APCERT
Asia Pacific Computer Emergency Response Team

APCERT Annual Report 2014

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

CONTENTS

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 information security;
2. Jointly developing measures to deal with large-scale or regional network security incidents;
3. Facilitating information sharing and technology exchange, including information security, computer virus and malicious code 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 information security and emergency 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 conducting education and training to raise awareness and encourage best practices in information security. APCERT coordinates activities with other regional and global organisations, such as 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/), a task force that promotes collaboration and coordination between CSIRTs in Europe; the Organisation of the Islamic Cooperation – Computer Emergency Response Team (OIC-CERT: www.oic-cert.net), a collaboration of information security organisations among the OIC member countries; and the STOP. THINK. CONNECT. (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 2014, **Lao Computer Emergency Response Team (LaoCERT)** of Lao People's Democratic Republic and **Mongolian Cyber Emergency Response Team (MNCERT/CC)** of Mongolia were approved its membership as Operational Member. **Bkav** (formerly known as BKIS, an Operational Member) made its membership transition into Supporting Member. **Microsoft Corporation** and **Dell SecureWorks** also joined APCERT as Supporting Member.

During the APCERT Annual General Meeting (AGM) held in March 2013 in Brisbane, Australia, APCERT adopted a new membership structure under the Operational Framework. Pursuant to the new scheme, as of 1 October 2013, the existing Full and General Members were transitioned to Operational Members (operational CSIRTs/CERTs in the Asia Pacific region) and Supporting Members (cyber security related organisations, regardless of the region, that can support APCERT's mission and operations). For further information on the new membership, please refer to the APCERT Operational Framework (www.apcert.org/documents/pdf/OPFW(26Mar2013).pdf).

As of December 2014, APCERT consists of 27 Operational Members from 20 economies across the Asia Pacific region and 3 Supporting Members.

Operational Members (27 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
HKCERT	Hong Kong Computer Emergency Response Team Coordination Centre	Hong Kong, China
ID-CERT	Indonesia Computer Emergency Response Team	Indonesia
ID-SIRTII/CC	Indonesia Security Incident Response Team of Internet Infrastructure/Coordination Center	Indonesia
JPCERT/CC	Japan Computer Emergency Response Team / Coordination Center	Japan
KrCERT/CC	Korea Internet Security Center	Korea
LaoCERT	Lao Computer Emergency Response Team	Lao People's Democratic Republic
mmCERT/CC	Myanmar Computer Emergency Response Team	Myanmar
MNCERT/CC	Mongolia Cyber Emergency Response Team / Coordination Center	Mongolia
MOCERT	Macau Computer Emergency Response Team Coordination Centre	Macao
MonCIRT	Mongolian Cyber Incident Response Team	Mongolia
MyCERT	Malaysian Computer Emergency Response Team	Malaysia
NCSC	New Zealand National Cyber Security Centre	New Zealand
SingCERT	Singapore Computer Emergency Response Team	Singapore
Sri Lanka CERT|CC	Sri Lanka Computer Emergency Readiness Team Coordination Centre	Sri Lanka

TechCERT	TechCERT	Sri Lanka
ThaiCERT	Thailand Computer Emergency Response Team	Thailand
TWCERT/CC	Taiwan Computer Emergency Response Team / Coordination Center	Chinese Taipei
TWNCERT	Taiwan National Computer Emergency Response Team	Chinese Taipei
VNCERT	Vietnam Computer Emergency Response Team	Vietnam

Supporting Members (3 Teams)

- Bkav Corporation
- Dell SecureWorks
- Microsoft Corporation

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

During the APCERT AGM 2014, the Japan Computer Emergency Response Team Coordination Center (JPCERT/CC) was re-elected as the Chair of APCERT, and the Korea Internet Security Center (KrCERT/CC) as the Deputy Chair, both for one-year terms for the fourth consecutive year. 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	
CNCERT/CC	March 2014 – September 2016	
JPCERT/CC	March 2013 – September 2015	Chair / Secretariat
KrCERT/CC	March 2013 – September 2015	Deputy Chair
MOCERT	March 2013 – September 2015	
MyCERT	March 2013 – September 2015	
TWNCERT	March 2014 – September 2016	

[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.

3. Working Groups (WG)

There are currently four (4) Working Groups (WGs) in APCERT.

1) Information Sharing WG (formed in 2011)

- Objective:
  - 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 (11): 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

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 2014

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 2014, APCERT Teams have hosted, participated and/or contributed in the following events:

- **APCERT Drill 2014 (19 February 2014)**

  http://www.apcert.org/documents/pdf/Drill2014_PressRelease.pdf

  APCERT Drill 2014, the 10th 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. 20 teams from 16 economies of APCERT (Australia, Bangladesh, Brunei Darussalam, People's Republic of China, Chinese Taipei, Hong Kong, Indonesia, Japan, Korea, Macao, Malaysia, Myanmar, Singapore, Sri Lanka, Thailand and Vietnam), and 3 teams from 3 economies of OIC-CERT (Egypt, Pakistan, and Nigeria) and a CSIRT from Germany from the European Government CSIRTs group (EGC) participated in the Drill. The theme of the drill was "Countering Cyber-ops with Regional Coordination".

- **Cyber Intelligence Asia (11-14 March 2014, Singapore)**

  http://www.intelligence-sec.com/events/cyber-intelligence-asia-2014

  APCERT teams delivered some talks at a half-day workshop "APCERT Day" under the theme "Regional Cyber Security Risk Reduction Approach: APCERT and Network Operators Network Clean-up Collaboration" at Cyber Intelligence Asia. The presentation from APCERT members included risk reduction efforts, case studies in incident response, threat landscape and web security in infrastructure.

- **APCERT Annual General Meeting (AGM) & Conference 2014 (18 - 21 March 2014, Taipei, Chinese Taipei)** *www.twncert.org.tw/apcert2014/*

The APCERT Annual General Meeting (AGM) & Conference 2014 was held on 18-21 March 2014 at Le Meridien Hotel and Howard Civil Service International House; Taipei, Chinese Taipei, hosted by TWNCERT.

Programme Overview:

18 March (Tue)	AM:	APCERT Steering Committee Meeting
	PM:	APCERT Working Group Meetings *(Closed to APCERT members)*
19 March (Wed)	AM:	TSUBAME Workshop *(Closed to TSUBAME members)*
	AM:	Closed Conference *(Closed to APCERT members and invited guests)*
	PM:	APCERT Team-Building Event
20 March (Thur)	AM:	APCERT AGM 2014 *(Closed to APCERT members)*
	PM:	Closed Conference *(Closed to APCERT members and invited guests)*
21 March (Fri)	AM:	Public Conference *(Open to public)*

APCERT AGM & Conference 2014 marked the 11th 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.

- <u>TSUBAME Workshop 2014 (19 March 2014, Taipei, Chinese Taipei)</u>

  The APCERT TSUBAME Workshop 2014 on Network Traffic Monitoring Project was held on 19 March 2014, in conjunction with APCERT AGM & Conference 2014. The workshop was organised by JPCERT/CC to enhance the TSUBAME project and the cooperation among its members.

- <u>ASEAN Regional Forum (25-26 March 2014, Kuala Lumpur, Malaysia)</u>

  As APCERT Chair team, JPCERT/CC represented APCERT at the Cyber

Confidence Building Measures Workshop during the ASEAN Regional Forum. For the session entitled "Building a Regional network of Contacts", APCERT representative introduced the activities of APCERT and the importance of trusted network among the teams.

- <u>5th Asia-Pacific Telecommunity (APT) Cybersecurity Forum (26-28 May 2014, Ulaanbaatar, Mongolia)</u>

  http://www.aptsec.org/2014-CSF5

  As APCERT Deputy Chair team, KrCERT/CC represented APCERT at the 5th APT Cybersecurity Forum. An introduction of APCERT members and main activities were given at the presentation session.

- <u>26th Annual FIRST Conference (21-27 June 2014, Boston, USA)</u>

  www.first.org/conference/2014

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

- <u>National CSIRT Meeting (28-29 June 2014, Boston, USA)</u>

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

- <u>The Internet Governance Forum (IGF) 2014 (1-5 September 2014, Istanbul, Turkey)</u>

  http://www.igf2014.org.tr/

  As APCERT Chair team, JPCERT/CC attended the Internet Governance Forum and presented about the importance of cross-comparable data on cyber security as well as APCERT activities.

- <u>APNIC 38 (9-19 September 2014, Brisbane, Australia)</u>

  https://conference.apnic.net/38/home

  APCERT teams attended the APNIC 38 and presented the latest cyber security activities during the APNIC Security Track.

- <u>ASEAN CERT Incident Drill (ACID) 2014 (24 September 2014)</u>

  ACID 2014, led and coordinated by SingCERT, entered its 9th 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 50 (29 September – 3 October 2014, Brisbane, Australia)

  CERT Australia represented APCERT at APEC TEL 50, and presented the APCERT's overview and latest activities for a safer cyber space base on the regional framework.

- OIC-CERT Annual Conference 2014 (20-22 October 2014, Bandar Seri Begawan, Brunei Darussalam)

  oic-cert.org/event2014/

  Pursuant to the Memorandum of Understanding on collaboration between APCERT and OIC-CERT in September 2011, JPCERT/CC represented APCERT at this conference and delivered a presentation on APCERT activity updates, as well as shared the concept of Cyber Green Initiative, which is a pilot project led by JPCERT/CC.

- CSIRT Trainings for AfricaCERT

  JPCERT/CC organised trainings for CERTs/CSIRTs in Africa and introduced APCERT activities during the trainings on behalf of APCERT.

  - 29-30 May 2014, Djibouti (in conjunction with AfricaCERT Workshop)
  - 25 November 2014, Mauritius (in conjunction with Afrinic 21)

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)**

  Dr. Suguru Yamaguchi of JPCERT/CC had served as a Steering Committee member of FIRST from June 2011 to April 2014. 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 the MoU (Memorandum of Understanding) since June 2012 in order to promote awareness towards cyber security and more secure network environment.

2. APCERT SC Meetings

From January to December 2014, SC members held five (5) teleconferences and three (3) face-to-face meeting to discuss APCERT operations and activities.

15 January	Teleconference
12 February	Teleconference
25 February	Face-to-face meeting in conjunction with APRICOT 2014 in Petaling Jaya, Malaysia
18 March	Face-to-face meeting in conjunction with APCERT AGM & Conference 2014 in Taipei, Chinese Taipei
9 May	Teleconference
17 July	Teleconference
15-16 September	Face-to-face meeting in conjunction with APNIC 38 in Brisbane, Australia
3 December	Teleconference

3. APCERT Training Calls

APCERT held one (1) training call in 2014 to exchange technical expertise, information and ideas.

Date: 5 November 2014
Topic: Introduction of Malware Analysis

Speaker/Organiser: TWNCERT

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

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

III. Activity Reports from APCERT Members

AusCERT

Australian Computer Emergency Response Team – Australia

1. 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

2.1. Security advisories and bulletins

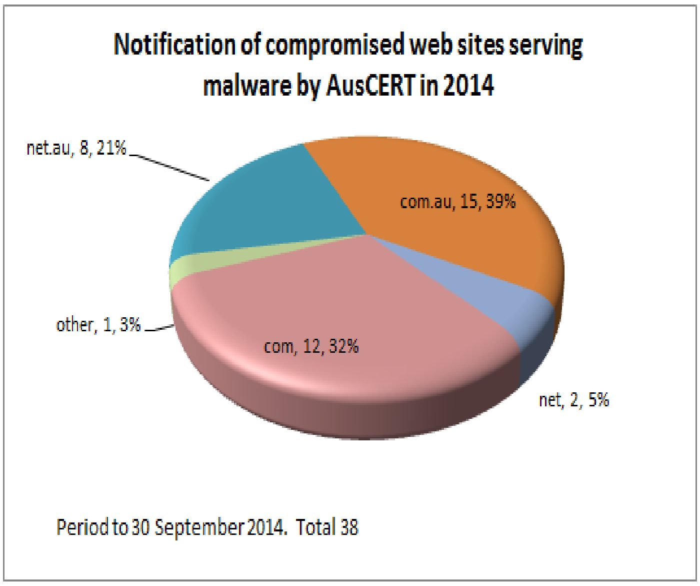
AusCERT distributes security advisories and bulletins to its members by email and publishes a portion of them to its public website. Bulletins are published in a standardised format with a consistent approach to classifications of vulnerabilities, impacts and affected operating systems.

During 2014, 2519 External Security Bulletins (ESBs) and 146 AusCERT Security Bulletins (ASBs) were published. This represents a 34% increase overall when compared with 2013 tallies. The increase is largely due to the widespread vulnerabilities in OpenSSL based products, affecting many different vendors.

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. 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. Weekly, AusCERT provides a report to each of its members that details activity that affected the member for that week.



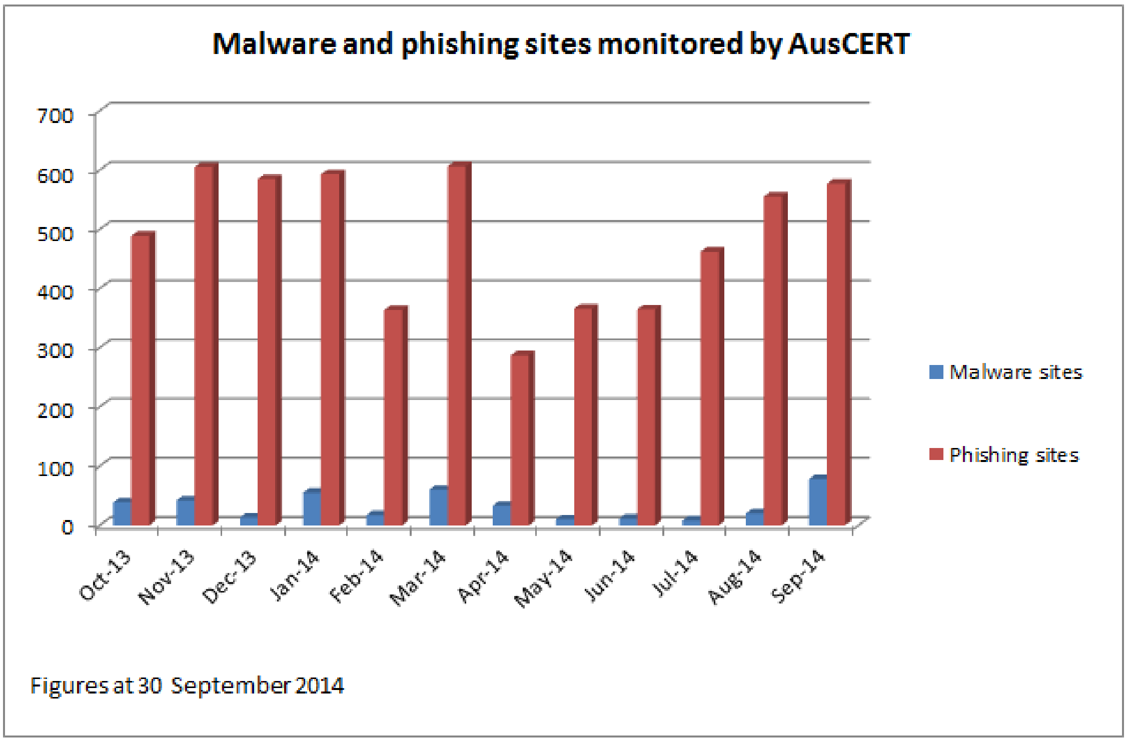
2.3. Threat processing

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.

2.4. Compromise evidence collection and data distribution

AusCERT notifies members of compromise of their web sites, hosts and accounts based on data collected using in-house expertise and analytics from open source data.

2.5. Phishing take down service



AusCERT provides a phishing take down service for members.

2.6. Certificate service

AusCERT provides a phishing take down service for members.

3. Events organised

3.1. AusCERT conferences

AusCERT hosts an annual information security conference in Queensland, on the Gold Coast. It attracts international speakers and attendees and is the largest event of its type in the southern hemisphere. Details here: http://conference.auscert.org.au

Additionally, AusCERT hosted "Security on the Move" conferences in various Australian cities.

3.2. Additional situational awareness monitoring for G20 Brisbane Summit

The G20 Summit in Brisbane during November 2014 presented physical and cyber security challenges for many organisations. AusCERT increased the sensitivity of its operational security monitoring tools for the duration of the summit, and extended analyst working hours to provide additional coverage for AusCERT members.

3.3. Drills

AusCERT participated in the 2014 APCERT drill.

3.4. Events attended

AusCERT attended the following events during 2014:

- APCERT 2014 Conference
- 2014 AISA National Conference
- Ruxcon Security Conference 2014
- 2014 Fraud and Cybercrime Symposium
- 2014 Digital Crimes Consortium (DCC)

4. Achievements

4.1. New structure

During July 2014, Thomas King took over the role of General Manager, AusCERT. A new internal structure was implemented for AusCERT to facilitate increased service delivery to its members.

- Kathryn Kerr took over responsibility for managing AusCERT's membership of over 250 members, including operating the Certificate Service for higher education and research members.
- Mike Holm incorporated development and infrastructure into his existing Operations Team of information security analysts.
- Claire Groves manages AusCERT's events including the major AusCERT Conference.

In August 2014, Thomas initiated a comprehensive review of AusCERT's operations, processes and member services. As part of this process AusCERT consulted with a broad range of members to determine improvements to existing services, and what new services members would like AusCERT to develop on their behalf.

4.2. Presentations

AusCERT presented at the Cyber Defence Conference, Sydney 2014.

5. International Collaboration

5.1. MOUs

AusCERT met and agreed to work with the Korean NSRI (National Security Research Institute) on mobile based malware in the future.

6. Future plans and services

- Increased threat intelligence processing and reporting.
- New request tracking system.
- Fee for service consulting for members.

7. Contacting AusCERT

AusCERT is contactable during Australian Eastern 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

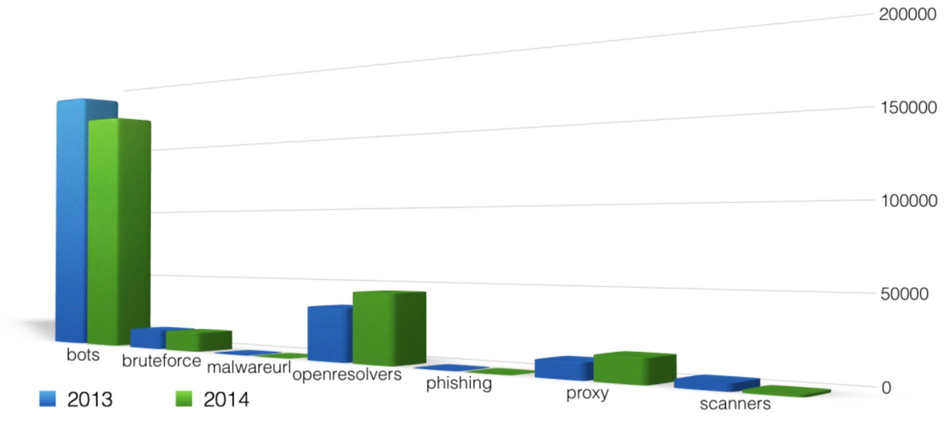
As a national CERT the constituencies of bdCERT are all the Internet users of Bangladesh. We work closely with all the ICT stake holders particularly with ISP Association of Bangladesh (ISPAB), Bangladesh Association of Software & Information Service (BASIS), Bangladesh Computer Samity (BCS), Bangladesh 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 increase in total no of incident in year 2014 as compare to the year 2013. bdCERT observe a significant increase of open-resolvers which causes large scale DDoS attack. 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 bots.



3. EVENTS ORGANIZED / CO-ORGANIZED

- bdCERT in collaboration with bdNOG (Bangladesh Network Operators Group) conduct 3 days Security workshop in "bdNOG1 Conference & APNIC Regional Meeting" which was held in Dhaka from May 19-21, 2014.
- bdCERT members participates in local & regional NOG which includes SANOG (South Asian Network Operators Group), APRICOT (Asia Pacific Regional Internet Conference on Operational Technologies).
- bdCERT members participates in 26th Annual FIRST conference which was held in Boston, Massachusetts.

4. International Collaboration

bdCERT participated in the APCERT Annual incident drill in February 2014 and OIC-CERT Annual incident drill in May 2014.

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 2014

2.1. Security Intelligent Report For Brunei

The statistics presented here are generated by Microsoft security programs and services running on computers in Brunei in 4Q13 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeds or not.

- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

2.2. Encounter and infection rate trends

In 4Q13, the MSRT detected and removed malware from 24.9 of every 1,000 unique computers scanned in Brunei in 4Q13 (a CCM score of 24.9, compared to the 4Q13 worldwide CCM of 17.8). The following figure shows the encounter and infection rate trends for Brunei over the last four quarters, compared to the world as a whole.

- The most common threat family infecting computers in Brunei in 4Q13 was Win32/Rotbrow, which was detected and removed from 16.7 of every 1,000 unique computers scanned by the MSRT. Win32/Rotbrow is a trojan that installs browser add-ons that claim to offer protection from other add-ons. Rotbrow can change the browser's home page, and can install the trojan Win32/Sefnit. It is commonly installed by Win32/Brantall.

- The second most common threat family infecting computers in Brunei in 4Q13 was Win32/Sefnit, which was detected and removed from 3.1 of every 1,000 unique computers scanned by the MSRT. Win32/Sefnit is a family of trojans that can allow backdoor access, download files, and use the computer and Internet connection for click fraud. Some variants can monitor web browsers and hijack search results.

- The third most common threat family infecting computers in Brunei in 4Q13 was Win32/Gamarue, which was detected and removed from 2.2 of every 1,000 unique computers scanned by the MSRT. Win32/Gamarue is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.

- The fourth most common threat family infecting computers in Brunei in 4Q13 was Win32/Dorkbot, which was detected and removed from 1.4 of every 1,000 unique computers scanned by the MSRT. Win32/Dorkbot is a worm that spreads via instant messaging and removable drives. It also contains backdoor functionality that allows unauthorized access and control of the affected computer. Win32/Dorkbot may be distributed from compromised or malicious websites using PDF or browser exploits.

2.3. Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

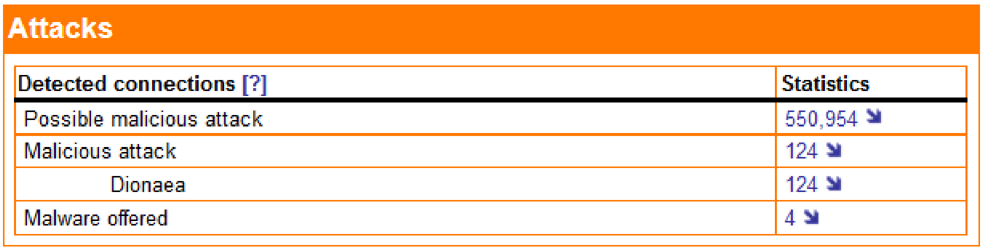
Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

2.4. 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 2014 until November 2014

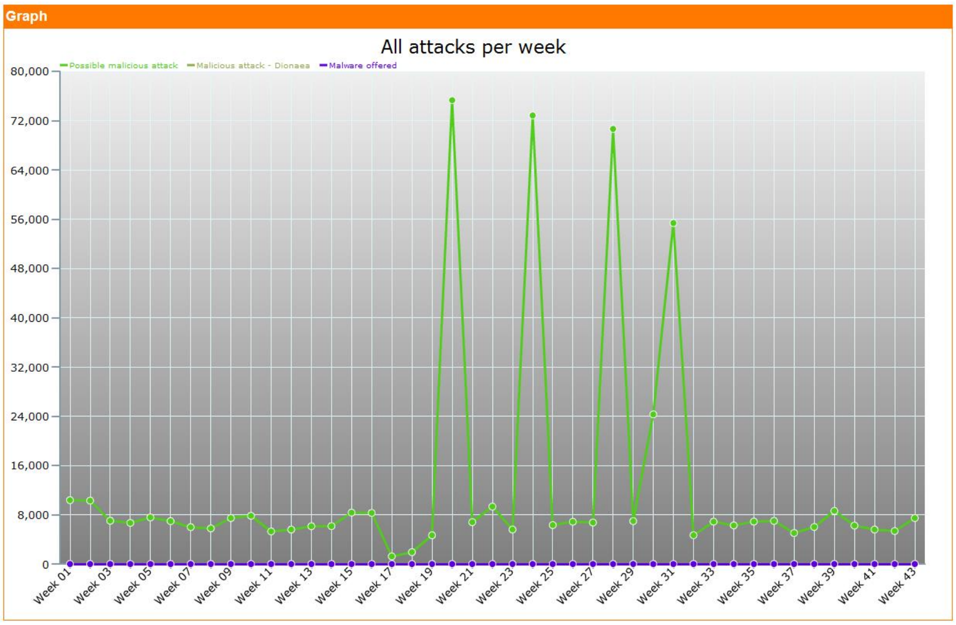


Attacks

Detected connections [?]	Statistics
Possible malicious attack	550,954 ↘
Malicious attack	124 ↘
Dionaea	124 ↘
Malware offered	4 ↘

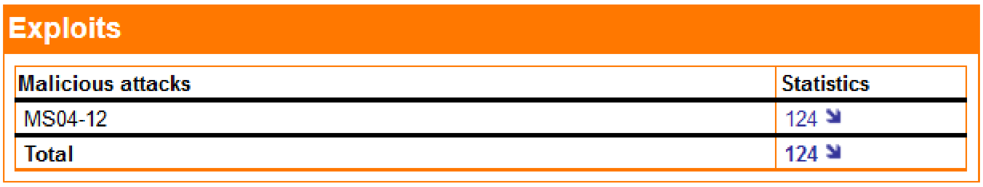
Total Malicious attack

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.

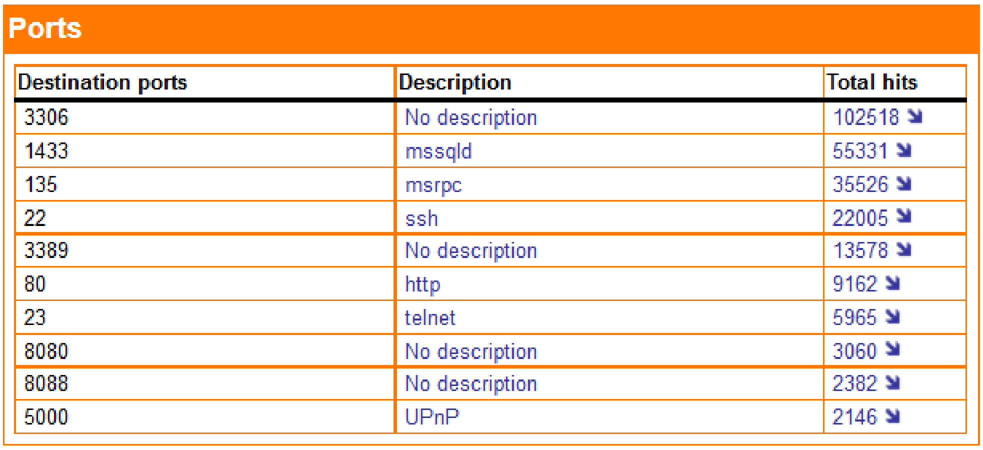


Exploits

Malicious attacks	Statistics
MS04-12	124
Total	**124**

Most attacked Port

Most attacked port and total number of hits.

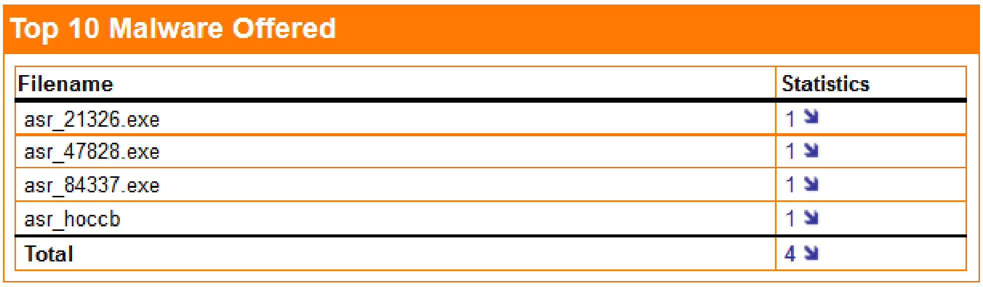


Ports

Destination ports	Description	Total hits
3306	No description	102518
1433	mssqld	55331
135	msrpc	35526
22	ssh	22005
3389	No description	13578
80	http	9162
23	telnet	5965
8080	No description	3060
8088	No description	2382
5000	UPnP	2146

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

Top 10 Malware Offered



Top 10 Malware Offered

Filename	Statistics
asr_21326.exe	1 ↘
asr_47828.exe	1 ↘
asr_84337.exe	1 ↘
asr_hoccb	1 ↘
Total	4 ↘

3. BruCERT Activities in 2014

3.1. Seminars/Conferences/Meetings/Visits

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

- On 18th March until 21th 2014 - Two BruCERT delegates attended the APCERT 2014 Annual General Meeting which takes place at Taipei Taiwan, hosted by TW-CERT.
- On 20th until 22nd November 2014, BruCERT Hosted the OIC-CERT Annual Conference 2014 and the 6th Annual General Meeting, Rizqun International Hotel, Brunei Darussalam.

4. Conclusion

In 2014, 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.

CCERT

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

1. About CCERT

CCERT, CERNET (China Education and Research Computer Network) Emergency Response Team, provides security support services of network security incidents not only for CERNET and its academic members.

2. Activities & Operations in 2014

The main activities & operations of CCERT in 2014 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

2.1. Handling security incidents complaints from CERNET users

In 2014, CCERT handled 6,544 security incident complaints, including 2,614 spams, 3,634 website Intrusion, 192 port scanning, 22 phishing, 14 DoS attack and 68 others.

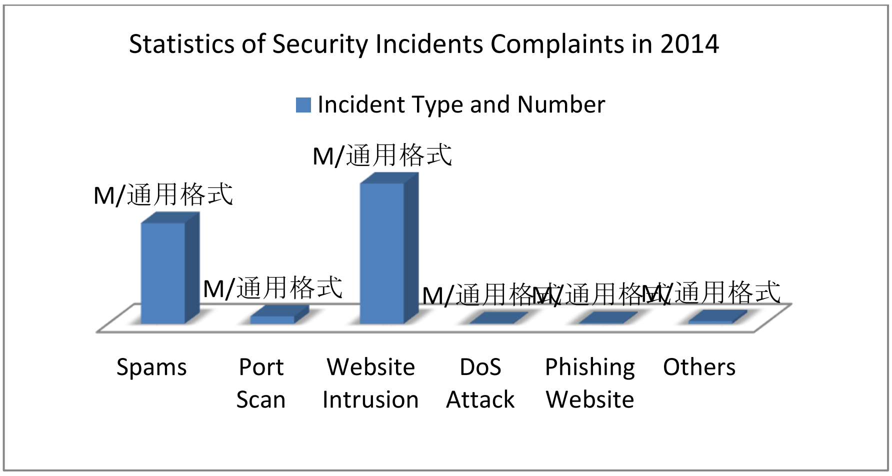


Figure 1

In 2014, CCERT focus on handling the security incident of website Intrusion. By analyzing the 3,634 Website Intrusion incidents handled in 2014, we find the following causes which result in the above website intrusion.

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

In which, SQL Injection Vulnerability and Weak Password Account Vulnerability are the main causes which result in the website intrusion.

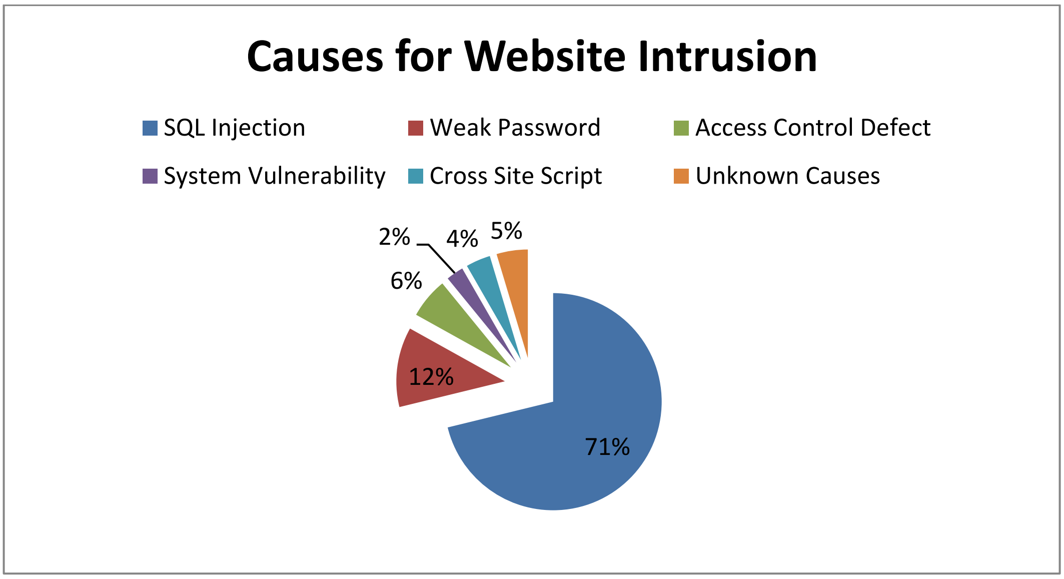


Figure 2

Most of the compromised websites are added by hidden links which are used to optimize illegal search. Different from before, now hacks use new techniques to hide the links in the compromised website. The compromised server will detect the browser type of the target web page with hidden link, and only when search engine crawler is found it will display the content with hidden link, otherwise, it will display the normal web page, which greatly increase the difficulty to detect the hidden link. Besides hidden links, back door programs running in website is also found in compromised sites which are used for attackers to control the compromised server.

2.2. Security Monitoring and Information Publishment

In 2014, through security monitoring, CCERT found many large scale DoS reflection attack incidents in CERNET Network, there about 1,274 compromised servers and hosts. These reflection attacks make use of multiple basic network services, which include:

1. Make use of the monlist function of the NTP Service to execute reflection attack
2. Make use of the DNS query function to execute reflection attack
3. Make use of the Chargen Character Generator Protocol to execute reflection attack

We not only informed the person in charge of the detected 1274 servers to handle the security incidents, but also sent to other CERNET users about the security warning of the above reflection attacks and how to prevent relative infrastructures from being exploited to execute the reflection attacks.

Other security monitoring and security bulletins:

1. Monitoring and Analysis report about the Heart Bleed Vulnerability
2. Monitoring and Analysis report about the Gnu Bash Shell Shock Vulnerability
3. Monitoring and Analysis report about the remote code execution vulnerability of the Schannel secure channel of Windows system

2.3. Technical Consultation and Security Service

In 2014, CCERT provided with free security scanning service for 6013 websites, and found that about 60% of the scanned websites exist security vulnerabilities, and about 19% of which belong to high risk.

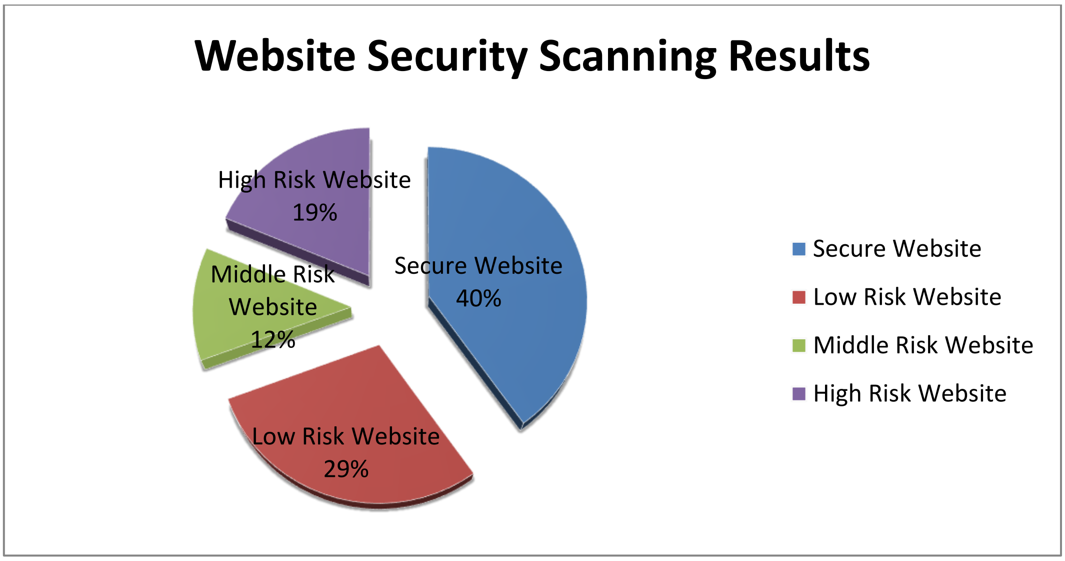


Figure 3

2.4. Security training & activities

In 2014, CCERT hosted 17 security trainings for 2,106 participants. The security training contents include:

1. Introduction of the next generation firewall technology
2. DNS Domain system security and protection
3. Utilize two-dimension code to simplify network access authorization for visitors
4. Cognition and Practice of Cloud Computing
5. Exploration and practice of campus website security management mode

2.5. Research on security technologies

In 2014, CCERT members found security vulnerabilities of HTTPS deployment in CDN: many top CDN providers don't encrypt users secret content in the backend communication from CDN node to original web sites, although the frontends (from browser to CDN node) use HTTPS. We also found the current practices for X509 certificate cause revocation and other problems. We also proposed solutions to solve these problems.

We publish our research in IEEE Symposium on Security and Privacy in 2014:"When HTTPS meets CDN: A Case of Authentication in Delegated Service". After the conference, several top CDN providers, including CloudFlare, have improved their products or services.

3. Future Plans

In 2015, 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. About CERT Australia

1.1. 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.

1.1.1. 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.

1.1.2. Workforce power

CERT Australia currently employs 23 core staff.

1.1.3. 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.

2. Activities & Operations

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 2014, 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
- coordinated the Australian Government's cyber security support to Australian business, particularly owners and operators of SNI and CI, for the G20 event held in Brisbane in November 2014
- hosted several 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 Australian Cyber Security Centre's ability to form a national picture of cyber threats
- responded to incidents involving targeted and untargeted attacks against Australian organisations.

2.1. Incident handling reports

In 2014, CERT Australia had 11,144 cyber incidents reported to it, a decrease of approximately 3 per cent from 2013. These incidents required a range of responses depending on their nature. CERT Australia also produced and disseminated sensitive advisories on cyber vulnerabilities affecting SNI.

3. Events organised/co-organised

3.1. Drills

In March 2014, CERT Australia co-facilitated with CyberSecurity Malaysia, the Malaysian Communications and Multimedia Commission and the Australian Strategic Policy Institute a cyber security discussion exercise as part of the ASEAN Regional Forum Workshop on Cyber Confidence Building Measures in Kuala Lumpur.

3.2. Meetings

CERT Australia hosted the September 2014 APCERT Steering Committee meeting in Brisbane. The SC Meeting was held in parallel with the APNIC Conference and adjacent to the joint APCERT-APNIC Security Track.

4. Achievements

At the March 2014 APCERT Annual General Meeting in Taiwan, CERT Australia was re-elected to the APCERT Steering Committee for a second term.

4.1. Presentations

CERT Australia delivered presentations at both the Asia Pacific Regional Internet Conference on Operational Technologies (APRICOT) in Kuala Lumpur in April and the APNIC Conference in Brisbane in September.

Throughout 2012, CERT Australia also presented at and/or participated in several other international forums including:

- S4 (SCADA Scientific Security Symposium), January - Miami
- APCERT AGM and Conference, March – Taiwan
- International Watch and Warning Network (IWWN) Annual Meeting, May – Japan

- FIRST conference, June – Boston
- Blackhat & DefCon, July – USA
- RuxCon and Breakpoint Conferences , October – Australia
- Kiwicon, November – New Zealand
- Other closed events organised by international government organisations and CERTs.

4.2. Publications – Cyber alerts, advisories and strategies

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.

5. International Collaboration

CERT Australia continues to establish new, and maintain existing, contact with international CERTs, engaging pro-actively in a wide range of international fora, from bilateral discussions to international conferences and meetings and cyber security exercises such as the APCERT Drill. Through this work CERT Australia is able to coordinate and improve linkages between national CERTs, and formalise existing arrangements which enables effective coordination on international cyber security issues.

Some examples of CERT Australia's international activity in 2014 are:

- CERT Australia participated in the 2014 APCERT Drill held in February
- In March 2014, CERT Australia co-facilitated with CyberSecurity Malaysia and Malaysian Communications and Multimedia Commission a cyber security discussion exercise as part of the ASEAN Regional Forum Workshop on Cyber Confidence Building Measures in Kuala Lumpur
- CERT Australia presented at the 2014 APCERT-APNIC Security Tracks of the APRICOT and APNIC Conference events in Kuala Lumpur and Brisbane respectively
- CERT Australia hosted the September 2014 APCERT Steering Committee meeting in Brisbane

- CERT Australia participated in the 2014 ASEAN CERT Incident Drill (ACID) held in September.

CERT-In

Indian Computer Emergency Response Team – India

1. About CERT-In

1.1. 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 designated CERT-In to serve as the national agency to perform the following functions in the area of cyber security:

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

1.1.1. 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.

1.1.2. Workforce power

CERT-In has a team of 75 technical members.

1.1.3. 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.

2. Activities and Operations of CERT-In

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

2.1. Incident handling Reports

The summary of activities carried out by CERT-In during the year 2014 is given in the following table:

Activities	Year 2014
Security Incidents handled	130338
Security Alerts issued	13
Advisories Published	69
Vulnerability Notes Published	290
Trainings Organized	22
Indian Website Defacements tracked	25037
Open Proxy Servers tracked	2408
Bot Infected Systems tracked	7728408

Table 1. CERT-In Activities during year 2014

2.2. Abuse Statistics

In the year 2014, CERT-In handled more than 1,30,000 incidents. The types of incidents handled were mostly of Spam, Website intrusion & malware propagation, Malicious Code, Phishing and Network Scanning & Probing.

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

Security Incidents	2014
Phishing	1122
Network Scanning / Probing	3317
Virus/ Malicious Code	4307
Website Defacements	25037
Spam	85659
Website Intrusion & Malware Propagation	7286
Others	3610
Total	130338

Table 2. Breakup of Security Incidents handled

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

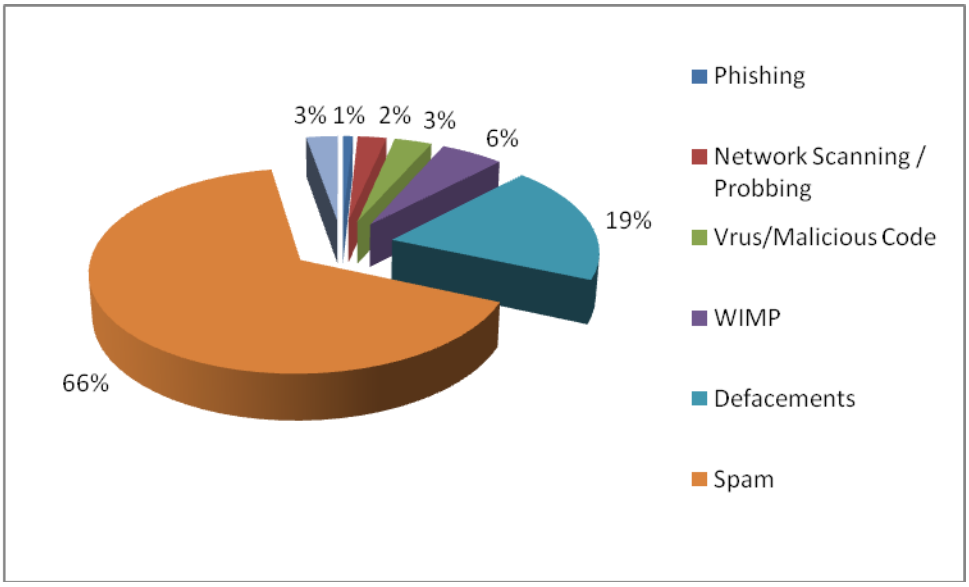


Figure 1. **Summary of incidents handled by CERT-In during 2014**

2.3. Incident Trends

The trends of incidents reported to and handled by CERT-In and cyber attack trends during the year 2014 are as follows:

- **Exploitation of Drupal Vulnerability in the wild**

  It has been observed that Drupal SQL Injection vulnerability exploitation was wild on the month of October 2014. This vulnerability exists due to insufficient sanitization of data by the database abstraction API. A remote attacker could exploit this vulnerability by sending specially crafted requests, resulting in execution of arbitrary SQL commands.

  Successful exploitation of this vulnerability could cause attacker to view, add, modify or delete information in the back-end database.

- **D4re|Dev|targeting Mass transit systems and E-Kiosks**

  It has been reported that a new point of sale systems malware, dubbed "D4re|Dev" a.k.a "DareDevil" targeting Mass transit systems is spreading. The malware mainly infect the machines used as public transport ticket vending machines or the interactive Kiosks. The attacker may gain the initial access due to the inadequate internal security policies such as weak passwords along with the use of the POS systems for other activities including web surfing, email accessing, games, accessing social networking sites etc. Once an initial access is gained, then attacker can upload other backdoors using the malware's "Remote File Upload "functionality. These backdoors run under the processes named "hkcmd.exe", "PGTerm.exe" and other legitimate processes of Google Chrome in order to bypass security restrictions and remain undetected. Successful compromise of the infected system gives full access of the infected system to the remote attacker.

- **Havex Malware targeting ICS/SCADA control systems**

  It has been reported that an industrial information stealing malware, dubbed Havex, is targeting ICS based systems by leveraging OPC protocol implementation. OPC is OLE for communication / Open platform communication - a standard for windows applications to communicate to process control hardware and transfer process data between systems from different vendor. The malware reported as performing intelligence gathering by mapping network resources and connected devices information from the process control network. The HAVEX RAT is reaches the machine via social engineering methods, website redirects, exploit kits or by watering hole.

- **Gameover aka Zeus-P2P malware surge**

  It has been reported that "GameOver" malware aka Zeus-P2P is surging with new tactics techniques and procedures (TTP). GameOver malware is the incarnation of the information stealing banking malware Zeus/ Zbot imbibed with Peer-2-Peer capabilities to communicate with the C2 server, majorly distributed through Cutwail spam bot. The malicious mails used social engineering techniques by impersonating financial institutions and government agencies, with a ".zip" file attached, the compressed archive contains an application titled UPATRE. The application UPATRE is used to download the encrypted file (to evade from perimeter defenses) from compromised websites and decrypt it to extract and execute the GameOver.
- Malware targeting Point of Sale (POS) systems were on the raise. Prominent POS malware reported are Dexter, BrutPOS, BackOff etc.
- Malicous apps affecting the Android Mobile phones are also reported during the year 2014. The android malware families prevalent were OpFake, Android/FakeInst, Android SmsSend, Badaccents etc. Such malicious Apps are capable of performing premium based texting / subscribe the user to expensive services, install backdoors, reading and intercepting SMS'es and send it to remote servers.

2.4. 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 25037 numbers of defacements have been tracked.

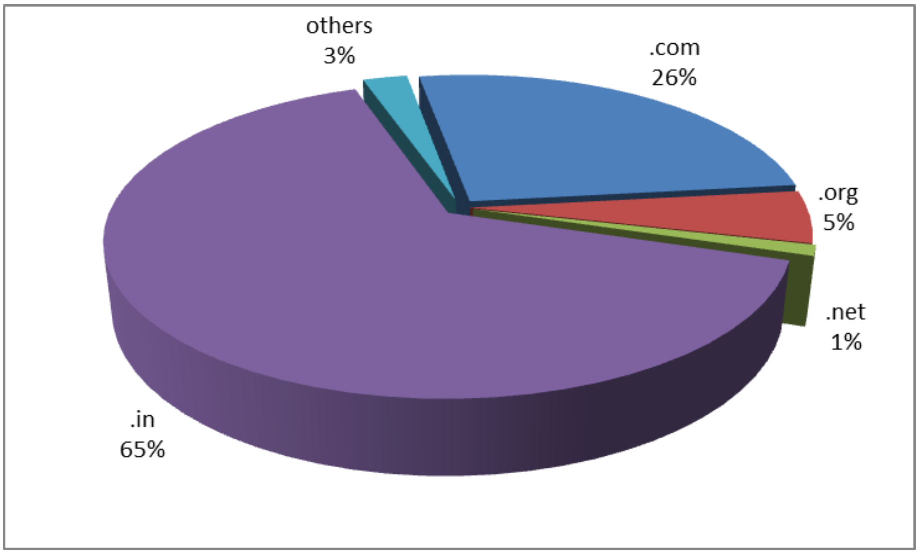


Figure 2 Indian websites defaced during 2014

2.5. Tracking of Open Proxy Servers

CERT-In is tracking the 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 2408 open proxy servers were tracked in the year 2014. The month-wise distribution of open proxy servers tracked during this year is shown in the figure 3.

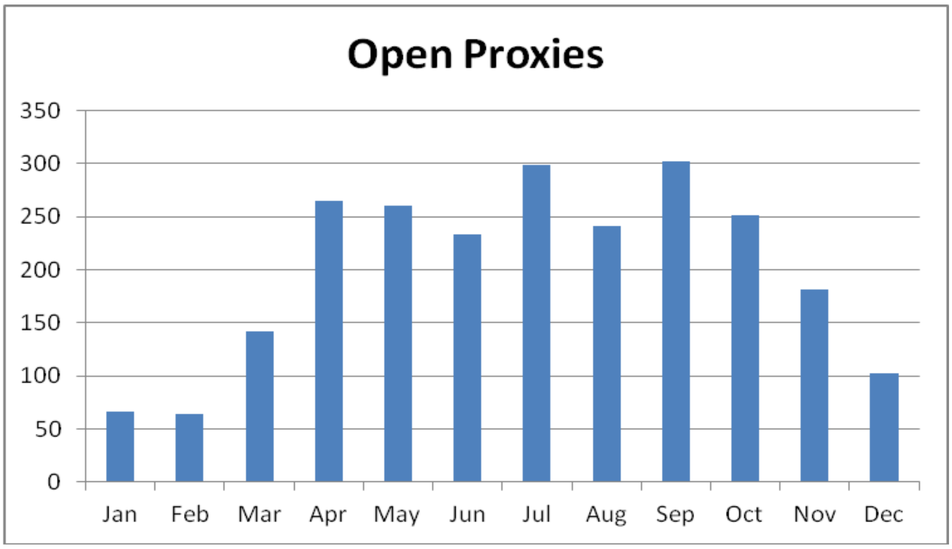


Figure 3. Monthly statistics of Open Proxy Servers in 2014

2.6. 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 2014.

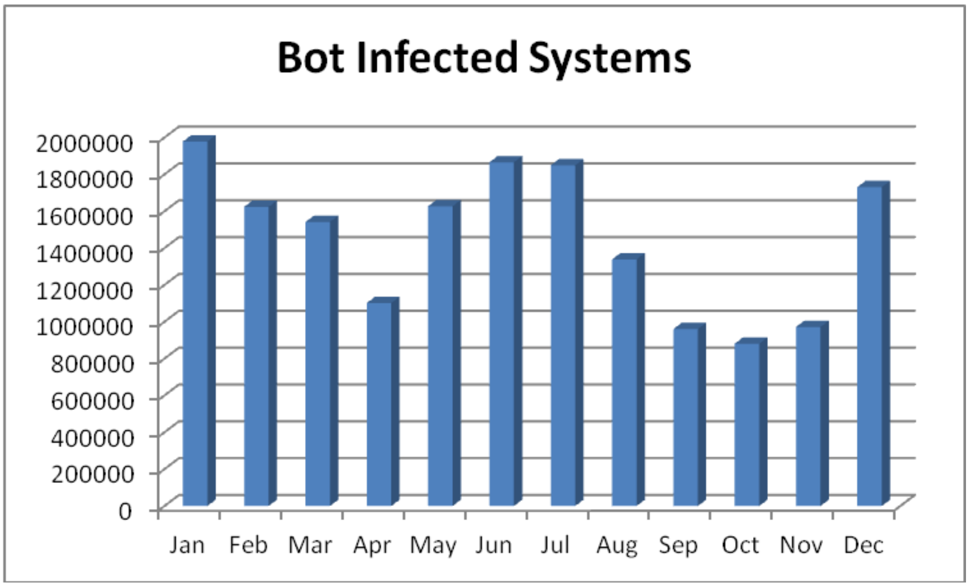


Figure 4. Botnet statistics in 2014

2.7. Collaborative Incident resolution

During the year 2014, CERT-In worked in collaboration with security/product vendors and Internet Service Providers in India to detect the botnet infected systems. Botnets such as Baldabindi, Jenxcus and Gameover/ZeuS P2P were tracked through collaborative actions.

2.8. Interaction with Sectoral CERTs

CERT-In plays the role of mother CERT and is regularly interacting with the Chief Information Security Officers (CISOs) of Sectoral CERTs in Defense, Finance, Power, Transport and other sectors to advise them in the matters related to cyber security.

2.9. Security Profiling and Audit Services

CERT-In has provisionally empanelled 45 information security auditing organizations, subject to background verification and clearance of organizations, under the revised process of empanelment for the block 2012-2015, 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.

2.10. 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.

3. Events organized/ co-organized

3.1. 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 2014:

- Workshop on "Web Application Security" on January 13, 2014
- Workshop on "Linux security" on January 24, 2014
- Workshop on "Critical Infrastructure Security Risk & Compliance" on February 20, 2014
- Workshop on "Data Centre Security" on February 21, 2014
- Workshop on "Cyber Security Threats and Cyber Security Policy" on February 26, 2014
- Workshop on "Cyber Security Threats, Cyber Crime and Cyber Forensics" on March 07, 2014

- Workshop on "Mobile Forensics" on April 16, 2014
- Workshop on "Advanced Web Application Security" on April 21, 2014
- Workshop on "Secure Cloud Computing" on May 30, 2014
- Workshop on "Vulnerability Assessment & Penetration Testing" on June 20, 2014
- Workshop on "Cyber Crime Investigations and Cyber Security Policy" on June 27, 2014
- Workshop on "Targeted Attacks - Trends & Mitigation" on July 25, 2014
- Workshop on "Big Data Analytics & Security" on August 14, 2014
- Workshop on "Windows 8 Security" on August 22, 2014
- Workshop on "Latest Security Trends" on August 27, 2014
- Workshop on "Cyber Security: Threats & Mitigations" on September 17, 2014
- Workshop on "Cyber Security Threats and Cyber Security Policy" on October 15, 2014
- Workshop on "Network Security" on October 17, 2014
- Workshop on "Mobile Forensics" on November 14, 2014
- Workshop on "Wireless Security" on November 26, 2014
- Workshop on "Cyber Security Threats: Advanced Detection & Prevention Techniques" on December 03, 2014
- Workshop on "MS SQL Database Security" on December 17, 2014

3.2. Cyber Security Drills

CERT-In successfully participated in the ASEAN CERTs Incident Handling Drill (ACID 2014) held in September 2014. 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. These drills at present are being carried out once in six months. 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. 9th Cyber Security Mock Drill was conducted on 23rd December 2014.

4. Achievements

4.1. 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.

4.2. Cyber Security Assurance initiatives

- National Cyber Security Policy-2013(NCSP-2013) was released by Government in August 2013 for public use and implementation with all relevant stakeholders. The objective of the policy is to create a framework for comprehensive, collaborative and collective response to deal with the issue of cyber security at all levels within the country.
- 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. So far, 10 implementation enabling workshops/interactions have been conducted. Services of CERT-In empanelled IT security auditors are being used to verify compliance.
- 45 auditors were empanelled for audit of IT infrastructure after a fresh round of skill assessment in the year 2014.
- CERT-In has also carried out security audits of some of the organizations in the critical sector.

5. International collaboration

- 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.
- CERT-In signed a MoU with Korea Internet & Security Agency (KISA) in January, 2014 to enable information sharing and collaboration for incident resolution.

6. Future Plans/Projects

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:

- Creation of a framework for comprehensive, collaborative and collective response to deal with the issue of cyber security at all levels within the country
- 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
- Creation of framework and facility for collection, correlation and analysis of security events in real time and generating early warning to constituency.
- Creation of facilities to detect and clean the Botnet infected systems in coordination with Industry

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: 0x9E346D2C
Fingerprint: 4871 0429 EB42 0423 4E6A FAD6 B2D5 5C16 9E34 6D2C
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/CC

1.1. Introduction

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

1.2. Establishment

CNCERT was founded in 2002, and became a member of FIRST in Aug 2002. It also took an active part in the establishment of APCERT as a founding member.

1.3. Workforce power

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

1.4. Constituency

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

1.5. Contact

E-mail:	cncert@cert.org.cn
Hotline:	+8610 82990999（Chinese）, 82991000（English）
Fax:	+8610 82990375
PGP Key:	http://www.cert.org.cn/cncert.asc

2. Activities & Operations

2.1. Incident handling

In 2014, CNCERT received a total of about 56.2 thousand incident complaints, a 77.3% increase from the previous year. And among these incident complaints, 878 were reported by overseas organizations, making a 9.6% drop from the year of 2013. As shown in Figure 2-1, most of the victims were plagued by vulnerability (36.4%), phishing (32.1%)and website defacement(16.3%). Vulnerability still overtook phishing to be the most frequent incident complained about. And website defacement ranked the third place with an increase of 1.9% from 2013.

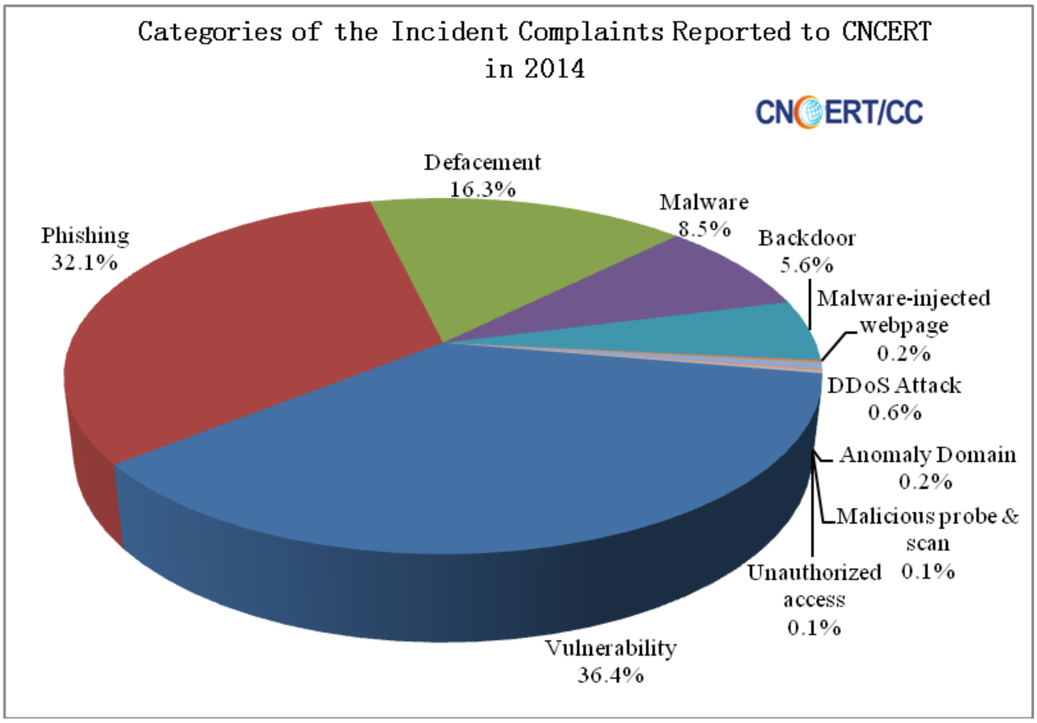


Figure 2-1Categories of the Incident Reported to CNCERT in 2014

In 2014, CNCERT handled almost 56.1 thousand incidents, a significant rise of 79.8% compare with that in 2013. As illustrated in Figure 2-2, vulnerability (36.1%) dominated the categories of the incidents handled by CNCERT in 2014, followed by phishing (32.0%) and website defacement (16.0%).

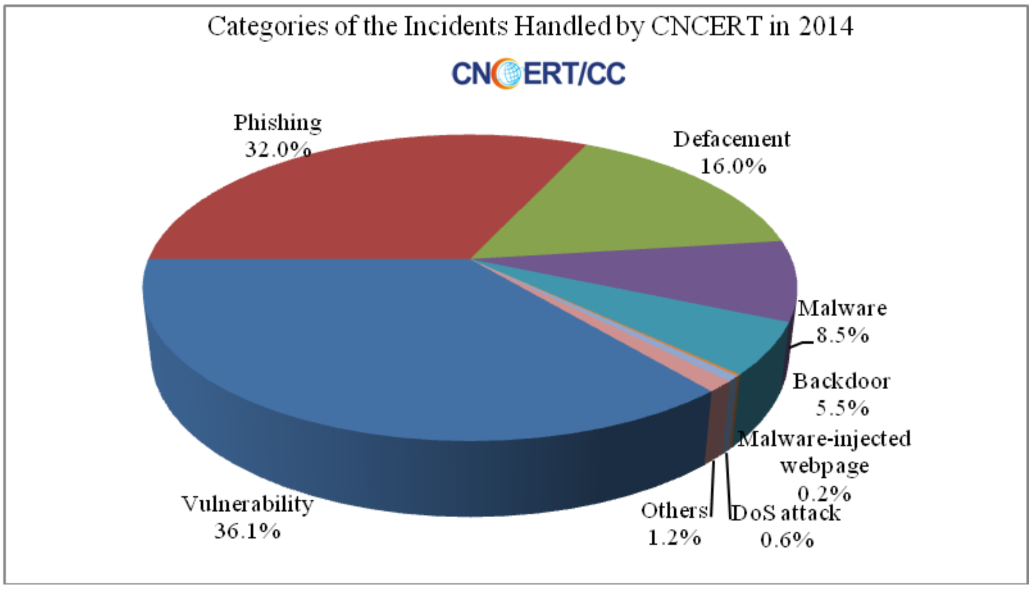


Figure 2-2 Categories of the Incidents Handled by CNCERT in 2014

2.2. Internet Awareness

2.2.1. Malware Activities

In mainland China, IPs of the hosts infected with Trojan or Botnet reached about 11.1 million, which decreased by 2.3% compared with that in 2013. Because CNCERT awareness systems are all located in mainland China, most IPs of Trojan or Botnet C&C servers we found were identified in local networks. But we still saw more than 42.3 thousand oversea C&C servers which increased 25.3% from 2013. As shown in Figure 2-3, the US hosted the largest number of oversea C&C servers' IPs of Trojan or Botnet, followed by China HongKong and South Korea.

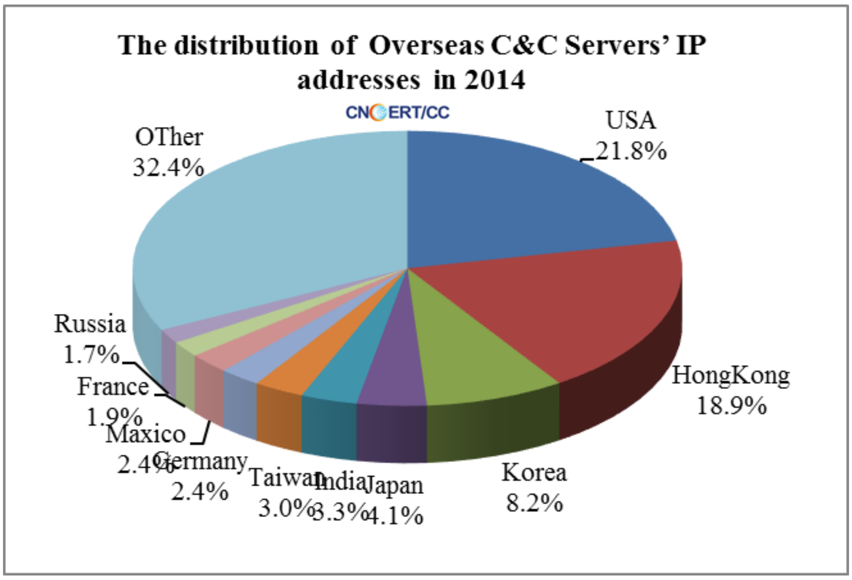


Figure 2-3 The distribution of overseas C&C server's IP addresses in 2014

By CNCERT's Conficker Sinkhole, over 70.1 million hosts were suspected to be infected all over the world. And 8.9 million compromised hosts were located in mainland China. As shown in Figure 2-4, mainland China (12.7%) had the most infection, followed by India (7.9%), and Brazil (6.9%).

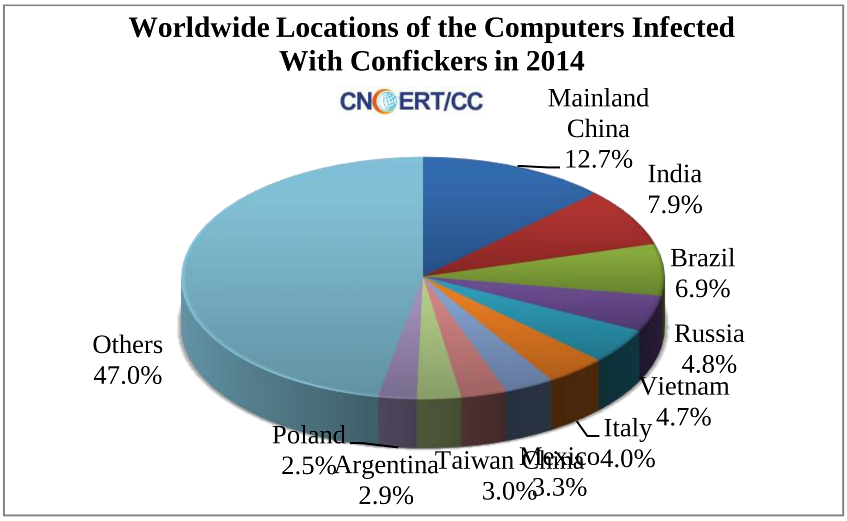


Figure 2-4 Worldwide Locations of the Computers Infected With Confickers in 2014

The malware-hosting websites is the jumping-off place for malware propagation. The malware-hosting websites monitored by CNCERT in 2014 involved about 10.4 thousand domains, about 5.1 thousand IP addresses and about 115.1 thousand malware download links. Among the 10.4 thousand malicious domains, 92.9% of their TLDs fell into the category of .com. Among the 5.1 thousand malicious IPs, 52.0% were located overseas. In 2014, CNCERT monitored about 15.9 million malware spreading incidents. Figure 2-5 depicts the monthly statistics of malware spreading incidents in 2014, with the most rampant malware activity in May.

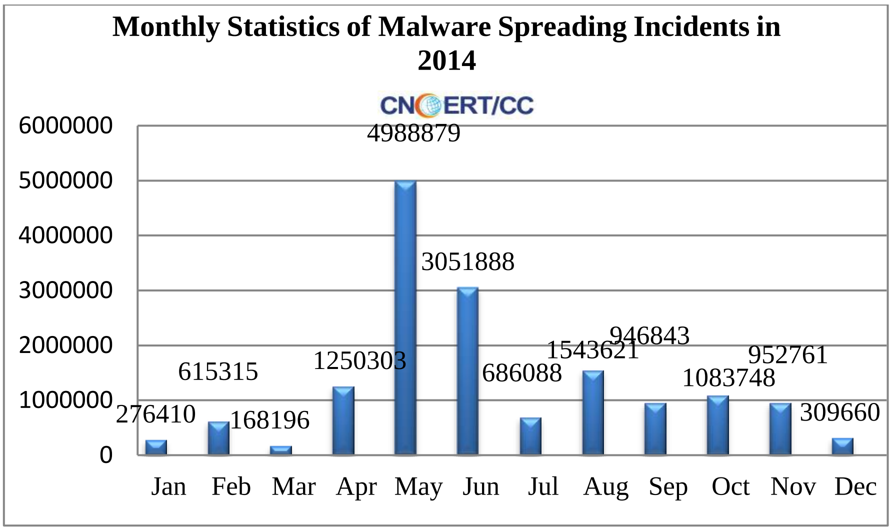


Figure 2-5 Monthly Statistics of Malware Spreading Incidents in 2014

2.3. Website Security

About 37.0 thousand websites in mainland China were defaced, a considerable increase of 54.2% compare with that in 2013, including 1763 government sites. Besides, about 40.2 thousand websites were detected to be planted with backdoors and secretly controlled, including 1529 government sites.

In 2014, CNCERT found about 99.4 thousand phishing sites targeting the websites in mainland China. About 6844 IPs were used to host those fake pages. About 89.4% were out of mainland China. Most of the phishing servers (17.7%) were located in US.

CNCERT found almost 19.2 thousand overseas IPs conducted remote control on over 33.6 thousand websites in mainland China. As shown in Figure 2-6, 4761 (24.8%) were located in the US, followed with 1280 (6.7%) in Korea and 1238 (6.5%) in China Hongkong .

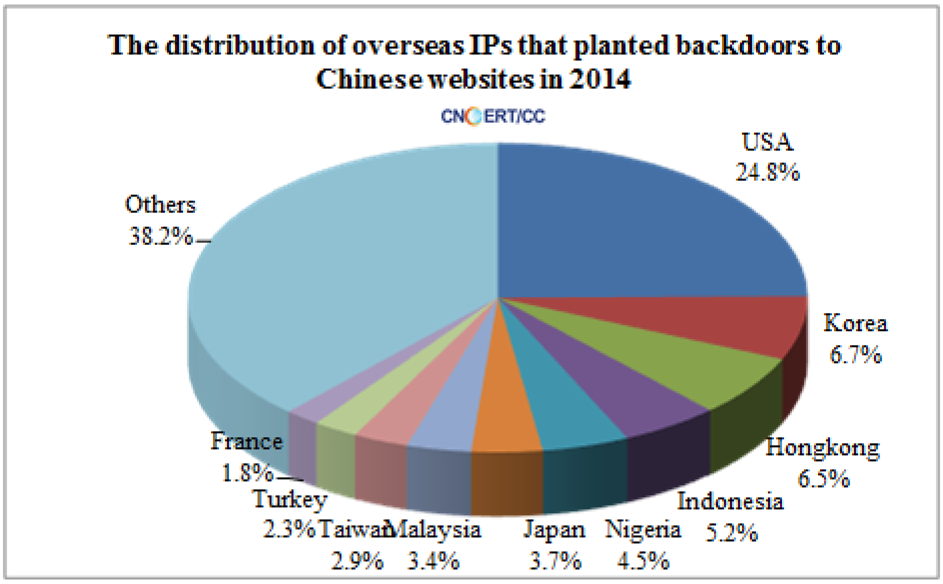


Figure 2-6 The distribution of overseas IPs that planted backdoors to Chinese websites in 2014

2.4. Mobile Awareness

In 2014, CNCERT collected about 951.1 thousand mobile malware samples in total. In terms of intentions of these mobile malware, the malicious fee-deducting malware continued to take the first place (55.0%), fee consumption (15.3%) stood the second place. And followed it were those intended for stealing information and Rogue behavior accounting for 12.9%and 9.7% respectively.

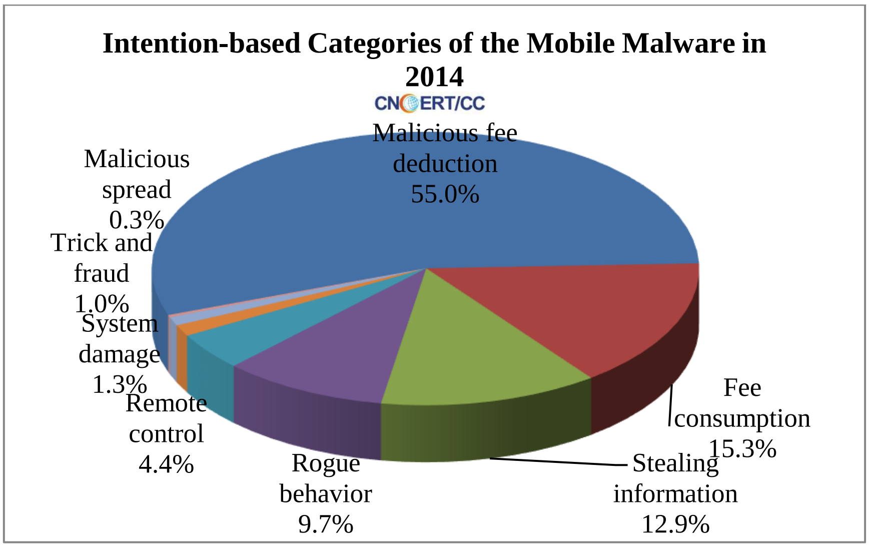


Figure 2-7 Intention-based Categories of the Mobile Malware in 2014

The majority of these mobile malware identified by CNCERT ran on Android platform, recording about 949.8 thousand (99.9%).

3. Events organized/co-organized

3.1. Conferences

The issue of "A Review of Network Security Situation in 2013"

CNCERT gave a press conference on 2013's Network Security Situation in Beijing on 28th March, 2014, introducing the overall picture and main features of China's network security in 2013. Specialists and representatives from 47 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 2013, looked forward to threats of much concern in 2014 and made a number of suggestions.

The hold of 2014 Annual Chinese Conference on Computer and Network Security in Shantou, Guangdong Province

CNCERT held 2014 Annual Chinese Conference on Computer and Network Security in Shantou Guangdong on 28th May, 2014. The theme of the conference is "Collaborative Protection for Safe Future". Sub-Forums had been set up according to the four subjects: the security of mobile Internet in 4G era, protection of personal information and defense of APT attack, security of key infrastructures and network security academic forum of CNCERT-CIE. More than 600 representatives from governments, important information systems departments, industries and enterprises, universities, research institutes and other organizations attended the meeting.

The hold of the second 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 Seoul, Korea to hold the second China-Japan-Korea Annual Meeting for Cyber Security Incident Response from

August 21st to 22nd , 2014 . The Parties reviewed handling and prevention efforts made in responding to serious security incidents. The technical experts from three sides exchanged latest information on cyber security threats at the meeting. Three parties reiterated their evaluation for the handling cases of major security incidents and further research in each other's ability and methods of incidents handling, which will strengthen the cooperation among the three parties. Three parties reached the consensus that they will make contributions to improving the global network environment by supporting the establishment of information sharing protocols, scope and criteria for network risk assessment.

The hold of The 6th China-ASEAN Network Security Seminar in Shantou

CNCERT organized the 6th China-ASEAN Network Security Seminar in Shantou, China from May 27 to May 29, 2014. Delegates from the telecom department of government and CERTs in Cambodia, Indonesia, Lao, Myanmar, the Philippines, Thailand and Viet Nam 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 2014

CNCERT participated in the APCERT 2014 Drill as a participant on 19 February 2014 and completed it successfully.

The theme of the APCERT Drill 2014 was 'Countering Cyber-ops (cyber operations) with Regional Coordination. The focus of the drill is to prevent attackers from launching DDOS attack against a Government Department information system 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 16 economies of APCERT took part in the exercise.

ASEAN CERT Incident Drill (ACID) 2014

CNCERT participated in the ASEAN CERT Incident Drill (ACID) 2014 on September 24th 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 2013.

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	32	Published on journals and magazines.

EC-CERT

Taiwan E-Commerce Computer Emergency Response Team - Chinese Taipei

1. About EC-CERT

1.1. 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.

1.2. EC-CERT Services

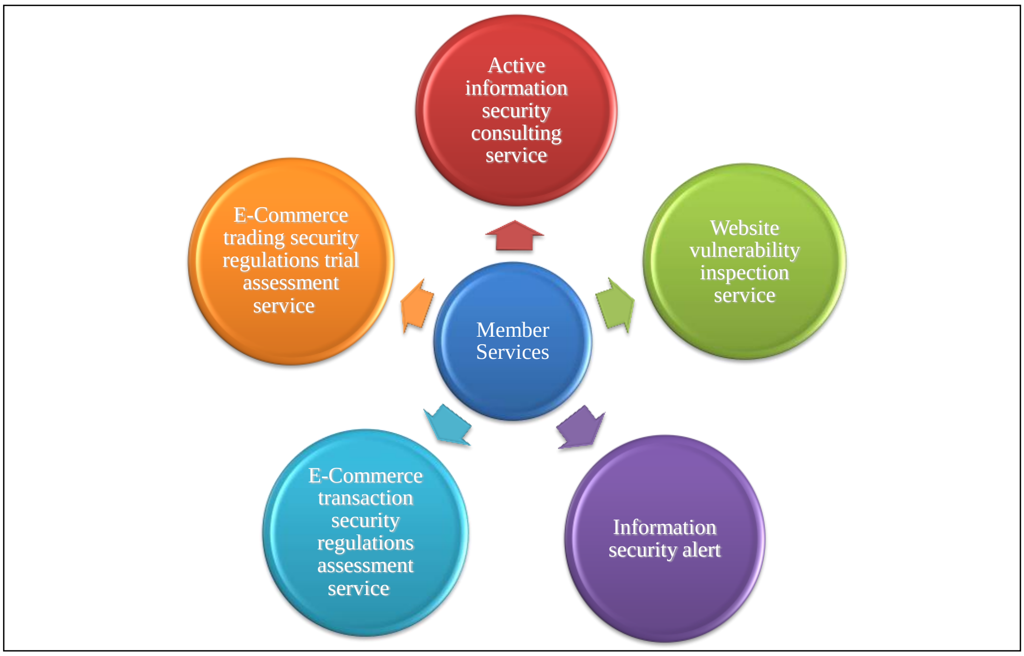

Active information security consulting service
E-Commerce trading security regulations trial assessment service
Website vulnerability inspection service
Member Services
E-Commerce transaction security regulations assessment service
Information security alert

Figure 1.EC-CERT Services

(1) Active information security consulting service

EC-CERT keeps exchanging security incidents report with G-ISAC and inform website operator caused by security incident. EC-CERT would contact web site owner and provide security solution to reduce and prevent further loss.

(2) Website vulnerability inspection and penetration testing service

EC-CERT vulnerability inspection and penetration testing service has been developed for a couple of years. The purpose of the service is help E-Commerce firm understand the what, why, when, where, and how to testing web applications. The service delivers complete inspection of website, not only a simple checklist or security issues that should be addressed but also correction procedures.

(3) Information security alert service

EC-CERT gathers various data regarding security threats, exchange security information with domestic and foreign information security organizations, then interpret these data into alerts such as security leaks, malicious websites, hackings and phishing, and recommend defensive measures so that E-Commerce operators can take advance prevention measures to reduce their information security threats and to avoid potential loss.

In additional, EC-CERT has been regularly issued lists of hacker relay station domain and IP addresses so that E-Commerce operators can renew their relay station blacklist and update their information defense mechanism, and effectively protect consumers from being linked to malicious relay stations, thus preventing security breach and sensitive information leaks.

(4) E-Commerce security incident investigation and response

EC-CERT work with Criminal Investigation Bureau to intervene security incident investigation and response with in E-Commerce firms depend on necessary. When EC-Commerce website been security assaulted caused personal information and transaction data leakage, EC-CERT offers security investigation and incident response handle.

(5) E-Commerce transaction security regulations assessment service

EC-CERT work out E-Commerce transaction security regulations, integrate information safety management standard to provide E-Commerce operators with free on-site regulation assessments in order to help them keep and follow security regulations.

2. Activities & Operations

2.1. Active information security consulting service

(1) EC-CERT recorded 42 E-Commerce industry information security reporting in 2014. Those reports including website system security on line consulting records and step by step real case resolution procedures and suggestions.

(2) Due to EC-CERT provided E-Commerce security recommendations and improvement instructions to a web develop company owned 19 E-Commerce websites after then they have never been reported any security incident from 2014, Aug.

2.2. Website vulnerability inspection Service

EC-CERT provided website vulnerability inspection service for information security event of E-Commerce industry. The results explained of the most common high-risk as in Figure 2. About 31% of the HTML forms without CSRF protection, 15% of the Cross site scripting (verified) and 10% of the Application error message.

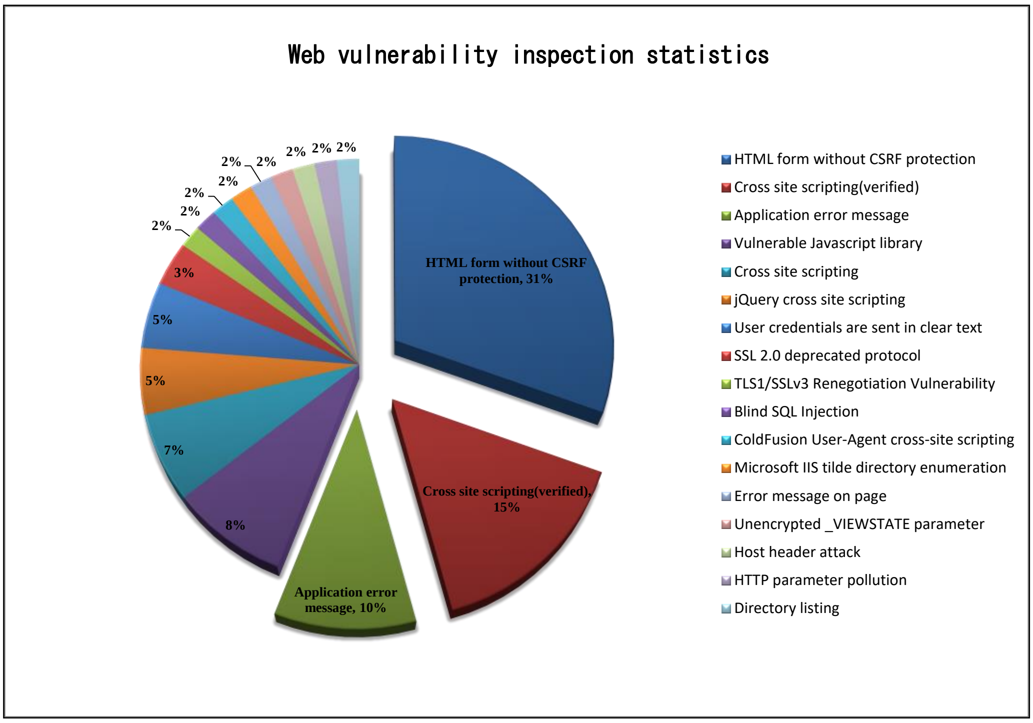


Figure 2.Web vulnerability inspection statistics

2.3. Information security alert service

EC-CERT informs member notices regarding the latest information security threat warnings and Internet vulnerabilities as in Figure 3. About 53% of the Alert reports are on Announcement Advisory, and early Warning and website defacement as well as Feedback Information.

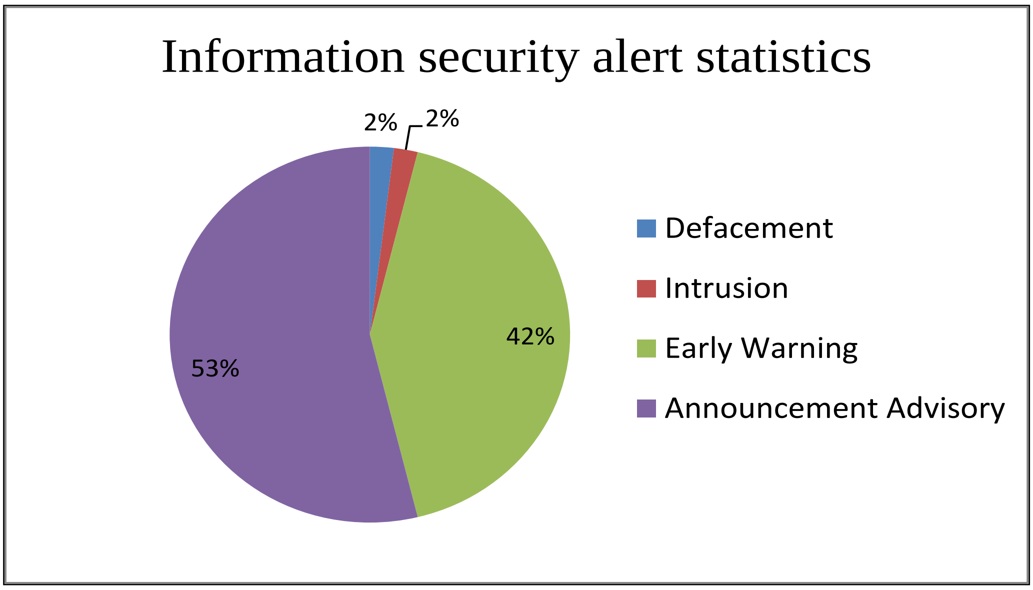


Figure 3.Information security alert statistics

2.4. E-Commerce information security regulation evaluation service

EC-CERT has been provided E-Commerce Information Security Regulation Evaluation service for five E-Commerce companies. The service evaluates E-Commerce firm if it is capable to provide safe transaction environment in information security, passing requirement up to 80%. EC-CERT would award to a certificates. EC-CERT appreciates and encourage E-Commerce vendor pass this evaluation.

2.5. E-Commerce security incident investigation and response services

EC-CERT has been worked with Criminal investigation bureau 165 Anti-Fraud Line unit for anti-fraud information exchanged. EC-CERT provides suggestions and procedures to E-Commerce platform about how to improve system security.

3. Events organized / co-organized

3.1. Training

EC-CERT organized three seminars regarding computer system security for E-Commerce Industry in 2014.

3.2. Seminars

EC-CERT organized one seminar E-Commerce Reliable Security Alliance Annual Meeting, inviting security experts to share the information security issues, to assist IT industry enhance security.

4. Conclusion

In order to enhance the security of E-Commerce network transaction, EC-CERT would do more jobs such as E-Commerce industry information security services provider freely. Such as real time alerts, incident monitoring, information exchange, consulting service, personal information prevention. In the future, EC-CERT would like exchange security relative information with other CERT and cost more resource to prevent E-Commerce transaction security work especially security incident investigation and response handling.

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 2014, HKCERT had handled 3,443 security incidents which was 103% increase of the previous year (see Figure 1).

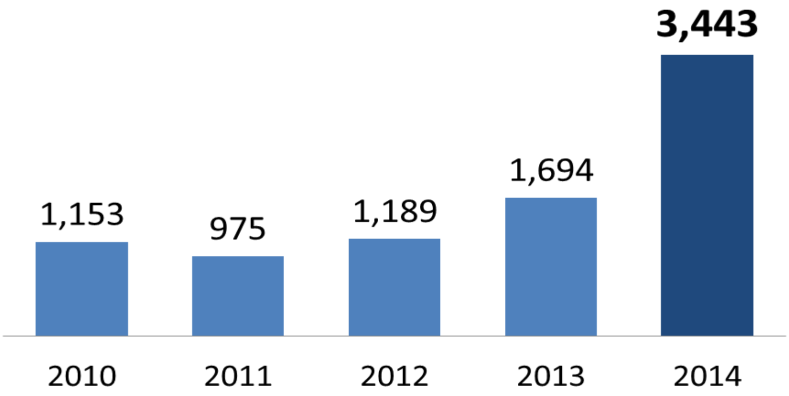


Figure 1. Incident Reports Handled by HKCERT

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 botnet (1,973 cases) which recorded a 357% increase. Next was phishing (594 cases) which recorded a 55% increase (see Figure 2).

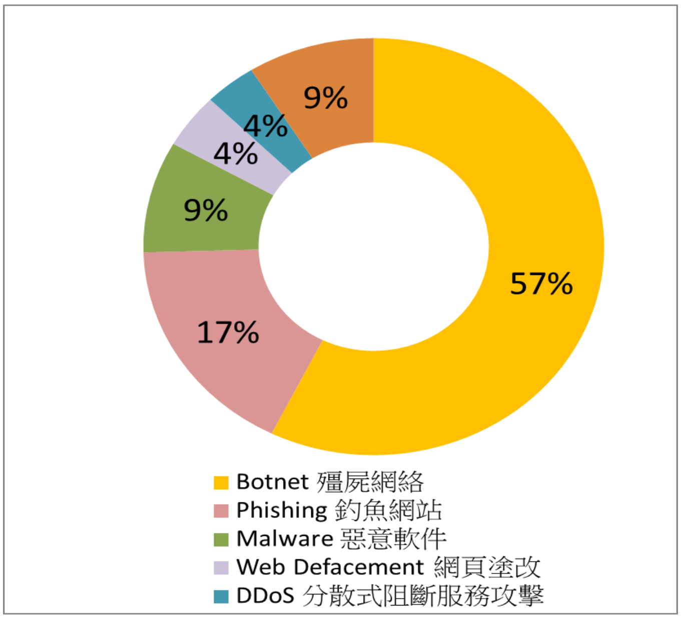


Figure 2. Distribution of Incident Reports in 2014

In the past few years, HKCERT had joined the global botnet takedown operations to fight cross border cyber attacks. During the period, HKCERT has participated in several global botnet take down operations against Citadel, Brobot, ZeroAccess, Zeus, GameoverZeus and Pushdo. The availability of data from overseas organizations like CERTs, security researchers, vendors and the HKCERT's automation and process streamlining allowed the handling of large amount of incidents. The number of botnet incident reports rose sharply in the past three years (see Figure 3). This increase indicated a progress of security status of Hong Kong to dig out and clean up previously "invisible" incidents.

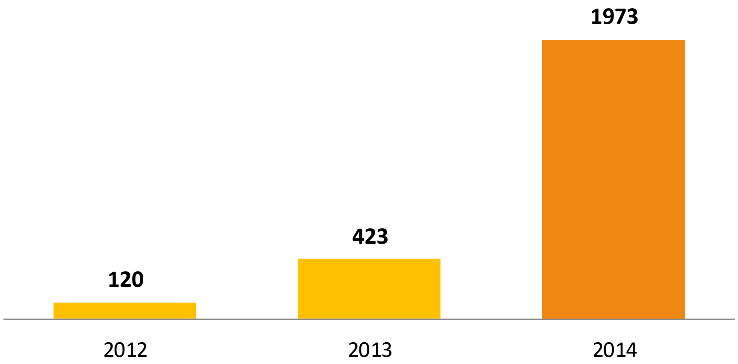


Figure 3. Number of Botnet Incident Reports in the past 3 years

2.1.1. Territory-wide Attack in October 2014

In October 2014, an international hacker group "Anonymous" declared a campaign called Operation Hong Kong (OpHongKong) against Hong Kong websites. It was the most extensive and longest territory-wide cyber attack in the history of Hong Kong, targeting websites of government departments, critical organizations, political organizations, press & media, and some other non-government organizations.

The attackers announced their target websites on social media websites and they openly recruited volunteers to join the attack. They even provide one-click DDoS (distributed denial-of-service) attack tools so that people without technical know-how could participate.

There were mainly 3 types of attacks in the campaign: web defacement, DDoS attack and intrusion of information systems respectively. For DDoS attack, attackers used web application attacks, malformed network protocols, SYN flood, volumetric attacks and Wordpress pingback as the means.

HKCERT worked closely with government information security team and the police to tackle this large scale attacks.

- informing the public of the attacks immediately and advised them how to secure their systems; warning Internet users not to participate in any cyber attacks
- monitored the target sites and exchanging information with government
- handling the incidents of non-government organizations
- informing the targets and advised them the recover actions; informed the hosting companies of the targets to be prepared for the attacks affecting their network
- issuing takedown requests to administrators of servers hosting DDoS attack scripts
- sharing the lesson learnt to the public

According to HKCERT's statistics[1], from 2nd to 22nd October 2014 there were 38 non-government websites defaced and 23 non-government websites attacked by DDoS. All of them had resumed to normal operation on 22nd October, 2014.

[1] Information Security Status Report -- Attacks Targeting Hong Kong (2014-10-22) https://www.hkcert.org/my_url/en/blog/14102201

2.2. Watch and Warning

During the period from January to December of 2014, HKCERT published 348 security bulletins (see Figure 4) on the website. In addition, HKCERT have also published 126 blogs, including security advisories on WinXP end-of-support, ransomware, Heartbleed vulnerability, Shellshock vulnerability, botnet attacks, point of sales malware and DDoS and web attacks of Operation Hong Kong campaign. HKCERT also published the best security reads of the week every week to inform the public of good security articles.

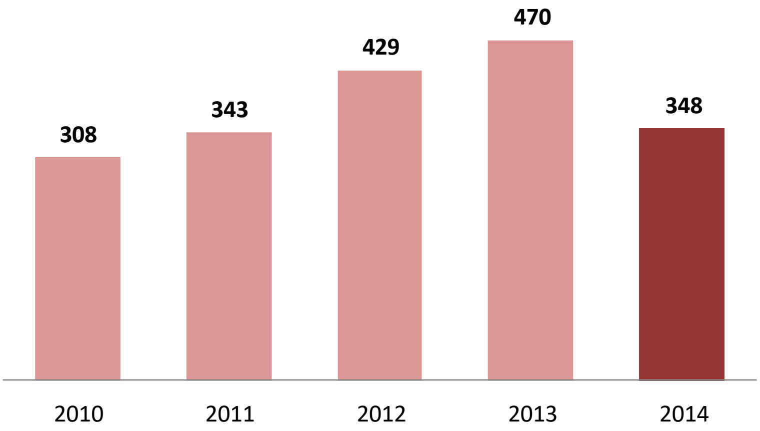


Figure 4. HKCERT Published Security Bulletins

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 decreasing from 9,958 in Q4 2013 to 6,172 in Q4 2014. It reflected the effectiveness of the botnet takedown operation in 2014.

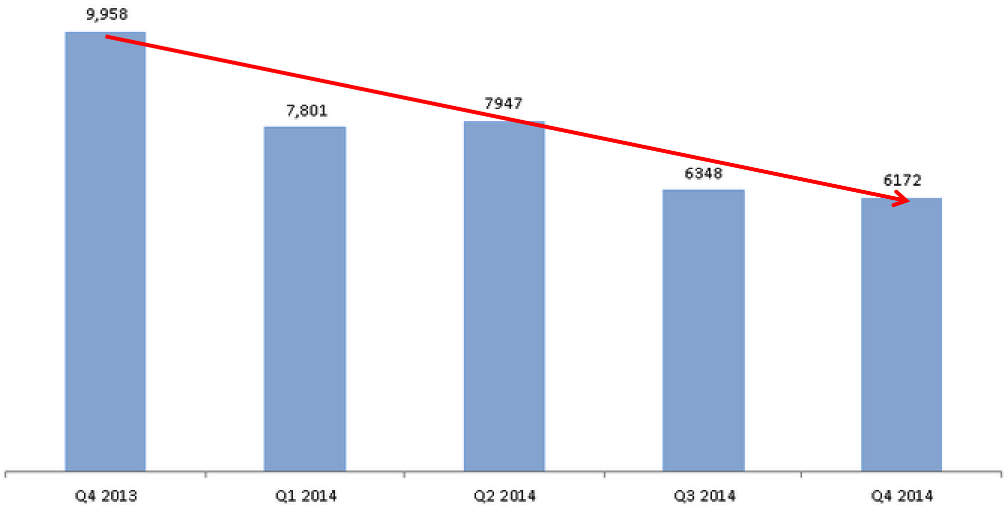


Figure 5. Trend of Bot related security events in the past year

(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.
- 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.
- HKCERT had published 12 issues of monthly e-Newsletter in the period.
- HKCERT had published the statistics of incident reports and security bulletins every quarter.

3. Events organized and co-organized

3.1. Seminars, Conference and Meetings

HKCERT jointly organized the “Build A Secure Cyberspace” campaign with the Government and Hong Kong Police Force. The campaign involved public seminars, a cyber security symposium for ISPs, and a 4-Panel Comic Drawing contest. Four public seminars were organized in February, April, August and November 2014.

We organized the Information Security Summit 2014 with other information security organizations and associations in October 2014, inviting local and international speakers to provide insights and updates to local corporate users.

3.2. Speeches and Presentations

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

3.3. Media promotion, briefings and responses

- HKCERT published two advertorials in November 2014 to promote the public seminar and the comic drawing contest.
- HKCERT published weekly column articles in Hong Kong Economic Times starting June 2014 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 Taipei and delivered talk on IFAS
- Participated in the FIRST AGM and Conference in Boston and jointly with CERT Austria delivered talk on cyber threat intelligence collection and analysis systems; participated in the Annual Meeting for CSIRTs with National Responsibility in Boston and shared in the panel discussion the future of CERTs.
- Participated in the APCERT Drill (February 2014) and acted as member of the Organizing Committee and the Exercise Control team. The theme of the drill this year was "Countering Cyber-ops with Regional Coordination". The drill was a great success with 20 APCERT teams from 16 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.

4.2. Local Collaboration

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

- Continued to work closely with the government 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 2014, HKCERT had worked with ISPs to clean up Citadel, Brobot, ZeroAccess GameoverZeus and Pushdo botnet machines in Hong Kong.

- Co-organized a local drill with HK Police and the Office of Government Chief Information Officer (OGCIO) on 31st October 2014 with players from ISPs and Domain Name registrars in Hong Kong. HKCERT led the preparation of the scenarios and acted as the lead of EXCON of the drill. The drill was a great success.
- 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. Strategy and Service Review

HKCERT had conducted a Strategy and Service Review (undertaken by AusCERT) in October 2013. The report was received by HKCERT and the Hong Kong SAR Government in March 2014.

5.2. CERT Study Tour

HKCERT, jointly with the OGCIO, had visited CERTs and other information security organizations in Australia, China and Japan in June and July of 2014. The mission of this tour was to broaden the horizon on contemporary CERT development and to exchange on the vision of the future of CERTs, so as to help reviewing the strategies of HKCERT. 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.

5.3. Advisory Group Meeting

HKCERT had held the Advisory Meeting in Hong Kong and met with overseas advisors in international meeting venues to solicit inputs from the advisors on the development strategy of HKCERT.

5.4. 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.

5.5. 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.

5.6. Year Ender press briefing

HKCERT organized a year ender press briefing to media in January 2015 to report on information security status of 2014, 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.

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 2015/2016. 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

Year 2014 was a year with big challenges in information security for Hong Kong. Hong Kong had encountered the biggest and longest territory wide attack campaign. HKCERT collaborated with the information security team of OGCIO and the Cyber Security and Technology Crime Bureau (CSTCB) of the Hong Kong Police closely to respond to the attack. This collaborated response mechanism proved to be working in the real life challenge and the communication protocol was further streamlined. The attack had also raised the public awareness on one-click DDoS. More awareness education would be required to follow up.

In 2014, 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 2014, 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, 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 2015.

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

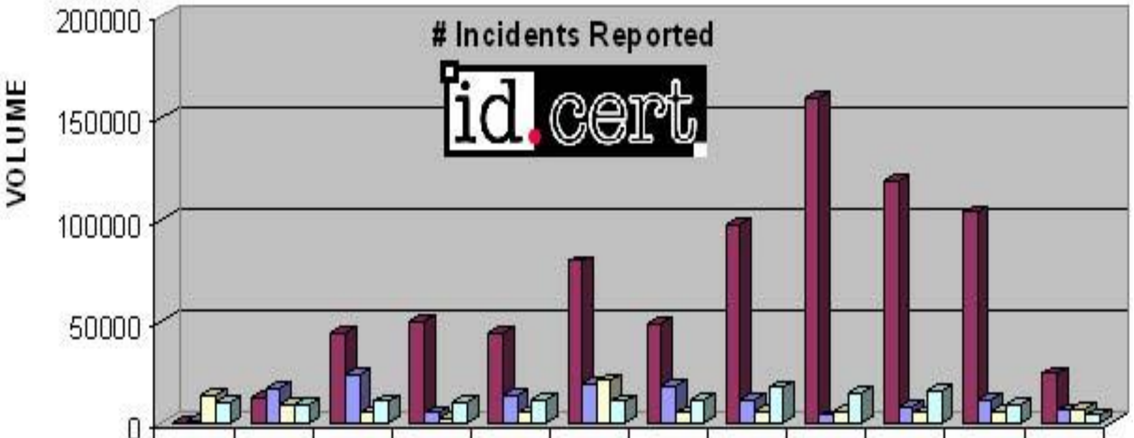
2.1. Incident Handling Report

133.297 reports received in 2014:

- Spam: 64.514 reports (48,4 %)
- Network Incident: 37.071 reports (27,81%)
- Malware 13.426 reports (10,07%)

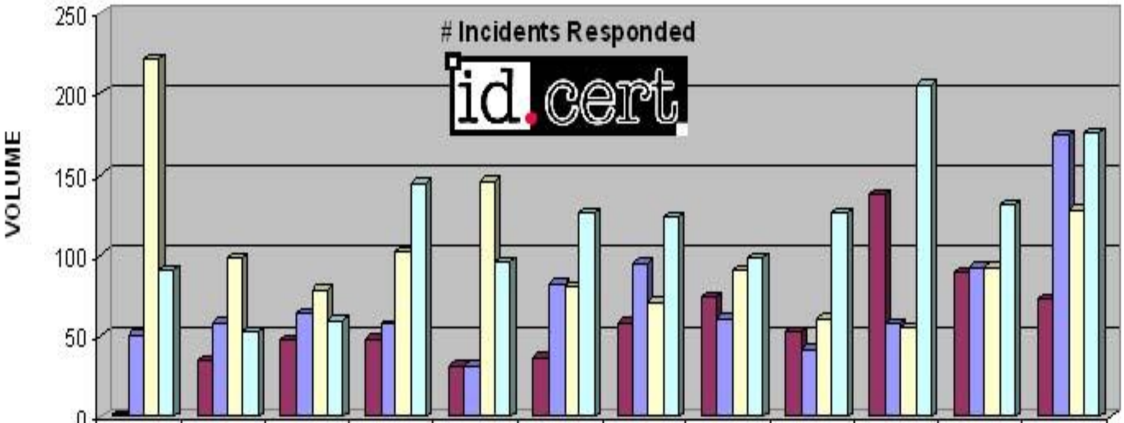
Respond to complaint in 2014 were 1.244 reports.

Incidents reported:



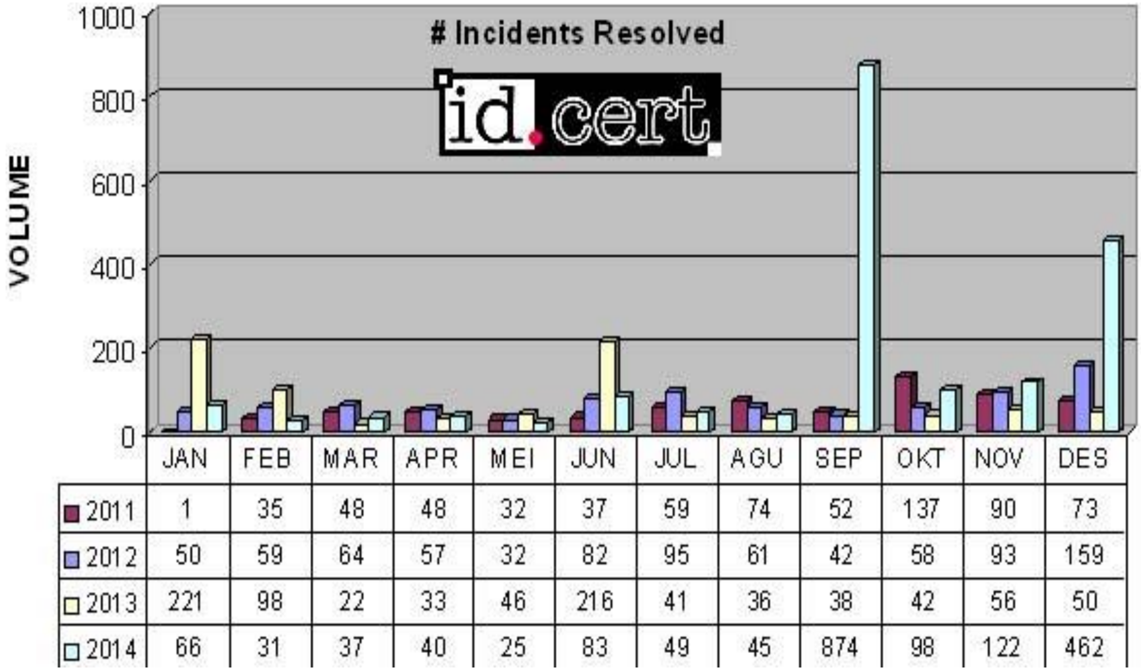
	JAN	FEB	MAR	APR	MEI	JUN	JUL	AGU	SEP	OKT	NOV	DES
■ 2011	1	12849	44707	49294	44281	79449	48287	97228	160455	118788	103916	24201
■ 2012	1382	17276	23423	4913	13670	19779	18166	11777	3661	8442	12164	6963
□ 2013	13788	9478	5211	1853	4947	20941	5927	6611	6369	5558	6224	7128
□ 2014	10.722	9.269	11.260	11.015	11.872	11.239	11.819	17.829	15.109	15.975	10.064	4.115

Incidents responded:

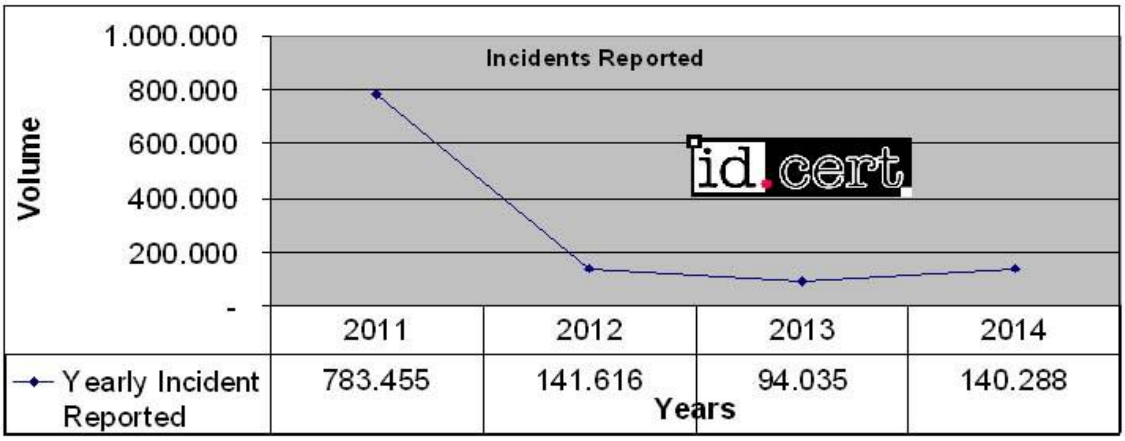


	JAN	FEB	MAR	APR	MEI	JUN	JUL	AGU	SEP	OKT	NOV	DES
■ 2011	1	35	47	48	32	37	59	74	52	137	90	73
■ 2012	50	59	64	57	32	82	95	61	42	58	93	175
□ 2013	221	98	78	102	146	80	71	91	61	55	93	128
□ 2014	91	52	60	145	96	126	124	98	126	206	131	176

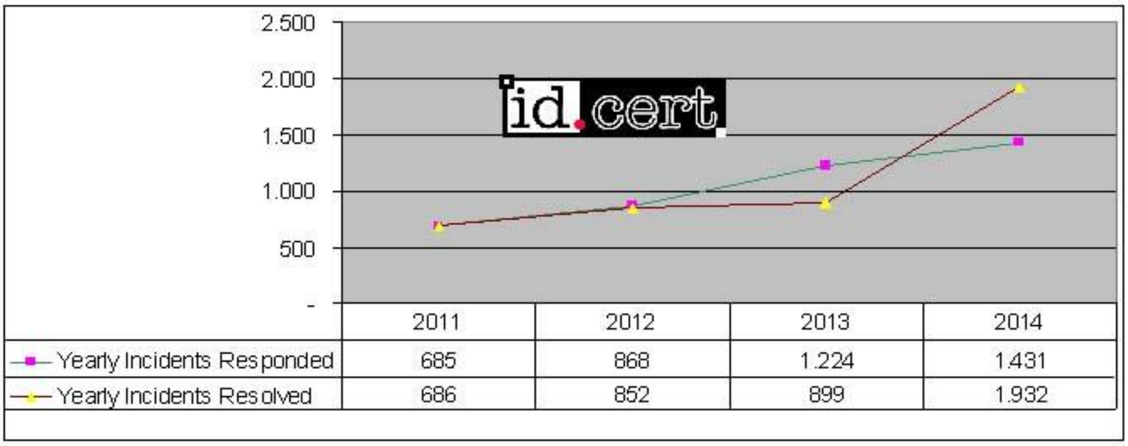
Incidents resolved:



	JAN	FEB	MAR	APR	MEI	JUN	JUL	AGU	SEP	OKT	NOV	DES
■ 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



	2011	2012	2013	2014
Yearly Incident Reported	783.455	141.616	94.035	140.288



	2011	2012	2013	2014
Yearly Incidents Responded	685	868	1.224	1.431
Yearly Incidents Resolved	686	852	899	1.932

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

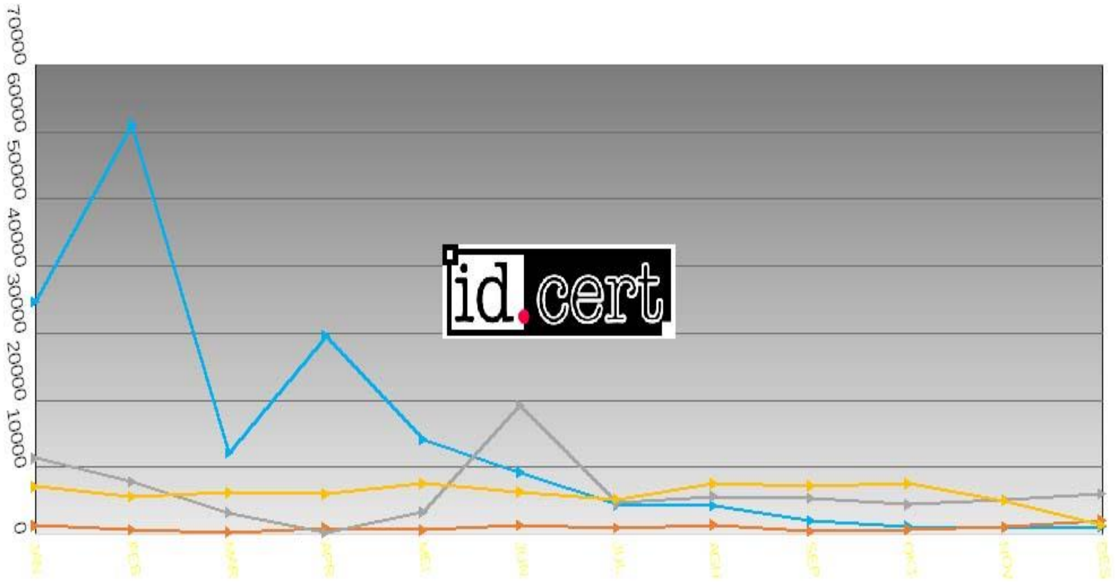
2.2. Abuse Statistic

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.

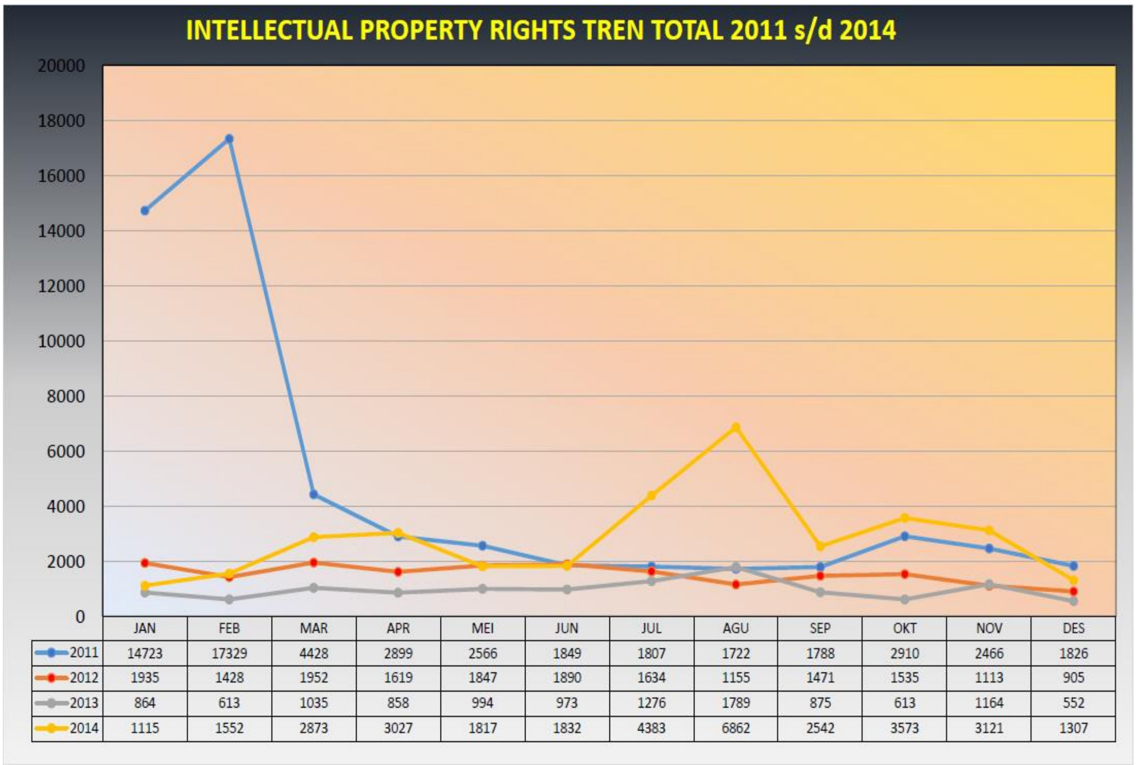
No.	*Complaint Category*	*Rating (%)*
1	Spam	51,78
2	Intellectual Property Right	24,14

3	Spam complaint	6,74
4	Network Incident (Deface, DdoS attack, etc)	6,61
5	Spoofing/Phishing	4,67
6	Malware	4,57
7	Complaint respond	1,49

Spam:

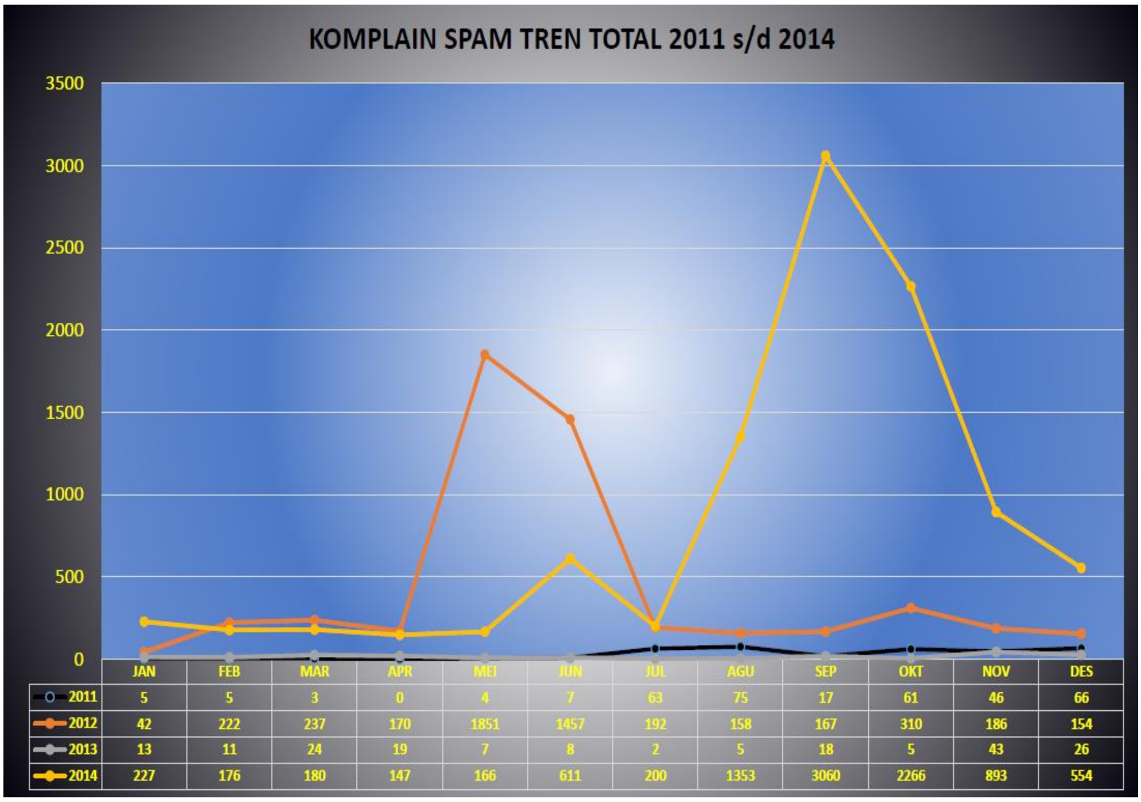


Intellectual Property Rights:



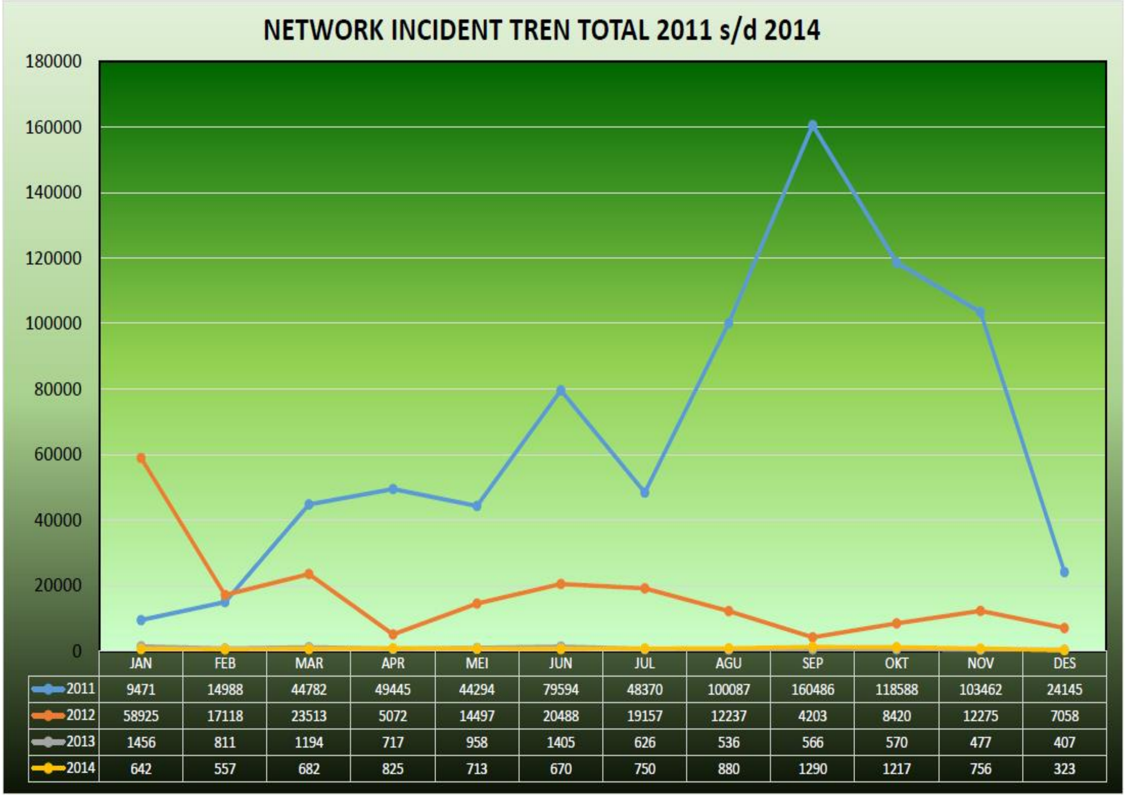
	JAN	FEB	MAR	APR	MEI	JUN	JUL	AGU	SEP	OKT	NOV	DES
2011	14723	17329	4428	2899	2566	1849	1807	1722	1788	2910	2466	1826
2012	1935	1428	1952	1619	1847	1890	1634	1155	1471	1535	1113	905
2013	864	613	1035	858	994	973	1276	1789	875	613	1164	552
2014	1115	1552	2873	3027	1817	1832	4383	6862	2542	3573	3121	1307

Spam complaint:



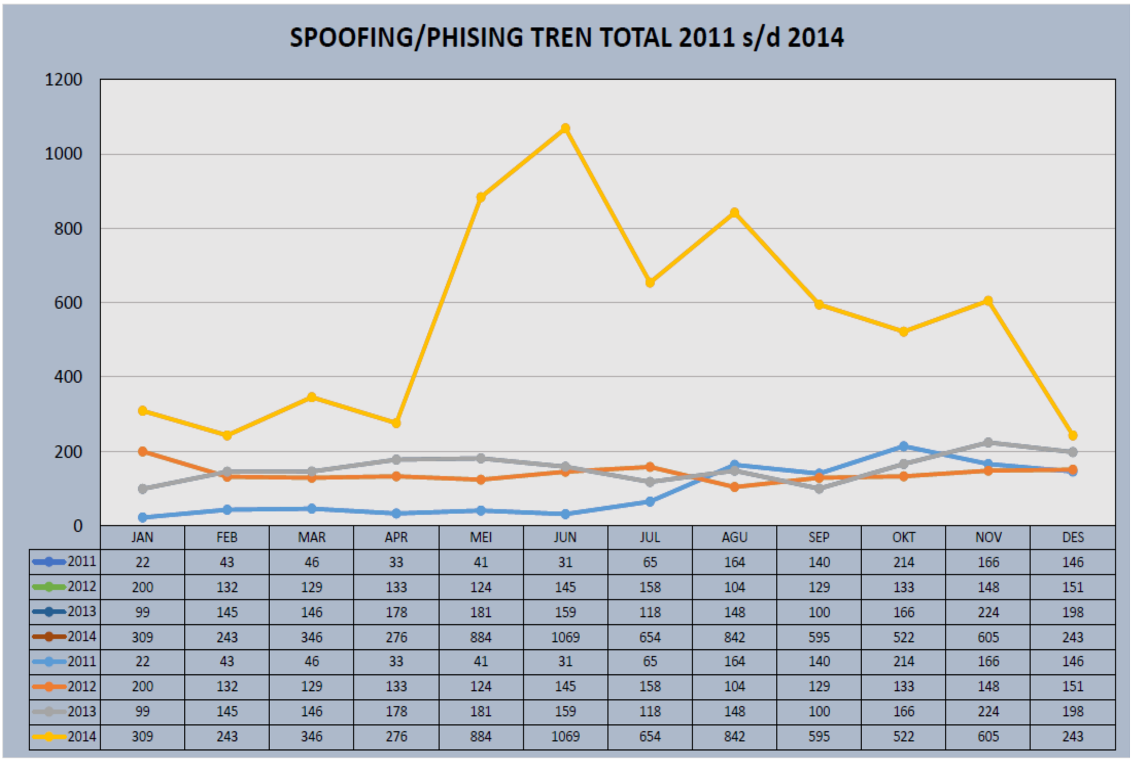
	JAN	FEB	MAR	APR	MEI	JUN	JUL	AGU	SEP	OKT	NOV	DES
2011	5	5	3	0	4	7	63	75	17	61	46	66
2012	42	222	237	170	1851	1457	192	158	167	310	186	154
2013	13	11	24	19	7	8	2	5	18	5	43	26
2014	227	176	180	147	166	611	200	1353	3060	2266	893	554

Network Incidents:



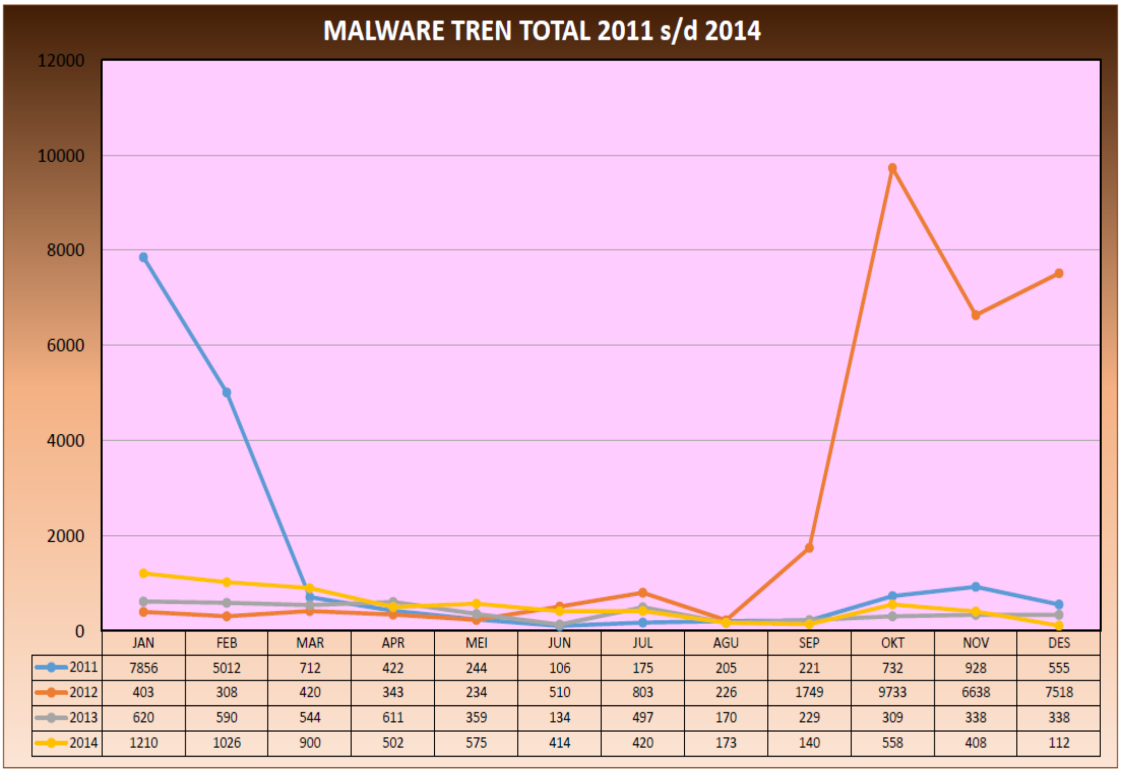
	JAN	FEB	MAR	APR	MEI	JUN	JUL	AGU	SEP	OKT	NOV	DES
2011	9471	14988	44782	49445	44294	79594	48370	100087	160486	118588	103462	24145
2012	58925	17118	23513	5072	14497	20488	19157	12237	4203	8420	12275	7058
2013	1456	811	1194	717	958	1405	626	536	566	570	477	407
2014	642	557	682	825	713	670	750	880	1290	1217	756	323

Spoofing/Phishing:



	JAN	FEB	MAR	APR	MEI	JUN	JUL	AGU	SEP	OKT	NOV	DES
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
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

Malware:



	JAN	FEB	MAR	APR	MEI	JUN	JUL	AGU	SEP	OKT	NOV	DES
2011	7856	5012	712	422	244	106	175	205	221	732	928	555
2012	403	308	420	343	234	510	803	226	1749	9733	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

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

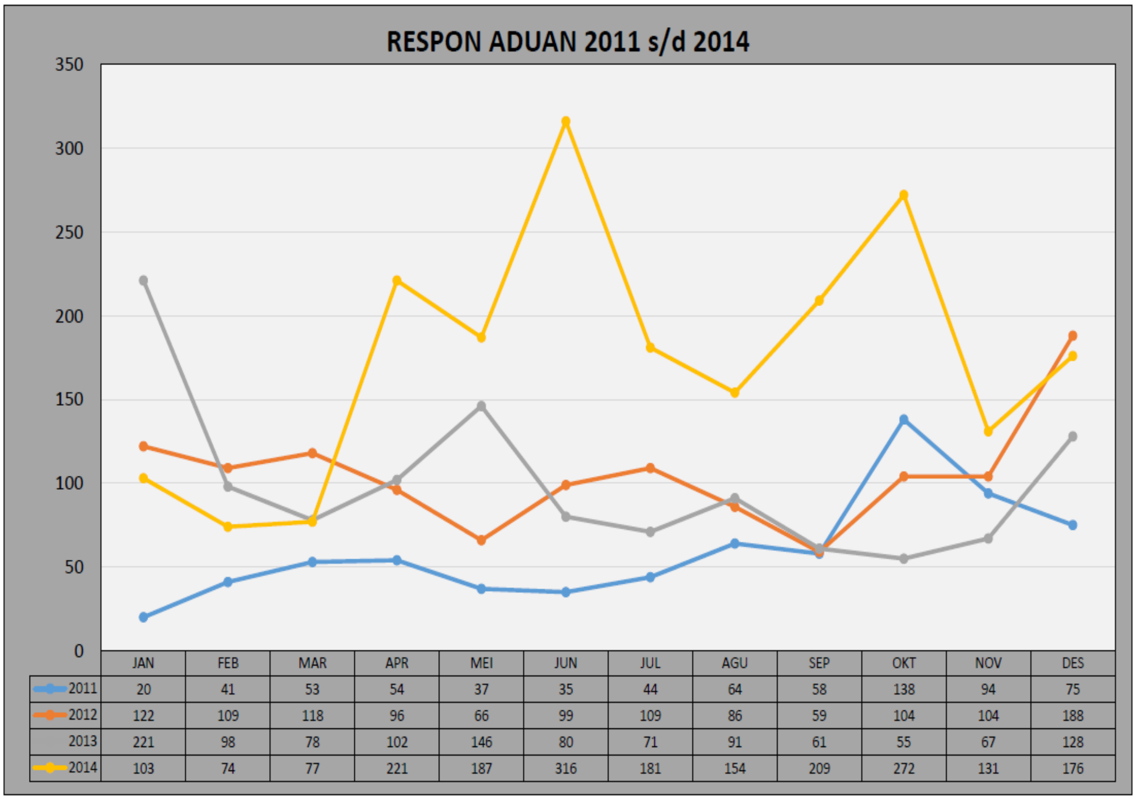
http://clg.utxao.bengk*****.go.id/

http://ebu.mhatr.bengk*****.go.id/

http://xjs.mhatr.bengk*****go.id/

http://loadp.bengk*****.go.id/

Complaint respond:



	JAN	FEB	MAR	APR	MEI	JUN	JUL	AGU	SEP	OKT	NOV	DES
2011	20	41	53	54	37	35	44	64	58	138	94	75
2012	122	109	118	96	66	99	109	86	59	104	104	188
2013	221	98	78	102	146	80	71	91	61	55	67	128
2014	103	74	77	221	187	316	181	154	209	272	131	176

Potential Loss and Current Loss of Fraud reported in Indonesia:

- Total loss January - March 2014: USD4.832,00 and Rp2.250.000,00
- 3 countries complained their citizen as victim: Saudi, Singapore, and France.
- Item bought: wood, birth control devices which not standard and not in accordance with the agreement, bicycle, villa/house rent.
- Communication media:
  - Via email

- proceeded bank transfer
- hijack company email account

2.3. New Service

Since March 2014, ID-CERT gives daily feed to DIKBUD (Education and Cultural Ministry) of cyber incident.

2.4. Etc

ID-CERT has issued 2 Security Alerts in 2014:

OpenSSL Heartbleed

http://www.cert.or.id/index-berita/id/berita/47/

At April 13, 2014, ID-CERT received information from a valid source of vulnerabilities that exist in the version of OpenSSL 1.0.1 to 1.0.1f which can reveal the user's sensitive information to the attacker.

The impact of this vulnerability is a remote, unauthenticated attacker may be able to take sensitive information, such as secret keys. By using sensitive information, an attacker may be able to decrypt, spoof, or perform man-in-the-middle attack on the network traffic that would otherwise be protected by the OpenSSL.

solution:

- applying updates
- Disable support for OpenSSL heartbeat
- Another recommendation is to recompile OpenSSL with DOPENSSL_NO_HEARTBEATS falg.

Bash

http://www.cert.or.id/index-berita/id/berita/50/

Product:	Bash
Publisher:	SUSE
Operating System:	SUSE
Impact/Access:	execute code / remote commands / unauthenticated / Unauthorized Access - from an existing account
Solution:	Patch / upgrade

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.

3.2. Drill

February 19, 2014:

ID-CERT participated in APCERT Drill as Organizing Committee.

3.3. Seminar & Etc

February 11, 2014:

ID-CERT was invited by KEMDAG (Ministry of Trade) to coordinate about Online Trading Fraud

February 26, 2014:

APCERT Day in APRICOT, Kuala Lumpur, ID-CERT participated as committee in facilitating the activity.

February 26, 2014:

ID-CERT was invited by APNIC to share knowledge and speak at Network Abuse BoF session.

March 11-13, 2014:

ID-CERT was one of speakers at Cyber Intelligence Asia, Singapore.

March 18-21, 2014:

ID-CERT attended APCERT Annual General Meeting & Conference in Taipei.

April 16, 2014:

ID-CERT was invited by PUSTEKKOM DIKBUD to share ID-CERT experience in Cyber Security.

April 21, 2014:

ID-CERT Annual Gathering VI at IDC, Baros-Cimahi, Bandung.

May 12-14, 2014:

ID-CERT spoke at BIMTEK LAN KEMDIKBUD in Bandung

June 13, 2014:

ID-CERT was one of the speakers at Seminar of Indonesia IT Security Trend in Education Sector in Jakarta

August 17, 2014:

ID-CERT was invited by PANDI in an event of domain .ID launching at Grand Indonesia, Jakarta

August 20, 2014:

ID-CERT was invited by National Indonesia Internet Governance Forum (ID-IGF) Dialogue 2014 as panelist in Jakarta.

August 25, 2014:

ID-CERT was invited by Direktorat Keamanan Informasi KOMINFO to discuss about Team of Information Security Incident Handling in Jakarta

October 15, 2014:

ID-CERT was invited by KOMINFO to be the speaker at Seminar of Information Security in Padang

November 1, 2014:

ID-CERT was invited by CISSReC to attend Seminar "MENGGAGAS KONSEP KEAMANAN SISTEM INFORMASI DAN KOMUNIKASI DI ERA PEMERINTAHAN JOKOWI", in Jakarta

November 5, 2014:

ID-CERT was invited by ID-SIRTII to attend National Security Day in Bandung.

November 27, 2014:

ID-CERT was invited by Australian Federal Police to be the speaker at "*Advanced Cyber Crime Investigations Workshop"* at JCLEC, Semarang.

November 27, 2014:

ID-CERT was invited by PANDI to attend Seminar of Domain .ID for the World in Jakarta

December 2, 2014:

ID-CERT was invited by Direktorat Keamanan Informasi KOMINFO to attend launching of Root CA Indonesia

December 11, 2014:

ID-CERT was invited by ID-SIRTII to attend *"Building Critical Information Infrastructure Protection (CIIP): Lessons Learned and Challenges"* in Jakarta.

December 18, 2014:

ID-CERT was invited by APJII to attend IDNIC OPM and meet ICANN representative.

December 22, 2014:

ID-CERT had a meeting with Pemkab Berau to discuss the possibility of cooperation in 2015

4. Achievement

4.1. Presentation

ID-CERT presentation at Network Abuse – APNIC BoF APRICOT, Februari 26, 2014:
http://www.cert.or.id/media/files/IMR-ID-CERT-APNIC-26022014.pdf

ID-CERT presentation at Cyber Intelligence Asia, Singapore, March 11, 2014:
http://www.cert.or.id/media/files/cyberintelligence_Indonesia_presented.pdf

ID-CERT presentation at Network Abuse – APNIC BoF, September 16, 2014:
http://www.cert.or.id/media/files/ID-CERT-2014-Half-Year.pdf

Trend of Information Security – ID-CERT 2014, October 15, 2014
http://www.cert.or.id/media/files/ID-CERT-15102014.pdf

5. International Collaboration

December 9, 2014:

ID-CERT had a meeting with ICANN at Jakarta to discuss Program Collaboration between Indonesia – ICANN.

6. Future Plan

6.1. Future Project

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

6.2. Framework

Future Operation

- Incident Handling
- IMR respondent addition
- Internal infrastructure improvement/development
- Antispam RBL

- ID-CERT Annual Gathering VIII
- Training

7. 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.

ID-SIRTII/CC

Indonesia Security Incident Response Team of Internet Infrastructure Coordination Center – Indonesia

1. About ID-SIRTII/CC

1.1. Introduction

ID-SIRTII/CC is the national CSIRT/CC of Indonesia. The purpose of Id-SIRTII is to coordinate security efforts and incident response for critical infrastructure and IT-security problems on a national level in Indonesia.

1.2. Establishment

ID-SIRTII/CC was established in 2006 by ICT Minister Decree Number 27/2006 and 26/2007 then revised with 16/2010.The main role of ID-SIRTII) is to conduct security surveillance of telecommunication network based on internet protocol in Indonesia, and also as a central coordination (Coordination Center/CC) and liaison (Single Point of Contact) with related agencies/institutions both in domestic and overseas.

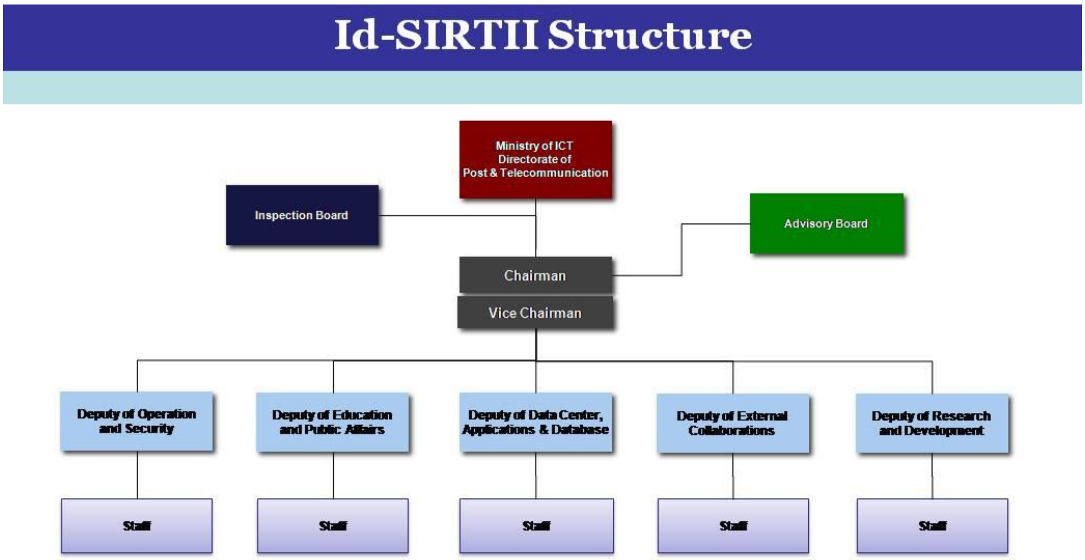
ID-SIRTII as a legal institution which has been granted the right and authority to conduct Internet traffic monitoring in Indonesia refers to the rule of law as follows below:

- Act No.36/1999 regarding National Telecommunication Industry
- Government Regulation No.52/2000 regarding Telecommunication Practices
- Ministry of Communication and Information Technology Regulation No.27/PER/M.KOMINFO/9/2006 regarding Telecommunication Network Management Security based on internet protocol
- Ministerial Regulation No.26/PER/M.KOMINFO/2007 regarding Indonesian Security Incident Response Team on Internet Infrastructure

On 2010, ID-SIRTII became a full member of APCERT. On 2011 became a member of FIRST and also National CSIRT Forum. On 2009 became a full member of OIC-CERT.

1.3. Management and Staffs

ID-SIRTII/CC now has 6 member Board of Directors, which is 1 Chairman and 5 deputies (Vice Chairman), and for supporting daily operations we employ 35 staffs in our office at Jakarta the Capital City of Indonesia.


Id-SIRTII Structure
Ministry of ICT
Directorate of
Post & Telecommunication
Inspection Board
Advisory Board
Chairman
Vice Chairman
Deputy of Operation and Security
Deputy of Education and Public Affairs
Deputy of Data Center, Applications & Database
Deputy of External Collaborations
Deputy of Research and Development
Staff
Staff
Staff
Staff
Staff

1.4. Constituencies and Stakeholders

- IT security teams (public sectors)
- Internet Service Provider (ISP)
- Network Access Provider (NAP)
- Local Internet Exchange Operator
- Law Enforcement Agency (LEA)
- Critical Infrastructure Operators
- Other Sectors CSIRT's in Indonesia.

1.5. Main activities:

- Monitoring, detection and early warning of threats and disturbance of the telecommunications network of IP-based in Indonesia
- Developing and / or providing, operating, and maintaining the database system of monitoring and conducting security activities of the telecommunications network utilization of IP-based at least for monitoring, early detection and early warning of threats and disturbance to the telecommunications network

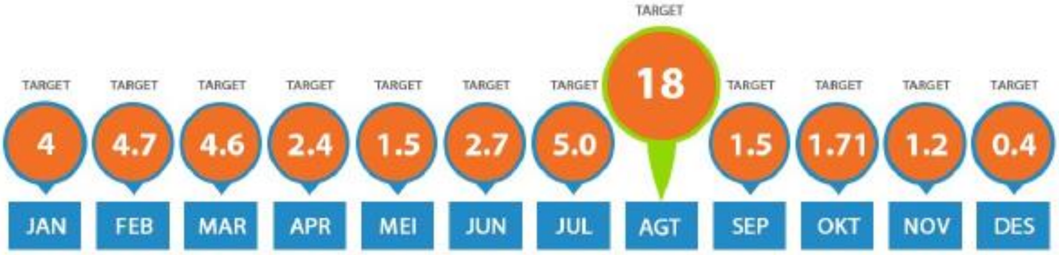
utilization of IP-based, keeping records of transactions (log files) for supporting the law enforcement process

- Performing the functions of information services to the threats and security disturbance of the telecommunications network utilization of IP-based
- Carrying out research and development activities, providing simulation lab and training activities of the telecommunications network utilization security of IP-based
- Providing consultancy services and technical assistance to strategic institutions/agencies
- As a central coordination (Coordination Center/CC) and liaison (Single Point of Contact) with related agencies/institutions both in the country and abroad.

2. Activities and Operation

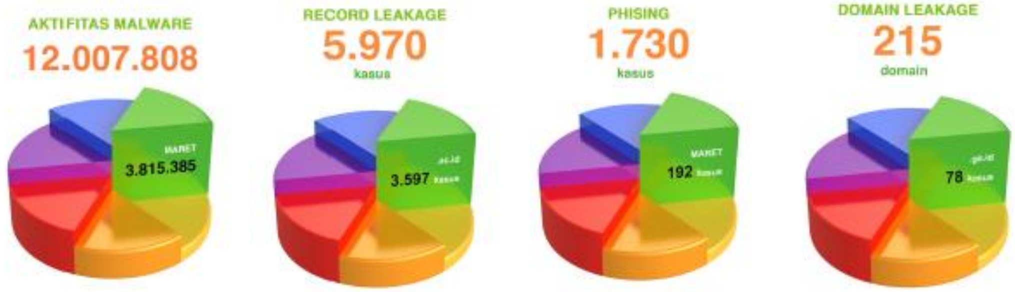
2.1. Incident Reports and Statistics

We provide Incident Reporting Service for public in final year 2014. We only authorized to address all types of computer security incidents, which occur, or threaten may occur in our Constituency and which require cross-organizational coordination. The level of support given will vary depending on the type and severity of the incident or issue, the type of constituent, the size of the user community affected, and the availability of Id-SIRTII`s resources at the time. Special attention will be given to issues affecting critical infrastructure. No direct support will be given to end users they are expected to contact their system administrator, network administrator, or department head for assistance. We committed to keep our constituency informed of potential vulnerabilities, and where possible, will inform this community of such vulnerabilities before they are actively exploited. The statistic during 2014 is shown as follow:



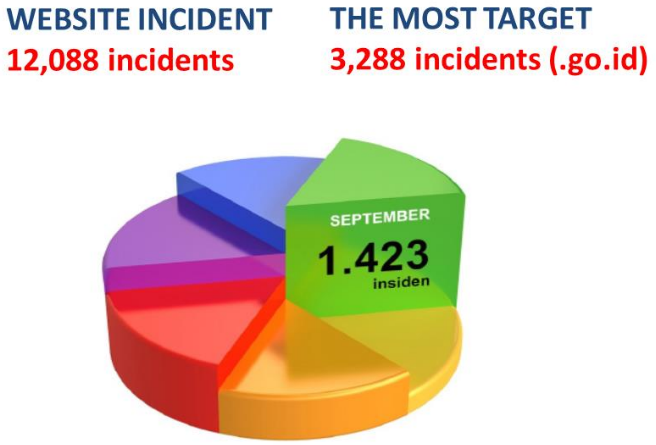
The figure above shows internet traffic monitoring result conducted by ID-SIRTII Monitoring division between January and December 2014, there are 48.8 million incidents reported. The graphic shows that there is a dramatically increased on August 2014 (18 million incidents), this escalation of incident allegedly associated with the several national issues against other countries.

The following figures also shows that during 2014, the biggest number of cases are related with the Malware Activities (more than 12 millions cases), followed by Record Leakage (almost 6 thousand cases), Phising (1.7 thousand cases) and Domain Leakage (215 cases).



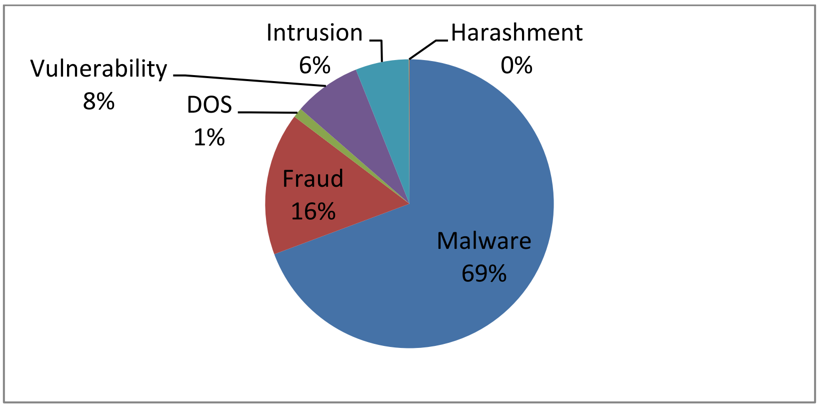
Web Defacement

Id-SIRTII/CC also conducted an intensive monitoring on critical websites especially the government institutions. During year 2014, there are 2,088 website incidents in total. Government websites (go.id) dominated the number of web defacement case (3,288 cases) especially on September with 1,423 cases which is shown on the following graph:



Public Report

Public could send internet incident report via email to incident@idsirtii.or.id or by accessing online ticketing system (OTRS system). Between January – December 2014, ID-SIRTII/CC received 1,533 incident reports. The biggest number of incident reported is related to Malware attack (69%) followed by Fraud, Vulnerability, Intrusion, and DOS. The following table is summary of public incident reports categorized by Incident Classification:



Number Report Percentage based on Incident Classification

APCERT-Team Report

ID-SIRTII also accepts incident report from APCERT-team. During 2014, ID-SIRTII accepts List of Bot infected IPs in Indonesia from APCERT-team. Most of APCERT-team report is categorized into malware classification. Based on the classification report, ID-SIRTII is conducting coordination with ISP, hosting company, website owner and other related stakeholders. There are three types of coordination result,

- Positive response, stakeholder confirmed and take necessary actions such as IP Blocking or refine their infrastructure;
- Negative response, stakeholder can be contacted but without follow-up action;
- Unreachable stakeholder, stakeholder has no valid contact or unreachable.

All incoming incident reports are managed in online integrated ticketing system named OTRS system.

2.2. Establishing and Supporting Sector based CSIRTs

As the cleaning cyber environment needs more strategic partnership with other institutions we have establishing sector based CSIRT such as Academic CSIRT, Gov-CSIRT (including some Local-Gov CSIRTs). In 2014, sector CSIRT which are successfully established are: West Java Province CSIRT (Local Gov-CSIRT located in Bandung) and Defence CSIRT (under Ministry of Defence). Now APJII-CSIRT (ISPs association) and Central Java Province (Local Gov-CSIRT located in Yogyakarta) is still under preparation.

3. Event Organized/Co-OrganizedAchievement

3.1. International Membership

- FIRST, Full Member (since 2011)
- National CSIRT Forum (since 2010)
- APCERT, Full Member (since 2010) and Steering Committee (2012-2013)
- OIC-CERT, Full Member (2009) and Steering Committee (2013-2014)

3.2. Community Cooperation

Research and Development Project with APTIKOM – Academic CERT, National Honey Net, NAWALA Foundation, ID-X. Special Program with EC-COUNCIL, University Indonesia, CIO Community, Indonesia CISO Forum, APJII (ISPs Association), AOSI (Association of Indonesia Open Source), FTII (Federation of Indonesia Information Technology)

3.3. Organizing Conference and Workshop/Training

- Security Awareness and Workshop Road Show in 5 major cities within the country and +20 seminars invitation.
- International Cyber Security Research Seminar and Technical Workshop in Bandung
- Critical Information Infrastructure Protection Seminar in Jakarta (in cooperation with JICA and JP-CERT/CC)
- National Internet Security Day (NISD) in Bandung

- National Drill Test and Amazing Trace in Jakarta with almost 100 participants from various sectors such as government, banking, law enforcement, ISPs and communities.
- A number of national seminar and workshop, such as: Incident Handling, Creating & Managing CSIRT and Forensics.
- Conducting National Cyber Defence Competition (CDC) and Cyber Jawara 2014 which consist of CND, Pentest, CTF and Forensics.

4. International Event and Cooperation (among others)

- AOTS/HIDA Training 2014, Tokyo – Japan
- APCERT AGM 2014, Taiwan
- FIRST AGM 2014, in Boston – United States
- OIC-CERT AGM 2014, in Brunei
- ASEAN-Japan Information Security Meeting 2014, Singapore
- Information Security Workshop (organized by JICA), in Tokyo
- ASEAN CERTs Incident Drill (ACID) 2014
- APCERT Drill Test 2014 as a ExCon and Participant
- TRANSIT II Workshop in Utrecht, Netherland

5. Future Plans

- Improving the system for Public Incident Reporting Service
- Increasing Research and Development Cooperation
- Increasing technical trainings and awareness program
- Supporting the establishment of new sectors CSIRT
- Assisting LEA to overcome the growth of cyber crimes
- Suggestions for improvement of regulations and future cyber legislation
- Providing technical support and assistance for security implementation in the critical infrastructure sectors.

6. Conclusion

Currently there was no large-scale network security incident happened with mass damage, but it is very important to increase attention level to issues affecting critical infrastructure. Thus, it is necessary for government, ISPs, Societies, Internet users, to pay much more attention and cooperate with one another more effectively. Id-SIRTII/CC is also in need of increasing the number of collaboration with CERTs community from all over the world to prevent and mitigate the impact of any cyber threat.

JPCERT/CC

Japan Computer Emergency Response Team / Coordination Center – Japan

1. About JPCERT/CC

1.1. 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, 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.

1.2. Constituency

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

2. Activities & Operations

2.1. Incident Handling Reports

In 2014, JPCERT/CC received 19,464 computer security incident reports from Japan and overseas.

	1st Qtr	2nd Qtr	3rd Qtr	4th Qtr	Total
Incident Reports	4,898	4,072	5,430	5,064	**19,464**

Figure 1. Incident reports to JPCERT/CC (2014)

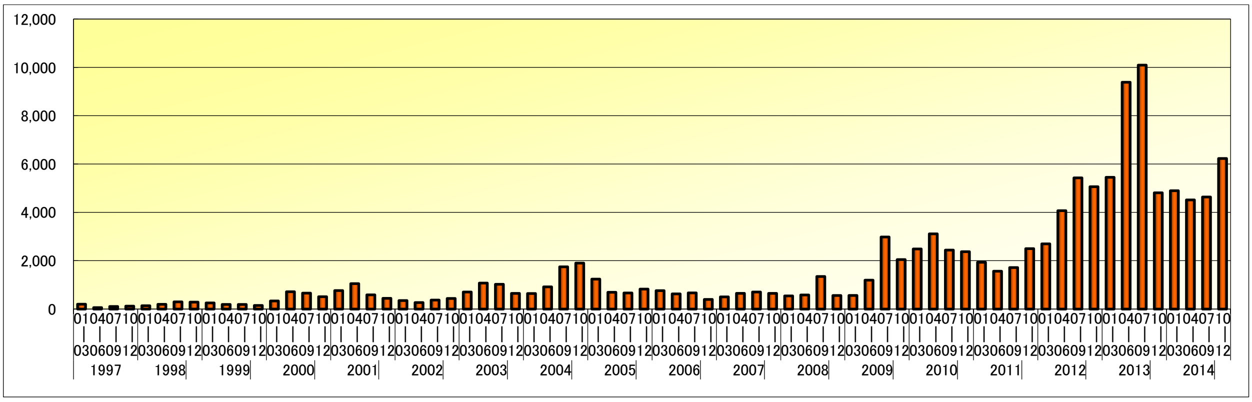


Figure 2. Incident reports to JPCERT/CC (1997-2014)

2.2. Abuse statistics

The incident reports to JPCERT/CC in 2014 were categorized as in Figure 3. About 47% of the incident reports were on scan, followed by website defacement and phishing.

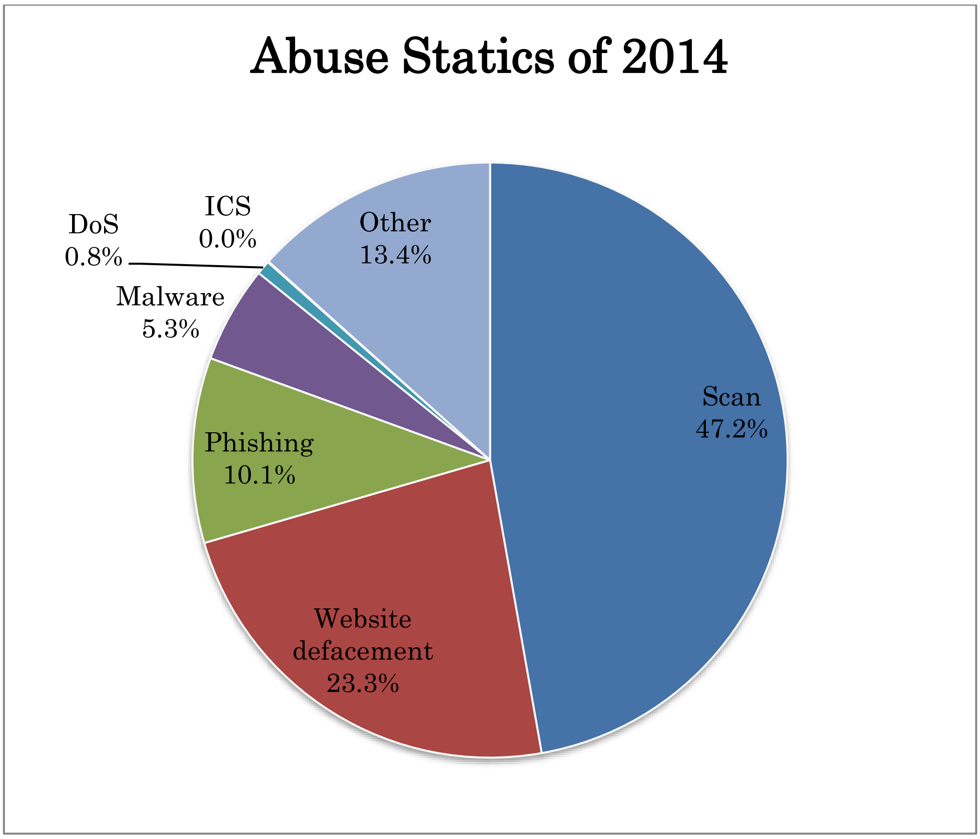


Figure 3. Abuse Statistics of 2014

2.3. 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 2014, 70 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/), CPNI (https://www.cpni.gov.uk/) and NCSC-FI (https://www.ncsc.fi/).
  In 2014, 301 vulnerabilities coordinated by JPCERT/CC were published on JVN. 140 were cases published through the Information Security Early Warning Partnership, and 161 were published through partnerships with overseas coordination centers or vendors.
  Of the 140 published through the Information Security Early Warning Partnership, 111 were reported to IPA by researchers, security vendors, etc. 28 were reported by developers against software they develop, and 1 was reported directly to JPCERT/CC by an overseas researcher.
  Of the 161 published through global partnerships, 136 were reported and published by CERT/CC, 2 by NCSC-FI, 4 by ICS-CERT and 16 were reported

by developers against software they develop. In addition, there were 3 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.

- **JPCERT/CC on Twitter**

  https://twitter.com/jpcert (Japanese)
  https://twitter.com/jpcert_en (English)
  Since January 2009, JPCERT/CC has been providing information security related alerts via Twitter.

- **JPCERT/CC Official Blog**

  http://blog.jpcert.or.jp/ (English)
  Since September 2010, JPCERT/CC has been providing security news related to Japan as well as activities happening at JPCERT/CC on its English blog. In 2014, 18 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. Since August 2014, its English versions are also available.

2.4. Industrial Control System Security

Since 2008, JPCERT/CC has been working on awareness-raising of the industrial control system (ICS) security in Japan. In January 2013, we extended our services on incident handling to ICS area. We have provided presentations at some seminars and support in cyber incident exercise to engineers of Japanese asset owners. We have also released an ICS security assessment tool “J-CLICS”, developed in collaboration with some experts from ICS vendors and asset owners.

2.5. 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.

2.6. Education / Public Awareness

- **Secure Coding**

  JPCERT/CC provides secure coding seminars on C/C++, Java and Android.

- **HTML 5 Security Report**

  In 2014, JPCERT/CC compiled a report entitled "Investigation Report Regarding Security Issues of Web Applications Using HTML5" to provide organized material which could serve as a basis for technical documentation and guideline for secure web application development using HTML5.
  https://www.jpcert.or.jp/english/pub/sr/html5.html

- **Open DNS Resolver Check Site**

  http://www.openresolver.jp/ (Japanese)
  http://www.openresolver.jp/en/ (English)
  JPCERT/CC released the “Open DNS Resolver Check Site” on 31 October, 2013. This web-based tool allows visitors to check whether the DNS server configured on their PC and/or network device connecting to the site is running as an open DNS resolver or not.

2.7. TSUBAME (Internet Threat Monitoring Data Sharing Project)

The TSUBAME project is designed to collect, share and analyze Internet traffic data, in order to better understand the Internet threats 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 in the Asia Pacific region. TSUBAME Working Group is active in APCERT and observation results are exchanged among the teams.

2.8. Associations, Projects 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 Chair 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.

3. Events

3.1. Trainings, Seminars and Workshops

JPCERT/CC offers trainings, seminars and workshops for technical staffs, system administrators, network managers, etc. Some of the events organized and/or supported by JPCERT/CC in 2014 are as follows:

On-site Training/Seminar	-TSUBAME Network Monitoring Workshop (March) -TSUBAME Training in Laos, Sri Lanka (May, September) -C/C++ Secure Coding Seminar in India (September) -Incident Handling, Network Forensics Training for MNCERT/CC (September) -CSIRT Training Course for AfricaCERT (May, November)
Domestic Seminars/Conference	-Control System Security Conference (February) …and many more

3.2. Dispatch of Experts and Speakers

JPCERT/CC dispatches experts and speakers abroad. Below are the events where our experts were dispatched.

Dispatch of Experts	-IT Security Inoculation in Thailand (March) -Malware Analysis Competition in Thailand (October)
Dispatch of Speakers	-CODE BLUE (February, December) -ASEAN Regional Forum (March) -CNCERT Conference (May) -26th Annual FIRST Conference (June) -Internet Governance Forum 2014 (September) -CERT-RO Annual Conference (November) -Security Day 2014 (November)…and many more

3.3. Participation to International Events

Below are some of the international events that JPCERT/CC joined in 2014:

APRICOT 2014 (February)
RSA Conference US 2014 (February)
APCERT AGM and Conference 2014 (March)
NCSC-NL Conference (June)
26th Annual FIRST Conference Boston (June)
National CSIRT Meeting (June)
2014 APISC Security Training Course (July)
Black Hat USA 2014 (August)
DEFCON 22 Hacking Conference (August)
23rd USENIX Security Symposium (August)
The Second China-Japan-Korea CSIRT Annual Meeting for Cybersecurity Incident Response (August)
The Internet Governance Forum 2014 (September)
OWASP AppSec USA 2014 (September)
APWG eCrime Research Symposium 2014 (September)
ICSJWG 2014 Fall Meeting (October)
Hack in the Box 2014 (October)
OIC-CERT Annual Conference 2014 (October)
OECD Working Party on Security Privacy in the Digital Economy (November)
Safe Cities 2014 (December)
ISO/IEC SC 27 WG 4 Meeting (October/December)

…and many more

3.4. Drills

JPCERT/CC participated in the following drills in 2014 to test our incident response capability:

- APCERT Drill 2014 (19 February)
- ASEAN CERT Incident Drill (ACID) 2014 (24 September)

4. MoU

To further strengthen cooperation, JPCERT/CC has been signing a Memorandum of Understanding (MoU) with various security organizations.

5. International Contribution

- **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.

- **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:
  ISO/IEC 29147: "Vulnerability Disclosure"
  ISO/IEC 27035 Part 1: Principles of incident management
  ISO/IEC 27035 Part 2: Guidelines to plan and prepare for incident response
  ISO/IEC 27035 Part 3: Guidelines for incident response operations
  ISO/IEC 30111: "Vulnerability Handling Processes"

- **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. Beginning in March 2011,

JPCERT/CC has been serving 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.

- **Cyber Green Initiative**

  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.

6. 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. About KrCERT/CC

1.1. Introduction

1.1.1. Establishment

Established in 1996, KrCERT/CC joined FIRST (Forum of Incident Response and Security Teams), the only global CSIRT forum, in 1998 as the first Korean member. KrCERT/CC has responded to many security challenges and has evolved to meet those challenges. Its first major challenge was the breakdown of Internet infrastructure for several hours caused by slammer worm outbreak on 25 January 2003. At that time, KrCERT/CC did not yet have an effective communication and coordination system in place. The Korean government realized that close collaboration between CERT and ISP is a key success factor for dealing with major incidents. KISC runs a 24/7 security operation center whose operation started in December 2003.

1.1.2. Workforce power

KrCERT/CC currently employs about 100 core staff.

1.1.3. Constituency

The Korea Computer Emergency Response Team/Coordination Center (KrCERT/CC) serves as the focal point in coordinating security incidents affecting all Korean constituencies. In the national cyber security framework, KrCERT/CC covers the incident handling and security of information systems and networks in the private sector such as telecommunication sector and home users. Internationally, KrCERT/CC cooperates with many leading national CSIRTs, international organizations, security vendors, and so on. KrCERT/CC, which is another name for the Korea Internet Security Center (KISC), belongs to the Korea Internet & Security Agency (KISA).

2. Activities & Operations

2.1. Operations

2.1.1. Operation of Malware-Concealing Site Detection System

KrCERT/CC developed the malware-concealing site detection system (MC-Finder) in-house, and it has been inspecting 2.5 million domestic domains since 2014. Its purpose is to inspect the homepages for any concealed malware and to delete and block the malware if found in order to prevent the user PCs from being infected. In 2014, 47,703 sites were confirmed to have concealed malware. This figure represents a 168.7% increase compared to 2013.

	2013 Total	2014												Total
		1	2	3	4	5	6	7	8	9	10	11	12	
Landing site	13,278	1,083	497	640	348	281	671	1,276	3,235	3,762	3,352	9,973	20,002	45,120
Exploit sites	4,472	244	190	283	204	177	117	161	217	210	121	260	399	2,583
sum	17,750	1,327	687	923	552	458	788	1,437	3,452	3,972	3,473	10,233	20,401	47,703

※ Landing site: Homepage that disseminates malware indirectly by automatically connecting the homepage visitors as the disseminating site

※ Exploit site: Homepage that directly disseminates malware to the homepage users

Among the malware-concealing sites detected in 2014, the homepages of small and medium enterprises constituted the biggest portion with 58%, followed by others (individuals, etc.), non-profit organization, and research institutes. The main types of malware disseminated over homepages included malware to leak financial data, pharming malware to induce users to go to banking phishing sites, remote controls, and droppers.

2.1.2. Cyber Shelter

KrCERT/CC began providing the DDoS Cyber Shelter service to small and medium enterprises in 2009 after several large-scale DDoS attacks took place in Korea. Since the service was launched, a total of 1,001 organizations have used the shelter as of 2014, with 449 successfully defending themselves against DDoS attacks.

Type	2010	2011	2012	2013	2014	Total
No. of enterprises using the service	52	101	175	260	413	1,001
No. of successful DDoS defenses	25	60	138	116	110	449

Moreover, the service carried out the treatment of zombie PCs collected during the defense against DDoS attacks and blocking of C&C servers to prevent secondary damage from the infection of malware.

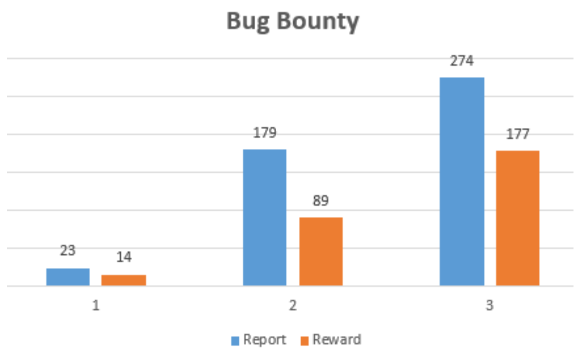
As the notable characteristics of DDoS attacks blocked by the DDoS shelter in 2014, there were more DDoS attacks targeting web applications such as DNS and NTP servers. Among the DDoS attack types, UDP/ICMP flooding, which depletes the bandwidth of the lines, accounted for the largest portion; large-scale attacks of 3Gbps or more increased visibly. Such trend of large-scale attacks was confirmed by the 76Gbps/8,800Kbps-level DDoS attack around November.

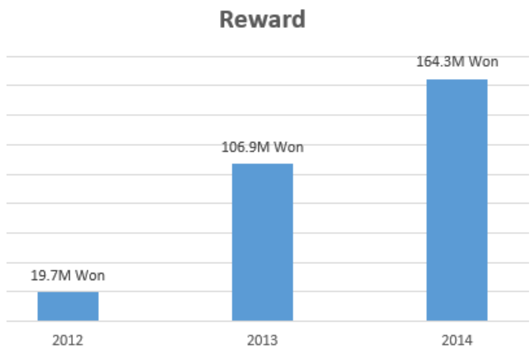
2.1.3. Bug Bounty

Because attacks using the vulnerabilities of popular software such as Hancom Office are occurring continuously in Korea, and new vulnerabilities are found worldwide, KrCERT/CC initiated a reward policy in October 2012 to prevent the incidents in advance and encourage the experts to discover new vulnerabilities.

Since the enactment of the policy in 2012, a total of 478 cases were registered as of 2014. Among them, the analysis data of 330 cases confirmed to be zero-day vulnerability were provided to software developers to request the development of patch and prevent intrusion incidents in advance.

In 2014, a total of 274 cases were reported, increasing 53% compared to the previous year; KRW 164.3 million was given as reward for 177 cases. In August, an inspection of ActiveX vulnerabilities used for malware dissemination was conducted. A total of 110 ActiveX vulnerabilities in the public, banking, commerce, and game sectors were reported, and KRW 65.1 million was given as reward for 81 cases.





In 2014, a joint bug bounty program was initiated with Hancom in the second quarter of 2014 as part of the voluntary security vulnerability discovery program by enterprises. A total of 9 vulnerabilities of Hancom Office were found, with rewards given accordingly. Hancom also awarded appreciation plaques to the top 3 reporters of vulnerabilities of Hancom Office.

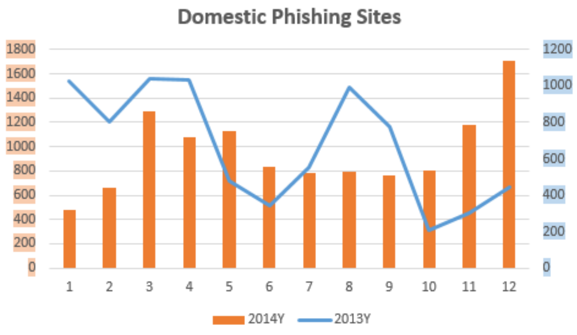
2.2. Abuse statistics

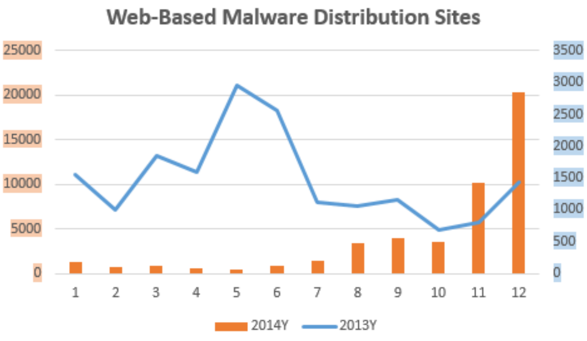
2.2.1. Domestic Phishing Sites

The number of phishing sites targeting domestic sites increased from 7,999 in 2013 to 11,511 in 2014.

2.2.2. Web-based Malware Distribution Sites

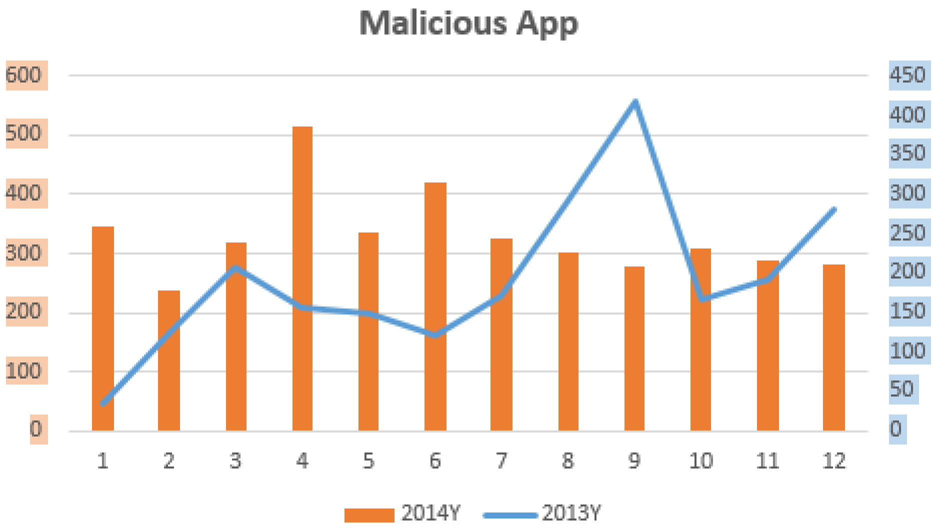
The number of web-based malware distribution sites also increased from 17,750 in 2013 to 47,703 in 2014.





2.2.3. Smishing (Text Message Phishing)

Although Korea was relatively late in adopting the smartphone, the number of smartphone users in the country rapidly increased after 2012. As such, security incidents using the convenience of smartphones have also increased, particularly smishing (SMS + phishing) attacks that abuse Internet access from smartphones and simple payment service. Since the end of 2013, smishing attacks against Android smartphone users have run rampant, with the explosive growth in 2014 causing serious damage. The security awareness failed to keep up with the rapid growth of smartphone usage, and smishing SMS usually disguised themselves as acquaintances or well-known franchises so that the victims were easily deceived. Smishing has evolved from manipulating the simple billing app to taking out the maximum monthly withdrawal when the malicious app is installed in the form of seizing the public certificate and personal information in the smartphone. As such, KrCERT/CC strives to minimize the damage by receiving reports from the users and mobile telecommunication carriers, quickly analyzing the malicious apps, and blocking the information-leaking site.



2.3. New services

2.3.1. Cyber Threat & Incident Information Analysis - Sharing System

The Cyber Threat & Incident Information Analysis Sharing System is the system developed by KrCERT/CC in 2013 for the purpose of collecting recent cyber threats and cyber incident information to manage them effectively and find correlations between them. On the other hand, the National Security Vulnerability Database established by the sharing system provides well-used software vulnerability information for S/W vendors and security companies before they are abused by hackers. The number of participants is not open, but KrCERT/CC plans to expand the participants continuously in the future.

3. Event

3.1. Training

3.1.1. 2014 APISC Training Course

KrCERT/CC hosted the 2014 APISC Security Training Course to support the strengthening of response capabilities of developing economies from the Asia-Pacific Region. The training has been held annually since 2005; its main objective is to assist developing economies that are interested in establishing Internet response capabilities -- such as CSIRT -- while providing training opportunities for establishing and managing CSIRT in their own economy. The course was held on July 7~11 in Somerset Palace, Seoul, Korea. A total of 18 trainees from 18 economies and 3 trainers from 2 economies attended a 5-day training course. On the first day of the course, all participants had the opportunity to share their domestic snapshot and experience on information security. The session helped identify where each CSIRT is positioned as well as its future steps considering the training curriculum.

On the second day of the course, educational materials for the TRANSITs were delivered. The dynamic interaction between trainers and sharing of responsibilities among trainers made the course more successful and fruitful.

아·태 정보보호 초청 교육
2014 APISC Security Training Course
July 7, 2014(Mon) ~ July 12, 2014(Sat)
Venue Somerset Palace Seoul
Host KISA
Organizer KrCERT/CC

3.2. Drills

KrCERT/CC participated in the APCERT Drill in February 2014 and organized 5 domestic drills in 2014.

3.3. Seminars

KrCERT/CC hosted 4 limited open seminars for Korean domestic specialists concerned. The main objectives were to share the trends of recent cyber attacks as well as how to respond to them.

4. Achievements

4.1. Presentation

KrCERT/CC gave presentations in several international conferences such as the following:

- APT Conference – Mongolia, May
- Infocomm Security Seminar 2014 – Singapore, August
- Romanian Annual Cyber Security Conference – Romania, November

4.2. Publication

KrCERT/CC publishes monthly statistics on Internet incident response (in Korean), and they are posted on its website. Security advisories are published on KrCERT/CC's website as well. These advisories contain software vulnerabilities and affected versions as well as how to fix them.

5. Collaboration

5.1. MOU

In 2014, KrCERT/CC(KISA) signed an MOU with India's CERT and the Cabinet Office in the UK(Office of Cyber Security and Information Assurance) to strengthen cooperation in cyber security.

5.2. Cooperation with Foreign CSIRTs

In 2014, KrCERT/CC had to request cooperation particularly with CNCERT/CC in China and JPCERT/CC in Japan. Because of smishing and pharming incidents, KrCERT/CC had to request steadily for shutdown of the e-mail accounts in Chinese portals or blocking of pharming IPs that were leaking personal information; for their part, CNCERT/CC and JPCERT/CC provided as much cooperation as possible through cause analysis, monitoring, etc.

KrCERT/CC Contact Information
Website: http://eng.krcert.or.kr
E-mail: first-team@krcert.or.kr
Phone: +82-2-118

LaoCERT

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

1. About LaoCERT

1.1. Introduction

Lao Computer Emergency Response Team is a national computer emergency response team, under the Ministry of Posts and Telecommunications which has the responsibilities for dealing with computer, cyber security incident, threat monitoring, training and education on cyber security in Laos. Now, LaoCERT is developing on capacity of it staffs to focus on building LaoCERT to be a national CERT to full operation against with cyber-attack. It was formed in last year and has been known among IT social, government agencies, private organizations in Laos PDR and also international CERTs. LaoCERT become a member of APCERT in October 2014.

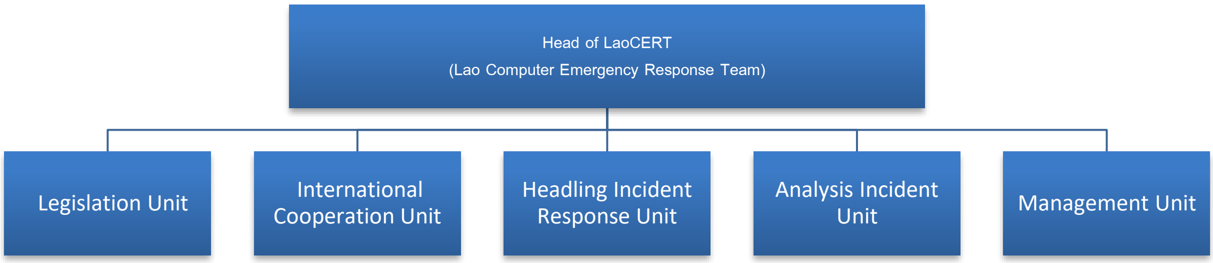
1.2. Establishment

LaoCERT was established in February 2012 by degree 220/MPT. Now LaoCERT is under the Ministry of Posts and Telecommunications (MPT), Government of Lao PDR. It was built by following up as ITU-IMPACT recommendation. Lao Computer Emergency Response Team is handling with cyber security incidents in Laos.

1.3. Workforce power

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

LaoCERT Organization Charts

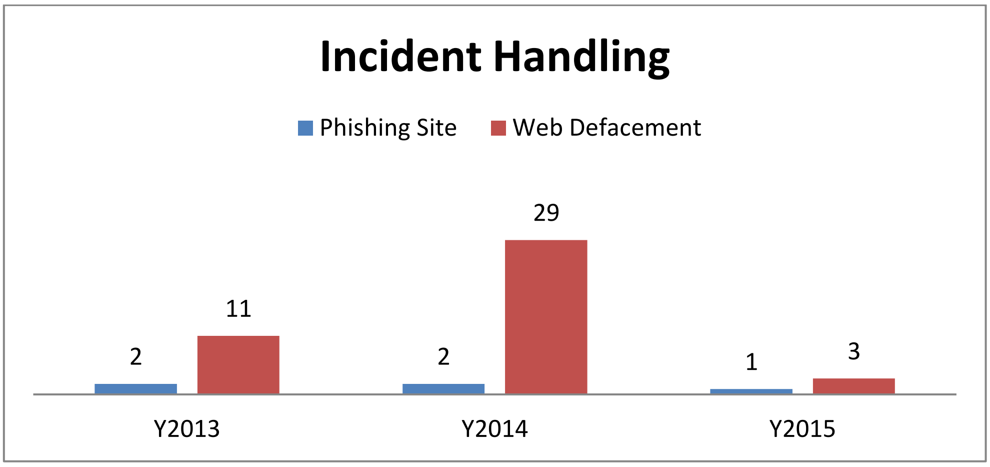

Head of LaoCERT
(Lao Computer Emergency Response Team)
Legislation Unit
International Cooperation Unit
Headling Incident Response Unit
Analysis Incident Unit
Management Unit

1.4. Constituency

LaoCERT is a coordination center or (POC) within Laos and also cooperation with international CERT organizations on cyber security. LaoCERT was disseminating information security awareness raising and internet threat protection to social. LaoCERT is responsible for doing incident handling for government agencies and private organizations to providing them the technical assistance to resolve the incident.

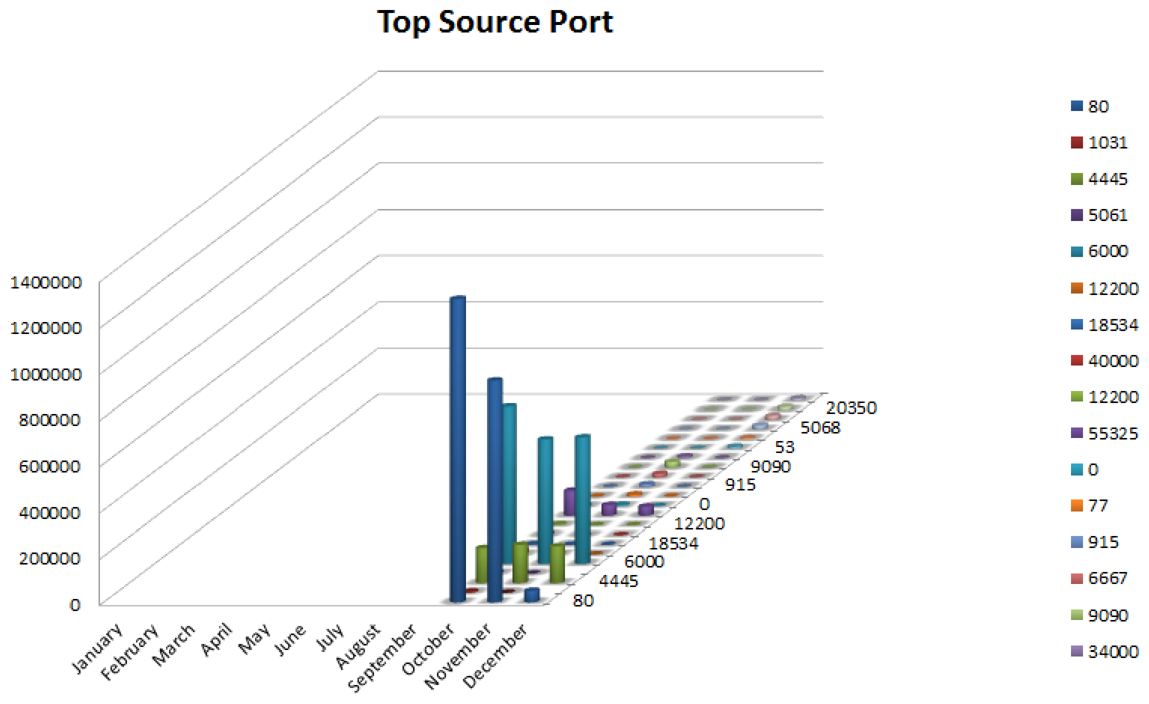
2. Activities & Operations

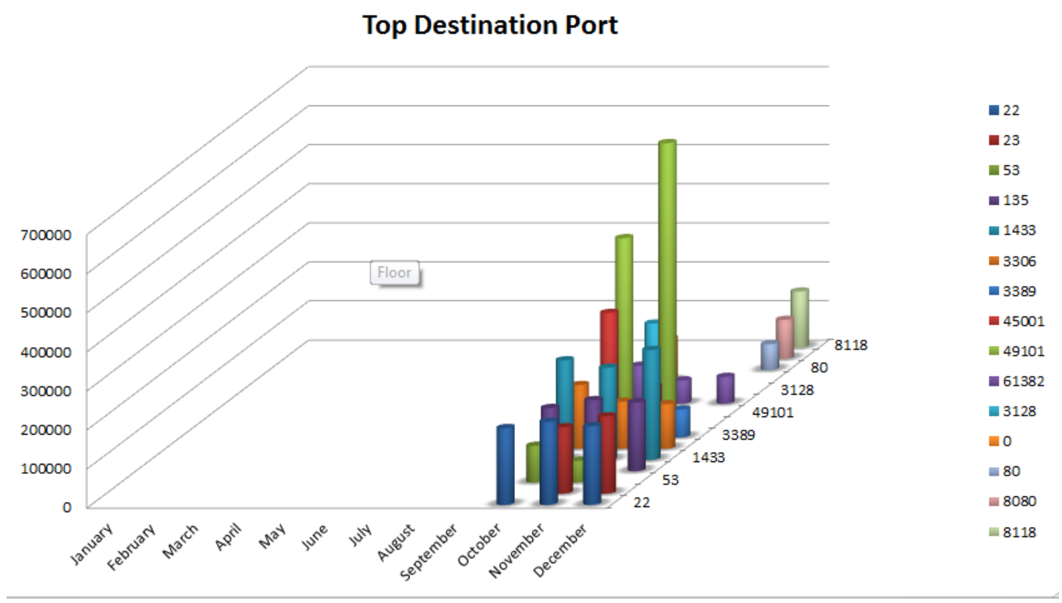
2.1. Incident handling

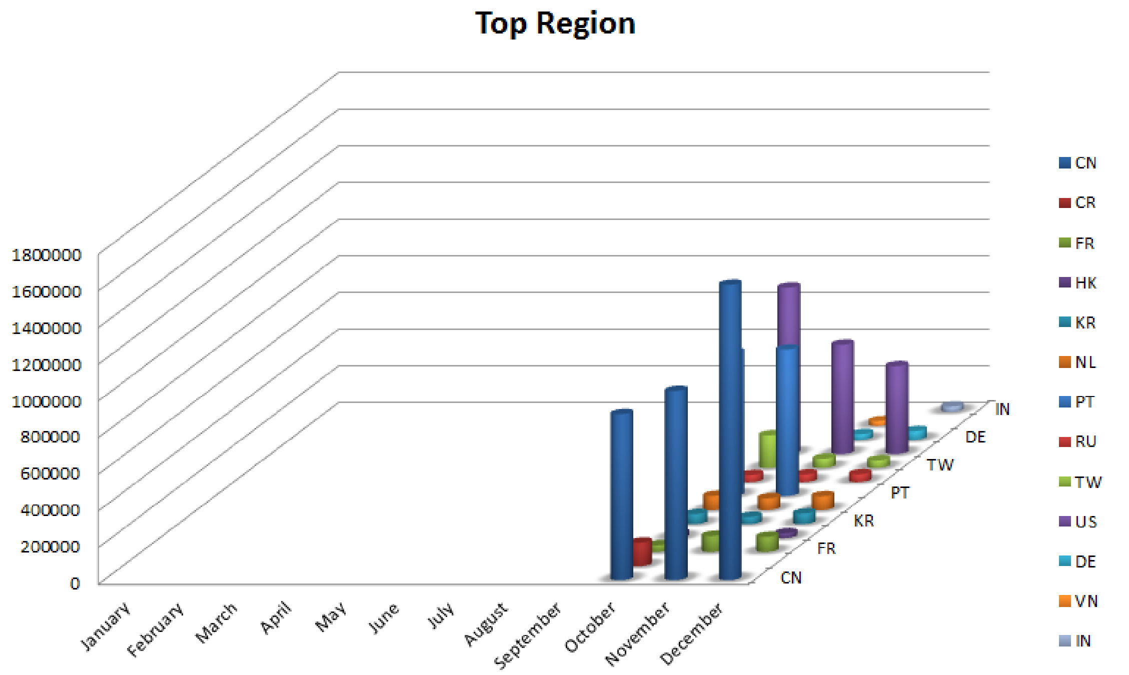


2.2 TSUBAME Statistics

The Following graph shows the top source port, top destination port and top region in 2014.


Top Source Port
1400000
1200000
1000000
800000
600000
400000
200000
0
January
February
March
April
May
June
July
August
September
October
November
December
20350
5068
53
9090
915
0
12200
18534
6000
4445
80
80
1031
4445
5061
6000
12200
18534
40000
12200
55325
0
77
915
6667
9090
34000


Top Destination Port
700000
600000
500000
400000
300000
200000
100000
0
Floor
January
February
March
April
May
June
July
August
September
October
November
December
8118
80
3128
49101
3389
1433
53
22
22
23
53
135
1433
3306
3389
45001
49101
61382
3128
0
80
8080
8118



3. Events organized / co-organized

3.1. Training

- Organized training course on Incident Management System and TSUBAME Sensor for LaoCERT staffs by supported from ThaiCERT and JPCERT/CC on 19th – 23rd May, 2014, held in Laos.
- Organized training course about Network Vulnerabilities Scanning and Threat Monitoring System for LaoCERT staffs on 27th October – 1st November, 2014, in Laos by invited the trainer from VNCERT.
- Participating the 1st Training for Information Security Staff from 1-13 December 2014 in Indonesia.
- LaoCERT and ITU-IMPACT Co-organized the ITU Penetration Testing Workshop for LaoCERT staffs by experts from ITU-IMPACT on 8th – 12th December 2014 in Laos.
- Participating the First Response Computer Forensics and Cybercrime Investigation on 27th June – 02nd July 2014 in Phnom Penh, Cambodia.

3.2. Drills

- LaoCERT and ITU-IMPACT Co-organized the Cyber Security Forum and Cyber Drill (CLMV) at Laos PDR. on December 9-11, 2013.
- Participating in ASEAN CERT Incident Drill (ACID 2014) on September 24, 2014.

3.3. Workshop

- Participating the 6th Japan-ASEAN Government Network Security Workshop on 27th -28th August, 2014 at Singapore.
- Participating the 5th Japan-ASEAN Information Security Workshop in Manila, Philippine on 1st - 2nd October, 2014.
- Participating the 7th ASEAN-Japan Information Security Policy Meeting and Symposium on 7th - 9th October, 2014 in Tokyo, Japan.

3.4. Seminars

- Participating the 5th China-ASEAN Network Security Seminar on 14th-18th May 2014 in China.
- Participating the 6th China-ASEAN Network Security Policy Seminar on 26th – 30th May 2014 in Shantou, China.

4. Achievements

4.1. Publication

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

5. International Collaboration

Although LaoCERT is a new organization and just become a member of APCERT in last year 2014, but we have coordinate to other CERT organizations for good relationship and cooperation.

5.1. MOD (Minutes of Discussion)

After MOD signed with Japan Emergency Response Team Coordination Center of Japan (JPCERT/CC) on 19th October 2012. LaoCERT, JPCERT/CC and ThaiCERT organized The Basic Understanding of CSIRT and Incident Response Training held in Lao PDR.

5.2. MOU (Memorandum of Understanding)

Being signed the MOU with Thailand Computer Emergency Response Team (ThaiCERT), Electronic Transaction Development Agency (ETDA) on July 2013. LaoCERT, JPCERT/CC and ThaiCERT organized training course on RTIR and network forensics to exchanged information, knowledge and experience on IT Security held in Lao PDR in October 2013.

5.3. MoM (Minutes of Meeting)

By signing the second MoM with Ministry of Information and Communication, Socialist Republic of Vietnam (VNCERT) on 27th October 2014 for collaboration on sharing CERT experiences and exchange knowledge of cyber security between the two countries.

6. Future Plans

6.1. Future projects

- Apply to be a member of FIRST (Forum of Incident Response and Security Teams).
- Finished the final drafting of cyber-crimes law and submitted to the National Assembly for approval by June of 2015.
- Send LaoCERT's technical quality staffs to the SAN/CEH cyber security professional course.
- LaoCERT plan to have a CEH diploma or certificate in the field of cyber security.
- Request training course on TSUBAME Sensor in advance level from JPCERT/CC.

7. Conclusion

Since 2012, LaoCERT was established as a CERT organization in Laos, It has learned a lot of knowledge, experiences and has been assistance from the national CERTs such as: ITU, JICA, JPCERT/CC, VNCERT, ThaiCERT…..for developing on capacity building of LaoCERT staffs. However, LaoCERT is willing to cooperate with national CERTs for good relationship and exchange information, knowledge, experiences, technical skill on cyber security to against with cyber-attack.

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 2014 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 Myanmar Posts and Telecommunications (MPT), MCIT and total eleven members worked for mmCERT/cc last year. The number of members didn't increase in 2014.

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 2014.

2. Activities & 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 Newsletters

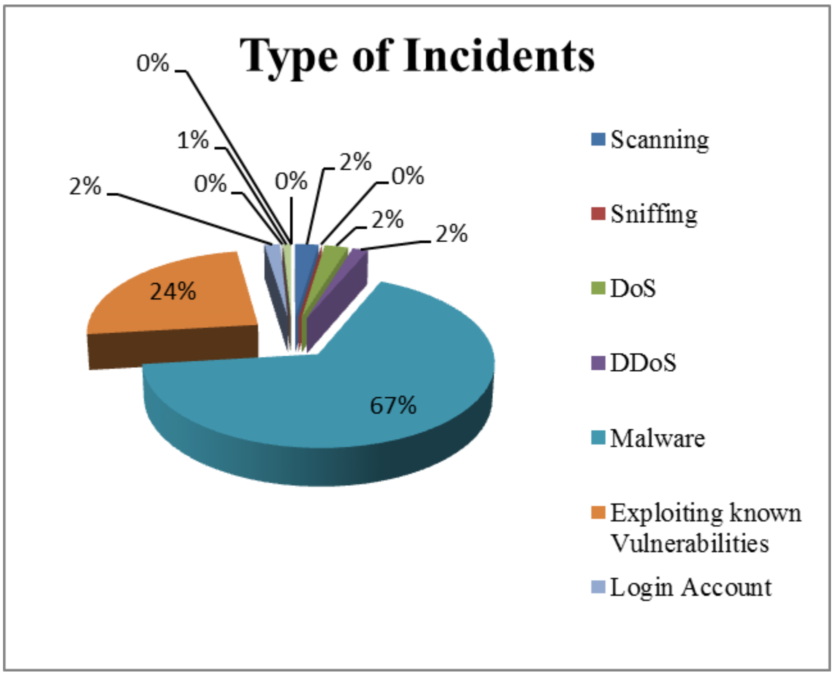
Every Friday, Weekly Email Newsletter was published and distributed to all local ISPs and constituencies starting from August 24, 2012 for the purpose of alerting the updated world-wide security news. These extracted resources are obtained as a member of APCERT and other security related information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

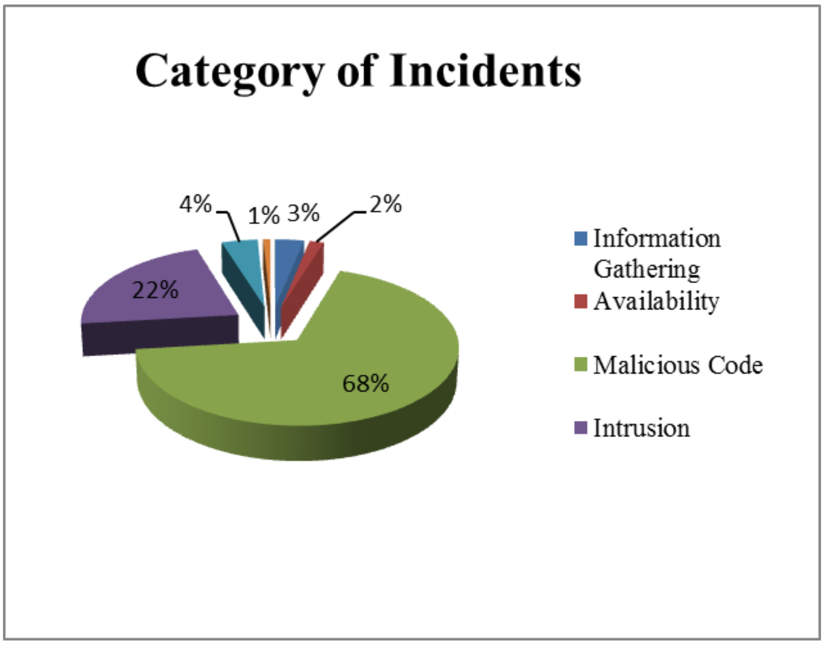
2.3. Weekly Technical Article

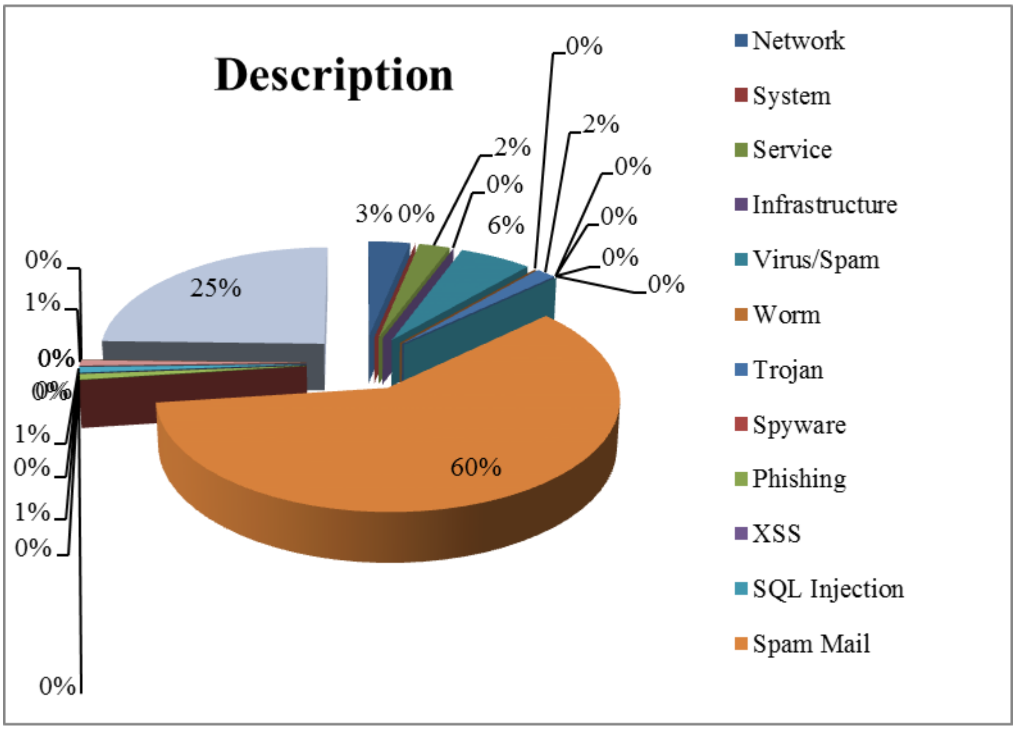
mmCERT publishes Weekly Technical Article, written in myanmar for the purpose of promoting technical expertise and awareness to the IT persons. It is also posted on mmCERT website (www.mmcert.org.mm) since May 2013, on every Thursday.

2.4. Incident Handling Reports

The following graph shows the incidents that were solved by mmCERT in 2014. According to the results on incident analysis by mmCERT/cc, Intrusion and Malicious cases were the most prominent incident cases in 2014.


Type of Incidents
0%
1%
2%
0%
0%
2%
0%
2%
2%
24%
67%
Scanning
Sniffing
DoS
DDoS
Malware
Exploiting known Vulnerabilities
Login Account

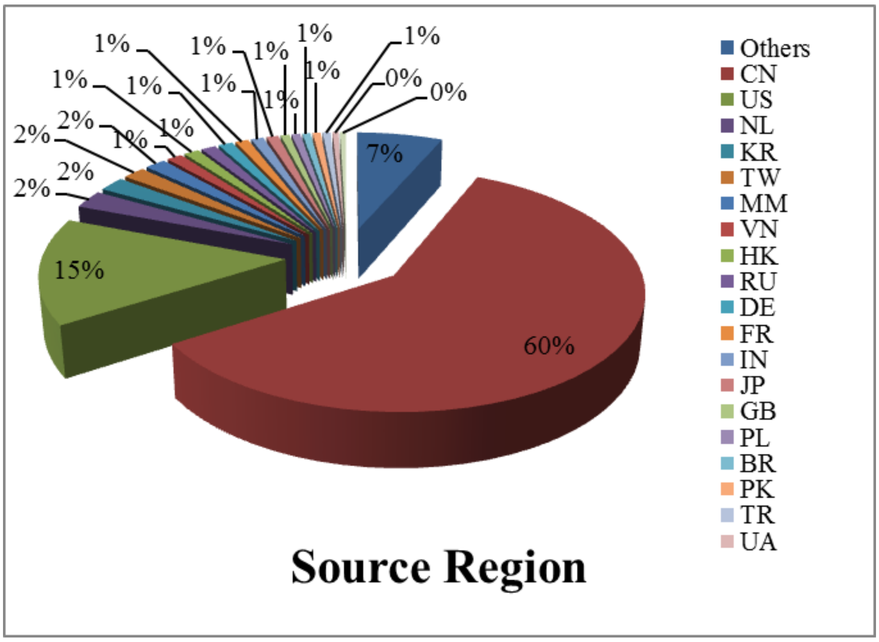

Category of Incidents
4%
1%
3%
2%
22%
68%
Information Gathering
Availability
Malicious Code
Intrusion

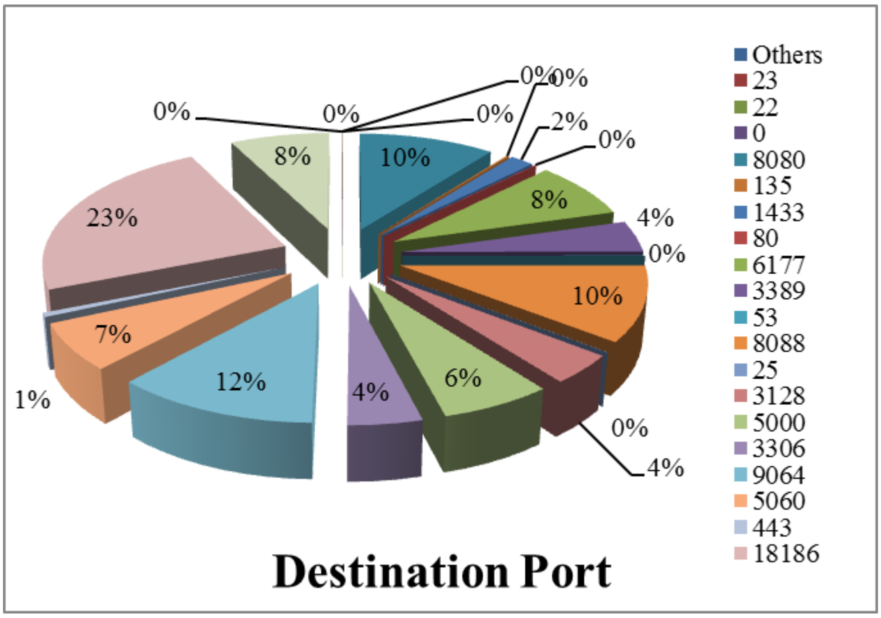


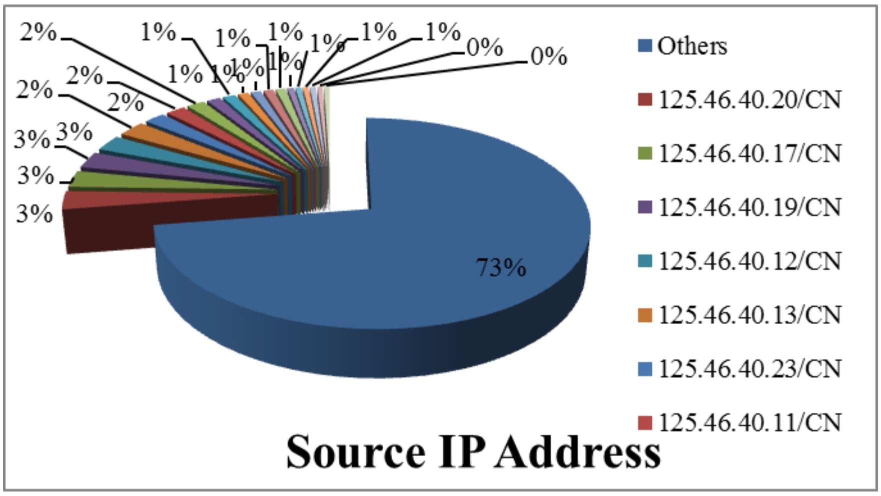
2.5. Abuse Statistics

2.5.1. Abuse Statistics on TSUBAME Sensor Log Data

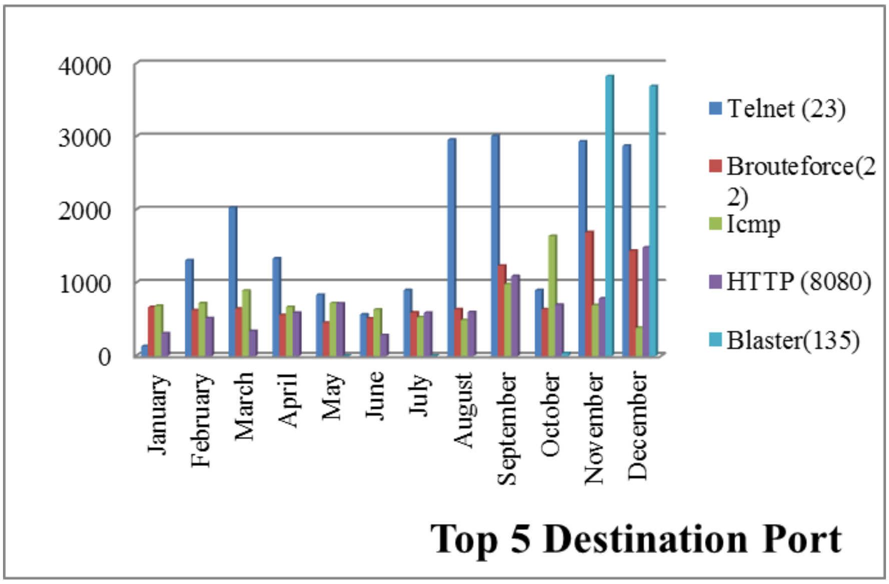
The following graph shows the top source country, top destination port and top source ip address statistics obtained from TSUBAME Sensor in 2014.

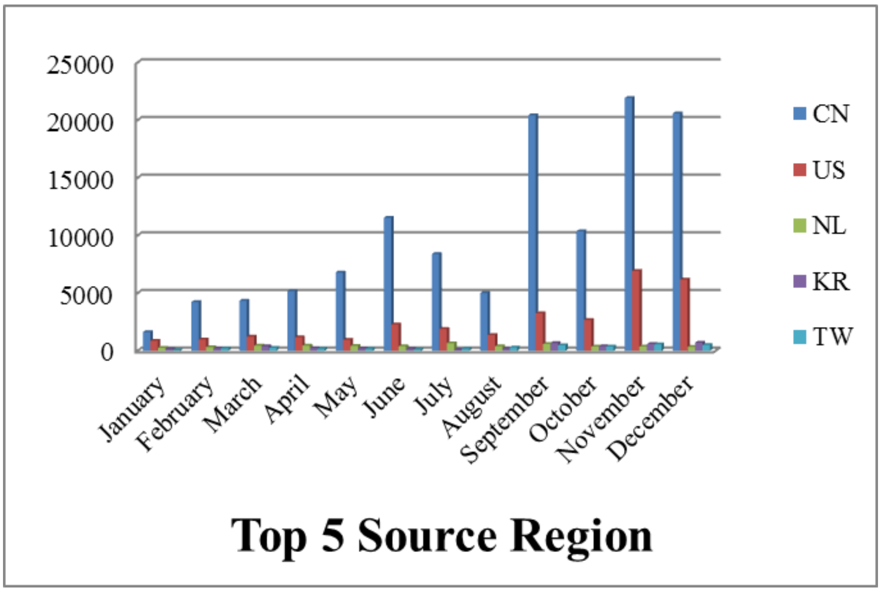

Source Region
7%
60%
15%
2%
2%
2%
2%
1%
1%
1%
1%
1%
1%
1%
1%
1%
1%
1%
1%
0%
0%
Others
CN
US
NL
KR
TW
MM
VN
HK
RU
DE
FR
IN
JP
GB
PL
BR
PK
TR
UA

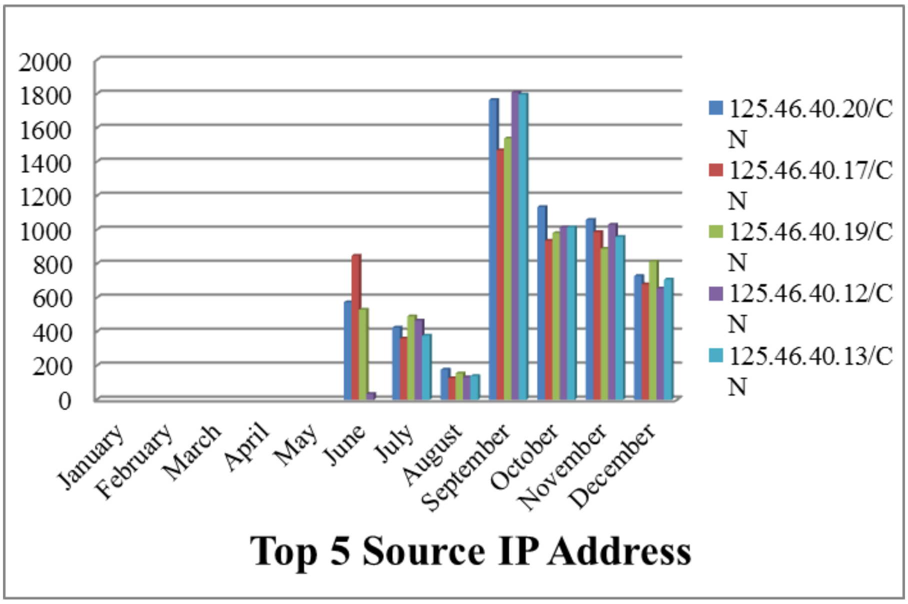

Destination Port
0%
0%
0%
0%
0%
2%
0%
10%
8%
8%
4%
0%
10%
0%
4%
6%
4%
12%
7%
1%
23%
Others
23
22
0
8080
135
1433
80
6177
3389
53
8088
25
3128
5000
3306
9064
5060
443
18186



The following graphs show the top five countries, 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 2014.

- "Information Security for e-government promotion (B)", provide by JICA, at Okinawa, Japan (January 21- May 31, 2014).
- "Training Program in Network Security Assessment and Proactive Defense", provide by ITEC, CDAC at Chandigarh, India (January 24- March 24, 2014).
- "Foundation Program for Fresh Software Engineering graduates of Myanmar",

provide by UN, at Mysore, India (February 5- April 24, 2014).

- Malware Behavior Analysis and Detection Online Training provide by TWNCERT on November 5, 2014.
- Participating in Information Security Training at Jakarta, Indonesia on December 1-13, 2014.

3. Events organized / co-organized

3.1. Seminar & Workshop

- Giving Seminar to Cyber Crime Unit (Myanmar Police Force) at CID, Insein in Yangon on July 8, 2014.
- Providing Communication Forum on Responsible Social media in Myanmar Cyber Crime Unit to public at MICT on July 20, 2014.
- Giving Seminar to West Yangon Technological University Students at mmCERT in Yangon on October 1-20, 2014.
- Giving presentations to all members of mmCERT and delegated persons by the individual mmCERT members in December, 2014

4. International Collaboration

4.1. Drills

- Participating in APCERT Drill on February 19, 2014.
- Participating in ASEAN CERT Incident Drill (ACID 2014) on September 24, 2014.

4.2. Other Activities

- Participating in "5th APT Cyber Security Forum" at Ulaanbaatar, Mongolia on May 24-30, 2014.
- Participating in "6th China-ASEAN Network Security Seminar" at Shantou, China on May 29-30, 2014.
- Participating in 5th ASEAN-JAPAN Information Security Workshop at Manila, Philippines on October 1-4, 2014.
- Participating in 7th ASEAN Japan Information Security Policy Meeting and Symposium at Tokyo, Japan on October 7-9, 2014.

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
- Updating Incident Management Guide book
- Updating Incident Handling Methodology Guide Book
- Secure and Updated Version of mmCERT Web server
- Applicable Online Ticketing System

6. Conclusion

During 2014, mmCERT has been made a progress on capacity building, proposing incident management policy, examining incident handling methodology, international co-operation and collaboration, arising public awareness activities. mmCERT intends to do research in incident attack cases, Tsubame log data analysis and to promote public awareness activities and distributing and sharing technical expertise to all citizens of Myanmar. We also intend to participate in international co-operation and collaboration more effectively and efficiently.

MNCERT/CC

Mongolia Cyber Emergency Response Team / Coordination Center – Mongolia

1. About MNCERT/CC

1.1. Introduction

"MNCERT/CC" non-government organization was established in 2014 and has been operating since under guidance and regulation of the Mongolian National Security Council. Our organization is responsible for monitoring and analyzing cyberattacks and responsiveness on a national level, creating awareness and providing assistance on national security, arranging amenities to exchange knowledge and experience with other CSIRT teams, receiving information of global and regional attacks and complications, delivering collaborative response, researching and analyzing in collaboration with teams from other nations.

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 cyberattacks 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. Workforce power

Human resource:

- Head of Organization – 1
- Officer–2
- Incident Handler – 4

- Analysts–2

1.1.3. Constituency

Our constituencies are:

- Internet Service Provider Companies
- Banks
- National Cyber Security Center
- Mobile Operation Companies
- MonCIRT
- DCERT
- Other CERTs

2. Activities & Operations

2.1. Incident handling reports

Incidents happened in Mongolia

The Black hat Asia 2014 has been organized in Singapore, March 25th -28th 2014. In this conference, one of many interesting presentations was presented by Mr. Takahiro Haruyama (Forensic investigator and malware analyst) and Mr. Hiroshi Suzuki (Forensic investigator and malware analyst). The presentation named "I know you want me – Unplugging PLUGX" showed about "Remote Access Trojan"(PlugX type of RAT) not being found in any anti-virus software and was aiming to gather necessary information from a target. Main target was Mongolia. This was confirmed by the findings of our team.

The "PlugX" RAT was expanded in Mongolian state and private sector organizations. In this framework, Mongolian National Security Council and related higher organizations are taking mitigation measures to eliminate it. Also, MNCERT/CC is taking measures to block access in timely manner for C&C servers registered and giving an advice how to protect from it and give a caution for state and private sectors.

During the reporting period, incidents were happenning continuously by email attacks that contain malicious codes, scripts towards especially Mongolian Government sectors which aimed specific target personnel from government agencies and private. Due to it, these attacks cannot be detected by common used anti-virus programs, e-mails with attached malicious codes were sent.

Below are methods used to install malicious software by e-mail:

- Send e-mail with MS Office file attachment
- Insert download link to e-mail content
- an archived file with password

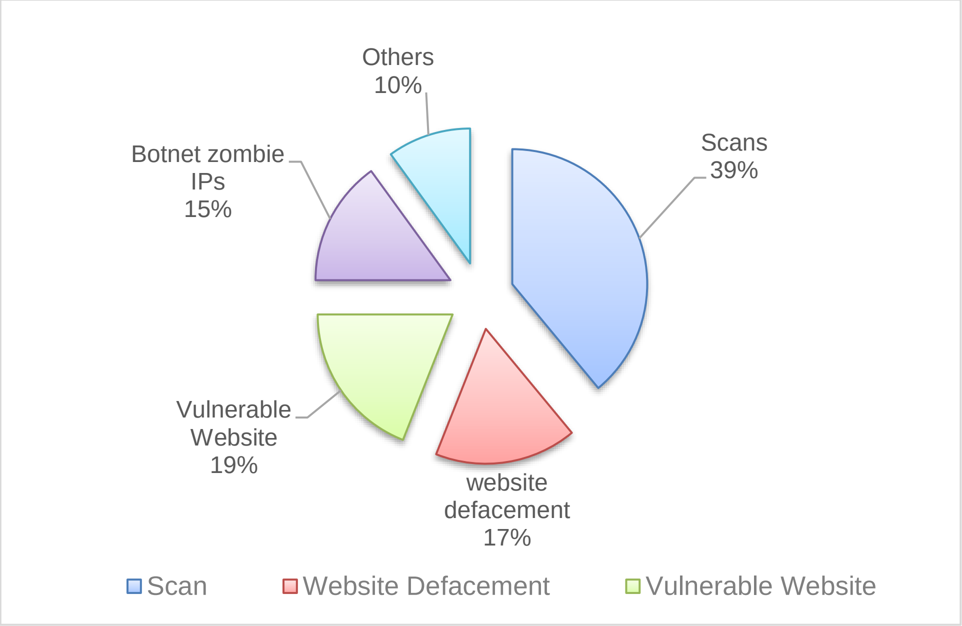
After it was reported that the e-mail containing registered malicious software was sent from addresses of government agencies and private sectors, it was clear that these were intended attacks.

By monitoring e-mail subject lines, we've concluded that e-mail subjects with global or Mongolian trending or breakthrough news were the main reason for opening suspicious e-mails. Examined e-mail subject lines:

- About government structure
- Vaccine tests against ebola virus were successful.
- For improving security of E-MAIL system.

2.2. Statistics

Currently, MNCERT/CC's constituency are all kind of organizations such as business companies, private sector organizations, NGO and general public. The summary of acitivities carried out by MNCERT/CC during the year 2014 is given in the following chart. This chart shows about summary of the critical incidents that were registered national wide: scan 36%, incidents towards web page 23%, web pages with security holes 19%, computers occupied by attackers 12%, others 10%. In 2014, Scan threats and vulnerable websites increased dramatically.



Scans

Reflecting on the security and threat landscape of 2014, one trend that stands out is the growing ability of malware hosts. In overall, after inspecting critical requests that came in 2014, the majority of the scans were to reveal website's sensitivity and to collect network hosts as well as information of hosts. ICMP protocol is used forgetting network host's information and recognizing specific service's functionality in every host on that network. These scans were made mostly to government agencies. It mainly shows malware propagation through websites of the private and government sectors were observed constantly. The growing popularity of the website incidents comes from not using the software license warranty and human resource's lack of knowledge.

Websites with Vulnerability

Government agencies - 21,3%

Private sectors - 17,15% are at "high risk" level.

Mostly due to responsible personnel's lack of knowledge, skills and incomplete setups, websites of government agencies and private sectors are under attack.

Website defacement:

Government agencies – 12%

Private sectors – 23%

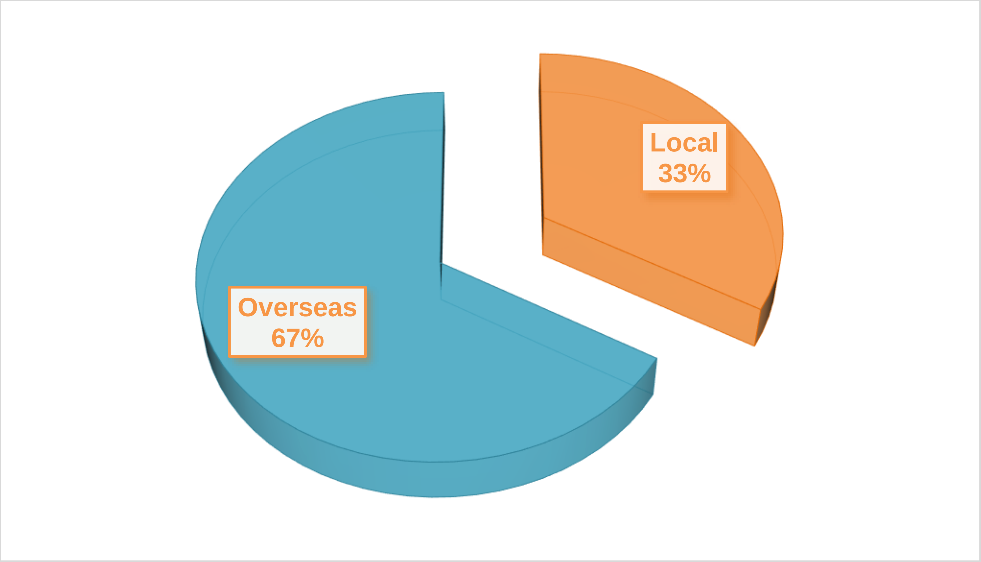
During monitoring terms, zombie botnets have become gradually widespread, resilient and camouflaged and they seem to be finding some dangerous new targets in the government and private sectors because consequently responsible personnel leave the server and computer on without using, and user's lack of academic knowledge and practice and also not making the necessary software updates.

Botnet and zombie IPs - 15,3%

In 2014, out of all data directed to government agencies and private sectors, 85,70% were by TCP, 13,36% were by UDP transmitted.

Others incidents 10%

In following chart shows about location of the host scans.



3. Events organized / co-organized

3.1. Competition

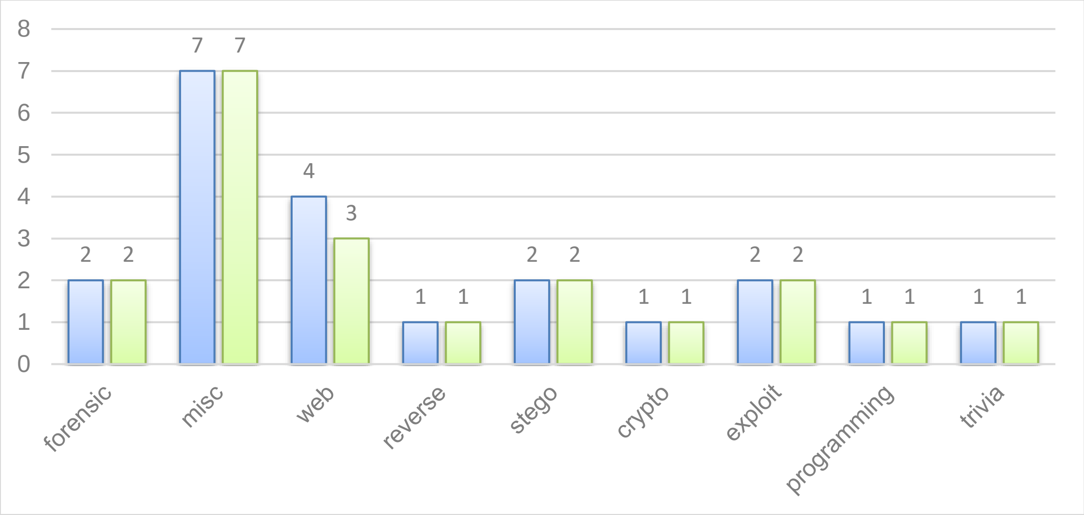
3.1.1. "Haruul Zangi 2014" National Cyber Security Competition

This competition was first organized in 2013 with a mission to bring awareness of data security, ethical hacker, attack, protection for specialists of Mongolian information technology and create positive understanding, consciousness and environment. We successfully organized "Haruul zangi" competition for the second year between 4/28 – 5/06, 2014, with 4 levels.

The competition consists of 4 stages with elimination policy.

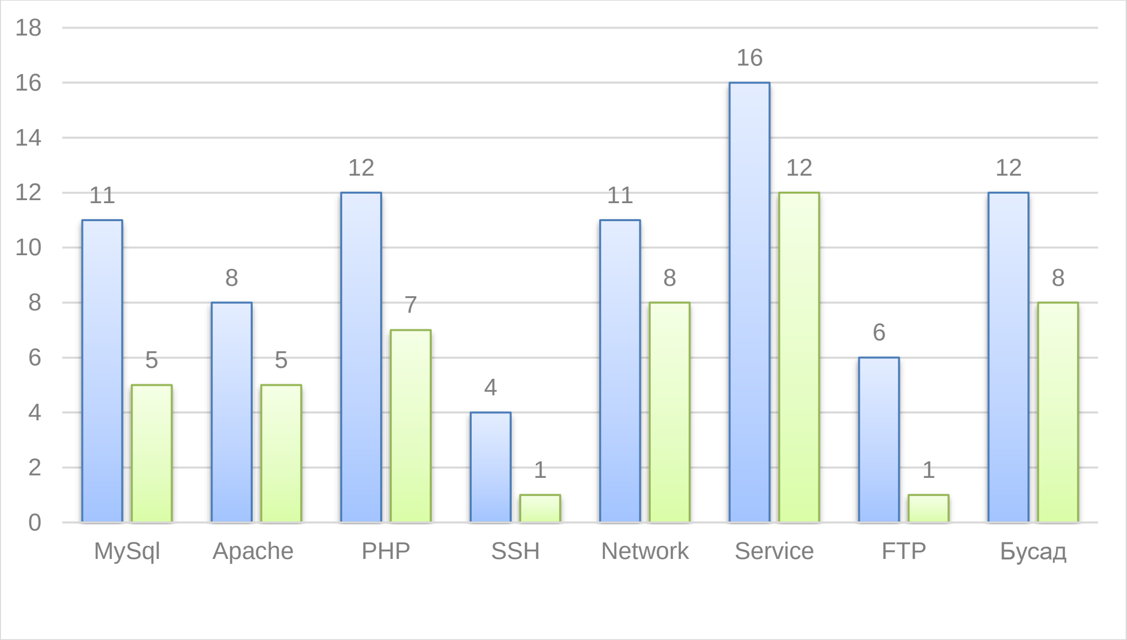
- Stage 1: Data analysis
- Stage 2: Fix the system
- Stage3: Attack the system and network
- Stage 4: Solve security's violation

1st, 2nd stages were designed to be completed online when the 3rd, 4th stages had to be completed on the network, systems designed by the organizers. Out of 125 teams with 600 members, 60 teams completed the tasks. Following chart shows the knowledge level of the participants who completed 9 different tasks on the 1st stage.



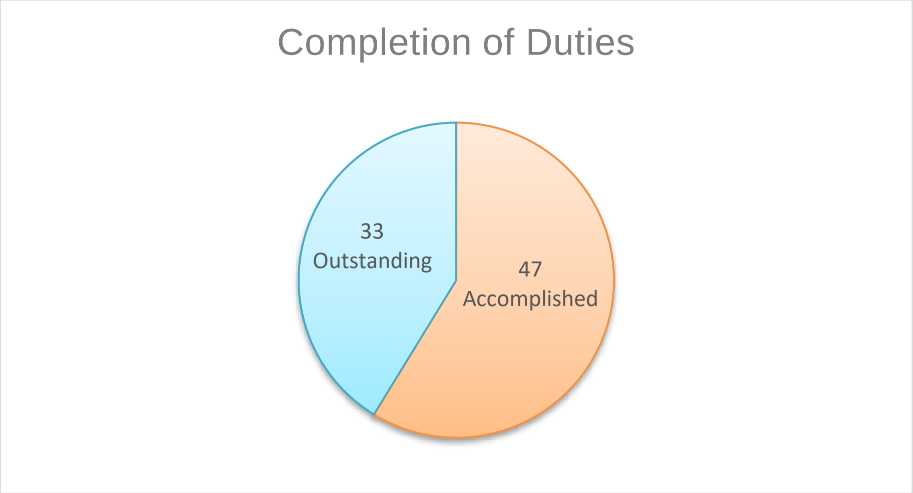
- **Forensic** –Make incidents analyse based on too given data.
- **Web** - Grip a network service in view of website service
- **Reverse** –Find vulnerability point, make analyse being opened activity file.
- **Stegno** –Find being hidden necessary information for other appropriation.
- **Crypto** –Encrypt data and then decrypt data.
- **Exploit** –Make attack based on any error of service and vulnerability points.
- **Programming** – Automatic software development.
- **Trivia** - Sample tasks for common usage.
- **Misc** - Other types

On the 2nd stage 80 tasks of 8 types were given, the progress results are shown on below graph.

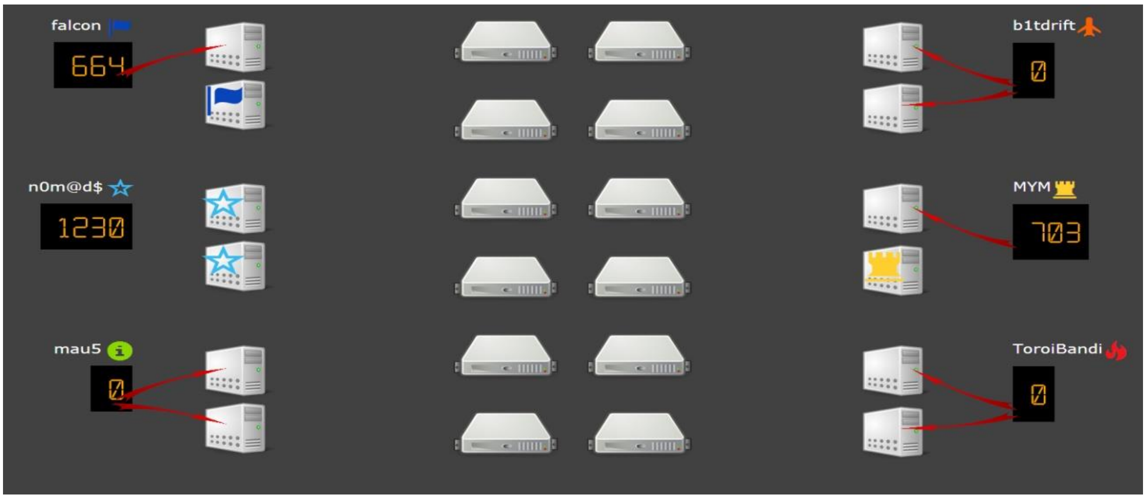


- **MySql** –Database vulnerability
- **Apache** –Webserver vulnerability
- **PHP** –Related with vulnerability points of internet software language
- **SSH** –Related with vulnerability of Secure shell
- **Network** –Vulnerability of network configuration and protocols
- **Service** –Service vulnerability that runs on system.
- **FTP** –Related vulnerability of FTP services.
- **Others** –Other system's security and safety vulnerabilities.

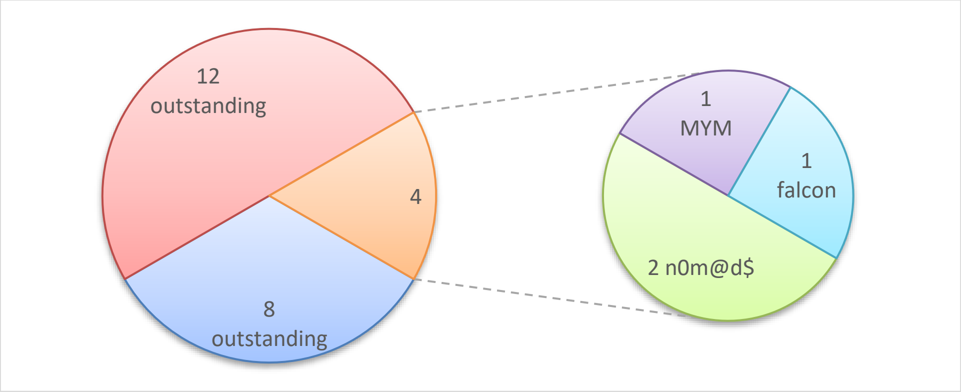
Teams solved 47 vulnerability points out of 80 that were created on the given server. Please see Graph –1.



On the 3rd stage, teams must find and dominate 12 joint servers by using their own 2 servers, then conquer the other teams' dominated servers.



Graph-2 shows competition's 3rd stage



On the final stage, teams have createdvulnerability points on the rival team's computer, and then fixed the vulnerability points on their own computers.

3.2. Drill

In collaboration with Cyber Security Department of Mongolia, we have organized "Cyber workshop 2014" attended by specialists from 64 government agencies. Nowadays intended e-mails consisting malicious codes are sent, targeting specific personnel of government agencies, therefore study cases were presented during workshop to demonstrate how these e-mail attacks are performed in order to steal data and information.

3.3. Seminars

MNSEC-2014

Information technology (IT) benefits the business world by allowing organizations to work more efficiently and to maximize productivity. Faster communication, electronic storage and the protection of records are advantages that IT can have on your enterprise. Information technology has to do with computer applications, on which nearly every work environment is dependent on. Since computerized systems are so widely used, it is advantageous to incorporate information technology into your organization. Therefore the crucial challenge is to continue the development, even with the lack of the skilled human resource, legal, software hardware and quality equipment for the Information Technology sector in the Mongolia and information security. Therefore, we have organized an event named "MNSEC-2014" seminar on 5th and 6th of September, 2014 in the Information Technilogy Park providing the opportunity to share experience, necessary information, knowledge, technology and new solution with international skilled experts with cyber securitybackground. We have been organizing the event "Information Security" annually since 2012 in Mongolian Information Technology sector. Seminar on safety in the online environment has been organized since 2012. This seminar's goal is to improve this sector in alliance with government agencies and private sectors by discussing current issues regarding Mongolian online safe environment, solutions to improve secure online environment, and exchanging trending latest information and news each other. MNSEC-2014 seminar was successfully organized in cooperation with MNCERT/CC /Mongolian National Computer Incident Response Team/ and Cyber Security Department of Mongolia on September 5,6th, 2014. During this seminar we presented solutions on how to protect ourselves from arising critical issues of the online safe environment. This seminar covered some of the most demanded topics in the sector of information technology, therefore 150 representatives, engineers and technical specialists have shared their knowledge & experience in participation from sectors such as financial institutions, univerisities, government agencies, mobile operators and online service providers.

Introduction of Digital Forensic

Seminar participants

In especially, the delegations of JPCERT/CC have participated according by respective invitation of MNCERT/CC and its following a principle along with questions and answer and free discussing about trends information security in the Mongolia. On the second day, seminar consisted by with two parts, products and solutions. During that day, JPCERT/CC have organized the "Network Forensic" training, and other Mongolian information security companies introduced their own products and solutions in the second part. The seminar has gathered participants' attention showing live demonstration on attacking a website and also by presenting interesting topics such as weaknesses of wireless network in Ulaanbaatar, introducing on how social networks (Google, Facebook, etc.) gather personal data and utilize them for their own advantage and purposes.

4. Achievements

4.1. Co-operate with internal relationship

On December 23rd, "No-tie" event was organized for information technology experts and delegations of leading companies of that sector. Following 3 presentations were presented:

1. Introduction of the "Online safety administration center", action plans for 2015.
2. "PlugX" presentation represented from Cyber Security Department of Mongolia
3. MNCERT/CC 2014 report

4.2. Certification

- CCNA, CCNP – 2 employees
- EC-Council Network Security Administrator – 1 employer
- GIAC Exploit Researcher & Advanced Penetration Tester GXPN – 1 employer
- GIAC System & Network Auditor GSNA – 1 employer
- EC-Council CEH– 2 employees

5. International Collaboration

5.1. Joining International Conference and Events

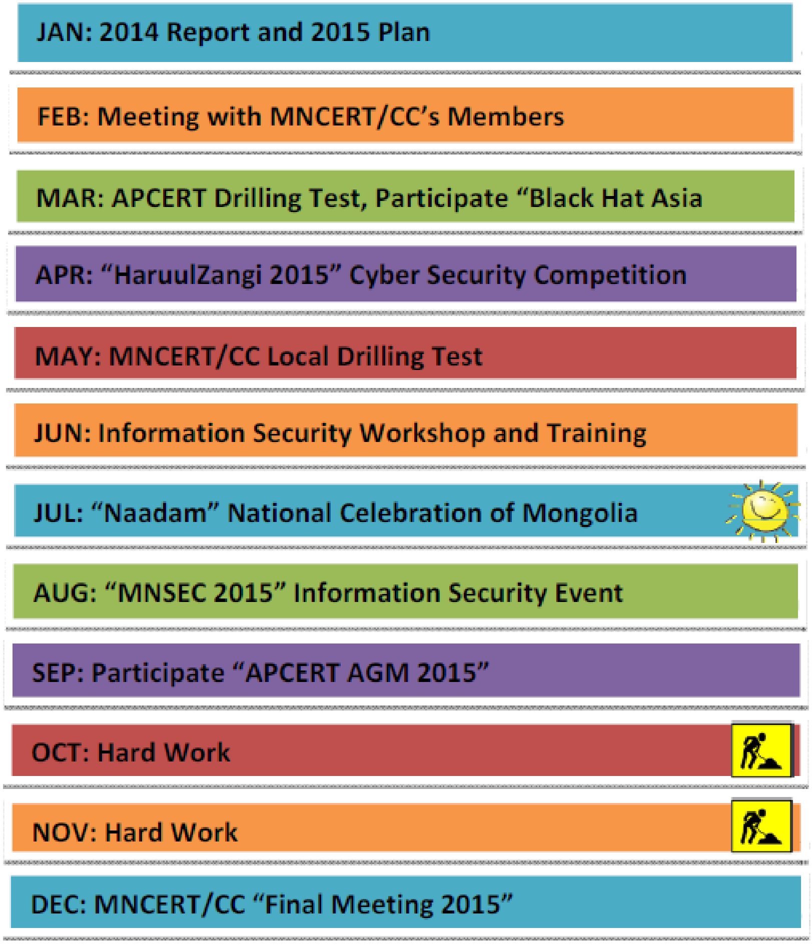
- APCERT AGM 2014, in Taipei - Taiwan
- APICS 2014, in Seoul - South Korea
- 5th APT Cyber Security Forum, in Ulaanbaatar – Mongolia
- Introduction of Malware Analysis, online training organized by TWCERT

5.2. International Membership

- MNCERT/CC joined APCERT Operational Member at 15th September 2014.

6. Future Plans

- Activity Summary of 2015



JAN: 2014 Report and 2015 Plan

FEB: Meeting with MNCERT/CC's Members

MAR: APCERT Drilling Test, Participate "Black Hat Asia

APR: "HaruulZangi 2015" Cyber Security Competition

MAY: MNCERT/CC Local Drilling Test

JUN: Information Security Workshop and Training

JUL: "Naadam" National Celebration of Mongolia

AUG: "MNSEC 2015" Information Security Event

SEP: Participate "APCERT AGM 2015"

OCT: Hard Work

NOV: Hard Work

DEC: MNCERT/CC "Final Meeting 2015"

- Research and develop the national intrusion sensor
- More research and training of the incident trends
- Establish the national security operation center
- Providing technical support and assistance for implementation in the critical infrastructure sectors and local members

7. Conclusion

Mongolian information and cyber security environment was at a critical and challenging state in 2014. This is due to consistent attacks of "PlugX" targeting government agencies and private sectors, to be specific 7 agencies were targeted after a thorough examination. Some attacks were also made from private sectors as well. With "The Cyber Security Department", we conducted investigations and took necessary measures. It's concluded that the most common reason of these attacks happening is the lack of academic knowledge and practice of human resource in the Information technology sectors. Therefore we need to improve end user's knowledge and provide assistance to information technology sector's member organizations to create common policy and its necessary documentations. Becoming a member of the APCERT in 2014 was the biggest achievement for us.

MOCERT

Macau Computer Emergency Response Team Coordination Centre – Macao

1. About MOCERT

1.1. 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.

1.1.1. 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.

1.1.2. 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 2014 there are two (2) staff providing the service with two (2) additional support staff. Service personnel numbers will be re-established back to three (3) as soon as practical to handle the influx of incidents reported.

1.1.3. 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.

1.1.4. Mission Statement

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.

2. Activities & Operations

During the year 2014 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 Clean PC Day
- Assisted in the APCERT Membership Working Group
- Assisted in the APCERT Policy Procedure and Governance Working Group
- Involved in the TSUBAME Working Group

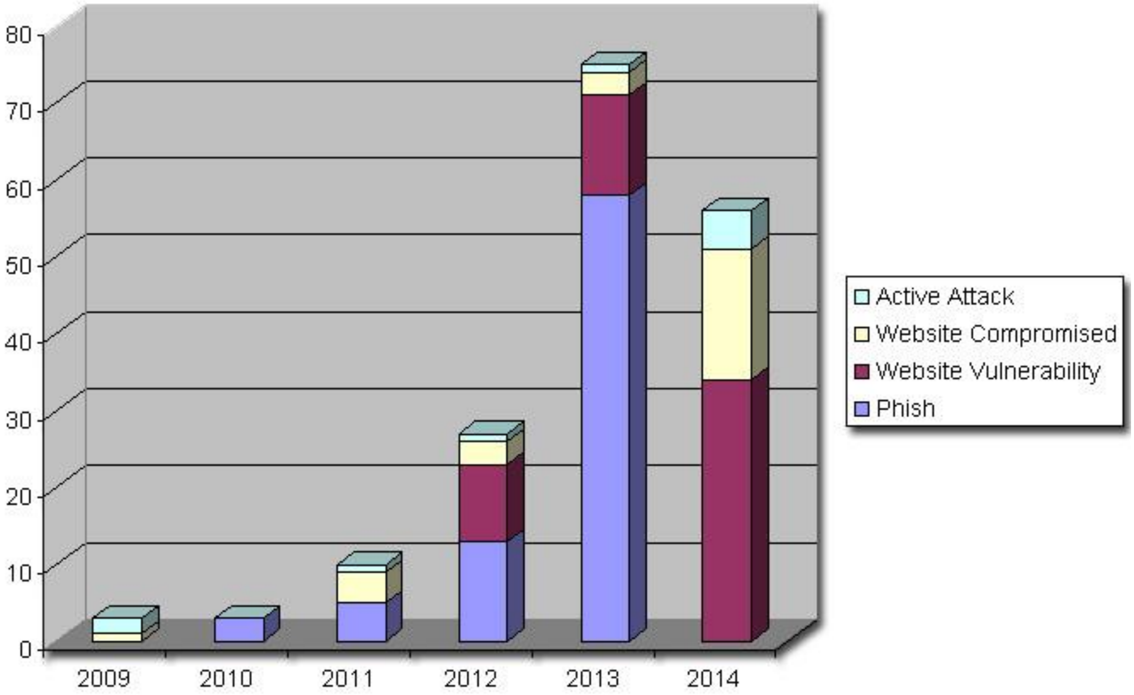
- Assisted in the APCERT Drill 2014 as OC, Player, Observer and EXCON
- Article publications in a local magazine called "Macau-ICT" magazine

2.1. 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.

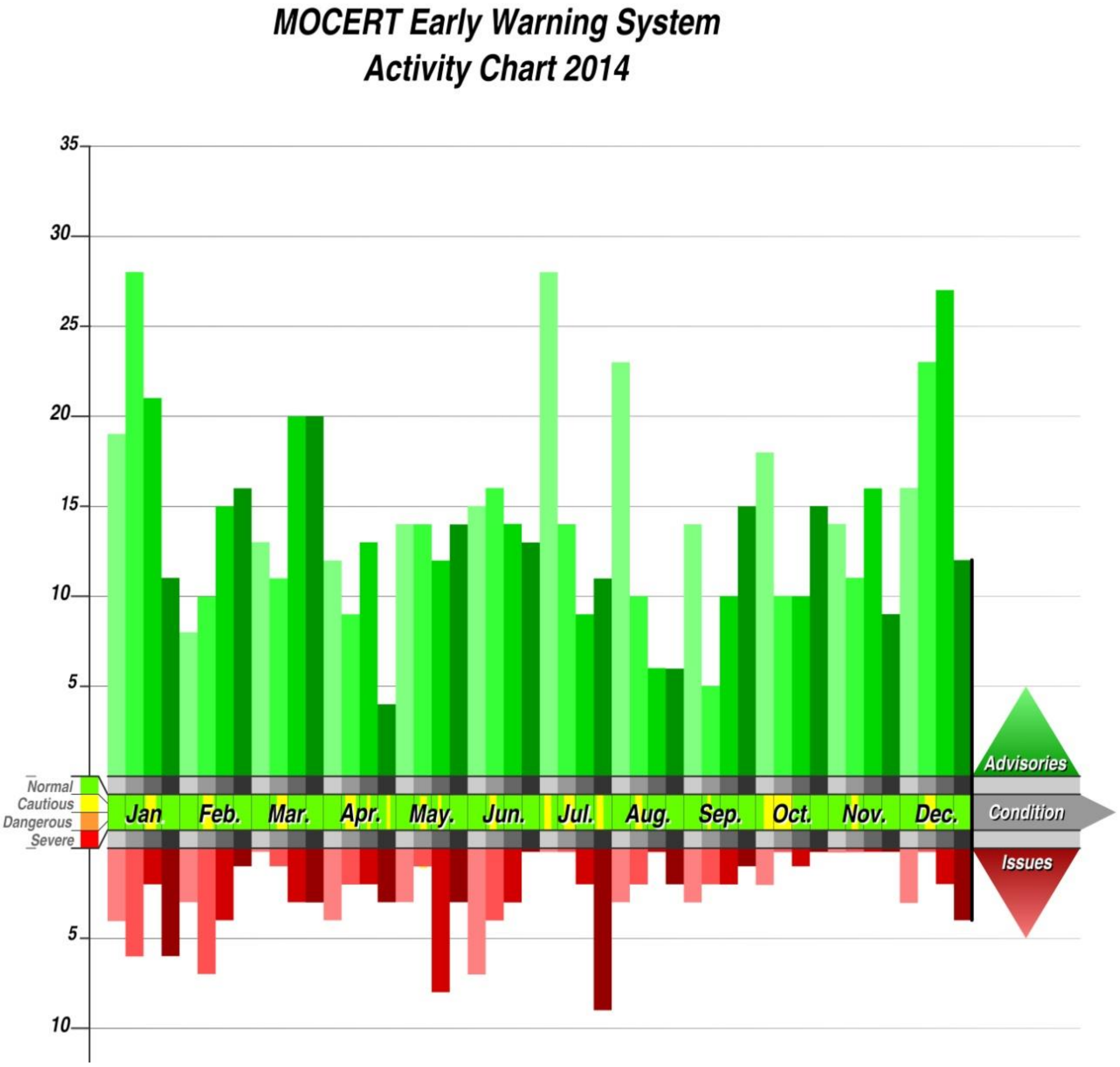
Sources of incidents are from three distinct channels.

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



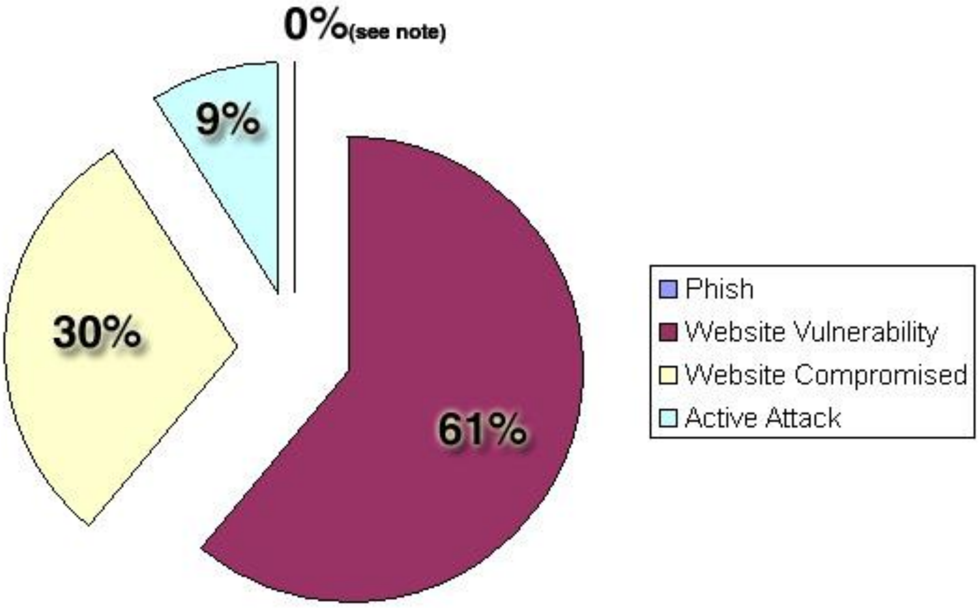
Early Warning Notices - A website collects notifications related to computer security, where all notifications are reviewed by staff to determine the impact to Macao constituency.

The notifications are then classified to Issues and Advisories and then posted. The following diagram shows the distribution of the 789 postings in 2014 with 670 postings being Advisories, and 119 Issues.



2.2. Abuse statistics

The following pie graph denotes the abuse distribution as noted for the year 2014. The numbers are drawn from the incidents handled with the removal of the "web notices" as they do not constitute an abuse.



note: Phishing Sources in 2014 handled incidents independently.

3. Events organized / co-organized

26th February 2014 - "Vapor Trails of Malware - Volatility"

The seminar was presented on the 26th February 2014 where it introduced the memory analysis framework called Volatility. This framework can be used by first line respondents and check of suspicious processes by accessing the information that resides in the memory of the computer

30th May 2014 - "OWASP Top 10 Mobile Security Risks"

The seminar was presented on the 30th May 2014 where the seminar provides information on the top ten (1) risks as listed by the Open Web Security Project (OWASP) and details the impact of the risk being realized and discusses about some prevention tips..

18th November 2014 - "DDoS Seminar"

The seminar was presented on the 18th November 2014 where the seminar reveals the impact of DDoS attacks temporarily or indefinitely interrupt or suspend services of a host connected to the internet.

20th November 2014 - "Cracks in the Pillars of IT Security" "Clean PC Day"

Titled "Cracks in the Pillars of IT Security" and "Clean PC Day"

Co-organized with Public Administration and Civil Service Bureau (SAFP) a string of seminars and a clean PC workshop to highlight the risks, and counter measures that internet users need to deal when using internet connected computers. This activity was held on the 20th November 2014, at Macau Science Center

3.1. 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.

3.2. Drills

The involvement in 2014 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 2014. The drill allowed for a better understanding of issues facing the CERT community outside of Macau and skill sets required to solve them. Similar level of involvement in the Organizing Committee for the 2015 drill has been sought.

3.3. Seminars

MOCERT attend both APCERT Taiwan and FIRST Boston meeting in the year 2014.

4. Achievements

4.1. Publication.

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

5. International Collaboration

5.1. Sensors

There are two (2) projects that MOCERT is involved in which are related to hosting a honey pot project

1. Tsubame for JPCERT-CC
2. Podrunner for DRG

6. Future Plans

MOCERT investigated cooperation with industry in handling and reducing the impact of phishing, which resulted in the incident reporter to be able to handle the events independently. Further work is needed on verifying latent vulnerabilities in the machines in Macau and proactive checking of machines on routable IP will need to be monitored closer in the coming year. Further effort in developing malware analysis skill sets will be very important for MOCERT's development.

7. Conclusion

2014 has been a year where our services metrics fluctuated as sources of incident changed and staffing number also changed. The major challenges up ahead are restructuring the team to restore capacity and functionality as further malware analysis and vulnerability scanning is sought. The changes envisaged will be beneficial to MOCERT's the constituencies as these changes are done progressively in the next few years to promote a clean and safe Internet.

MonCIRT

Mongolian Cyber Incident Response Team – Mongolia

1. About MonCIRT

1.1. Introduction

A Mongolian Cyber Incident Response Team (MonCIRT) is a Non Governmental, Nonprofit organization aimed to securing Mongolian Business sector's cyber space. MonCIRT provides Incident Prevention and Response services as well as Security Quality Management Services as allow our financial situation. MonCIRT perform the following functions in the area of cyber security:

- Collection, analysis and dissemination of information on cyber incidents, internet threats
- Forecast and alerts of cyber security incidents
- Consult to business entities in handling of cyber security incidents
- Issue guidelines, advisories, vulnerability notes and white papers on information security practices, procedures, prevention, response and reporting of cyber incidents
- Improve information security awareness, literacy, provide comprehensive trainings.
- Provide information on incident and vulnerability trends and characteristics
- Build an infrastructure of increasingly competent security professionals who respond quickly to attacks on Internet-connected systems and are able to protect their systems against security compromises
- Such other functions relating to cyber security as may be prescribed

MonCIRT services are available for all business entities, personals.

The MonCIRT helps constitutes to deal with its immediate problems and analyzes the scope and nature of the problems. To increase awareness of security issues and help organizations improve the security of their systems, we continue to disseminate information through multiple channels:

- telephone and email
    - hotline: + 976 - 70113151
    - email: info@moncirt.org.mn

- World Wide Web: http://www.moncirt.org.mn/

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, entities and business sector.

1.1.2. Workforce

MonCIRT currently has a total of 6 constant staffs such as: executive director-1, experts 3, the bookkeeper 1, system administrator-1. Due to lake of financial support and self financing we constantly feel shortage of the qualified experts.

1.1.3. Constituency

Currently MonCIRT‘s constituency encompasses the Business Sector of Mongolia because government organizations covered by Cyber Security Authority of Mongolia by law. Therefore our constituency consist of business companies, private sector organizations, NGO and general public. We works closely with Chief Information Officers and system administrators of business sector. In 2014 we approved MonCIRT’s new regulations, procedures and launched new web site, email system.

2. Activities & Operations

2.1. Activities

The summary of activities carried out by MonCIRT during the year 2014 is given in the following table:

Activities	Year 2014
Security Incidents handled	193
Security Alerts issued	105
Advisories Published	9
Vulnerability Notes Published	36
Security Guidelines Published	1

Trainings Organized	4
Mongolian Website Defacements tracked and advised	32
Open Proxy Servers tracked	3
Bot Infected Systems tracked	424
Phishing (mirror) web sites tracked and removed	6
Projects	1

This part of the report describes the statistics of team activities and security incident reports handled by MonCIRT, both from external and internal sources. In 2014 MonCIRT handled manually 193 incidents. Similarly to the previous years, most of them were related to fraud (around 48%), malware (nearly 26%) and spam (over 13%). Mostly, submitters and victims were coming from IPs belonging to companies (respectively 61.8%, and 49%) and usually were foreign (80.3% and 40.3%), while the attackers were unknown in 88.6% of the cases. In 2014 we registered a large number of identity theft incidents. The scale of the problem was similar to that in 2013. It should be emphasized that it were phishing incidents both when the sites were located on Mongolian servers and when the attack targeted Mongolian institutions. From the global perspective, the scale of the problem was much larger. In June and July we observed an increasing number of phishing attacks launched against on-line banking and social sites customers. Criminals were sending emails, allegedly in the name of the bank, on a mass scale. However, the most serious attacks on Mongolian on-line banking customers were launched with the use of malicious software such as ZeuS or Citadel. The attacks were carried out in several scenarios. In the first one criminals sent a fake message which informed victim about an incorrect wire transfer and an obligation to return funds (of course to the money mule's account). In another scenario, when a user wanted to perform wire transfer, malicious software changed the number of target account. Phishing attacks overwhelmingly come from popular and trusted web sites hacked by cybercrime.

From January through December 2014, the MonCIRT received 286 email messages and more than 130 hotline calls reporting computer security incidents or requesting information. 108 of these messages, information was related with real incidents and we provided with recommendations. We received 34 vulnerability reports and handled 37 computer security incidents during this period. We cannot retrieve incident handling statistics from organizations, administrators due to executive's restriction.

We continue to provide advice to system administrators in the Internet community who report security problems. We working now on establishing of regular chat system with administrators of organizations and to offer information on state of Internet security to the system administrators, network managers, and others in the Internet community.

2.2. Threats

Malware and the malicious web

- The year began Gameover ZeuS peer-to-peer botnet activities which is also responsible for distributing Cryptolocker ransomware. Gameover ZeuS is a banking trojan that aims to steal banking and other sensitive private information. If this fails to deliver significant financial information, the criminals can deploy Cryptolocker, which encrypts your personal files on your computer and then attempts to extort money out of you in return for the decryption key. Without the key the files are permanently locked and the only way to recover the contents is from backup files.
- The National Cyber Security Authority (NCSA) led the Mongolian effort in the global operation. Partnering with NCSA, MonCIRT provided dedicated page with information and explanations, as well as links to tools that would scan to determine if you were infected as well as cleaning up infected hosts. NCSA also provided useful advice about how the malware spreads and how you can defend yourself against it.
- In 2014 more personal details, such as email addresses, passwords (both encrypted and clear text), and even national ID numbers were put on public display.
- Based on data for 2014, 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.
- The relative volume of the various alerts can help to describe how attacks are established and launched. They also frequently provide hints about how methods have evolved. Based on this, the main focus in 2014 may have been

the subversion of systems, with larger coordinated attacks being executed across fairly broad swaths of 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.

2.3. Incident trends

In 2014 we was a major reporting center for incidents and vulnerabilities in private sector and established MonCIRT reputation for discretion and objectivity among business organizations, general public. As a result of connection with NDC's monitoring system, IPS and Tsubame system and sharing of attack data we able to obtain a broad view of incident and vulnerability trends and characteristics.

The MonCIRT, in conjunction with law enforcement, performed extensive analysis of the control system and historical trending data around the four dates provided by the asset owner. The team was unable to conclusively determine if the suspected employee had unauthorized access on the date of the overflow or if that access resulted in the basin overflowing. The factors that significantly contributed to the inconclusive findings included:

- Each host did not record logon events
- Typically, only one username was used throughout the network
- A lack of network monitoring systems in place to verify the alleged activity
- Logging was not enabled or was irrelevant for any of the remote access tools seen on the hosts (pcAnywhere, RealVNC, NetVanta VPN client, Windows Remote Desktop)
- Operating system records were eliminated due to the age of reported access event.

In 2014 we handled incidents shown on figure 1.

TYPE OF INCIDENT	NUMBER	PERCENTAGE
Abusive content	26	13.6%
Spam	21	11.1%
Harassment	1	0.5%
Child/Sexual/Violence	1	0.5%
Unclassified	3	1.5%
Malicious code	51	26.7%
Virus	5	2.5%
Worm	3	1.5%
Trojan	32	16.7%
Spyware	1	0.5%
Dialer	0	0
Unclassified	10	5.5%
Information gathering	7	3.5%
Scanning	5	2.5%
Sniffing	0	0
Social engineering	1	0.5%
Unclassified	1	0.5%
Intrusion Attempts	3	1.5%
Exploiting of known vulnerabilities	1	0.5%
Login attempts	1	0.5%
Exploiting of unknown vulnerabilities		
Unclassified	1	0.5%
Intrusions	5	2.5%
Privileged Account Compromise	2	1.0%
Unprivileged Account Compromise	3	1.5%
Application Compromise	0	0
Unclassified	0	0
Availability	12	6.2%
Denial-of-service attack (DoS)	4	2.0%
Distributed denial-of-service attack	7	3.7%

(DDoS)		
Sabotage	0	0
Unclassified	1	0.5%
Information Integrity	7	3.5%
Unauthorized Access to Information	5	2.5%
Unauthorized Modification of Information	1	0,5%
Unclassified	1	0.5%
Fraud	82	42.5%
Unauthorized Use of Resources	3	1.5%
Copyright infringement	5	2.5%
Identity theft	65	33.9%
Unclassified	9	4.6%

In May there was a new version of a malicious mobile software. Criminals displayed to a victim a message informing her that she should install an E-Security certificate on her smartphone in order to improve the bank transactions security. When the installation was finished, the phone became infected by malware. It gave criminals the ability to send fake text messages. When the scenario with E-Security ceased to be effective, criminals invented a new scheme with fake antivirus program which allegedly was expected to prevent cases similar to E-Security. Once again it took control over victim's phone. The malware VBKlip proved to be unique and brilliant in its simplicity. Every time a user copied a bank account number, the malicious application switched this number with another one, provided by the criminals. The application was very effective and difficult to detect. Despite a significantly lower number of incidents connected to these scenarios, they are much more dangerous in comparison to classic phishing cases and affect larger groups of people.

For many of these incidents it was found that attackers gained access to the server in generally one of two ways:

1. Weak passwords on administrator accounts
2. Unpatched software, including website plugins

Defending against either of these is simple and straight-forward – use strong and unique passwords for administrator accounts and ensure that all software is kept patched and up-todate, including any plugins that maybe used (e.g. WordPress Plugins).

2.4. New services

2.4.1. New bilingual web site in English and Mongolian

In 2014 MonCIRT developed and deployed bilingual (English and Mongolian) web site, new reliable email system. On the new web site we publishing constantly the security advisories, alerts, vulnerability notes.

2.4.2. Setting up new CSIRT

We supporting the establishment of new CSIRT at Ministry of Defense. We provided MoD with guideline for establishment of CSIRT, draft procedures.

3. Events organized / co-organized

3.1. Training / Education

In 2014 the MonCIRT organized workshops and trainings focused on targeted audience such as government and financial sector IS officers, System Administrators, ISPs etc. 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 2014 included the following:

- *Network security management and configuration*
- *Information Security System of Organization based on MNS ISO/IEC 27001*
- *Internal Information Security audit and Self evaluation*
- *Network Monitoring*
- *Fundamentals of Incident Handling and Management*

In addition MonCIRT organized following workshop:

« Workshop on "Advanced Persistent Treats" on April 21, 2014

3.2. Drills

In 2014 MonCIRT cannot organize local network security drill-IV due to financial limitation and economic crisis.

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 ICTPA expo 2014 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.

b. With sponsorship of Security Solution Service LLC and National Data Center organized annual "Security Open Day Mongolia 2014" and "Kharuul Zangi 2014" the ethical hacking contest in August.

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" 2014 conference on themes "Modern APTs and how to combat with them".

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 9 advisories and 36 vulnerability notes in 2014. Among the criteria for developing an advisory are the urgency of the problem, potential impact of intruder exploitation, and existence of a software patch or workaround. On the day of release, we send advisories to a mailing list of MOSA 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

No Certification and Memberships obtained in 2014:

5. International and Domestic Collaboration

5.1. MoU

We offered to sign MOU with National Cyber Security Authority on close cooperation and information sharing and waiting for positive reply.

5.2. Event participation

Our representative participated in 3d specialized conference "Protection of Industrial Networks - SAINT-PETERSBURG 2014" held in Saint Petersburg, Russia in 26-27 November.

5.3. International incident coordination

Upon request of some security companies from Europe, Italian and Poland CERTs we handled incidents related to 6 phishing web sites installed illegally in Mongolian web servers.

6. Future Plans

6.1. Future projects

We now working on development of all necessary documents, handbooks of CSIRT in Mongolian language. In addition our experts will train staffs of expected MoD

CERT. Also the General Authority for Border Protection (GABP) expresses interest to implement project on creation of CSIRT within GABP in 2015.

6.2. Future plan

In relation with our new regulation it is planned to reorganize our membership procedure and expand our operation, establish new services aimed on Business sector entities.

7. Conclusion

Due to constant financial difficulty MonCIRT gives the basic attention on the new financing strategy, proactive and quality management services including educational program, awareness campaigns, presentations and publications 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 will act as an real general private sector oriented CSIRT

To help new appearing CSIRTs MonCIRT develops methodological guides, incident handling guide, CSIRT setting up guide on Mongolian and updated CERT handbook (on Mongolian) and will use these materials for establishment of MoD CERT and GABP CERT.

We will continue to conduct the Annual "Security Open Day" and will organize National Conference on Cyber Security under name "InfoSec Mongolia 2015" while finding new ways to reach an even wider audience.

MonCIRT shall continue to participate in regional events of APCERT and will begin to participate in FIRST events and join to FIRST.

Contact Information

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

.

Incident Response Help Desk

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

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 started its operation as the Malaysia Computer Emergency Response Team (**MyCERT**) in 1997 and in 2009, established as CyberSecurity Malaysia by providing services in the area of Digital Forensics, Cyber Security Assurance, Information Security Best Practises, Security Policies, Outreach Programs and Information Security Professional Development. Currently, CyberSecurity Malaysia has more than 150 staff.

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 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, the agency has developed various services for the country 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. Malaysia Common Criteria Certification Body (MyCB);
viii. Cyber Security Professional Development;
ix. Outreach Programmes; and
x. Cyber Security Policy Research.

For the APCERT Annual Report, CyberSecurity Malaysia is emphasising on the services and activities provided by MyCERT, as the relevant department for this collaboration.

More information about CyberSecurity Malaysia can be found at: http://www.cybersecurity.my/en/

2. THE MALAYSIA COMPUTER EMERGENCY RESPONSE TEAM (MyCERT)

MyCERT provides point of reference for the Internet community in Malaysia to deal with computer security incidents. It provides assistance in handling cyber security incidents such as intrusion, identity theft, malware infection, cyber harassment and other computer security related incidents.

Currently, MyCERT operates the Cyber999 computer security incident handling and response help centre as well as the CyberSecurity Malaysia Malware Research Centre.

More information on MyCERT can be viewed at: http://www.mycert.org.my/en/

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/en/ displays the channels to report security incidents, internet abuses and grievances to the Cyber999 Help Centre.

To date are:

i. Responded to 11,918 incidents, with 98% incident resolution;
ii. Increased in receiving more data feeds related to incidents originating from Malaysia;

iii. Successfully handle high profile incidents such as Advanced Persistence Threat (APT) attacks, Trojans, and mobile phone malware;
iv. Automate the incident response processes; and
v. Launched Cyber999 Mobile Apps for Internet users to report incidents.

2.2. Malware Research Centre (MRC)

MyCERT also manages the CyberSecurity Malaysia Malware Research Centre (MRC) 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 provides opportunity to strengthening and understanding the threats. Among the activities of the MRC are as follows:

i. Conduct research and development work in mitigating malware threats;
ii. Produce advisories and reports related to the latest threats;
iii. Monitor threats via the distributed Honeynet project; and
iv. Collaborate in malware research with Universities, CERT's and international organizations.

2.3. Constituency

MyCERT's constituency is the Malaysian Internet Users. Incidents within Malaysia that have been reported either by the Malaysian public or international organizations will be resolved by assisting on technical matters. If the reported case involves international connection, MyCERT will request trusted parties in that particular country or constituency 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 2014, MyCERT has produced the following cyber threat notifications:

i. 38 Advisories
ii. 32 Alerts

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

http://www.mycert.org.my/en/services/advisories/mycert/2014/main/index.html

MyCERT under its Cyber999 service has successfully resolved more than 98% out of 11,918 incidents reported, an increase of 12% incidents reported compared to the year 2013. The bulk of the reported incidents was related to Fraud (37.6%) and followed by Spam (30.6%) and Intrusion Attempt (10.9%).

Other significant cases reported, according to the percentage of report were Intrusion (9.4%), Malicious Codes (6%) and Cyber Harassment (4.6%).

The figures below show the reported cases handled by MyCERT for the year 2014:

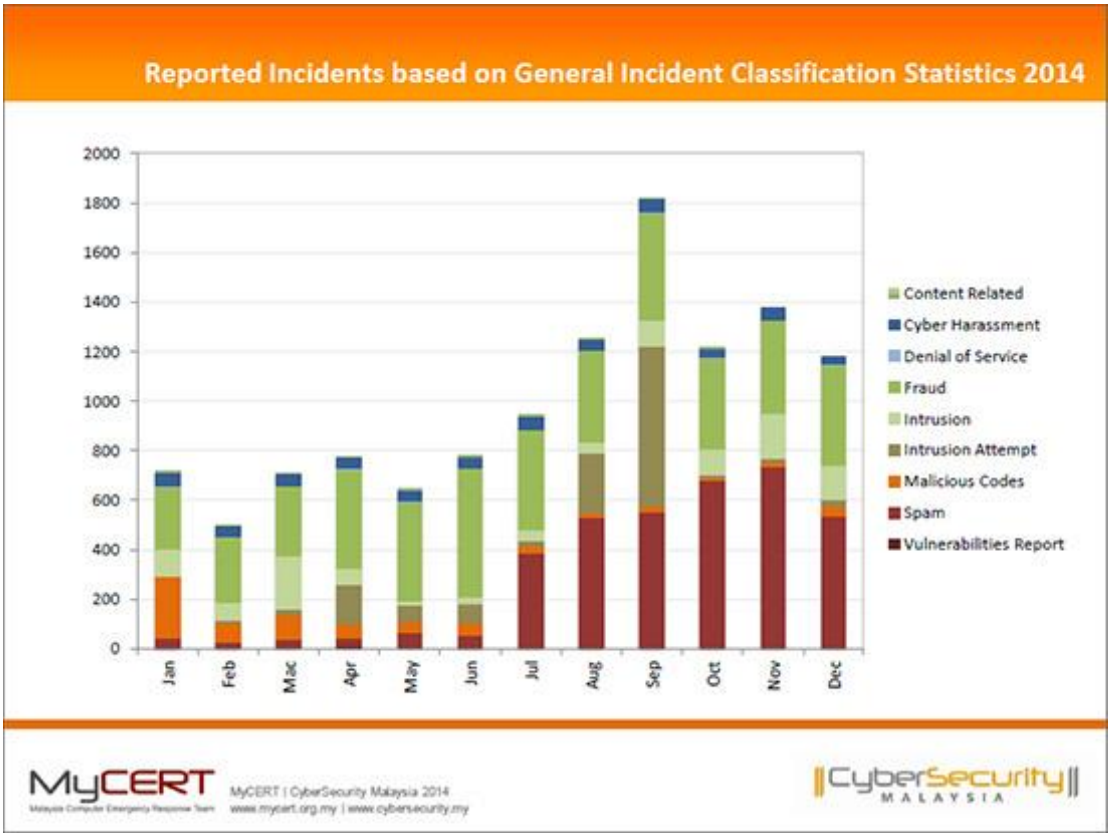


Figure #1: Reported Incidents handled by MyCERT in 2014

Further information on Cyber999 statistics can be viewed at:

http://www.mycert.org.my/en/services/statistic/mycert/2014/main/detail/949/index.html

2.5. MyCERT's Events Involvement And Achievements

MyCERT has actively participated in providing support for IT security events by 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 OIC-CERT Cyber Drill. This international exercise was conducted on June 4, 2014. 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 twelve (12) countries had participated in the exercise.

Besides the OIC-CERT Cyber Drill, MyCERT has also involved in three (3) other international Cyber Drills, namely:

i. APCERT Drill (19th February 2014);
ii. IMPACT International Cyber Exercise (13th May 2014); and
iii. ASEAN CERT Incident Drill – ACID (24th September 2014).

2.5.2. Trainings

Several workshops or hands-on training were conducted by MyCERT in year 2014 which includes:

i. Incident Handling and Network Security (IHNS) Training for Private and Government Sectors;
ii. Incident Handling and Network Security (IHNS) Training for Nigeria CSIRT; and
iii. Workshop on Cyber999 Customer Relations Management (CRM) System for local Law Enforcement Agencies (LEA).

2.5.3. Presentations

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

i. Artificial Intelligence & Computer ScienceAICS 2014, Bandung, Indonesia, 15 September – 16 September 2014;
ii. APCERT AGM & Conference 2014, Taipei, Taiwan, 18 – 21 March 2014;
iii. National CSIRT Meeting 2014, Boston, USA, 28 – 29 June 2014;
iv. OIC-CERT Annual Conference and AGM 2014, Bandar Seri Begawan, Brunei, 20 – 22 October 2014; and
v. Tokyo International Conference on Engineering and Applied ScienceTICEAS 2014, Tokyo, Japan, 17 – 19 December 2014.

2.5.4. Tools Developed

i. Cyber999 Mobile Application for Android and iOS (Apple);
ii. Android Sandbox; and
iii. HeartBleed Verification Site.

2.5.5. Paper Publication

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

i. Title: Automated Enhancement Tool for Malware Incident Handling;
Published: Artificial Intelligent Computer System (AICS 2014);
Proceedings.
ii. Title: Automating Big Data Analysis: Malaysia CERT Experience;
Published: Proceeding of the Tokyo International Conference on Engineering and Applied Sciences 2014.

2.5.6. Social Media

Technological advancement through social media has provided invaluable tool for MyCERT to disseminate information across a wide audience. MyCERT through Facebook account https://www.facebook.com/mycert.org.my had gathered 1,782 likes and 947 followers at MyCERT Twiiter account https://twitter.com/mycert.

Being the technical reference centre of the country, MyCERT has been invited by the media organizations for radio and television interview on cyber security related matters.

3. INTERNATIONAL COLLABORATION

The Malaysian National Cyber Security Policy identified International Cooperation as one of the areas in enhancing cyber security. In line with this, CyberSecurity Malaysia has been actively involved in establishing collaborative relationships with foreign parties.

3.1. Working Visits

CyberSecurity Malaysia made several working visits to various international organizations to further enhance the country's cyber security condition. The objective of the visit is to seek potential collaboration in knowledge exchange. Among the visits are:

i. University of Oxford e-Research Center;
ii. University of Surrey;
iii. Trend Micro CSIRT, Taiwan;
iv. Myung Information Technologies Co. Ltd (MIT Korea); and
v. CERT-UK.

CyberSecurity Malaysia also received several working visits from foreign organizations who have the similar objectives, such as from:

i. International IT University, Kazakhtan;
ii. The Republican State Enterprise Technical Service. Kazakhtan;
iii. Ministry of Awdaf and Islamic Affairs, Kuwait; and
iv. Organization of the Islamic Cooperation, Saudi Arabia

3.2. Memorandum of Understanding (MoU)

Listed below are the official collaborations in the area of cyber security between CyberSecurity Malaysia and international organizations:

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 Center 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; and
xi. Indonesia Security Incident Response Team On Internet Infrastructure/ Coordination Centre (ID-SIRTII/CC), Indonesia.

3.3. New Partnership and Existing Cooperation

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

i. 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. Chair of the World Trustmark Alliance (WTA).

4. FUTURE PLANS

Since the establishment of CyberSecurity Malaysia, the agency strives to improve the service capability and encourage local Internet users to report security incidents to 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.

In order to achieve the world-class capability, CyberSecurity Malaysia will relentlessly encourage its staffs to be information security certified. This will assist the staffs to improve their contribution by sharing of their knowledge and experience in the security field. This is done by attending trainings, presentations and publications in international security events.

Development of in-house tools in mitigating security threats are planned and developed to assist the public and industry to secure and utilize their computer when performing online activities.

To encourage safer cyber environment, CyberSecurity Malaysia realizes the need to work together with local and international security organizations through the establishment of formal arrangement such as Memorandum of Understandings (MoU), seminars and conferences such as:

i. Hack in the Box Conference;

ii. International Conference on Prevention and Suppression of Hi-Tech Crime;

iii. Malaysian Internet Governance Forum; and

iv. The Meridian Conference and Critical Information Infrastructure Protection;

The agency will continue to organize events such as the Cyber Security Malaysia - Award, Conference and Exhibition (**CSM-ACE**), the 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.

With such understanding, CyberSecurity Malaysia supports newly established Computer Security Incident Response Team (CSIRT) by providing advise and assistance especially in becoming members to international security community such as APCERT, FIRST and OIC-CERT.

5. CONCLUSION

CyberSecurity Malaysia, observes an increase in computer incidents that were reported to Cyber999 Help Centre in 2014 compared to the previous year. This agency will continuously working with the constituencies and international allies to generate useful cooperation in safe guarding the cyber environment.

In line with the Malaysian National Cyber Security Policy that is emphasis 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 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. New cooperation between CyberSecurity Malaysia and other security organization had been created especially concerning mobile security and malware threats. CyberSecurity Malaysia will continuously pursue new cooperation with cyber security agencies in this region and globally in its effort to make cyberspace a safer place for all.

NCSC

New Zealand National Cyber Security Centre – New Zealand

1. About NZ NCSC

1.1. Introduction

The role of the New Zealand National Cyber Security Centre (NCSC) is to improve the protection of Government systems and information, to receive, plan and respond to significant cyber security incidents, and to work with the providers of critical national infrastructure, to improve the protection and computer security of such infrastructure against cyber-borne threats.

The statutory basis for this mission are the Government Communications Security Bureau Act 2013 and the Telecommunications (Interception Capability and Security) Act 2013. These articulate the information infrastructures we are mandated to work with and our approach to managing security risks on critical telecommunications networks.

In support of this mission we provide a range of specialist services in the area of cyber security and communications security technologies.

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;
- 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)

1.1.2. Workforce

The NCSC comprises of a team of cyber security focussed relationship, technical, policy and incident coordination professionals.

1.1.3. NCSC Customers

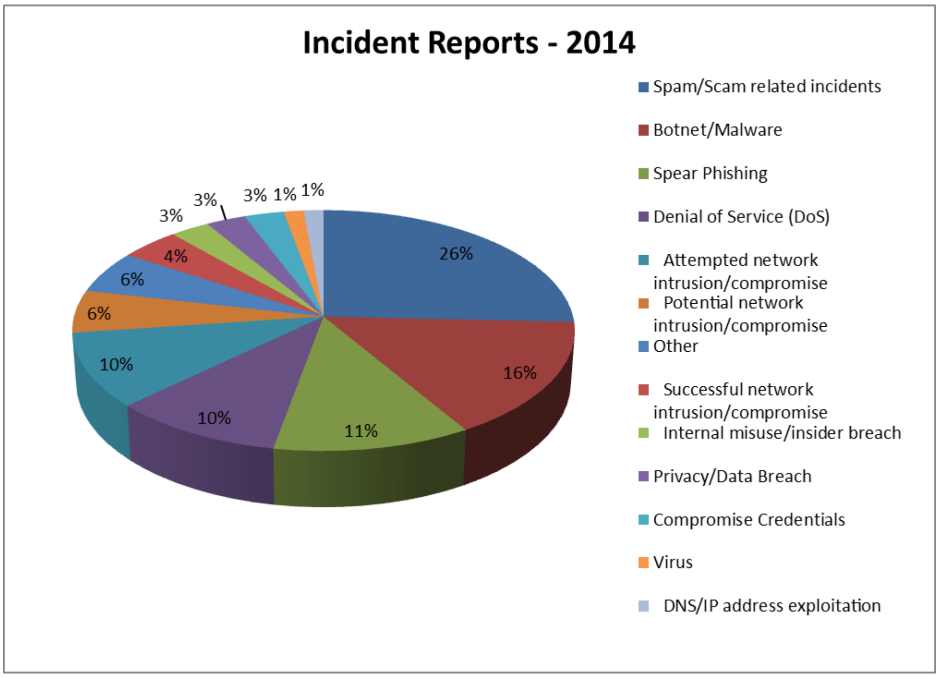
Primarily New Zealand government agencies, law enforcement, Critical National Infrastructure operators, registered New Zealand Network Operators and other key industry stakeholders, in addition to wider engagement with other customers in the private sector.

2. Activities and Operations

2.1. Incident handling reports

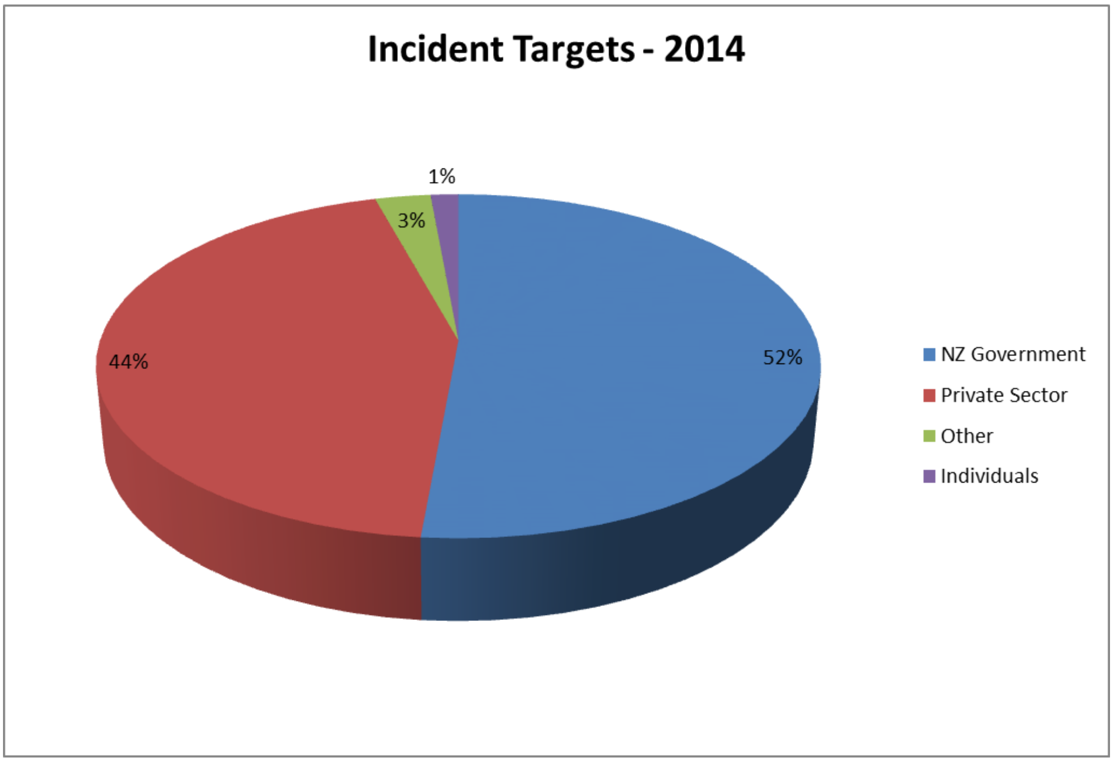
In 2014, the NCSC received a total of 70 incident reports which met the reporting criteria. The largest category of Incident Report type (fig 1.1) was scam and scam related incidents, these made up 26% of the incidents captured. Botnet/Malware and Spear Phishing with the second most reported categories making up 16% and 11% of incidents respectively. Attempted network intrusions/compromises and Denial of Service attacks also made up a significant number of incidents reported at 10% each.

Fig 1.1



Of the customers that were targeted (fig 1.2) the New Zealand Government reported the majority of the incidents. The private sector reported slightly less than half of the incidents reported to the NCSC at 44%. The Government and Private sector customers incidents reported represent 96% of all of the incidents reported to the NCSC in 2014. This highlights the NCSC's increased focus on both the Government and Private sectors.

Fig 1.2



2.2. The Telecommunications Intercept Capability and Security Act (TICSA)

The Telecommunications Interception Capability Act (TICA) was replaced in 2014 with the Telecommunications (Interception Capability and Security) Act (TICSA).

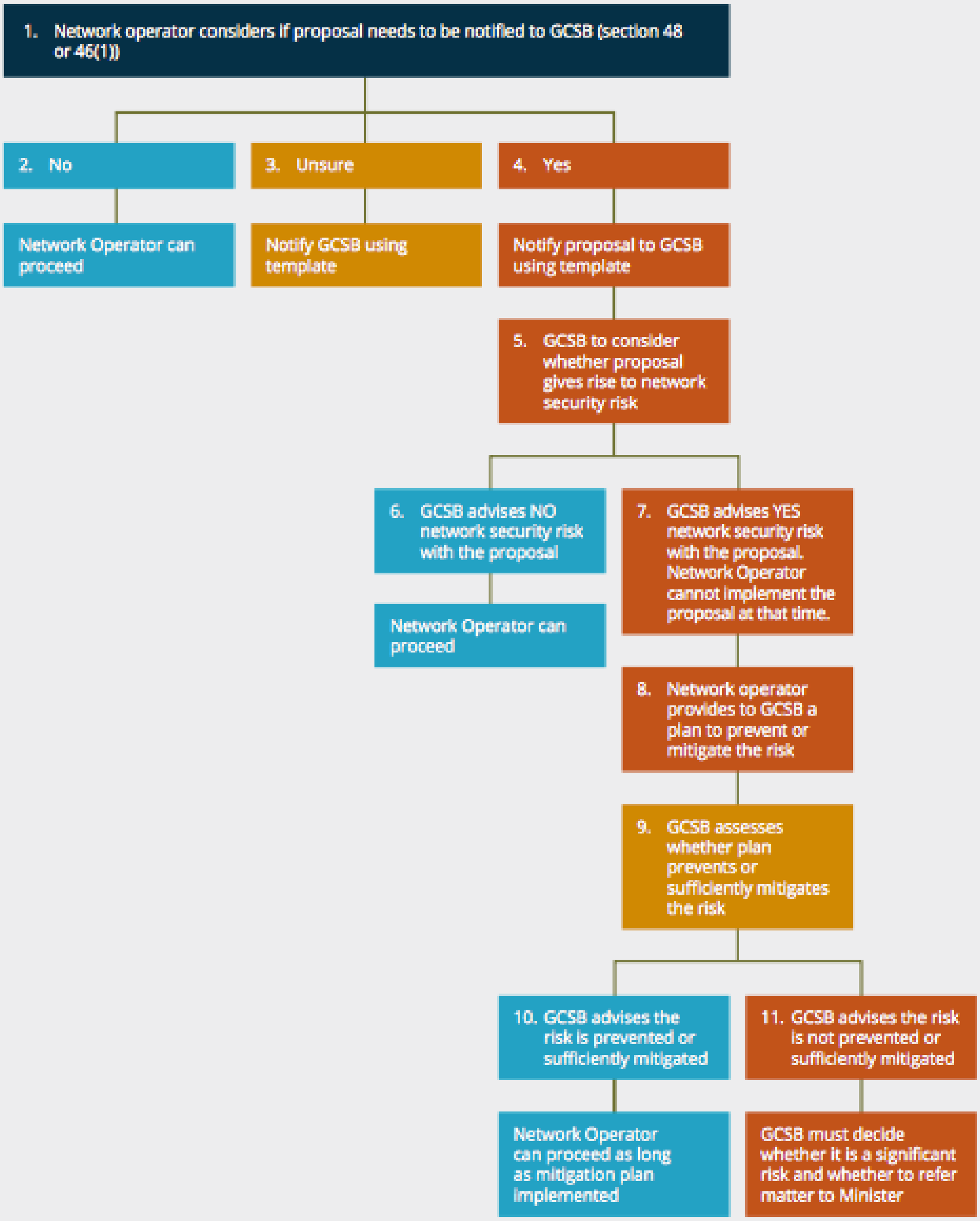
The TICSA is designed to assist network operators and the NCSC to work co-operatively and collaboratively with each other, so that network security risks can be identified and addressed as early as possible.

The NCSC works together with New Zealand network operators in an on-going dialogue based on good faith to ensure the TICSA network security process is implemented and operates in a pragmatic and practical way for the New Zealand telecommunications industry.

The NCSC has worked in consultation with New Zealand telecommunications industry to provide guidance to the TICSA and has published the TICSA guidance paper. The guidance paper can be located at http://www.ncsc.govt.nz/assets/TICSA/TICSA-Guidance-July-2014.pdf

The TICSA process (fig 2.1) can also be found in the TICSA Guidance paper.

Fig 2.1


1. Network operator considers if proposal needs to be notified to GCSB (section 48 or 46(1))
2. No
3. Unsure
4. Yes
Network Operator can proceed
Notify GCSB using template
Notify proposal to GCSB using template
5. GCSB to consider whether proposal gives rise to network security risk
6. GCSB advises NO network security risk with the proposal
7. GCSB advises YES network security risk with the proposal. Network Operator cannot implement the proposal at that time.
Network Operator can proceed
8. Network operator provides to GCSB a plan to prevent or mitigate the risk
9. GCSB assesses whether plan prevents or sufficiently mitigates the risk
10. GCSB advises the risk is prevented or sufficiently mitigated
11. GCSB advises the risk is not prevented or sufficiently mitigated
Network Operator can proceed as long as mitigation plan implemented
GCSB must decide whether it is a significant risk and whether to refer matter to Minister

Note: A proposal may be withdrawn at any time by supplying notification in writing to the GCSB.

The TICSA came into effect on 11 May 2014, there are now 138 registered Network Operators with a good number of TICSA notifications of proposal being submitted to the TICSA team within the NCSC for consideration.

Common feedback from the Network Operators includes that the TICSA has assisted with enhancement of the existing Security Industry best practices and that Network Operators are making use of the NCSC TICSA team as an extension to their existing Security Governance checks. The TICSA has contributed to further enhanced awareness on the importance of Security for all Network Operators.

2.3. Additional Activities during the period

In addition to receiving incident reports and the TICSA, the NCSC:

- Issued unique advisories to customers;
- Produced content for and highlighted significant issues via the NCSC website;
- Coordinated and hosted industry engagement forums (Security Information Exchanges i.e. Scada voluntary standards created;
- Participated in the NZ Internet Task Force (NZITF), a domestic security community, to promote collaborative approaches to security issues;
- Supported the launch and ongoing establishment of the NZ Connect Smart. Connect Smart is a partnership that promotes ways for individuals, businesses and schools to protect themselves online. (www.connectsmart.govt.nz)
- Produced an updated New Zealand Information Security Manual (NZISM) including consultation with customers and integration into the updated New Zealand Protective Security Requirements (PSR).
- Worked with Government and private sector customers to provide a unique range of cyber security services.

3. Events organised / co-organised / attended

3.1. International Collaboration

The NCSC has been through a period of review and growth throughout 2014. Participation in APCERT and other international operations was been challenging due to resource constraints.

3.1.1. Future International Collaboration

The NCSC will actively participate in activities with the APCERT forum.

3.2. Industry Engagement

The NCSC organised and hosted several industry and government engagement forums, held at regular intervals throughout the year.

3.3. TICSA Consultation

The NCSC completed a four month consultation process with New Zealand Network Operators on the TICSA. This included;

- presentations at the New Zealand Network Operators annual conference
- customer TICSA consultation meetings; and
- a final walk through of the TICSA guidance paper prior to the TICSA coming into effect on 11 May 2014.

3.4. 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.

3.5. Training

The NCSC helped to prepare and participate in a number of training activities through the NZITF, Weltec and other forums.

3.6. Drills

The NCSC worked with other Government agencies in a cyber drill in preparation for the 2015 Cricket World Cup.

4. Presentations

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

- AusCERT Conference, Australia
- Kiwicon, New Zealand

- NZITF Conference, New Zealand
- Business groups including NZ Institute of Directors and various Boards

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 has been through a process of review while also maintaining a domestic focus on engagement across a number of sectors and the introduction of the TICSA. It will now seek to build on the new 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. About SingCERT

1.1. 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.

1.1.1. Establishment

SingCERT was set up in 1997 to facilitate the detection, resolution and prevention of security related incidents on the Internet. SingCERT is a government funded national initiative, and is managed and driven by the Infocomm Development Authority of Singapore.

1.1.2. Constituency

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

2. Activities & Operations

2.1. Incident Reports

There is a increase in the total number of incidents reported to SingCERT in the year 2014 as compared to the year 2013.The significant increase in the reported incidents were due to the reported defacement of websites incidents. The incidents included defacement both to the government and public sectors' websites. SingCERT continues to work with other CERTs and our Internet Service Providers (ISPs) to track down affected users and keep them informed on how to secure their systems. On the regional and international fronts, collaboration and cooperation among CERTs have proved effective in the resolution of our cross-border incidents.

3. Events organised / co-organised

3.1. Seminars and Workshops

In our continued efforts to keep our constituency updated on security trends and developments, SingCERT organised 4 seminars plus workshops for the year 2014. These events were co-organised with industry partners to bring the latest technology and knowledge to our security practitioners.

3.2. ASEAN CERTs Incident Drill 2014

The ASEAN CERTs Incident Drill (ACID) 2014 was conducted successfully on 24 September 2014. In order to develop scenarios which reflected prevailing cyber threats that were confronting the CERTs, the theme selected for the drill was focused on participants playing the roles of hackers and incident responders. 13 CERTs from 12 countries from ASEAN and Asia took part in the drill, and good feedbacks were received from all the participants.

4. International Collaboration

4.1. Incident Drill

- SingCERT organised the ASEAN CERT Incident Drill (ACID) in 24 September 2014
- SingCERT participated in the APCERT Annual incident drill in 18 March 2015.

5. Future Plans and Projects

5.1. ACID Drill

SingCERT will be organising the 10th ASEAN CERTs Incident Drill for the year 2015. 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. About Sri Lanka CERT|CC

1.1. 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.

1.1.1. 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 about the latest threats and vulnerabilities affecting computer systems and networks, and a source of expertise to assist the nation and member organizations, in responding to and recovering from Cyber-attacks.

It was anticipated that cyber security incidents in Sri Lanka would increase dramatically due to IT infrastructure growth as a result of the National ICT Policy related activities, primarily, the e-Sri Lanka initiative and the rapid development of IT/BPO Sector. Sri Lanka CERT therefore 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.

In early 2011, Sri Lanka CERT | CC, along with its parent body, ICTA was brought under the purview of the newly formed Ministry of Telecommunications and IT.

Sri Lanka CERT|CC is presently under the purview of Ministry of Foreign Affairs from January 2015 and is fully financed by the state budget.

1.1.2. Workforce

Sri Lanka CERT|CC has a total staff strength of ten team members consisting of the Chief Executive Officer, Manager Operations, Principal Information Security

Engineer, Senior Information Security Engineer, Information Security Engineer, Information Security Analyst, three Junior Information Security Analysts and an Officer-in-charge of HR & Admin. This team is supported by four 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.

1.1.3. 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 and Operations

2.1. Activity Summary

Sri Lanka CERT|CC maintains an inter-dependent structure, with expertise in the field of cyber security that has the capacity to prevent, analyze, identify and respond to cyber security incidents that threaten Sri Lanka's national cyber-space.

As the national contact point for matters relating to cyber security incidents, during 2014 (1st of January – 31st of December), Sri Lanka CERT|CC was informed by various domestic or international partners about various cyber security incidents/vulnerabilities that affected/may affect our national cyber-space, as follows;

- Compromised unique IP's extracted from the information collected by

automated systems
- Vulnerabilities on applications, operating systems and firmware etc.

This report analyzes the cyber security incident information collected / managed by Sri Lanka CERT|CC in 2014, 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;

- Approximately 90% of the incidents refer to systems in Sri Lanka that have been compromised through the exploitation of some technical vulnerability and got infected with different versions of malware and have become part of a botnet; the total number of unique IPs identified is around 750.
- 85% of the compromised IPs refers to systems in Sri Lanka which had become zombies of Sirefef/ZeroAccess botnets.
- 90 % of all the unique compromised IPs reported to Sri Lanka CERT|CC, were identified as running Microsoft Windows operating systems, versions 98, 2000, XP or 2003;
- Over 20% of the phishing incidents refer to entities in Sri Lanka that host phishing web pages, affecting the activity of financial institutions abroad and around 80% of reported phishing incidents were targeting Sri Lankan financial institutions and were hosted overseas.
- 32 .lk domains were compromised in 2014, representing approximately 60% of the total number of reported defacements.

The above findings lead to the following conclusions:

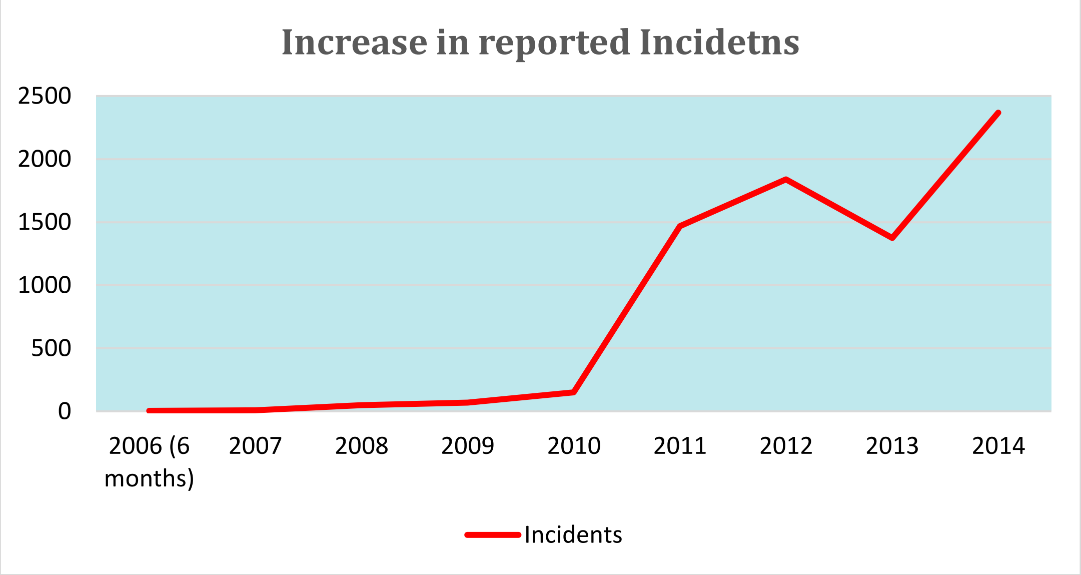
- Cyber security threats upon our national cyber-space have diversified, and have evolved both in terms of quantity and in terms of technical complexity;
- The majority of the compromised systems in Sri Lanka, are part of botnets tat are being used as proxies for carrying out attacks on targets outside the country, thus representing potential threats to other systems connected to the Internet;
- Based on the analysis of the malware types specific to our national cyber-space

and of the types of compromised systems, both revealed in this annual report, it appears that, in quantitative terms, most attacks are directed towards outdated, obsolete systems, lacking security features (e.g. systems affected by Conficker) or are not updated with the latest security patches/updates;

- An increasing number of entities in Sri Lanka become targets of APTs, attacks with a high degree of complexity that are launched by groups with the capacity and motivation to persistently attack a target in order to obtain certain benefits (usually sensitive information); we expect an increase in the number and severity of such attacks nationwide during 2014;
- Sri Lanka cannot be considered as just a generator of cyber security incidents anymore, because the analysis of the data presented in the current report demonstrates that is mostly used as a proxy by other attackers.

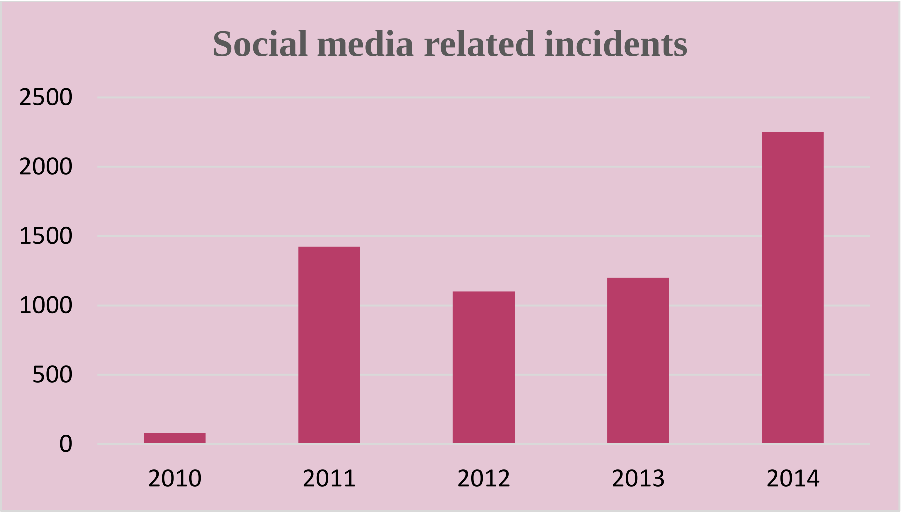
2.2. Incident Handling Statistics

Incidents reported to Sri Lanka CERT have increased to 2,368 in the year 2014. In the year 2013, 1,275 incidents were reported. This represents a 90% increase in reported incidents compared to the year 2013.



Graph 1: Total number of reported incidents

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

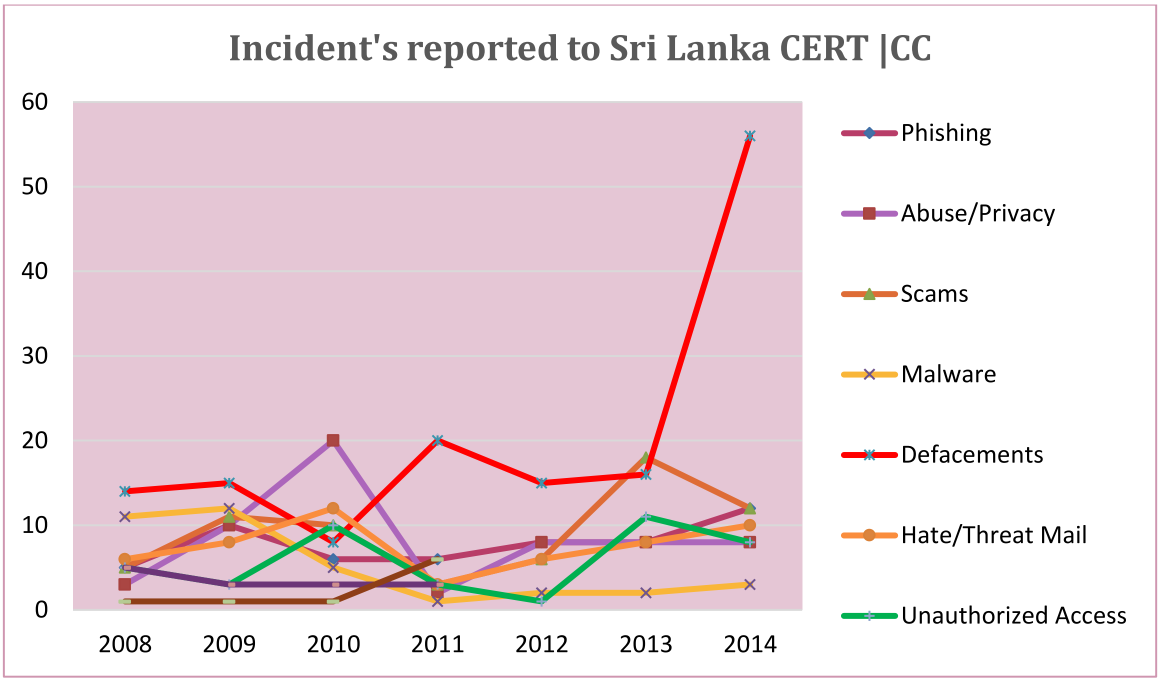


Graph 2: Total number of social media related incidents

The following table depicts the distribution of various types of incidents reported to Sri Lanka CERT in the year 2014. All the incidents reported to Sri Lanka CERT have been resolved satisfactorily.

Type of Incident	No
Phishing	12
Abuse/Privacy	8
Scams	12
Malware	3
Defacements	56
Hate/Threat Mail	10
Unauthorized Access/Attempted	8
Intellectual property violation	3
DoS/DDoS	6
Fake Accounts/social media	2,250
Total	2,368

Table 1: Number of reported incidents in year 2014



Graph3: Types of incidents reported to Sri Lanka CERT|CC

3. New Services

- **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.

Sector-based CSIRTs will provide industry specific services to their constituents. For example, the Telco CSIRT will provide content filtering services to ISPs while Bank CSIRT provides vulnerability alerts specific to banking applications and implement security standards to ensure a minimum level of security compliance within the industry.

The net result of setting up sector based CSIRTs and certifying and coordinating the activities of these CSIRTs is that Sri Lanka CERT will eventually transform itself to being a true coordinating body.

Sri Lanka CERT|CC launched its first sector based CSIRT for the banking and finance sector called "BankCSIRT" on 1st of July 2014. Almost 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. This is a unique model that will soon be emulated by other nations.

- **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) CA for Government establishments and Lanka Sign CA (for Banks) exist, the universal acceptance of their certificates is in question.

  On 24th September 2013, by virtue of the powers vested by section 18 of the Electronic Transactions Act, No. 19 of 2006, the Minister of Telecommunication and Information Technology, being in charge of the subject of Information and Communication Technology, designated the Information and Communication Technology Agency of Sri Lanka (ICTA) registered under the Companies Act, No. 7 of 2007 and recognized under the Information and Communication Technology Act, No. 27 of 2003, as the Certification Authority for the purposes of Act, No. 19 of 2006.

  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. It is now in the process of testing the processes and technical environment of NCA before going ahead with the launch. The key ceremony will be held during the year 2015.

4. Events Organized / Co-organized

4.1. Training / Education

In order to fulfil its mandate to create awareness and build IS skills within the constituency; Sri Lanka CERT|CC continues to conduct and facilitate training programs and education sessions targeting various audiences including CIOs, Engineers, System Administrators, Banking and Telecom Sector Staff, Students, and the General Public.

During the year 2014 Sri Lanka CERT|CC conducted the following awareness, training and education programs successfully:

- 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 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.

Sri Lanka CERT staff has in addition continued to assist in the delivery of courses in Computer security topics at tertiary education institutions.

Publication of leaflets and posters designed for distribution at seminars, exhibitions and other forums is a key strategy for Sri Lanka CERT's awareness campaign.

4.2. Consultancy

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

Typical consultancy services provided during the year 2013 included;

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

4.3. Seminars & Workshops

- Cyber Security Week 2014:

  Since 2008, Sri Lanka CERT | CC has been conducting an annual security awareness programme titled Cyber Security Week (CSW). This international event draws attention of the local as well as regional information security professionals.

  Cyber Security Week 2014 was held in the month of October 2014, and featured a series of events:

  - Annual National Conference on Cyber Security 2014
  - Workshop for law enforcement agencies by APNIC
  - Three full-day Workshops for professionals, namely:

- Technical workshop on "IT Fraud-Discovery and Mitigation
- Technical workshop on "Mobile Application Security"
- Technical workshop on " Network security"

- Hacking challenge: Hacking Challenge is a contest for IT Professionals to attack and 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.

- Contributed to organizing of the Council of Europe GLACY Mission conference on Cyber Crime and Cybercrime Legislation, including technical assistance for the adaption of the Budapest Convention.

  Consequently, Sri Lanka has become a priority country to benefit from the Capacity Building Programme of the Council of Europe project titled "Global Action on Cyber Crimes" (GLACY). Under this project the Judiciary, Prosecution and Law Enforcement authorities would benefit from training and capacity building to better deal with Cyber Crime enforcement issues.

- CIO Forum in collaboration with (ISC)2 Sri Lanka Chapter.
- Carrying out training sessions and presentations on Information security for SLAS (Sri Lanka Administrative Services) officers at SLIDA

5. Achievements

5.1. Publications & Other Media

- 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 and

FAQs are among some of the other published items.

- E-mails

  Disseminating security related information via e-mail alerts to Sri Lanka CERT website subscribers. The Cyber Guardian e-newsletter was initiated in mid-2010 and 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.

5.2. 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 will benefit from receiving threat intelligence from the region and also becoming part of the global incident response teams.

c) International Information Systems Security Certification Consortium, Inc.,(ISC)^2

d) Thread Intelligence from ShadowServer

6. International Collaboration

6.1. MOUs

In addition to being members of FIRST and APCERT, Sri Lanka CERT has signed Memoranda of Understanding (MoU) with Microsoft, to be a member of Microsoft Security Cooperation Program (SCP) and with IMPACT, the security arm of ITU.

Sri Lanka CERT has also signed MoUs with Team Cymru, Tsubame, JPCERT/CC (Japan), and ShadowServer; as a result of the above MoUs Sri Lanka CERT gets daily statistics for its "Threat Visualization System" which is used for alerting ISPs about possible suspicious network traffic.

In October 2014, Sri Lanka CERT|CC entered into an MOU with CNCERT|CC to further enhance collaborative activities with China.

6.2. Event Participation

- March 17th – 22nd
  2014-APCERT AGM & Conference, Taipei, Taiwan
- May 15th – 16th
  International Cyber Shield Exercise, Istanbul, Turkey
- June 5th – 6th
  UNRCPD International workshop on Information and Cyber Security, Beijing-China
- June 22nd – 27th
  2014-FIRST AGM & Conference, Boston-USA
- June 28th – 29th
  CERT|CC conference for CERTs with National responsibility
- December 8th – 12th
  ITU Penetration Testing Training, Vientiane, Lao PDR

6.3. International Incident Coordination

Sri Lanka CERT|CC actively participated in the APCERT Drill 2014 as 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

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

- 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 2015

8. Framework

- **Future Operations**

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

  - Establish a more formalised Cyber Security Research unit within Sri Lanka CERT|CC.
  - Recruit replacements for the 2 senior IS professionals that left Sri Lanka CERT|CC to take up positions overseas.
  - 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.

- **Operational Support Projects**

  Sri Lanka CERT continues to maintain a sensor for the JPCERT/CC hosted TSUBAME Internet Scan Data Acquisition System project, while collaborating with the Dragon Research Group (DRG) based in Brazil by deploying a sensor to collect and monitor data to identify emerging threats.

  Further, Sri Lanka CERT proposes the placement of sensors at all ISP networks to cover the IP blocks in order to gather data on attack traffic generating to and from the country. Sri Lanka Telecom has agreed to place a sensor in the network which will facilitate the coverage of a large part of IP's in the country. SLT plans to deploy the sensor in the first quarter of 2015 after finalizing the MoU with Team Cymru.

9. Conclusion

By analyzing the data received by Sri Lanka CERT|CC and presented in this report, we can conclude that cyber threats targeting the Sri Lankan national cyberspace have diversified. Evolutionary trends are being observed, both in terms of quantity and of technical degree of complexity.

Most incidents analyzed by Sri Lanka CERT|CC, from the automatic or individual segment of incidents, refer to entities in Sri Lanka. Attackers have usually exploited technical vulnerabilities in applications and operating systems. The main goal of the attacks was to infect the computer systems with various malicious applications in order to make them part of different types of botnets (zombies).

These compromised systems (victims), which pose as real threats to other entities connected to the Internet, are often used to serve as "proxies" for carrying out other attacks on targets outside Sri Lanka. There are significant advantages for the attacker for using such an approach, for example the possibility to hide their real identity and also the use of a large number of computers (depending on the number of infected computer systems) to launch attacks.

Also, based on the malware types specific to the Sri Lankan national cyberspace and on the types of compromised systems, it appears that, from a quantitative point of view, most attacks are directed towards obsolete systems, outdated, with no native security features (i.e. systems affected by Sirefef) or that are not updated with the latest security patches/updates.

It is worth noting that Sri Lankan entities are becoming more frequent targets for APT threats, cyber-attacks with a high degree of complexity, launched by groups that have the capacity and motivation to persistently attack a target in order to obtain certain benefits (usually sensitive information). Although a smaller number of analyzed incidents revealed APT behavior, it shows a moderate evolutionary trend, and we can expect a nationwide growth in the number and severity of such attacks during 2015;

In this context, we maintain that Sri Lanka cannot be considered just a source of cyber-security incidents or threats, but the analysis of the presented data demonstrating the intermediate/transit character of some significant systems *connected to the Internet in Sri Lanka, used as proxy for launching attacks on other targets on the Internet.*

Among the main difficulties encountered in the incident response activity, we can mention the 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, this is hindering our activities and the real-time response to such incidents. In this context, we consider it necessary to supplement the national legislation framework with the stipulations contained in certain documents that are found at European level.

Since the establishment of Sri Lanka CERT|CC in 2006, the conduct of awareness campaigns to notify the public about our presence and the activities have continued unabated. Through the use of seminars and conferences and through the use of mass media it was possible to achieve this target which resulted in an increase in number of incidents reported and handled by Sri Lanka CERT|CC in the past consecutive years.

During this year a majority of the incidents reported to Sri Lanka CERT were related to social networking sites on 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 2014 were very successful, well attended and were in high demand. We will continue to conduct the Annual Cyber Security Week and the Annual National Conference on Cyber Security while finding new ways to reach an even wider audience, and also 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.

In addition to securing Sri Lanka's cyber space, Sri Lanka CERT is committed to build 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 is the Sri Lanka's first and largest Computer Emergency Readiness Team (CERT) and helps general public and Sri Lankan organizations to keep their computer systems and networks secure.

TechCERT is a division of LK Domain Registry and has its origins in a pioneering joint project of the LK Domain Registry and the academic staff members of the Department of Computer Science & Engineering of the University of Moratuwa, Sri Lanka. TechCERT has collaborative partnerships with several national and global information security organizations that provide latest data on computer and network security threats and vulnerabilities.

As a core part of its mandate to secure the cyber space of Sri Lanka, TechCERT provides the public and its member organizations with information security incident response services and conducts public awareness programs on safe use of computers and the Internet.

1.2. TechCERT Technical Team

The present technical staff strength of TechCERT is 15 personnel and their professional qualification status is listed below (please note that most staff members have multiple qualifications in different areas of information security, computer systems security, network security specializations):

PhD	3
MEng/MSc/MPhil	6
PG Diploma	4
BSc Eng/BSc/BIT/BEng	12
CISSP	2
C|HFI	1
Certified ISMS Auditor (ISO27000)	4

CCNA / CCNA Security	2
CCNP	1
Chartered Engineers	3
CISM	1
CISA	1
C|EH	5
ITIL v3	2
PMP	1
CPISI	3
RHCSA/RHCE	1

1.3. Constituency

TechCERT works with its member organizations, selected governmental organizations as well as provide incident response services and awareness programs for the general public of Sri Lanka.

1.3.1 Activities & Operations

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

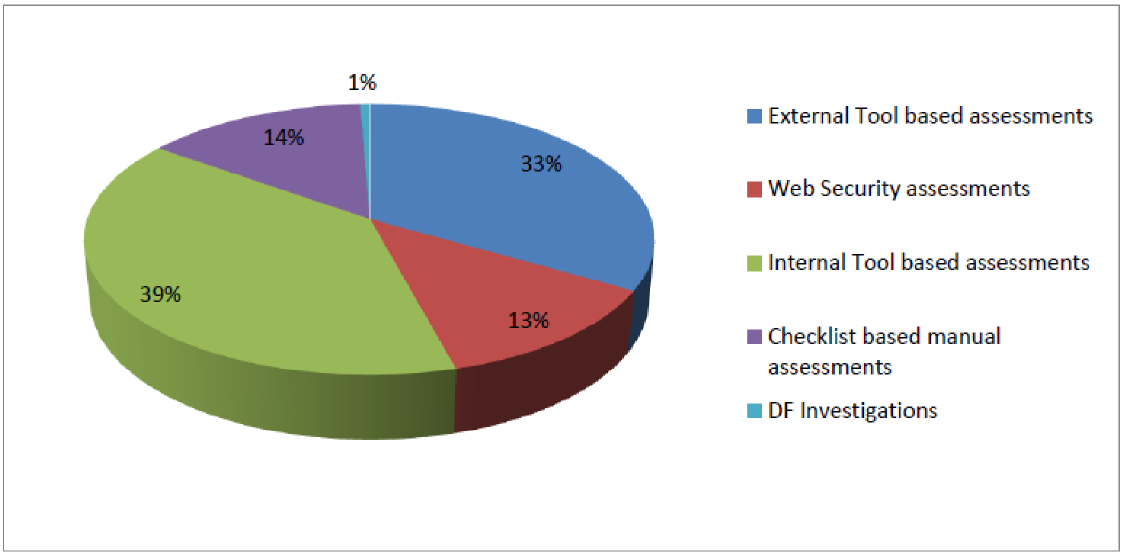
- Network surveying, penetration tests and vulnerability assessments
- Emergency response and damage control for computer security incidents
- Vulnerability research and verification and white-hat exploitations
- Wireless network security assessment and reconfiguration
- Firewall and router security 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
- 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

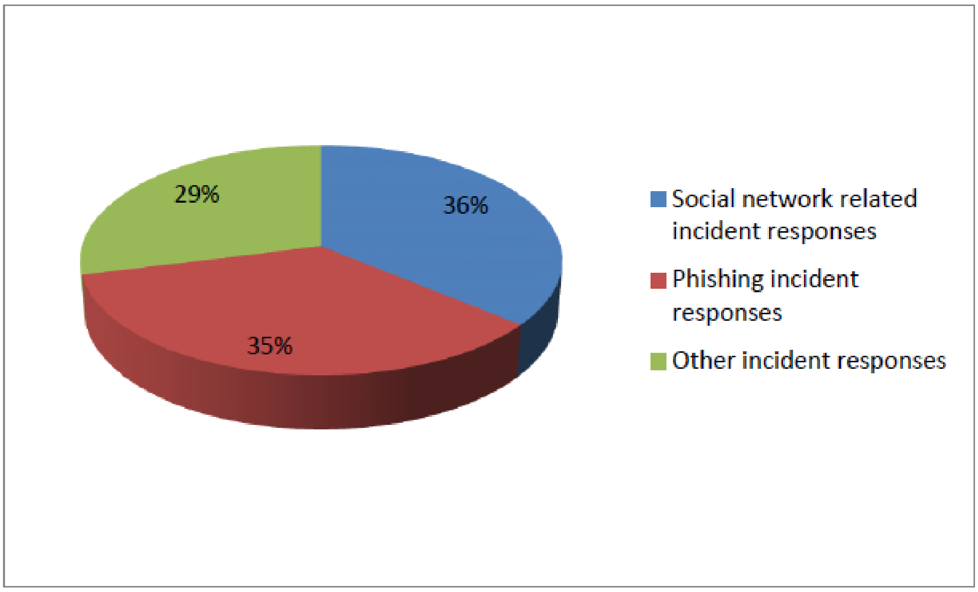
Activity Type	Count
External vulnerability assessments	1664
Web based Security vulnerability assessments	622
Internal vulnerability assessments	1948
Other Specialized assessments	721
DF investigations	33
Awareness Trainings	12

Security Assessments



Incident Response

Type of Incident Response	Count
Social network related incident responses	71
Phishing incident responses	69
Other incident responses	57



3. Events

3.1. Organizing of Training Seminars, Workshops and Demonstrations

25th April 2014	**Public Seminar and Demonstration – Dangers of Browsing the Internet and How to Avoid Attacks– Southern Province** TechCERT conducted a public seminar and demonstration session enhancing knowledge about Dangers of Browsing the Internet and How to Avoid Attacks. This seminar was conducted in University of Ruhuna - Faculty of Engineering in Hapugala, Sri Lanka.
23rd May 2014	**Public Seminar and Demonstration – Dangers of Browsing the Internet and How to Avoid Attacks– Nothern Province** TechCERT conducted a public seminar and demonstration session enhancing knowledge about Dangers of Browsing the Internet and How to Avoid Attacks. This seminar was conducted in Euroville Auditorium, Nallur, Jaffna.
23rd July 2014	**Public Seminar and Demonstration – Dangers of Browsing the Internet and How to Avoid Attacks– Sabaragamuwa Province**

	TechCERT conducted a public seminar and demonstration session enhancing knowledge about Dangers of Browsing the Internet and How to Avoid Attacks. This seminar was conducted in Samudi Hall, Rathnapura.
4th August 2014	**An Unexpected Exploit - Are your own devices safe to use for business?** TechCERT conducted a demonstration on mobile device security and how to safe your own mobile device when you are using it for business purposes. This seminar was conducted in Hotel Galadari, Colombo 01.
17th September 2014	**Public Seminar and Demonstration – Privacy Lost and Never Found – Western Province** TechCERT conducted a public seminar and demonstration session on the theme of Privacy Lost and Never Found. This seminar was conducted in The Institution of Engineers, Colombo 7.
24th September 2014	**Incident Detection, Verification, Analysis and Forensics Essentials** TechCERT conducted a seminar and demonstration session enhancing knowledge about Incident Detection, Verification, Analysis and Forensics Essentials. This seminar was conducted in Sri Lanka Institute of Development Administration, Colombo 07.
24th September 2014	**Effective Incident Response - Why should you respond to incidents?** TechCERT conducted a seminar and demonstration session enhancing knowledge Effective Incident Response. This seminar was conducted in Sri Lanka Institute of Development Administration, Colombo 07.
22nd January 2015	**Incident Detection, Verification, Analysis and Forensics**

	Essentials TechCERT conducted a seminar and demonstration session enhancing knowledge about Incident Detection, Verification, Analysis and Forensics Essentials. This seminar was conducted at South Asian Network Operators Group (SANOG) 25th annual conference in Amaya Hills Hotel, Kandy, Sri Lanka.
24th January 2015	**Seminar and Demonstration - "Information Security and Controls"** TechCERT conducted a seminar and demonstration session enhancing knowledge about Information security and controls. This seminar was conducted in Sri Lanka Army - Wahara Camp, Kurunegala

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

Program Name	Date	Audience	Venue
Better Search Techniques and Safe Internet Browsing	24th June 2014	Students	Nalanda College, Colombo 10.
Internet for Education and Safe Internet Browsing	27th June 2014	Students	Roman Catholic Junior School, Pahathgama, Hanwella.
Safe use of Internet	25th September 2014	Teachers & Students	Gurulugomi College, Kaluthara.

3.3. Participation in Conferences, Workshops and Training Programs

- Dileepa Lathsara, Chief Operating Officer of TechCERT participated for the, 26th Annual FIRST Conference, Getting Back to the Roots at Boston USA.
- Dileepa Lathsara, Chief Operating Officer of TechCERT participated for the National IT Conference organized by Computer Society of Sri Lanka(CSSL).
- DIleepa Lathsara & Madusanka Hettige participated for the 7th Annual

National Conference on Cyber Security organized by SLCERT|CC & ICTA Sri lanka held on 1st of October 2014.

- Madusanka Hettige & Kasun Chathuranga participated for the APCERT AGM and Conference 2014 held on 24-27 March 2014 at Taipe, Taiwan.
- Madusanka Hettige participated for the workshop 'Qualys Guard Vulnerability Management & Policy Compliance' conducted by Qualys Inc on 24-25 October 2014 at Colombo, Sri Lanka.
- Technical work shop on TSUBAME sensor. Two of the JPCERT representatives have conducted the work shop on 2nd of October 2014 at TechCERT office.
- Amila Perera & Nalinda Herath participated for the SANOG 25th annual Conference & workshop held on 16th to 24th January 2015.

3.4. Cyber Security Drills

19th February 2014	**APCERT Cyber Security Drill 2013** TechCERT participated in the Drill as a member of the Organizing Committee and member of EXCON
6th March 2014	**Cyber Security Drill for Sri Lankan Finance & Insurance organizations** TechCERT conducted a cyber-security drill for the Sri Lankan Finance & Insurance Sector on the theme of "The strength of chain lies on its weakest link".
9th July 2014	**Cyber Security Drill for Sri Lankan Banking Sector** TechCERT conducted a cyber-security drill for the Sri Lankan Banking Sector on the theme of "The strength of chain lies on its weakest link".
5th November 2014	**Cyber Security Drill for Sri Lankan Telcos and ISPs** TechCERT conducted the first ever cyber-security drill for the Telcos and ISPs within Sri Lanka on theme of "The strength of chain lies on its weakest link".

4. Achievements

4.1. Technological Achievements

- Deployment of the Dark Lab to enhance the Digital Forensics services.
- Deployment of Incident Response Hot-Line
- Deployment of free web site security assessment program for Sri Lankan sites together with LK Domain registry.
- Improvements for Knowledge base for Incident response support
- Improvements for the "PhishHook" Phishing Early warning system and increase in number of deployments within Sri Lanka

4.2. Publications

- More than 30 articles published in https://techcert.lk/en/ web site to enhance the basic security knowledge of the general public.

5. Future Plans

- Researching on threat intelligence gathering
- Development of an anomaly detection system for e-commerce applications
- Develop a system to automate the detection and containment of Security Information Leakages
- Develop a framework to improve web application vulnerability detection.

6. Conclusion

TechCERT has consistently improved and expanded its capability to respond and assist its constituency in information security incidents and handle emergencies in a timely and professional manner.

With the experience possessed by participating and organizing the APCERT drill activities, TechCERT was able to conduct cyber drills for the Banking Sector and other sectors for the 4th consecutive time. TechCERT has conducted the first ever cyber drill for Telcos and ISPs in Sri Lanka in this year.

Similar to year 2013, there was a significant increase in phishing attacks and web site defacement/hacking incidents in Sri Lanka in 2014. TechCERT successfully responded to most of the incidents reported and assisted 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 and will provide pro-active response.

Towards this goal, TechCERT will be further increasing its staff strength, acquire advanced training and tools, and build even stronger bonds with the regional and global CERT community and other initiatives dealing on cyber safety.

ThaiCERT

Thailand Computer Emergency Response Team – Thailand

1. About ThaiCERT

1.1. 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.

1.2. Constituency

The constituents of ThaiCERT are all public, private and home sectors of Internet users in Thailand. ThaiCERT also provides the incident coordination service to other international entities, where the sources of attacks originate from Thailand.

1.3. Staffing

ThaiCERT technical staffs consist of 2 specialists and 8 engineers who are responsible for incident response, threat analysis and digital forensics.

2. Activities & Operations

2.1. Abuse statistics

- **Reported Incidents Received through E-mail**

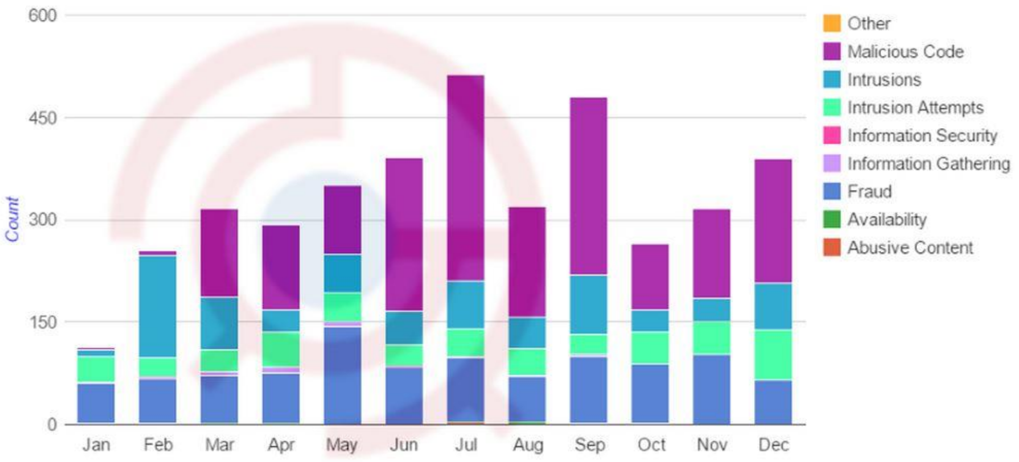


Figure 1: The number of reported incidents in 2014

Through our official e-mail address, ThaiCERT received a total of 4,008 reported incident cases (tickets) in 2014, which is an increase of 229.68% compared to those of 2013 (1,745 cases). The received reports per month varied approximately between 112 to 514 cases, as shown in Figure 1, significantly higher than the previous year (80 to 213 cases per month).

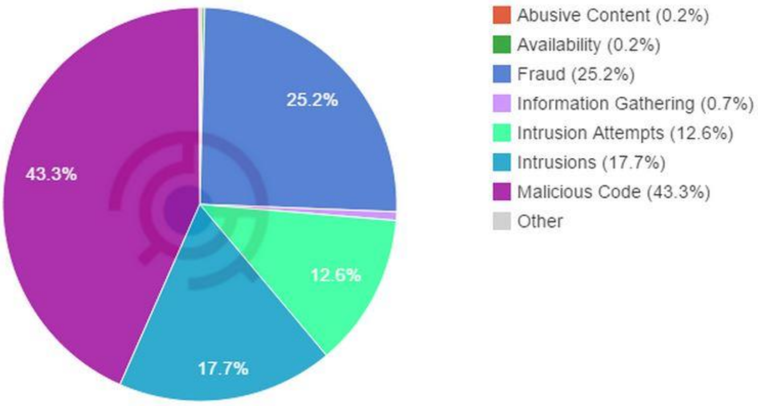


Figure 2: The proportion of reported incidents by incident type in 2014

According to the reported incidents in 2014, classified by the eCSIRT incident classification[1], malicious code (mostly malware URLs) dominated with 43.3%, followed by fraud at 25.2%, where all fraud cases were phishing, and intrusions at

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

17.7%. Compared to only 3.7% of malicious code cases in 2013, the reason behind the dramatic increase of malicious code incidents was due to a new collaboration between ThaiCERT and a security research firm to receive an intelligence feed related to malware URLs occurring in Thailand. All such information was handled and notified to the relevant parties through e-mail channels.

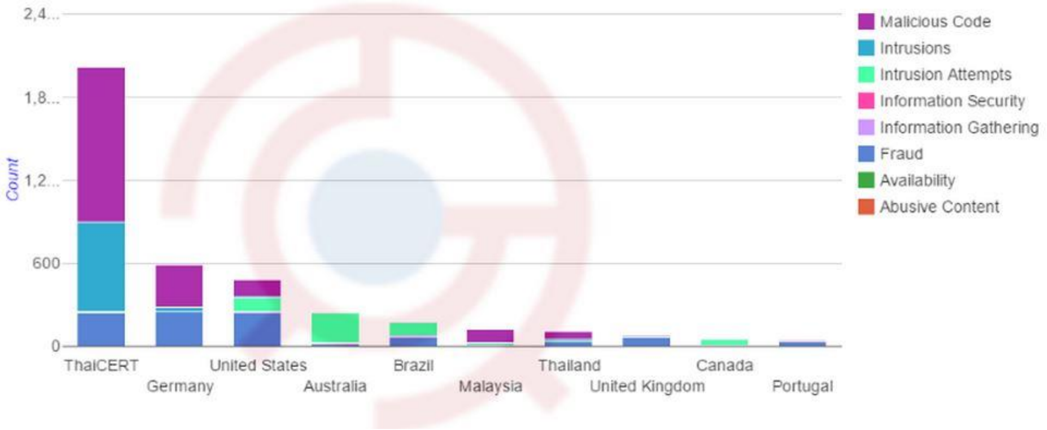


Figure 3: Top 10 incident reporters by country in 2014

Regarding the incident reporters classified by country, Figure 3 shows that most of the security incidents reported by ThaiCERT security watch system, comprising 2,016 cases or 50.29% of all reports, which is a significant increase from those of the previous year (895 cases). The source of Fraud, Malicious Code and Intrusions incident reports generally came from automatic feeds. Germany, which was never in the top 10 in 2012, moved up to the second position (587 cases), followed by the United States (482 cases), who were in 2nd position in 2012 (392 cases).

- **Reported Incidents Received from Automatic Feeds**

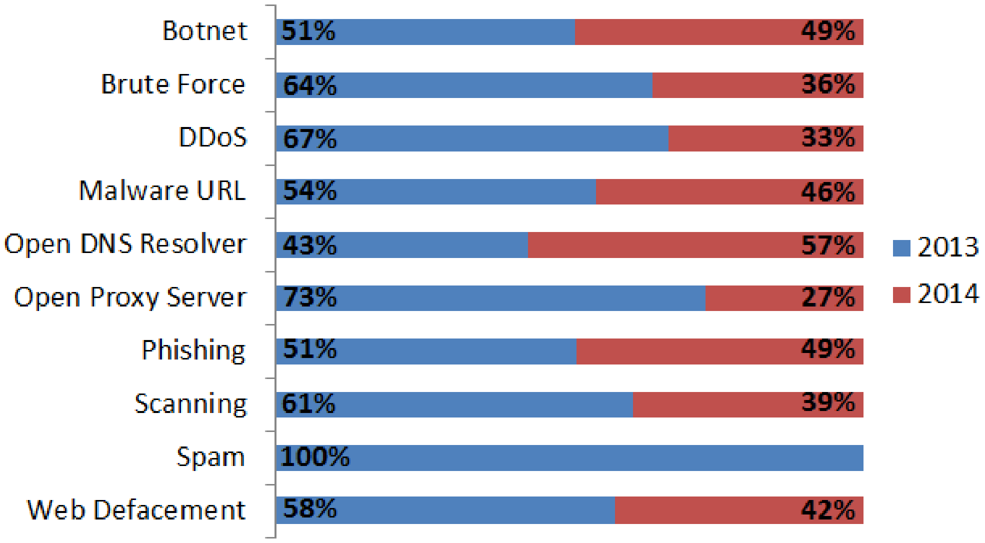


Figure 4: Proportion of number of reports received from Automatic Feeds in 2013-2014 counted by unique IPs

Regarding the number of reports received from automatic feeds in 2013-2014, while there is no significantly change in number of reports of Botnets, Malware URLs, Phishing and Web defacements, there were a dramatic 2-time decreases of reports for Brute Force, DDoS and Scanning and even a 3-time decrease of reports for Open Proxy Servers. There is no report for Spam because our source of information stopped sending this type of reports in 2014.

3. Events Organized / co-organized

3.1. Training

Organized:

- SANS Secure Thailand 2014, Bangkok, Thailand, May 2014
- Invited to be a trainer of incident response training co-organized by JPCERT/CC and LaoCERT, Lao PDR, May 2014
- MAC 2014 (Malware Analysis Competition) with JPCERT, Thailand, Nov 2014
- Local certificate training and exam: iSEC, Thailand, June 2014

3.2. Drill

Organized:

- Cybersecurity drill for financial institution and ISP in Thailand, May 2014

Participated:

- APCERT Drill 2014 under the theme "Countering CyberOps with Regional Coordination", Feb 2014
- ASEAN CERT Incident Drill (ACID) 2014, Sep 2014

3.3. Seminars

Organized:

- ETDA/ThaiCERT Security Seminar "The War against Advanced Cyber Threats", Mar 2014
- Cyber Security Thought Leadership and Framework, July 2014
- The RAISE Forum, Bangkok, Aug 2014

Participated:

- ASEAN-Japan Information Security Workshop, Jan 2014
- RSA Conference 2014, Feb 2014
- APCERT AGM 2014, Mar 2014
- ASEAN Regional Forum (ARF) Workshop on Cyber Security Confidence Building Measures, Mar 2014
- NCSC @ NDSI Security Week 2014, May 2014
- The 6th China – ASEAN Network Security Seminar, May 2014
- Cyber Attacks: The Biggest Threat to National Security, June 2014
- CDIC (Cyber Defense Initiative Conference), July 2014
- Annual FIRST Conference 2014, USA, July 2014
- The 6th ASEAN-Japan Government Network Security Workshop, Aug 2014
- The 1st China-ASEAN Cyberspace Affairs Forum, Sep 2014
- Underground Economy, Sep 2014
- The 7th ASEAN-Japan Information Security Policy Meeting, Oct 2014

4. MoU

MoU with Cybersecurity Malaysia, Aug 2013

5. **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.

1.1.1. 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:

(1). To assist the handling of the intrusion incidents in the constituency, .tw domain.

(2). To announce the system vulnerability information.

(3). To provide security training and education on protection and defending technologies and skills.

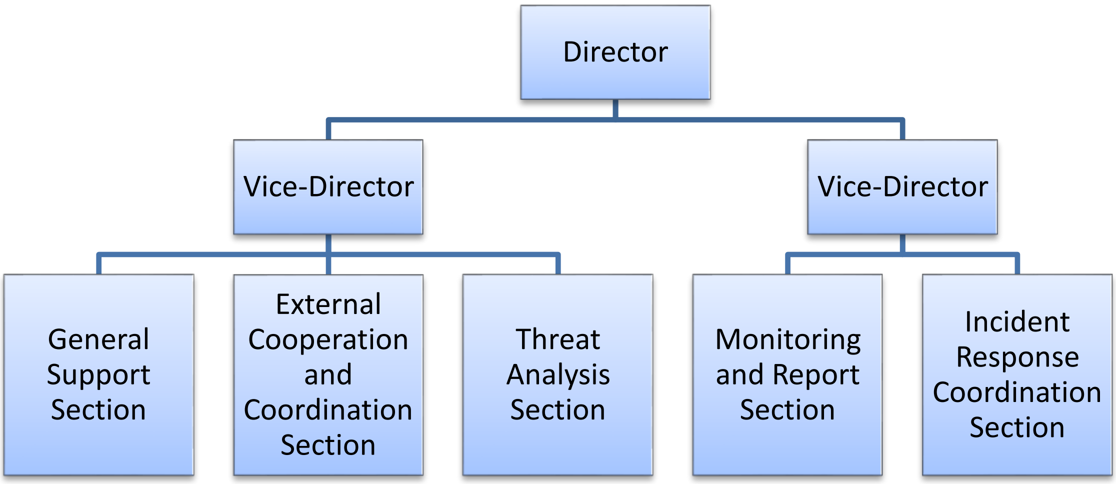
(4). To assess periodically the national-wide security level in the Internet.

(5). 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.

1.1.2. Organization


Director
Vice-Director
Vice-Director
General Support Section
External Cooperation and Coordination Section
Threat Analysis Section
Monitoring and Report Section
Incident Response Coordination Section

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. Expect to achieve the following goals:

Year	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014
Total	2874	1824	788	660	1087	679	1094	6666	8,126	140,250	15,150

Table 1. TWCERT/CC incident response statistics

(1) Possible incidents prevention: provide an incident response channel and the prevent mechanism for the victims to avoid analogous events happening.

(2) Real-time incidents handling: offer an immediate warning and defense force to effectively restrain and control incidents extending.

(3) Recovery support: provide technological consultant and support to recovery operation and reduce damage.

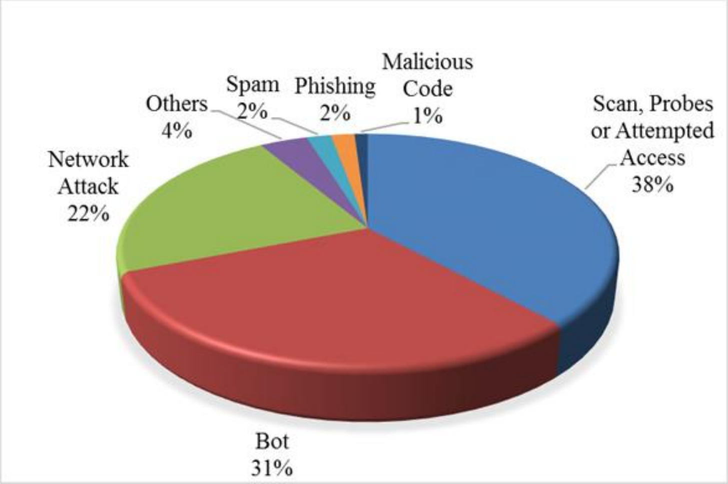


Figure 1 TWCERT/CC incident response classification statistics

2.2. 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.

Year	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014
Advisory	197	140	138	119	49	44	234	98	115	154	131

Table 2. TWCERT/CC advisory statistics

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 49 categories and up to 29 thousands records. We will continuously invest manpower to maintain and update. The major categories are shown in Fig. 2.

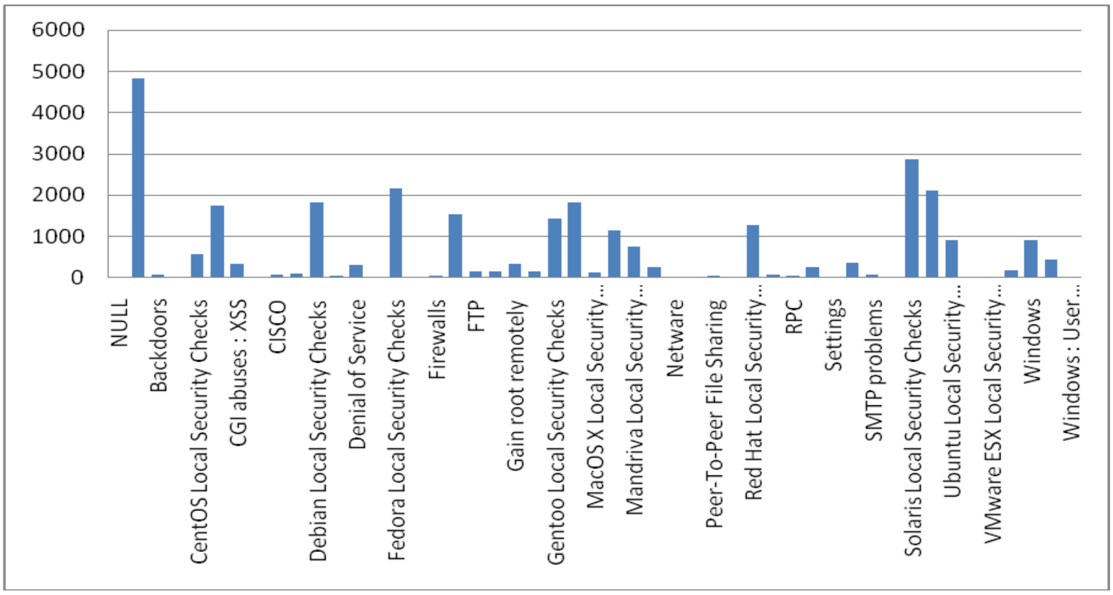


Figure 2. Categories of TWCERT/CC Vulnerability Database

2.3. Spam Analysis Report

TWCERT/CC handles and analyzes spam reported from online. Over five hundred millions of spam received in 2014 and originated from 87 countries. The geographic distribution of the spam sources is shown in Figure 3 and the amount of the spam over the year of 2014 in Figure 4.

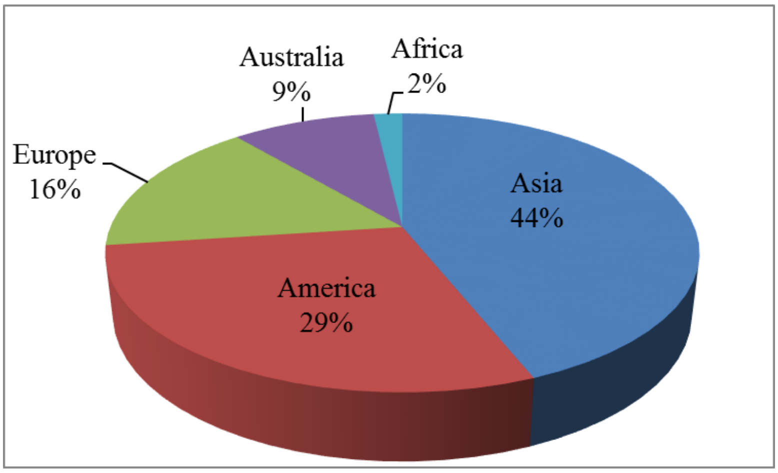
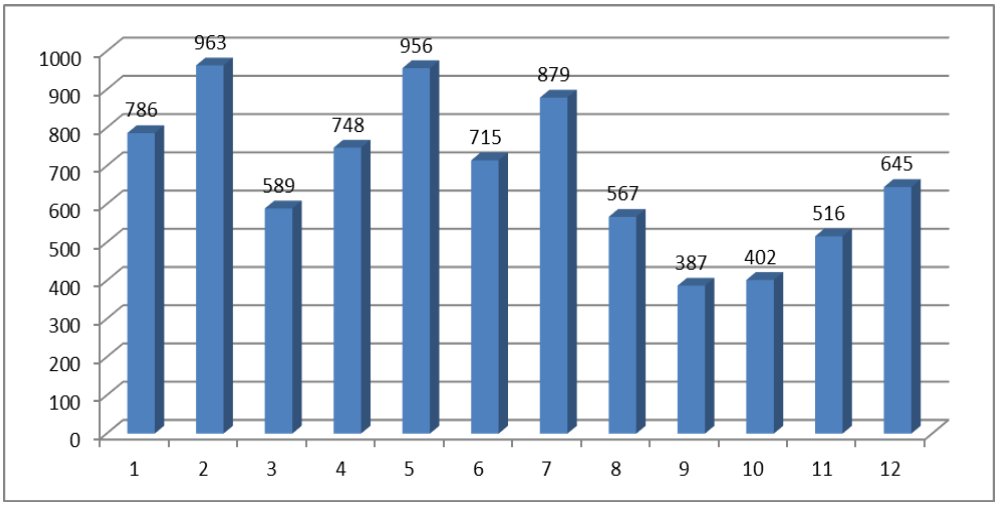


Figure 3 The geographic distribution of the spam sources.



Unit : One Hundred

Figure 4 The amount of spam each month in 2014.

2.4. Anti-Phishing Now

TWCERT/CC provides a phishing report service (Anti-Phishing Now) to stop phishing sites promptly and to prevent further personal privacy leakage. When a phishing site or a phishing web page injected to a victim website is found by a user, he can report the phishing site through the online service. TWCERT/CC then informs the corresponding ISP and the domain owner for shutting down the phishing site. The phishing report service can be found in : http://www.apnow.tw/index.cgi

3. Events organized / co-organized

3.1. Information Security Training

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. By adopting e-learning, TWCERT/CC education courses feature a synchronous/asynchronous on-line learning, a flexible study schedule, and independence learning without time/space restriction to accommodation the different needs of the learners.

TWCERT/CC hosts 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
2014/5/14	Information Security Trend and Case Studying
2014/9/5	Critical Information Infrastructure Protection

Table 3 list of TWCERT/CC workshops and training courses in 2014

3.2. Drill

TWCERT/CC supports TANet (Taiwan Academic Network) to operate an incident handling drill in the fourth quarter of 2014. Total of 4,027 educational institutions and over ten thousands of security officers were involved in this drill program with a high completion rate of 100%.

4. Achievements

4.1. 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.

4.2. 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.

4.3. Certificates

The staff members hold the following certificates.

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

5. International Collaboration

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

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

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

  The well-known security organization, FIRST, is an important platform for computer emergency teams to exchange information and to collaborate with others on various security issues. It brings together a wide variety of security and incident response teams including especially product security teams from the government, commercial, and academic sectors.

  TWCERT/CC joined FIRST in 2001 and became the official contact point of Taiwan. It shares the security information and technologies in many security organizations, such as FIRST, and participates FIRST conferences and technical colloquiums to establish a security joint defense system and enhances incident-handling capability for integrated early-warning mechanism.

- **Asia Pacific Computer Emergency Response Team (APCERT)**

  APCERT established in 2002 is a regional coordination organization of Asia Pacific to enhance regional and international cooperation on cyber security. APCERT cooperates with CERTs and CSIRTs to maintain a trusted contact network of security experts in the Asia Pacific region to improve the region's awareness and competency in relation to cyber security incidents.

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

6. Future work and Conclusion

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

- Work for security related research and development to advance the international visibility.
- Participate in international interchange and coordination to form a transnational joint defense mechanism.
- Train the awareness and capability in information security and risk management through information sharing and international cooperation.
- Develop national critical information infrastructure protection mechanism to enhance the robustness of Taiwan national infrastructure.

TWNCERT

Taiwan National Computer Emergency Response Team – Chinese Taipei

1. About TWNCERT

1.1. Establishment

TWNCERT (Taiwan National CERT) 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.

1.2. Workforce Power

TWNCERT has four task forces, which are Information Gathering, Coordination Service, Research and Development, and Consulting Service.

1.3. Mission and Constituency

TWNCERT aims to enhance the government's ability to respond and deal with security incidents and internationalize our efforts. 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 missions of TWNCERT include:

- To coordinate among relevant agencies and organizations to identify pertinent response and actions in case of security incident.
- To provide information analysis and exchange center for information at home and abroad.
- To help relevant government agencies to set up computer emergency response team (CERT).
- To provide government agencies reference information for formulation of security policies.

TWNCERT director leads the organization, takes charge of formulation and development of policy strategies, and supervises over the routine operation of task forces under TWNCERT and organizational development. TWNCERT services including:

- Alert and publication: Guarding against and publishing probable security threats (e.g. vulnerability analysis).
- Technical service: Providing technical service to government agencies.
- Assistance in the setup of CERT: Assisting interested agencies to set up their own CERT.
- Consultation: Making suggestions regarding operation and R&D of computer security and Internet issues.
- Strategy recommendation: Making suggestion to government agencies regarding strategic planning.
- Risk analysis: Undertaking risk assessment.
- Collaboration: Building collaborative relationship with legal community, information security business and ISP.
- Coordination: Building coordination and communication channels with domestic and foreign incident response organizations.

2. Operations & Activities

2.1. Incident Handling

In 2014, TWNCERT published 1,528 notice advisories to government sectors. The categories were distributed as in Figure 1.

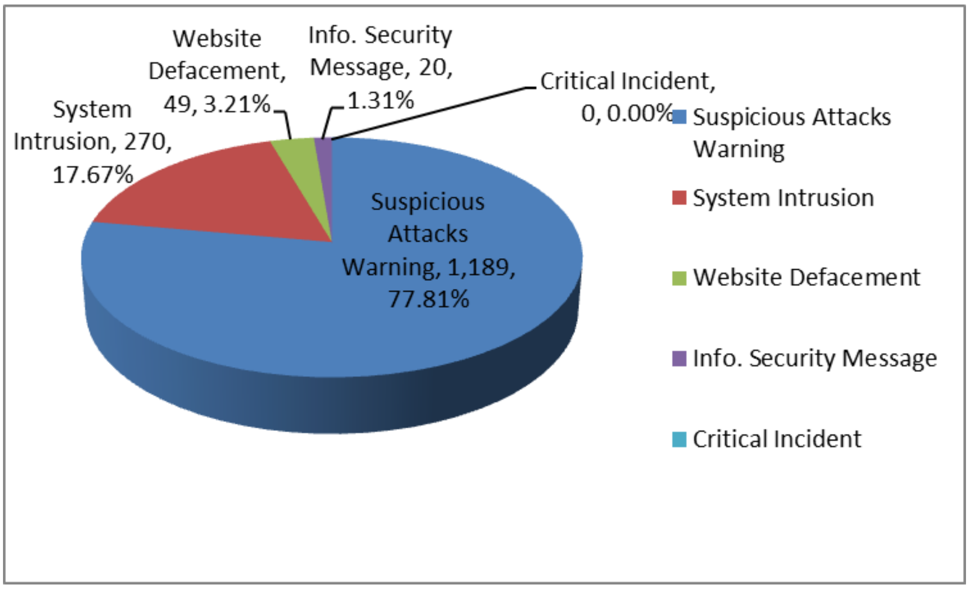


Figure 1 Distribution of notice advisories

TWNCERT received 514 reports on computer information security incidents from Taiwan government sectors in 2014. The top 3 incident categories are Intrusion, Website Defacement and DDoS attacks.

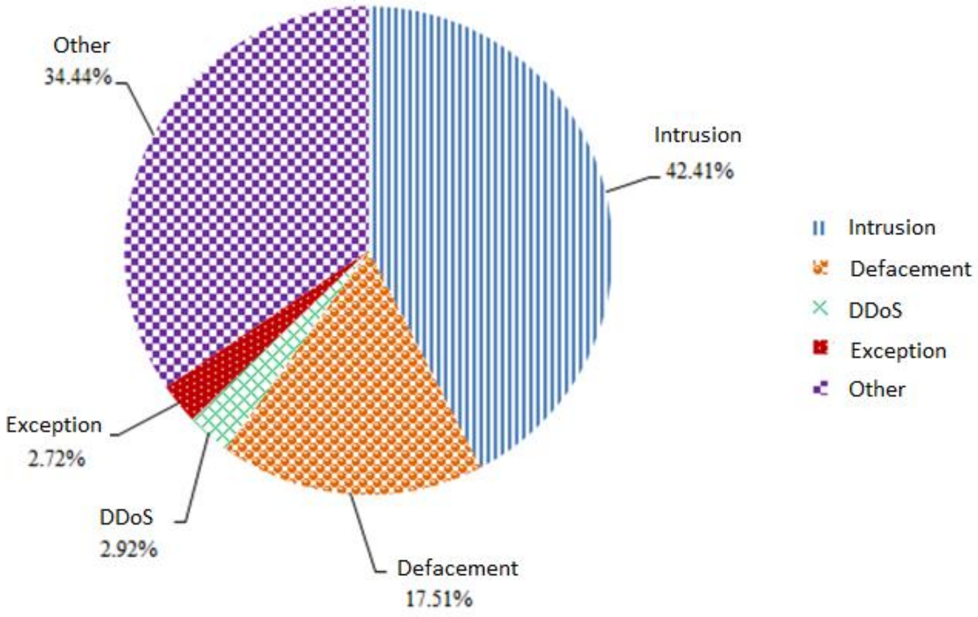


Figure 2 Security incidents from government sectors

2.2. Government Information Sharing and Analysis Center

TWNCERT is intended for improving incident response and information security awareness and sharing in Taiwan. Therefore, we started operating the government ISAC since 2009, called G-ISAC (Government Information Sharing and Analysis Center).

TWNCERT is not only deal with government sectors information security relevant issues, but also sharing security information with Academic ISAC (A-ISAC), National Communications Commission ISAC (NCC-ISAC), which includes most major ISPs in Taiwan. In addition, major SOCs, law enforcement, CERTs such as TWCERT/CC and EC-CERT (Electronic Commerce CERT) also are G-ISAC members.

G-ISAC is using IODEF format and secure API system to make sure the information is correct, useful, in time and based on a trust membership. In 2014, G-ISAC has covered over 98.97% IPs in Taiwan and has shared total of 112,514 security incident and critical information.

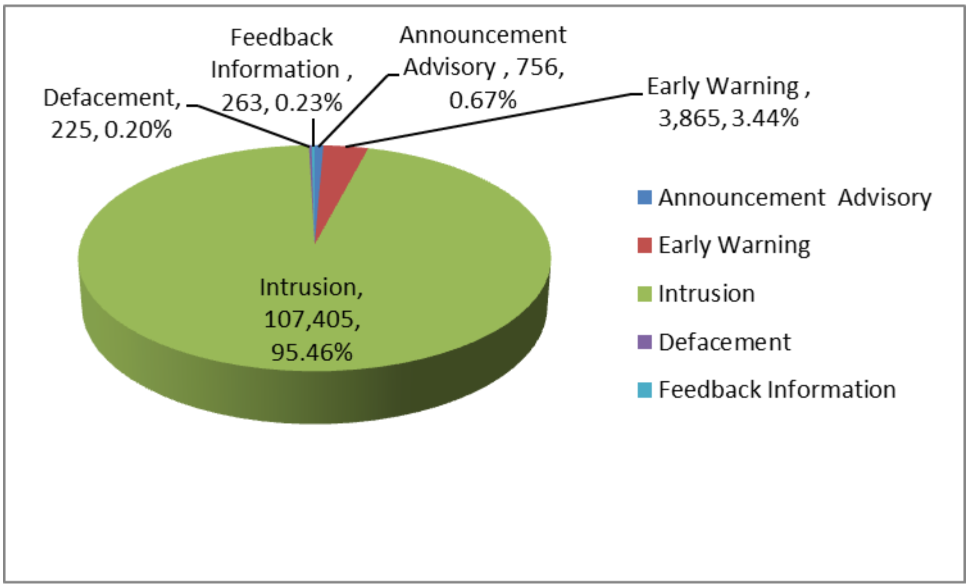


Figure 3 Distribution of G-ISAC

3. Events Organized/Co-Organized

3.1. Training

In 2014, TWNCERT has joined the APCERT Steering Committee and is responsible for APCERT Education and Training program. The goal of the training program is to raise comprehensive cyber security technical skills and awareness of members, provide a channel for members to share and exchange valuable experiences with other member teams and thus creates a better cyber environment within Asia Pacific region. On November 5th, APCERT had 10 member teams attend the first training course event, Malware Behavior Analysis and Detection, presented by TWNCERT.

3.2 Drills

TWNCERT participated in the APCERT Drill in February 2014, and also conducted an annual cyber exercise among the Taiwan government sectors in October.

3.3 Conference

TWNCERT hosted APCERT 11th AGM & Conference on March18-21TH. The theme of APCERT Conference 2014 is “Prepare for a Better Future – The Role of CSIRT

Community". There are 21 APCERT teams from 17 economies and up to 200 attendees to join the annual event on cyber security throughout the Asia Pacific and beyond.

4. Achievements

4.1. Presentation

In 2014, TWNCERT has presented in the following international annual conferences:

- APCERT AGM and Conference 2014, March – Taipei
- FIRST conference, June – Boston
- 14th Regional Asia Information Security Exchange Forum Meeting, July-Bangkok
- APEC TEL 50, September- Brisbane
- Meridian Conference 2014, November- Tokyo

TWNCERT also convened several forums/conferences for the Taiwan Government sectors in 2014.

4.2. Publication

TWNCERT collect and publish security advisories, news or guidelines via its website. In 2014, TWNCERT website published 173 security related awareness news.

TWNCERT defined Taiwan Government Configuration Baseline (TWGCB) since 2013. The purpose of TWGCB is to create security configuration baselines for information technology products widely deployed across the government agencies. There are 213 government agencies under poll, 157 agencies have applied TWGCB on business computers.

5. International Collaboration

5.1. Incident Report

In 2014, TWNCERT received more than 3,417 international information security incident reports, provided assistance and cooperation to other CERTs and governments. Chart below is the classification of the incident reports:

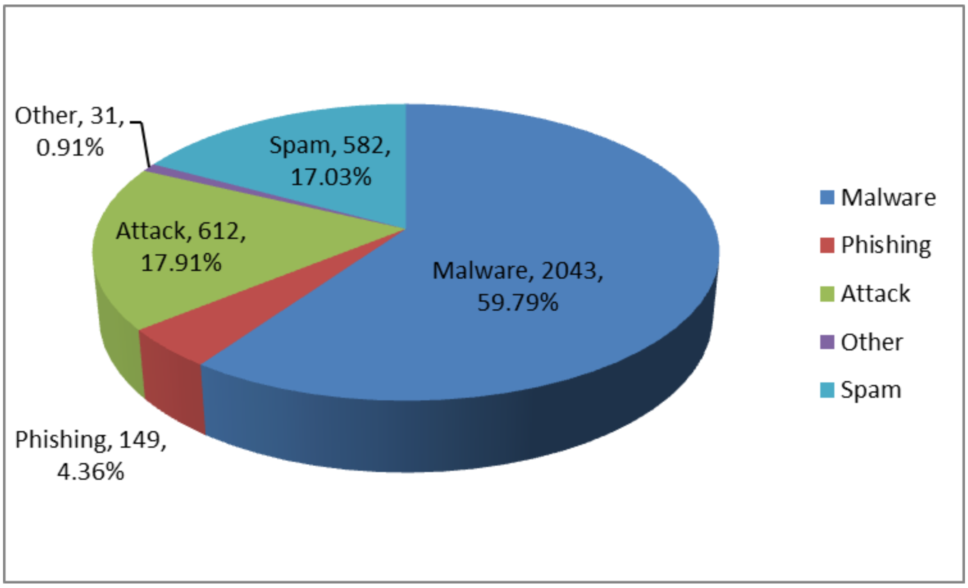


Figure 4 Classification of the international incident reports

TWNCERT has reported Botnet Information via G-ISAC to 19 countries, including Australia, Belgium, Brazil, China, France, Germany, Indonesia, India, Japan, Malaysia, Netherlands, Philippines, USA, Russia, Spain, Singapore, South Korea and Thailand.

5.2. International Organization Membership

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)

5.3. Participation to International Events

Below are some of international events TWNCERT participated in 2014:

- APCERT AGM and Conference 2014, March – Taipei
- APEC TEL 49, April- Yangzhou
- FIRST and National CSIRT conference, June – Boston

- 14th Regional Asia Information Security Exchange Forum Meeting, July- Bangkok
- Black hat USA 2014 & Defcon 22, August- Las Vegas
- APNIC's 38th Conference, September- Brisbane
- APEC TEL 50, September- Brisbane
- AVAR Conference 2014, November- Sydney
- Meridian Conference 2014, November- Tokyo

5.4. MOU

TWNCERT has MOU with JPCERT/CC and Team Cymru for CSIRT Assistance Program.

6. Future Plans and Conclusion

In order to reinforce the cyber security team's capability and capacity, TWNCERT has contributed the cyber security education and training program to APCERT members. . In 2015, TWNCERT will continue

- Nurture cooperation and collaboration among members, providing education and training activities;
- Plan to conduct bi-monthly live streaming/webinar courses;.
- Evaluate the effectiveness of the overall education and training program and improve the program persistently

The online training program could provide a channel for members to share technical skills and exchange valuable experiences with other members. Moreover, TWNCERT will further enhance the international collaboration and also horizontal collaboration with the government sectors and domestic public-private partnerships, to strengthen the security awareness and optimize the incident handling capability.

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:

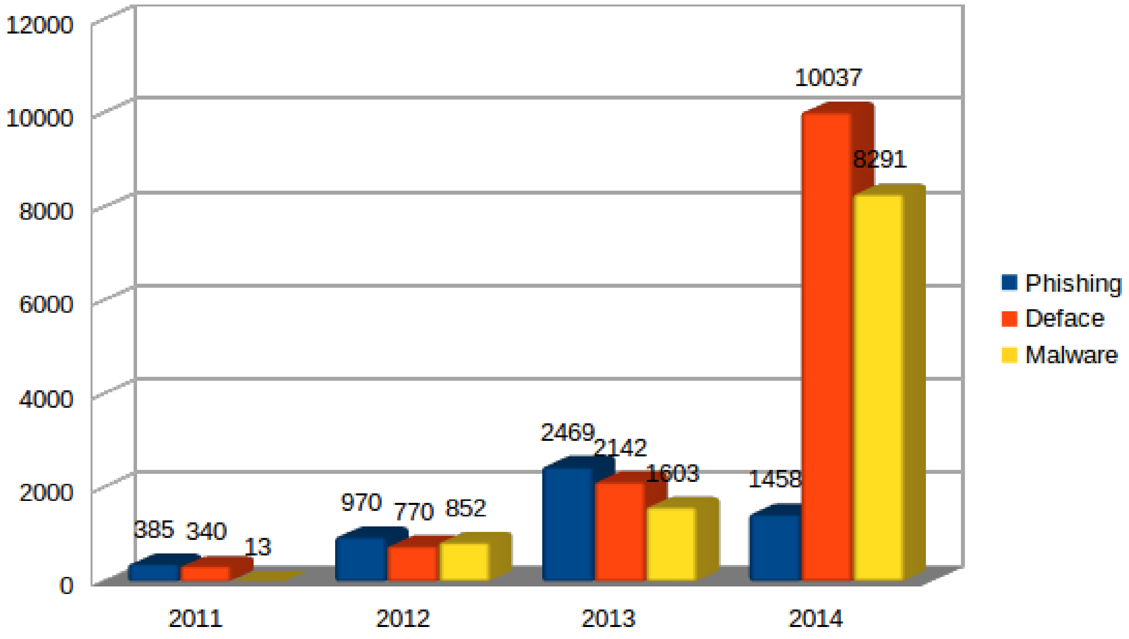
- Being Coordination Center of Vietnam CSIRT Networks with more than 100 members. (Including information technology centers of Ministries, ministerial agencies, governmental agencies, telecommunication enterprise, internet service providers, the organizations in charge of information systems of national importance).
- Coordinating national computer incident response activities.
- Watching and warning computer network security problems.
- Heading and coordinating to build computer network security technical standards.
- Promoting to build CERTs in the organizations, enterprises, and agencies in Vietnam.
- VNCERT is the point of contact of Vietnam with the oversea CERTs in this area.
- Support Ministry of Information and Communications with activities in state management about information security.

- Paticipating to deploy the Anti-spam activities of Ministry of Information and Communication.
- VNCERT has four specialized divisions: Division of Operation, 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 55 members.

2. Activities & Operations

2.1. Incident handling reports

In 2014, VNCERT processed 19.786 information security incidents (including 1458 phishings, 10.037 Malwares, 8291 Defaces).



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

In 2014, VNCERT reported 3.770.179 IPs of large botnets (Conficker, Sality, Traficonverter and Downadup, etc.) and sent 8233 botnet warnings to government agencies and supported them to process.

2.2. Abuse statistics

Security Incidents	2010	2011	2012	2013	2014
Phishing	233	385	970	2469	1458
Deface	19	340	770	1603	8291
Malware	8	13	852	2142	10037
Other	11	17	----	165	8400
Total	**271**	**757**	**2179**	**4810**	**28186**

2.3. Incident Coordinating, warning and supporting activities

- Implemented testing and auditting 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.
- Supported USCERT and US Banks to remove malicious code on 79 websites that was attacked by bRobot botnet.
- Built documents and guidelines about new vulnerabilities, threads and new dangerous malwares for members of Vietnam CSIRT Network.
- Warned all members of Vietnam CSIRT Network of 03 importance vulnerabilities (HeartBlead, ShellShock and USB Firmware).

2.4. Anti-spam activities

- Coordinated mobile operators and SMS content providers to process 157 incidents in SMS Spam.
- Researched and proposed the countermeasures with the fake-emails.

2.5. Legal Framework Update on Information Security

- Drafting the Information Security Law, this draft will be submitted to the Government and the Vietnam National Assembly at the end of this year.
- Drafting the Circular to guideline the cyber security monitoring follows the Decree 72/2012/ND-CP on Anti spam, that will be released on second quarter of 2015.

3. Events organized / Co-organized

3.1. Training

- Organized training courses about CERT activities and Incident Response for LaoCERT in Vientian - Lao.
- Organized information security training course for 30 government agencies.
- Cooperated with VNISA to organize the Information Security Survey and the Information Security Contest for students of universities.

3.2. Seminars & Etc

Participated to organize some meeting event at national level such as Security World 2014, National Information Security Day 2014, ASEAN CIO/CSO Awards, etc.

4. International Collaboration

4.1. Incident Drill

- Participated in 03 international drills: APCERT Annual Drill 2014, ASEAN-JAPAN Drill and ASEAN CERTs Incident Drill (ACID 2014).
- Supported 03 provinces to organize the internal drills of incident handling.

4.2. MoU

No MoU signed in 2014.

4.3. Presentation

In 2014, VNCER participated in and had presentations at 18 international conferences and forums.

5. Future Plans

- To coporate with Authority of Infomation Security to complete the draft of Information security Law to submit to the National Assembly.
- To prepare for promulgating the Decree 77/2012/ND-CP on Amendment and Supplement for the Decree 90/2008/ND-CP on Anti spam.

- 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 Vietnam CSIRT's drill 2015.
- To issue the traning framework of Infomation Security.

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.