TLP: WHITE

APCERT Annual Report 2015

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

CONTENTS

TWNCERT	225
VNCERT	235

Chair's Message 2015

2015 was a significant year for APCERT and the APCERT community. APCERT's Vision of 'working to help create a safe, clean and reliable cyber space in the Asia Pacific region through global coordination' is well-established and APCERT as a community is maturing and seeking more ways to achieve this vision. A significant element of this for the coming year will be further developing and better coordinating APCERT's capacity building activities in support of its members, its partners and the region more broadly.

A true highlight of the year was the joint APCERT and OIC-CERT Annual General Meeting and Conference, hosted by Malaysia in Kuala Lumpur. The event itself was enormous, being combined with the annual Cyber Security Malaysia Awards, Conference & Exhibition, but was of particular significance for APCERT. It was the first such joint event with another CERT forum – in this case the OIC-CERT, with which APCERT signed an MOU in 2011. The event brought all the teams together for the first time and provided an invaluable opportunity for members to meet and share information and ideas. It also saw the first joint APCERT and OIC-CERT Steering Committee meeting, which enabled the two leaderships to share priorities and perspectives and to seek further areas for cooperation and collaboration.

APCERT was also delighted to formalise its long-standing relationship with the Asia Pacific Network Information Centre (APNIC) through signing an MOU in September during the Annual General Meeting and Conference. We look forward to working more closely with APNIC in the future and collaborating on activities such as cyber security training, drills and the emerging APCERT-APNIC Security Track as part of the Asia Pacific Regional Internet Conference on Operational Technologies (APRICOT) and the APNIC Annual Conference.

Internally, APCERT's maturing structure and work program was reflected by the addition of two new Working Groups: Training and the Cyber Threats Mitigation project. The former, convened by TWNCERT, will be a key mechanism for developing APCERT members' capabilities and APCERT's ability to build cyber security capacity throughout the region. The Cyber Threats Mitigation Project Working Group, convened by MyCERT,

will take the lead in coordinating APCERT's contribution to the internet ecosystem and data sharing methods and metrics work initiated by JPCERT/CC's Cyber Green project.

In 2015 APCERT also welcomed a new member from Hong Kong, GovCERT.HK. As always, into 2016 APCERT will look to strengthen its membership base across the region with the addition of new members from qualified CERTs and CSIRTs. And with the Steering Committee considering how best to strengthen APCERT's liaison and strategic partnership arrangements, it is anticipated that APCERT will formalise more relationships with CERT and non-CERT partners both in the Asia Pacific and globally.

I would like to thank my colleagues on the Steering Committee for all their hard work and contributions throughout the year. I would also like to acknowledge both JPCERT/CC and KrCERT/CC who together served an unprecedented four consecutive terms as Chair and Deputy Chair of the Steering Committee. The value of their leadership and guidance over that period should not be underestimated. I would further like to acknowledge the ongoing contribution of the APCERT Secretariat; without the Secretariat APCERT would not be able to function effectively.

I would also like to thank the Convenors of the various Working Groups, and the members of those groups. The collective efforts of these teams have made great strides in developing APCERT as a community and a platform for genuine regional collaboration. And finally, but most importantly, I would like to thank all APCERT members for their contributions over the year. APCERT is a forum of CERTs and CSIRTs and would not exist without its collective members and their efforts.

CERT Australia is honoured to have been 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 the Asia Pacific Network Information Centre (APNIC: www.apnic.net); the Forum of Incident Response and Security Teams (FIRST: www.first.org); the Trans-European Research and Education Networking Association (TERENA: www.terena.org) task force (TF-CSIRT: www.terena.nl/tech/task-forces/tf-csirt/); the Organisation of the Islamic Cooperation – Computer Emergency Response Team (OIC-CERT: www.oic-cert.net); and the 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. In 2015, Government Computer Emergency Response Team Hong Kong (GovCERT.HK) joined APCERT as an Operational Member. 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 2015, 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	Chinese Taipei

	Response Team	
VNCERT	Vietnam Computer Emergency Response Team	Vietnam

Supporting Members (3 Teams)

- Bkav Corporation
- Dell SecureWorks
- Microsoft Corporation

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

At the APCERT AGM 2015, CERT Australia was elected as the new Chair of APCERT, and Malaysian Computer Emergency Response Team (MyCERT) as the new Deputy Chair. JPCERT/CC was also re-elected as the APCERT Secretariat.

The following teams were elected to/remained on the APCERT Steering Committee (SC).[1]

Team	Term	Other positions
CERT Australia	March 2014 – September 2016	Chair
CNCERT/CC	March 2014 – September 2016	
JPCERT/CC	September 2015 – September 2017	Secretariat
KrCERT/CC	March 2014 – September 2016	
MOCERT	September 2015 – September 2017	
MyCERT	September 2015 – September 2017	Deputy Chair
TWNCERT	March 2014 – September 2016	

3. Working Groups (WG)

There are currently six (6) Working Groups (WGs) in APCERT.

1) Information Sharing WG (formed in 2011)

- Objective:

[1] It was also decided, with regards to the time shift of the APCERT AGM from March to September starting in 2015, that the current Steering Committee's term to be extended for another 6 months, in order for the term to be concluded in September of 2015/2016 respectively.

  - To identify different types of information that is regarded as useful for APCERT members to receive and/or to share with other APCERT members.
- 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

2) Membership WG (formed in 2011)

- Objective:
  - To review the current membership criteria/classes and determine whether the membership should be broadened to include new criteria/classes, and if so how should the new arrangements work.
- 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

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

- Objective:
  - To devise an approach and assist in defining APCERT organisational processes into policies and procedures appropriate to the running of APCERT.
- Convener (1) : CERT Australia
- Members (5): HKCERT, JPCERT/CC, KrCERT/CC, MOCERT, Sri Lanka CERT|CC

  *Operational Framework WG (formed in 2011) was merged into Policy, Procedure and Governance WG in March 2014.

4) TSUBAME WG (formed in 2009)

- Objectives:
  - Establish a common platform for Internet threat monitoring, information sharing & analyses in the Asia Pacific region;
  - Promote collaboration among CERTs/CSIRTs in the Asia Pacific region by using the common platform; and

- Enhance the capability of global threat analyses by incorporating 3D Visualisation features to the common platform.

- Secretariat (1): JPCERT/CC
- Members (23): AusCERT, bdCERT, BruCERT, CamCERT, CCERT, CERT-In, CNCERT/CC, HKCERT, ID-SIRTII/CC, KrCERT/CC, LaoCERT, mmCERT, MOCERT, MonCIRT, MyCERT, PacCERT, PHCERT, SingCERT, Sri Lanka CERT|CC, TechCERT, ThaiCERT, TWCERT/CC, TWNCERT

5) Training WG (formed in 2015)

- Objectives
  - Establish an overall education and training program to assist members to develop, operate, and improve their incident management capabilities.
- 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) Cyber Green WG (formed in 2015)

- Objectives
  - Discuss security metrics in order to identify ways to improve on currently available security metrics.
  - Discuss best practices on clean-up activities as well as data sharing methods. This working group will be in conjunction with OIC-CERT members.
- Convener (1): MyCERT
- Members (14): CNCERT/CC, AusCERT, bdCERT, BruCERT, CERT-In, GovCERT.HK, ID-CERT, JPCERT/CC, MNCERT/CC, TechCERT, ThaiCERT, TWNCERT, VNCERT

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 2015

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 2015, APCERT Teams have hosted, participated and/or contributed in the following events:

- **APCERT Drill 2015 (18 March, 2015)**

  http://www.apcert.org/documents/pdf/APCERTDrill2015PressRelease_Final.pdf

  APCERT Drill 2015, the 11th 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. 25 teams from 19 economies of APCERT (Australia, Bangladesh, Brunei Darussalam, People's Republic of China, Chinese Taipei, Hong Kong, India, Indonesia, Japan, Korea, Lao People's Democratic Republic, Macao, Malaysia, Mongolia, Myanmar, Singapore, Sri Lanka, Thailand and Vietnam), and 3 teams from 3 economies of OIC-CERT (Egypt, Morocco and Tunisia) participated in the Drill. The theme of the drill was "Cyber Attacks beyond Traditional Sources".

- **APEC-TEL 51 (12-16 May, 2015, Boracay, the Philippines)**

  TWNCERT represented APCERT at APEC TEL 51, and presented the APCERT's overview and latest activities for a safer cyber space base on the regional framework.

- **26th Annual FIRST Conference (14-19 June 2015, Berlin, Germany)**

  https://www.first.org/conference/2015

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

- National CSIRT Meeting (20-21 June 2015, Berlin, Germany)

  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 2015 (6-10 September, 2015, Kuala Lumpur, Malaysia)

  http://csm-ace.my/apcert-oiccert2015/index.html

  The APCERT Annual General Meeting (AGM) & Conference 2015 was held on 6-10 September, 2015 at The Royale Chulan, Kuala Lumpur, Malaysia, concurrently with Organisation of The Islamic Cooperation – Computer Emergency Response Teams (OIC-CERT) AGM and Conference.

  Programme Overview:

6 September (Sun)	AM:	Cyber Green Workshop
	PM:	APCERT Working Group Meetings
7 September (Mon)	AM:	APCERT Steering Committee Meeting
	PM:	APCERT AGM 2015
8 September (Tue)	AM:	TSUBAME Workshop
	PM:	APCERT & OIC-CERT Desktop Exercise
9 September (Wed)	AM:	APCERT Closed Conference
	PM:	APCERT & OIC-CERT Steering Committee Discussion
10 September (Thur):		APCERT & OIC-CERT Public Conference

  The AGM & Conference 2015 was the first official event bringing together the APCERT and OIC-CERT communities. It also marked the 12th anniversary of APCERT, providing an opportunity for CSIRTs in the Asia Pacific region, as well as our closely related organisations, to come together and reflect on the cyber threat landscape over the past ten years, share current trends, and also look forward to future challenges and opportunities.

- TSUBAME Workshop 2015 (8 September 2015, Kuala Lumpur, Malaysia)

  The APCERT TSUBAME Workshop 2015 on Network Traffic Monitoring Project was held on 8 September, 2015, in conjunction with APCERT AGM & Conference 2014. For the first time, the workshop welcomed OIC-CERT members. The

workshop was organised by JPCERT/CC to enhance the TSUBAME project and the cooperation among its members.

- **ASEAN CERT Incident Drill (ACID) 2015 (28 October, 2015)**

  ACID 2015, led and coordinated by SingCERT, entered its 10th 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 a cyber espionage scenario in a company, including malware analysis to uncover its characteristics and subsequently escalating to the necessary parties for mitigation.

- **APEC-TEL 52 (19-23 October, 2015, Auckland, New Zealand)**

  TWNCERT represented APCERT at APEC TEL 52, and presented the APCERT's overview and latest activities for a safer cyber space base on the regional framework.

- **6th Asia-Pacific Telecommunity (APT) Cybersecurity Forum (20-22 October, 2015, Bangkok, Thailand)**

  http://www.aptsec.org/2015-CSF6

  As APCERT Chair team, CERT Australia represented APCERT at the 6th APT Cybersecurity Forum. 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 Board of Directors of FIRST.org 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.

1 **Asia Pacific Network Information Security Centre (APNIC)**

  APCERT and Asia Pacific Network Information Centre (APNIC) signed a Memorandum of Understanding during the APCERT AGM & Conference in Kuala Lumpur, Malaysia in September, 2015.

2. APCERT SC Meetings

From January to December 2015, SC members held five (5) teleconferences and two (2) face-to-face meeting to discuss APCERT operations and activities.

28 January	Teleconference
2-3 March	Face-to-face meeting concurrently held with APRICOT 2015 in Fukuoka, Japan
20 May	Teleconference
29 July	Teleconference
19 August	Teleconference
7 September	Face-to-face meeting in conjunction with APCERT AGM 2015 in Kuala Lumpur, Malaysia
20 November	Teleconference

3. APCERT Training Calls

APCERT held six (6) training call in 2015 to exchange technical expertise, information and ideas.

Date	Title	Presenter
4 February	Computer forensics approach to computer compromises and network intrusions	Microsoft

1 April	Introduction and Demonstration to APCERT Data Exchanger (ADE)	CNCERT/CC
3 June	Vulnerability Handling - What goes on and how to use information that comes out of it	JPCERT/CC
5 August	E-mail Driven Financial Frauds	Sri Lanka CERT|CC
7 October	Debugging and Exploiting Security Vulnerabilities on Routers	Bkav Corporation
2 December	Inside the APCERT Drill: Player, Observers, Excon and OC	MOCERT

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. About AusCERT

AusCERT is the premier Cyber Emergency Response Team (CERT) established in Australia in 1993 and a leading CERT in the Asia/Pacific region. AusCERT operates within a worldwide network of information security experts to provide computer incident prevention, response and mitigation strategies for members. As a not-for-profit, self-funded organisation based at The University of Queensland, AusCERT relies on member subscriptions to cover its operating costs. AusCERT is also a member of FIRST.

2. Activities and Operations

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

2.1 Security advisories and 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 2015, 3242 External Security Bulletins (ESBs) and 121 AusCERT Security Bulletins (ASBs) were published. This represents a 26% increase overall when compared with 2014 tallies.

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

2.2 Flying squad service

New in 2015, the Flying Squad Service allows members wanting more than basic telephone or email incident response to access AusCERT's member-only daily rate of $990 (AUD including GST) for a dedicated information security analyst. This service can be delivered on site (member pays travel expenses) or remotely from AusCERT's

office in Brisbane. During 2015 AusCERT performed a number of on site and remote Flying Squad engagements.

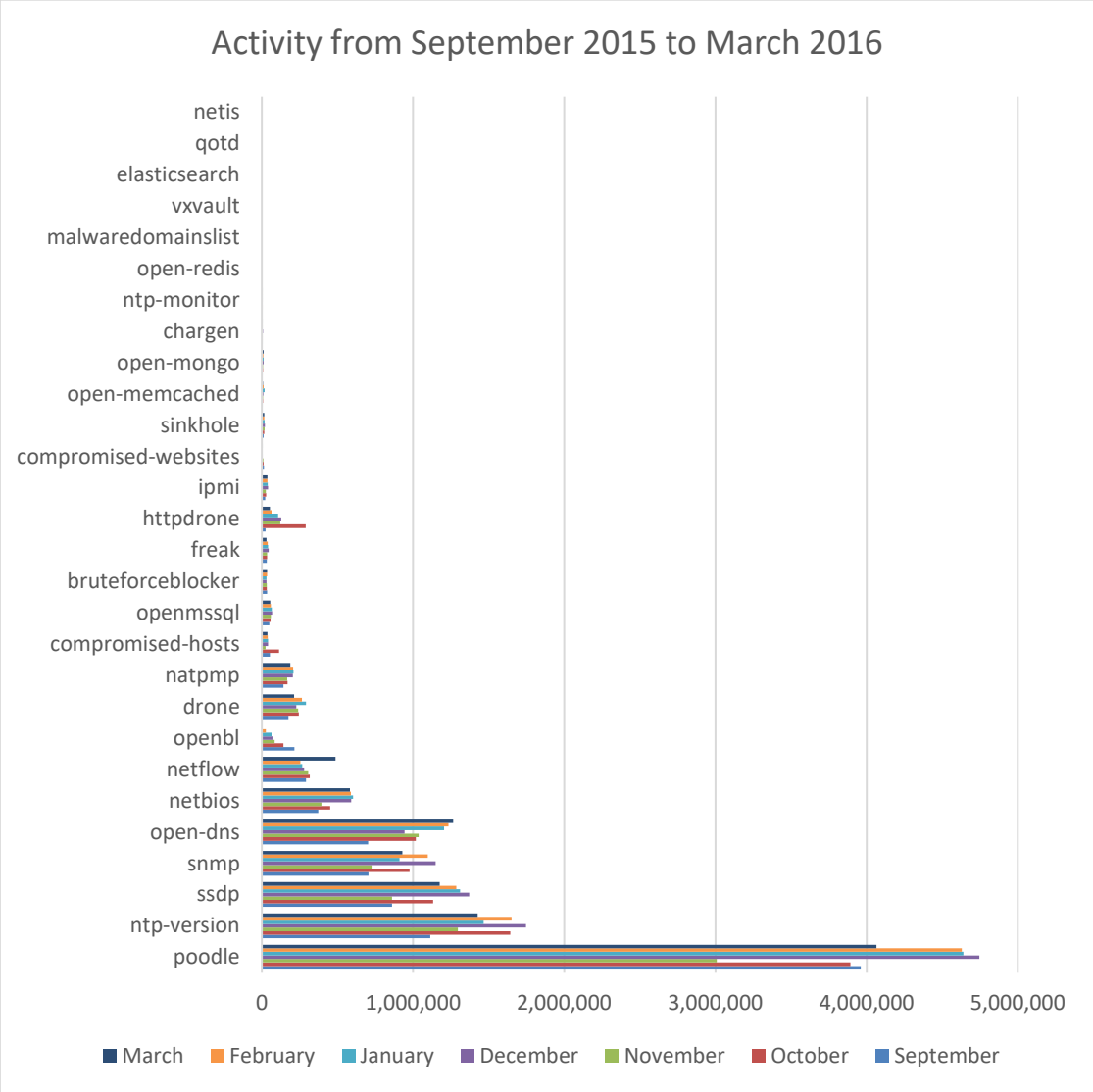
The Flying Squad Service was introduced as a direct result of members' requests for access to trusted, independent information security professionals.

2.3 Incident response

AusCERT coordinates incident response on behalf of its members and generates pro-active reports of incident activity, based on its data collection activities. During 2015 AusCERT introduced the MSIN product featuring highly advanced data collation and processing capability. Members are notified via a daily digest of vulnerabilities (such as POODLE, misconfigured services and open ports) and incidents (such as compromised web sites and stolen credentials) detected from the wide range of open and closed source data that AusCERT processes.

Drawing upon the significant amount of incident data across all industries that AusCERT now has access to, more detailed analysis is expected to be delivered to members, APCERT and the public as AusCERT's capability grows.

The following chart shows some of the incident and vulnerability types along with their relative rates of occurrence during the time since AusCERT's MSIN capability was launched. As expected, POODLE represented the highest number of vulnerabilities during this period.



2.4 Early warning service (EWS)

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.

2.5 Malicious URL feed

AusCERT provides a Malicious URL Feed to members only, containing the output of AusCERT's processing of malware, phishing and other dangerous URLs. This feed is as accurate as possible, as each entry is checked by an analyst instead of relying on automated pattern matching. Additionally malware samples are automatically compared against multiple vendors' detection engines using the Virus Total service, and

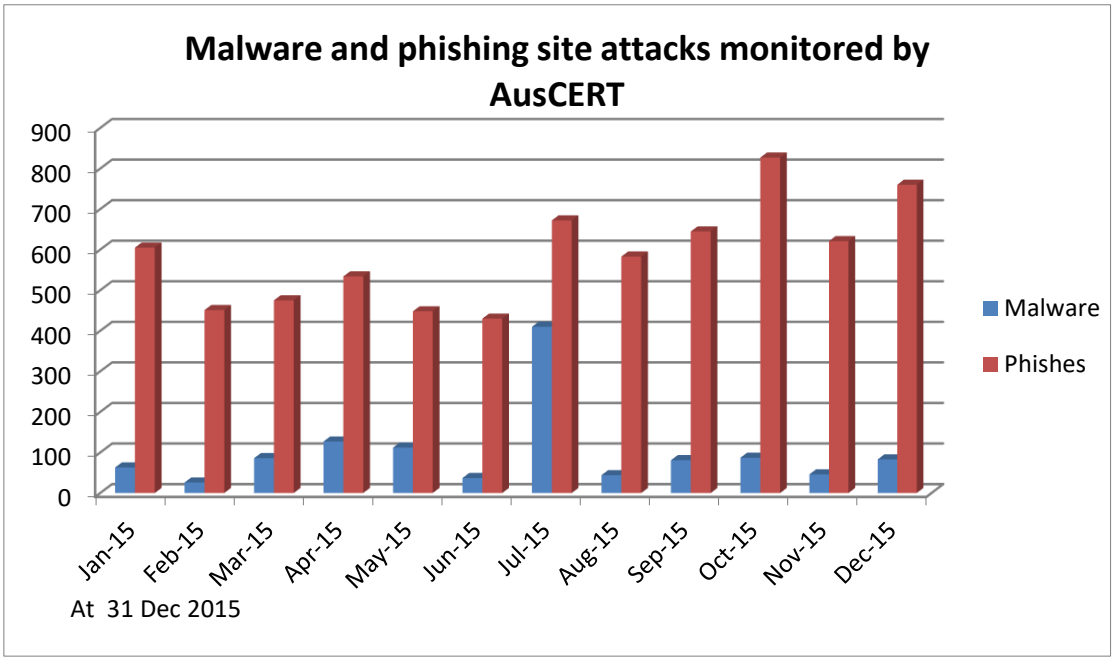
those samples achieving poor detection rates are submitted to as many AV vendors as possible for inclusion in signatures.

2.6 AusCERT remote monitoring service (ARMS)

Members can subscribe to monitor externally facing services such as web, email and DNS for availability. SMS and email alerts are sent whenever unexpected activity is detected. This service provides members early warning of events such as denial of service attacks, or equipment failure.

2.7 Phishing take down service

AusCERT Members can utilise AusCERT's considerably large overseas and local contact network for removal of phishing and malware sites.



2.8 AusCERT IRC channel

An IRC channel is available for AusCERT members to share information, collaborate and contact like-minded information security professionals. Typical conversations during 2015 on this channel usually included information on the latest, ever changing binaries for ransomware attacks.

2.9 Certificate service

AusCERT provides a PKI certificate service to the Australian higher education and research sector. This enables institutions to self-issue SSL, S/MIME and code-signing certificates at a discounted rate.

3. Events

3.1 AusCERT conferences

AusCERT hosts an annual information security conference in Queensland on the Gold Coast, attracting international speakers and attendees. Details here: http://conference.auscert.org.au

Additionally, AusCERT hosts events in various Australian cities.

3.2 Drills

AusCERT participated in the 2015 APCERT drill.

3.3 Events attended

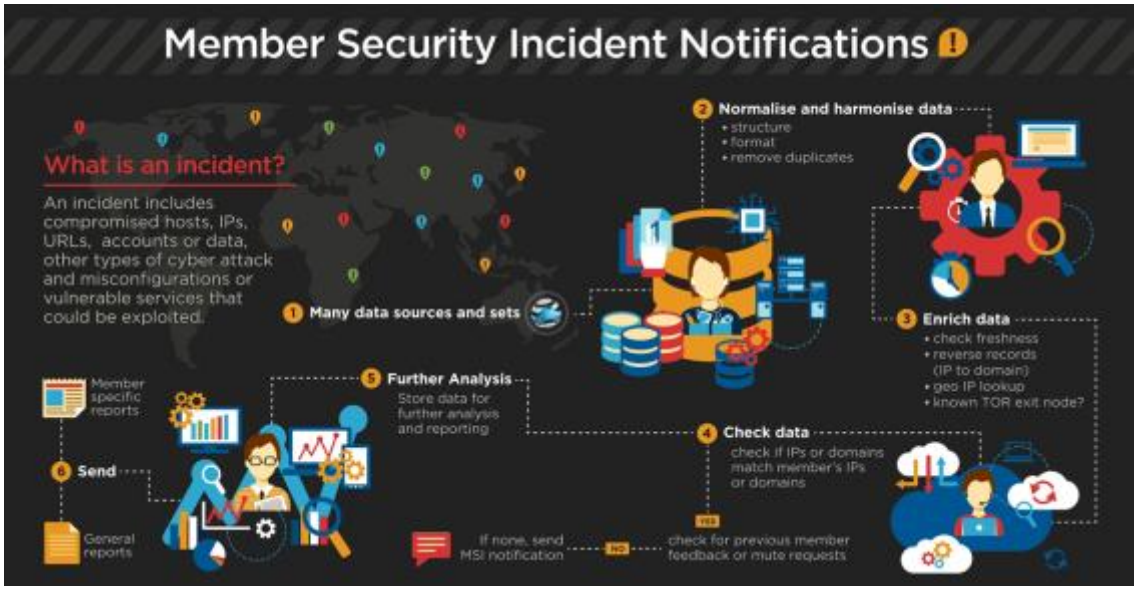
AusCERT attended the following events during 2015:

- APCERT 2015 Conference
- 2015 AISA National Conference
- ACSC Conference 2015
- Ruxcon Security Conference 2015
- FIRST Conference 2015

4. Achievements

4.1 MSINs (Member Security Incident Notifications)

Member security incident notifications (MSINs) provide an improved method to proactively inform members about security incidents affecting members' data, systems or networks and are a daily customised composite security report containing incident notifications relevant to AusCERT member organisations' domains and IP ranges. MSINs are produced from a range of sources and data sets and processing.



5. Future plans and services

AusCERT has responded to member's requests by announcing the "Watching the Watcher" managed security provider review service, expected to launch during 2016.

6. Contacting AusCERT

AusCERT is contactable during Australian Eastern Standard business hours and by its members 24x7.

Email: auscert@auscert.org.au

Web: http://auscert.org.au/

Telephone: +61 7 3365 4417

bdCERT

Bangladesh Computer Emergency Response Team – Bangladesh

1 ABOUT bdCERT

1.1. Introduction

bdCERT is the Computer Emergency Response Team for Bangladesh and is the primary Point of Contact for handling incidents in Bangladesh. We work for improving Internet security in the country.

We provide information about threats and vulnerabilities that could affect the users. We work closely with various organizations and associations such as ISPAB, BASIS, BCS, SANOG, BTRC and Law Enforcement Agencies to stop attacks that are either sourced from Bangladesh or outside.

We provide training and awareness programs on Information Security and issues affecting Internet security in Bangladesh.

1.2 Establishment

bdCERT was formed on July 2007 and started Incident Response on 15th November 2007. bdCERT is initiated by some IT professionals who have long experience in data and Internet communication and technologies industry. It is funded voluntarily with limited resource but highly motivated professionals.

1.3. Workforce power

We currently have a working group of 12 professionals from ISP, Telecommunication, Vendors, University, Media, Bangladesh Internet Exchange (BDIX) & International Internet Gateway (IIG) who are working voluntarily with great enthusiasm and motivation. Some of the major activities that we are involved with, are, Incident Handling, National POC for national and international incident handling, Security Awareness program, Training & Workshops, News Letters, Traffic Analysis, etc.

1.4 Constituency

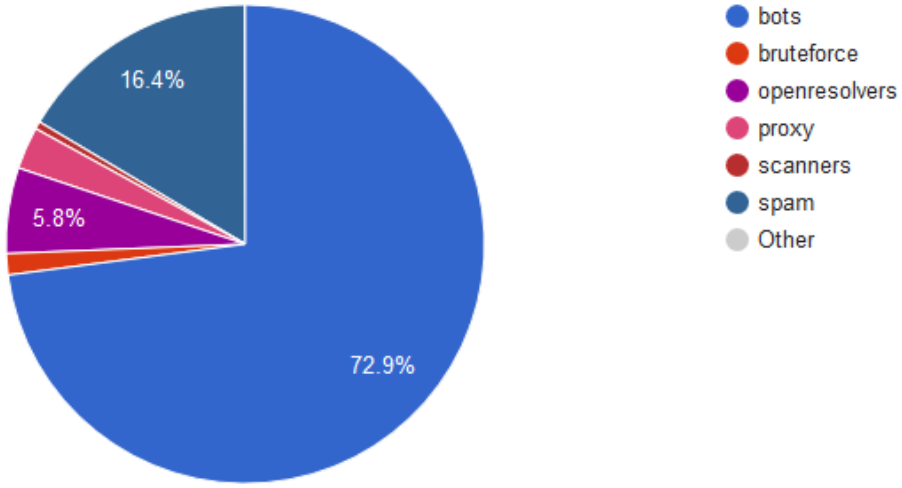
As a national CERT the constituencies of bdCERT are all the Internet users of Bangladesh. We work closely with all the ICT stake holders particularly with ISP

Association of Bangladesh (ISPAB), Bangladesh Association of Software & Information Service (BASIS), Bangladesh Computer Samity (BCS), Bangladesh Computer Council (BCC), Bangladesh Telecommunication Regulatory Commission (BTRC) and various Government Organization, Non Government Organization, Universities and Government Law Enforcement Agencies to mitigate Internet threats.

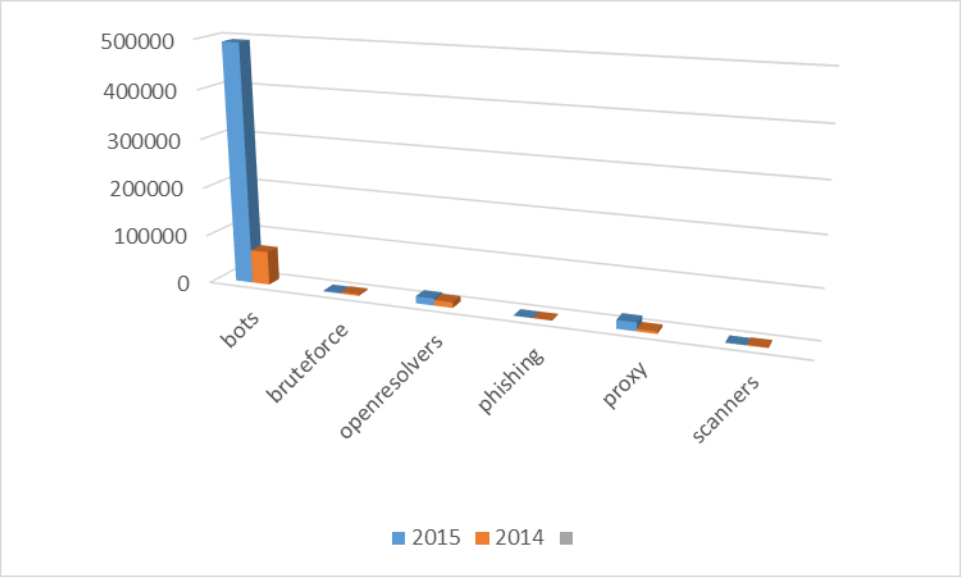
2 ACTIVITIES & OPERATIONS

2.1 Incident handling reports & Abuse Statistics

bdCERT observe significant decrease in total no of incident in year 2015 as compare to the year 2014. bdCERT observe a significant increase of bots which causes DDoS attack and Clickfraud. Beside this bdCERT reported website defacement/hack specially on government website. Most of the cases Content Management System vulnerabilities (especially Joomla & Wordpress) were widely getting exploited for website defacement. Phishing attack also increased and bdCERT continues to work with other CERTs and Internet Service Providers (ISPs) to track down affected users and keep them informed on how to secure their systems.



Taxonomy statistics of incidents report are shown in figure 1. Majority of incidents are related with Bots, Open Proxy, Open Resolvers and proxy.



3 EVENTS ORGANIZED / CO-ORGANIZED

- 18 - 23 May, 2015: bdCERT update at bdNOG 3 conference, Dhaka, Bangladesh.
- 5 - 12 July, 2015: APISC Security Training Course arranged by KrCERT/CC, KISA
- 6 - 10 September 2015: APCERT & OIC-CERT AGM & Annual Conference, Kuala Lumpur, Malaysia hosted by Cyber Security Malaysia.

4 International Collaboration

- bdCERT has become member of APWG in June 2015.

5 FUTURE PLANS & Projects

a) Government Endorsement for BDCERT
b) FIRST membership
c) Building Awareness
d) Fund Raising
e) Consulting to form other CERTs within the constituents

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 –

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.

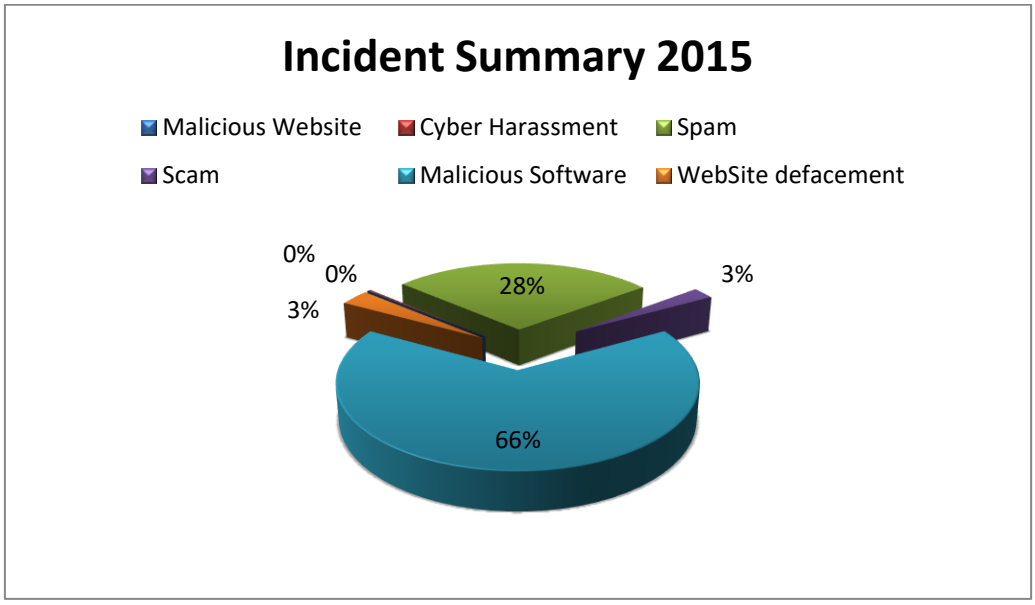


Figure 1

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

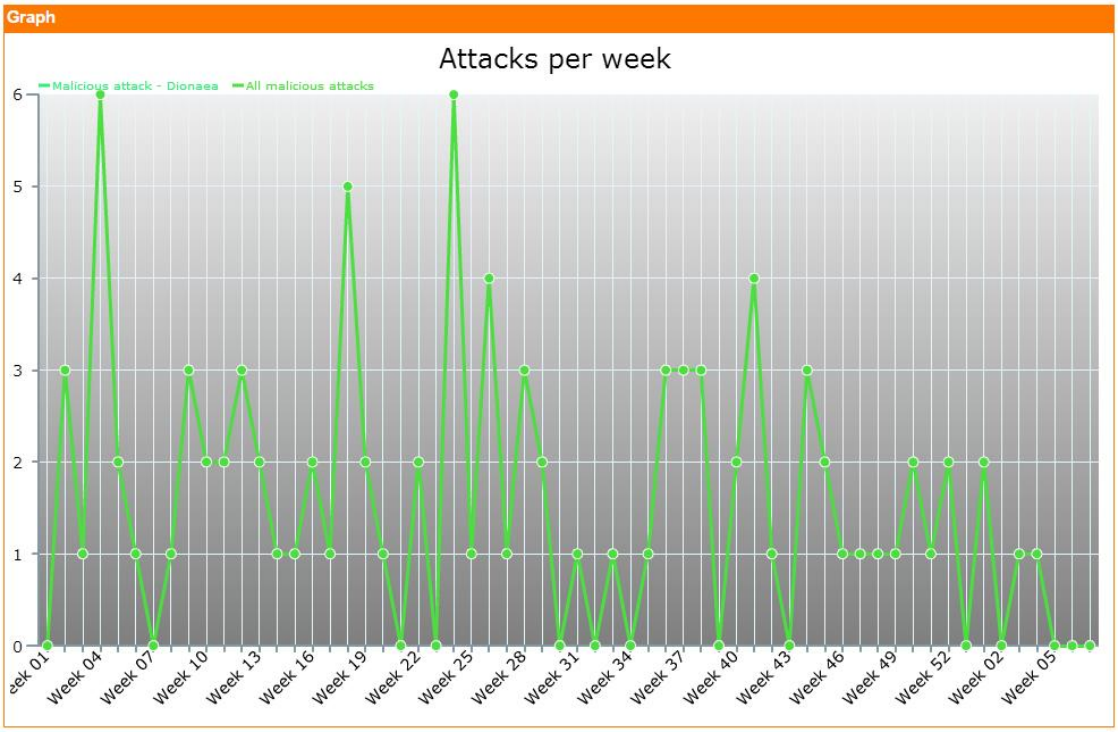
This data shows the overall activities from the honeypot starting from January 2015 until December 2015

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**

  Oct 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 refer to CERNET network security emergency response system. CCERT provides with quick response and technical support services of network security incidents not only for China Education and Research Computer Network and its member units, but also for other social users.

The main works 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 Activities and Operations

2.1 Handling security incidents complaints from CERNET users

In 2015, CCERT handled 4281 security incident complaints, which include: 973 for Spams, 3020 for Website Intrusion, 171 for Port Scanning, 22 for Phishing Site Complaints, 14 for DoS Attack, 31 for System Intrusion and 52 for other network security complains.

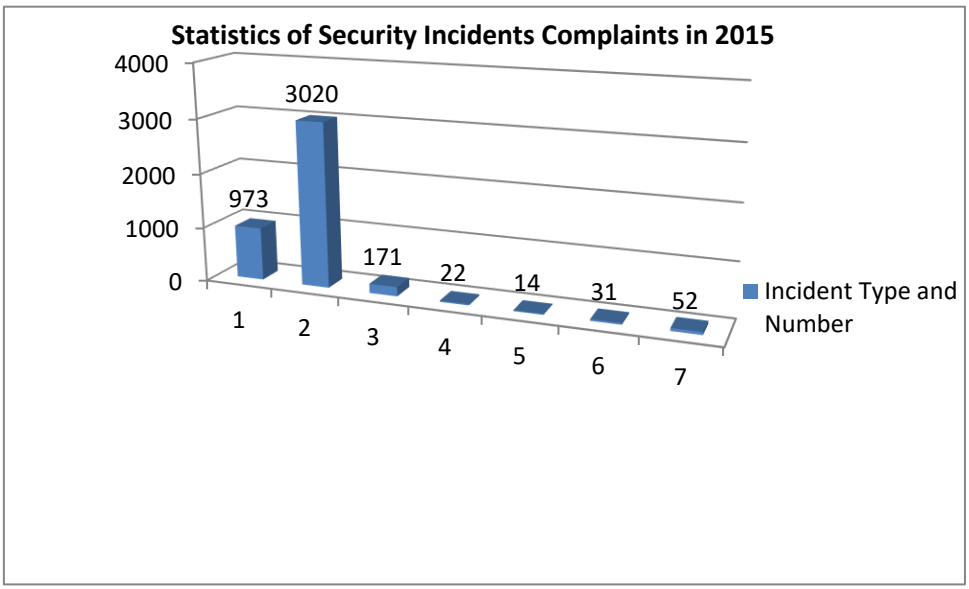


Figure 1

In 2015, CCERT focus on handling the security incident of Website Intrusion. By analyzing the 3020 Website Intrusion incidents handled in 2015, we find the following causes which result in the above website intrusion:

1. SQL Injection Vulnerability
2. Permission Control Vulnerability (Uncontrolled Uploading, Parallel Access Holes etc.)
3. System Vulnerabilities existed in website servers
4. Weak Password Account Vulnerability
5. Information Leakage in Website
6. Cross Site Scripting Vulnerability

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.

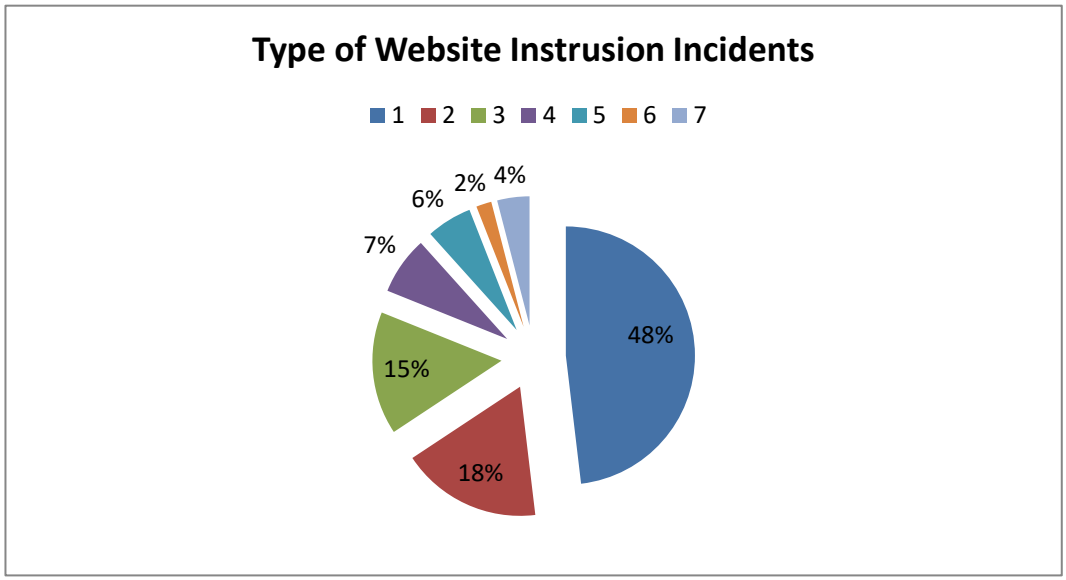


Figure 2

In the past, the compromised websites are mainly used for adding hidden links, while now more and more compromised websites are used for Stealing user information of the compromised websites. In addition, the intrusion incidents which are used to plant political orientation information in the compromised website is increasing.

2.2 Security Monitor and Information Publish

In 2015, through security monitor, CCERT found that, most of the large scale DoS attacks in the CERNET network are still DNS Reflection Attacks, after analyzing the attacking sources we found that, not only the DNS severs 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.

2.3 Technical Consultation and Security Service

In 2015, CCERT provided with free security testing service for 10443 websites, and found that there are about 16677 websites with high-risk vulnerabilities, accounting for 16.06%, 863 websites with middle-risk vulnerabilities, accounting for 8.26%, and 2404 websites with low-risk vulnerabilities, accounting for 23.02%. Only 52.66% of the websites were not detected with security problems.

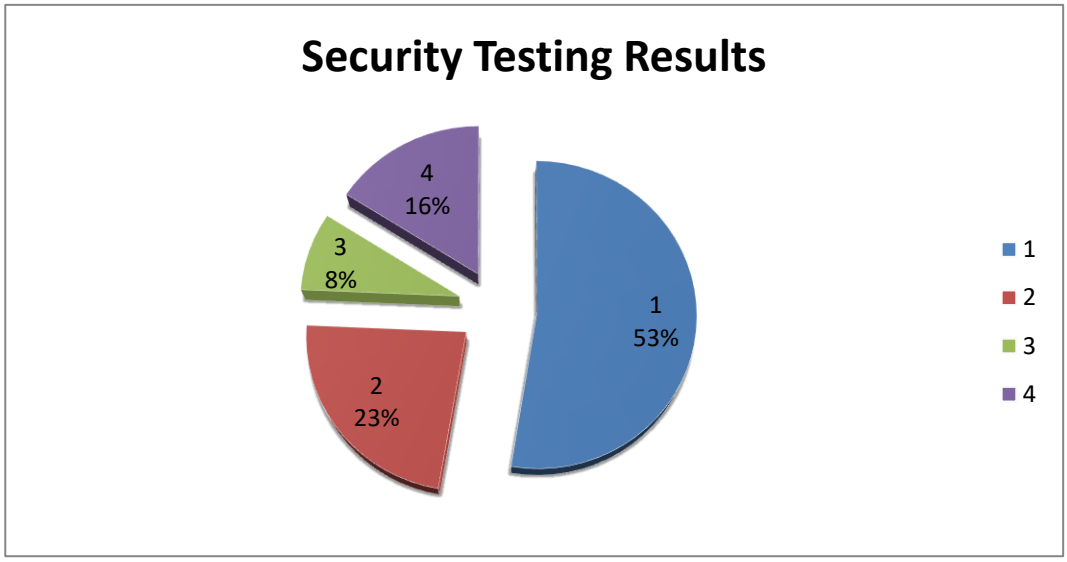


Figure 3

2.4 Security training and activities

In 2015, CCERT hosted 16 security trainings for 1931 participants. The security training contents include:

1. Secure operation and maintenance of applications
2. Ideas and Methods of security management for Campus Network/Enterprise Network
3. How-To for Information Security Classified Protection
4. Exploration and practice of campus website security management
5. Data Visualization Analysis
6. Sharing of campus website platform development and website operation experience
7. Application of Python in the Campus Informatization Construction

3 Future Plans

In 2016, CCERT will continue to focus on network security emergency response work, and strengthen the cooperation with other security organizations to contribute our strength for Internet security.

CERT Australia

CERT Australia – Australia

1 Highlights of 2015

1.1 Summary of major activities

CERT Australia continued its APCERT and other regional and global representational and awareness raising activities in 2015, presenting on cyber security threats, vulnerabilities and information sharing initiatives at the APRICOT Security Track event in Japan in March, FIRST in Germany in June, the APCERT AGM & Conference in Malaysia in September, the Asia Pacific Telecommunity Cyber Security Forum in Thailand in October and Kiwicon in November in New Zealand.

CERT Australia continued to work with its domestic and international partners in advancing information sharing through the STIX-TAXII format and platform, building its capability and partnership base.

1.1 Achievements & milestones

CERT Australia's most significant achievement in 2015 was its election as Chair of the APCERT Steering Committee. Having joined APCERT in 2011 and first been elected to the Steering Committee in 2012, CERT Australia was deeply honoured to succeed JPCERT/CC as Chair of the Committee in September 2015.

2 About CERT Australia

2.1 Introduction – CERT Australia's Mission Statement

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 23 core staff.

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 CERT's to support more effective international cooperation.

Throughout 2015, CERT Australia:

- provided unique cyber security threat and vulnerability information relevant to the Australian private sector; specifically those organisations identified as

SNI and CI, the purpose of which is to assist the private sector to protect their networks

- coordinated, facilitated and performed vulnerability analysis and disclosure, especially where vulnerabilities were identified by Australian stakeholders
- hosted information exchanges with SNI partners that included members of the banking and finance, control systems and telecommunications sectors and enabled government and business to share sensitive cyber-security technical information and experiences in a trusted environment, enhancing the ability of both government and business to understand and respond to Australia's cyber security threat environment
- maintained an awareness of cyber threats facing the private sector, contributing to the ACSC's ability to form a national picture of cyber threats
- responded to incidents involving targeted and untargeted attacks against Australian organisations.

3.2 Incident handling reports

In 2015, CERT Australia had 14,401 cyber incidents reported to it, an increase of approximately 29 per cent from 2014. These incidents required a range of responses depending on their nature. 310 of these incidents specifically affected the CI and other SNI.

3.3 Abuse statistics

In 2015 the Australian Cyber Security Centre (ACSC) published its first Threat Report on the cyber security environment in Australia. The report is available at https://www.acsc.gov.au/publications/ACSC_Threat_Report_2015.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.

In 2015, the ACSC published its first Cyber Security Survey: Major Australian Businesses. Industry data was collected from major Australian businesses that partner with CERT Australia. These businesses underpin the social and economic welfare of

Australia by delivering essential services such as banking and finance, defence industry providers, communications, energy, resources, transport and water.

3.5 New services

In 2015, CERT Australia continued to develop and expand its STIX-TAXII platform for sharing threat information with its partners. It also expanded its Information Exchange program with partners across Australian industry sectors.

4. Events organised/co-organised

4.1 Training

CERT Australia did not deliver a dedicated training program for domestic partners in 2015. However, CERT Australia contributed to the training and awareness raising efforts of Australian organisations through the delivery of presentations on a range of topics including the current cyber threat environment and collaborative information sharing tools such as STIX-TAXII.

4.2 Drills & exercises

CERT Australia also developed and facilitated a range of discussion exercises for its domestic partners, particularly the owners and operators of CI and other SNI. These exercises included raising awareness of cyber security, testing internal incident response procedures, and coordination with external organisations and agencies.

4.3 Conferences & seminars

CERT Australia supported the organisation and conduct of the first Annual ACSC Conference, held in Canberra in April 2015. CERT Australia is part of the Centre, with responsibility for providing cyber security advice and assistance to Australian businesses.

Domestically, CERT Australia also participated in the RuxCon and Breakpoint Conferences in Melbourne in October, and a range of other national and local cyber security conferences and events.

5. International Collaboration

5.1 International partnerships and agreements

CERT Australia has a range of bilateral and multilateral partnerships in place with counterparts in the Asia Pacific region. In addition to these CERT-CERT relationships,

in 2015 CERT Australia also participated in formal Government-Government cyber security dialogues between Australia and India, and Australia and New Zealand.

5.2 Capacity building

CERT Australia was involved in a range of capacity building activities in the region and further afield in 2015.

5.2.1 Training

CERT Australia does not maintain a dedicated training program for cyber security and CERT activities. In 2015 its training activities were limited to awareness raising and some targeted presentations on the cyber security threat environment (from an Australian perspective) and specific collaborative and information sharing tools such as STIX-TAXII.

5.2.2 Drills & exercises

In September 2015, CERT Australia co-facilitated with CyberSecurity Malaysia a discussion exercise for members of APCERT and the Organisation of Islamic Cooperation CERT (OIC-CERT). This was part of the program of events for the APCERT Annual General Meeting (AGM) and Conference and OIC-CERT AGM and Conference hosted concurrently by CyberSecurity Malaysia.

CERT Australia participated in the 2015 APCERT Drill held in February.

In October, CERT Australia joined other members of APCERT in participating in the ASEAN Cyber Incident Drill (ACID) hosted by Singapore

5.2.3 Seminars and presentations

CERT Australia delivered presentations at both the Asia Pacific Regional Internet Conference on Operational Technologies (APRICOT) in Fukuoka, Japan in March and the APCERT Conference in Kuala Lumpur in September.

Throughout 2015, 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 – Finland
- FIRST conference, June – Germany
- Blackhat & DefCon, August – USA

- Asia Pacific Telecommunity Cybersecurity Forum, October - Thailand
- 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

CERT Australia will continue to refine and expand its STIX-TAXII platform for the automated sharing of cyber security threat indicators with partners. In future, CERT Australia hopes to be able to share tools and training with interested APCERT members and other partners in the region.

6.2 Future operations

The Australian Government is finalising a new national Cyber Security Strategy. A key element of this strategy will be the public-private partnership, bringing together government agencies such as CERT Australia through the ACSC, and partners in the business, academic and other non-government sectors. International partnerships and collaboration will also continue to be essential to the operations of CERT Australia and the cyber security in Australia, including through collaborative forums such as APCERT.

7. Conclusion

CERT Australia's mandate is well-established. In Australia, it core mission is to provide cyber security advice and assistance to Australian businesses, particularly CI and other owners and operators of SNI. Internationally, CERT Australia is the national point of contact for the CERT community. Within the region, CERT Australia hopes to continue to be able to contribute to the APCERT vision and mission, including as current Chair of the Steering Committee.

CERT-In

Indian Computer Emergency Response Team – India

1. Highlights of 2015

1.1 Summary of major activities

a) In the year 2015, CERT-In handled 49,455 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, 61628 spam incidents were also reported to CERT-In. Remedial measures for handling incidents were suggested and implemented in coordination with relevant stakeholders.

b) CERT-In is keeping track on latest cyber threats and vulnerabilities. 16 security alerts, 70 advisories and 316 Vulnerability Notes were issued during the year 2015

c) 25 Training programmes on specialized topics in the area of cyber security were organized for constituency

d) Around 9 million botnet infected systems tracked and notifications sent to Internet Service Providers along with remedial measures.

1.2 Achievements & milestones

- 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. 9 such mock drills have been conducted so far.
- CERT-In has initiated actions for setting up of "Botnet Cleaning and Malware Analysis Centre" to detect and enable cleaning of malware infected systems. The project is being implemented in coordination and collaboration with Internet Service Providers (ISPs) and Industry. This would help in enhancing the security of computer systems across the country.
- CERT-In signed a Cooperation Framework with CERT- Australia and MoUs with Cyber Security Malaysia, Singapore Computer Emergency Response Team (SingCERT) and JPCERT/CC, Japan to enable information sharing and collaboration for incident resolution.

2. About CERT-In:

2.1. Introduction

CERT-In is a functional organisation of Department of Electronics and Information Technology, Ministry of Communications 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 is 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 75 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 Govt., 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 2015 is given in the following table:

Activities	Year 2015
Security Incidents handled	49455
Security Alerts issued	16
Advisories Published	70
Vulnerability Notes Published	316
Trainings Organized	25
Indian Website Defacements tracked	26244
Open Proxy Servers tracked	1698
Bot Infected Systems tracked	9163288

Table 1. CERT-In Activities during year 2015

3.3. Abuse Statistics

In the year 2015, CERT-In handled 49,455 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, 61628 spam incidents were also reported to CERT-In.

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

Security Incidents	2015
Phishing	534
Network Scanning / Probing	3673
Virus/ Malicious Code	9830
Website Defacements	26244
Website Intrusion & Malware Propagation	961
Others	8213
Total	49455

Table 2. Breakup of Security Incidents handled

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

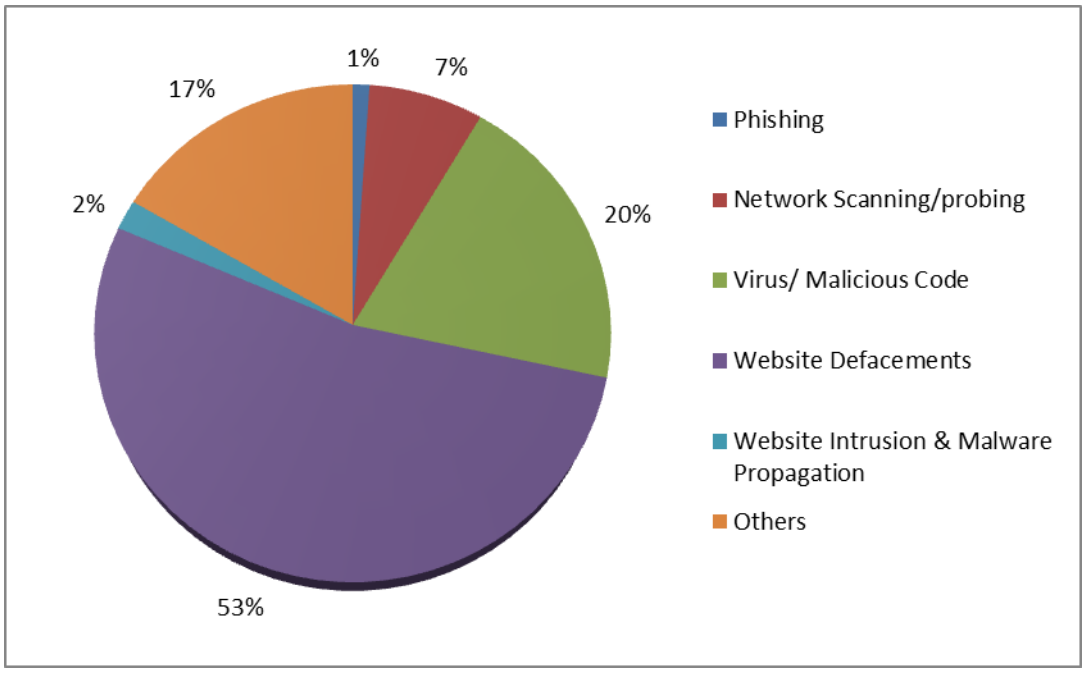


Figure 1. Summary of incidents handled by CERT-In during 2015

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. In all 26244 numbers of defacements have been tracked.

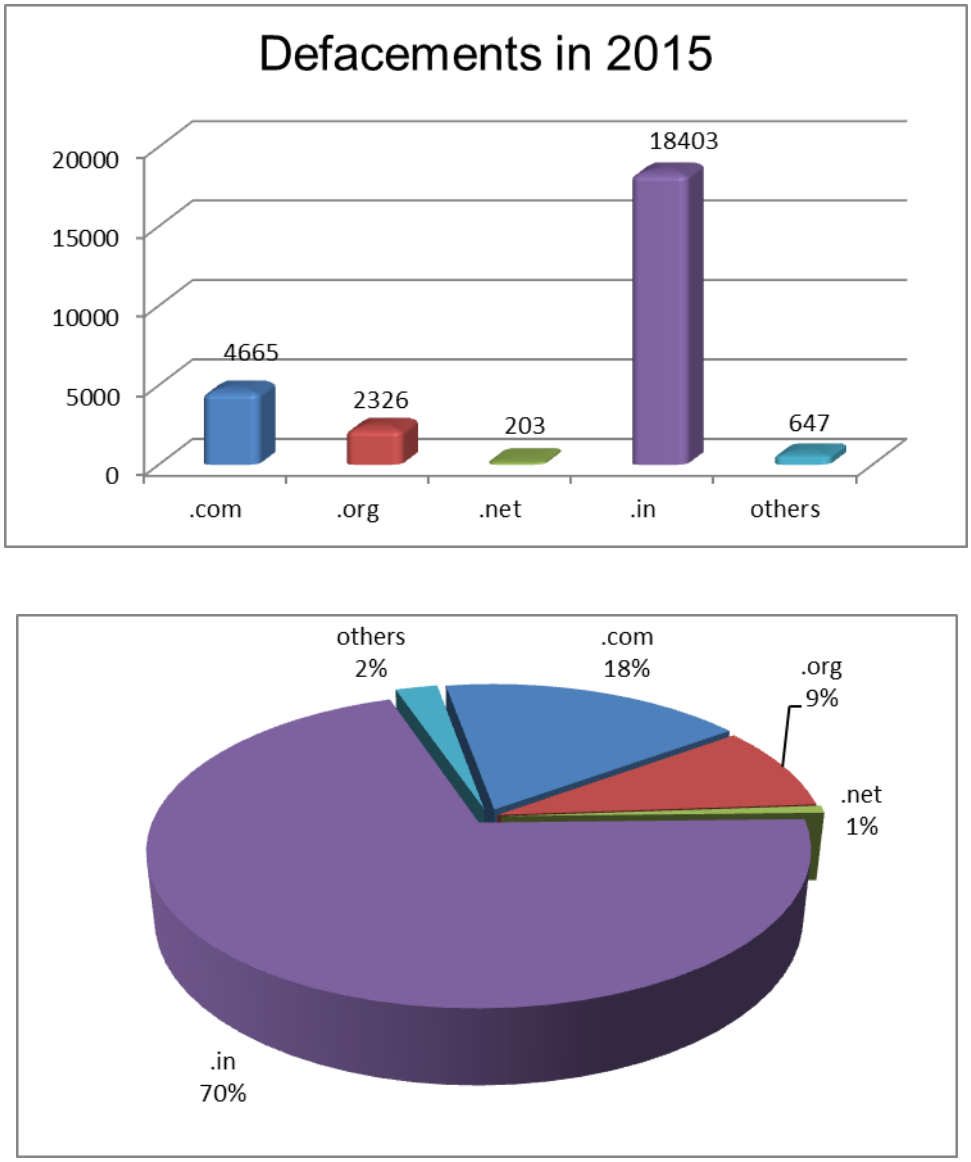


Figure 2: Domain-wise Breakup of Indian Websites Defaced in 2015

3.3.2. Tracking of Open Proxy Servers

CERT-In is tracking open proxy servers existing in India and proactively alerting concerned system administrators to properly configure the same in order to reduce spamming and other malicious activities originating from India. In all 1698 open proxy

servers were tracked in the year 2015. The month-wise distribution of open proxy servers tracked during this year is shown in the figure 3.

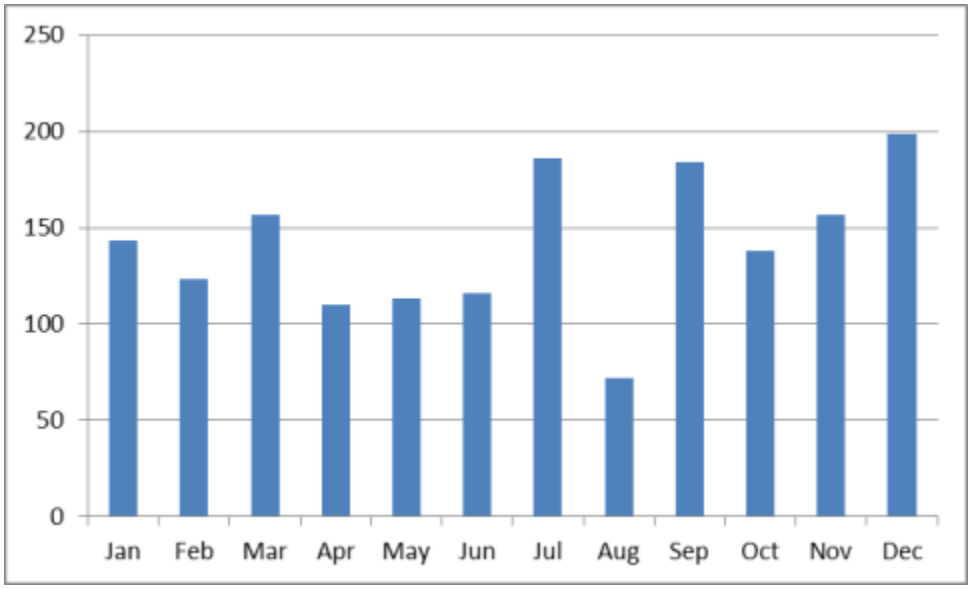


Figure 3. Monthly statistics of Open Proxy Servers in 2015

3.3.3. 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 2015.

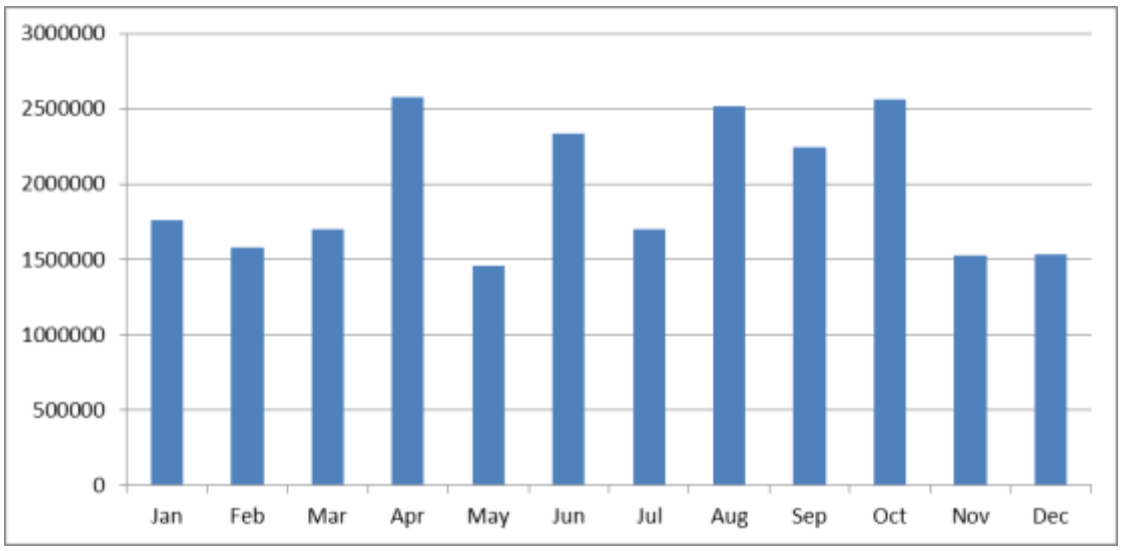


Figure 4. Botnet statistics in 2015

3.4. Publications

Monthly security bulletins: Monthly security bulletin comprises of Statistics of incidents handled by CERT-In, information on vulnerabilities in various Operating Systems and applications tracked, Cyber intrusion trends and other relevant IT security issues.

Summary of Website Defacements depicting break-up of the websites defaced, top defacers and vulnerabilities and suggestions on best practices to secure web applications and web servers is published and circulated to all CISOs on monthly basis.

Security Tips: Security tips for general users advising best practices to secure Mobile Devices, USB storage, Broadband routers, Desktops etc and secure usage of credit/debit cards online, preventive steps against phishing attacks were published.

3.5. New Services

3.5.1. Collaborative Incident resolution

During the year 2015, CERT-In worked in collaboration with security/product vendors and Internet Service Providers in India to detect the botnet infected systems. Botnets such as Sality, ZeroAccess and Dorkbot were tracked through collaborative actions.

3.5.2. Security Profiling, Assurance framework and Audit Services

- CERT-In has provisionally empanelled 57 information security auditing organizations, subject to background verification and clearance of organizations, under the revised process of empanelment for the block 2012-2016, to carry out information security audit, including the vulnerability assessment and penetration test of the networked infrastructure of government and critical sector organizations. The technical competency of the empanelled organizations is regularly reviewed by CERT-In with the help of in-house designed practical skill tests.
- 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

3.5.3. 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 either captured or scanned. CERT-In is analyzing this network traffic information for providing immediate alerts, 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 2015:

- Workshop on "Enterprise Architecture & Security" on January 16, 2015
- Workshop on "Endpoint Security" on January 22, 2015
- Workshop on "Trends in Endpoint Security" on January 23, 2015
- Workshop on "Linux Security" on February 09, 2015
- Workshop on "Cyber Crime & Cyber Forensics" on February 26, 2015
- Workshop on "Cyber Security Threats and Mitigation" on March 05, 2015
- Workshop on "Advanced Persistent Threats" on April 10, 2015
- Workshop on "Phishing Attacks and Countermeasures" on April 24, 2015
- Workshop on "Advanced Web Application Security" on May 22, 2015
- Workshop on "Big Data Analytics & Security" on June 25, 2015
- Workshop on "Cyber Security Threats and Countermeasures" on July 30, 2015
- Workshop on "Mobile Forensics" on July 03, 2015
- Workshop on "Cloud Security" on July 17, 2015
- Workshop on "Data Leakage Detection & Prevention" on July 30, 2015
- Workshop on "Advanced Threats Prevention" on August 07, 2015

- Workshop on "Network Security" on August 24, 2015
- Workshop on "Web Application Security" on September 30, 2015
- Workshop on "Auditing and Testing of Windows Active Directory & Domain Controller Environment" on October 16, 2015
- Workshop on "Crisis Management Plan, Compliance & Auditing" on October 26, 2015
- Workshop on "Cyber Security Threats and Mitigation" on November 04, 2015
- Workshop on "Vulnerability Assessment & Penetration Testing" on November 27, 2015
- Workshop on "Latest Cyber Security Threats & Mitigations" on December 11, 2015
- Workshop on "Mobile Security" on December 18, 2015
- Workshop on "Cyber Crime Investigations" on December 21, 2015
- Workshop on "Cyber Crime Investigations" on December 21, 2015

4.2 Drills and exercises

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. 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 9 Cyber security drills of different complexities with organizations covering various sectors of Indian economy i.e. Finance, Defence, Space, Atomic Energy, Telecom/ISP, Transport, Power, Petroleum & Natural Gas, and IT / ITeS / BPO industry.

5. International collaboration

5.1. International Partnerships and agreements

- CERT-In signed a Cooperation Framework with CERT, Australia and MoUs with Cyber Security Malaysia, Singapore Computer Emergency Response Team (SingCERT) and JPCERT/CC, Japan to enable information sharing and collaboration for incident resolution.
- CERT-In has established collaborations with international security organisations and CERTs to facilitate exchange of information related to latest cyber security threats and international best practices. CERT-In is a member

of Forum of Incident Response and Security Teams (FIRST), APCERT and Anti-Phishing Working Group (APWG).

- Collaborating with overseas CERTs such as US-CERT, for information exchange and Joint cyber exercises.

5.2. Drills & exercises

CERT-In successfully participated in the ASEAN CERTs Incident Handling Drill (ACID 2015) held in October 2015 and APCERT Drill in March 2015.

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.
- Creation of facilities to detect and clean the Botnet infected systems in coordination with Industry
- Promotion of R&D activities in the areas of attack detection & prevention, Cyber Forensics and malware detection & prevention.
- Development and 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

1.6 Incident handling

In 2015, CNCERT received a total of about 126.9 thousand incident complaints, a 125.9% increase from the previous year. And among these incident complaints, 492 were reported by overseas organizations, making a 44.0% drop from the year of 2014. As shown in Figure 2-1, most of the victims were plagued by phishing (59.8%), vulnerability (20.2%) and website defacement (9.8%). Phishing overtook vulnerability to be the most frequent incident complained about.

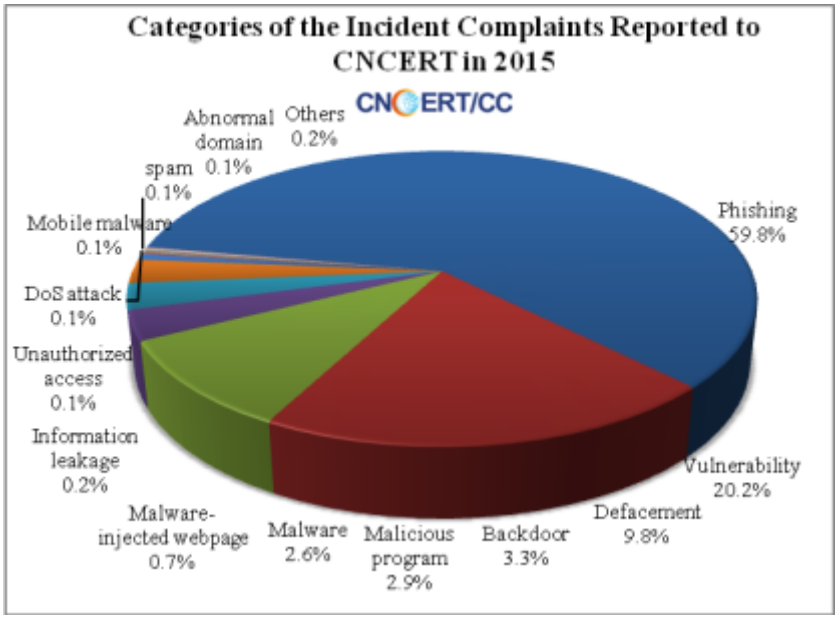


Figure 2-1Categories of the Incident Reported to CNCERT in 2015

In 2015, CNCERT handled almost 125.8 thousand incidents, a significant rise of 124.4% compare with that in 2014. As illustrated in Figure 2-2, phishing (59.7%) dominated the categories of the incidents handled by CNCERT in 2015, followed by vulnerability (20.2%) and website defacement (9.8%).

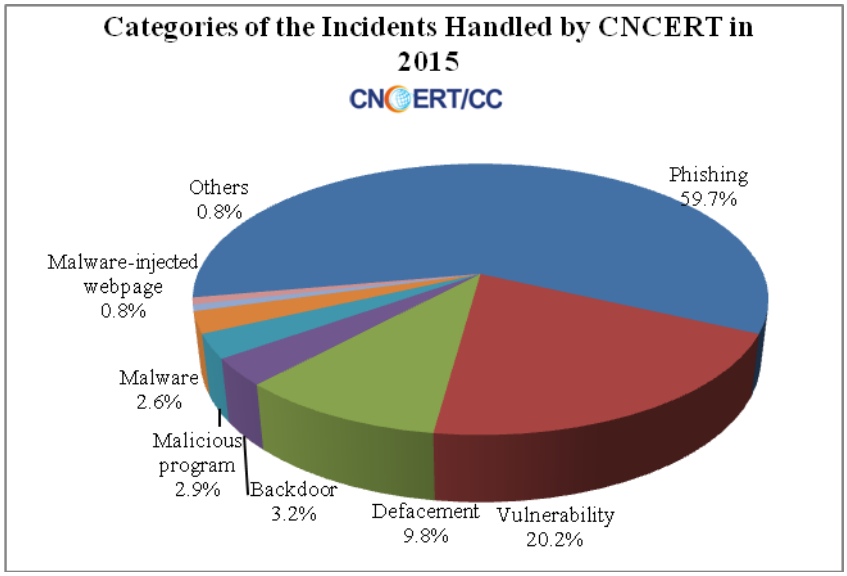


Figure 2-2 Categories of the Incidents Handled by CNCERT in 2015

1.7 Internet Threats

1.7.1 Malware Activities

In mainland China, IPs of the hosts infected with Trojan or Botnet reached about 19.8 million, which increased by 78.4% compared with that in 2014. We saw more than 64.3 thousand oversea C&C servers which increased 51.8% from 2014. As shown in Figure 2-3, the US hosted the largest number of oversea C&C servers' IPs of Trojan or Botnet, followed by Chinese Taibei and Germany.

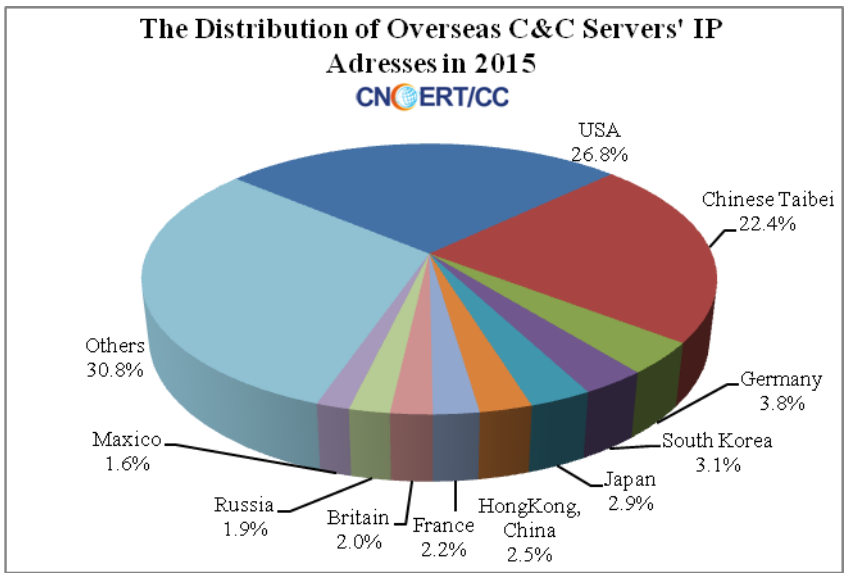


Figure 2-3 The Distribution of Overseas C&C Server's IP Addresses in 2015

By CNCERT's Conficker Sinkhole, over 33.6 million hosts were suspected to be infected all over the world. And 4.2 million compromised hosts were located in mainland China. As shown in Figure 2-4, mainland China (12.4%) had the most infection, followed by India (7.1%), and Brazil (7.0%).

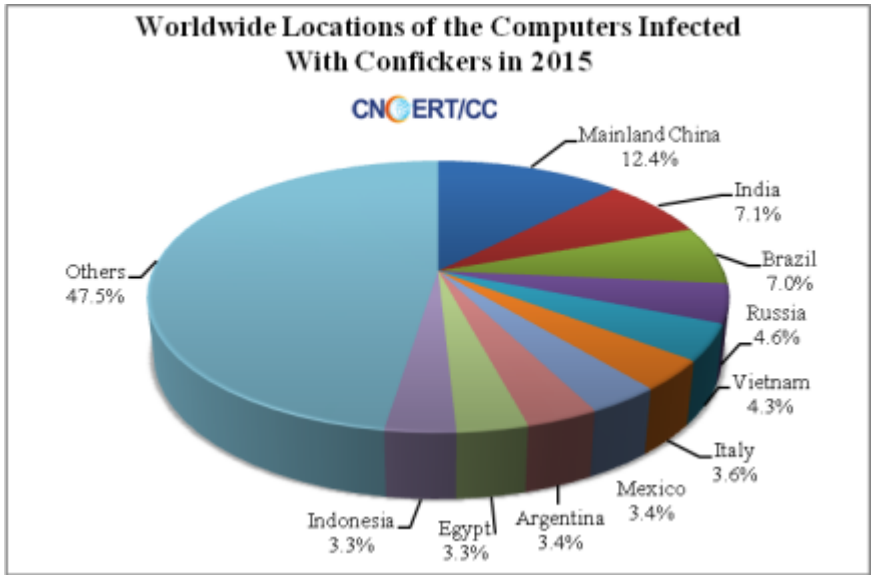


Figure 2-4 Worldwide Locations of the Computers Infected With Confickers in 2015

The malware-hosting website is the jumping-off place for malware propagation. The malware-hosting websites monitored by CNCERT in 2015 involved about 8.3 thousand domains, about 3.7 thousand IP addresses and about 105 thousand malware download links. Among the 8.3 thousand malicious domains, 55.9% of their TLDs fell into the category of .com. Among the 3.7 thousand malicious IPs, 28.8% were located overseas. In 2015, CNCERT monitored about 6.8 million malware spreading incidents. Figure 2-5 depicts the monthly statistics of malware spreading incidents in 2015, with the most rampant malware activity in October.

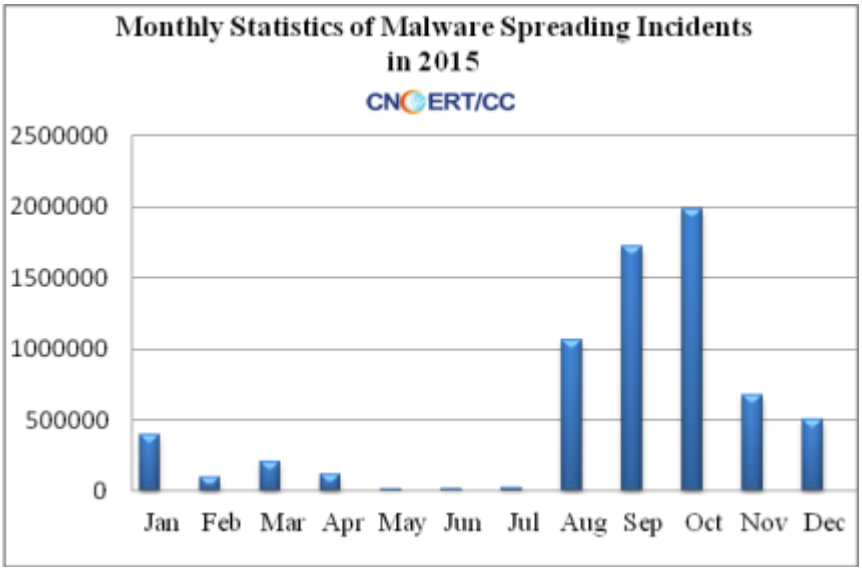


Figure 2-5 Monthly Statistics of Malware Spreading Incidents in 2015

1.8 Website Security

About 24.6 thousand websites in mainland China were defaced, a decrease of 33.6% compare with that in 2014, including 898 government sites. Besides, about 75.0 thousand websites in mainland China were detected to be planted with backdoors and secretly controlled, including 3,514 government sites.

In 2015, CNCERT found about 184.6 thousand phishing sites targeting the websites in mainland China. About 20.5 thousand IPs were used to host those fake pages. About 83.2% were out of mainland China. Most of the phishing servers (32.6%) were located in China HongKong.

CNCERT found almost 31.3 thousand overseas IPs conducted remote control on over 60.2 thousand websites in mainland China. As shown in Figure 2-6, 4361 (13.9%) were located in the US, followed with 2051 (6.5%) in Hongkong, China and 1871 (6.0%) in South Korea.

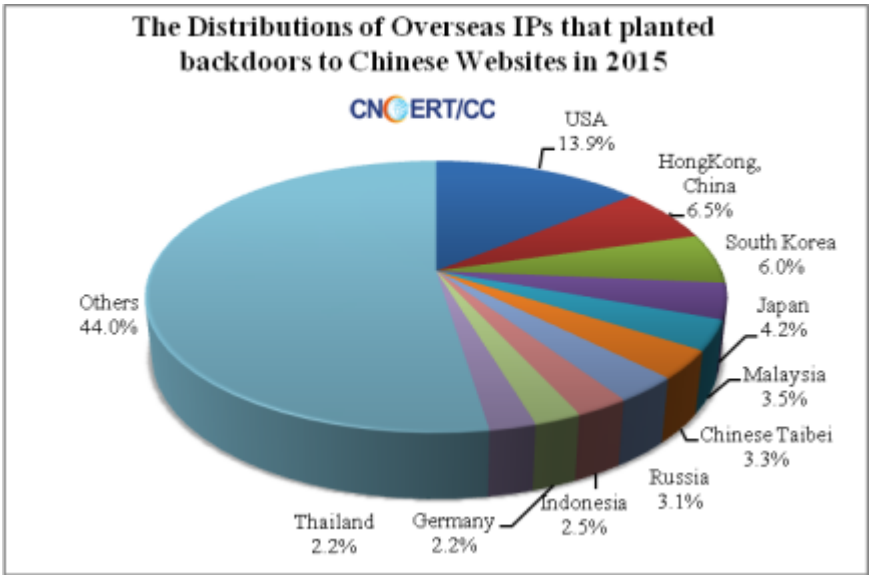


Figure 2-6 The Distribution of Overseas IPs that Planted Backdoors to Chinese Websites in 2015

1.9 Mobile Threats

In 2015, CNCERT collected about 1.48 million mobile malware samples in total. In terms of intentions of these mobile malware, the malicious fee-deducting malware continued to take the first place (23.6%), rogue behavior (22.2%) stood the second place. And followed it were those intended for remote control and resource consumption accounting for 15.1% and 9.7% respectively.

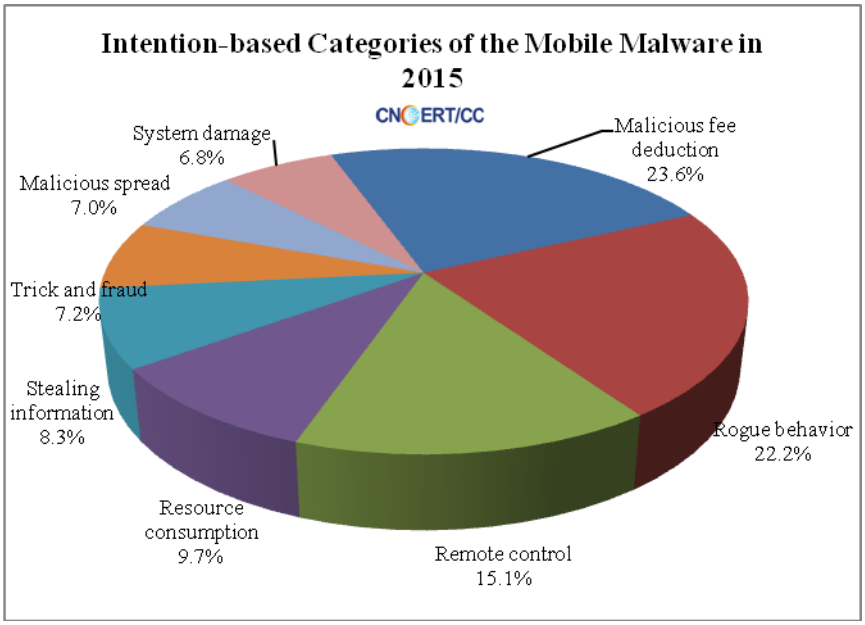


Figure 2-7 Intention-based Categories of the Mobile Malware in 2015

The majority of these mobile malware identified by CNCERT ran on Android platform, recording about 1.47 million (99.7%).

3. Events Organized/Co-organized

3.1 Conferences

The issue of "A Review of Network Security Situation in 2014"

CNCERT gave a press conference on 2014's Network Security Situation in Beijing on 30th April, 2015, introducing the overall picture and main features of China's network security in 2014. Specialists and representatives from more than 30 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 2014, looked forward to threats of much concern in 2015 and made a number of suggestions.

The hold of 2015 Annual Chinese Conference on Computer and Network Security in Wuhan, Hubei Province

CNCERT held 2015 Annual Chinese Conference on Computer and Network Security in Wuhan Hubei from May 26th to 28th, 2015. The theme of the conference is "Intelligent Network with Security Escort". Sub-Forums had been set up according to the four subjects: Environment Governance of Network Security, Intelligent Network Security, Network Security and Life, and CNCERT-CIE Network Security Forum. More than 700 representatives from governments, important information systems departments, industries and enterprises, universities, research institutes and other organizations attended the meeting.

The hold of the third 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 Tokyo, Japan to hold the third China-Japan-Korea Annual Meeting for Cyber Security Incident Response from August 24th to 25th, 2015. One of the key achievements this year was the evaluation of joint emergency incident handling cases using evaluation metrics, which effectively proved that the cases were handled

successfully in a timely and appropriate manner. The parties reassured to enhance the existing cooperation by: engaging in ongoing efforts to improve cyber health, including malware cleanup, through sharing of Indicators of Compromise (IOC), cyber risk condition measurement and mitigation action; further exploring each party's capacity and approach to incident handling; seeking further opportunities for face-to-face and/or online meetings and trainings.

The hold of The 7th China-ASEAN Network Security Seminar in Beijing

CNCERT organized the 7th China-ASEAN Network Security Seminar in Beijing, China from November 3rd to 5th, 2015. Delegates from the telecom department of government and CERTs in Cambodia, Indonesia, Lao, Myanmar, the Philippines, Thailand, Viet Nam, Malaysia and Singapore attended this conference. They 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 2015

CNCERT participated in the APCERT 2015 Drill as a participant on 18 March 2015 and completed it successfully.

The theme of the APCERT Drill 2015 was "Cyber Attacks beyond Traditional Sources". The focus of the drill is to prevent large-scale network attacks against government by the use of home router vulnerability through collaboration between CSIRT-CERT locally and internationally.

This walkthrough is designed to test the participating teams' incident response handling arrangements. The CSIRT teams from 19 economies of APCERT took part in the exercise.

ASEAN CERT Incident Drill (ACID) 2015

CNCERT participated in the ASEAN CERT Incident Drill (ACID) 2015 on October 28th and completed it successfully. 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 2015.

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 2015

1.1 Summary of major activities

In 2015, EC-CERT has been provided multiple security services, and come out PII protection reference guideline as well as have adapted of correctly manner in taking care of incident handling and security protection. EC-CERT also provided EC industry security consulting, incident investigation and response prevent series of PII leakage and hacking.

In the other hand, EC-CERT works with other CERT and regular attend activity of APCERT to receive up-to-date security information and skill. EC-CERT share useful knowhow via alert inform membership.

2. About EC-CERT

2.1 Introduction

EC-CERT stands of "Electronic Commerce - Computer Emergency Response Team", which is long term project supported by Ministry of Economic Affairs of ROC. EC-CERT main job is included information security consulting service and website vulnerability inspection and penetration testing and security incident investigation and response as well as security alert notice。 EC-CERT offers those services in order to prevent E-fraud behavior caused monetary loss and keep 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.

2.3 Resources

Human resource: -

Head of Organization – 1

- Incident Handler – 2

- Analyst – 1

2.4 Constituency

EC-CERT mainly in Taiwan 's electrical business is counseling objects , respectively as a platform , logistics providers and service provider , counseling by electronic commerce to enhance information security protection in case of external attack.

3. Activities & Operations

3.1 Scope and definitions

EC-CERT recorded 65 E-Commerce industry information security reporting in 2015. Those reports including website system security on line consulting records and step by step real case resolution procedures and suggestions.

3.2 Incident handling reports

EC-CERT provided 35 times on line consulting. 35 times event investigation, 30 times event response, 70 times alert, 129 times information exchange with other CERT.

3.3 Abuse statistics

3.4 New services

Joined with Criminal Investigation Bureau while event investigation and response.

4. Events organized / hosted

4.1 Training

Information security training 35 people

4.2 Drills & exercises

4.3 Conferences and seminars

Information security promotion activities * 2

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

E-commerce trust SA Annual meeting * 1

Participation Asian PKI Union Conference * 2

5. International Collaboration

5.1 International partnerships and agreements

5.2 Capacity building

5.2.1 Training

Attended one CEH course got one license and two ECSA courses and got two licenses.

Attrition Forensics for incident response and investigation.

20150603_JPCERTCC_Vulnerability Handling

5.2.2 Drills & exercises

APCERT Drill 2015

5.2.3 Seminars & presentations

APCERT AGM & conference 2015

5.3 Other international activities

6. Future Plans

6.1 Future projects

E-commerce industry lost PII resulting in consumer fraud cases is frequently, how to help E-commerce industry conduct prevention work, deal with detail during progress and fulfill improvement is key point of EC-CERT 2016.

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 2015

1.1 Summary of Major Activities

On 1 April 2015, the Government Computer Emergency Response Team Hong Kong, GovCERT.HK, was formed and officially commenced its services 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 step up collaboration with local and global Computer Emergency Response Teams (CERTs) to bolster cyber security capabilities of the territory.

1.2 Achievements and Milestones

As a new governmental CERT organisation, the GovCERT.HK proactively attended the NatCSIRT 2015, FIRST Annual Conference 2015, and APCERT AGM & Conference 2015, and subsequently succeeded in registering as a national CERT of CERT/CC, and joining as a full or operational member of FIRST and APCERT respectively.

Since its establishment, the GovCERT.HK has built up close working relationship with the CERT community and has been working smoothly on handling alleged security threats and imminent cyber attacks.

2. About GovCERT.HK

2.1 Introduction

The Government Computer Emergency Response Team Hong Kong, GovCERT.HK, is a governmental CERT responsible for coordinating incident response for the HKSAR Government.

Locally, the GovCERT.HK works closely with the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) on sharing of threat information and organising public awareness activities. The GovCERT.HK focuses on

government-related matters while the HKCERT provides incident response related services to all ICT users in the HKSAR covering public and private sectors as well as individuals.

Globally, the GovCERT.HK collaborates with the CERT community in sharing of 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

The GovCERT.HK was formed in April 2015 through consolidation of different internal IT security teams within the Office of the Government Chief Information Officer (OGCIO) of the HKSAR Government.

2.3 Resources

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

2.4 Mission and Constituency

Being the governmental CERT, the 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's information infrastructure and data assets.

3. Activities and Operations

3.1 Scope of Services

The 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 capability; and engaging global CERT community with a view to enhance information and cyber security in the region.

3.2 Incident Handling Reports

In 2015, the GovCERT.HK have received and handled various types of information security incidents that are related to HKSAR Government installations. The issues varied from vulnerable websites, malware infection, web defacement, distributed denial-of-service (DDoS) attack, fraudulent emails, unauthorized access and loss of computing devices.

3.3 Alerts and Advisories

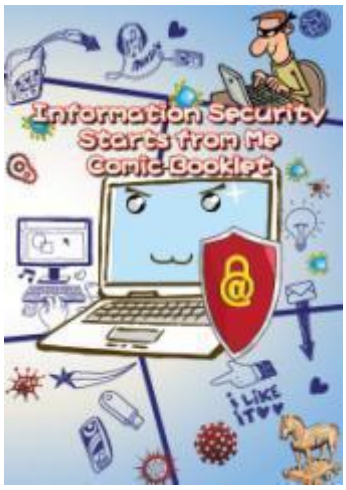
Since the establishment of the GovCERT.HK in April 2015, the GovCERT.HK issued 62 product security alerts, eight security reminders, and one security advisory requesting the disablement of SSLv3 protocol.

3.4 Publications and Mass Media

To raise public awareness and knowledge on the importance of information security, we resorted to different promotion channels to reach out to our target audience and collaborated with the industry players during the process.

- In order to raise the awareness of youth, information security promotional materials such as leaflets, booklets, and posters were distributed to all primary and secondary schools in Hong Kong and Scout Association of Hong Kong.
- Radio episodes entitled "e-World Smart Tips" were broadcasted to help the public to understand more about information security in various aspects and raise the public awareness on information security. On each month, the radio episode featured a different theme and associated tips subject to the recent security incidents or foreseeable cyber threats. For instance, the tips of "Beware of Online Traps for Holidays" were broadcasted in December 2015 to remind the public about cyber traps before the Christmas.

- "Information Security Starts from Me" Comic Booklet with practical cyber security tips was published at the Cyber Security Information Portal to encourage readers to understand more on information security risks and the preventive measures while enjoying the comics. (www.cybersecurity.hk/en/resources.php)



- Leaflets were also produced with different promotion themes.

- Social media, including Twitter and Facebook, were used to share news on information security and promote upcoming security seminars and events.
- Security alerts and advisories were published on the GovCERT.HK website (www.govcert.hk) to provide latest information on security threats and vulnerabilities for the public to take appropriate actions in response.

4. Events Organized / Hosted

With the objectives to continuously enhance information and cyber security capabilities of the HKSAR Government, the GovCERT.HK regularly organises awareness training and solution workshops to share latest knowledge on security measures, best practices, skills and security solutions with government users.

4.1 Training

Over 12 security awareness seminars and training were organised in 2015 to ensure

that government staff remains vigilant in protecting their systems and safeguarding sensitive information.

- 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 anti-DDoS solutions
- Seminars were organised for departmental IT security officers to refresh their security knowledge and update them on the Government's latest approaches in dealing with cyber security threats and adopting mitigation measures.
- Professional web application security training and sharing sessions for government IT staff were arranged. The sessions specifically addressed common weaknesses of websites and web applications, and offered practical advice on the corresponding improvement measures to upkeep information security at a high level.

4.2 Drills and Exercises

The GovCERT.HK actively coordinated government departments to conduct cyber security drills to assess the participants' capabilities of incident analysis, the standing incident response procedures with a view to enhancing the overall incident response capabilities. In 2015, we conducted eight drill exercises involving different government departments and their respective services contractors.

4.3 Conferences and Seminars

In 2015, the GovCERT.HK adopted the slogan "Cyber Security is Everywhere" as the key message to government users and the public. The target audience included businesses especially small and medium enterprises (SMEs), organisations, schools, and general public.

- Two seminars were organised under the "Build a Secure Cyberspace"

campaign in April and November 2015, aiming to promote public awareness of information security and the adoption of security best practices. The one-day seminar in November 2015 has 13 sessions covering trends in cyber crimes, information security challenges, threats related to mobile banking, mobile and smart device security, cloud security, and security measures to combat cyber attacks.

- A security seminar with the theme of "Cyber Crime Prevention, Information Security Best Practice for SME and e-Commerce" was conducted to raise the awareness of SMEs in cyber crimes and share information security best practices in September 2015.
- 25 seminars were conducted at primary and secondary schools from June 2015 to December 2015 for 10,870 teachers, parents and students to raise their awareness of cyber security and enhance their knowledge of protecting personal information.
- A graphic design contest with the theme "Cyber Security is Everywhere" was organised from June 2015 to October 2015 to promote public awareness of information security and security best practices, and appeal to the public to be vigilant and thereby avoid falling into the trap of criminals. The winning entries of the contest were posted at the Cyber Security Information Portal to continue the promotion effect (www.cybersecurity.hk/en/contest-2015.php).
- A talk was delivered at a seminar of Mass Transit Railway Corporation in July 2015 to raise their awareness of phishing and ransomware and provide advice on protection against those attacks.

5. Local and International Collaboration

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

5.1 Local collaboration

To raise public awareness, the GovCERT.HK collaborated with the HKCERT and security service providers to gather information on security vulnerabilities and timely issue alerts on malicious cyber activities to the public and private sectors.

The GovCERT.HK also steered the Internet Infrastructure Liaison Group (IILG) with members from Internet infrastructures (including Hong Kong Internet Exchange, and the Hong Kong Internet Registration Corporation Limited), major Internet service providers, and stakeholders to closely monitor the Internet operation status with a view to mutually alert on abnormal activities.

5.2 International Collaboration

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

The GovCERT participated in the following activities in 2015:

- Attended NatCSIRT Annual Technical Meeting and registered as a national CSIRT in June 2015.
- Attended FIRST Annual Conference 2015 in June 2015 and registered as a full member in October 2015.
- Attended APCERT Annual General Meeting and Conference in conjunction with Organisation of Islamic Cooperation (OIC-CERT) and registered as an Operational Member in September 2015.
- Attended the APCERT on-line training on "Debugging and Exploiting Security Vulnerabilities on Routers" in October 2015 and on-line training on APCERT drill in December 2015.
- Attended and delivered a speech at the Cloud Security Alliance Asia Pacific (CSA APAC) Congress in December 2015.
- Subscribed to the mailing lists of APCERT and FIRST.
- Participated in the Information Sharing Working Group of APCERT.

6. Future Plans

6.1 Future Projects

The GovCERT.HK will explore appropriate tools and solutions to establish a cyber health index as a base reference on the cyber security landscape of Hong Kong. We will also explore the need to implement an information sharing and analysis platform with big data analytics capability to cope with the massive information flow of security intelligence with a view to formulating early warning for our stakeholders in an efficient and effective manner.

Apart from general public awareness training and promotion initiatives, the GovCERT.HK will work with local universities and the industry to organise a cyber security competition entitled "Build a Secure Cyberspace 2016" to promote awareness of information security and proper cyber etiquette.

6.2 Future Operation

The GovCERT.HK will continue to expand its operations appropriately to cope with anticipated workload generated from the increasing security threats and alleged cyber attacks in the region.

7. Conclusion

In light of the proliferation of hacking activities and growing complexity in each incident, it is essential for the GovCERT.HK to establish and maintain close collaboration and operations with local and global CERTs to meet the ever-increasing challenges on cyber security. The GovCERT.HK will strive to work closely with the industry, professional organisations, and various stakeholders to maintain a secure, stable and trustworthy cyber world for people from all walks of life.

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 2015, HKCERT had handled 4,928 security incidents which was 43% increase of the previous year (see Figure 1).

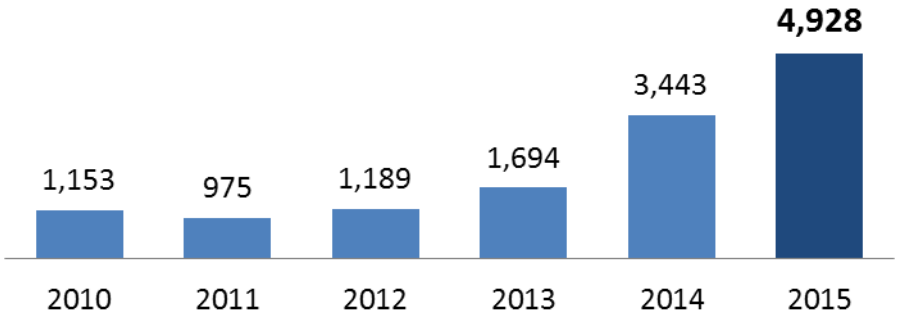


Figure 1. Incident Reports Handled by HKCERT

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 80% of the total number of security incidents.

The major category of security incidents was phishing (1,978 cases) which recorded a 233% increase. Next was botnet (1,943 cases) (see Figure 2).

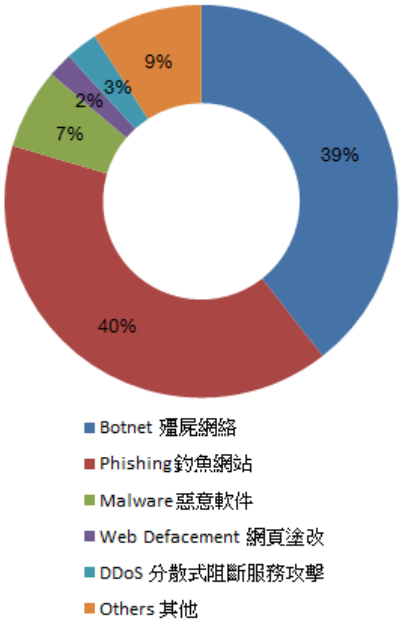


Figure 2. Distribution of Incident Reports in 2015

In the past few years, HKCERT keeps working on the phishing website taken down operations to protect the Internet users from phishing fraud. In 2015, the number of phishing incident reports rose sharply by 233% (see Figure 3). These phishing websites were running as new "flash" phishing attacks that were launched using local web hosting services as cover.

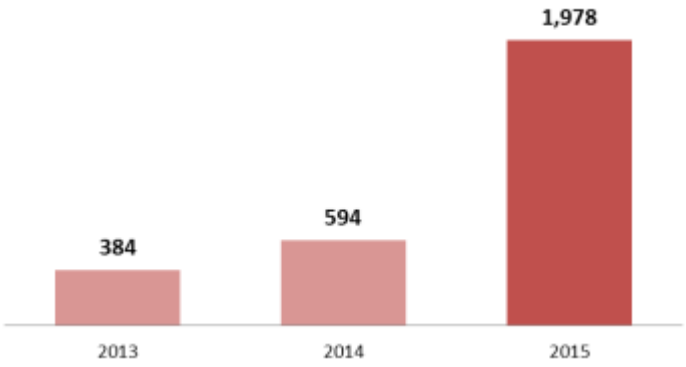


Figure 3. Number of Phishing Incident Reports in the past 3 years

2.2. Watch and Warning

During the period from January to December of 2015, HKCERT published 352 security bulletins (see Figure 4) on the website. In addition, HKCERT have also published 111 blogs, including security advisories on Windows Server 2003 end-of-support, fraudulent email, phishing scam, ransomware, mobile malware, vulnerabilities on Internet devices, and botnet attacks. HKCERT also published the best security reads of the week every week to inform the public of good security articles.

Figure 4. 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 had implemented 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 can check the effectiveness of the security operations. For example, Figure 5 showed the trend of bot related security events slightly decreasing from 6,172 in Q4 2014 to below 6,000 in 2015. Figure 6 showed the trend of top 5 botnet families in the past year. Besides a new botnet family Bamital raised in Q2 2015, the overall decreasing trend of other botnet families reflected the effectiveness of the botnet takedown operation.

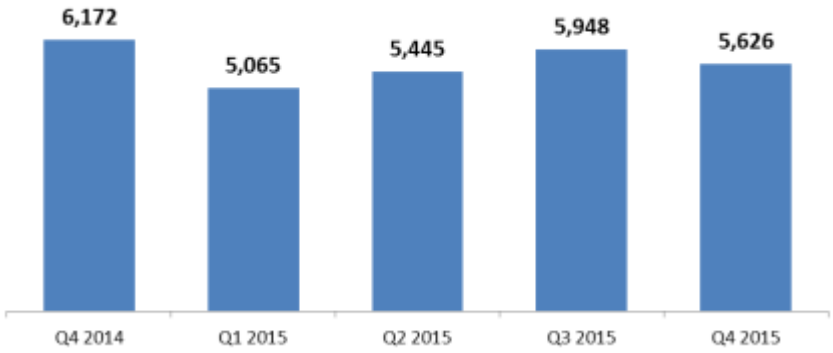


Figure 5. Trend of Bot related security events in the past year
(Source: data feeds from overseas security researchers, not from incident reports)

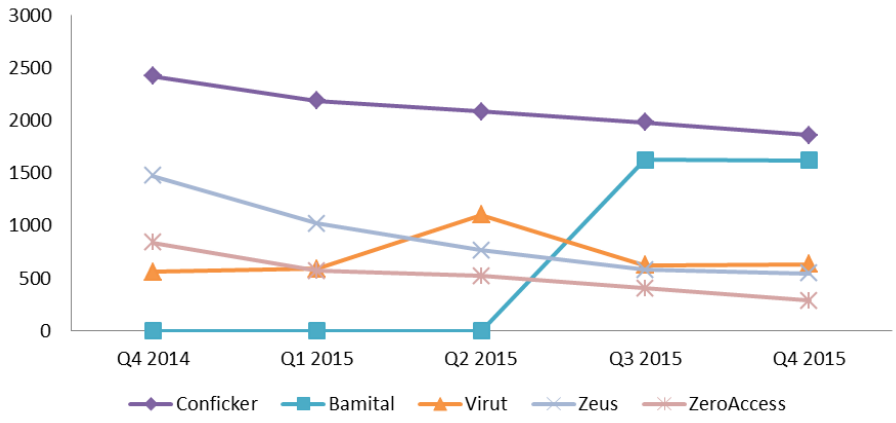


Figure 6. Trend of Top 5 Botnet Families in the past year
(Source: data feeds from overseas security researchers, not from incident reports)

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 of China (see https://www.hkcert.org/play-store-srr).

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

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

3. Events organized and co-organized

3.1. Seminars, Conference and Meetings

HKCERT jointly organized the "Cyber Security is Everywhere" campaign with the Government and Hong Kong Police Force. The campaign involved public seminars, and a graphic design contest. Two public seminars were organized in April and November 2015.

For the graphic design contest, HKCERT had received 1,536 applications from Open group, Secondary School group and Primary School group. A professional judge panel selected winners with good attractive designs (See Figure 7).

Figure 7. Champion entries of Open, Secondary School and Primary School Group (from left to right)

We organized the 2-day Information Security Summit 2015 with other information security organizations and associations in October 2015, inviting local and international speakers to provide insights and updates to local corporate users.

We jointly organized a seminar of "Transaction Security of Mobile Apps in Hong Kong Study" with other information security organizations and associations in November 2015, sharing research study conducted by HKCERT to mobile apps owners and developers.

1.10 TRANSITS CSIRT Training

HKCERT brought the first TRANSITS program to Hong Kong. HKCERT had organized a 3-day CSIRT training in December 2015. The workshop informs trainees with the global perspective of CSIRT and local knowledge of security incident coordination. There are 11 and 3 participators come from Hong Kong and Macau respectively.

1.11 Speeches and Presentations

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

1.12 Media promotion, briefings and responses

- HKCERT published two advertorials in November 2015 to promote the public seminar and the graphics design contest.
- HKCERT published weekly column articles in Hong Kong Economic Times to give information of current information security trends and advices.
- 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 Malaysia and delivered a workshop on IFAS
- Participated in the FIRST AGM and Conference in Berlin and delivered talk on cyber threat intelligence collection and analysis systems; participated in the Annual Meeting for CSIRTs with National Responsibility in Berlin and shared in the panel discussion the future of CERTs.
- Participated in the APCERT Drill (March 2015) and acted as member of the Organizing Committee and the Exercise Control team. The theme of the drill this year was “Cyber Attacks beyond Traditional Sources”. The drill was a great success with 25 APCERT teams from 19 economies, and 3 economies of OIC-CERT participating.
- 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 Singapore
- Represented APCERT in the Advisory Council of DotAsia Organization

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. AusCERT started to use DSMS and had developed some modules to DSMS.

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

GovCERT.HK was established April 2015. HKCERT, together with MOCERT, sponsored GovCERT.HK to join APCERT and FIRST membership, HKCERT had paid a visit to the GovCERT.HK office for this purpose.

HKCERT worked with a number of local organizations in different areas:

- Continued to work closely with the government (GovCERT.HK since April 2015) and law enforcement agency, and held meetings to exchange information and to organize joint events regularly.
- 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 2015, HKCERT had worked with ISPs to clean up Citadel, ZeroAccess, GameoverZeus, Pushdo, Ramnit and XcodeGhost botnet machines in Hong Kong.
- Participated in the government's Information Infrastructure Liaison Group and the Cloud Security and Privacy Working Group.
- 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 CNCERT Visit

HKCERT had visited CNCERT/CC in China in December of 2015. The mission of this tour was to understand and discuss with CNCERT their business services, the enabling factors and the lesson learnt. The collaboration opportunities were also sought during the visits. The visits allowed HKCERT to open the eyes and collected extremely useful information and sparked insights for the future development of HKCERT

5.2 Advisory Group Meeting

HKCERT had held the Advisory Meeting in July of 2015. The meeting provides solicit inputs from the advisors on the development strategy of HKCERT.

5.3 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 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.

5.4 Embrace global intelligence and build security health metrics

HKCERT had implemented the IFAS to collect intelligence of compromised machines in Hong Kong. The system provided a better picture of security status of Hong Kong and help clean up the botnets and C&C servers in Hong Kong. HKCERT publicized the information to the public quarterly and used the information in decision making.
HKCERT also joined the Cyber Green project initiated by JPCERT/CC in an attempt to collaborate with other CERTs to build useful metrics for measuring cyber health.

5.5 Year Ender press briefing

HKCERT organized a year ender press briefing to media in January 2016 to report on information security status of 2015, and to give perspective of the trends of security attacks in the coming year to warn the public for better awareness and preparedness. It received very good press coverage.

Figure 8. Mr Wilson Wong, General Manager (IT Industry Development) of HKPC (left), and Mr Leung Siu-Cheong, Senior Consultant of HKCERT of HKPC, review the information security situation in Hong Kong in 2015, and introduce the upcoming trends in the press briefing.

6. Future Plans

6.1 Strategy

"Proactivity", "Share to Win" and "Security is not an Island" are three directions of HKCERT. HKCERT will work closer with CERTs, security researchers and Internet stakeholders to build a more secure Hong Kong and Internet.

6.2 Funding

HKCERT would secure Government funding to provide the basic CERT services in 2016/2017. 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 intranet to increase the efficiency of information search and sharing. HKCERT is also developing automation modules to enhance the use of data in the IFAS to select prioritized incidents and collect intelligence about compromised machines in Hong Kong to follow up.

7. Conclusion

In 2015, HKCERT was also 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.

In 2015, HKCERT had set up the communication platform with some critical infrastructure organizations. To this end, we will continue to adopt collaborative approach to share information, conduct joint research and development, and develop closer relationship with our partners.

With the Internet security facing more crises from cyber conflicts, ransomware, phishing, POS attacks, exposure of Internet devices 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.

ID-CERT

Indonesia Computer Emergency Response Team – Indonesia

1. About ID-CERT

1.1. Introduction

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

1.1.1. Establishment

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

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

1.1.2. Workforce Power

Chair :	Budi Rahardjo, MSc., PhD.
Co-chair:	Andika Triwidada
Manager & Researcher :	Ahmad Alkazimy
Help Desk :	Rahmadian L. Arbianita
Technical Editor :	Wayan Achadiana
Volunteers :	Setia Juli Irzal (Malware Analyst)
	Ade Yoseman
	David Setiadi
	Anggi Elanda
	Maman Sutarman

Rizky Ariestiyansyah
Samuel Cahyawijaya
Andreas Wenra Alfa
Denny Nugraha
Ridwan Akbar
Andri Aprijal
Nurwin Hermansyah
Indra Suryana
Oki Bagja
Other volunteers

1.1.3. Constituency & Etc

Constituent

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

Respondent

ID-CERT has 39 respondents participating in Incident Monitoring Report. ID-CERT still welcome to new respondents who wish to join in the various researches/studies conducted by ID-CERT.

Volunteer

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

2. Activity & Operation

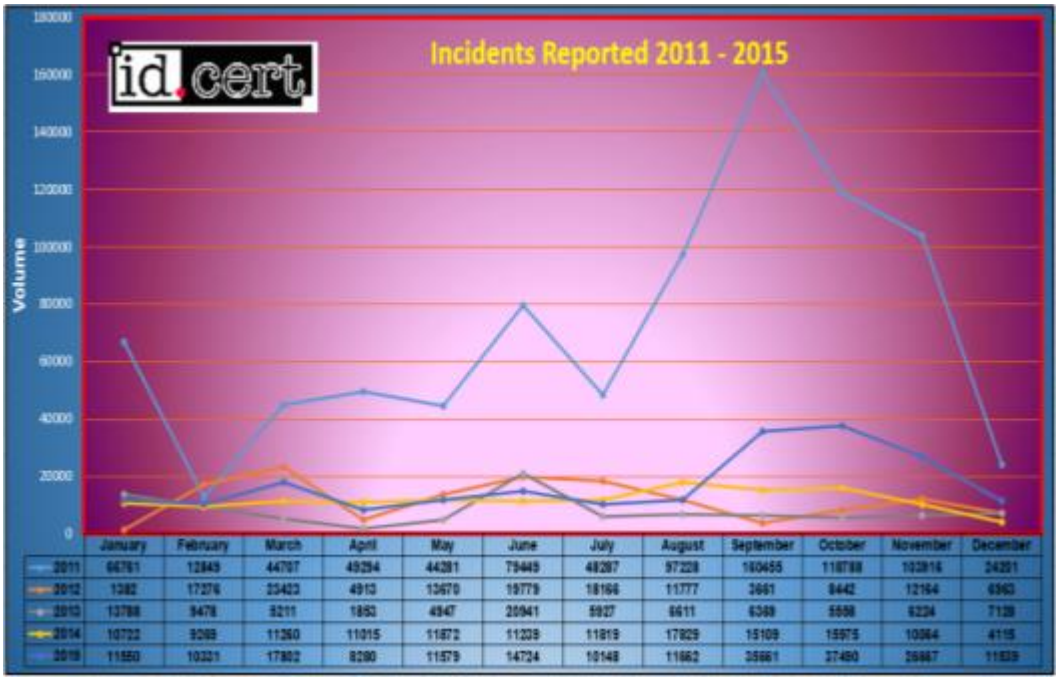
2.1. Incident Handling Report

207,433 reports received in 2015:

- IPR : 89,036 reports (42.92 %)
- Spam: 65,382 reports (31.52 %)
- Complain Spam : 22,959 reports (11.07 %)
- Network Incident: 15,975 reports (7.70%)
- Spoofing/Phising : 8,031 reports (3.87 %)
- Malware 6,050 reports (2.92%)

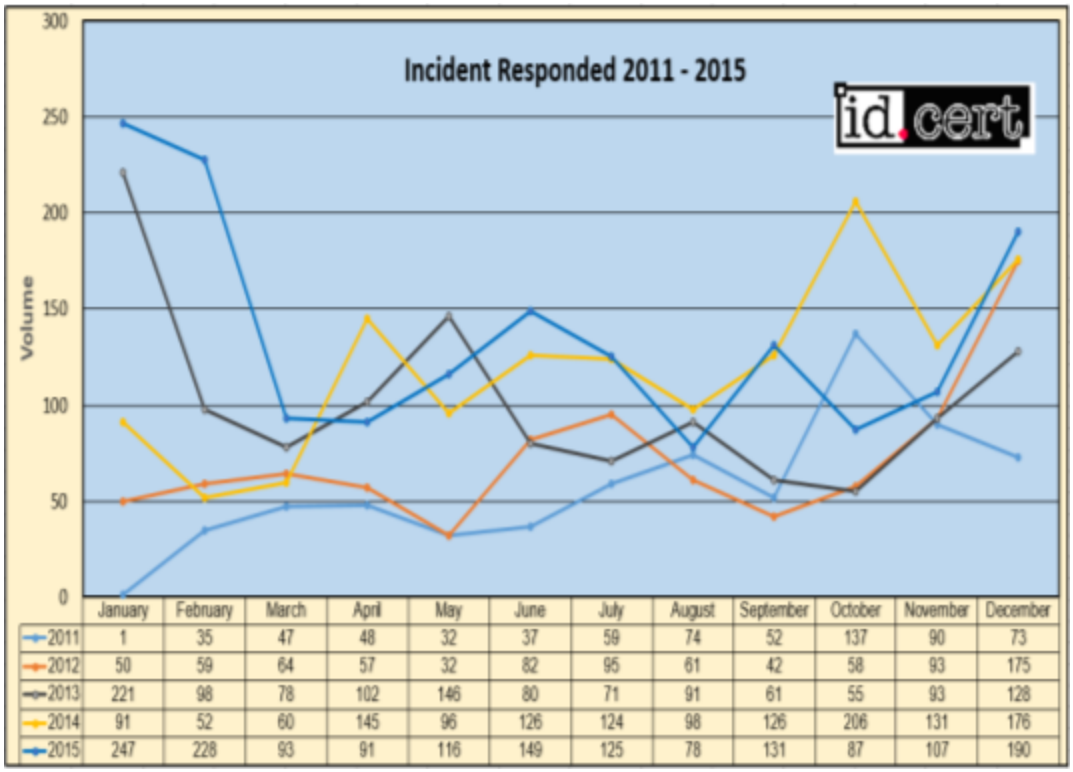
Respond to complaint in 2015 were 9,851 reports.

Incidents reported:



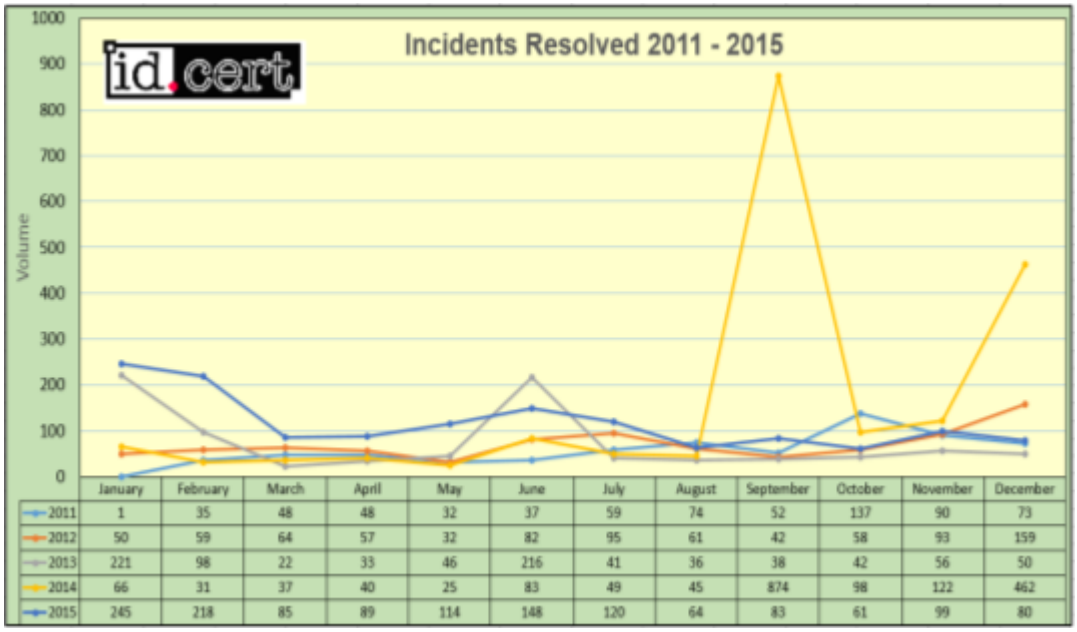
	January	February	March	April	May	June	July	August	September	October	November	December
2011	66761	12949	44707	49294	44281	79449	48287	97228	160455	118788	103816	24201
2012	1382	17276	23423	4913	13670	19779	18166	11777	3661	8442	12164	6363
2013	13788	9478	8211	1853	4947	20941	5927	6611	6389	5558	6234	7128
2014	10722	9269	11260	11015	11872	11239	11819	17829	15109	15975	10064	4115
2015	11550	10331	17302	8280	11579	14724	10148	11662	35661	27480	25667	11839

Incidents responded:



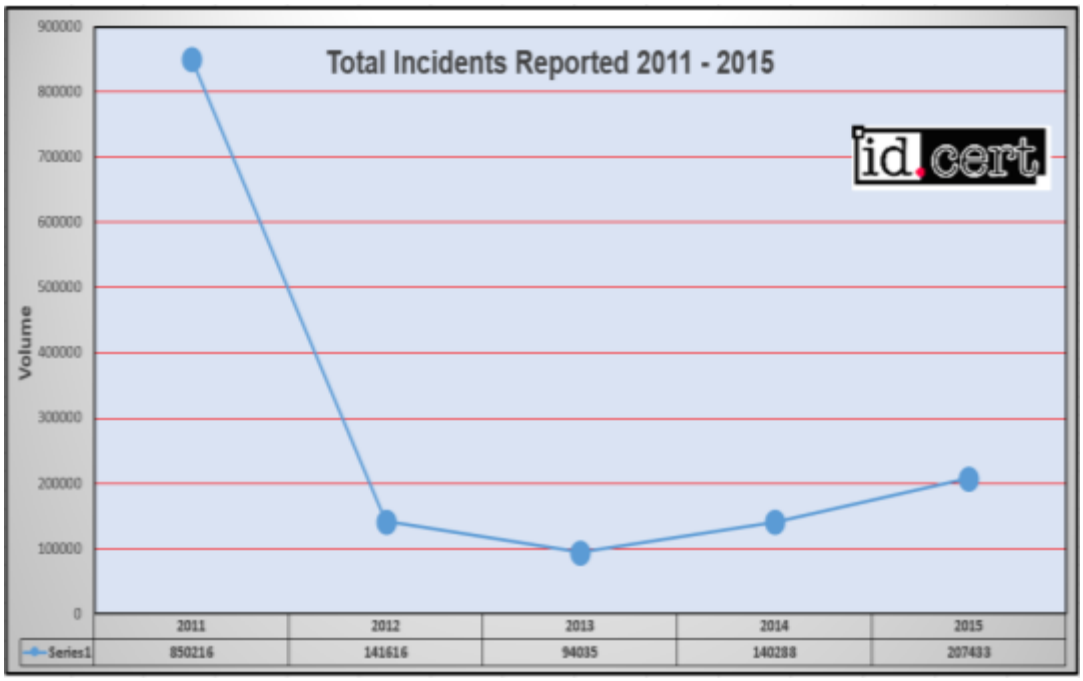
	January	February	March	April	May	June	July	August	September	October	November	December
2011	1	35	47	48	32	37	59	74	52	137	90	73
2012	50	59	64	57	32	82	95	61	42	58	93	175
2013	221	98	78	102	146	80	71	91	61	55	93	128
2014	91	52	60	145	96	126	124	98	126	206	131	176
2015	247	228	93	91	116	149	125	78	131	87	107	190

Incidents resolved 2011 – 2015 :



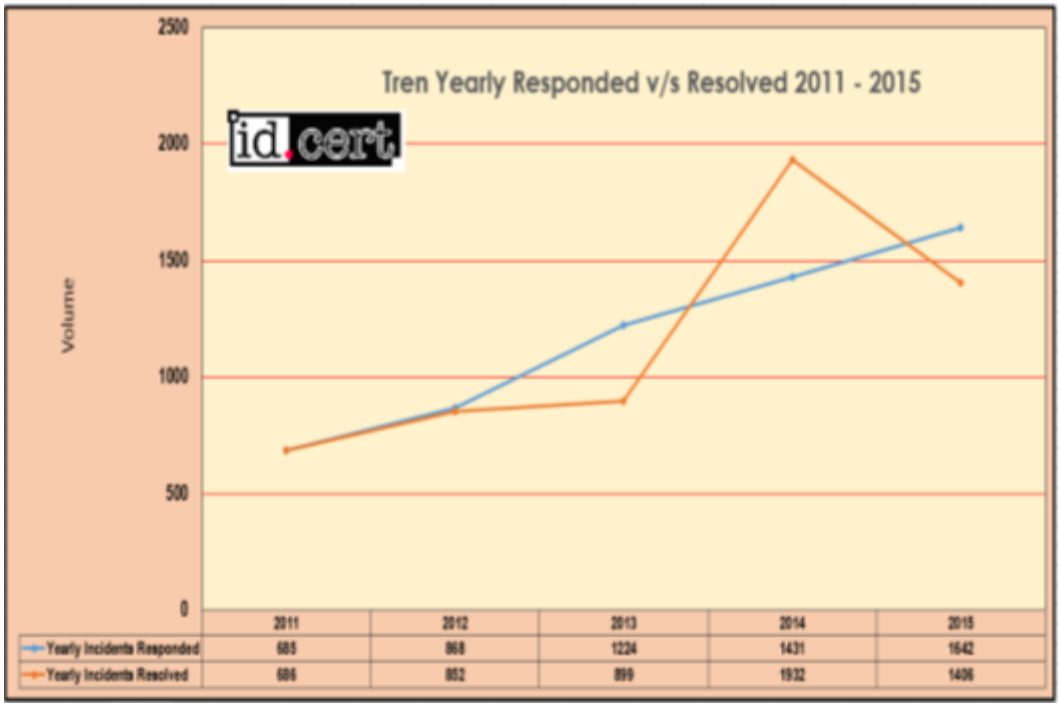
	January	February	March	April	May	June	July	August	September	October	November	December
2011	1	35	48	48	32	37	59	74	52	137	90	73
2012	50	59	64	57	32	82	95	61	42	58	93	159
2013	221	98	22	33	46	216	41	36	38	42	56	50
2014	66	31	37	40	25	83	49	45	874	98	122	462
2015	245	218	85	89	114	148	120	64	83	61	99	80

Total Incidents Reported 2011 – 2015:



	2011	2012	2013	2014	2015
Series1	850216	141616	94035	140288	207433

Tren Yearly Incidents Responded versus Resolved 2011 – 2015:



Most complaint cases:

- Hijacking of social media account (FB, Twitter, etc)
- Hijacking of domain name
- Deface
- Phishing
- Intellectual Property Rights
- Malware
- Network Incident
- Spam
- Brute force login

Some difficulties in handling complaint:

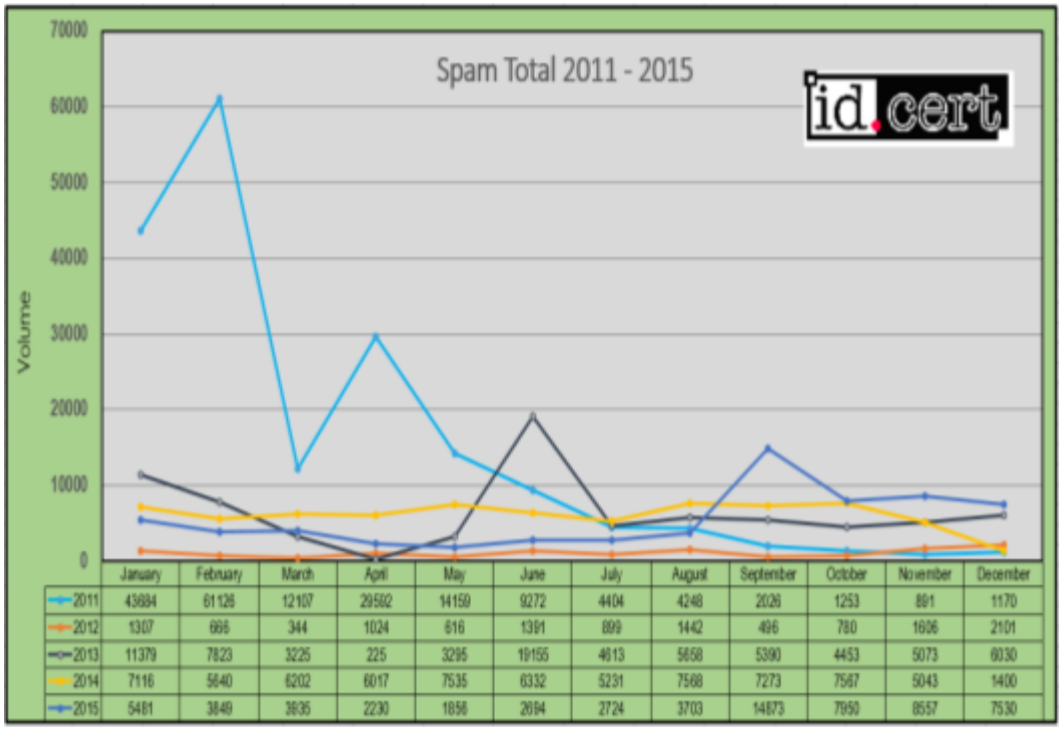
- Email is not valid
- Telephone number is not valid
- Address is not valid or changed address
- Contact is third party which is not valid
- Legal/law issues

2.2. Abuse Statistic

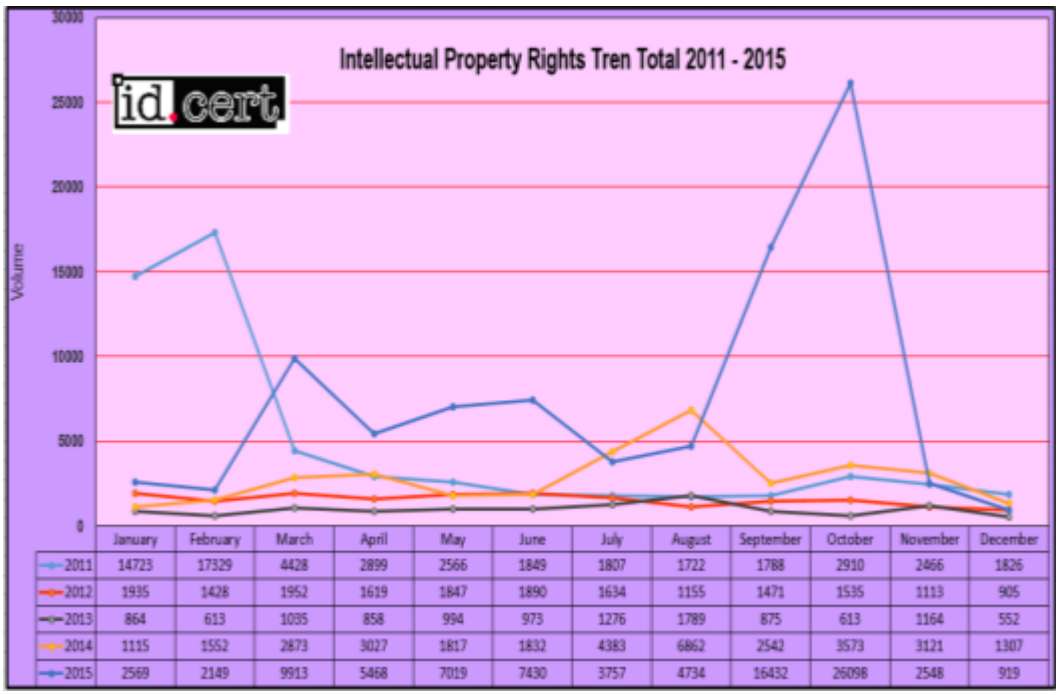
It is **Incident Monitoring Report (IMR)**, a joint monitoring activity that involve active constituents of ID-CERT by sending email copy of the incident complaint.

No.	*Complaint Category 2015*	*Rating (%)*
1	Spam	31,52
2	Intellectual Property Right	42,92
3	Spam complaint	11,07
4	Network Incident (Deface, DdoS attack, etc)	7,70
5	Spoofing/Phishing	3,87
6	Malware	2,92

Spam:

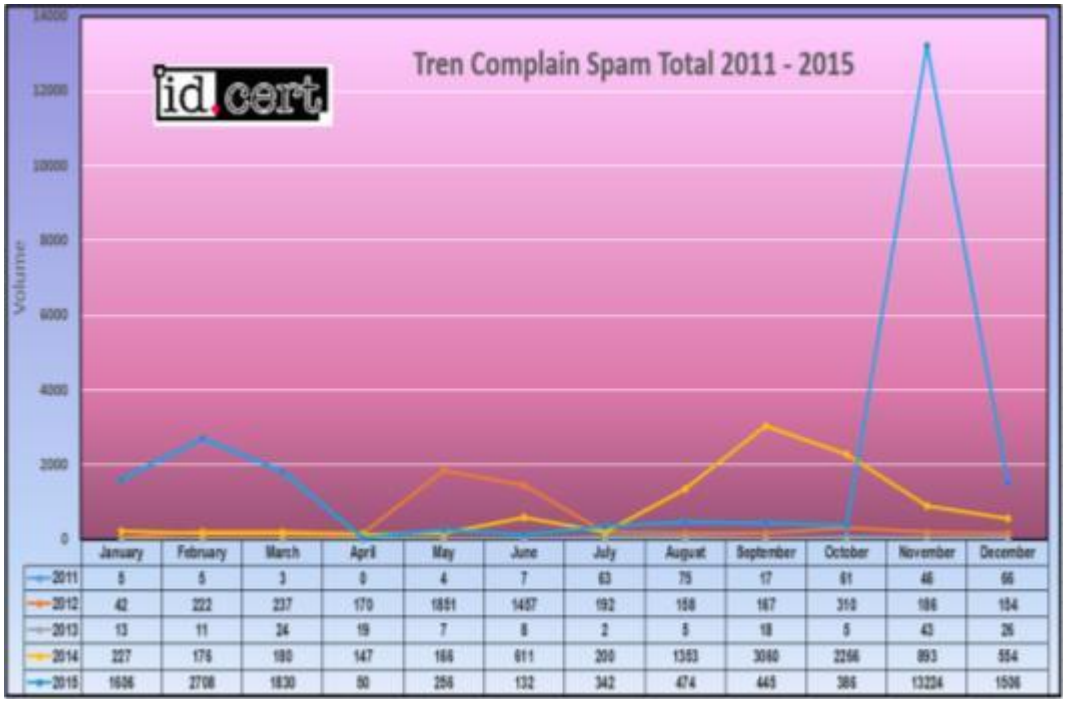


Intellectual Property Rights:



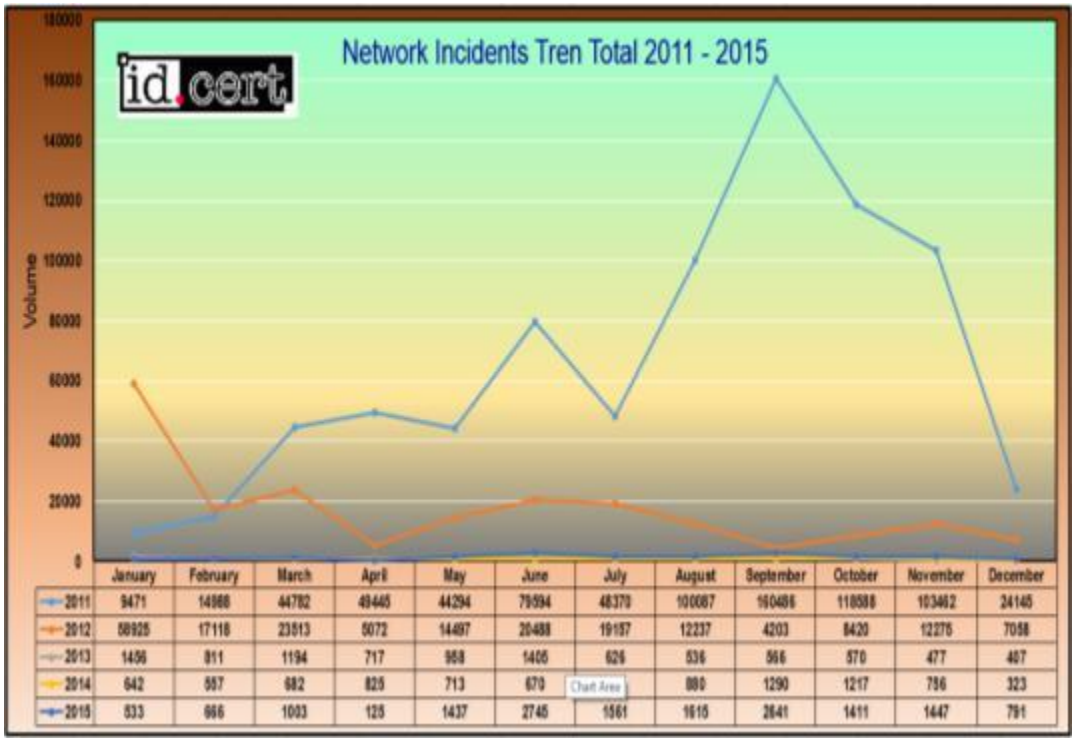
	January	February	March	April	May	June	July	August	September	October	November	December
2011	14723	17329	4428	2899	2566	1849	1807	1722	1788	2910	2466	1826
2012	1935	1428	1952	1619	1847	1890	1634	1155	1471	1535	1113	905
2013	864	613	1035	858	994	973	1276	1789	875	613	1164	552
2014	1115	1552	2873	3027	1817	1832	4383	6862	2542	3573	3121	1307
2015	2569	2149	9913	5468	7019	7430	3757	4734	16432	26098	2548	919

Spam complaint:



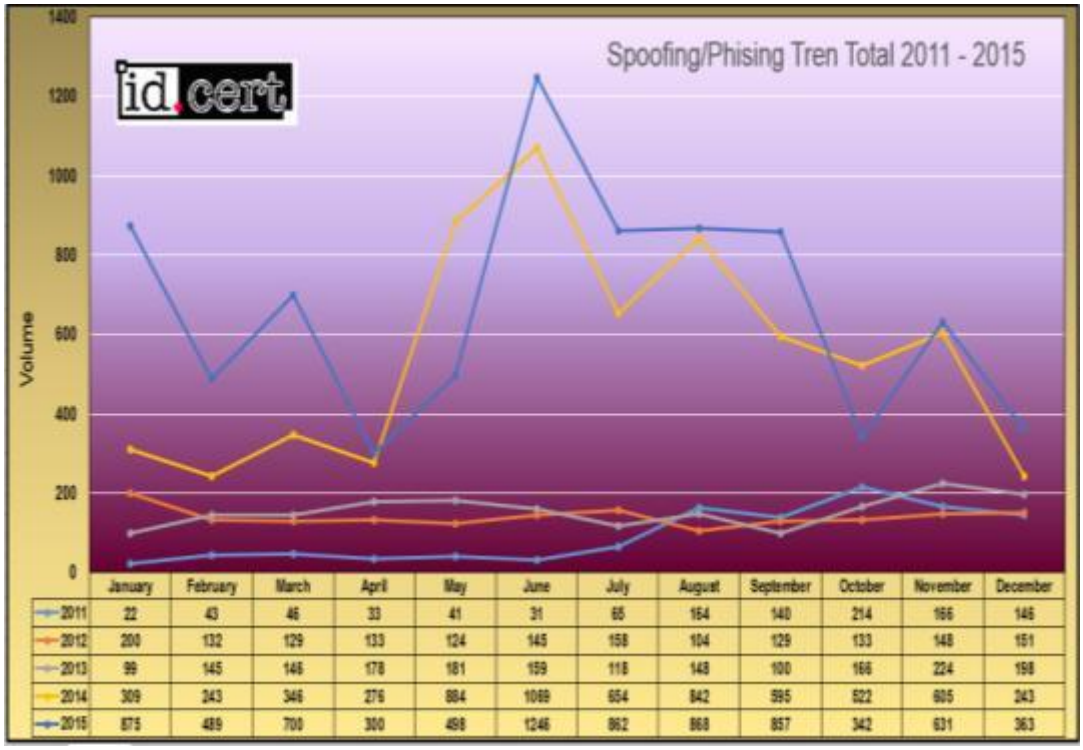
	January	February	March	April	May	June	July	August	September	October	November	December
2011	5	5	3	0	4	7	63	75	17	61	46	66
2012	42	222	237	170	1851	1457	192	158	167	310	186	104
2013	13	11	24	19	7	8	2	5	18	5	43	26
2014	227	176	180	147	166	611	200	1353	3060	2266	893	554
2015	1606	2708	1830	80	256	132	342	474	445	386	13224	1506

Network Incidents:



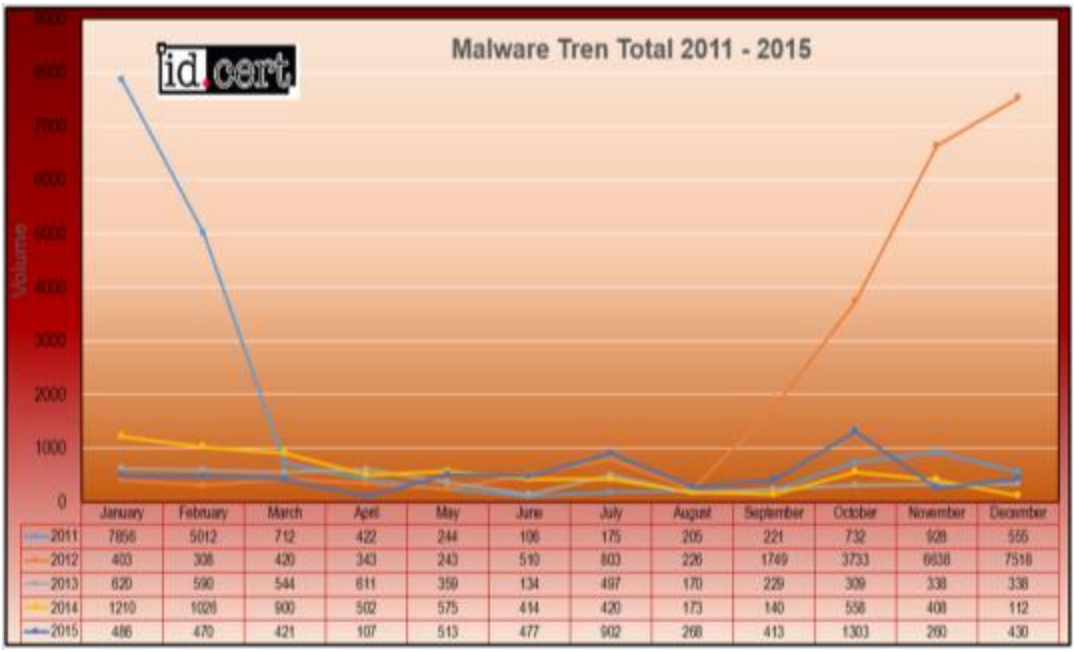
	January	February	March	April	May	June	July	August	September	October	November	December
2011	9471	14988	44782	49445	44294	79594	48370	100087	160486	118588	103462	24145
2012	58925	17118	23513	5072	14497	20488	19157	12237	4203	8420	12276	7058
2013	1456	811	1194	717	958	1406	626	536	566	570	477	407
2014	642	557	682	825	713	670	Chart Area	880	1290	1217	756	323
2015	533	666	1003	125	1437	2745	1561	1615	2641	1411	1447	791

Spoofing/Phishing:



	January	February	March	April	May	June	July	August	September	October	November	December
2011	22	43	46	33	41	31	65	164	140	214	166	146
2012	200	132	129	133	124	145	158	104	129	133	148	151
2013	99	145	146	178	181	159	118	148	100	166	224	198
2014	309	243	346	276	884	1069	654	842	595	522	605	243
2015	575	489	700	300	498	1246	862	868	857	342	631	363

Malware:



	January	February	March	April	May	June	July	August	September	October	November	December
2011	7858	5012	712	422	244	106	175	205	221	732	928	555
2012	403	308	420	343	243	510	803	226	1749	3733	6638	7518
2013	620	590	544	611	359	134	497	170	229	309	338	338
2014	1210	1026	900	502	575	414	420	173	140	558	408	112
2015	486	470	421	107	513	477	902	268	413	1303	260	430

Sample Phishing-Malware:

Phishing-Malware case in government domain, with motives to target certain site, spread malware, create fake site (phishing):

2014-09-26 11:10:21 CEST Up(nil): unknown_html RIPE FR
abuse@gandi.net 92.243.30.248 to 92.243.30.248 go.id
http://clg.utxao.bengkayang.go.id/
http://ebu.mhatr.bengkayang.go.id/
http://xjs.mhatr.bengkayang.go.id/
http://loadp.bengkayang.go.id/

3. Event

3.1. Training

Eventhough ID-CERT has not made any training events, we had been invited by several Government Agencies to do some hands-on training about Cyber Security. We are also being invited as an Advisor for province Government CSIRT.

3.2. Drill

March 18, 2015:

ID-CERT participated in APCERT Drill as Organizing Committee.

3.3. Seminar & Etc

January 23, 2015

Speaker at JCLEC-Semarang, invited by Australian Federal Police

January 29, 2015

ID-CERT Annual Gathering VII at Telkom-Japati Bandung

February 22, 2015

Meeting with Desk of Defense and Security of National Cyber Information (DKKCNI) - The Ministry of POLHUKAM RI, discussing the Threat of Cyber Attack related to the dead-execution of Foreign Convicts

March 2, 2015

Continued meetings with Desk of Defense and Security of National Cyber Information (DKKCNI) - The Ministry of POLHUKAM RI, discussing the Threat of Cyber Attack related to the dead-execution of Foreign Convicts

March 5, 2015

EduCERT Establishment Preparation Training

March 11-14, 2015

ID-CERT participated as a speaker at the Cyber Intelligence Asia 3 in Manila by Mr. Budi Rahardjo

March 18, 2015

APCERT Drill, ID-CERT participated as one of the OC and contributed PCAP manufacture in one of Drill scenarios.

March 19, 2015

Meeting with Directorate of Information Security, discussed the Anti-Spam Policy

March 20, 2015

Speaker at The Role of Diplomacy in Support of Indonesia Cyberspace as National Economy Modality, invited by KEMLU (Ministry of Foreign Affairs)

April 17, 2015

Speaker at JCLEC-Semarang, invited by Australian Federal Police

May 5, 2015

Indonesia Malware Summit 2015, Bandung, organized by ID-CERT

May 19, 2015

Meeting of handling negative-content sites (Joint DNS), invited by the Directorate of eBusiness KOMINFO

May 27, 2015

ID-CERT was requested by APNIC to become a member of the Fellowship Committee APNIC 40 in Jakarta. ID-CERT membership was represented by Ahmad Alkazimy.

May 28, 2015

Speaker at Security Trends 2015 in Bandung, invited by UNIKOM

June 26, 2015

Fasting break invited by IDC Indonesia

June 30, 2015

Fasting break invited by PANDI

July 1, 2015

Fasting break invited by QWords

July 1, 2015

Meeting with KLBI KEMKOMINFO

July 10, 2015

Fasting break invited by KEMKOMINFO

July 29, 2015

Meeting TELSOM and Cyber SEA GAMES 2015 at Hotel Discovery Ancol, invited by the ASEAN Secretariat via KOMINFO

August 7, 2015

Speaker at JCLEC-Semarang, invited by Australian Federal Police

September 1, 2015

Speaker at Security Awareness for DISKOMINFO Jabar (West Java)

September 6-9, 2015

ID-CERT attended APCERT annual meeting in Kuala Lumpur, Malaysia, represented by Ahmad Alkazimy

September 16, 2015

Meeting FGD KEMDAG (Ministry of Trade), discussed about tort trade

October 20-22, 2015

ID-CERT in cooperation with PT Insan Infonesia and KOMINFO provide Application Security training to DISKOMINFO Jabar in order to establish JabarProvCSIRT

November 12, 2015

Speaker at the National Security Day at Sari Pan Pacific Hotel, requested by ID-SIRTII, represented by Mr. Andika Triwidada

November 12, 2015

Awarded by ID-SIRTII at the Sari Pan Pacific Hotel, represented by Mr. Andika Triwidada

November 27, 2015

Speaker at JCLEC-Semarang for International Class

December 3, 2015

ID-CERT as a resource person for the inauguration JabarProv-CSIRT in Bandung. ID-CERT together with the Directorate of Information Security and GovCSIRT are the advisors to JabarProv-CSIRT.

December 19, 2015

ID-CERT was officially in collaboration with Team Cymru in providing data feeds log ASN Indonesia

4. International Collaboration

March 18, 2015:

ID-CERT had signed an agreement with KZ-CERT.

December 19, 2015:

ID-CERT had signed an agreement with Team CYMRU regarding on data sharing for AS Number incident related to Indonesia.

5. Future Plan

5.1. Future Project

- Malware Survey
- Android Anti Malware Scanner (AndroScan Project)
- Malware Wiki
- Malware Advisory

5.2. Framework

5.2.1. Future Operation

- Incident Handling
- IMR respondent addition
- Internal infrastructure improvement/development
- Antispam RBL
- ID-CERT Annual Gathering IX

6. Conclusion

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

JPCERT/CC

Japan Computer Emergency Response Team / Coordination Center – Japan

1. Highlights of 2015

1.1 Summary of major activities

- Partnership forged with NISC on international collaborative activities and information sharing

  JPCERT/CC and National center of Incident readiness and Strategy for Cybersecurity (NISC) entered into a partnership on 10 February 2015. This aims to contribute to the effective promotion of cyber security measures in Japan, mainly through international collaborative activities and information sharing between the organisations.

- Trends in enterprise CSIRTs in Japan

  In Japan, there have recently been a number of CSIRTs established in the private sector. Nippon CSIRT Association (NCA), which consists of enterprise and private sector CSIRTs in Japan, plays an active role to promote information sharing and cooperation among such CSIRTs. Since its foundation in 2007, the membership has gradually grown and almost doubled in 2015, which now counts up to 112 teams (as of December 2015). With the increase of sophistication and complexity in cyber attacks, CSIRTs are in great demand in Japanese enterprises, and many organisations are seeking for know-how on establishing and managing CSIRT operations as well as interaction with other CSIRTs through information sharing. JPCERT/CC serves as NCA's secretariat and will continue to support its activities.

- TSUBAME policy reviewed and workshop at APCERT & OIC-CERT Conference 2015

  TSUBAME, a joint network packet monitoring project led by JPCERT/CC, opened its gate to a wider area. The membership eligibility used to be limited within National CSIRTs in the Asia Pacific region, however, it now has been extended to include those of other regions as well. Furthermore, since APCERT AGM & Conference was held concurrently with OIC-CERT AGM & Conference in 2015, TSUBAME Workshop (which is held annually taking advantage of this APCERT event) invited prospective project members of OIC-CERT. Through this Workshop,

we expect to further expand the project by involving a wider range of National CSIRTs beyond the Asia Pacific region.

1.2 Achievements & milestones

JPCERT/CC completed its 4th consecutive term as APCERT Chair (2011-2015), and was re-elected as a member of the Steering Committee and the Secretariat for the organisation at the APCERT AGM held in September 2015. JPCERT/CC was also chosen to host the next APCERT AGM & Conference in Tokyo, Japan in 2016.

2. About JPCERT/CC

2.1 Introduction & Establishment

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

2.2 Constituency

JPCERT/CC coordinates with network service providers, security vendors, government agencies, as well as the industry associations in Japan.

3. Activities & Operations

3.1 Incident Handling Reports

In 2015, JPCERT/CC received 19,624 computer security incident reports from Japan and overseas.

	1st Qtr	2nd Qtr	3rd Qtr	4th Qtr	Total
Incident Reports	6,869	5,187	4,128	3,440	**19,624**

Figure 1. Incident reports to JPCERT/CC (2015)

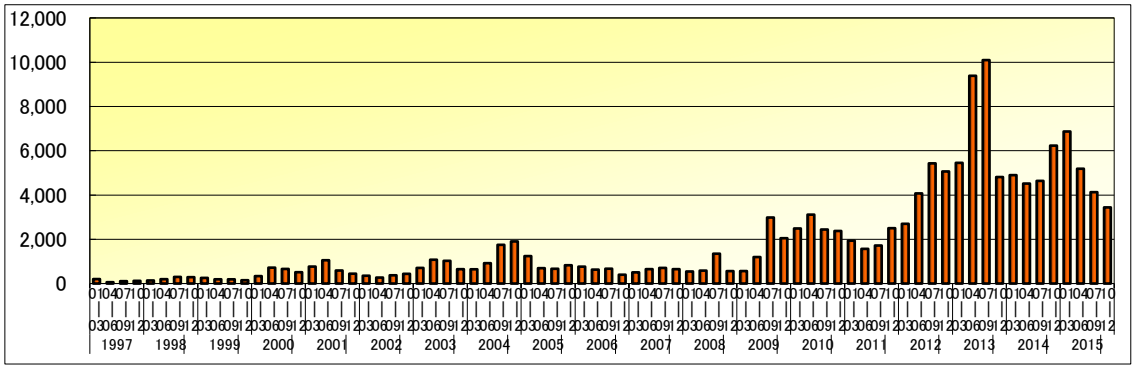


Figure 2. Incident reports to JPCERT/CC (1997-2015)

3.2 Abuse statistics

The incident reports to JPCERT/CC in 2015 were categorized as in Figure 3. About 53% of the incident reports were on scan, followed by website defacement and phishing.

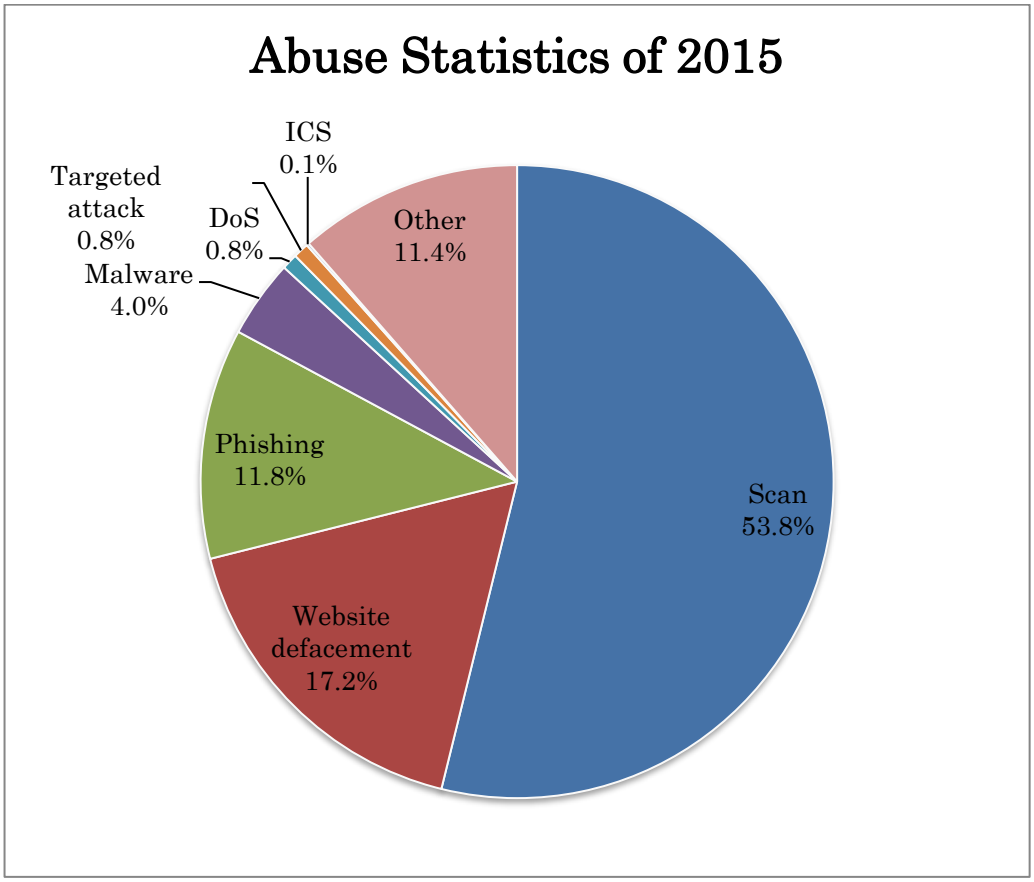


Figure 3. Abuse Statistics of 2015

3.3 Security Alerts, Advisories and Publications

- **Security Alerts**

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

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

  JPCERT/CC publishes security alerts on widespread, emerging information security threats and their solutions, on an as-needed basis. In 2015, 43 security alerts were published.

- **Early Warning Information**

  JPCERT/CC publishes early warning information to the Japanese government and to organizations providing national critical infrastructure services and products. Early warning information contains reports on threats, threat analysis and their solutions.

- **Japan Vulnerability Notes (JVN)**

  https://jvn.jp/ (Japanese)

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

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

  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/), and NCSC-FI (https://www.ncsc.fi/).

  In 2015, 338 vulnerabilities coordinated by JPCERT/CC were published on JVN. 188 were cases published through the Information Security Early Warning Partnership, and 150 were published through partnerships with overseas coordination centers or vendors.

  Of the 188 published through the Information Security Early Warning Partnership, 179 were reported to IPA by researchers, security vendors, etc. 9 were reported by developers against software they develop, and 1 was reported directly to JPCERT/CC by an overseas researcher.

  Of the 150 published through global partnerships, 125 were reported and published

by CERT/CC, 2 by ICS-CERT and 18 were reported by developers against software they develop. In addition, there were 5 issues published to serve as technical alerts, based on publicly available information.

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

- **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 on Twitter**

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

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

  Since January 2009, JPCERT/CC has been providing Security Alerts via Twitter.

- **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 2015, 20 articles were published.

- **Quarterly Activity Reports**

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

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

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

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 starting in January 2013, JPCERT/CC's incident handling service was extended to ICS area as well. JPCERT/CC has provided presentations at seminars and supported cyber incident

exercises to engineers of Japanese asset owners, and also released an ICS security assessment tool "J-CLICS", developed in collaboration with some experts from ICS vendors and asset owners.

- **Analysis Center**

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

- **TSUBAME (Internet Threat Monitoring Data Sharing Project)**

  http://www.apcert.org/about/structure/tsubame-wg/index.html

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

3.5 Projects

- **Cyber Green Initiative**

  http://www.cybergreen.net/

  Cyber Green is a global initiative designed to efficiently create a "healthy" cyberspace through the cooperation with technical partners, such as CSIRTs, ISPs and security vendors across the globe. This will be attempted through the use of metrics and statistical analysis that can be cross-compared across nations and regions. Currently in the pilot phase, JPCERT/CC is working with global partners to improve upon the metrics, statistical analysis methods and visualization.

3.6 Associations and Communities

- **Nippon CSIRT Association**

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

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

This 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 2015, 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 cooperation, JPCERT/CC signs a Memorandum of Understanding (MoU) with various security organizations. For 2015, JPCERT/CC renewed the MoU with NCSC-FI and CERT-In respectively.

- **FIRST (Forum of Incident Response and Security Teams)**
  http://www.first.org
  JPCERT/CC contributes to the international CSIRT community by serving as a Board of Director member (formerly referred to as Steering Committee) of the FIRST organization since 2005. JPCERT/CC offers support in sponsorship for CSIRTs who wish to be a member of FIRST.

- **APCERT (Asia Pacific Computer Response Team)**
  http://www.apcert.org/
  Since its establishment, JPCERT/CC has been serving to the community as a Steering Committee member and Secretariat. From 2011 to 2015, JPCERT/CC served as the Chair team. 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/seminars in 2015.

- CSIRT technical training for mmCERT (March, Yangon)
- CSIRT technical training for Indonesia, Cambodia, Laos and Myanmar, as part of JICA's (Japan International Corporation Agency) Project for Strengthening Capacity Building in Information Security (May, Jakarta)
- AfricaCERT Cybersecurity Day (May, Tunis) (through video message)
- Java, Android Secure Coding Seminar (July, Bangkok)
- FIRST Accra Regional Symposium (September, Accra)
- CSIRT training for ASEAN CIIP officials as part of HIDA's (Overseas Human Resources and Industry Development Association) Training Program (November, Jakarta)
- CSIRT technical training for AfricaCERT, AFRINIC (November, Pointe Noire)

5.2.2 Drills & Exercises

JPCERT/CC participated in the following drills in 2015 to test our incident response capability:

- APCERT Drill 2015 (18 March)
- APCERT & OIC-CERT Desktop Exercise (8 September)
- ASEAN CERT Incident Drill (ACID) 2015 (28 October)

5.2.3 Seminars & presentations

In 2015, JPCERT/CC dispatched speakers to the following international cyber security events:

- Pacific Telecommunications Council (PTC'15) (January, Hawaii)
- NCSC One Conference (April, The Hague)
- Global Conference on CyberSpace 2015 (April, The Hague)
- Australia Cyber Security Centre Conference (April, Canberra)
- APWG eCrime 2015 (May, Barcelona)
- 27th Annual FIRST Conference (June, Berlin)
- National CSIRT Meeting (June, Berlin)
- CGI.br Conference (September, Sao Paulo)
- Code Bali 2015 (September, Bali)
- MNSEC-2015 (September, Ulaanbaatar)

- CERT-RO Annual Conference (October, Bucharest)
- 2015 NAPCI (Northeast Asia Peace and Cooperation Initiative) Forum 2015 (October, Seoul)
- JavaOne2015 (October, San Francisco)
- GFCE (Global Forum on Cyber Expertise) International Kickoff Meeting (November, The Hague)
- Cyber and Space Security: Creative Policy Approaches to New Technical Challenges (November, London)
- Seoul 2015 FIRST Technical Colloquium (November, Seoul)
- 11th US-Japan Critical Infrastructure Protection Forum (December, Washington DC)

...and many more

5.3 Other international activities

Below are some of the international events that JPCERT/CC joined in 2015:

- APRICOT 2015 (March, Fukuoka)
- CanSecWest 2015 (March, Vancouver)
- RSA Conference US 2015 (April, San Francisco)
- ISO/IEC JTC 1/SC 27 Information Standard Meeting (May, Kuching)
- Safe Cities Asia (May, Singapore)
- CNCERT/CC Annual Conference (May, Wuhan)
- 2015 APISC Security Training Course (July, Seoul)
- Black Hat USA 2015 (August, Las Vegas)
- DEFCON 23 Hacking Conference (August, Las Vegas)
- 24th USENIX Security Symposium (August, Washington D.C.)
- The Second China-Japan-Korea CSIRT Annual Meeting for Cybersecurity Incident Response (August, Tokyo)
- APCERT AGM and Conference 2015 (September, Kuala Lumpur)
- OWASP AppSec USA 2015 (September, San Francisco)
- 4SICS (October, Stockholm)
- ISO/IEC JTC 1/SC 27 Information Standard Meeting (October, Jaipur)

…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

- APCERT AGM 2016 and JPCERT/CC 20th Anniversary

  JPCERT/CC will be hosting the next APCERT AGM & Conference, which will take place in October 2016 in Tokyo, Japan. JPCERT/CC will also celebrate its 20th anniversary of its establishment in October 1996.

- DNS sinkhole

  In 2015, DNS sinkhole project was launched for threat analysis on domains that were previously used for malware communication used in targeted attacks. JPCERT/CC has been notifying victim organisations in Japan and in the Asia Pacific region, and hopes to continue this effort towards 2016.

7. JPCERT/CC Contact Information

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

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 2015

1.1 Summary of Major Activities

Although there were no major incidents in 2015, the cyber threat to Korean citizens continued as existing pharming malware and the Korean version of ransomware, which is designed to extort money from domestic users, were detected and new vulnerabilities in commercial software were continuously discovered. As such, KrCERT/CC steadily carried out programs aimed not only at guaranteeing a quick response to such incidents, but also at raising public awareness through seminars and PR campaigns for the prevention of incidents and at strengthening the basis for coping with trans-border incidents.

1.2 Achievements & Milestones

The infection of websites with malware is one of the most common paths of malware dissemination. Since 2006, KrCERT/CC has been operating a service to detect compromised, while last year it expanded its search range to inspect 2.8 million domestic domains.

Cases of malware infecting smartphones are also being discovered continuously in South Korea as the use of smartphones has greatly increased. As there are many Android users and the mobile payment environment is unique in South Korea, there have been numerous cases of victims of Smishing, which appropriates money from unaware users in particular. KrCERT/CC launched the 'Mobile cyber curing service' to protect such users by notifying them of infection and encouraging them to treat their smartphones accordingly.

KrCERT/CC is also operating the 'New vulnerability report reward program(Bug bounty)' to encourage experts to expose security vulnerabilities during the transition period until domestic commercial enterprises recognize the vulnerabilities of their programs or homepages and deal with them in house. In December 2015, it rewarded four people after evaluating the severity and technical difficulties of the reported vulnerabilities.

In addition, KrCERT/CC has conducted an APISC Security Training Course in a bid to strengthen trust through exchange with other CERTs. Sixteen teams participated in

the program to share their procedures and technical know-how and strengthen the human network through training.

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 and Security Agency (KISA), KrCERT/CC is composed of three divisions, one center, one planning team, and twelve teams under it.

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

2.2 Establishment

KrCERT/CC was established in 1996 as a small team to respond to hacking accidents under the Korea Information Security Agency (a former of KISA). Since its foundation, it has responded to and handled numerous security issues and tasks. The first major incident was the Internet crisis caused by the so-called 'slammer worm' in 2003. At that time, KrCERT/CC had difficulties in 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 in December 2003, and has since evolved into its current form by responding to the 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 and the Korea Internet Security Center.

2.3 Resources

Currently, around 150 employees work for the 3 divisions of KrCERT/CC.

2.4 Constituency

KrCERT/CC serves as the focal point to coordinate security incidents in all Korean constituencies. In the national cyber security framework, 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, security vendors, and so on.

3. Activities & Operations

3.1 Scope and definitions

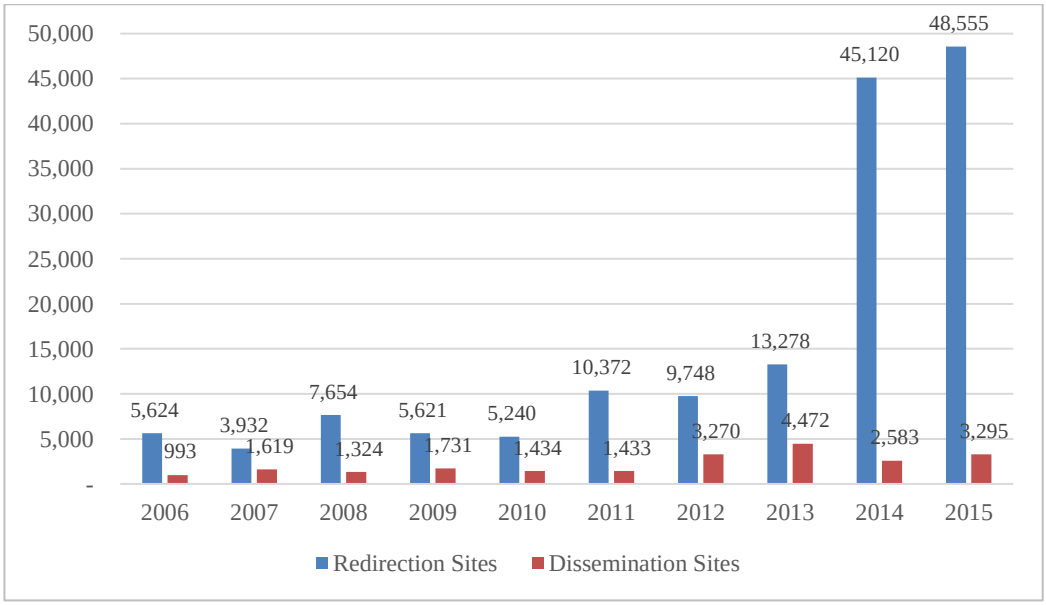
The key duty of KrCERT/CC is to respond to Internet security incidents related to users and general businesses. Its other duties include raising user awareness and promoting international cooperation.

3.2 Statistics on Abuse

3.2.1 Malware via compromised websites

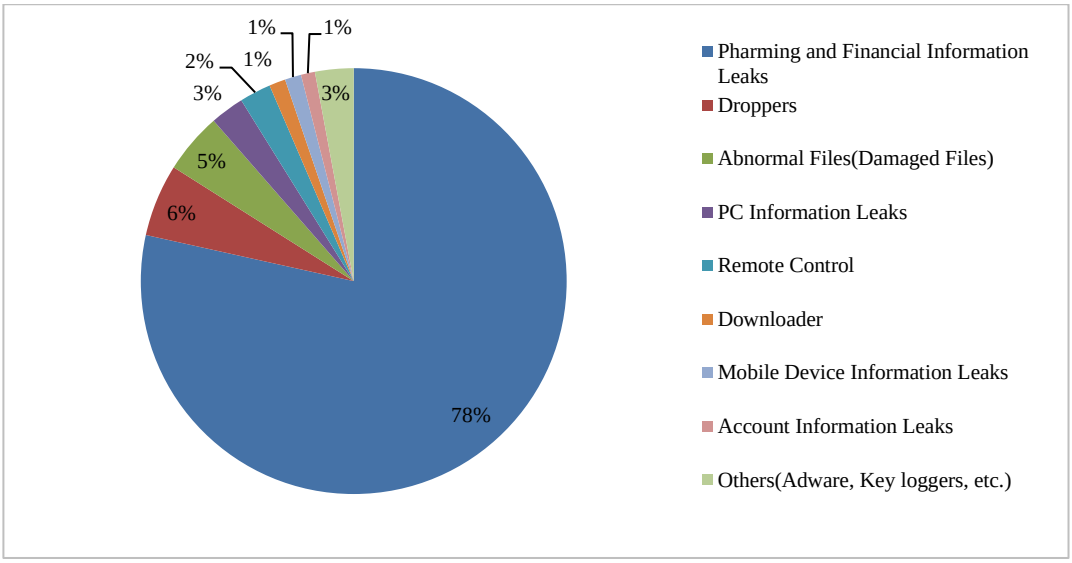
Malware is continuously being disseminated and hidden in websites. The number of sites that directly disseminate malware in 2015 increased by 27.6% over the previous year (2,583 cases → 3,295 cases), while the number of redirection sites linking to the dissemination sites decreased by 3.5% (45,120 cases → 43,555 cases) from the previous year.

Malware Redirection Sites and Dissemination Sites Detected



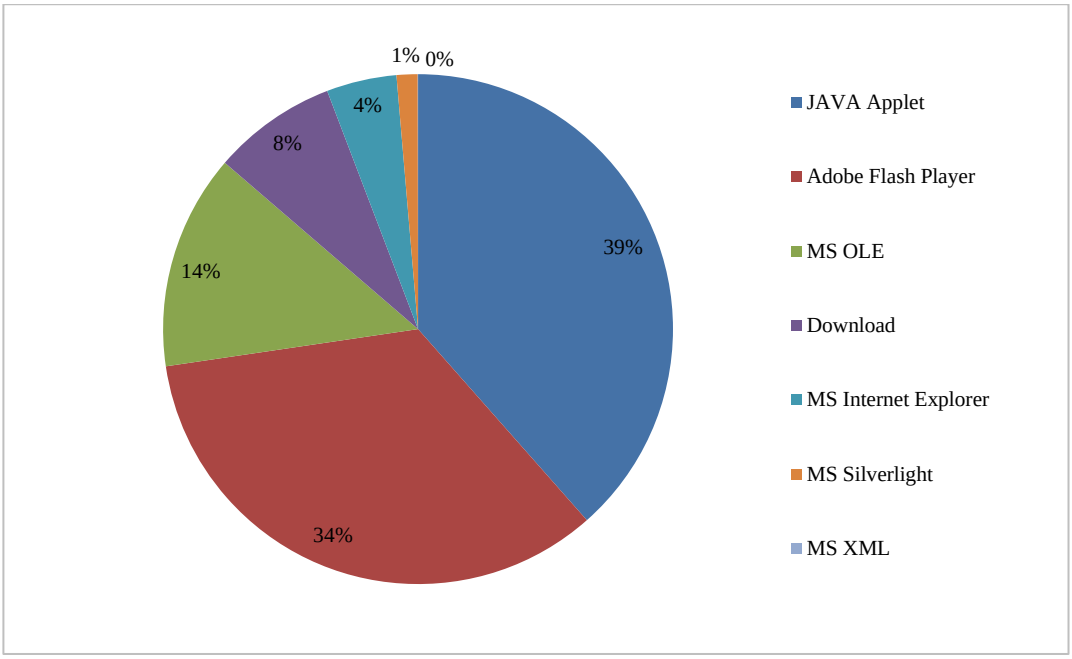
Concerning the types of malware disseminated through infected sites, the majority were Pharming and financial information leakages, followed by droppers and PC information leakages.

Malwares Types in 2015



These types of malware typically take advantage of the vulnerabilities of software installed on the users' PCs. The most commonly used type of software was Java applet (39%), followed by Adobe Flash Player (34%) and MS OLE (14%).

Software Vulnerabilities in 2015



3.2.2 DDoS attack

Although bandwidth consumption attacks such as UDP/ICMP flooding have been steadily occurring, the number of UDP/ICMP flooding attacks decreased in 2015, while the number of reflection based DDoS attacks related to SSDP, DNS and NTP increased, indicating a change in the DDoS attack trend.

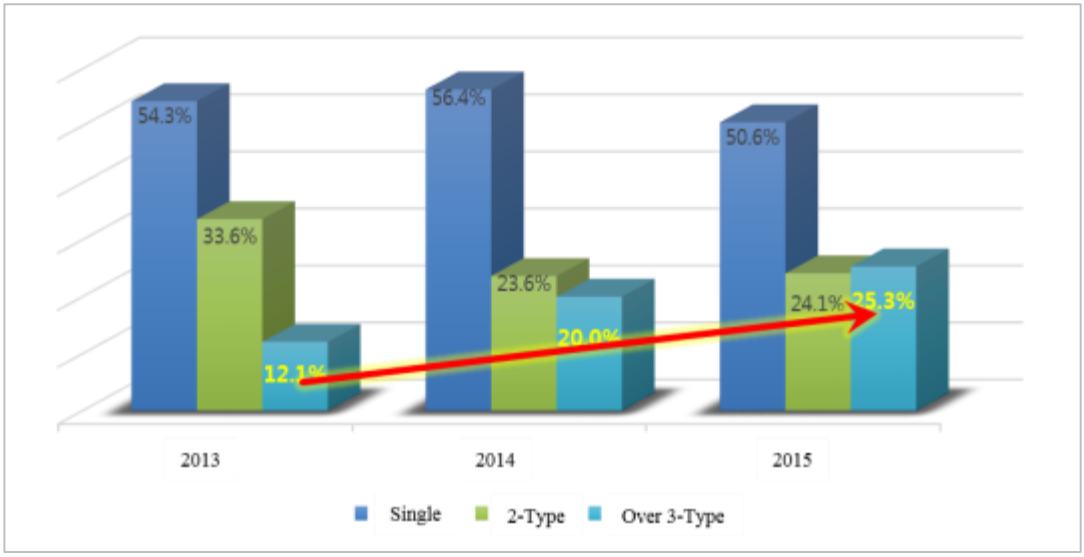
DDoS attacks involved the creation of artificial attack traffic in the past, but the technique has evolved to become a more effective form of using SSDP, NTP and DNS services, which are open in the Internet, so attacks have not needed to create bots since 2014 and 2015.

GET flooding attacks, whose purpose is to interrupt the normal service of an web application, have also been used continuously. The technique has advanced to the recent form of inserting Java script-based malware into a web page bulletin board to induce GET flooding by visitors to the web page.

One notable form of attack identified in 2015 was the 'complex attack', which uses up to 8 different attack techniques in a single attack. The DDoS attacks collected and analyzed by KrCERT/CC in 2013 ~ 2015 showed that simple attacks using one type of

attack technique are decreasing, whereas complex attacks using three or more types of attack techniques are increasing. Such a trend has been analyzed and attributed to the popularity of attack services and the appearance of web services such as BOOTER, which provide DDoS attacks free or for a fee, thus enabling attackers to easily launch DDoS attacks without requiring a technical understanding of the attacks.

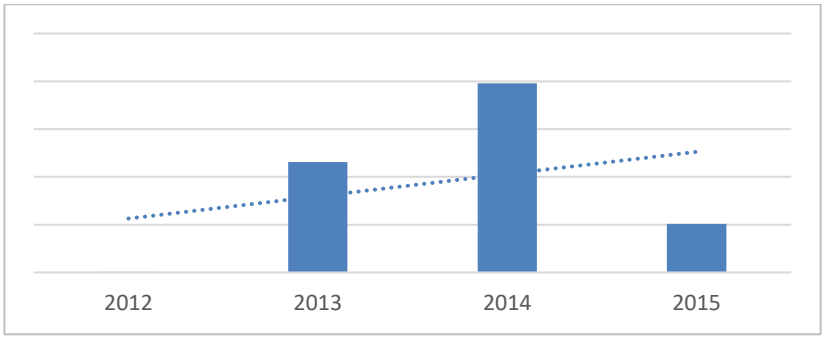
Trend toward Increasingly Complex Attacks



3.2.3 Response to Smishing

Although Smishing (SMS + Phishing) attacks, which cause leakages of personal information or monetary damage by sending a malicious text message to induce the installation of a malicious app, had been increasing each year, the number of new malicious apps related to Smishing reported in 2015 decreased by more than 74% from 2014.

Trend of Detected Smishing by KrCERT/CC



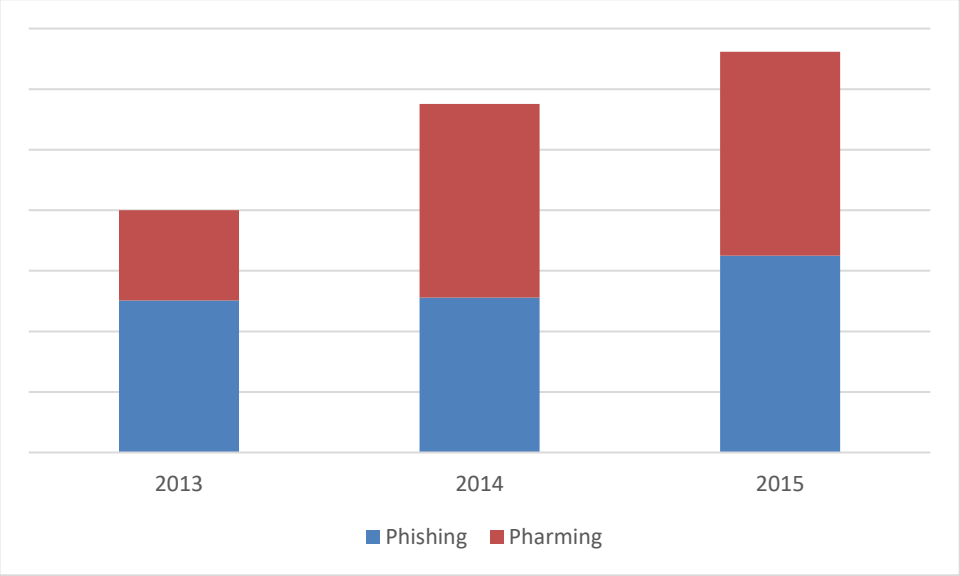
Although the number of analyzed malicious apps and detected Smishing text messages greatly decreased, the malicious function has become more advanced. According to our analysis, malicious apps detected in 2015 has shown that most of these malicious apps hide the app icon, thereby preventing users from realizing that their mobile phones had been infected. And a function that continuously demands the device administrator privilege and disables the users from deleting the app. Moreover, we could see a function that sends a random text to a contact point in the address book saved in the infected mobile phone as well as the remote control type.

3.2.4 Phishing/Pharming trend

Up until May 2015, the number of Pharming incidents in which the DNS of a router was altered using its vulnerabilities and the user was induced to connect to a falsified site opened by the attacker even when connected to a normal site had increased rapidly. However, such Pharming incidents decreased after Access Point security measures by KrCERT/CC were implemented in June 2015, although the overall number was still slightly larger than that recorded in the previous year.

The number of Phishing sites detected and blocked by KrCERT/CC in 2015 increased by 27% from the previous year, while the number of pharming sites increased by 5%. The total number of blocked Phishing and Pharming sites increased by 15%.

Trend of Blocking Phishing and Pharming sites by KrCERT/CC



3.3 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 detected.

3.4 New services

KrCERT/CC is cooperating with domestic ISP to provide a notification service to notify users whose PCs are used to cause attacks leading to security incidents without the users' awareness, and to guide the treatment. When users open a web browser, it displays a popup window to notify them of an infection and provides a one-time free vaccine and a link to the instructions page.

As the increased distribution of smartphones and the promotion of mobile Internet use have led to an ever growing number of victims of not only Smishing and other malware in the PC environment but also of malicious apps in the mobile environment, security in the mobile environment has become an extremely serious issue. As such, KrCERT/CC developed the pilot 'Mobile cyber Curing system' in 2014 to provide notification of infection and treatment measures for smartphones infected by malicious apps, and launched it as an official service in 2015.

4. Events organized / hosted

4.1 Training

KrCERT/CC has been conducting an invitation-based security training program on CSIRT development and operation for countries in mainly the Asia-Pacific region each year since 2005. As it is widely recognized that the establishment of a human network of working level personnel in each country is the most important measure for responding effectively to cyber incidents, this program was designed to assist such efforts. In 2015, 16 people from 16 countries including Cambodia, Thailand and India participated in the program with the aim of sharing information on the cyber security systems and CSIRT development know-how of each country. To date, 237 people from 47 countries have participated in the APISC security training course.

Moreover, KISA, to which KrCERT/CC reports, opened the GCCD (Global Cyber security Center) and is holding joint seminars with CERTs in the Asia-Pacific regions as part of a program to strengthen the capability of the international community. In 2015, it held a cyber security seminar with CRC in Mongolia and VNCERT in Vietnam, in which a KrCERT/CC employee participated in order to share know-how on effective responses to malware.

4.2 Drills & exercises

KrCERT/CC has been conducting cyber drills with the relevant domestic agencies since 2004. It conducted three times in 2015.

4.3 Conferences and seminars

4.3.1 FIRST Technology Seminar Seoul

KrCERT/CC held the Forum for Incident Response and Security Teams (FIRST) Technology Seminar in November 2015 in preparation for the FIRST Seoul Meeting in 2016. The purpose of the 2-day seminar was to focus the attention of the international community on information security and to build trust among domestic teams. The first day began with an introduction to FIRST presented by Mr. Koichiro Komiyama, a member of the FIRST steering committee, followed by FIRST training supervised by Adli Wahid. The second day consisted of a workshop. More than 30 people from CERTs in Korea and other countries participated in the 2-day event.

4.3.2 Information Security Day Ceremony

The fourth 'Information Security Day' celebration was jointly held by the Ministry of Science, ICT and Future Planning, the Ministry of Government Administration and Home Affairs, and the National Intelligence Service on July 8, 2015 (i.e. the second Wednesday in July as designated by the law). Held under the theme of 'Information Security for All Citizens,', with the participation of 3,011 people from 604 agencies, the event was designed to promote a campaign aimed at raising the general public's awareness of the paramount importance of information security and encouraging it to actually put it into practice.

Fourth Information Security Day Celebration

Cyber space is a secondary sphere of life where everything is connected over the Internet. During the ceremony, the animation characters Robocar Poly and Friends – i.e. Poly the police car), Roy the fire engine, Amber the ambulance, and Heli the helicopter, together protectors of the public - were appointed as information security ambassadors with the task of promoting Korean citizens' practice of information security in the online world. As such, it marked a departure from the general practice of appointing famous people (entertainers, politicians, etc.) as ambassadors. Appointing characters that are very popular with children and developing a special character dedicated to information security generated a novel synergy effect at a time when it is highly important to declare a new beginning in reestablishing information security as a culture for everyone, by going beyond merely increasing public awareness of the need for information security.

At the K-ICT International Conference on Information Security (ICIS), three sessions titled *Security Start-up*, *Security Spark*, and *Security K-ICT* were held following the keynote speech titled *Ceaseless Efforts to Create a Safe Internet World*.

Six projects were participated in the exhibition of information security R&D outputs and 11 products were exhibited at the exhibition of security products. Thirty companies participated in the information security job fair, and more than seventy outstanding

information security posters were exhibited. Around 12% more parties participated compared to the previous year, with many major scale concurrent events, the ceremony is considered very effective in alerting the citizens to information security and increase the participation in awareness programs.

5. International Collaboration

5.1 International partnerships and agreements

In 2015, numerous events were held in a bid to strengthen cooperation with agencies in countries that have established their own official cooperation system. KrCERT/CC participated in and hosted workshops with India CSIRT and the UK Academic professionals on the diplomatic perspective and actively participated in the intergovernmental cooperation meetings. KrCERT/CC also joined businesses from both countries to participate in the Korea-China workshop on security strategies and current issues in both countries, which was held concurrently with the departmental meeting.

5.2 Capacity building

5.2.1 Drills & exercises

KrCERT/CC participated in the joint drill held by APCERT in March 2015 to solve a set task within a deadline of 3 hours and 50 minutes and to review the organic incident response capabilities of the coordination, analysis and response teams of the organization.

5.2.2 Seminars & presentations

APCERT AGM: Response to IoT DDoS attack in September 2015

CERT-RO Cyber Security Annual Conference: Introduction of KrCERT/CC and Response Activities in October 2015

Mongolia: GCCD-CRC Joint Seminar in December 2015

Vietnam: GCCD-VNCERT Joint Seminar in December 2015

6. Future Plans

6.1 Future Operation

It is expected that the everyday threats posed by ransomware targeting domestic users and Pharming attacks, whose techniques are being continuously upgraded, will continue unabated. As such, KrCERT/CC intends to quickly and automatically detect such incidents by continuously investigating attack techniques and enhancing the

relevant systems. It will also try to gather as much information as possible by strengthening trust among people and participating in international communities to help create a safer Internet environment.

7. Conclusion

Although there were no major incidents in 2015, there was still a series of threatening incidents related with the Korean version of ransomware and wireless router vulnerabilities due to improper setting. Believing that prevention is the best method of incident response and protection, KrCERT/CC will work to raise awareness and strengthen cooperation with other agencies to enable a quick and effective response to incidents and prevention.

LaoCERT

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

1. About LaoCERT

1.1 Introduction

Almost for four year that LaoCERT has been established and we have been trying to study and implement/practice a lot in the role of CERT, so It is very challenge for us to implement/conduct so many activities in order to make constituency realize on threat from Internet/cyber space and the strategy to protect information technology or property of human, however we already started dealing with cyber incident, threat monitoring, training and education on cyber security in Laos. On the other hand, LaoCERT is almost completed to developing on capacity of it staffs for become a national CERT to against with cyber-attack. It was formed in a few years ago and has been known among IT social, government agencies, private organizations in Laos PDR and also international CERTs. This annual report includes activities and operation which have been conducted in last year, 2015.

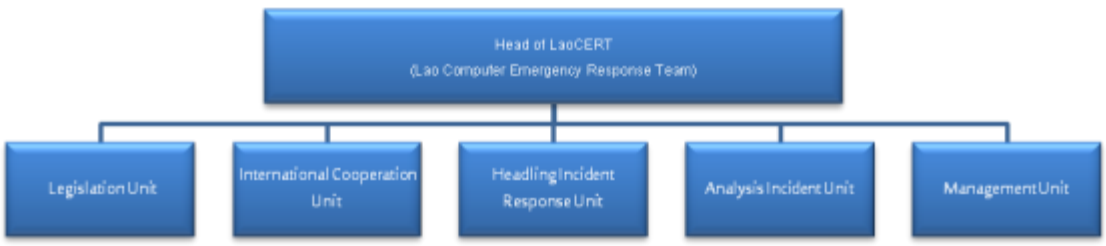
1.2 Establishment

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 built by following up as ITU-IMPACT recommendation.

1.3 Organization

LaoCERT currently contain 17 staffs, 5 females and divide into 5 units.

LaoCERT Organization Charts



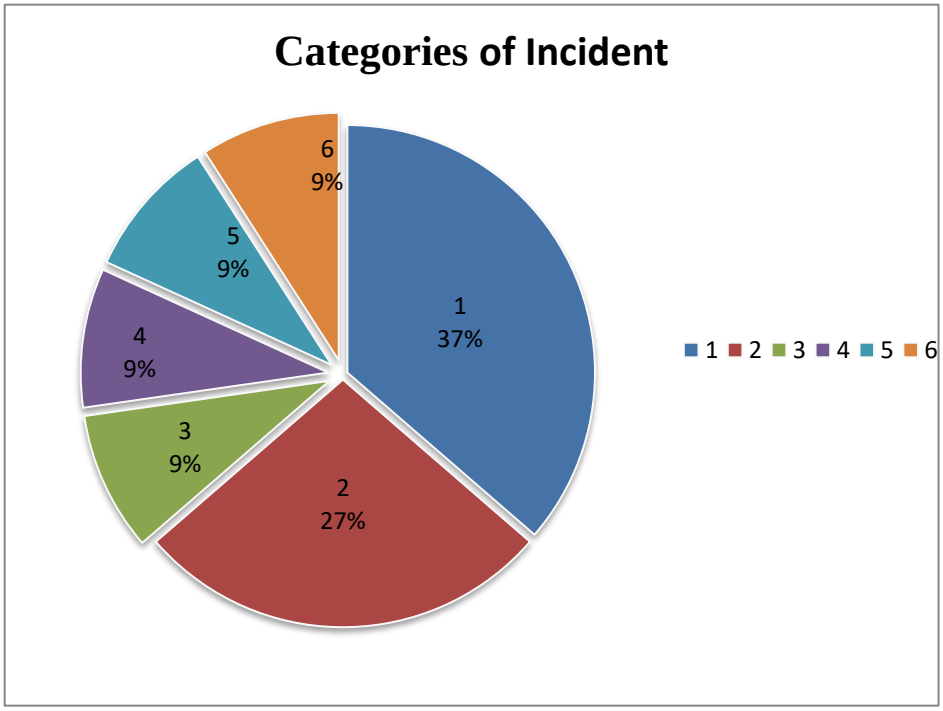
1.4 Constituency

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

2. Activities & Operations

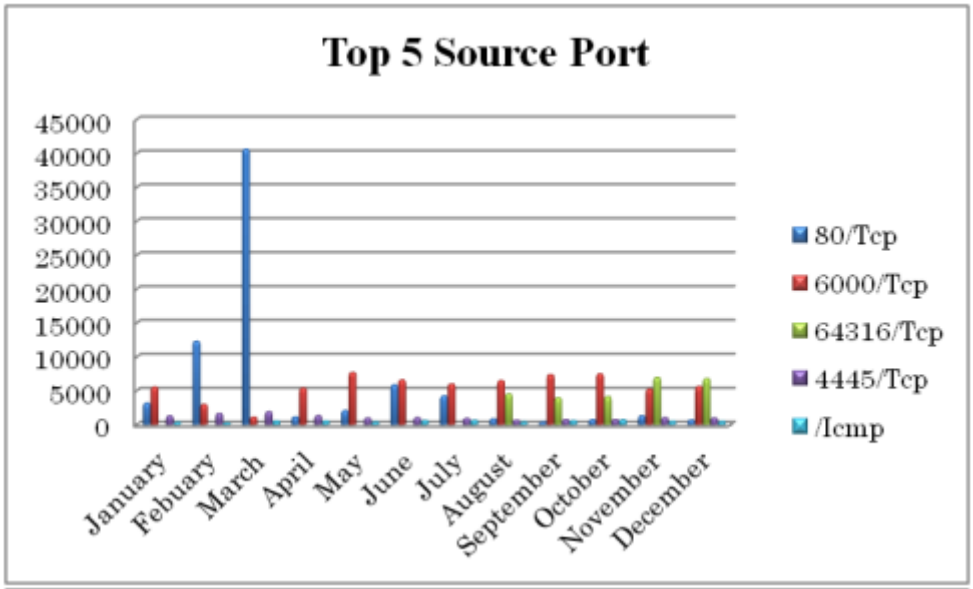
2.1. Incident handling

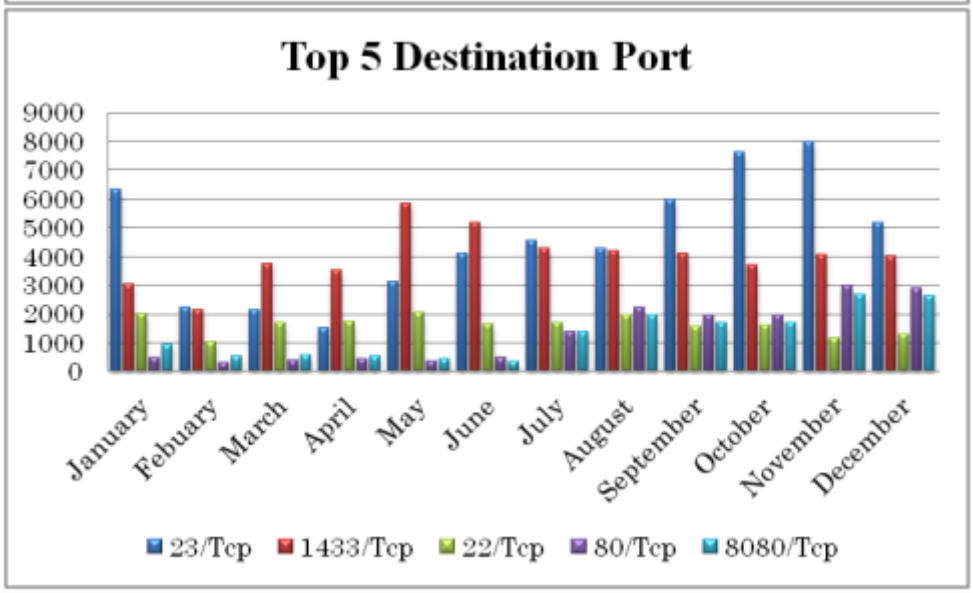
The following graph shows the incidents that happening in 2015.

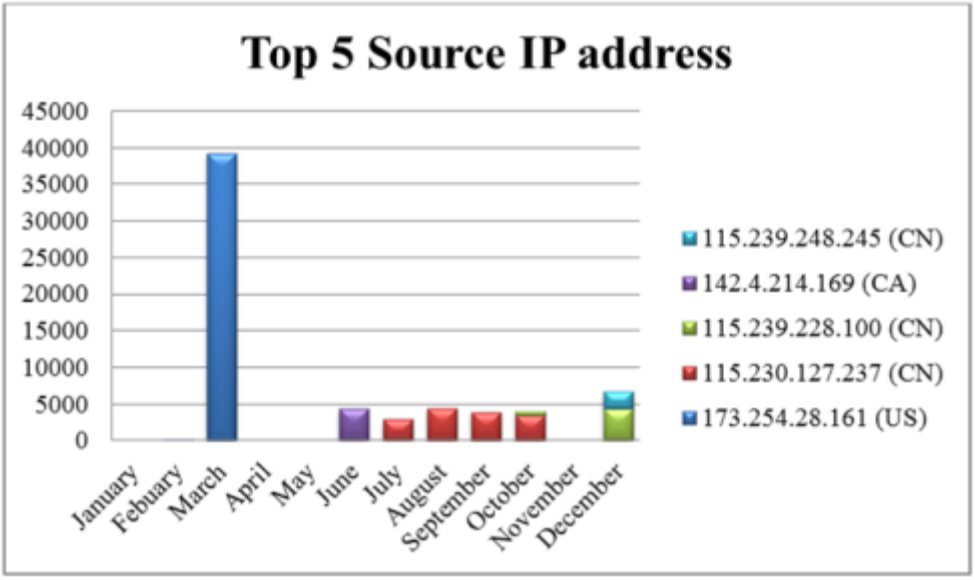


2.2. TSUBAME Statistics

The following graph shows the top 5 of Source port, top 5 of Destination port, top 5 of Source region and top 5 of Source IP Address by TSUBAME Sensor in 2015


Top 5 Source Port
45000
40000
35000
30000
25000
20000
15000
10000
5000
0
January
Febuary
March
April
May
June
July
August
September
October
November
December
80/Tcp
6000/Tcp
64316/Tcp
4445/Tcp
/Icmp


Top 5 Destination Port
9000
8000
7000
6000
5000
4000
3000
2000
1000
0
January
Febuary
March
April
May
June
July
August
September
October
November
December
23/Tcp
1433/Tcp
22/Tcp
80/Tcp
8080/Tcp


Top 5 Source IP address
45000
40000
35000
30000
25000
20000
15000
10000
5000
0
January
Febuary
March
April
May
June
July
August
September
October
November
December
115.239.248.245 (CN)
142.4.214.169 (CA)
115.239.228.100 (CN)
115.230.127.237 (CN)
173.254.28.161 (US)

2.3. Publication

- Website: www.laocert.gov.la
- E-mail:
  - Contact for administration: admin@lacert.gov.la
- Telephone: +856 305764222
- Fax: +85621 254150

3. Events organized / co-organized

3.1. Attended Training

- Participating the Training Program on Enhancing Information Security for ASEAN: focusing on ISMS and ICS (Industrial Control System) Security from 16-25 February 2015 in Tokyo, Japan.
- Participating the Basic Investigation of Computer and Electronic Crimes Program (BICEP) from 16-20 February 2015 in Bangkok, Thailand.
- Participating the Internship Training Program for Information Security Staff from 9-20 March 2015 in Jakarta, Indonesia.
- Participating the 2nd Training for Information Security Staff from 9-28 May 2015 in Jakarta, Indonesia.
- Joint the Basic Computer Network Intrusion Course from 25-29 May 2015 in Bangkok, Thailand.
- Participating the Basic Computer Network Intrusion Course from 01-05 June 2015 in Bangkok, Thailand.
- Participating the Cyber Security Fundamental on 17-21 August 2015 in India.
- Participating the Advanced Computer Network Intrusion Course from 31 August - 04 September 2015 in Bangkok, Thailand.
- Participating the Advanced Computer Network Intrusion Course from 06-10 September 2015 in Bangkok, Thailand.
- The training course on Information Security Staff for LaoCERT, organised by VNCERT on 7-11 September 2015 in Hanoi, Vietnam.
- Participating the 3rd Training for Information Security Staff from 28 September to 9 October 2015 in Jakarta, Indonesia.
- Participating the Training Program on ISMS Accreditation Bodies from 09-13 November 2015 in Jakarta, Indonesia.

3.2 Drills

- Participating the APCERT Drill on March 18, 2015.
- Participating the ASEAN CERT Incident Drill (ACID 2015) on October 28, 2015.

3.3 Workshop and Conference

- Joint the 1st ASEAN-Japan WG for Communication Check Exercise, CIIP, Capacity Building on 25-26 February 2015 in Jakarta, Indonesia.
- Participating the 2nd ASEAN-Japan information security working group on 7-8 April 2015 in Hanoi, Vietnam.
- Participating the 1st ASEAN-Japan Information Security Joint Working Group Meeting and the 3rd WG for CIIP and Capacity building on 2-4 June 2015 in Tokyo, Japan.
- Participating the Cyber Security Capacity Building: Cyber Security Compliance, Incident Handling and Assessment Training Programme from 17-26 August 2015 in Kuala Lumpur, Malaysia.
- Participating The INTERPOL' tools and service and cyber forensic investigation technique on 25-31 October 2015 in Singapore.
- The Regional Cybercrime – Cyber security Assessment Conference on 11-12 November 2015 in Manila, Philippine.
- Participating the ASEAN-Japan Information Security workshop for ISP on 9-11 December 2015 in Tokyo, Japan.

4. International Collaboration

4.1. MOU (Memorandum of Understanding)

- Being signed the MoU with Indonesia Security Incident Response Team on Internet Infrastructure Coordination Center (ID-SIRTII/CC) on May 2015 for collaboration on sharing CERT experiences and exchange knowledge of cyber security between the two countries.
- Signing the MoU with Ministry of Information and Communication, Vietnam Computer Emergency Response Team (VNCERT).

4.2. Event Participation

- The India–ASEAN Conference on Cyber Security from 18-20 January 2015 in India.
- The Cyber NEEDS (Networks Enchancing the Economy, Developmet and Security) and Development on 23-24 February 2015 in Brussels, Belgium
- The APCERT AGM & Conference on 6-10 September in Kuala Lumpur, Malaysia.
- The China-ASEAN Information Harbor Forum on 13-14 September 2015 in Nanning, China.
- The 8th ASEAN-Japan information Security Policy on 14-15 October 2015 in Jakarta, Indonesia.

5. Certifications

LaoCERT technical staff currently holds the following professional information security certificates:

- Cellebrite Certified Physical Analyst
- Computer Hacking Forensic Investigator

6. Future Plans

6.1. Future projects

- Implementing the threat monitoring system.
- Extending the TSUBAME Sensor system.
- Expending awareness the Law on preventing and combating cybercrimes to public and private sectors.
- Drafting National cyber security policies.
- Planning for Monitoring Critical National Information Infrastructure (CNII).
- Planning for Establishing Government Threats Monitoring (GTM).

7. Conclusion

During 2015, LaoCERT was trying very much to develop our team on capacity building as we had been participant the training course quite often to improve skills, knowledge and experience. However, LaoCERT have to learn more from the others CERTs in order to enhance itself to be stronger to against with cyber-attack, because LaoCERT is still less of experience comparing to the other countries in the field of cyber security,

moreover is lack of funding for staffs to attend the cyber security event which was hold by APCERT or other organizations regarding the area of cyber security.

mmCERT

Myanmar Computer Emergency Response Team – Myanmar

1. About CSIRT/ CERT

1.1. 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. mmCERT has been gradually known to Public, IT Companies, Financial Institutions, Government Organizations and Academic Service Centers in Myanmar. This 2015 annual report describes the operation and progress of mmCERT/cc during last year.

1.1.1. 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.

1.1.2. Workforce Power

Members of mmCERT/cc include from two ministries: MCIT 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 2015.

1.1.3. Constituency

mmCERT/cc, a National CERT in Myanmar is responsible for ensuring the cyber safety of all citizens as well as Government and Business Organizations include Internet Service Provider, Financial Institution, Research and Education, Vendors and Economy. mmCERT/cc has been enhancing for disseminating security information and advisories and providing technical assistance to constituencies. Some Government agencies, IT industries and service providers were closely dealing with mmCERT in 2015.

2. Activities and Operations

2.1. Daily Security News

Daily Security News is posted on mmCERT website (www.mmcert.org.mm) for the purpose of raising the security awareness among the public. It is to accomplish one of the missions of mmCERT.

2.2. Weekly Email Newsletter

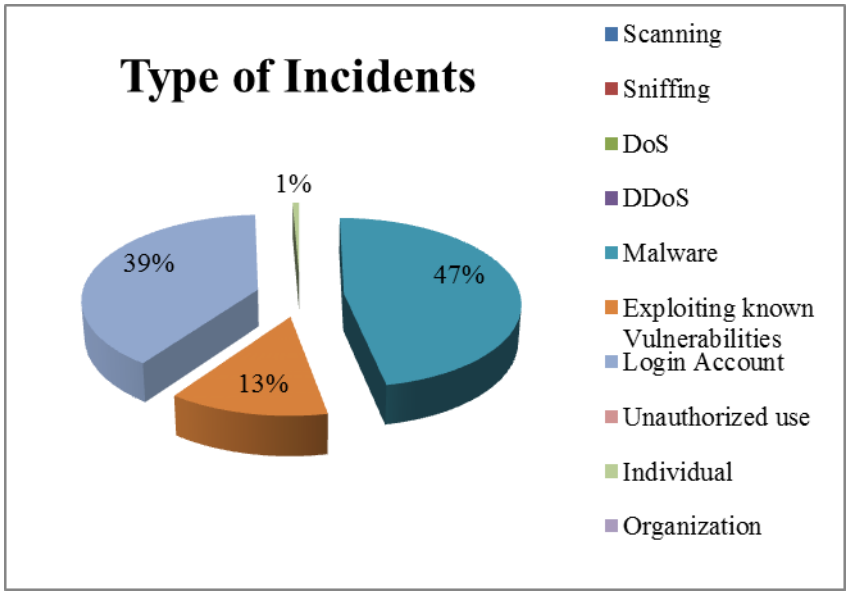
Every Friday, Weekly Email Newsletter was published and distributed to all local ISPs and constituencies starting from August 24, 2012 for the purpose of alerting the updated world-wide security news. These extracted resources are obtained as a member of APCERT and other security related information are from internet and security organizations.

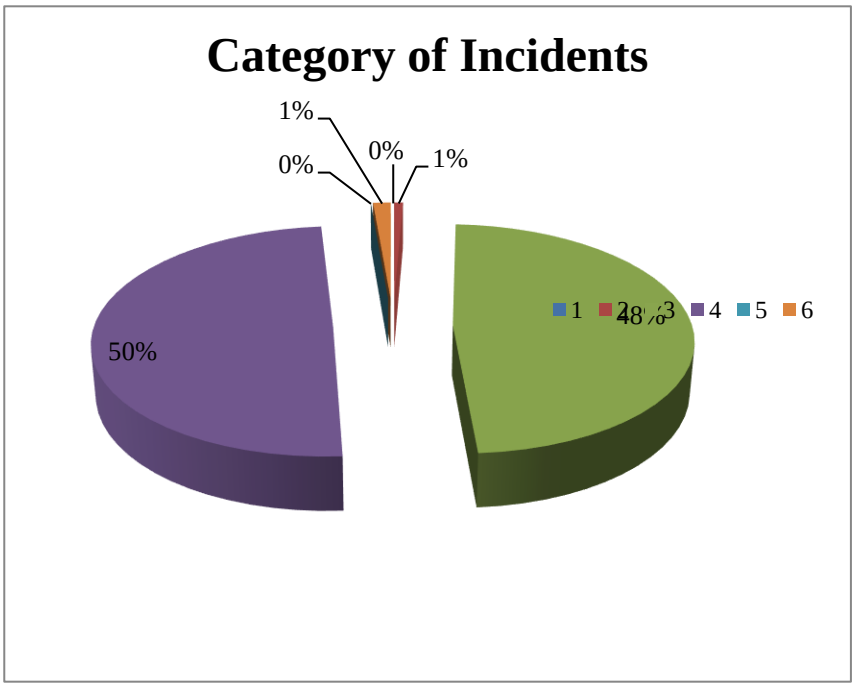
2.3. Weekly Technical Article

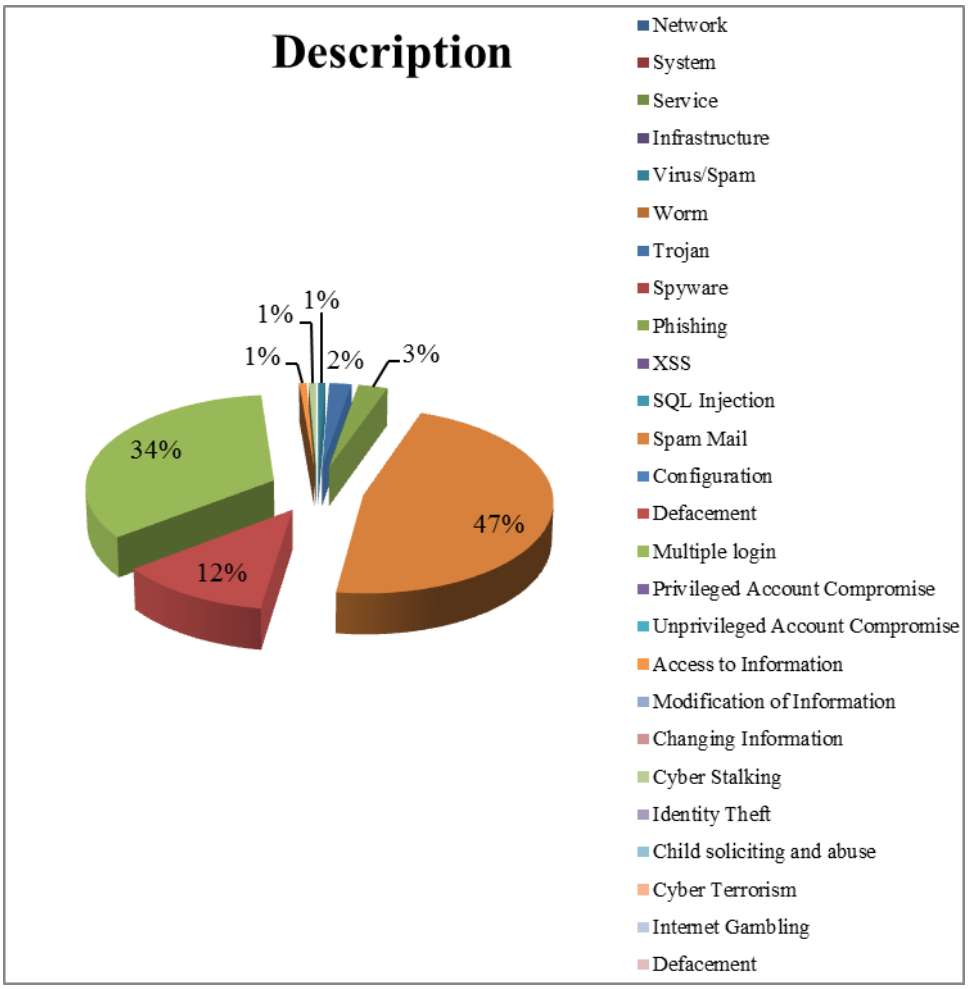
mmCERT publishes Weekly Technical Article, written in our language (Myanmar) for the purpose of promoting technical expertise and awareness to the IT persons. It is also posted on mmCERT website (www.mmcert.org.mm) since May 2013, on every Thursday.

2.4. Incident Handling Reports

The following graph shows the incidents that were solved by mmCERT in 2015. According to the results on incident analysis by mmCERT/cc, Intrusion and Malicious cases were the most prominent incident cases in 2015.

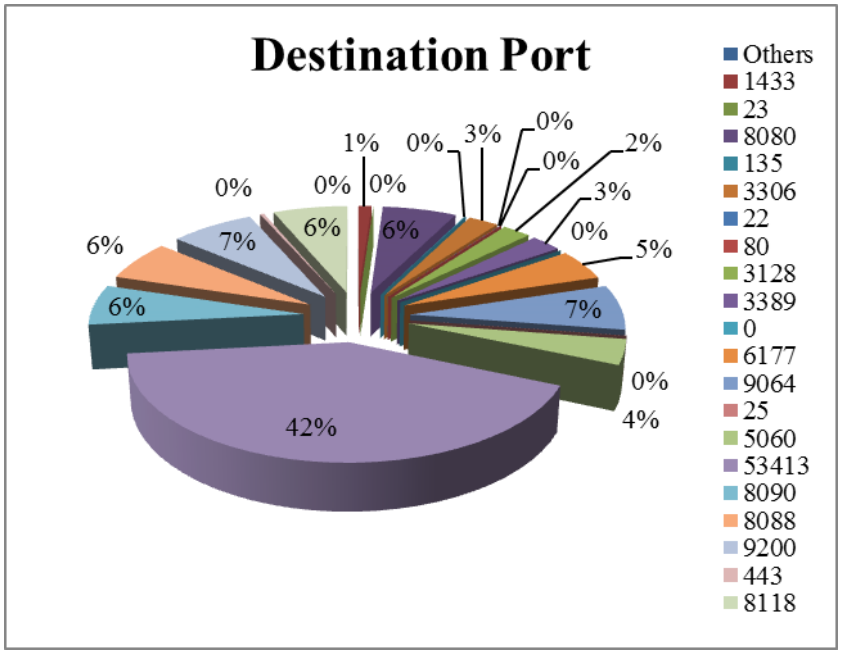


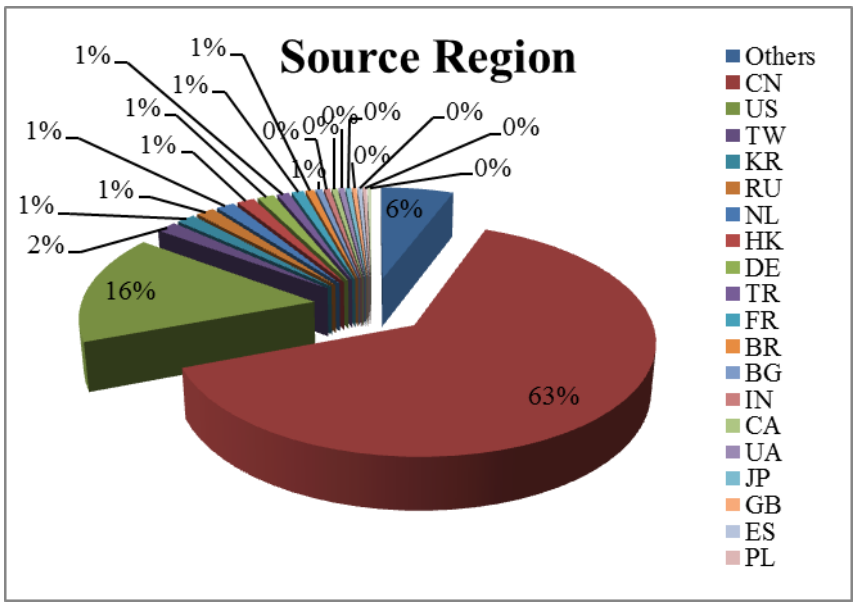


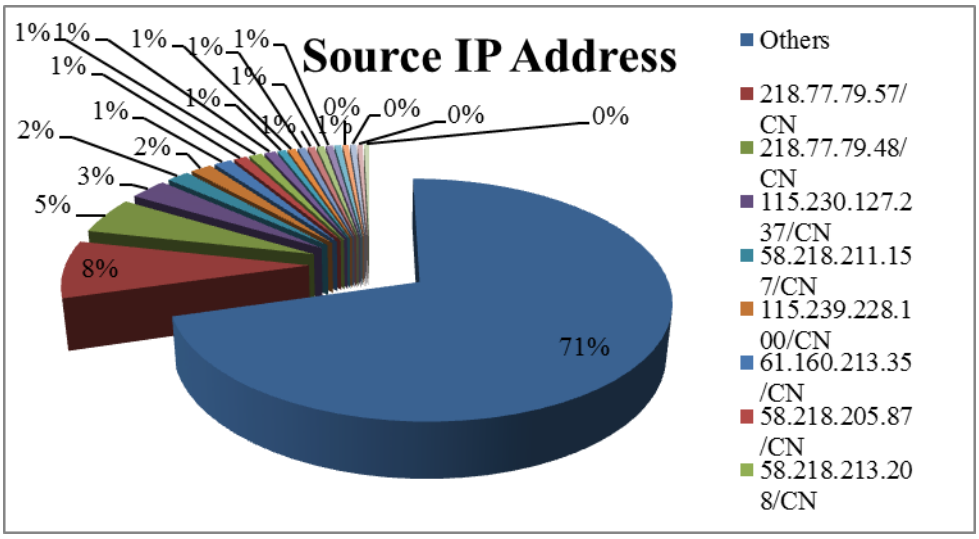

Description
1%
1%
1%
2%
3%
34%
47%
12%
Network
System
Service
Infrastructure
Virus/Spam
Worm
Trojan
Spyware
Phishing
XSS
SQL Injection
Spam Mail
Configuration
Defacement
Multiple login
Privileged Account Compromise
Unprivileged Account Compromise
Access to Information
Modification of Information
Changing Information
Cyber Stalking
Identity Theft
Child soliciting and abuse
Cyber Terrorism
Internet Gambling
Defacement

2.5. Abuse Statistics

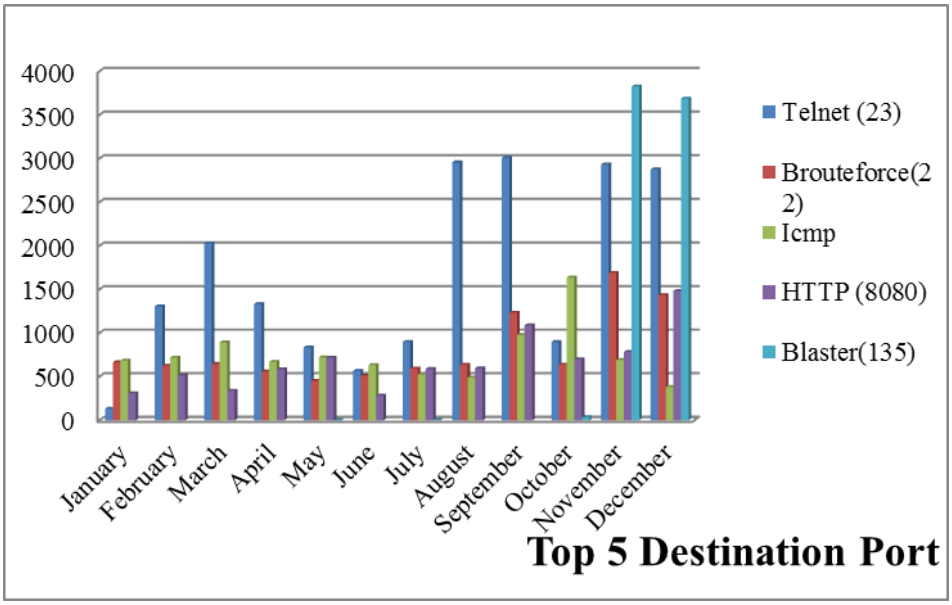
The following graph shows the top destination port and top source ip address statistics obtained from TSUBAME Sensor in 2015.

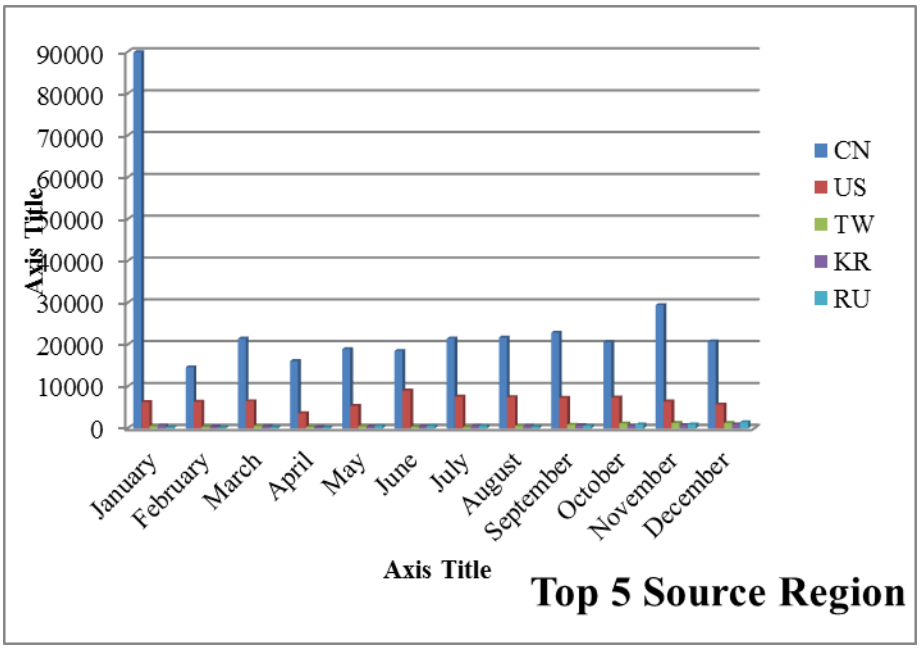






The following graphs show the top five destination ports and top five source ip addresses statistics per month in 2014.





2.6. Capacity Building

As aims to promote Capacity Building of mmCERT Members, MCIT selected the participants from mmCERT/cc. These are training programs which they attended in Oversea during 2015.

- Attending in "Advance IT Course in Law Enforcement Training", at New Delhi, India on January 7 - March 29, 2015".
- Attending in "Advanced Incident Handling Training, provide by JPCERT/cc, at mmCERT, at Yangon on March 9-12, 2015".
- Attending in" the 2nd Information Security Training" at Indonesia on May 19 - May 29, 2015".
- Attending to "Cyber Security Capacity Building Training" at Malaysia on August 16-27, 2015.
- Attending to "3rd Training Information Security for staff" at Indonesia on September 29 - October 1, 2015.

3. Events Organized/Co-organized by mmCERT

3.1. Seminar & Workshop

- Giving Seminar to Cyber Crime Unit (Myanmar Police Force) at CID, Insein in Yangon on March 17, 2015.

- Giving Seminar to West Yangon Technological University Students at mmCERT in Yangon on October 5-12, 2015.
- Giving presentations to all members of mmCERT and delegated persons by the individual mmCERT members in December, 2015.

3.2. Other Activities

- Cyber SEA Game Coaching at MICT on October 2, 2015.
- Cyber SEA Game National Level at MICT on October 28, 2015.

4. International Collaboration

4.1. Drills

- Participating in APCERT Drill on March 18, 2015.
- Participating in ASEAN CERT Incident Drill (ACID 2015) on September 24, 2015.

4.2. Other Activities

- Attending to "ASEAN-JAPAN Working Group Meeting" at Jakarta, Indonesia on February 25-26, 2015
- Participating in "the 1st ASEAN_JAPAN Information Security Joint Working Group Meeting" at Malaysia on June 3 - 4, 2015.
- Participating in “China-ASEAN Network Security Seminar” at China on November 1-5, 2015.
- Participating in "the Training Program on Enhancing Information Security: Focusing on ISMS and ICS Security & the Workshop on ISMS Promotion Policy and Accreditation Scheme in ASEAN Countries" at Indonesia on November 9 - 13, 2015.

5. Future Plan

mmCERT would like to participate and conduct in International Capacity Building projects as well as to proceed the following pending jobs and new plans.

- Incident Drill
- Standardize Cyber Security Guideline for Myanmar

- Focusing on ISMS
- Secure and Updated Version of mmCERT Web server
- Applicable Online Ticketing System

6. Conclusion

mmCERT is a developing team, we are still in need of supporting facilities and human resources. But we do hope that these necessities are going to be fulfilled in a very near future. So far, we are trying our best for our team by elaborately doing Incident Handling, efficiently providing Technical Advisories, Trainings, Seminars and Workshops to Constituencies, 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.

However the structure, working process of mmCERT were not changed too much in 2015. It still needs to develop in all sectors in terms of frame work, policy, human resources and budget. mmCERT looks forward National IT image by cooperating with international CERTs for cyber security and cybercrime as well as communication with local partners and constituencies in 2016.

MNCERT/CC

Mongolia Cyber Emergency Response Team / Coordination Center – Mongolia

1. About MNCERT/CC

1.1. 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.

1.1.1. 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 attacks 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)"

1.1.2. 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. 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

1.1.3. Constituency

Our constituencies are:

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

2. Activities & Operations

2.1. Incident handling reports

Incidents occurred in Mongolia

- 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 have contacted the owners of phishing web sites and removed seven of phishing URLs.
- On 24th November of 2015, according to the notice from IID (http://internetidentity.com), MNCERT/CC has made secure the fraudulent phishing website http://gobieducation.org by contacting its owner. Details are as follows:

  Ip address: 103.48.116.79

  URL: http://www.gobieducation.org/elitesend/1.php
- In 2015, 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.

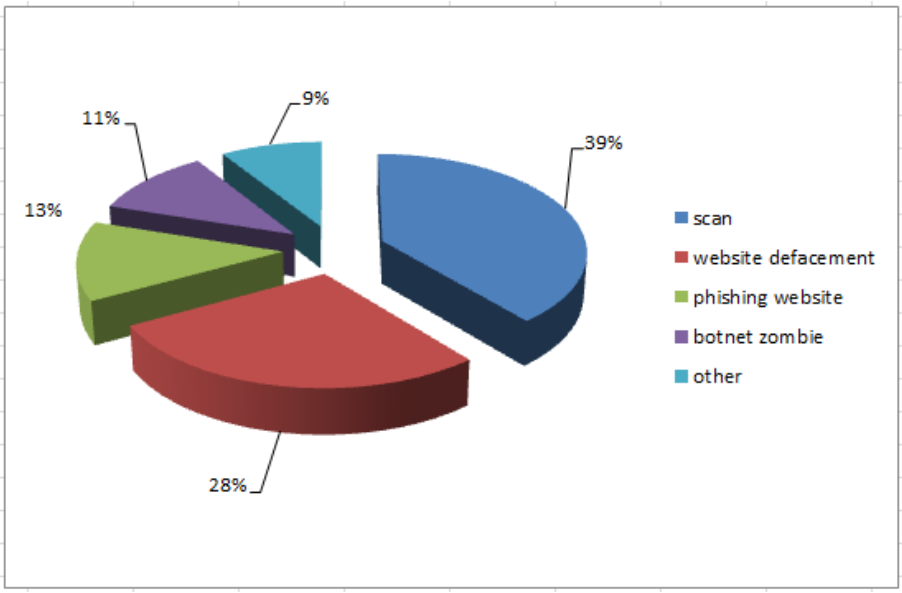
Totally, the malicious emails have sent to about 4500 clients and 6 (six) incidents have been registered.

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.

- We have detected and disinfected 9 websites of governmental organizations, in province (rural region) of Mongolia, which had been infected with malware.

2.2. Abuse statistics

MNCERT/CC's constituency covers various types of organizations such as business companies, private sector organizations, universities, non-governmental organizations and general public. The summary of acitivities carried out by MNCERT/CC during the year 2015 is given in the following chart. This chart shows about summary of the critical incidents that were registered national wide: scan 39%, website defacement 28%, phishing websites 13%, computers compromised by attackers 11%, others 9%. Comparing with the previous year, botnet zombie has been reduced slightly, but the website defacement has increased abruptly and scan threats are same as the previous year.



Scans

39% of the total threats.

Overall, after inspecting critical requests that came in 2015, the majority of the scans were to reveal website's sensitivity and to collect network hosts as well as information of hosts. These scans were made mostly to government agencies as well as individuals. It mainly shows malware propagation through websites of the private and government sectors were observed constantly. Attempt to compromise was made by examining the system whether its version is updated and patched. The growing popularity of the website incidents comes from not using the software license warranty and human resource capability.

Website defacement:

28% of the total threats.

In 2015, the number of 39 websites have been defaced due to the fault of governmental organizations' system administrators such as misconfiguration of significant file permission into "777".

Phishing website

13% of the total threats.

This type of threats have been detected mostly on hosting service providers. Links have been placed by possessing the other hosts using frequently accessed host.

Botnet and zombie IPs

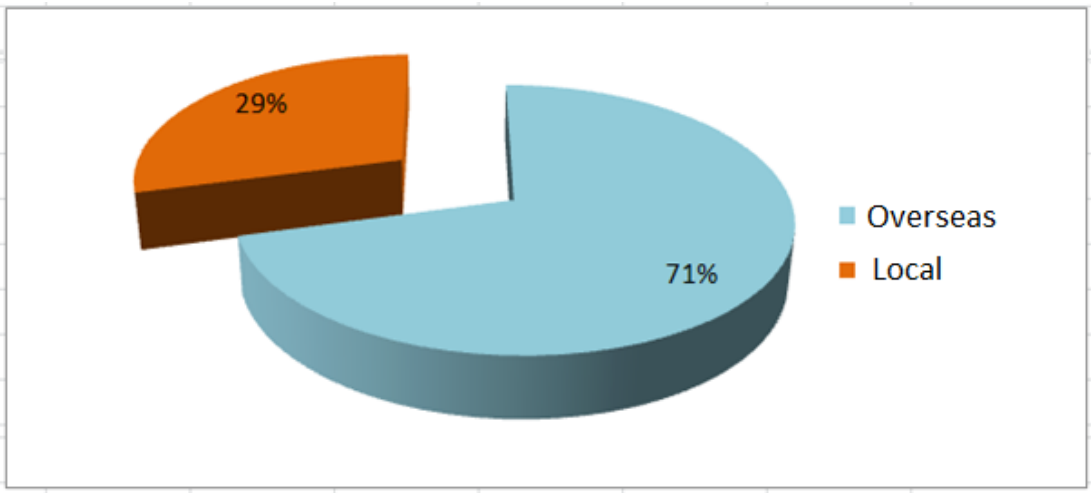
11% of the total threats.

The main reason of the compromise is that the individuals and members of governmental organizations and private sectors lack cyber security knowledge such as checking the fake email addresses, fake attachment files, fake URLs and not using the officially licensed software.

Others incidents

9% of the total threats.

In following chart shows about location of the host scans.



2.3. Publications

- "APT Threat" - Mr.Otgonpurev Mendsaikhan, MNCERT/CC board member, http://mncert.org/post.php?p=1#/10/zoomed (in Mongolian)
- "DDoS Attack" – Mr.Enkhsaikhan Pagva, MNCERT/CC board member, http://mncert.org/post.php?p=4 (in Mongolian)
- "Content Filter" – Mr.Ganbold Tsagaankhuu, MNCERT/CC consultant team member, http://mncert.org/post.php?p=6#/4/zoomed (in Mongolian)

2.4. New Services and Local Projects

"Eagle Eye" Project

We successfully initiated the project named "Eagle Eye" of which the main objective is to build an infrastructure for monitoring and detecting the attacks and intrusions from overseas into Mongolia using the sensors developed by MNCERT/CC team. In 2015, we have finished the attack map development of user interface which shows live attacks (shown on the following map).

User interface

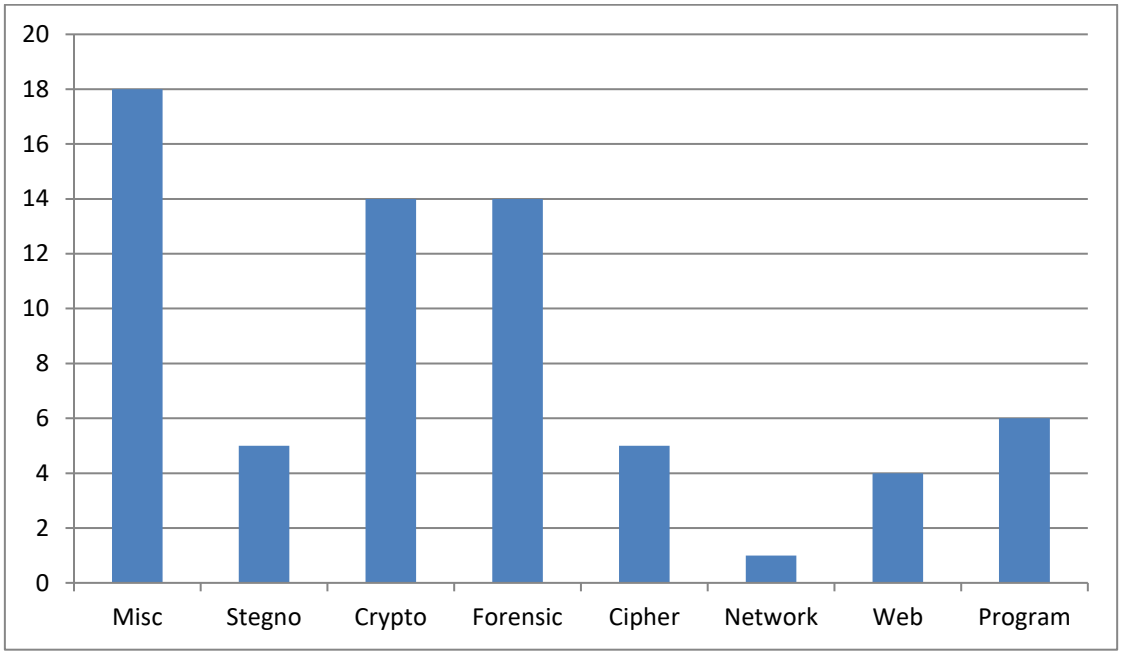
3. Events organized / co-organized

3.1. Competition

3.1.1. "Kharuul Zangi 2015" National Cyber Security Competition

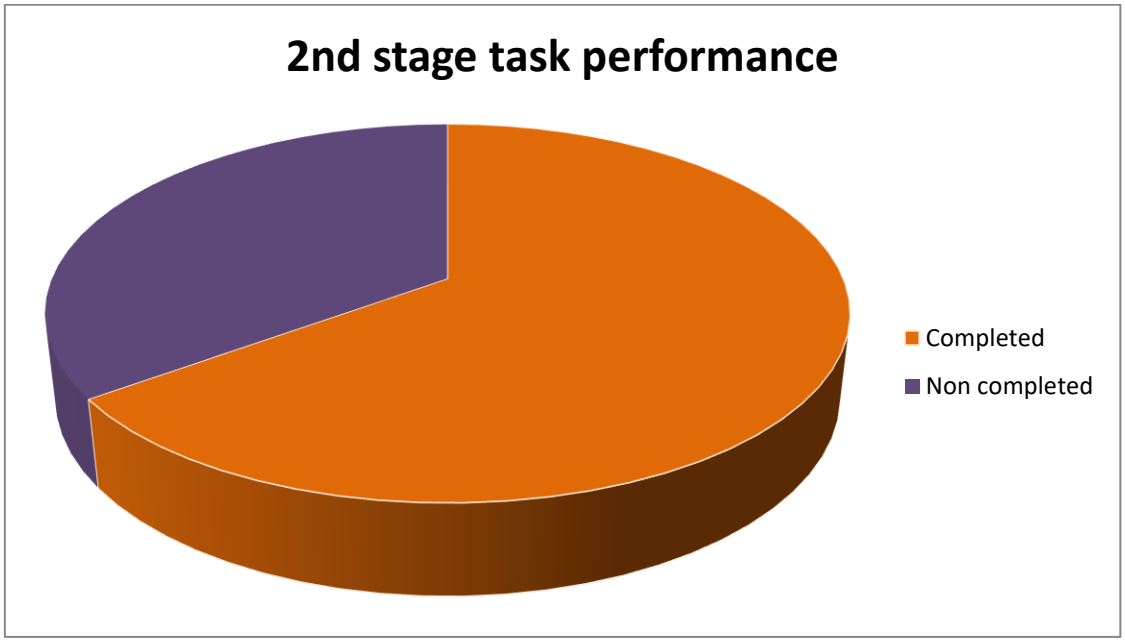
MNCERT/CC organizes a cyber security contest named "Kharuul Zangi" in order to promote the real life challenges and proper knowledge of cyber security to general public. MNCERT/CC has successfully organized "Kharuul Zangi 2015" competition between 19th September to 29th September of 2015, in collaboration with Mongolian national data center, National cyber security department, Communications regulatory commission of Mongolia, "SafeBit" LLC, Mongolian youth federation, National information technology park, Mongolian university of science and technology - School of information and communication technology 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 123 teams of 369 members, 50 teams qualified from the 1st stage. Total of 71 tasks of 8 categories have been given to be completed at 1st stage and 54 tasks have been completed out of them by the competitor teams. Following chart shows the knowledge level of the participants who completed 8 different tasks on the 1st stage.



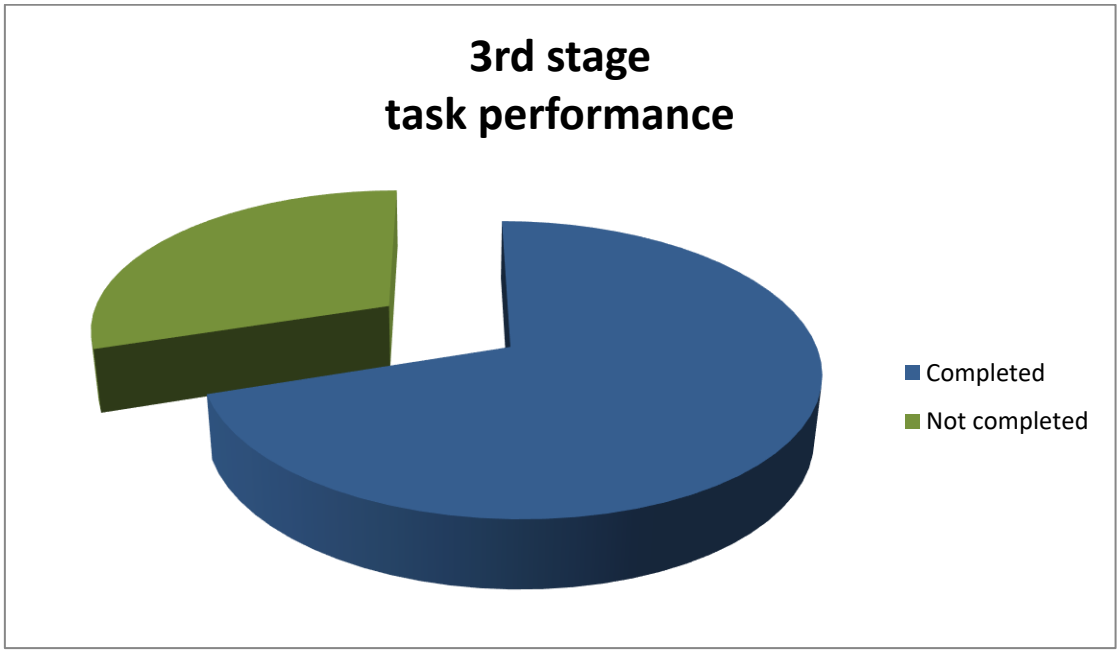
- **Forensic** –Make incident analyse based on the given data.
- **Web** – Compromise the system using website service
- **Stegno** –Find necessary information hidden in other purpose file.
- **Crypto** –Encrypt data and then decrypt it.
- **Program** – Automatic software development.
- **Cipher** - Keep the data secret and analyze it.
- **Network** – Network related task.
- **Misc** - Other types

On the 2nd stage, 20 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. 13 tasks out of 20 advanced level tasks have been completed by the teams and the task performance is shown on the following chart.



3rd stage of the competition has been held on 29th September 2015, on MNSEC-2015 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-2015.

On final stage, 7 tasks have been completed out of 10 tasks and task performance is shown on the following chart.



3.2. Conferences and seminars

MNSEC-2015 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-2015" event on 29th and 30th September of 2015 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-2015 event has been conducted successfully with the great contribution from JPCERT/CC and Team Cymru. Dr. Shinichi Horata, Information security analyst in JPCERT/CC has been invited to the event and presented "Current cyber security situation in Japan" and "How to analyze modern exploit and malware". Moreover, Jacomo Piccolini from Team Cymru has presented interesting topic through online livestream.

This event covered some of the most popular topics in cyber security field, therefore about 150 representatives, engineers and technical specialists have shared their knowledge & experience. Participation included from sectors such as financial institutions, universities, government agencies, mobile operators and internet service providers.


TRIDUM
MNSEC 2015
ЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН өдөрлөг

3.3. Training

MNCERT/CC have conducted the following trainings during MNSEC-2015 event.

- What is “information”? Firewall function, process and NG firewalls
- Information security – Audit process
- Cryptography
- Unix like system and its security

4. International Collaboration

4.1. International partnerships and agreements

- MNCERT/CC has joined the TSUBAME Project on 9th September, 2015.

- NDA with Team Cymru on 16th September 2015 and has joined as 88th member.

4.2. Capacity building

4.2.1. Training

- "Computer forensics approach to computer compromises and network intrusions" online training organized by TWNCERT on February, 2015
- "Demonstrate the using method of ADE Platform and promote the information sharing safely and easily between APCERT members" online training organized by TWNCERT on April, 2015
- "Vulnerability Handling - What goes on and how to use information that comes out of it" online training organized by TWNCERT on June, 2015
- "E-mail Driven Financial Frauds" online training organized by TWNCERT on August, 2015
- "Debugging and Exploiting Security Vulnerabilities on Routers" online training organized by TWNCERT on October, 2015

4.2.2. Drills & exercises

MNCERT/CC participated to the following Drilling excersices:

- APCERT Drill 2015 on March, 2015
- OIC-CERT 2015 Cyber security drill on August, 2015

4.2.3. Seminars & presentations

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

- Black Hat Asia 2015, on March 2015 in Singapore.
- APCERT and OIC-CERT Annual General Meeting and Annual Conference 2015, on September 2015 in Kuala Lumpur, Malaysia.
- Participated as a speaker 2015 Northeast Asia Pease and Cooperation Initiative Forum, on October in Seoul, Korea.

4.3. Other international activities

- MNCERT/CC has been taking part in APCERT Cyber Green Working Group led by MyCERT.

5. Future Plans

5.1. Future Operations

MNCERT/CC planned the following activities in 2016.

Organizations to join as a member are as follows:

- FIRST (Forum of Incident Response and Security Teams)
- APWG (Anti-Phishing Working Group)
- Global Forum on Cyber Expertise
- KZ-CERT

Events, conferences and drill to participate are as follows:

- APCERT Drill 2016 on March 2016.
- Black Hat Asia 2016 on March in Singapore
- Asia Cyber Security Conference 2016 on April
- Team Cymru Annual Event UE16 on April in Doha, Qatar
- FIRST Annual General Meeting 2016 on June in Seoul, Korea
- APCERT Annual General Meeting 2016 on October in Tokyo, Japan

Activities to organize are as follows:

- Organizing MNSEC-2016 Cyber Security Event
- Organizing “Kharuul Zangi” Cyber Security Contest among two categories: high schools and IT specialists.

6. Conclusion

2015 was year of great success and progress for MNCERT/CC. We’ve restructured our organization, established an advisory board as well as reformed our board with new members.

Also MNCERT/CC was able to establish partnership with Team Cymru as well as we were able to join the TSUBAME project. We are looking forward to a more progressive year in 2016 and greater collaboration with APCERT.

MOCERT

Macau Computer Emergency Response Team Coordination Centre – Macao

1. Highlights of 2015

1.1 Summary of major activities

During the year 2015 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 publicly available seminars on cyber security;
- Conducted workshops at the public, tertiary education and secondary education institutes on cyber security;
- Maintenance of a website as point of reference for MOCERT services;
- Assisted in the delivery of a course in cyber security topics at university and high schools.
- Performed a web server scan of Macau IP and Domain space in search of infectious code, twice a year, yielding incidents.
- Actively taking part in the cyber security community through conferences
- Speech to government IT staff 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 FIRST SIG for Traffic Light Protocol.
- Assisted in the APCERT Drill 2015 as OC, Player, Observer and EXCON
- Article publications in a local magazine called “Macau-ICT” magazine

1.2 Achievements & milestones

The following are major achievements and milestones of MOCERT

1) Transformed the Clean-PC day into a Summit

   Previously a technical workshop, Clean PC day has evolved into a major speaker heavy event in Macao. To reflect this evolution the event is heralded by the name Secure, Audit, and Forensically Evaluate Technology (SAFE-T) Summit

2) First Local Cyber Drill.

   In conjunction with the need to elevate Cyber readiness, MOCERT has test run a local cyber drill exercise.

3) Deepened cross delta interactions.

   This year brought deepening connections with the government sector both locally as well as across the pearl delta in collaboration with HKCERT.

2 About CSIRT

2.1 Introduction

MOCERT (Macau Computer Emergency Response Team) is service that is public facing from Macau New Technologies Incubation Centre.

This service is funded by MANETIC, a non-profit organization that is supported through industry and government sourced funding. This 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 2015 there are four (4) 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

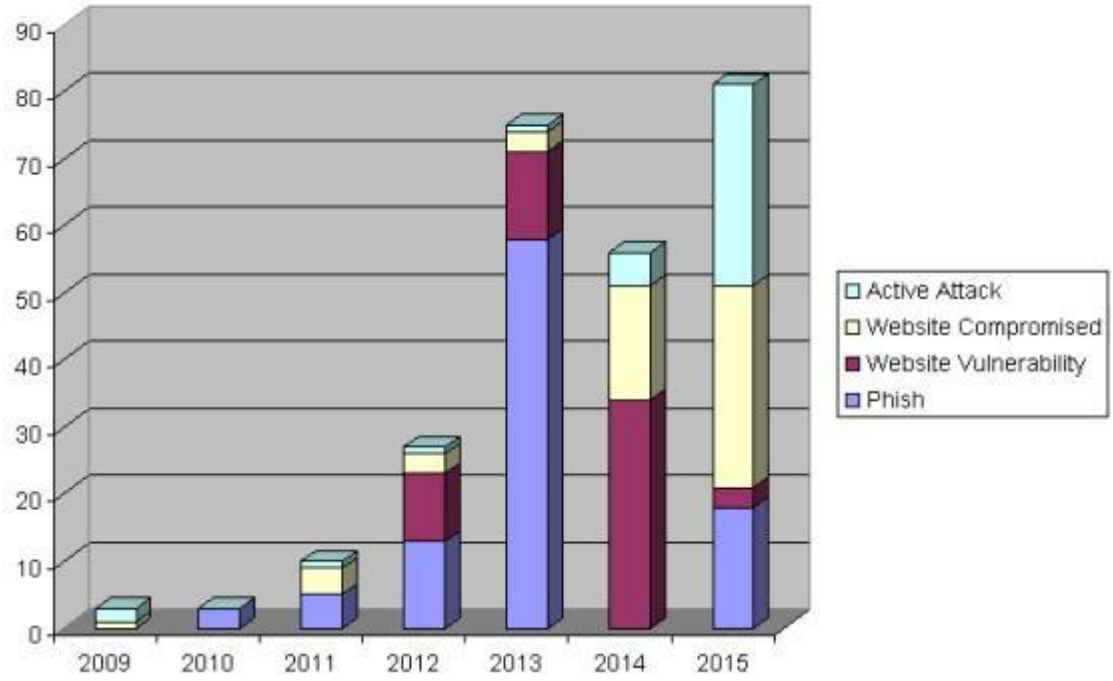
Macau Computer Emergency Response Team Coordination Centre (MOCERT) is managed by Macau New Technologies Incubator Centre in providing Macau with computer security incident handling information, promoting information security awareness, as well as coordinating on an international and local level, computer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

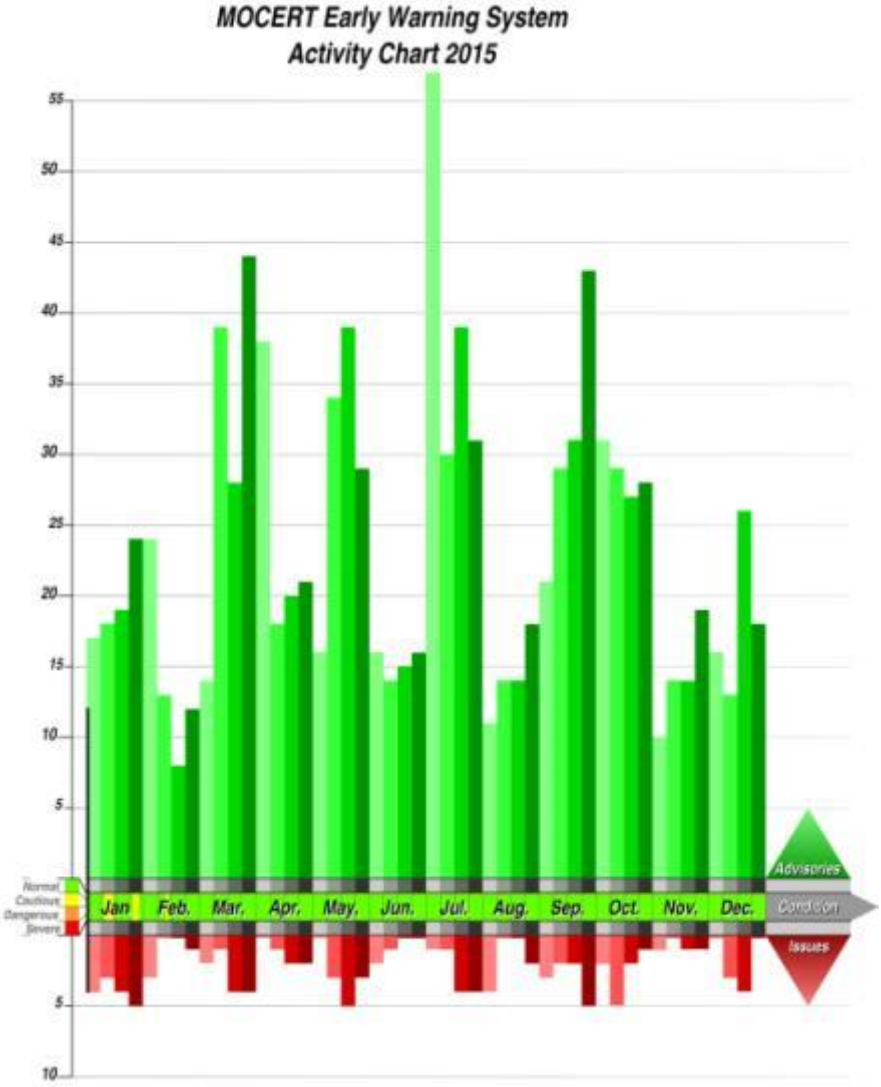
Sources of incidents are from three distinct channels.

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



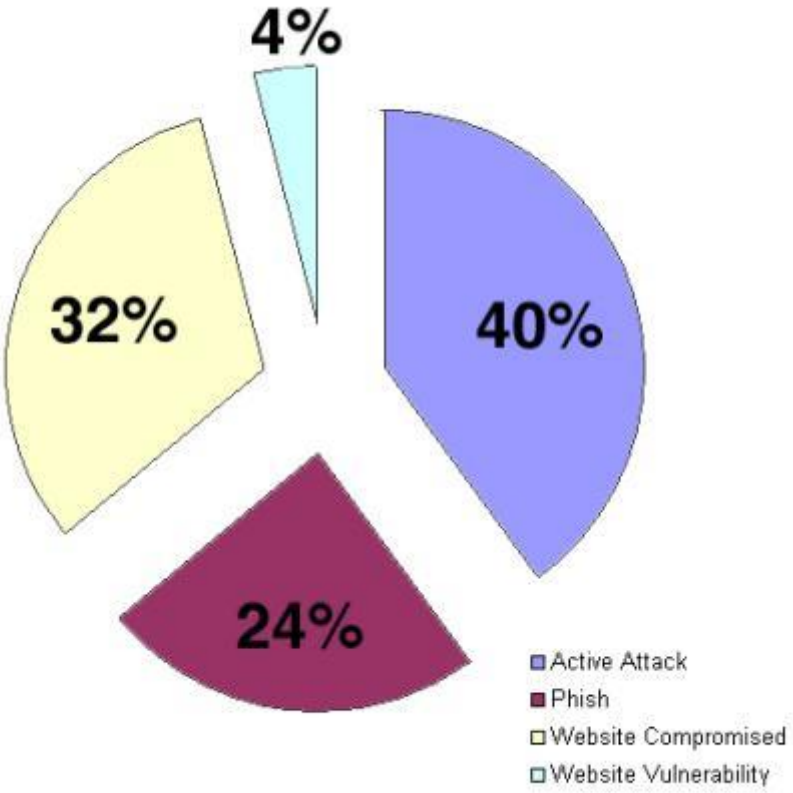
Early Warning Notices - A website collects notifications related to computer security, where all notifications are reviewed by staff to determine the impact to Macao constituency.

The notifications are then classified to Issues and Advisories and then posted. The following diagram shows the distribution of the 1216 postings in 2014 with 1119 postings being Advisories, and 97 Issues.


MOCERT Early Warning System
Activity Chart 2015
55
50
45
40
35
30
25
20
15
10
5
Normal
Cautious
Dangerous
Severe
Jan
Feb.
Mar.
Apr.
May.
Jun.
Jul.
Aug.
Sep.
Oct.
Nov.
Dec.
Advisories
Condition
Issues
5
10

3.3 Abuse statistics

The following pie graph denotes the abuse distribution as noted for the year 2015. The numbers are drawn from the incidents handled with the removal of the "web notices" as they do not constitute an abuse.



3.4 Publications

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

3.5 New services

3.5.1 CSIRT Drill Development Training

Stemming from the effort of helping out in the APCERT Drill as well as the running of the first local Industry wide cyber drill in Macau, MOCERT offers the skills back to industry that requires to develop their own cyber drill.

4 Events organized / hosted

4.1 Training

Staff 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 Drills & exercises

4.2.1 APCERT Drill

The involvement in 2015 in the APCERT drill included as a Player, Observer and EXCON. Also MOCERT assisted the Organising Committee in designing the Detailed Scenario. The event continues to be instrumental in reshaping some of the services provided by MOCERT for 2015.

4.3 Conferences and seminars

MOCERT attend both APCERT AGM in Malaysia and FIRST Berlin meeting in the year 2015.

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 Training

5.2.1.1 CSIRT Development Training

Based on ENISA material MOCERT offers to local industry training on how to set up a CSIRT.

5.2.2 Drills & exercises

5.2.2.1 First Local Cyber Drill

MOCERT has started in organizing local Cyber Security Drills as well as providing assistance in designing and running drills to local industry.

5.2.3 Seminars & presentations

5.2.3.1 Seminar on "CyberLife and Security" in UMAC

Wednesday, 02 September 2015 - A public awareness seminar designed for University students.

5.2.3.2 "Vulnerability Testing - Know thyself" Seminar

Tuesday, 21 July 2015 - A public awareness seminar about knowing on how to self check what services are placed online, from the outside looking in.

5.2.3.3 Manetic and MOCERT attended APrIGF 2015

Wednesday, 01 July 2015 - Provided a talk on the Cyber Security situation in Macau

6 Future Plans

6.1 Future projects

Future projects include automation of data collection, presentation, and reporting for the purpose of better understanding the weaknesses of the constituency in protecting against cyber attacks.

6.2 Future Operation

The above expected project will release some work staff from current operation and allow the staff to perform more teaching and training roles. This will mean that MOCERT will alter part of its operation to expand the workforce effort in assisting CSIRT function in other organization within its constituency to make MOCERT function more effective.

7. Conclusion

2015 has been a year where our services improved as sources of incident were refined and staffing stabilized. The major challenges up ahead are automation of services whilst grabbing the opportunity of recently trained staff that have restored capacity and functionality, and expanded the available skill set with malware analysis and in depth vulnerability scanning. With the planned changes of automation it is envisaged MOCERT will be able to allocate more time in training its constituency in CSIRT development 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 Business and Education sector's cyber space. MonCIRT provides Incident Prevention and Response services as well as Security Quality Management Services. 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;
- Share cyber security information with Mongolian Chamber of Trade and Industry, MOSA, Erdemnet ISP, other ISPs, MNCERT and Government Organizations coordinate activities with them;
- Such other functions relating to cyber security as may be prescribed.

MonCIRT services are available for all business entities, education institutions and 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 - 76113286
  - email: info@moncirt.org.mn
- World Wide Web: http://www.moncirt.org.mn/

1.1.1. Establishment

MonCIRT was established in 2006 as NGO. From 2006 till 2013 MonCIRT operate as sole national CSIRT of Mongolia. In December 2011 the Government of Mongolia established National Cyber Security Authority and whole government entities covered by this organization. From 2014 MonCIRT acts as the focal point for cyber security for the private persons, educational institutions and business entities.

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. The senior management of MonCIRT oversees the overall direction and operation of the team. In 2015 we hired 5 new staffs, organized internal trainings for them.

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 & Operation

2.1. Activities

The summary of activities carried out by MonCIRT during the period from January to

December 2015 is given in the following table 1:

Activities	Year 2015
Common Security Incidents (failure, email attack, malware, improper usage, attrition e.t.c) handled	312
Security Alerts issued	164
Advisories Published	15
Vulnerability Notes Published	39
Security Guidelines Published	2
Trainings Organized	2
Mongolian Website Defacements tracked and handled	29
Open Proxy Servers tracked and handled	3
Bot Infected Systems tracked and handled	424
Phishing (mirror) web sites tracked and removed	6
Phishing cases (email, chat, social sites) handled	458

Table 1. Summary of activities

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 2015 MonCIRT handled 1232 incidents which was 8 times increase of the previous year. The 8 times increase of the number of incidents was due to the our direct chat system, number of new experts and referral cases as a result of closer collaboration with global security researchers and organizations. The major category of security incidents was phishing (458 cases) and Botnet. The phishing cases increased 810%.
In 2016 we ask our constituency to pay more attention on phishing activities.

From January through December 2015, the MonCIRT received 735 email messages and more than 250 hotline calls reporting computer security incidents or requesting information. About 61% 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.

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.

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 mail list. Once serious alerts, vulnerabilities, threats appears we publish them on web site, social

and news portals on Mongolian language,

During reported period we published 220 alerts, advisories, notes on our web site, other web sites like news.mn, cybersafety.mn, medee.mn, time.mn e.t.c.

2.3. Cyber threats intelligence

Malware and the malicious web

In 2015 MonCIRT had implemented real time chat system with administrators and this system helped us to collect more information on faced threats. Благодаря этой системы мы собирали 180 процентов больше информации об угрозах чем в прошлом году. Кроме того мы открыли "System Admins" face page (https://www.facebook.com/Монголын-Систем-Администраторуудын-Холбоо-1413925735581985/) and allow to discuss threats trends interactively.

From September 2015 MonCIRT start some joint activities with Mon Pass CA and promoting the usage of digital certificates in Mongolia.

Based on data for 2015, it is not surprising that the bulk of the security incidents disclosed were carried out with the majority of attackers going after a broad target base while using off-the-shelf tools and techniques. We attribute this to the wide public availability of toolkits and to the large number of vulnerable web applications that exist on the Internet.

MonCIRT participated in the information sharing campaign, raising awareness of the event and hosting a copy of the advice and links to the clean-up tools. Additionally we received and processed the sinkhole data, which we then distributed to Internet Service Providers (ISPs) to allow them to assist their customers who had been infected. For commercial organisations, the impact of ransomware cannot be underestimated. User education about cyber risks, along with robust security controls and a proven incident management capability, will help businesses to minimise the risk from, and impact of, crimeware like Gameover ZeuS and Cryptolocker.

3. Events organized / co-organized

3.1. Training / Education

In 2015 the MonCIRT jointly with Government Cyber Security Division, ITPTA, MNCERT organized workshops and trainings like "Infosec open day", "Security to everyone", Kharuulzangi 2015 contest e.t.c focused on targeted audience such as government and financial sector IS officers, System Administrators, ISPs. Experts from industry are delivering lectures in these workshops apart from MonCIRT staff.

The MonCIRT offers different training courses. 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 2015 included the following:

- *Network security management and configuration*
- *Information Security System of Organization based on MNS ISO/IEC 27001*
- *Network Monitoring and Intrusion Prevention.*
- *Fundamentals of Incident Handling and Management*

In addition MonCIRT was invited to deliver speeches and presentations on various occasions for the Government, Universities, Banks and associations.

3.2. Drills

In 2015 MonCIRT cannot organize local network security drill-IV due to financial limitation and economic crisis. Because in 2015 hired new, skilled experts MonCIRT plan to regularly participate drills of APCERT, FIRST from 2016.

3.3. Seminars

In order to create awareness and build Network Security skills within the constituency MonCIRT conducted the following conferences, seminars successfully:

a. MonCIRT was one of the partner in organization of ITPTA open seminar of 2015 and participated in conference dedicated to this event. The governing board director of MonCIRT prof Khaltar Togtuun was one of key speaker of this conference.

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:

a. Conducted presentations during the Annual "Security Open Day" 2015 conference on themes "**The rise of machine-to-machine attacks**".

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

4.2. Publications

The MonCIRT published 15 advisories and 39 vulnerability notes in 2015. Among the criteria for developing an advisory are the urgency of the problem, potential impact of

intruder exploitation, and existence of a software patch or workaround. On the day of release, we send advisories to a Mongolian Chamber of Trade and Industry (MCTI) mailing list and network administrators mailing list.

MonCIRT Security Practices

MonCIRT security practices are easy-to-implement guidance for experienced system administrators. The practices are technology-neutral, so they apply to many operating systems and platforms. Practices available in the repository of MonCIRT.

Other Security Information

The MonCIRT captures lessons learned from handling incidents and vulnerability reports and makes them available to users of the Internet through a web site archive of security information. These include answers to frequently asked questions and "tech tips" for systems administrators.

4.3. Certification & Membership

We applied for FIRST Memberships in the end of 2015:

5. International and Domestic Collaboration

5.1. MoU

We signed MOU with Mongolian Chamber of Trade and Industry (MCTI) on cooperation in cyber security field and distribution of security alerts, notes, advisories to MCTI member companies.

5.2. Event participation

MonCIRT participated in a number of international collaboration events listed below:

- Participated in the APCERT AGM and Conference in Malaysia
- Participated in the FIRST AGM and Conference in Berlin and participated in discussions actively;
- Newly deployed 2 new sensors of Tsubame project of JPCERT/CC.

5.3. International incident coordination

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

6. Future Plans

In 2016 MonCIRT plan to pay more attention on capacity building and to organize more internal trainings for new staffs. In addition we would like to participate in International Capacity Building events as well as to proceed the following pending jobs and new plans.

- Develop internal Information dissemination system
- Sign MOUs with Mongolian ISPs
- Build Incident Monitoring system in Mongolia

7. Conclusion

MonCIRT will continue to improve our financing strategy, proactive and quality management services including educational program, awareness campaigns, presentations and publications and also will pay attention on attracting of new members. Henceforth, MonCIRT shall focus on extending and empowering its constituency area involving more and more companies, creating membership. Thus, MonCIRT continue to act as an real general private sector oriented CSIRT

We will continue to conduct the Annual "Security Open Day" and will organize National Conference on Cyber Security under name "InfoSec Mongolia 2016" while finding new ways to reach an even wider audience.

MonCIRT shall continue to participate in regional events of APCERT and will become FIRST member, participate in events and workshops of FIRST.

MonCIRT is a self-financing team and still in need of supporting facilities. We are trying our best for our team by elaborately doing Incident Handling, efficiently providing Technical Advisories, Trainings, Seminars and Workshops to Constituencies, effective Capacity Building to our Technical Team members, enhancing Public Awareness Activities as much as we can.

Contact Information

Postal Address: Mongolian Cyber Incident Response Team (MonCIRT).
Tokyo street, Nisora Tower 702. Bayanzurkh District. Ulaanbaatar, Mongolia, 13381
info@moncirt.org.mn

Incident Response Help Desk
Phone: +976-76103286
Fax : +976-76113286

MyCERT

Malaysian Computer Emergency Response Team – Malaysia

1. CYBERSECURITY MALAYSIA

CyberSecurity Malaysia, an agency of the Ministry of Science, Technology and Innovation of Malaysia, has been given the mandate by the Government to provide expertise and support in ICT security and to continuously assess and mitigate cyber threats to the nation. This agency begins as the Malaysian Computer Emergency Response Team (**MyCERT**) in 1997 and in 2009, established as CyberSecurity Malaysia with expanded services in the area of cyber security.

CyberSecurity Malaysia has the vision of being a globally recognized national cyber security reference and specialist centre by 2020 with the mission of creating and sustaining a safer cyberspace that will promote national stability, social well-being and wealth creation.

The main roles of CyberSecurity Malaysia are:

i. To assist the Government in the implementation of the National Cyber Security Policy (**NCSP**);
ii. To provide Cyber Security Emergency Services and to act as the national cyber security technical coordination centre;
iii. To conduct Cyber Threat Research and Risk Assessment;
iv. To provide Cyber Security Quality Management Services; and
v. To build the capability and capacity in the field of cyber security (Training) and to create awareness and a culture of cyber security (Outreach).

In fulfilling these roles, this agency has developed various services, namely:

i. The Cyber999™ Help Centre;
ii. Computer Emergency Response Services;
iii. Digital Forensics / CyberCSI™;
iv. Security Management and Best Practices;
v. Cyber Security Assurance;
vi. Vulnerability Assessment Services;
vii. The Malaysia Common Criteria Certification Body (MyCB);
viii. Information Security Professional Development;
ix. Outreach Programmes; and

x. Cyber Security Policy Research.

For the APCERT Annual Report, CyberSecurity Malaysia will emphasis on services and activities provided by the MyCERT Department, as the services provided by this Department is relevant to the collaboration.
More information about CyberSecurity Malaysia can be found at: http://www.cybersecurity.my.

2. THE MALAYSIAN COMPUTER EMERGENCY RESPONSE TEAM (MyCERT)

MyCERT provides a point of reference for the Internet community in Malaysia to manage computer security incidents. It provides assistance in handling incidents such as intrusion, identity theft, malware infection, cyber harassment and other computer security related incidents.
Currently, MyCERT provides the Cyber999 service, which is the computer security incident handling and response help centre, and the CyberSecurity Malaysia Malware Research Centre.
More information on MyCERT can be viewed at: http://www.mycert.org.my.

2.1 The Cyber999

MyCERT operates the Cyber999 services for Internet users and organizations to report or escalate computer security incidents. MyCERT's website at: http://www.mycert.org.my displays the channels to report security incidents, Internet abuses and grievances to the Cyber999 Help Centre.
To date, this service has:

i. Responded to 9,915 incidents, with 98% incident resolution;
ii. Increased in receiving more data feeds related to Cyber Blackmail and Ransomware; and
iii. Successfully handle high profile incidents such as the Advanced Persistence Threat (APT) attacks, Trojans, and mobile phone malware.

2.2 The Malware Research Centre

MyCERT also manages the CyberSecurity Malaysia Malware Research Centre (**MRC**) that was launched on December 2, 2009. The centre operates a distributed research network for analysing malware and computer security threats. Collaboration with trusted parties and researchers in sharing cyber threat research information allow for

further strengthening and understanding of the threats being faced. Among the activities of the MRC are as follows:

i. To conduct research and development work in mitigating malware threats;
ii. To produce advisories and reports related to the latest threats;
iii. To monitor threats via the distributed Honeynet project; and
iv. To collaborate in malware research with universities, CERT's and international organizations.

CyberSecurity Malaysia through MyCERT, has marked another success story in 2015 through the launched of the Lebahnet 2.0, a Honeypot based distributed system that able to alert security administrator on source of attack. In addition, MyCERT has increased the collaboration with various CERTs/CSIRTs by sharing the malware analysis and coordinating facility services at the international level.

2.3 Constituency

MyCERT's constituency is the Malaysian Internet Users. Computer security incidents within Malaysia that are reported either by the Malaysian public or international organizations will be resolved by assisting the complainants on technical issues regarding the incident. If the incident involves cross border matters, MyCERT will request trusted parties in the respective countries or constituencies to assist in resolving the security issues.

2.4 MyCERT's Activities & Operation

2.4.1 Incident handling reports and abuse statistics

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

In 2015, MyCERT had produced the following cyber threat notifications:

i. 69 advisories
ii. 19 alerts
iii. 12 security summary reports

The specific list of the advisories, alerts and summary reports can be viewed at:

https://www.mycert.org.my/en/services/advisories/mycert/2015/main/index.html

MyCERT under its Cyber999 service had successfully resolved more than 98% of the 9,915 incidents reported. As in the previous years, the bulk of the reported incidents was related to the following:

i. Spam 35.7%
ii. Fraud 32.8%
iii. Intrusion 17.3%
iv. Malicious Codes 5.7%
v. Cyber Harassment 4.5%
vi. Denial of Service 0.4%
vii. Intrusion Attempt 3.1%
viii. Content Related 0.3%
ix. Vulnerabilities Report 0.2%

The following chart shows the reported cases managed by MyCERT for the year 2015:

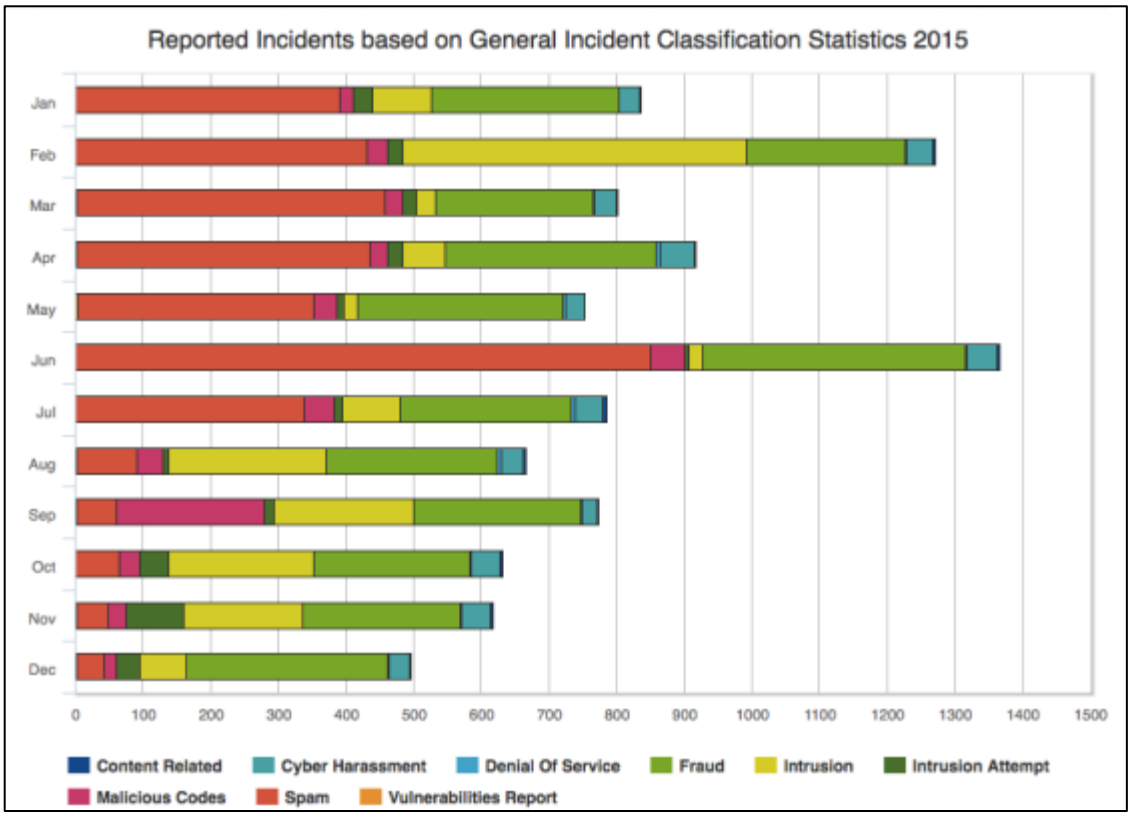


Chart 1: Reported Incidents handled by MyCERT in 2015

More information on the Cyber999 service statistics can be viewed at https://www.mycert.org.my/statistics/2015.php

2.5 MyCERT's Events Involvement And Achievements

As in the previous years, MyCERT actively participated in IT security events by providing technical support, attending various trainings, seminars/conferences and meetings. MyCERT members contributed their expertise in the following events:

2.5.1 Cyber Drills

MyCERT is the organizer of the Organization of the Islamic Cooperation – Computer Emergency Response Team (**OIC-CERT**) Cyber Drill. This international exercise was conducted on 5th August 2015 with the theme "Global Alliance for Cyber Green Achievement". The objective of the drill is to test the communication channels, procedures in handling contingencies and the technical capabilities of participating teams in handling cyber incidents. Thirteen (13) CERT teams from eleven (11) countries had participated in the exercise.

Besides the OIC-CERT Cyber Drill, MyCERT was also involved in two (**2**) other international Cyber Drills which are:

i. APCERT Drill (18th March 2015); and
ii. ASEAN CERT Incident Drill – ACID (28th October 2015).

2.5.2 Trainings

Several workshops or hands-on training were conducted by MyCERT in year 2015 on topics such as:

i. Network Security
ii. Log Analysis
iii. Information Security Management
iv. Intrusion Detection Prevention
v. Incident Handling & Network Security

2.5.3 Presentations

MyCERT has been invited to talk in various international conferences or seminars. Among the distinguished events were:

i. The CISCO International Conference on Cyber Security and Cyber Law 2015, Kathmandu, Nepal;

ii. The FIRST TC, Amsterdam, Netherlands;
iii. The APWG E-Crime 2015, Barcelona, Spain;
iv. The FIRST Conference, Berlin, Germany;
v. The CARIS Workshop, Berlin, Germany;
vi. The NatCSIRT Meeting, Berlin;
vii. The 3rd International Conference Recent Treads in Engineering and Technology (ICRET), Istanbul, Turkey;
viii. The China-ASEAN Information Harbour Forum, Naning, China;
ix. The 3rd International Conference on Artificial Intelligence and Computer Science (AICS), Penang, Malaysia; and
x. The FIRST TC, Istanbul, Turkey

Apart from the international security events, MyCERT members had also participated in 20 local events throughout 2015. This is MyCERT's contribution towards providing awareness of security awareness at the national level.

2.5.4 Tools Developed

MyCERT has developed a Consolidated Cyber Threat Research Centre (**CTRC**) Portal Prototype that allowed multiple malware projects be consolidated through one portal. This enabled the team to efficiently and effectively conduct research on malware.

2.5.5 Paper Publication

MyCERT has contributed to the cyber community by providing few articles in various publications:

i. Application of Case Based Reasoning in IT Security Incident Response, 3rd International Conference Recent Treads in Engineering and Technology (ICRET), Istanbul, Turkey [September 2-3, 2015]
ii. Utilizing Past Experiences of Incident Handlers For Realizing A CBR Recommender in IT Security Incident Response, 3rd International Conference on Artificial Intelligence and Computer Science (AICS), Penang, Malaysia [October 12 – 13, 2015]

2.5.6 Social Media

Technological advancement through social media has provided valuable tools for MyCERT to disseminate information across a wide audience. MyCERT through

Facebook account https://www.facebook.com/mycert.org.my had gathered 1,898 likes and 1,122 followers at MyCERT Twitter account https://twitter.com/mycert.

Being the technical reference centre of the country, MyCERT is always invited by the media to talk on radio and television programs regarding cyber security related matters.

3. INTERNATIONAL COLLABORATION

Malaysia 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.

3.1 Working Visit

CyberSecurity Malaysia conduct working visits to relevant organizations overseas to further enhance the country's cyber security condition. The objective of the visit is to seek potential collaboration in a two way knowledge sharing.

This agency also received working visits from foreign organizations whom have the similar objectives among them are:

i. ICT Czech Republic;
ii. The National Commission On Research, Science And Technology (NCRST), Namibia; and
iii. Organization of the Islamic Cooperation, Saudi Arabia.

3.2 Memorandum of Understanding (MoU)

Listed are some of the official collaborations in matters of cyber security between CyberSecurity Malaysia and the following agencies:

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);
iv. CERT Australia, Australia;
v. The National Information Technology Development Agency of Nigeria (NITDA);
vi. King Saud University of Saudi Arabia;
vii. Traffic Observation and Management Ltd, Ireland;
viii. Decision Group Inc., Singapore;

ix. Military College of Signals – National University of Sciences & Technology (MCS-NUST) Humayun Road, Rawalpindi, Pakistan;
x. The State Technical Service Republican Enterprise Founded On The Right Of Economic Competence Of The Agency Of The Republic Of Khazakhstan On Communication And Information;
xi. Indonesia Security Incident Response Team On Internet Infrastructure/ Coordination Centre (ID-SIRTII/CC), Indonesia;
xii. Direction Generale de la Securite des Systemes d' information "DGSSI", Morocco;
xiii. Alliacom France;
xiv. IT Protective Security Services Sdn. Bhd. (ITPSS), Brunei; and
xv. Thailand Computer Emergency Response Team (ThaiCERT).

3.3 New Partnerships and Existing Cooperation

Amongst the potential partnerships and existing cooperation in the area of cyber security that CyberSecurity Malaysia is involved in is:

i. As the Permanent Secretariat of the Organization of Islamic Cooperation - Computer Emergency Response Team (**OIC-CERT**), CyberSecurity Malaysia is facilitating cooperation and interaction among the member countries; and
ii. Convenor for the APCERT Cyber Green Working Group - CyberSecurity Malaysia 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 objective is to have a healthy Internet network environment in the region.

4. FUTURE PLANS

Since the establishment of CyberSecurity Malaysia, this agency strives to improve the service capabilities and encourage local internet users to report security incidents to the Cyber999 help centre. 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 capability, CyberSecurity Malaysia will relentlessly encourage the staffs to obtain certifications in information security. In addition, staffs are encourage to attend trainings, give presentations and write publications at the

international security platforms. This will assist the staffs to improve their contribution in knowledge and experience sharing in the information security field.
Development of in-house tools used in mitigating security threats to assist the public and industry to secure and utilize their computer when performing online activities.
To encourage a safer cyber environment, CyberSecurity Malaysia realizes the need to work together with the local and international security organizations through the establishment of formal relationship arrangements such as the Memorandum of Understandings (MoU) and agreements.
This agency will continue organizing national events such as the Cyber Security Malaysia Award, Conference and Exhibition, 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 organize 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 advise and assistance especially in becoming members to international security community such as the APCERT, FIRST and OIC-CERT.

5. 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 the constituencies and 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 develop new and enhance existing 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 in the region 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 NZ 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 is a key element of the New Zealand Cyber Security Strategy released in December 2015.

This strategy recognises that the use of the internet in New Zealand increases, so too does our vulnerability to cyber threats.

We work with national significant organisations to help protect them against advanced malware.

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;
- The provision of a single point of contact for enquiries;
- 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 CERT community and global partners to promote greater cooperation; and
- Work in coordination with other organisations acting in the domestic cyber security space (e.g. Connect Smart www.connectsmart.govt.nz, New Zealand Police, the department of Internal Affairs, New Zealand Internet Task Force, Netsafe etc)

1.1.1. Workforce

The NCSC comprises of a team of cyber security focussed technical, policy and incident coordination professionals. Over the 2014-15 year the NCSC has grown its capacity and capability in a number of areas, particularly Outreach and Engagement team, increasing the NCSC's capacity to engage with public and private sector organisations, promoting cyber awareness and providing incident support and mitigation advice.

1.1.2. 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. Activities & Operations

2.1. Incident handling reports

The NCSC recorded a total of 190 cyber security incidents for the 12 months to 30 June 2015.

Of the 190 reported (fig 1.1), 114 incidents were identified as targeting government systems, 56 targeting private sector –with a further 20 incidents where the sector targeting was not identified in the reporting.

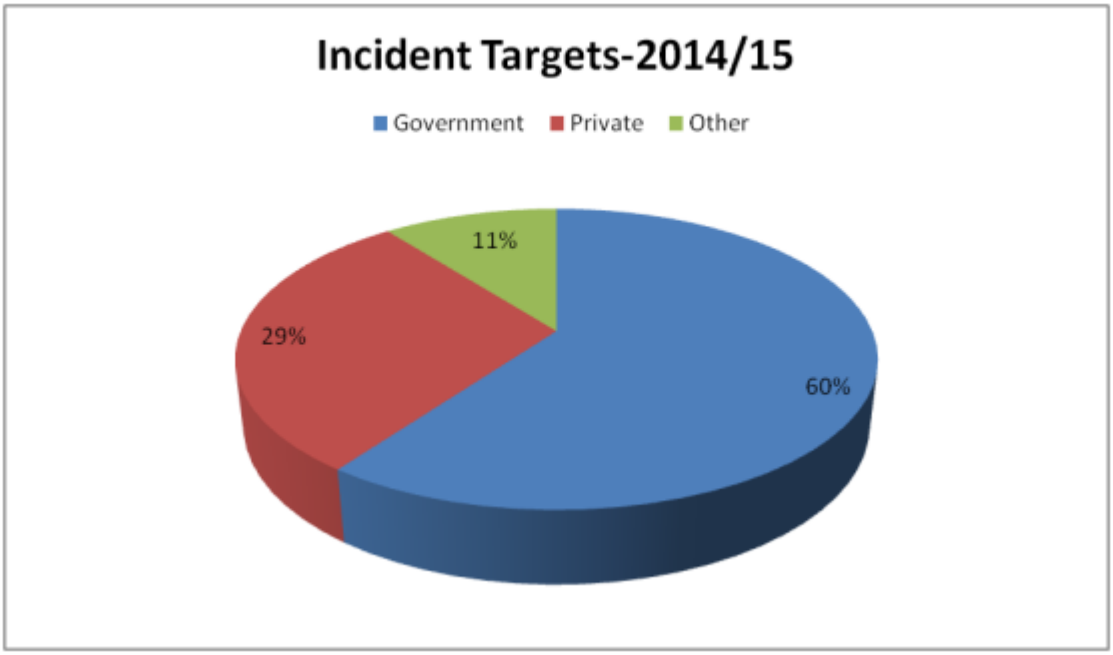


Fig 1.1

While the total number of reported incidents is slightly lower than the 12 month period to December 2013, where 219 incidents were recorded, this was likely due to changes to recording and reporting practices, rather than a reduction in incidents.

The NCSC incident response team is recording an average of one serious incident a day. Of the total incidents (fig 1.2) spear phishing made up 30.5% (58 incidents), followed by network intrusion/compromise with 21.5% (41 incidences), and botnets, 9.5% (18 incidences).

Denial of service and "drive by" download incidents were both equal at 5.8%, (11 recorded incidents each), followed by credentials compromise with 9%.

Over the 2014-15 year the NCSC recorded significantly fewer scam/spam incidents with only 7 reported incidents accounting for just 4% of the reporting, compared with 30% in 2013 and 31% in 2012.

There were 35 other recorded incidents, including virus (2), website hacks (5) and internal misuse/breach/loss of device (4).

It is important to note that although there has been a slight reduction on overall incidences in comparison to previous calendar year figures; it is likely as a result of reporting incidences such as spam and website defacement now being reported to other

agencies and not the NCSC.

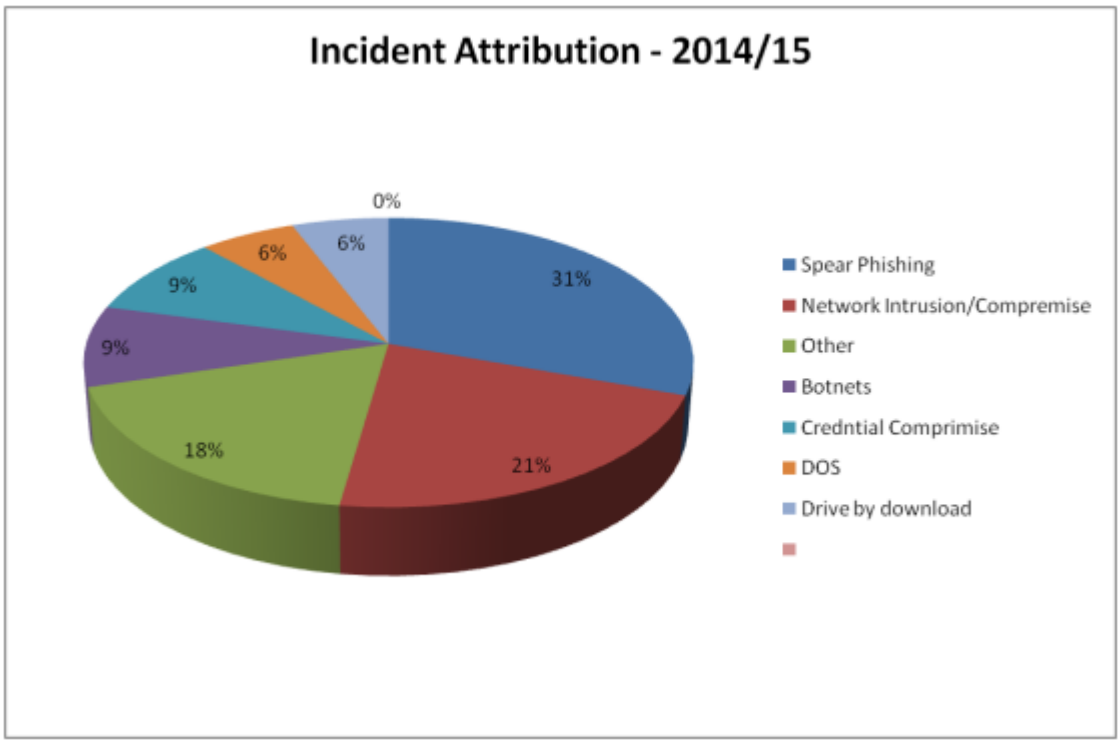


Fig 1.2

2.2. Additional activities

In addition to receiving incident reports, the NCSC:

- Issued cyber threat and incident advisories to customer and partners.
- Facilitated Security Information Exchanges (SIE) to 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.
- Provided high level cyber briefings to key organisations, sector groups and information security forum including the NZ Internet Task Force, and Kiwicon.

3.

3.1. International Collaboration

The NCSC is continuing to go through a period of review and growth throughout 2014-15.

Participation in international operations has improved from previous years with attendance at APCERT, IWWN, and MNSIE conferences.

3.1.1. Future International Collaboration

The NCSC will continue to actively participate in activities with the APCERT forum. Development of a NZ CERT over the coming year will also likely engage with AP-CERT once established.

3.2. Industry Engagement

The NCSC organised and hosted several industry and government engagement forums, held at regular intervals throughout the year. There has also been an increase in the number of board level presentations over a number of industries covering awareness of information assurance.

3.3. The New Zealand Information Security Manual (NZISM)

The NCSC released an updated version of the NZISM following:

- Significant research and development
- Consultation with NCSC customers
- Integration with the New Zealand Protective Security Requirements (PSR).

The Protective Security Requirements (PSR) outlines 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

Throughout 2014/15 year the NCSC presented at and/or participated in several forums, both domestic and international including:

- AusCERT Conference, Australia
- Kiwicon, New Zealand
- MNSIE, USA

4.1. Publications

The NCSC publishes a number of security alerts and advisories via its website, through direct exchanges with customers and partners and on a bi-lateral basis where

appropriate.

5. Future projects

- Expanded engagement with domestic and international partners
- Training and awareness programmes

6. Conclusion

The NCSC continues through a process of growth while maintaining a domestic focus on engagement across a number of sectors.

We will continue to build on this foundation into a sustainable model enabling additional expansion of personnel and expertise coupled with a growing customer set, including at the international level in 2015/16.

SingCERT

Singapore Computer Emergency Response Team - Singapore

1. Highlights of 2015

1.1 Summary of major activities

As SingCERT had a major transition from the Infocomm Development Authority of Singapore to the Cyber Security of Singapore, changes were made to the SingCERT's website portal, email address and location. The website portal and email address has changed to https://www.csa.gov.sg/singcert and singcert@csa.gov.sg respectively.

2. About SingCERT

2.1 Introduction

The Singapore Computer Emergency Response Team (SingCERT) is a one-stop centre for security incident response in Singapore. Besides providing assistance to its constituency in incident resolution and co-ordination, SingCERT also broadcasts security alerts, advisories and security patches. To promote security awareness and to educate the general public, SingCERT organises regular seminars, workshops and sharing sessions covering a wide range of security topics.

2.2 Establishment

SingCERT was set up in 1997 by the Infocomm Development Authority of Singapore to facilitate the detection, resolution and prevention of security related incidents on the Internet. In 2015, SingCERT transited to a newly set up agency, the Cyber Security Agency of Singapore.

2.3 Resources

Advisories and alerts will be released on the SingCERT's website on the latest issues that affects the constituency.

2.4 Constituency

SingCERT provides services primarily to the Singapore local constituency comprising of companies and end users.

3. Activities & Operations

3.1 Scope and definitions

SingCERT's focus is on providing technical assistance and coordinating responses to security compromises. SingCERT does not conduct criminal investigations as it is not a law enforcement or investigative agency.

3.2 Incident handling reports

SingCERT receives incident reports via both email and phone. SingCERT analyst will then assess and follow-up with the respective agency or service provider for further actions.

3.3 Abuse statistics

There is an increase in the number of phishing, defacements and data/information leakage incidents in the year 2015 as compared to the year 2014. This is mainly due to a re-organization of SingCERT which provided SingCERT with more access to sources of abuse information. There is also an increase in frauds and scams in the area of cyber due to the increase usage of technology.

3.4 Publications

SingCERT's publications are in the following chronological order:

1. Vulnerabilities in Singapore Home Routers
   https://www.csa.gov.sg/singcert/news/advisories-alerts/vulnerabilites-in-routers---updated
2. Dyre Malware
   https://www.csa.gov.sg/singcert/news/advisories-alerts/dyre-malware
3. Business Email Frauds
   https://www.csa.gov.sg/singcert/news/advisories-alerts/singcert-business-email-frauds
4. Defacement of .sg Websites
   https://www.csa.gov.sg/singcert/news/advisories-alerts/defacement-of-sg-websites
5. Fake Singapore Websites
   https://www.csa.gov.sg/singcert/news/advisories-alerts/fake-websites-hosted-by-jinanyuz
6. Mobile Banking Malware

https://www.csa.gov.sg/singcert/news/advisories-alerts/malware-targeting-mobile-banking

4. Events organized / hosted

4.1 ASEAN CERTs Incident Drill 2015

The ASEAN CERTs Incident Drill (ACID) 2015 was conducted successfully on 28 October 2015. In order to develop scenarios which reflected prevailing cyber threats that were confronting the CERTs, the theme selected for the drill was "Virtual Currencies Incidents". 15 CERTs from 14 countries from ASEAN and Asia took part in the drill, and good feedbacks were received from all the participants.

5. International Collaboration

5.1 ASEAN CERTs Incident Drill 2015

SingCERT conducted the ACID involving 15 CERTs from 14 countries from ASEAN and Asia.

6. Future Plans

6.1 Future projects

SingCERT will be organising the 11th ASEAN CERTs Incident Drill for the year 2016. Discussions are in progress to work out the scope and coverage.

Sri Lanka CERT|CC

Sri Lanka Computer Emergency Readiness Team Coordination Centre – Sri Lanka

1. Introduction

The Sri Lanka Computer Emergency Readiness Team | Coordination Centre (Sri Lanka CERT|CC) is the 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.

1.1. 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 & Digital Infrastructure and is fully financed by the state budget.

1.2. Workforce

The Sri Lanka CERT|CC has a total staff strength of fourteen team members consisting of Chief Executive Officer, Manager Operations, Principal Information Security Engineer, Senior Information Security Engineer, Research and Policy Development Specialist, Junior Information Security Engineer, four Associate Information Security Analysts 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].

1.3. Constituency

Sri Lanka CERT's Constituency encompasses the whole of the cyber community of Sri Lanka (private & public sector organizations, and the general public). Sri Lanka CERT maintains a good rapport with government and private sector establishments, and extends assistance to the general public as permitted by available resources. In accordance with its mandate, Sri Lanka CERT | CC gives priority to requests for assistance from government. 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

Given the expertise in the field of cyber security and the capacity to prevent, analyze, identify and respond to cyber security incidents that threaten Sri Lanka's national cyber-space, Sri Lanka CERT|CC continues to work with government, non-government and international organizations.

As the national contact point 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 2015 (1st of January – 31st of December);

- 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 2015, 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 a relatively new type of incident that Sri Lanka CERT | CC encountered. This happens mainly in the Small and Medium Enterprises (SME) sector where local exporters/importers are exporting or importing various items to or from foreign countries. Hackers have used social engineering techniques to gain access to the email accounts of these businessmen and then sending emails pretending to be their business partner convincing them to deposit money to fraudulent bank account.
- 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 stolen.
- It was observed that hackers were not targeting particular organizations when they attempt to compromise company websites. Instead they were targeting vulnerable web servers which may have hosted several web sites of various organizations. Once they compromise the server, hackers could deface multiple sites hosted in that server. In some cases it was observed that the vulnerability was with the content management panel, where the user who has being entrusted to update the site used a simple password to access the content management panel.
- There is an increase in the phishing emails specially targeting email accounts of businessmen. This might be the first step towards targeting those businessmen for financial frauds.
- Phishing mails targeting on-line banking customers continue to pose a problem, and regular complaints are received from banks as well as bank customers.

The above findings lead to the following conclusions:

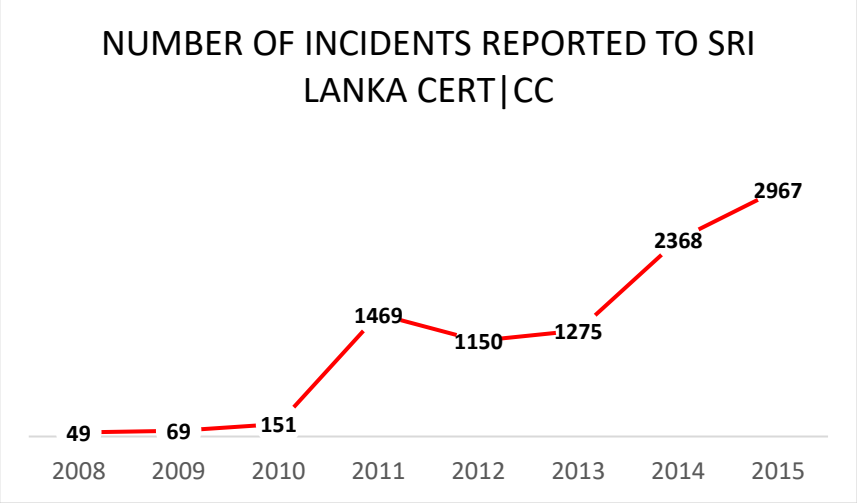
- Cyber security is a part of every individual and each and every one is responsible for contributing to a secure online environment.
- Attackers might be shifting their focus on targets which can easily be compromised. For example, the average internet user many have

comparatively less knowledge on information security and hence be more vulnerable to online attacks.

- Some Website owners believe that confidential information is not stored in the web site hence investing money on the security of the web site is not worth it. But they fail to realize that their compromised Website can be used to host malware sites that have the possibility of becoming a part of a botnet.
- 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 benefits of Internet rather than be a victim in the cyber world.

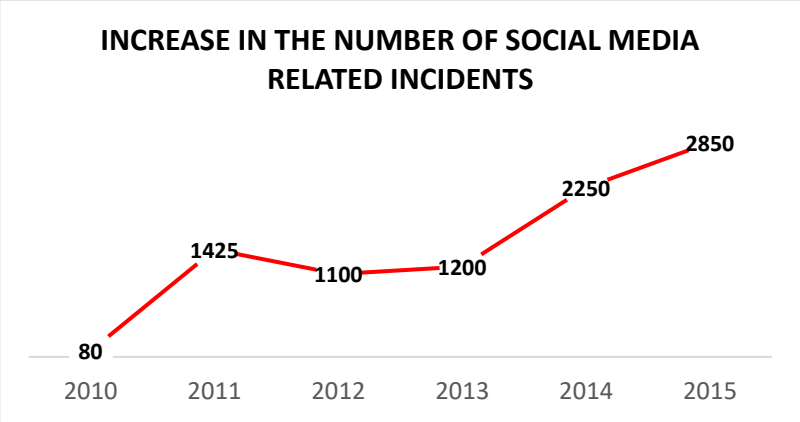
2.2. Incident Handling Statistics

Incidents reported to Sri Lanka CERT have increased to 2, 967 in the year 2015. In 2014 2,368 incidents were reported. This represents a 25% increase in reported incidents compared to the year 2014.



Graph 1: Total number of reported incidents

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

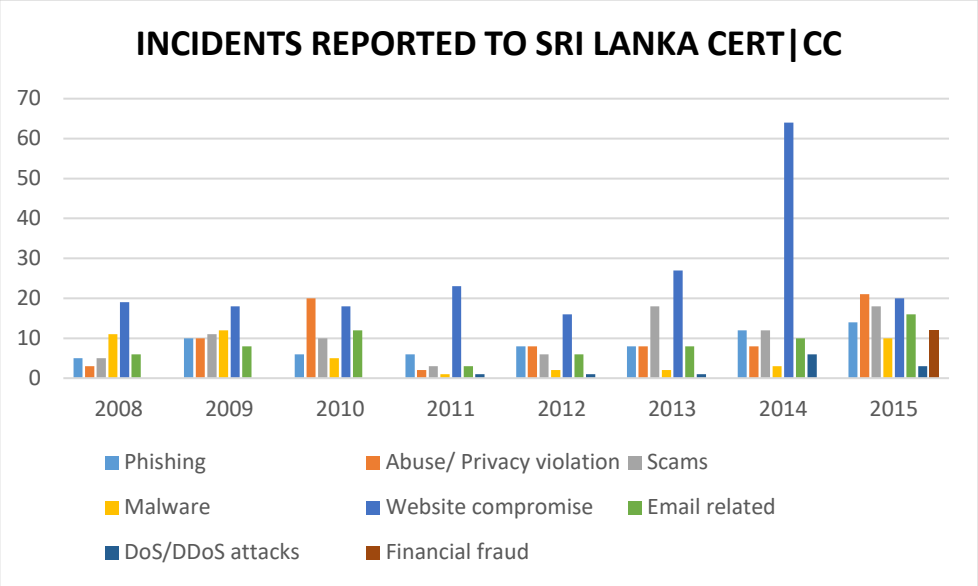


Graph 2: Total number of social media related incidents

The following table depicts the distribution of various types of incidents reported to Sri Lanka CERT during 2015. All the incidents reported to Sri Lanka CERT have been resolved satisfactorily.

Type of Incident	Year 2015
Phishing	14
Abuse/Hate/Privacy violation (via mail)	21
Scams	18
Financial Frauds	12
Malicious Software issues	10
Web site Compromise	20
Compromised Email	16
Intellectual property violation	3
DoS/DDoS	3
Social Media related incidents	2850
Total	**2967**

Table 1: Number of reported incidents in year 2015



Graph3: Types of incidents reported to Sri Lanka CERT|CC from 2008- 2015

From Graph 3 it is evident that attacks targeting Websites are on the increase. Also, new types of incidents such as DoS/DDoS attacks and financial frauds have been reported in 2015.

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 2015 include;

- Assisting several government organizations and private sector organizations to develop an Information Security Policy for their organizations.
- 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 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, Students, and the General Public.

During the year 2015 Sri Lanka CERT|CC conducted the following awareness, training and education programs successfully:

- Training sessions for police officers at the Police Training Academy and Police Training College.
- Awareness session for judges.
- Regular press releases to the media about incidents and impending vulnerabilities.
- Awareness programs for School Teachers.
- Cyber Guardian e-newsletter distributed monthly through School Net. This is the fourth consecutive year of this circulation which is widely accepted and read.
- Train-the-trainer on-line safety awareness programs island wide in collaboration with the Ministry of Education for IT Teachers of schools.
- Child on-line safety awareness presentations at private and government schools.
- Participating in regular radio programs, and in particular the "Subarathi" programme conducted by the Sri Lanka Broadcasting Cooperation as part of Sri Lanka CERT's awareness creation campaign.
- Conducting regular training programmes for SOCO (Scene of Crime) officers at the Police training college focussing on Cyber Crime first responder's role.
- National Child Protection Authority - Member of the panel to develop a training module for Ministry of Education for online safely.

- Awareness programs for high level government officers.

In addition, Sri Lanka CERT|CC staff has continued to assist in the delivery of courses in computer security topics at tertiary education institutions.

Sri Lanka CERT|CC was involved in the coordination and organizing of First Responder Training for law enforcement officers at Sri Lanka Police training college. Another training workshop on Live Data Forensics was also conducted for the law enforcement officers of Sri Lanka Police. These were funded by the Council of Europe project titled Global Action Against Cybercrime (GLACY).
As a key strategy, Sri Lanka CERT uses publications developed in-house such as leaflets and posters during public awareness sessions such as seminars, exhibitions and other forums.

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 2015;

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 2015 was held in the month of November 2015, and featured a series of events including the following;

- Annual National Conference on Cyber Security 2015.
- Four full-day Workshops for professionals, namely:

✓ Technical workshop on "Internet Abuse Handling"
✓ Technical workshop on "Network Security in depth"
✓ Technical workshop on "Using Cuckoo Sandbox for Malware Analysis"
✓ Technical workshop on "Run your own Honeypots"

- Hacking Challenge: Hacking Challenge is a contest for IT Professionals to attack or defend an actual network within a given timeframe. The invited participants are 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 these events were well attended and were conducted by international industry experts. The conference and the workshops also saw the participation of information security professionals from APNIC, ICANN and Team Cymru.

- Application Security Awareness Session: A session on application security and CSSLP conducted by (ISC)2.

- First Responder Training: A five day first responder training was conducted by Council of Europe trainers for 15 local law enforcement officers.

- Carrying out training sessions and presentations on Information security for SLAS (Sri Lanka Administrative Services) officers at SLIDA

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 2015. Stakeholder consultations have been initiated in order to discuss this in detail with the relevant stakeholders during the year 2016 before finalising it.

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. As a first step, the research team has conducted a pilot survey to assess the level of cyber security awareness among citizens of 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.

Sri Lanka CERT|CC launched its first sector based CSIRT for the banking and finance sector called "BankCSIRT" on 1st of July 2014. All of the banks operating in Sri Lanka have joined as members of BankCSIRT and continuing its services with the regulatory blessings of the Central Bank of Sri Lanka. Bank CSIRT is funded by member banks, hosted by the national clearing house Lanka Clear and managed by a Steering Committee chaired by the Central Bank of Sri Lanka. Sri Lanka CERT|CC serves as a member of the Steering Committee, and provides the necessary technical assistance.

Bank CSIRT continued to be in operation during the year 2015 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.

5.2. National Certification Authority

The Electronic Transactions Act no. 19 of 2006 creates a foundation for the existence of a national certificate authority. With the launch of e-Citizen services and the increased use of online banking and other e-commerce facilities, the use of a digital ID is becoming more important. While the Lanka Government Network (LGN) Certification Authority (CA) for Government establishments and Lanka Sign CA (for Banks) exist, there is a lack of universal acceptance of their certificates.

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 lack of funding, NCA is expected to start the operations during the year 2016.

6. International Collaboration

6.1. Event participation

- February 8th – 12th
  ICANN 52 | International public ICANN meeting, Singapore.
- May 26th -28th
  CNCERT | CC Annual Conference.
  Wuhan, China
- June 14th-19th
  FIRST AGM and Annual Conference.
  Berlin, Germany
- June 15th -19th
  OCTOPUS Conference.
  Strasbourg, France
- September 6th – 10th
  APCERT AGM and Conference.
  Kuala Lampur, Malaysia
- October 12th – 14th
  2nd PMAP Annual Conference.
  Manila, Philippines

6.2. International incident coordination

Sri Lanka CERT | CC actively participated in the APCERT Drill 2015 as the lead team in the organizing committee, a player and an EXCON member.

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 (SOC).

- Establishment of the National Certification Authority (ongoing).
- Establishment of sector based CSIRT's.
- Cyber Security Week 2016.

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.
- Conducting inter-organisational research in the area of cyber crime victimization and user behavior (e.g. cross- cultural research) which will be useful in guiding policy makers and the law enforcement.
- Expand the aforementioned 'cyber security awareness survey' into a national level survey to gather data that could be useful in identifying training needs when educating the public.

9. Conclusion

Since its establishment in 2006, Sri Lanka CERT|CC has successfully increased the public's awareness of its presence and the nature of the activities it is involved in. It has been possible to achieve this target through the use of seminars, conferences and the use of mass media. This has led to an increase in the number of incidents reported and handled by Sri Lanka CERT|CC in the past consecutive years.

During 2015, 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.

All the events organized by Sri Lanka CERT during the year 2015 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 future, Sri Lanka CERT|CC will find new ways to reach an even wider audience and maintain a calendar of regularly running technical and management training workshops.

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.

Lack of explicit legal regulations regarding the responsibilities for notification, responding, prevention and mitigation of cyber security incidents by the state institutions or companies in the private sector is one of the main difficulties encountered in handling incident response activities and real-time response to such incidents. In this context, we considered it necessary to supplement the national legislation framework with the stipulations contained in certain documents that are found at European level.

In this respect, one of the key achievements this year was Sri Lanka's ratification of the UN Electronic Communications Convention. This was another first for South Asia and ensures greater legal certainty for e-Commerce and e-Business providers who will want to use Sri Lankan law as the applicable law and ensure International validity for such e-Contracts. Ratification of this Convention will also ensure legal validity for Electronic Bills of Lading and other International legal instruments, enhancing the ability for Sri Lanka in its move towards paperless trade facilitation, whilst further strengthening the use of Technology Neutral authentication frameworks under National Certification Authority (NCA) Project.

The other key achievement in this respect was when the Government of Sri Lanka was invited to accede to the Budapest Convention on Cyber Crime in February 2015. This is the only international treaty seeking to address Internet and computer crime by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations. In addition to harmonizing the domestic criminal law for offences connected to provisions in the area of cyber-crime, the main benefit to Sri

Lanka from this initiative was the setting up of a fast and effective regime of international cooperation

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

TechCERT

TechCERT – Sri Lanka

1 About TechCERT

1.1 Introduction

TechCERT, Sri Lanka's first and largest Computer Emergency Readiness Team (CERT) helps general public and Sri Lankan organizations keep their computer systems and networks secure.

TechCERT - a division of LK Domain Registry - 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 Technical 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.):

PhD	3
MEng/MSc/MPhil	10
PG Diploma	2
MBA	1
BSc Eng/BSc/BIT/BEng	17
CISSP	1
C|HFI	1

Certified ISMS Auditor (ISO27001)	4
CCNA / CCNA Security	3
Chartered Engineers	1
CISM	1
CISA	1
C | EH	5
ITIL v3	2
PMP	1
CPISI	3
RHCSA/RHCE	2
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

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

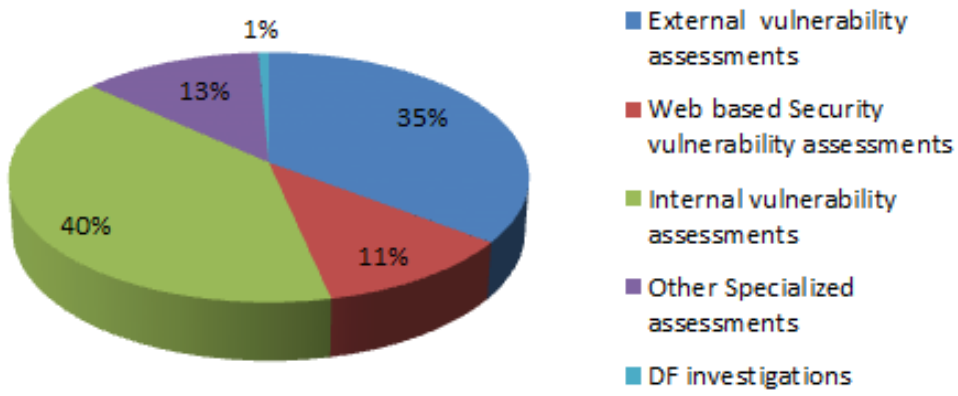
- Host discovery assessment
- Providing PCI-DSS certification to Sri Lankan clients in collaboration with QSA company
- Business IT risk assessment and advisory services on BCP and DRP
- Evolving a security strategy against malware and other attacks
- Consultancy for PKI implementation, certificate authority (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

2.1 TechCERT Activities and Operations

The details of activities and operations conducted by TechCERT during the year 2015 are as follows:

2.1.1 Security Assessments

Activity Type	Count
External vulnerability assessments	2145
Web-based Security vulnerability assessments	684
Internal vulnerability assessments	2436
Other Specialized assessments	763
DF investigations	45



2.1.2 Incident Response

Type of Incident Response	Count
Social network related incident responses	75
Phishing incident responses	83
Other incident responses	70

3 Events

3.1 Organizing of Training Seminars, Workshops and Demonstrations

20th March 2015	**Seminar – "Dangers of browsing the Internet and how to avoid attacks"** TechCERT conducted a public seminar and demonstration session on the theme "Dangers of browsing the Internet and how to avoid attacks" in Kurunagala, Sri Lanka.
25th April 2015	**Seminar – "Dangers of browsing the Internet and how to avoid attacks"** TechCERT conducted a public seminar and demonstration

	session on the theme "Dangers of browsing the Internet and how to avoid attacks" at the University of Ruhuna - Faculty of Engineering, Hapugala, Sri Lanka.
08th May 2015	**Seminar – "Dangers of browsing the Internet and how to avoid attacks"** TechCERT conducted a public seminar and demonstration session titled "Dangers of browsing the Internet and how to avoid attacks" at the IESL Information Technology and Communications Engineering Section, Faculty of Engineering, University of Peradeniya, Sri Lanka.
23rd May 2015	**Seminar – "Dangers of browsing the Internet and how to avoid attacks"** TechCERT conducted a public seminar and demonstration session on the theme "Dangers of browsing the Internet and how to avoid attacks" at the Euroville Auditorium, No 17, Agrarian Service lane, Nallur, Jaffna, Sri Lanka.
9th – 11th June 2015	**Workshop – "Dealing Cyber Crimes in a globalized world"** TechCERT conducted this workshop to enhance the digital forensics capabilities & effective incident management techniques, when dealing with cyber-crimes at the OZO Hotel, Colombo, Sri Lanka.
18th June 2015	**Presentation – "Sector Based Cyber Security Drills - Lessons Learnt"** Mr. Dileepa Lathsara, Chief Operating Officer of TechCERT delivered a presentation on "Sector Based Cyber Security Drills - Lessons Learnt" at the 27th Annual FIRST Conference held in Berlin, Germany.

23rd July 2015	**Seminar – "Threats from Internet and How To Avoid Them"** TechCERT conducted a public seminar and demonstration session titled "Threats from Internet and how to avoid them" at the IESL Information Technology and Communications Engineering Section, Samurdi Hall, Rathnapura, Sri Lanka.
17th September 2015	**Seminar – "Privacy Lost and Never Found"** TechCERT conducted a public seminar and demonstration session on the theme "Privacy Lost and Never Found" at the IESL Meeting Room 1, The Institution of Engineers, 120/15, Wijerama Mawatha, Colombo 7, Sri Lanka.
9th November 2015	**Workshop – "Securing Your Web Site"** TechCERT conducted this workshop to enhance the OWASP top 10 guidelines and secure maintenance of websites at the Distance Learning Centre, 4th Floor, SLIDA Building, Colombo, Sri Lanka.
26th January 2016	**Seminar – "IT Security and Safe Use of Internet"** TechCERT conducted a public seminar and demonstration session titled "Dangers of browsing the Internet and how to avoid attacks" at the SL Navy Head Quarters, Colombo, Sri Lanka.

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

Program Name	Date	Audience	Venue
Safe Use of Internet	10th June 2015	Teachers & Students	Gurulugomi College, Kaluthara, Sri Lanka

3.3 Participation in Conferences, Workshops and Training Programs

1. Dileepa Lathsara, Chief Operating Officer of TechCERT participated in the, 27th Annual FIRST Conference, "Getting Back to the Roots" held on 14th-19th June 2015 in Berlin, Germany.

2. Dileepa Lathsara participated in the 8th Annual National Conference on Cyber Security organized by SLCERT|CC & ICTA Sri Lanka held on 03rd November 2015.

3. Madusanka Hettige & Kalana Guniyangoda participated in the APCERT AGM and Conference, "Bridging the World go Cyber Green" held on 06th -10th September 2015 in Kuala Lumpur, Malaysia.

4. Nalinda Herath & Harshana Porawagama participated in the SISA Summit on 05th February 2016 in Mumbai, India.

5. Nalinda Herath participated in the Technical Workshop on "Run Your Own Honeypots" at the Annual National Conference on Cyber Security and Workshops conducted by SLCERT on 06th November 2015.

6. Kalana Guniyangoda participated in the Technical Workshop on "Using Cuckoo Sandbox for Malware Analysis" at the Annual National Conference on Cyber Security and Workshops conducted by SLCERT on 04th November 2015.

3.4 Cyber Security Drills

18th March 2015	**APCERT Cyber Security Drill 2015** TechCERT actively participated in the APCERT Drill 2015 as a member of the Organizing Committee and a member of EXCON.
20th May 2015	**Cyber Security Drill for Sri Lankan Finance & Insurance organizations**

	TechCERT conducted a cyber-security drill for the Sri Lankan Finance & Insurance Sector Organizations on the theme "Cyber Attacks beyond Traditional Sources".
22nd July 2015	**Cyber Security Drill for the Banking Sector in Sri Lanka** TechCERT conducted a cyber-security drill for the Banking Sector in Sri Lanka on the theme "Cyber Attacks beyond Traditional Sources".
23rd September 2015	**Cyber Security Drill for Sri Lankan Telcos and ISPs** TechCERT conducted the first ever cyber-security drill for the Telecommunication Companies and ISPs in Sri Lanka titled "Cyber Attacks beyond Traditional Sources".

4 Achievements

4.1 Technological Achievements

- Deployment of free website security assessment program for Sri Lankan websites together with LK Domain Registry.
- Improvements to the Knowledge Base developed for incident response support.
- Improvements to the "PhishHook" Phishing Early warning system and increase in number of deployments within Sri Lanka.

4.2 Publications

[1] 126 articles were published in the TechCERT official website https://techcert.lk/en/ during the year 2015 in order to enhance the basic security knowledge of the general public.

5 Future Plans

- Conduct research on Threat Intelligence Gathering
- Develop a system to automate the detection and containment of Security Information Leakages.
- Develop a framework to improve the web application vulnerability detection in

distributed environments.

6 Conclusion

TechCERT has been able to consistently improve and expand its capability to respond and assist its constituency in information security incidents and handle emergencies in a timely and professional manner.

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

There was a significant increase in phishing attacks and website defacement/hacking incidents in Sri Lanka in 2015, when compared to previous year. TechCERT was able to successfully respond to most of the incidents reported and assist the relevant authorities to mitigate the threats with minimum effect. TechCERT is confident of its ability and readiness to successfully assist its constituency in computer emergencies by providing pro-active response.

In achieving the organizational objectives, TechCERT shall continue to increase its staff strength, acquire advanced training and tools and improve its standards to provide a faster and more efficient service to the clients as well as the public through global collaboration.

ThaiCERT

Thailand Computer Emergency Response Team – Thailand

1. 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 Information and Communication Technology, 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 2 specialists and 22 engineers who are responsible for incident response, threat analysis and digital forensics.

2. Activities & Operations

2.1 Incident Statistics

Reported Incidents Handled via Triage

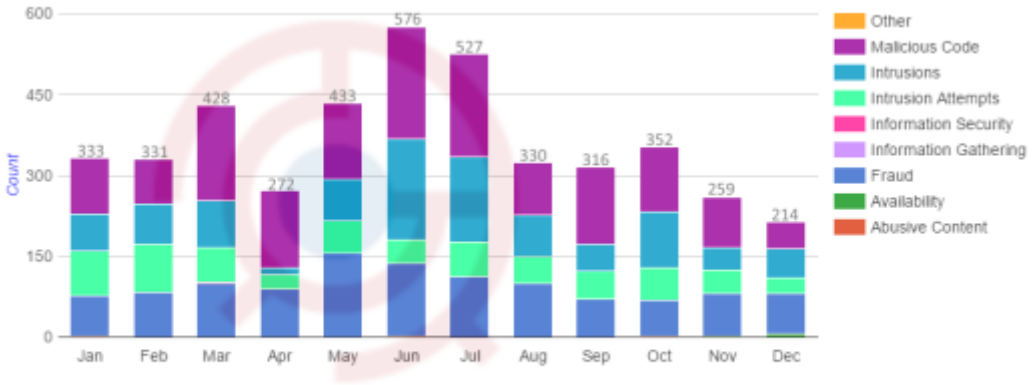


Figure 1: The number of reported incidents in 2015

Via triage, ThaiCERT handled a total of 4,371 reported incident cases (tickets) in 2015, which is an increase of 9% compared to those of 2014 (4,007 cases). The received reports per month varied approximately between 259 to 514 cases, with an average of 364 cases per month.

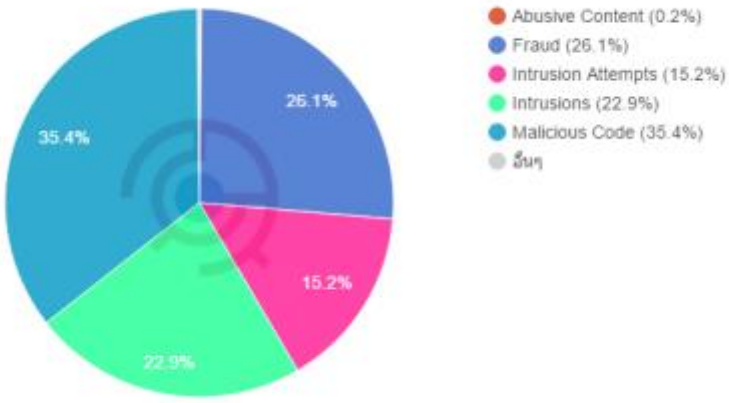


Figure 2: The proportion of reported incidents by incident type in 2015

According to the reported incidents in 2015, classified by the eCSIRT incident classification[1], malicious code (mostly malware URLs) dominated with 35.4%, followed by fraud at 26.1%, where all fraud cases were phishing, and intrusions at 22.9%. All

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

such information was handled and notified to the relevant parties through e-mail channels.

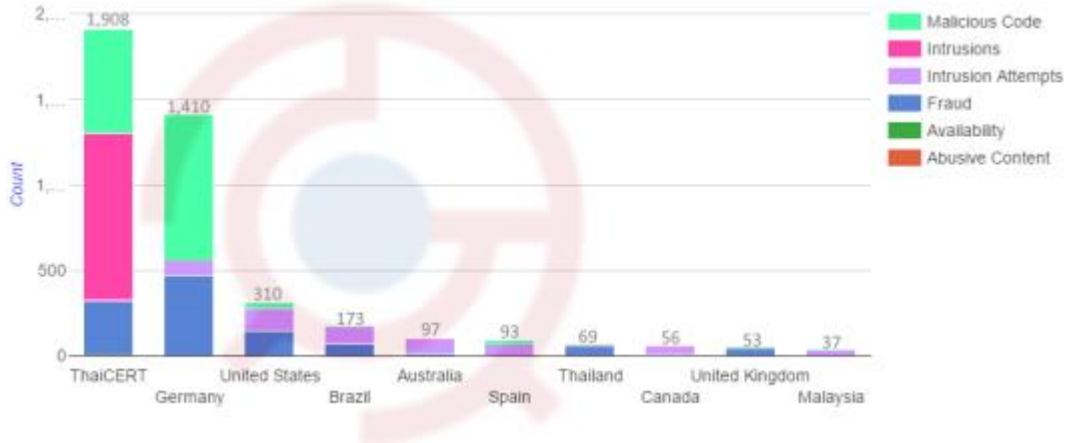


Figure 3: Top 10 incident reporters in 2015

Regarding the incident reporters classified by country, Figure 3 shows that most of the security incidents reported by ThaiCERT security watch system, comprising 1,908 cases or 43.7% of all reports. The source of Fraud, Malicious Code and Intrusions incident reports generally came from automatic feeds. Number of incident reports from Germany as 2nd position (1,410 cases) increased 2.4 times, while number of incident reports from the United States (310 cases) slightly decreased.

2.2 Reported Incidents Received

Type of Incidents		Number of reported unique IPs
Abusive Content	Abusive Content	8
Malicious Code	Malware	2,093,979
	Malware URL	907
Information Gathering	Scanning	31
Information Security	Data Leakage	81
Intrusion Attempts	Brute Force	570

Intrusion	Web Defacement	430
Availability	Open DNS Resolver	46,463
	DDoS	5
Fraud	Web Phishing	540
Others	Open Proxy Server	5,418

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 2015, ThaiCERT has received incident reports comprising 2 million unique IPs where the top 3 of incident reports were Malware (2,093,979 IPs), Open DNS Resolver (46,463 IPs) and Open Proxy Server (5,418 IPs).

2.3 Training

Organized:

- Local certificate training and exam: iSEC, Jan and Feb 2015
- Digital Forensics: AccessData Bootcamp, May 2015
- Digital Forensics: X-Ways, May 2015
- PHP/JAVA/Android Secure Coding with JPCERT, Jul 2015
- Sector-based CERT Training, Aug 2015
- Digital Forensics: Applied Decryption, Aug 2015
- Digital Forensics: Macintosh, Aug 2015
- Digital Forensics: Hard Disk Physical Repair, Aug 2015
- Thailand CTF Competition 2015 & Security Health Check Day, Oct 2015
- CYDER Training, Oct 2015
- Digital Forensics: Video analysis, Oct 2015

2.4 Drill

Participated:

- APCERT Drill 2015 under the theme "Cyber Attacks beyond Traditional Sources", Mar 2015
- ASEAN CERT Incident Drill (ACID) 2015, Oct 2015

2.5 Meetings and Seminars

Organized:

- Client-side Attacks: Use-after-Free Exploitation, Mar 2015
- Open forum discussion, Feb, April, May, June, July, Sep 2015

Participated:

- ASEAN TELSOM Joint Working Group, Myanmar, Mar 2015
- RSA Conference 2015, United States of America, Apr 2015
- Global Conference on Cyberspace 2015, Netherlands, April 2015
- 51st APEC Telecommunications and Information Working Group and Symposium on the Internet Economy, Philippines, May 2015
- Visa Security Summit, Australia, May 2015
- 27th Annual FIRST Conference, Germany, Jun 2015
- 1st ASEAN-Japan Information Security Joint Working Group Meeting and the 3rd ASEAN-Japan Working Group 2015 for CIIP, Capacity Building, Japan, June 2015
- ASEAN Regional Forum (ARF) Workshop on Cyber Security Capacity Building, July 2015
- 4th ASEAN Network Security Action Council (ANSAC), Indonesia, July 2015
- APCERT and OIC-CERT Annual General Meeting (AGM) & Annual Conference 2015, Malaysia, Sep 2015
- China-ASEAN Information Harbor Forum, China, Sep 2015
- 52nd APEC Telecommunications and Information Working Group, New Zealand, Oct 2015
- 7th ASIAN Forensic Sciences Network Annual Meeting & Symposium: Necessity vs. Luxury, Malaysia, Nov 2015
- Cyber Offensive and Defensive Exercise (CODE), Taiwan, Nov 2015
- 15th ASEAN Telecommunications and IT Ministers Meeting and 16th ASAN Telecommunications and IT Senior Officials Meetings, Vietnam, Nov 2015
- 6th ASEAN-Japan Information Security Workshop, Japan, Dec 2015

2.6 MoU

- MoU with Central Institute of Forensic Science of Thailand, Feb 2015

3. Certifications

ThaiCERT technical staff currently holds the following professional information security

certificates:

- AccessData ACE/AME
- CompTIA Security+
- EC-Council CEH
- EnCase EnCE
- GIAC GCFA/GCFE/GCIA/GCIH/GPEN/GREM/GWAPT
- IACIS CFCE
- IRCA ISO/IEC 27001 ISMS Lead Auditor

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

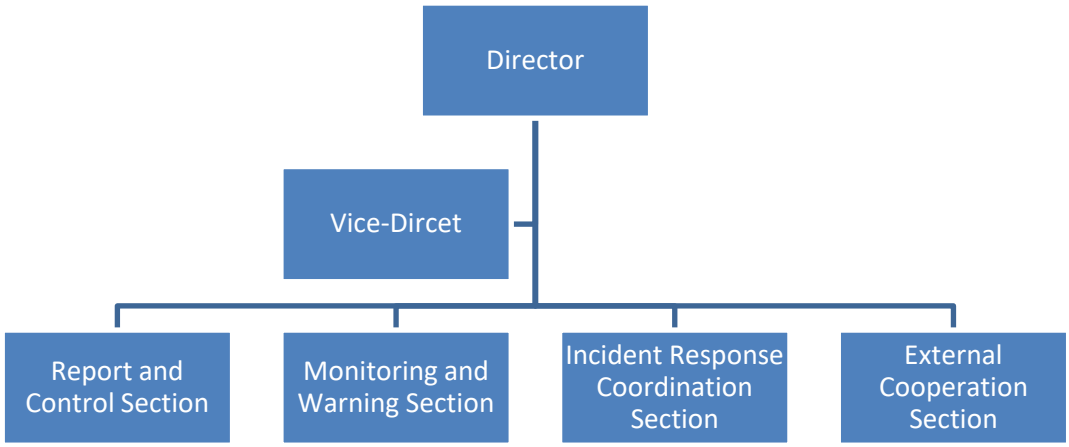


Figure 1.Organization of TWCERT/CC

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 2015, TWCERT/CC received 24,116 computer security incident reports.

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

Table 1. Incident reports to TWCERT/CC (2015)

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 2015 have categorized as in Fig. 2.

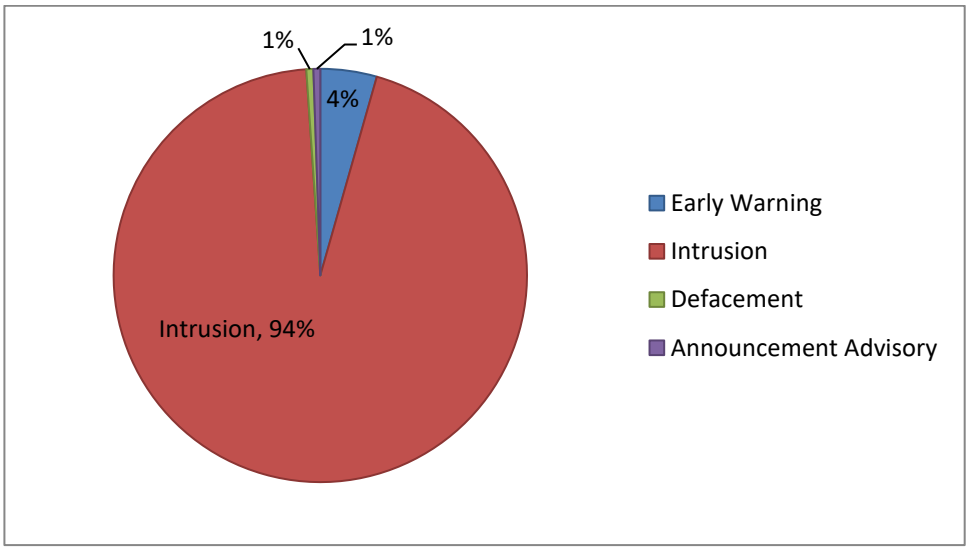


Figure 2. Distribution of incident response

1.1. 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.

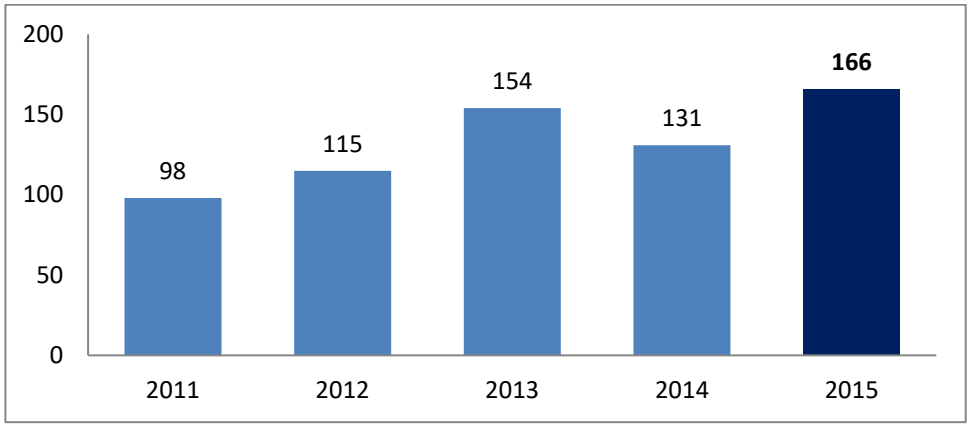


Figure 3. Annual Statistics of Vulnerability by TWCERT/CC

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 166 numbers of vulnerabilities in 2015. 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	29	Cross site scripting	7
Gain information	28	Cross-Site Request Forgery	3
Code execution	28	Others	3
Overflows	17	Injection	2
Memory corruption	15	Memory corruption	2
Gain privilege	15	Http response splitting	2
Bypass something	14	File inclusion	1

Table 2. Categories of the Vulnerability in 2015

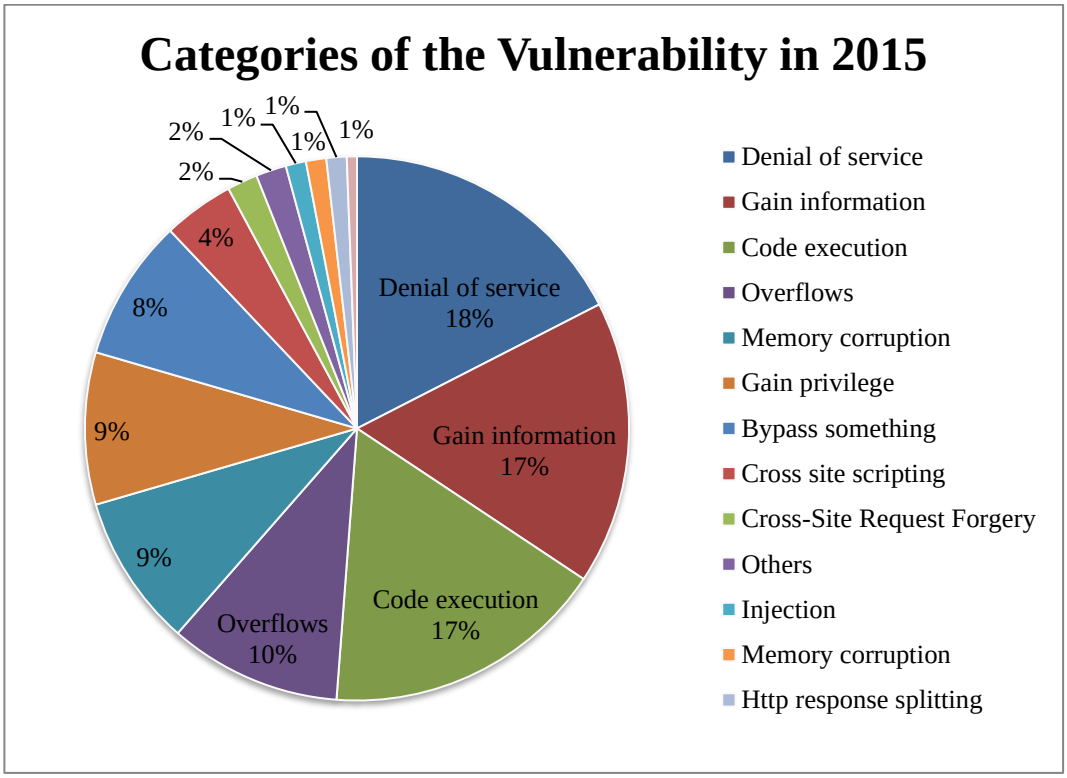


Figure 4. Categories of TWCERT/CC Vulnerability Database

- **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.

2. Events organized / co-organized

2.7 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
2015/6/29	Hacker Events and Security Protection Technology Workshop
2015/8/21	An Overview of Critical Information Infrastructure Protection (CIIP) in Taiwan. (IRCON)
2015/12/30	Information Security Trend and Case Studying of the Financial Sector.

Table 3. list of TWCERT/CC workshops in 2015

2.8 Drill

TWCERT/CC participated in the APCERT Drill in March 2015, and also supported the Financial Information Service Co., LTD to operate a cyber exercise in July 2015.

3. 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 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

4. 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.

■ **Security SCADA, Smartgrid, Smartmeter and Industrial Control Systems(4SICS)**

4SICS is a Stockholm international summit on cyber-security in SCADA and Industrial Control Systems, and it's an annual summit that gather the most important ICS/SCADA cyber security stakeholders across critical industries for example energy, oil and gas, water, transportation, smartgrid and so on. During twenty October, 2015 to twenty-two October, 2015, 4SICS, the most important SCADA/ICS conference was hold in Stockholm. 4SICS information security conference had taken place with FIRST in 2015.

The goal of 4SICS is sharing the last cyber security events of global industrial control systems. TWCERT/CC can use these information to handle cyber security of critical information infrastructure protection. In addition, it's also helpful for the trend of cyber crime controlling in the future to carry out the relate cyber security business.

■ Visit National Information Security Center(NISC) of Japanese Cabinet

TWCERT/CC visited NISC of Japanese cabinet in 2015 to discuss the public-private partnerships policies of critical information infrastructure protection and cyber security drill. Japanese party offered the suggestion for exchanging visits to enhance connecting. Moreover, TWCERT/CC visits JPCERT/CC to get some intelligences from WAISE which is the group of critical information infrastructure of Japanese private departments.

■ **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.

5. 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 national critical information infrastructure protection mechanism to enhance the robustness of Taiwan national infrastructure.

TWNCERT

Taiwan National Computer Emergency Response Team – Chinese Taipei

1. Highlights of 2015

1.1 Summary of major activities

TWNCERT dedicates to support and enhance the government's ability to respond and deal with security incidents. In 2015, TWNCERT received 731 reports on security incidents from Taiwan government and published 1,578 security advisories to government sectors as well as provide consulting services.

1.2 Achievements & milestones

In 2015, TWNCERT conducted a national large-scale cyber security exercise, named Cyber Offensive and Defensive Exercise (CODE) for government agencies, and launched a cyber security competition for university students. To raise the security awareness, TWNCERT held total of 10 national cyber security seminars for the government agencies.

To strengthen the international cooperation on information security, TWNCERT have participated more than 10 international events and has convened 6 APCERT online training programs in 2015.

2. About TWNCERT(Taiwan National Computer Emergency Response Team)

2.1 Introduction

TWNCERT aims to enhance the government's ability to respond to and deal with security incidents and internationalize our efforts, serving as a national point of contact for the CSIRTs in Taiwan and has been conducting incident report and response, technical services, consulting services among government agencies, and engage in international collaboration.

The strategies of TWNCERT are:

- Help government agencies on enhancing cyber security resilience, system security and staffs' competence.
- Build the comprehensive legal system of cyber security, and promote the critical information infrastructure protection.
- Expand public-private partnerships network, and facilitate cyber security industry development.

- Setup cooperation mechanism between academia and industry to promote application value of R&D results.

TWNCERT has four task forces, which are Information Gathering, Coordination Service, Research and Development, and Consulting Service. It is mainly dedicated to create a response center that can help optimize the capability of real-time monitoring, coordination, response and handing in the face of security incidents. The responsibilities and services of TWNCERT are listed below:

- To plan and promote cyber security protection mechanism of government agencies.
- To assist government agencies in major national cyber security incidents response.
- To support government agencies of special sensitivity in cyber security protection work.
- To plan and support the cyber security protection of critical infrastructure.
- Planning and assisting government agencies in cultivating information and security talents; promoting cyber security awareness nationwide.
- To promote the research and development, integration, application and international cooperation and exchange of cyber security technologies.
- To support the major development strategy respective to the demands of the industry's cyber security.
- Other matters relating to cyber security technologies.

2.2 Establishment

TWNCERT was established in 2001. It is under the Government Security Working Group, one of working groups of the National Information and Communication Security Taskforce (NICST), which is in charge of cyber security issues of the Taiwan Government. The formation of TWNCERT aims to create a government response center that can help optimize the capability of immediate monitor, coordination, response and handling in the face of security incident.

2.3 Constituency

TWNCERT aims to enhance the government's ability to respond and deal with security incidents and other related issues. Moreover, TWNCERT coordinates with different field including Academic ISAC, National Communications Commission ISAC, which

includes most major ISPs in Taiwan, major SOCs, law enforcement, other CSIRTs in Taiwan as well as information security industries in Taiwan and worldwide.

3. Activities & Operations

3.1 Scope and definitions

Chapter 3.2 defines the incident handling reports TWNCERT has received in 2015, and an overview of the statistics is shown in chapter 3.3. The incident reports and cyber information sharing by TWNCERT are described in chapter 3.4.

3.2 Incident handling reports

TWNCERT received 731 reports on computer information security incidents from Taiwan government sectors and more than 2,526 international information security incident reports from overseas in 2015.

In addition, an information sharing mechanism established by TWNCERT in 2009 named Government Information Sharing and Analysis Center (G-ISAC), the largest information sharing networks in Taiwan, is a public-private partnership has reduced response time through improved coordination and collaboration capabilities and efficiencies to enhance cybersecurity efforts nationally. In 2015, G-ISAC has shared total of 84,027 security incidents and critical information among members including Academic ISAC (A-ISAC), National Communications Commission ISAC (NCC-ISAC), major SOCs, law enforcement, CSIRTs such as TWCERT/CC and EC-CERT (Electronic Commerce CERT).

3.3 Abuse statistics

The top 3 incident categories from government agencies are Intrusion, Website Defacement and Other.

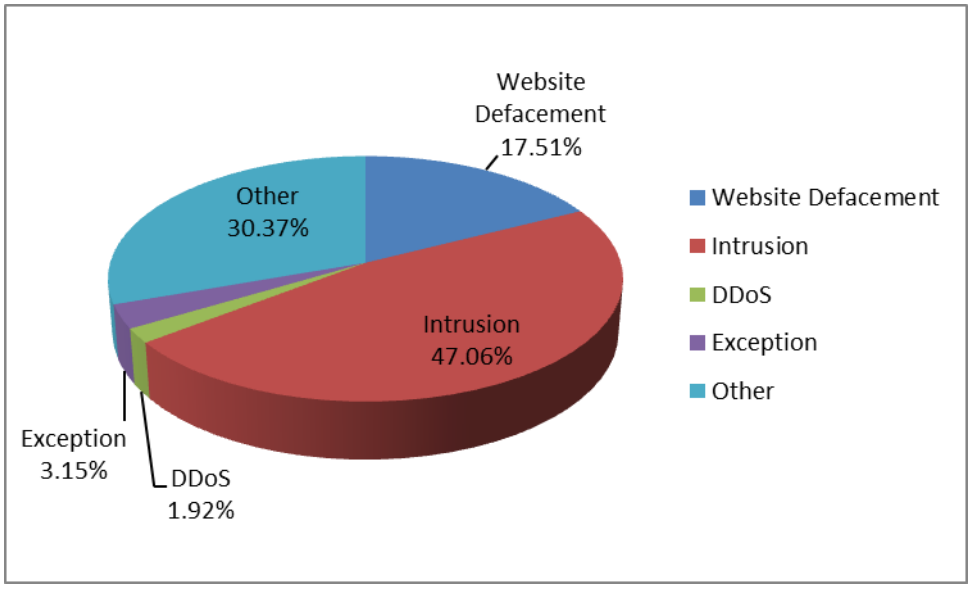


Figure 1 Security incidents from government sectors

The international information security incident reports in 2015 were categorized as in Figure 2. About 40% of the incident reports were on attack, followed by phishing and spam.

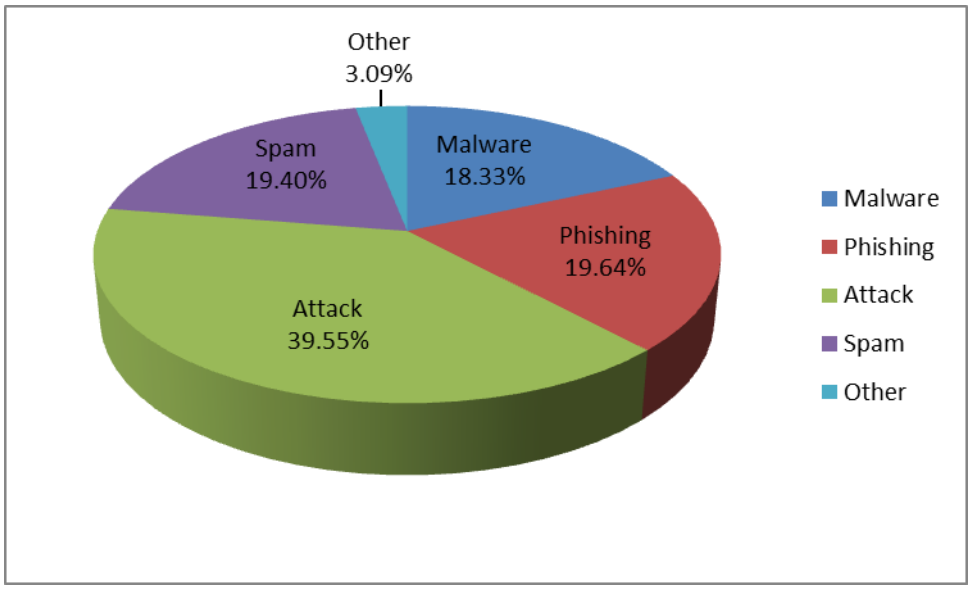


Figure 2 Classification of the international incident reports

Currently, G-ISAC has covered over 99.001% IPs in Taiwan, and has shared thousands of security incident and critical information each year. G-ISAC members shared a total of 84,027 security information in 2015.

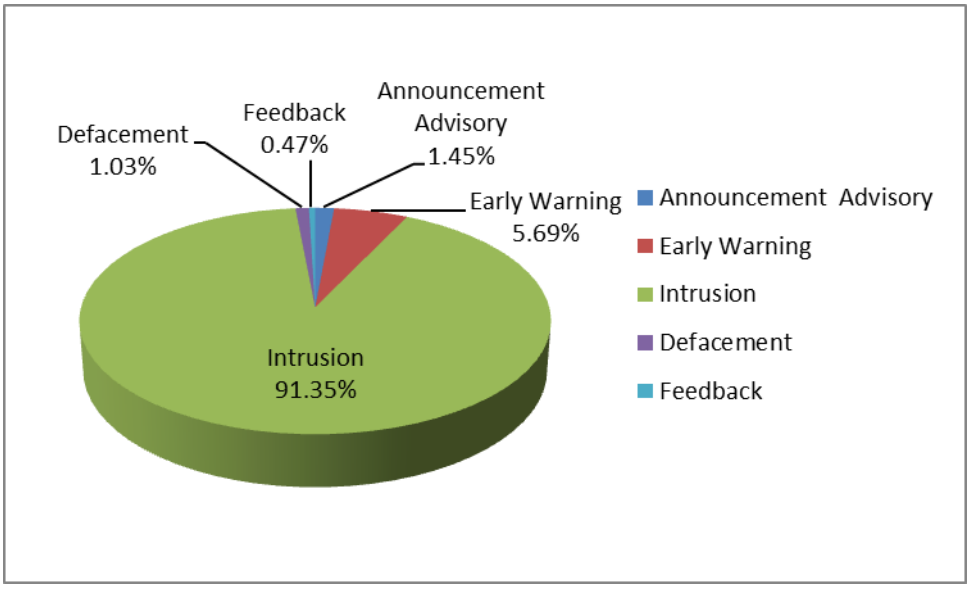


Figure 3 Information sharing distribution of G-ISAC

3.4 Publications

- Government sectors

In 2015, TWNCERT published 1,578 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	6	13	242	1	262
2nd Qtr.	0	23	26	201	7	257
3rd Qtr.	0	27	20	229	20	296
4th Qtr.	0	367	58	314	27	766
Total	0	422	117	986	53	1,578

Figure 4 Notice advisories to government

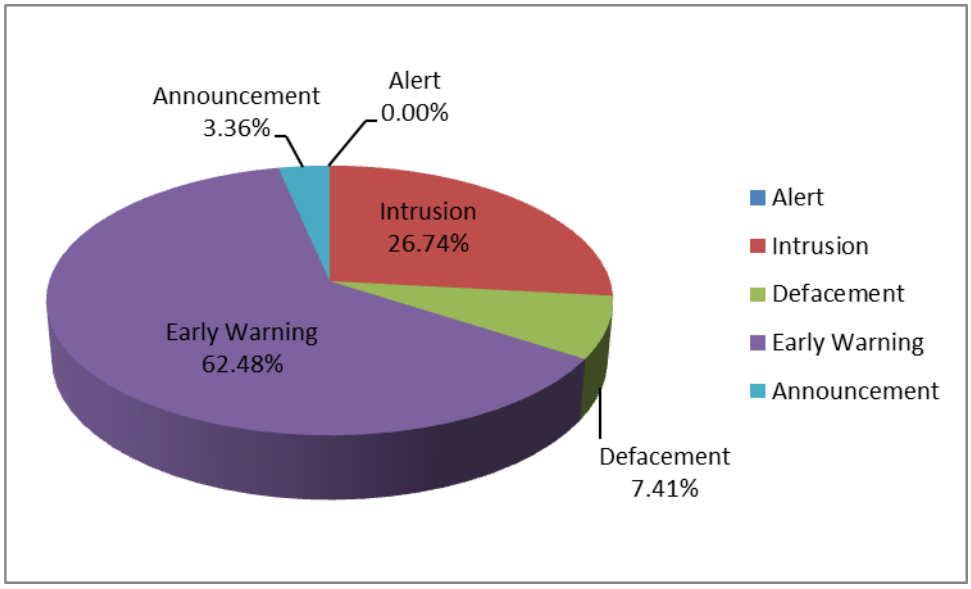


Figure 5 Distribution of government notice advisories

- International incident sharing

Regarding the international incident sharing, TWNCERT has reported total of 406 reports via G-ISAC to 30 countries shown as figure 6.

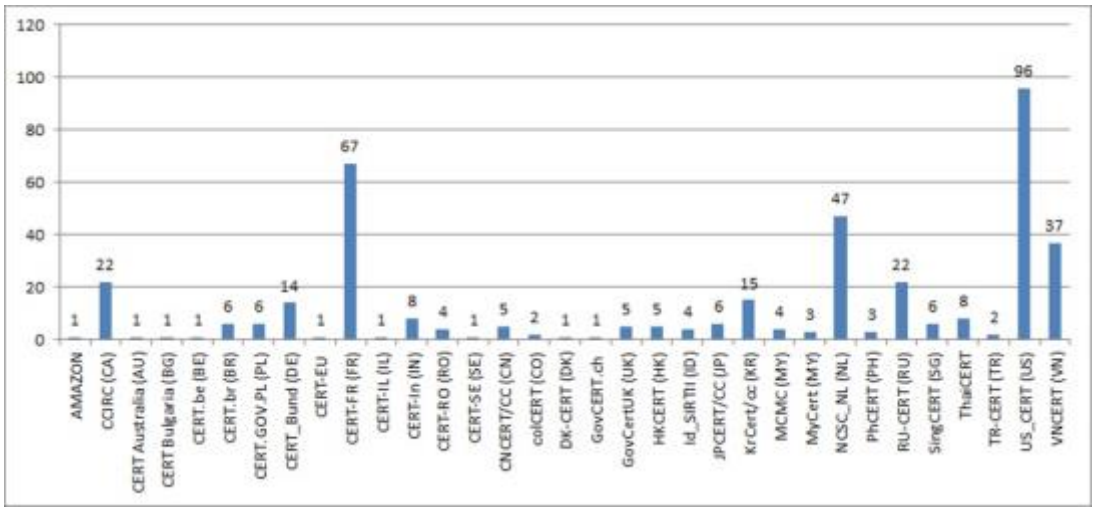


Figure 6 International incident report via G-ISAC

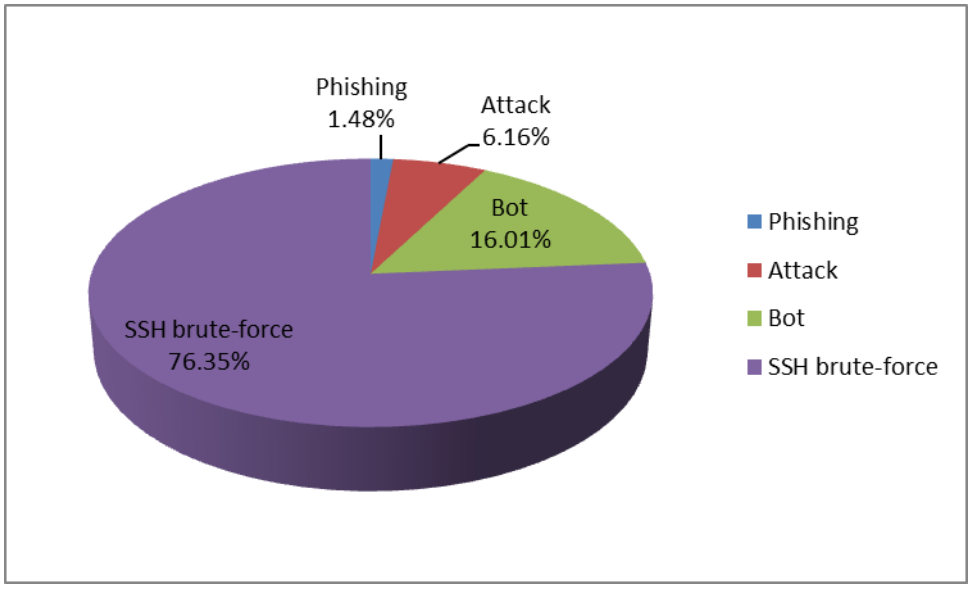


Figure 7 Categories of international incident report via G-ISAC

- Website publication

TWNCERT collect and publish security advisories, news or guidelines via its website. During the period from January to December of 2015, TWNCERT published 432 news including security news and bulletins on the website. It is about 10% increase from the previous year.

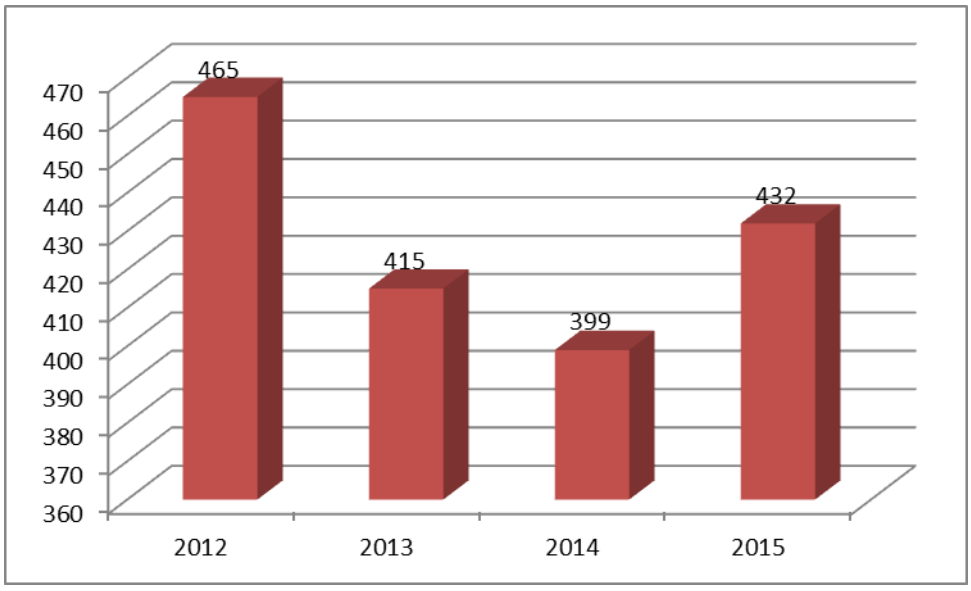


Figure 8 TWNCERT Published news on website

4. Events organized / hosted

4.1 Drills & exercises

- Drill

TWNCERT conducted a national large-scale cyber security exercise during mid-October to November 2015, mobilized more than 100 people from different agencies and private sectors to join the Cyber Offensive and Defensive Exercise (CODE) taskforce, to strengthen its preparedness against cybercrimes, technology failures as well as Critical Information Infrastructure (CII) incidents. In order to learn more experiences, TWNCERT invited total of 13 representatives from 10 international organizations participating in the drill event and share their valuable experiences.

- Cyber security competition

Additionally, in order to promote security general awareness, TWNCERT launched a cyber security competition in 2015. It aimed to improve the cyber security awareness among university students. In the period time, TWNCERT held 17 promotion activities in the universities and more than total of 16,000 attendees participated.

4.2 Conferences and seminars

TWNCERT hosts national security workshops and seminars regularly to raise the security awareness among government agencies. In 2015, TWNCERT held 10 national security workshops for government agencies and total of 3,660 government technical staffs attended.

For G-ISAC (Government Information Sharing and Analysis Center) 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 2015, two full member meetings, one normal member meeting, and one all member meeting have been held.

5. International Collaboration

5.1 International partnerships and agreements

TWNCERT is the member of international organizations listed below and actively participates in member activities including organization events, working groups, 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 has MOU with JPCERT/CC and Team Cymru for CSIRT Assistance Program.

5.2 Capacity building

5.2.1 Training

TWNCERT is the member of APCERT Steering Committee and chairs 11 APCERT member teams in Education and Training WG in 2015. In the year of 2015, TWNCERT has convened 6 live streaming training programs and a total of 23 APCERT member teams have participated. In order to improve the training program, TWNCERT conducted a survey to evaluate the effectiveness of the overall education and training program in August.

5.2.2 Drills & exercises

TWNCERT participated in the following drill events in 2015 to evaluate the capability of incident report and response.

- APCERT Drill on Mar. 18th 2015.
- APCERT & OIC-CERT Conference Discussion Exercise on Sep.8th 2015, in Kuala Lumpur.

5.2.3 Seminars & presentations

Below are some of international events TWNCERT participated in 2015.

- APRICOT 2015, March- Fukuoka, presented “Cyber Threat Trends in Taiwan.”
- RSA Conference, April- San Francisco
- APEC TEL 51, May- Boracay
- FIRST and National CSIRT conference, June – Berlin
- Black hat USA 2015 & Defcon 23, August- Las Vegas
- APCERT AGM and Conference 2015, March- Kuala Lumpur, presented “SC Activity Report by TWNCERT.”
- 15th Regional Asia Information Security Exchange Forum Meeting, August- China
- APEC TEL 52, October- Auckland
- Meridian Conference 2015, October- Leon
- AVAR Conference 2015, December- Vietnam

6. Future Plans

6.1 Future Operation

TWNCERT is known as the Information & Communication Security Technology Center (ICST) domestically. Since 2016 ICST has restructured to the National Center for Cyber Security Technology (NCCST). TWNCERT is led by Ministry of Science and Technology (MOST). MOST is the competent authority for cyber security, which is in charge of cyber security issues of the Taiwan Government. TWNCERT aims to create a government response center that can help optimize the capability of immediate monitor, coordination, response and handling in the face of security incident.

7. Conclusion

In 2015, TWNCERT has made progress on training, national large-scale cyber security drill, international cooperation and collaboration. TWNCERT will continuously enhance the collaboration with the government sectors, build the public-private partnerships and collaborate with local and global CERTs to strengthen the security awareness and incident handling capability. We look forward to domestic and international cooperation opportunities to establish a safe and secure cyber space 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 on 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:

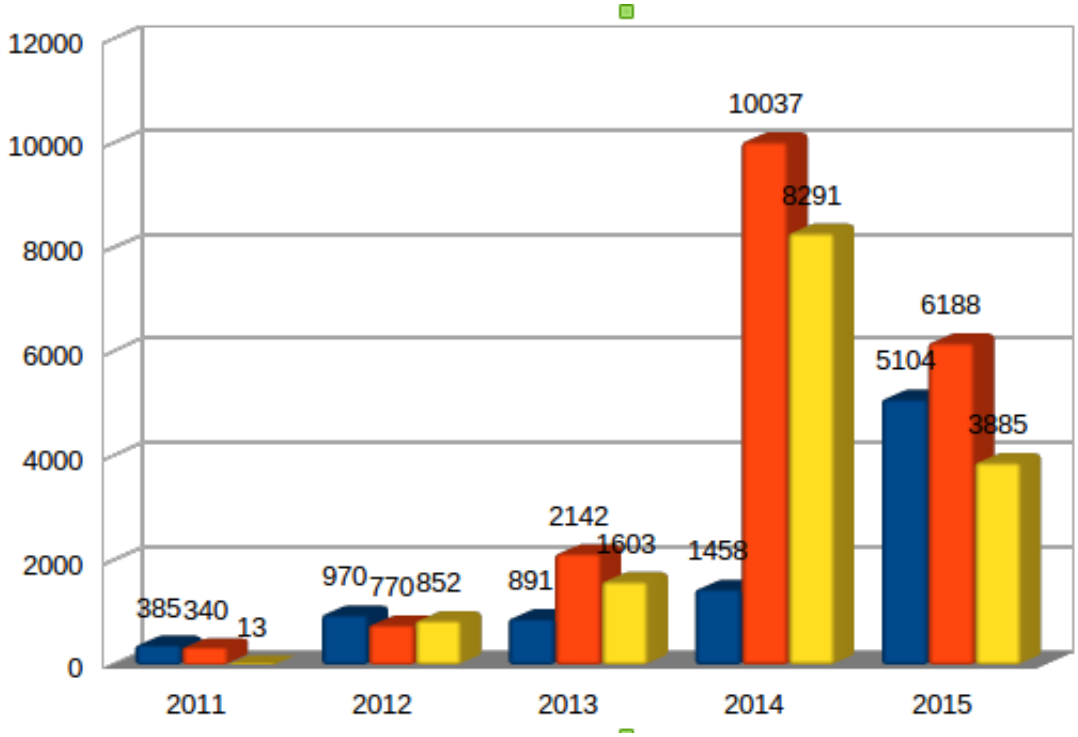
- Being Coordination Center of Vietnam CSIRT Networks with 121 members. (Including information technology centers of Ministries, ministerial agencies, governmental agencies, telecommunication enterprise, internet service providers, the organizations in charge of information systems of national importance).
- 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 oversea CERTs in this area.
- Support Ministry of Information and Communications with activities in state management about Information Security.
- Implementing and Deploying the Anti-spam activities.
- VNCERT has four specialized divisions: Division of Coordination and Response,

Division of System technique, Division of Training & Consultancy and Division of Research and Development. VNCERT also has two branches, one in Ho Chi Minh City and another in Danang City with 52 members.

2. Activities & Operations

2.1 Incident handling reports

In 2015, VNCERT processed 15.177 information security incidents (including 5.104 phishings, 6.188 Defaces and 3.885 Malwares,).



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

In 2015, VNCERT reported 1.451.997 IPs of large botnets (Conficker, Sality, Traficonverter and Downadup, etc.) and sent 3.779 botnet warnings to government agencies and supported them to process.

2.2 Abuse statistics

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

2.3 Incident Coordinating, warning and supporting activities

Implemented testing and auditing for 116 websites of government agencies about information security.

Removed botnet malwares from thousands of computers in government agencies.

Participated in the Microsoft removing botnet operations focused on Conficker, Sality, Traficonverter and Downadup, etc.

Co-operate with other CERTs to remove phishing sites on 200 websites that faked VietNam's websites.

Warned all members of Vietnam CSIRT Network of 02 importance vulnerabilities (BIND, Lenovo)

2.4 Anti-spam activities

In 2015, VNCERT received 96.223.668 advertising text messages (including 555.293.651 advertising email; có 15.124 advertising SMS over Internet).

In 2015, VNCERT also received 554.865 spam SMS on mobile.

2.5 Legal Framework Update on Information Security

National Assembly promulgated Information security Law on November, 19th, 2015.

Drafting the circulars to Monitoring network information security and preventing networking incident.

3. Events organized / hosted

3.1 Training

Organized training courses about CERT activities and Incident Response for LaoCERT

in VietNam.

Supported and leaded 2 VietNam teams paticiate 2015 Cyber Sea Game in Jakarta, Indonesia. And VietNam's team is champion in this contest.

Cooperated with KISA (Korea Internet & Security Agency) hosted a conference to review their cooperation on cyber security on December.

Organized information security training course for 30 government agencies, training course "Kill Chain and IOC Analysis Workshop" for Csirt teams in VietNam.

Cooperated with VNISA to organize the Information Security Survey and the Information Security Contest for students of universities.

Supported and organized 06 information security training and exercise courses for 06 government agencies.

3.2 Seminars & Etc

Participated to organize some meeting event at national level such as Security World 2015, National Information Security Day 2015, ASEAN CIO/CSO Awards, etc.

4. International Collaboration

4.1 Incident Drill

Participated in 03 international drills: APCERT Annual Drill 2015, ASEAN-JAPAN Drill and ASEAN CERTs Incident Drill (ACID 2015).

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

4.2 MoU

Re-signed MoU with KISA.

Re-signed MoU with LaoCERT.

4.3 Presentation

In 2015, VNCERT participated in and had presentations at 21 international conferences and forums.

5. Future Plans

Completed the draft of Circulars to Monitoring network information security and preventing networking incident;

To build circulars that replace for circulars 27/2011/TT-BTTTT, 4-Oct-2011, regulations on coordination of emergency response activities Vietnam Internet;

To buid the botnet monitoring and removing plan in Vietnam;

To deploy the incident monitoring project for incident in Vietnam;

To deploy the SMS and email monitoring and anti-spams project for in Vietnam;

To organize the 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.