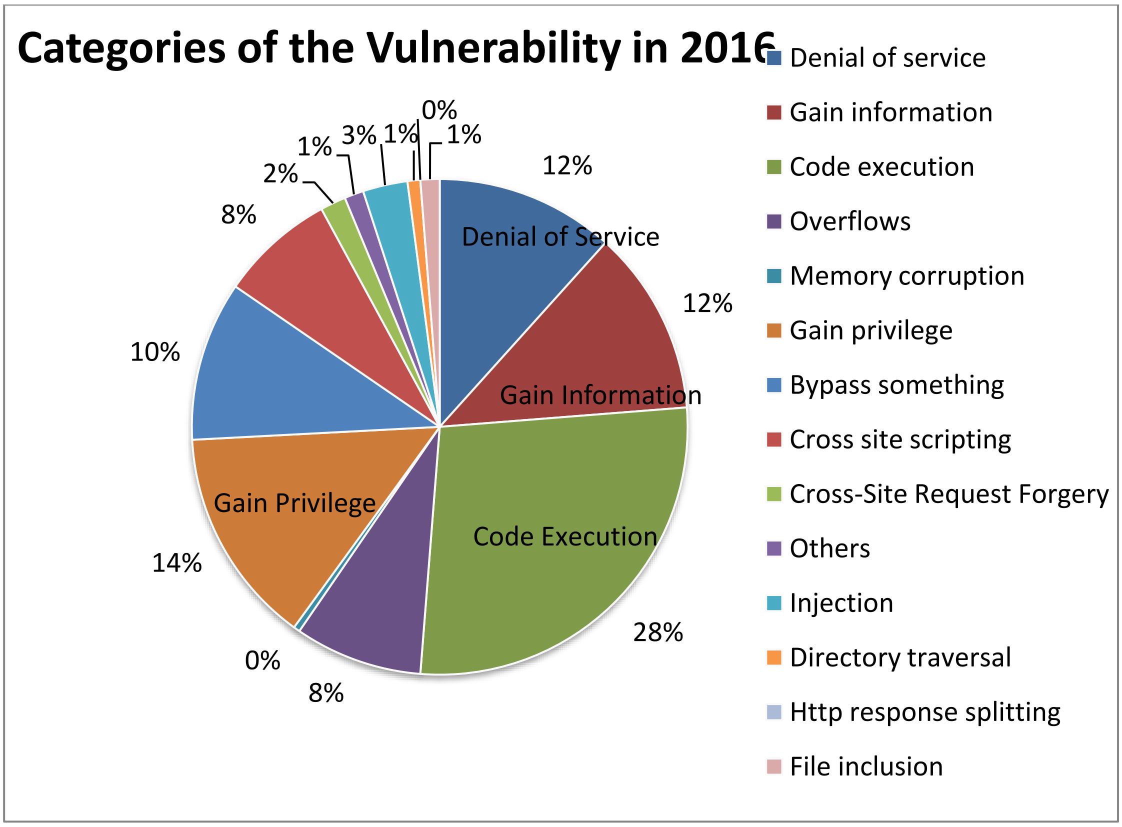


Figure 12. Categories of TWCERT/CC Vulnerability Database

- **TWCERT/CC Monthly and Daily Report and Monograph**

TWCERT/CC publishes monthly reports on early warning information of the preceding month to the Taiwanese government, general corporations and national critical infrastructures. The monthly report contains information on domestic and international information security news. In addition, TWCERT/CC also update vulnerability intelligence information on official website and facebook. Monograph is a study of a single specialized subject of information security.

3. Events organized / co-organized

3.1 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 security workshops 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.

Date	Subject
2016/3/7	Taiwan Cyber Security Coordinator. Your Security、We Care. (Taiwan InfoSec Conference 2016)
2016/4/19	2015 TWCERT/CC Incident Report (Symantec ISTR Media Briefing)
2016/7/11	Data Breach (IRCON 2016)
2016/10/6	Panel Discussion - Face of Cyber Security Financial Technology Development (HITCON Financial Talk)

Table 3. list of TWCERT/CC workshops in 2016

3.2 Drill

TWCERT/CC participated in the APCERT Drill in March 2016. 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. Achievements

The government and organizations recently pay much attention to information and communication security promotion and development. TWCERT/CC has made great efforts to manage in security field many years for enhancing network safeguard to protect against the increasing intrusion and attack.

- **Enhance domestic network security**

The main purpose of TWCERT/CC is to provide assistance to handle the incidents regarding information and network security. By raising the attention of network community to security issues and conducting the research on computer systems, we manage to enhance the fail-safe systems of computers and networks, and proceed to prevent the incident beforehand. We disseminate system vulnerability information to raise the awareness of network security, identify and resolve the system vulnerabilities on various platforms, and work with security researchers to develop the prevention and protection techniques to improve the network security.

- **Encourage and coordinate incident response**

TWCERT/CC is devoted to promote collaborative research and development on cyber security to reduce the loss caused from incidents. TWCERT/CC plays a major communication agent for encourage and coordinating the exchanges and cooperation with domestic ISPs and international CERTs or CSIRTs to maintain global network security.

- **Security promotion**

TWCERT/CC works to create an international workforce skilled in information assurance and survivability by developing curricula and training for executives, managers, engineers, network administrators and operators. Furthermore, TWCERT/CC held seminars and education training programs to promote the importance of security awareness and to enhance the ability of security administrators in a proactive way. Such interactively training provides a great channel for information sharing as well as skill improvement.

- **Security training**

Recently frequent incidents encourage security awareness and professional demand. Personal training is the major work in technology development. TWCERT/CC offers many introductory and advanced training for executive, managers, educators, engineers, cyber administrators/operators and so on. TWCERT/CC has trained many good talent of security field who are responsible for the security of information assets in different organizations. Hope to enhance domestic research and development capacity by mutual support and cooperation.

- **International relationship**

TWCERT/CC actively participates in international organizations and activities, and improves our capabilities and services. We have joined in FIRST, APCERT, Anti-Phishing Working Group, US-CERT Homeland Security Information Network(HSIN), Automated Indicator Sharing (AIS) Program and Anti-spam MoU to be the international coordination in Taiwan to reinforce the information exchange and collaborations among all the other CERTs around the world. On account of the cooperation among the network security organizations, we expect to provide a secure and convenient network environment for the Internet users.

- **Publication**

Each month, TWCERT/CC issues Information Security E-News to provide Information Security notice, activity, and News summary in that month. Security experts and scholars share wide range of security knowledge in the newsletter column or special report to promote information security and to improve the security skills. Technical reports were published in nation or international conferences to promote the new technology developed by the society.

- **Certificates**

The staff members hold the following certificates.

- ISO 27001 Lead Auditor
- ISO 20000 Lead Auditor
- Capability Maturity Model Integration Personnel Training
- Project Management Professional Certification
- Certified Ethical Hacker

5. International Collaboration

In addition to make efforts in security improvement in our domain, TWCERT/CC actively participates in the international security organizations and actions to enhance communication and cooperation. TWCERT/CC plays a major communication agent for encouraging and coordinating the exchanges and cooperation with the international emergency response institutions to maintain the global network security.

- To participate in international forums and meetings, to exchange the related security intelligence with each emergency response center.
- To form a transnational defense system to handle international incidents.

- **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 to enhance regional and international cooperation on cyber security. APCERT cooperates with CERTs and CSIRTs to maintain a trusted contact network of security experts in the Asia Pacific region to improve the region's awareness and competency in relation to cyber security incidents.

TWCERT/CC jointly develops measures to deal with large-scale security incidents and phishing attack, and exchange technologies and experiences with APCERT members to manifest Taiwan much effort in security and help to understand the latest development and tendency in the Asia Pacific region.

- **Memorandum of Understanding (MoU)**

To further strengthen cooperation, TWCERT/CC has been signing a MoU with various security organizations, such as Verint and Symantec to exchange intelligence.

- **ATM Hacking Incident in Thailand**

In Taiwan, First Bank ATM hacking incident happened in July 2016. Lots of sectors investigated the ATM hacking incident and shared the analysis report to TWCERT/CC. In addition, TWCERT/CC also surveys lots of related report about this ATM hacking incident. So TWCERT/CC grasps this ATM hacking situation. When ATM hacking incident happened in Thailand, TWCERT/CC shares some reports and intelligences to ThaiCERT to help them to solve ATM hacking incident in Thailand.

6. Future work and Conclusion

The future work of TWCERT/CC will emphasize the harmonic and efficiency of the coordination among different levels and across the nation.

- Work for security related research and development to advance the international visibility.
- Participate in international interchange and coordination to form a transnational joint defense mechanism.
- Train the awareness and capability in information security and risk management through information sharing and international cooperation.

- Develop a malware analysis platform for Taiwan sectors to avoid some confidential data breach incidents.

TWNCERT

Taiwan National Computer Emergency Response Team – Chinese Taipei

1. Highlights of 2016

1.1 Summary of major activities

TWNCERT aims to support and enhance the government's ability to respond and deal with security incidents. In 2016, TWNCERT received 821 reports on security incidents from Taiwan government and published 2,110 security advisories to government sectors as well as provide 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 14 national cyber security seminars for the government agencies as well as launched total of 17 promotion activities and cybersecurity competitions for university students.

In 2016 TWNCERT also attended various international events and delivered presentations on cyber security threats at the APRICOT Security Track event in New Zealand in February, APCERT AGM & Conference in Japan in October and Mauritius 2016 FIRST Technical Colloquium in November.

1.2 Achievements & milestones

TWNCERT was elected to remain on duty as APCERT Steering Committee member at the AGM 2016. As the convener of APCERT Training Working Group, TWNCERT convened 6 APCERT online training programs in 2016, and a total of 20 CERTs member teams have 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 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 national cybersecurity issues. The formation of TWNCERT aims to create a government 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 110 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 821 reports on computer information security incidents from Taiwan government sectors, and more than 1,107 international information security incident reports from overseas in 2016.

In addition, 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 cybersecurity efforts nationally. In 2016, G-ISAC has shared a total of 81,736 security incidents and critical information among members including Academic ISAC (A-ISAC), National Communications Commission ISAC (NCC-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 Intrusion, Other, and Website Defacement.

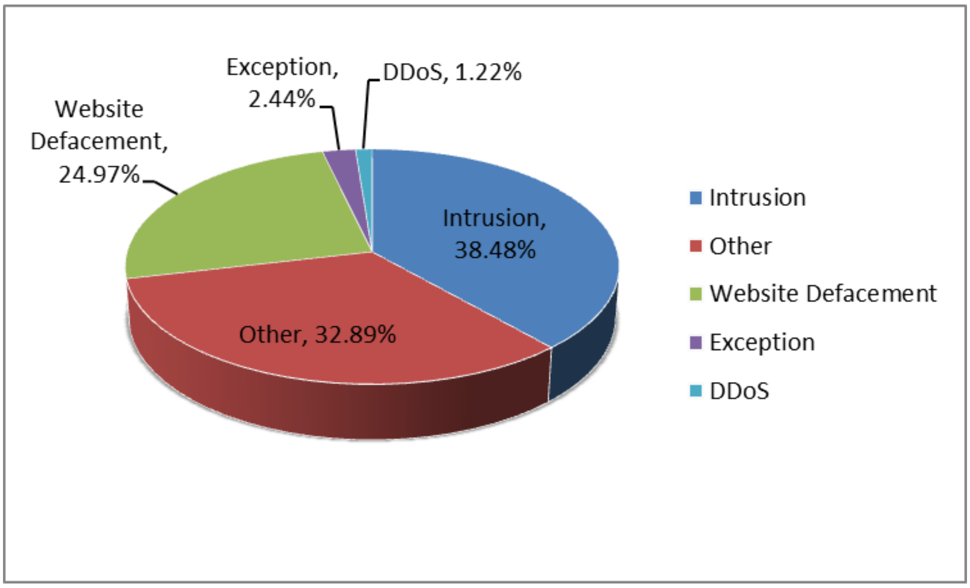


Figure 1 Security incidents from government sectors

The international information security incident reports in 2016 were categorized as in Figure 2. About 43.48% of the incident reports were Phishing, followed by Malware and Attack.

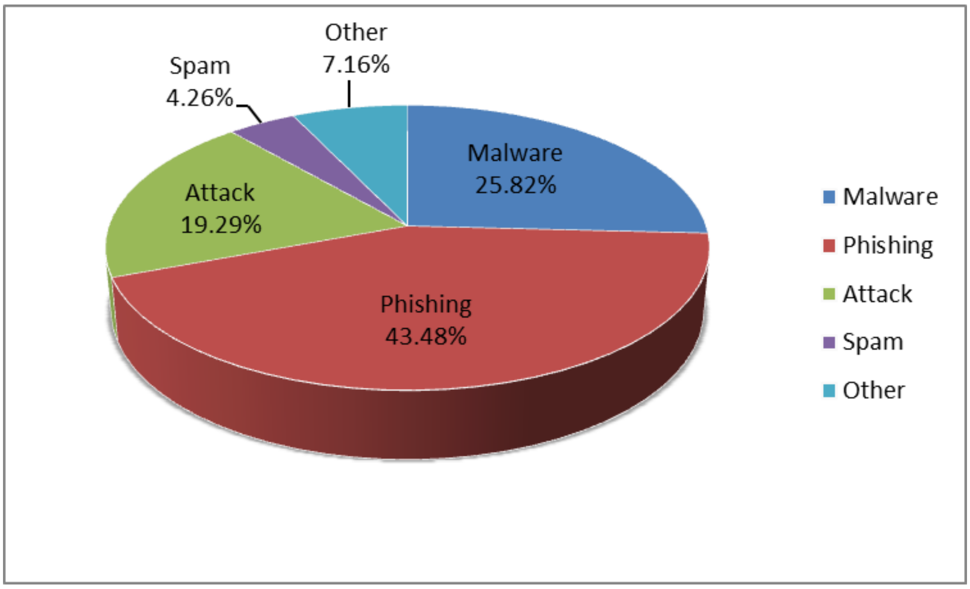


Figure 2 Classification of the international incident reports

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 81,736 security information in 2016.

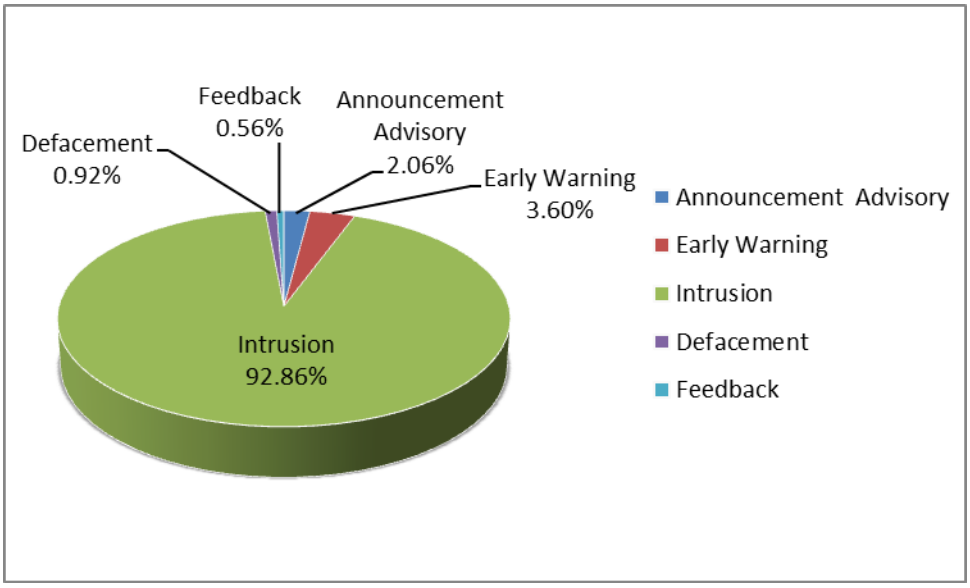
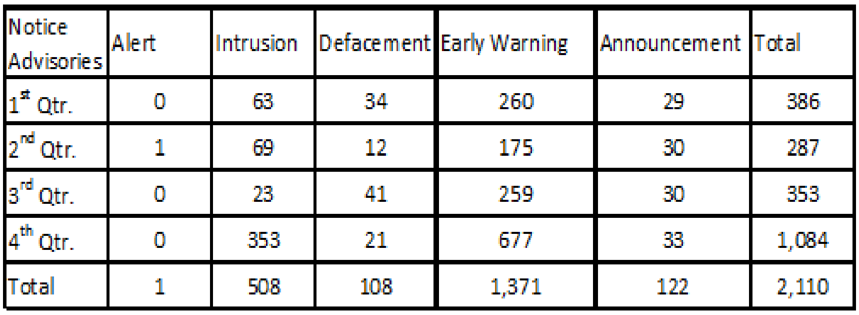


Figure 3 Information sharing distribution of G-ISAC

3.4 Publications

- Government sectors

In 2016, TWNCERT published 2,110 notice advisories to government sectors. The categories were distributed as in Figure 4 and 5.



Notice Advisories	Alert	Intrusion	Defacement	Early Warning	Announcement	Total
1st Qtr.	0	63	34	260	29	386
2nd Qtr.	1	69	12	175	30	287
3rd Qtr.	0	23	41	259	30	353
4th Qtr.	0	353	21	677	33	1,084
Total	1	508	108	1,371	122	2,110

Figure 4 Notice advisories to government

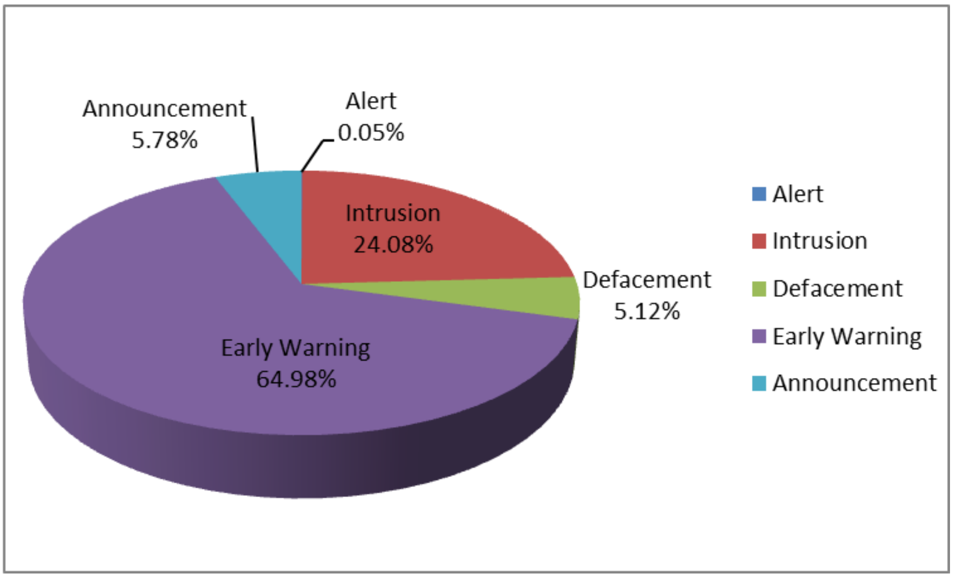


Figure 5 Distribution of government notice advisories

- International incident report sharing

Regarding the international incident report sharing, TWNCERT has reported a total of 31 incident reports via G-ISAC to 17 countries shown in figure 6 and 7.

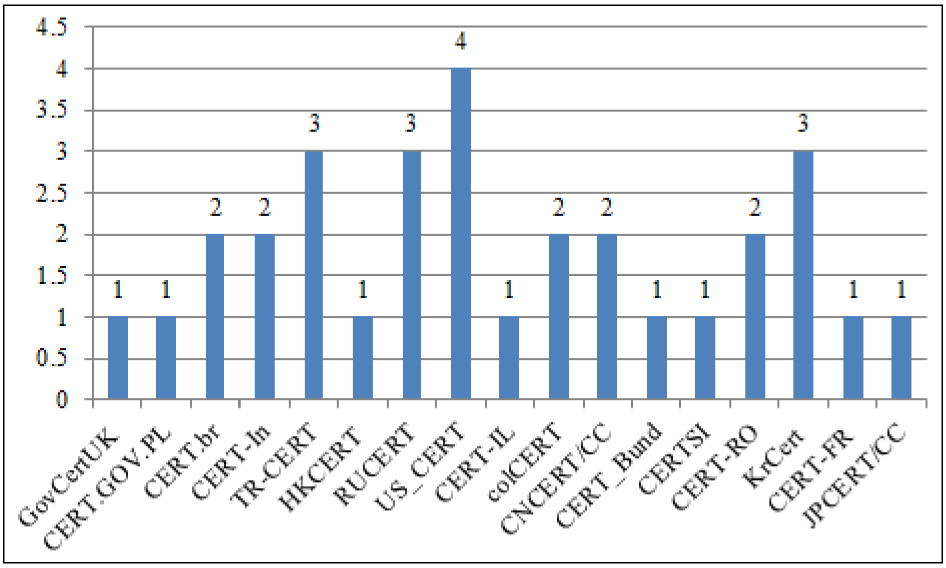


Figure 6 International incident report via G-ISAC

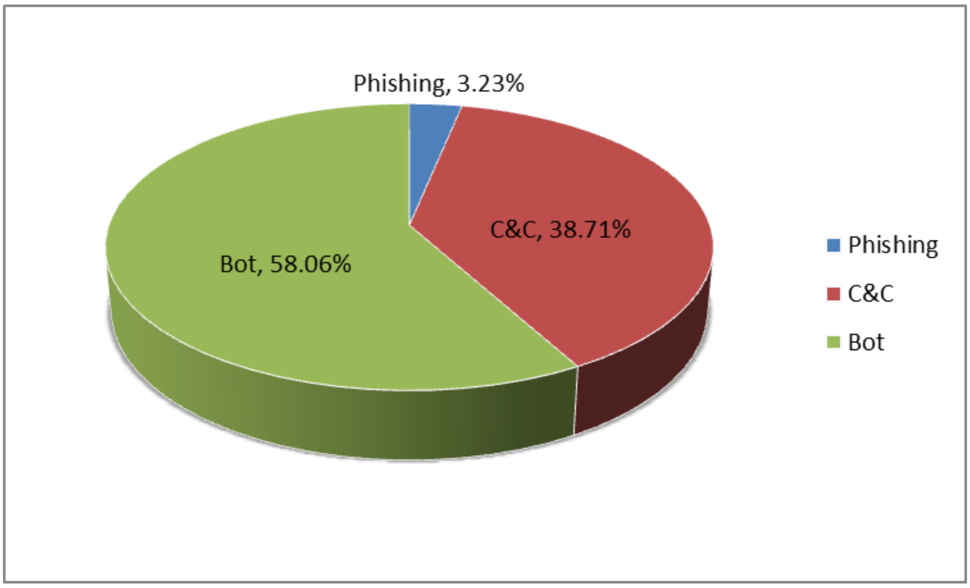


Figure 7 Categories of international incident report via G-ISAC

- Web site publication

TWNCERT collects and publishes security advisories, news or guidelines via its website. In 2016, TWNCERT published 478 news including security news and bulletins on the website, about 10.64% increases from the previous year.

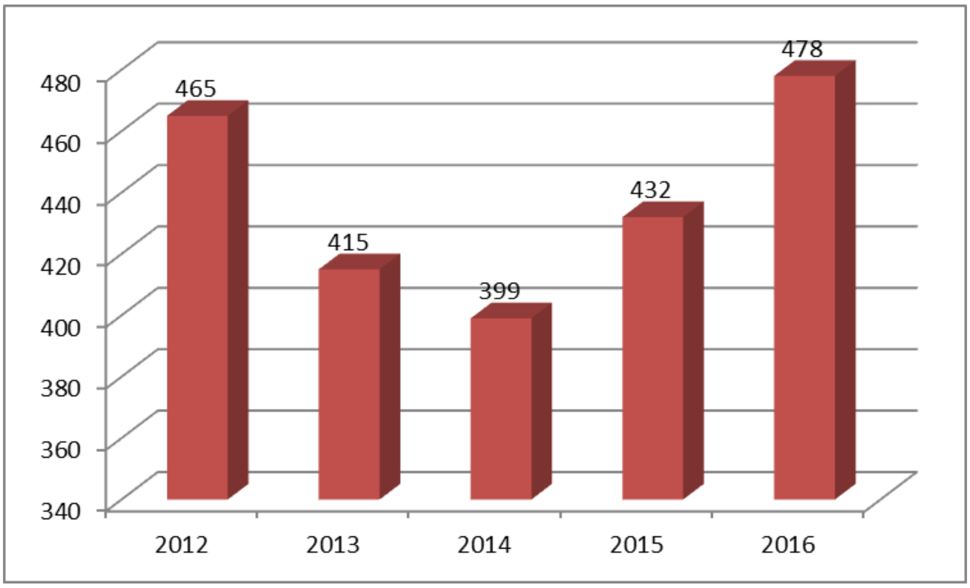


Figure 8 TWNCERT Published news on website

4. Events organized/hosted

4.1 Training

TWNCERT offers training for government technical staffs. In 2016, over 16 security awareness training courses were organized.

TWNCERT is promoting GCB (Government Configuration Baseline) within government agencies since 2012. Currently, 33 Ministries have fully deployed. Agencies under Ministry and local governments will start to deploy in 2017.

4.2 Drills & exercises

- Drill

TWNCERT has been conducting a national large-scale cyber security exercise, Cyber Offensive and Defensive Exercise (CODE). This year CODE was mobilized relevant domestic agencies including National Security Bureau, Ministry of National Defense, Office of the President and local government agencies, to strengthen the preparedness against cybercrimes, technology failures as well as Critical Information Infrastructure (CII) incidents.

- Cybersecurity competition

In order to promote cyber security general awareness, TWNCERT launched cyber security series competitions in 2016. It aimed to improve the cyber security awareness among university students. TWNCERT held 17 promotion activities in the universities and more than 7,000 attendees participated.

4.3 Conferences and seminars

TWNCERT hosts national cyber security workshops and seminars regularly to raise the cyber security awareness among government agencies. In 2016, TWNCERT held 14 national cyber security workshops for government agencies, and a total of 3,866 government technical staffs attended.

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 2016, a total of 4 member meetings has been held.

Figure 9 Conferences and seminars

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, international annual conferences and other cooperation.

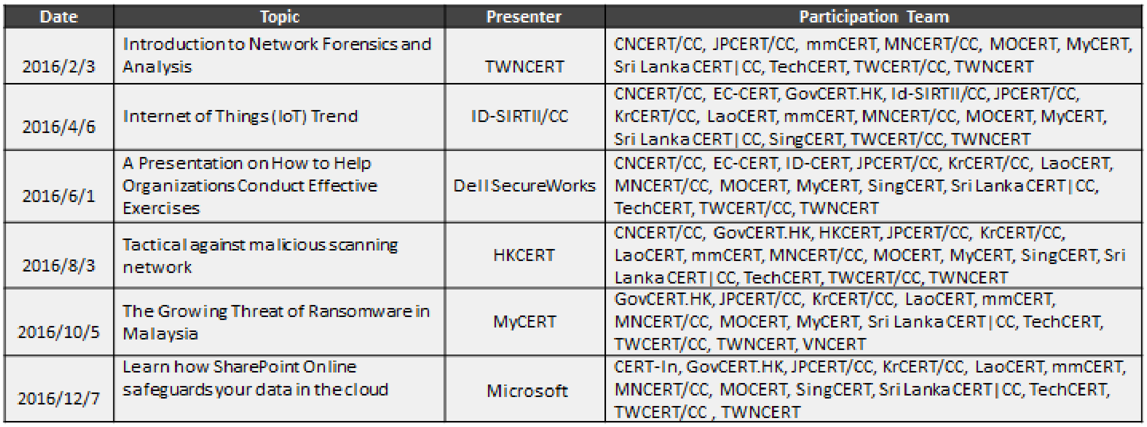
- Asia Pacific Computer Emergency Response Team (APCERT)
- Forum for Incident Response and Security Teams (FIRST)
- APEC TEL
- Meridian
- Anti-Phishing Working Group(APWG)

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 2016, a total of 6 APCERT online training programs have been convened, with a total of 20 CERTs, member teams participated. In order to improve the training program, TWNCERT conducted a survey to evaluate the effectiveness of the overall education and training program in September and delivered the statistics results at APCERT AGM & Conference in Japan in October.



Date	Topic	Presenter	Participation Team
2016/2/3	Introduction to Network Forensics and Analysis	TWNCERT	CNCERT/CC, JPCERT/CC, mmCERT, MNCERT/CC, MOCERT, MyCERT, Sri Lanka CERT|CC, TechCERT, TWCERT/CC, TWNCERT
2016/4/6	Internet of Things (IoT) Trend	ID-SIRTII/CC	CNCERT/CC, EC-CERT, GovCERT.HK, Id-SIRTII/CC, JPCERT/CC, KrCERT/CC, LaoCERT, mmCERT, MNCERT/CC, MOCERT, MyCERT, Sri Lanka CERT|CC, SingCERT, TWCERT/CC, TWNCERT
2016/6/1	A Presentation on How to Help Organizations Conduct Effective Exercises	Dell SecureWorks	CNCERT/CC, EC-CERT, ID-CERT, JPCERT/CC, KrCERT/CC, LaoCERT, MNCERT/CC, MOCERT, MyCERT, SingCERT, Sri Lanka CERT|CC, TechCERT, TWCERT/CC, TWNCERT
2016/8/3	Tactical against malicious scanning network	HKCERT	CNCERT/CC, GovCERT.HK, HKCERT, JPCERT/CC, KrCERT/CC, LaoCERT, mmCERT, MNCERT/CC, MOCERT, MyCERT, SingCERT, Sri Lanka CERT|CC, TechCERT, TWCERT/CC, TWNCERT
2016/10/5	The Growing Threat of Ransomware in Malaysia	MyCERT	GovCERT.HK, JPCERT/CC, KrCERT/CC, LaoCERT, mmCERT, MNCERT/CC, MOCERT, MyCERT, Sri Lanka CERT|CC, TechCERT, TWCERT/CC, TWNCERT, VNCERT
2016/12/7	Learn how SharePoint Online safeguards your data in the cloud	Microsoft	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 2016

5.2.2 Drills & exercises

TWNCERT participated in APCERT Drill under the theme "An Evolving Cyber Threat and Financial Fraud" on March 16, and solved a set of drill scenario within the given time limit (3 hours and 30 minutes).

5.2.3 Seminars & presentations

Below are international events which TWNCERT has participated in 2016.

- APRICOT 2016, February- New Zealand, presented "Cyber-Attack Threats and Cases."
- Cyber Security for Critical Information Infrastructure, April- Singapore
- APEC TEL 53, June- Peru
- FIRST and National CSIRT conference, June – South Korea
- Blackhat USA 2016 & Defcon 24, July- Las Vegas
- OWASP AppSec USA 2016, October- United States of America
- APISC 2016, October- South Korea
- APCERT AGM and Conference 2016, October- Japan, presented "SC Activity Report by TWNCERT," "Training Working Group Activity and Survey Report," and "IoT Threat and IoT Botnet."
- APEC TEL 54, October- Japan
- Meridian Conference 2016, November- Mexico
- FIRST Symposium TC 2016, November- Mauritius
- AVAR Conference 2016, December- Malaysia

6. Future Plans

TWNCERT will be hosting FIRST Technical Colloquia in cooperation with APNIC, which will take place in September 2017 in Taichung, Taiwan. 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 sectors, 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 of 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 Team (VNCERT)".

Roles of VNCERT:

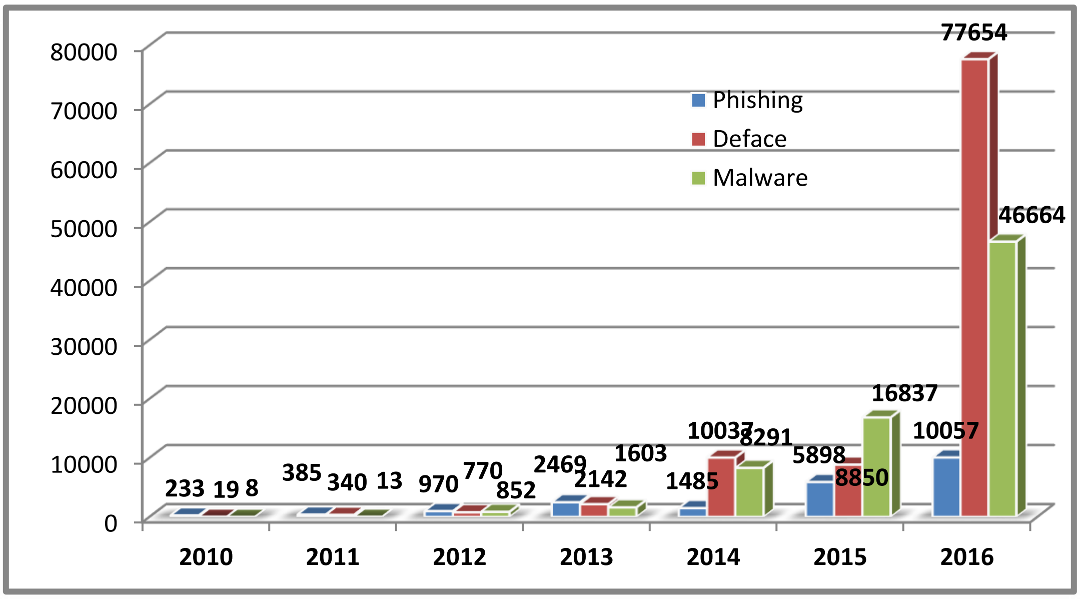
- Being Coordination Center of Vietnam CSIRT Networks with 130 members.(Including information technology centers of Ministries, ministerial agencies, governmental agencies, telecommunication enterprise, internet service providers, the organizations in charge of information systems of national importance).
- Coordinating national computer incident response activities.
- Watching and warning computer network security problems.
- Building and coordinating to build computer network security technical standard.
- Promoting to build CERTs in the organizations, enterprises, and agencies in Vietnam.
- VNCERT is the point of contact of Vietnam with the other CERTs in the world.
- Supporting Ministry of Information and Communications of Vietnam with activities in information security state management.
- Implementing and deploying the anti-spam activities.
- Currently VNCERT has 52 employees working at the head office in Hanoi, one branch in Ho Chi Minh City and one branch in Danang City. Beside administration and financial divisions there are four specialized technical divisions at the head

office: Division of Coordination and Response, Division of System Technique, Division of Training & Consultancy and Division of Research and Development.

2. Activities & Operations

2.1 Incident handling reports

In 2016, VNCERT processed 134.375 information security incidents (including 10.057 phishings, 77.654 Defaces and 46.664 Malwares,).



Picture 1: Incidents in Vietnam on 2011, 2012, 2013, 2014, 2015 and 2016

2.2 Abuse statistics

Security Incidents	2010	2011	2012	2013	2014	2015	2016
Phishing	233	385	970	2.469	1.458	5.104	10.057
Deface	19	340	770	1.603	8.291	6.188	77.654
Malware	8	13	852	2.142	10.037	3.885	46.664
Other	11	17	----	165	8.400	3.979	---
Total	271	757	2.179	4.810	28.186	19.156	134. 375

2.3 Incident response coordinating, warning and supporting activities

In 2016 VNCERT had:

- implemented information security testing and auditing for 116 websites of government agencies.
- removed botnet malwares from thousands of computers in government agencies.
- warned all Vietnam CSIRTs Network members of 02 critical malware (ransomware, backdoor).
- supported VietNam Airline to handle DDoS attack.

2.4 Anti-spam activities

In 2016, VNCERT received 591.427 advertising text messages (including advertising emails; advertising SMS over Internet) which had decreased 18% comparing to 2015.

2.5 Information security legal framework update on

The Law of Information Security had been promulgated by National Assemblyon November, 19th, 2015.

The circular on cyber security incident preventing and network monitoring has been drafting.

Decree No 85/2016 / NĐ-CP regulates the information systems safety ensuring according to their importance levels had been issuedon July, 01, 2016.

3. Events organized / hosted

3.1 Training

VNCERT had organized:

- a training courses on CERT activities for LaoCERT in Laos
- a workshop on “Kill Chain and IOC Analysis” for 30 government agencies and CSIRT teams in VietNam.
- 05other information security exercises and training courses for 05 different government agencies.

3.2 Seminars & Etc

VNCERT cooperated with other organizations to organize annual events such as “Security World 2016”, “National Information Security Day 2016”; organize 4other conferences for CSIRTs Network members and information security departments from all over the country named “Cybersecurity Today”, “Cybersecurity Vietnam”, and a conference on incidents monitoring and responding for e-government.

VNCERTcooperated with NTT-EAST, Japan to implement a collaborative research project for development of CSIRTs in Vietnam sponsored by APT. This project helped to train the Vietnamese trainers and provided Vietnam a guiding toolkit to develop incident response teams in Vietnam.

4. International Collaboration

4.1 Incident Drill

Participated in 03 international drills: APCERT Annual Drill 2016, ASEAN-JAPAN Drill and ASEAN CERTs Incident Drill (ACID 2016).

Supported 02 provinces to organize the internal drills of incident handling.

4.2 Presentation

In 2015, VNCERT participated and had presentations in 09 international conferences and forums.

VNCERT also supported LaoCERT to develop network security, exchanged information and shared experiences with other regional and global CERTs. VNCERT cooperated with oversea companies to organize events and deployed international projects.

5. Future Plans

To build a circular replacing circulars 27/2011/TT-BTTTT, 4-Oct-2011 to regulate coordination of emergency response activities on Vietnam Internet;

To build a national plan of botnet monitoring and removing for Vietnam;

To submit an incident monitoring project and a project of anti-spams and SMS, email monitoring to Vietnam government

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.