APCERT Annual Report 2013

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

APCERT
Asia Pacific Computer Emergency Response Team

CONTENTS

Chair's Message 2013

APCERT has established as its primary goal making the Internet ecosystem cleaner and healthier as a basis for improved cyber security in the Asia Pacific region for the mutual beneficial for all parties using cyberspace. We have been focused on cleaning up malware and cooperation in removing botnets. Going further this year, we are trying to measure the prevalence of malware and the success of remediation approaches as the basis of sharing best practice and providing transparency globally as to the sources of cyber risks.

One of the things we are missing in pursuing our goals is strong sources of data cross-comparable and robust enough to develop statistics to measure the risk levels nationally and globally. Such risk measurement based on sound metrics can enable policy makers to evaluate challenges and the potential effectiveness of a wide range cyber security approaches in managing limited resources. Even more significantly the metrics can serve as the common language between policy and technical operations. I often play a liaison role between technical and policy communities and worry about the very different views the two communities have about cyber security challenges. We talk different languages. Metrics can be a great tool to create agreement around the sources of risk and how to invest in lowering those risks. And the good news is that our members have started to look at this challenge and initiated efforts to create such metrics and measurement approaches with partners such as OECD, our international technical gurus and global data sources.

APCERT has turned its focus from "security" to "regional risk reduction" and we view the cyber security challenges as part of improving the global environment. We must identify the common goals for our measurement and clean up efforts focused on the long term. And I believe such a focus on a healthier, cleaner cyberspace will prove the crucial underlying success factor in achieving global cyber security collaboration based on a common, positive vision rather than focusing on national security competitions.

APCERT members are sharing global risk data and now members will start collaborate developing data aggregation and statistics tool to accelerate the collaboration. As a regional organization, APCERT is clearly leading the best practice collaboration in the

world. Let's continue our great work and extend it to others across the globe.

Lastly I'd like to express my gratitude for all the members your effort within APCERT in continuing to make the globe's cyberspace a better place together, especially the Steering Committee members, Working Group conveners, project leaders and lastly the secretariat for their real hard work. It's been a great pleasure to serve as your chair.

All the best,

Yurie Ito

Chair, APCERT
Director, Global Coordination, JPCERT/CC

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." In collaboration with our liaison 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. (http://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:

http://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 2013, **Macau Computer Emergency Response Team Coordination Centre (MOCERT)** of Macao, China, was approved from General Member to Full 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 2013, APCERT consists of 26 teams from 19 economies across the Asia Pacific region, of which all teams are Operational Members.

Operational Members (26 Teams / 19 Economies)

Team	Official Team Name	Economy
AusCERT	Australian Computer Emergency Response Team	Australia
bdCERT	Bangladesh Computer Emergency Response Team	Bangladesh
BKIS	Bach Khoa Internetwork Security Center	Vietnam
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	Indonesia Security Incident Response Team of Internet Infrastructure	Indonesia
JPCERT/CC	Japan Computer Emergency Response Team / Coordination Center	Japan
KrCERT/CC	Korea Internet Security Center	Korea
mmCERT	Myanmar Computer Emergency Response Team	Myanmar
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

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

During the APCERT AGM 2013, 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 third 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).

Team	Term	Other positions
CERT Australia	March 2012 – March 2014	
CNCERT/CC	March 2012 – March 2014	
ID-SIRTII/CC	March 2012 – March 2014	
JPCERT/CC	March 2013 – March 2015	Chair / Secretariat
KrCERT/CC	March 2012 – March 2014	Deputy Chair
MOCERT	March 2013 – March 2015	
MyCERT	March 2013 – March 2015	

3. Working Groups (WG)

There are currently five (5) Working Groups (WG) 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 (12): AusCERT, BKIS, HKCERT, ID-CERT, ID-SIRTII/CC, JPCERT/CC, KrCERT/CC, Sri Lanka CERT|CC, TechCERT, ThaiCERT, TWNCERT, VNCERT

2) Membership WG (formed in 2011)

- Objective:
  - To review the current membership criteria/classes and determine whether the membership should be broadened to include new criteria/classes and if so how should the new arrangements work.
- Convener (1): KrCERT/CC
- Members (13): AusCERT, BKIS, BruCERT, CNCERT/CC, HKCERT, ID-CERT, ID-SIRTII/CC, JPCERT/CC, MOCERT, MyCERT, Sri Lanka CERT|CC, TechCERT, VNCERT

3) Operational Framework WG (formed in 2011)

- Objective:
  - To identify the changes that need to be made to the existing APCERT Operational Framework
- Convener (1): HKCERT
- Members (9): AusCERT, CNCERT/CC, ID-CERT, ID-SIRTII/CC, JPCERT/CC, KrCERT/CC, MOCERT, MyCERT, Sri Lanka CERT|CC

4) Policy, Procedure and Governance WG (newly 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: MOCERT
- Members: To be determined

5) 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 (22): AusCERT, bdCERT, BruCERT, CamCERT, CCERT, CERT-In, CNCERT/CC, HKCERT, ID-SIRTII/CC, KrCERT/CC, 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 2013

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 2013, APCERT Teams have hosted, participated and/or contributed in the following events:

- **APCERT Drill 2013 (29 January 2013)**

  www.apcert.org/documents/pdf/APCERTDrill2013PressRelease_AP.pdf

  APCERT Drill 2013, the 9th 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 second time. 22 teams from 18 economies of APCERT (Australia, Bangladesh, Brunei Darussalam, People's Republic of China, Chinese Taipei, Hong Kong, India, Indonesia, Japan, Korea, Macao, Malaysia, Myanmar, New Zealand, Singapore, Sri Lanka, Thailand and Vietnam), and 4 teams from 4 economies of OIC-CERT (Egypt, Pakistan, Oman and Tunisia) participated in the Drill. The theme of the drill was "Countering Large Scale Denial of Service Attack."

- **AP*Retreat Meeting (24 February 2013, Singapore)**

  http://www.apstar.org/

  AP* is a community of Asia Pacific Internet related organisations, with the vision to provide a strong united front for all Asia Pacific Internet organisations to deal with international issues of governance, administration, management, research, development, education and public awareness of the Internet.

  SingCERT, as the local team in Singapore, represented APCERT at the AP*Retreat Meeting (held twice a year) and delivered a presentation on APCERT activity updates.

- **APCERT Annual General Meeting (AGM) & Conference 2013 (24 - 27 March 2013, Brisbane, Australia)**

  www.apcert.org/events/conferences/APCERT_2013_Program.pdf

  The APCERT Annual General Meeting (AGM) & Conference 2013 was held from 24-27 March 2013 at Novotel Hotel, Brisbane, Australia, hosted by CERT Australia.

  Programme Overview:

24 March (Sun)	AM:	APCERT Steering Committee Meeting,
		APCERT Working Group Meetings
		(Closed to APCERT members)
	PM:	APCERT Team-Building Event
		APNIC-hosted function
25 March (Mon)	AM:	TSUBAME Workshop
		(Closed to TSUBAME members)
	All day:	Presentations / Panel discussions
		(Closed to APCERT members and Invited guests)
26 March (Tue)	AM:	APCERT AGM 2013
		(Closed to APCERT members)
	PM:	Closed Conference
		(Closed to APCERT members and Invited guests)
		APCERT Gala Dinner
27 March (Wed)	All day:	Public Conference
		(Open to public)

  APCERT AGM & Conference 2013 marked the 10th anniversary of APCERT, providing an opportunity for CSIRTs in the Asia Pacific region, as well as our closely related organisations, to come together and reflect on the cyber threat landscape over the past ten years, share current trends, and also look forward to future challenges and opportunities.

- **TSUBAME Workshop 2013 (25 March 2013, Brisbane, Australia)**

  The APCERT TSUBAME Workshop 2013 on Network Traffic Monitoring Project was held on 25 March 2013, in conjunction with APCERT AGM & Conference 2013. The workshop was organised by JPCERT/CC to enhance the TSUBAME project

and the cooperation among its members.

- **APEC TEL 47 (22 - 27 April 2013, Bali, Indonesia)**

  APCERT Teams participated in APEC TEL 47 SPSG (Security and Prosperity Steering Group) and contributed to a workshop on Combating Botnets. JPCERT/CC, as APCERT Secretariat, also represented APCERT and delivered a presentation on APCERT activity updates, as well as shared APCERT's collaborative activities with OECD's indicator study – OECD's new project to improve cross comparability of CSIRT statistics.

  APCERT holds the APEC TEL guest status (until 2015), and will continue to provide advice and expertise to the SPSG as the security expert community in the Asia Pacific region.

- **25th Annual FIRST Conference (16 - 21 June 2013, Bangkok, Thailand)**

  http://www.first.org/conference/2013/

  APCERT Teams attended the Annual FIRST Conference Bangkok, hosted by ThaiCERT, and shared valuable experience and expertise through various presentations. Participating teams also attended an APCERT lunch meeting.

- **National CSIRT Meeting (22 - 23 June 2013, Bangkok, Thailand)**

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

- **AP*Retreat Meeting (25 August 2013, Xi'an, People's Republic of China)**

  http://www.apstar.org/

  CNCERT/CC, as the local team in China, represented APCERT at the AP*Retreat Meeting (held twice a year) and delivered a presentation on APCERT activity updates.

- **APEC TEL 48 (16 - 21 September 2013, Honolulu, Hawaii)**

  As APCERT Chair, JPCERT/CC represented APCERT at APEC TEL 48 SPSG (Security and Prosperity Steering Group), and shared APCERT's vision to help create a safe, clean and reliable cyber space in the Asia Pacific region through global partnership, as well as introduced national programmes and best practices on bot clean-up in the Asia Pacific region, at SPSG's Workshop on Botnet.

- **APCERT Technical Workshop on Security (TWS) 2013 (23 - 24 September 2013, Yogyakarta, Indonesia)**

  http://apcert-tws2013.idsirtii.or.id/

  APCERT Technical Workshop on Security (TWS) 2013, hosted by ID-SIRTII/CC in conjunction with the FIRST Technical Colloquium (TC), provides a discussion forum and hands-on trainings for APCERT members and invited guests to share and learn information about vulnerabilities, incidents, tools and all other issues that affect the operation of incident response and security teams. Topics included combating botnets and spam, and network forensics.

- **ASEAN CERT Incident Drill (ACID) (2013 (9 October 2013)**

  ACID 2013, led and coordinated by SingCERT, entered its 8th iteration with participation including ASEAN CERTs and APCERT Teams. The drill was completed successfully, providing a platform 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.

- **Seoul Conference on Cyberspace 2013 (17 - 18 October 2013, Seoul, Korea)**

  http://www.seoulcyber2013.kr/en/

  As APCERT Chair, JPCERT/CC (Ms. Yurie Ito) attended the Seoul Conference and presented APCERT's vision, activities and achievements. The Seoul Conference was a follow-up to the conferences on cyberspace that were held in London (2011) and Budapest (2012) respectively. The theme of this year's Conference was *Global Prosperity through an Open and Secure Cyberspace – Opportunities, Threats and Cooperation*, and was composed of plenary sessions and panels on economic growth and development, social and cultural benefits, cyber security, international security, cybercrime, and capacity building.

- **2nd Annual CISO Asia Summit (12 November 2013, Kuala Lumpur, Malaysia)**

  www.cisoasiasummit.com

  APCERT served as a supporting organisation for the event.

- **CSM-ACE 2013 (13 - 14 November 2013, Kuala Lumpur, Malaysia)**

  www.csm-ace.my

APCERT served as a supporting organisation for the event.

- OIC-CERT Annual Conference 2013 (18 - 20 November 2013, Bandung, Indonesia)
  http://agmoicert2013.idsirtii.or.id/
  Pursuant to the Memorandum of Understanding on collaboration between APCERT and OIC-CERT in September 2011, JPCERT/CC, as APCERT Secretariat, represented APCERT at this conference and delivered a presentation on APCERT activity updates, as well as shared the TSUBAME Network Traffic Monitoring Project.

- The 4th APT Cybersecurity Forum (3 - 5 December 2013, Kuala Lumpur, Malaysia)
  http://www.apt.int/2013-CSF4
  The 4th APT Cybersecurity Forum was organised by the Asia-Pacific Telecommunity.
  MyCERT, as the local team in Malaysia, represented APCERT at this Forum and delivered a presentation on APCERT activity updates.

- CSIRT Trainings for AfricaCERT
  JPCERT/CC organised trainings for CERTs/CSIRTs in Africa and introduced APCERT activities during the trainings on behalf of APCERT.
  - 9 - 14 June 2013, Zambia (in conjunction with AfNOG-14)
  - 24 - 28 November 2013, Cote d'Ivoire (in conjunction with AFRINIC 19, in cooperation with FIRST and KrCERT/CC)

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 serves as a Steering Committee member of FIRST since June 2011.

- **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 2013, SC members held seven (7) teleconferences and two (2) face-to-face meeting to discuss on APCERT operations and activities.

16 January	Teleconference
27 February	Teleconference
24 March	Face-to-face meeting in conjunction with APCERT AGM & Conference 2013, Brisbane, Australia
4 June	Teleconference
5 August	Teleconference
26 August	Teleconference
23 - 24 September	Face-to-face meeting in conjunction with APCERT TWS 2013, Yogyakarta, Indonesia
15 November	Teleconference
4 December	Teleconference

3. APCERT Study Calls

Following the discussions during APCERT AGM 2012, APCERT held one (1) study call in 2013 as a knowledge sharing platform for APCERT Teams to exchange technical know-how, information and ideas.

Date: 25 January 2013
Topic: "Manual malware detection and cleaning"
Speaker/Organiser: BKIS (Vietnam)

For further information on APCERT, please visit the APCERT website or contact

the APCERT Secretariat as below.

URL: http://www.apcert.org

Email: apcert-sec@apcert.org.

III. Activity Reports from APCERT Members

1. AusCERT

Australia Computer Emergency Response Team - Australia

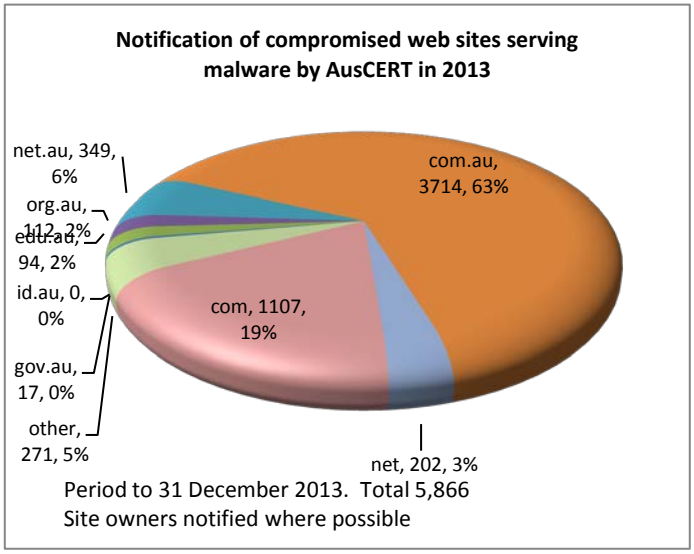
1. About AusCERT

AusCERT is the premier Computer 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

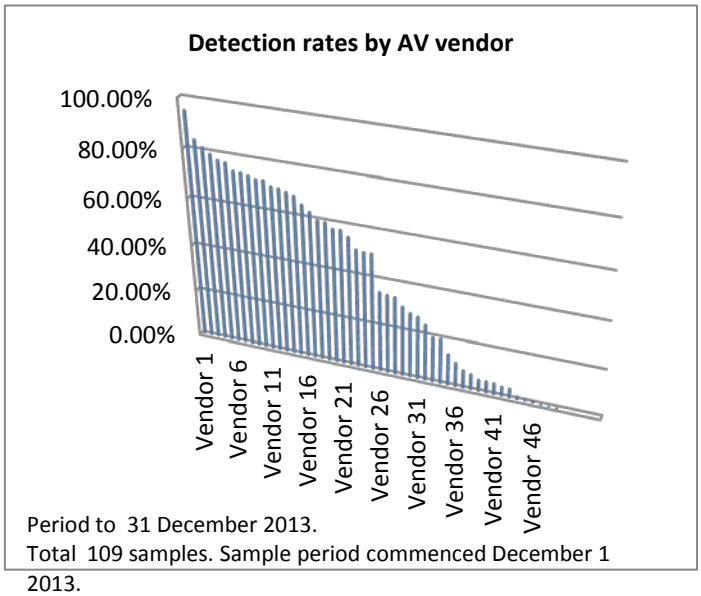
AusCERT distributes security advisories and bulletins to its members by email and publishes a portion of them to its public website. Bulletins are published in a standardised format with a consistent approach to classifications of vulnerabilities, impacts and affected operating systems.



During 2013, 1853 External Security Bulletins (ESBs) and 140 AusCERT Security Bulletins (ASBs) were published. The ESBs are made publicly available immediately however the ASBs are available to members only for a period of one month after release, beyond which time they are made public.

2.2 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.



Processing of malware using AusCERT's automated system commenced late in 2013, therefore statistics do not represent the manual processing carried out during most of the year, however future (2014) statistics will cover the full year period.

Malware is automatically compared against multiple vendors' detection engines using the Virus Total service.

2.3 Compromise evidence collection and data distribution

AusCERT notifies members of compromise of their web sites, hosts and accounts.

2.4 Certificate service

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

3. Events 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 hosts "Security on the Move" conferences in various Australian cities.

4. Achievements

4.1 Carna Botnet research and presentations

AusCERT contacted the anonymous researcher who deployed the Carna Botnet via devices using default telnet credentials to carry out a census of the Internet IPv4 space. The researcher handed over approximately 1.3 million IP addresses representing compromised devices within the Carna Botnet, from which AusCERT was able to extract individual countries and provide relevant data to owners and CERT teams.

AusCERT published a research paper and presented the work at numerous conferences worldwide including Blackhat (Sao Paulo), DeepSec (Vienna), AusNOG (Sydney), APNIC (Xian), The Hackers Conference (New Delhi), AusCERT 2013 (Gold Coast) and AusCERT Security on the Move Conferences (Sydney and Brisbane). The research paper is available here: http://bit.ly/carna-paper

4.2 Compromised Adobe credentials and MS Zero Access

AusCERT processed the stolen Adobe credentials and Microsoft Zero Access botnet host list, detected affected members and disseminated information as appropriate.

4.3 Malware processing

During the latter part of 2013, AusCERT automated processing of malware including submission of poorly detected samples to AV vendors. Statistics are now captured for this activity.

5. 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

2. 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 2013 as compare to the year 2012. In year 2012, bdCERT has received 361972 incident reports, which has been originated from unique IPs. Taxonomy statistics of incidents report are shown in figure 1. Majority of incidents are related with Bots, Spam, Open Resolvers and bots.

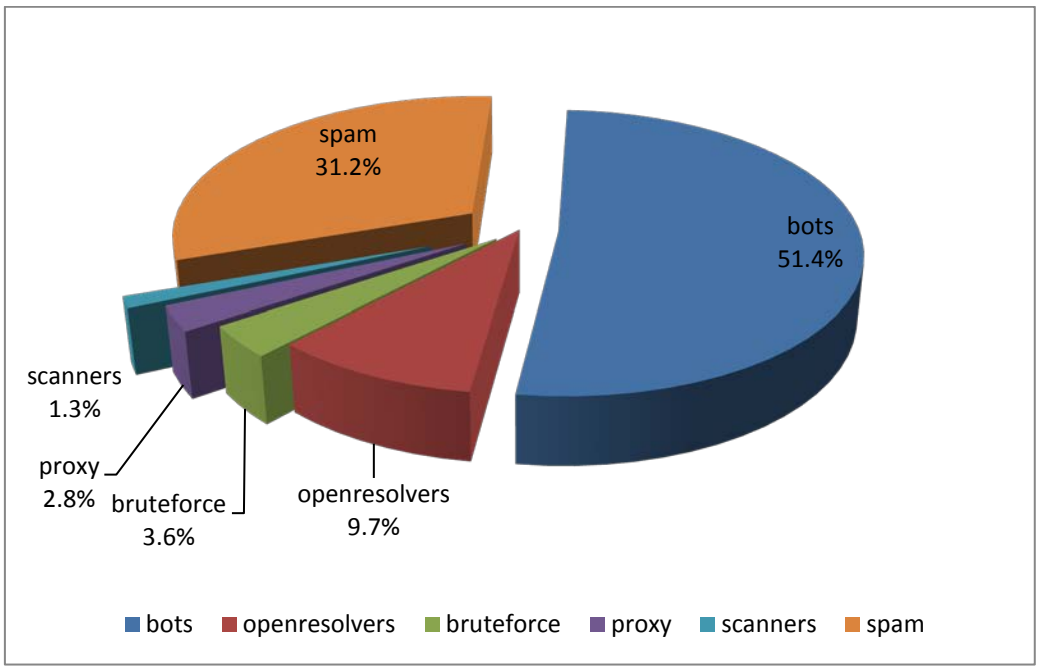


Figure 1: Taxonomy statics of Incident

3. EVENTS ORGANIZED / CO-ORGANIZED

3.1 Trainings & Seminars Organized

bdCERT have successfully organized various Information Security training, workshops and seminars with sponsors from various Government and Private Organizations.

- Training program on DNS/DNSSEC and Network Security Workshop (8-11 November 2013):

  bdCERT team collaborated with ISOC Chapter in Bangladesh and APNIC to host this training.

- Workshop: Network Security 22-24 May 2013

  bdCERT team collaborated with ISOC Chapter in Bangladesh and APNIC to host this workshop.

3.2 Trainings & Seminars Participated

- 2013 APISC Security Training Course
  bdCERT representative participate in 2013 APISC Security Training Course held at Korea and supported by KrCERT/CC.

4. Collaboration

4.1. International Collaboration

- Participated in the APCERT Drill (January 2013). The theme of the drill this year was "Countering Large Scale Denial of Service Attack".

4.2. Location Collaboration

- National Cyber Security 2013 (17th Feb - 3rd June 2013)

bdCERT actively participated in drafting the first National Cyber Security Strategy endorsed by Access to Information (a2i), Prime Minister's Office. The strategy was drafted by a special committee under the supervision of Controller of Certificate Authorities, Ministry of ICT. bdCERT has played a vital role by providing valuable inputs and expert opinions.

- 19th September 2013

  bdCERT has been actively consulting and supporting Leveraging ICT for Growth, Employment and Governance Project under Ministry of ICT, who are trying to establish a Government CERT by the name of Computer Incidence Response Team (CIRT). A special committee consisting law enforcement agencies, defense wings, government agencies and other stake holders have been incorporated. Several meetings has been held and a special information security training was held for the better understanding of the committee. bdCERT is advising and providing all kinds of information and experience as required by the government agency.

5. FUTURE PLANS & Projects

a) Government Endorsement for BDCERT
b) Full Membership of APCERT
c) Full Membership of OIC-CERT
e) Building Awareness
f) Fund Raising
f) Consulting to form other CERTs within the constituents

3. BKIS

Bach Khoa Internetwork Security Center - Vietnam

1. About Bkis - Vietnam

Bkis is a Vietnam's leading organization in researching, deploying network security software and solution. Bkis was established on December 28th, 2001, and became full member of APCERT in 2003.

Head Office: 5th Floor, Hitech Building, Hanoi University of Technology, 1A Dai Co Viet, Hanoi, Vietnam.

2. Activities & Operations

2.1 Security Statistics in Vietnam

Installing spyware without vulnerability exploitation

Spreading viruses has truly become an "industry" of espionage activities in 2013, as predicted by Bkav from the beginning of the year. This "industry" exists not only in developed countries like the U.S., Germany, France, etc. but also in Vietnam. According to records of Bkav, in the past year, spyware appeared in most of important organizations, from government agencies, National Assembly to the Ministry of Defense, Ministry of Public Security or banks, research institutes, universities, etc. These spywares took advantage of security vulnerabilities in text files (Word, Excel, PowerPoint) to spread.

Since the end of 2013, taking advantage of text files to install spywares has stepped up. Hackers switch to using fishing, which makes **exploiting vulnerabilities become unnecessary in installing spywares**. By December, Bkav discovered a series of malicious code being inserted into text files despite no vulnerabilities exploited. The malware hide themselves in forms of thumbnails embedded directly into the file. To read the contents, users will definitely click to open the larger images, thus activate the malware. *"With this method, any computer can be installed spywares with even no vulnerabilities. Phishing to install spywares will be widely used and become the trend in 2014",* said Mr. Ngo Tuan Anh, Bkav's Vice President of Internet Security.

Malicious code spreading across multi platforms

"Connecting mobile and computer being no longer safe" is the message of Bkav's Internet security bulletin released in November 2013. DroidCleaner and SuperClean are the first viruses having the ability to infect cross between computer and smartphone.

Multi-platform malware is highly concerned when the world of smartphones and computers are becoming a "unity". This similarity helps hackers easily create a malware operating simultaneously on many different platforms. In 2014, this trend will strongly continue and even bloom because of smartphone market's rapid development. More than 1 billion smartphones were sold worldwide in 2013, and this figure is predicted to reach 1.7 billion in 2017 (according to IDC). Particularly in Vietnam, there were 17 million smartphone users and approximately 7 million computers in use in 2013.

Faking browser for smartphone to spread malware

In a prediction of Internet security situation in 2013, Bkav experts stated the trend of faking softwares and applications to infect viruses on mobile would continue to grow in the coming years. In 2013, fake softwares targeting smartphones not only increased in quantity but also extended their object range in order to blind antivirus softwares and cheat users.

After Instagram, Angry Birds, and even antivirus software are faked by malwares, now most popular browsers like Firefox, Google Chrome and so on are also disguised to attack users. Last November, a series of these browsers' fake updates were launched onto unofficial app markets with the aim of taking advantage of users' high searching demand to spread malware. Faking softwares and popular applications has become headache and will continue to be a trend in 2014.

DDoS attacks continuing when users' consciousness remaining unchanged

Reviewing Internet security situation of the year 2013, we cannot skip mentioning DDoS attacks paralysing a series of online newspapers. According to research of Bkav's experts, these attacks were carried out through a giant botnet system made up of countless users' computers. Taking advantage of users' habit to arbitrarily download softwares and applications without regarding to their origins, hackers

spread viruses by inserting malcious code into popular softwares such as Unikey, download managers, video editors, etc. then post them on forums. Users downloading these fake softwares accidentally turn their computers to be a zombie in the botnet system.

Unless users change their habits of installing softwares from unknown origins, unintentionally abetting DDoS will remain. Bkav advises users to search for safe sources or app stores supplied by reputable vendors to download softwares.

Mr. Ngo Tuan Anh, Bkav's Vice President of Internet Security, concluded: *"The year 2013 has passed with too many Internet security issues. Connected world brings us a lot of benefits but also many downsides. That is the reason why Bkav always makes efforts to alert users as well as release technological solutions to protect them, raise social awareness about Internet security"*.

3. Events organized / co-organized

3.1 Training Courses

Network Security Training Courses:

August 2012: 2 classes for Network Administrators in provincial offices

Security Awareness Training Courses:

August, November 2012: 2 classes for officials in provincial offices

3.2 Security Articles

In 2013, Bkis sent Vietnamese presses 7 researches on the Internet security, 5 other researches were sent to international newspapers.

3.3 Seminar

October 2012: Organized a white hat conference, established a white hat forum.

4. 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 2013

2.1 Incidents response

In 2013, defacement have increased enormously especially in the private sector. Most for the private sector website are hosted using third party website provider which some did not provide any security control measure at all. A Distributed Denial of Service attack (DDOS)had occur to our local ISP which disrupt their daily operations and affected some of their clients. Most of the clients have difficulty to access their resources from the internet since the border router which they used are being DDOS attack. BruCERT provide assistance in identifying the attackers origins country and notifying the relevant CERTS in requesting to take down those system. . The statistic of the security incident is shown as Figure 1.

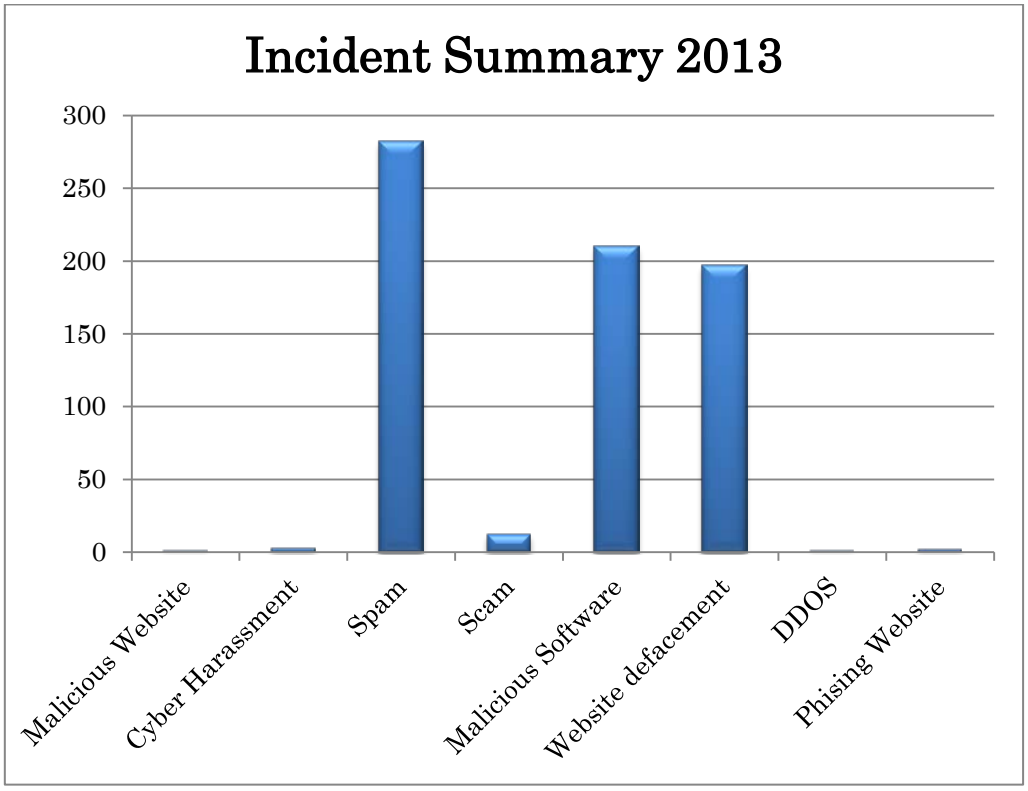


Figure 1

Types of Attack	Count
Malicious Website	1
Cyber Harassment	2
Spam	282
Scam	23
Malicious Software	660
Website defacement	32
DDOS	1
Phising Website	2

Table 1

3. BruCERT Activities in 2013

3.1 Seminars/Conferences/Meetings/Visits

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

- On 24th March until 27th 2013 - Three BruCERT delegates attended the APCERT 2013 Annual General Meeting which takes place at Brisbane Australia, hosted by CERT Australia.

- On 18th until 20th November 2013, BruCERT Attended the OIC-CERT Annual Conference 2013 and the 5th Annual General Meeting, Hilton Hotel Bandung, Indonesia.

3.2 BruCERT Awareness Campaign

- Handover of Digibytes booklets to Maktab Sains *(3rd January 2013)*

- BruCERT presented 200 copies of Digibytes booklets to Maktab Sains, for the new intake of Year 7 students. The booklets will be used as part of their studies in Business, Art and Technology (BAT).

- Awareness Ads in Brunei Times *(March 2013 Onwards)*

  - Brunei Times has agreed to periodically publish public awareness ads in the newspaper. The ads consist of excerpts from Digibytes, educating the public on information security threats and best practices, aiming to reduce the risk of individuals falling victim to cybercrimes.

- Cyber Security Seminar for Secondary Schools *(Throughout 2013)*

  - AITI has organized a series of school talks conducted by BruCERT and RBPF at public and private secondary schools around the country. In addition to the talk, BruCERT also conducted information security awareness surveys and distributed awareness booklets and t-shirts.

- "Secure Verify Connect" website Launch and Roadshow *(November 2013)*

  - As part of an awareness campaign, BruCERT has developed an informational website for the general public to learn about online safety. The website is divided into 3 sections to cater for different audiences: adults, teens & kids. There is also an e-learning feature where registered participants can take online courses in IT Security Awareness.
  - Following the official launch of the SVC awareness website, BruCERT will hold a 3-day roadshow at The Mall, Gadong. The booth will highlight the new website, and offer activities for the general public to participate and learn about IT security as they play.
  - Planned activities include:
    - Website treasure hunt – Players look for treasures on the website in order to win a prize. This game encourages people to browse through the SVC website.

- Password Challenge – The objective is for the participant to create the most secure password. The password which takes the longest time to crack would win a grand prize.
- Quiz – The participant answers 3 multiple choice questions on the iPad in order to win a prize. The questions cover a variety of topics.
- Think Before You Post – Players are given a series of items and have to choose whether it is safe to post such information online.
- Spot The Difference – Players are shown two screenshots of the same website, with some small differences. The objective is to identify the fake website, which could be used as a phishing website.

4. Conclusion

In 2013, 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 roadshows, security awareness to schools and publication of security awareness magazine will better educate the people the importance of Information security and online safety.

5. 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 providers.

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 Government Cyber Security Operations Centre (CSOC), and
- providing a single Australian point of contact in the expanding global community of national CERT's to support more effective international cooperation.

Throughout 2013, 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
- provided a data repatriation capability to CERT Australia constituents & foreign partner CERT and security teams
- 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 Cyber Security Operations 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 2013, CERT Australia had over 11,500 cyber incidents reported to it, an increase of approximately 57 per cent from 2012. These incidents required a range of responses depending on their nature. CERT Australia also produced and disseminated sensitive advisories on cyber vulnerabilities affecting SNI.

2.2 Data repatriation

CERT Australia continued to repatriate stolen records to the responsible organisations (including Australian businesses and peer national CERTs and other major international security teams). These records contained a range of information including sensitive data, user credentials and https-secured communications.

3. Events organised/co-organised

3.1 Training

CERT Australia facilitated participation by the Australian Communications and Media Authority (ACMA) in the September 2013 Technical Workshop on Security hosted by ID-SIRTII/CC in Yogyakarta.

3.2 Drills

CERT Australia participated in the APCERT Drill in January 2013 and the ASEAN CERT Incident Drill (ACID) held in October.

3.3 Seminars

CERT Australia co-hosted a CERT 'Birds of a Feather' session at the AusCERT 2013 conference in May. The meeting was attended by representatives from a range of Australian and international CERTs and information security organisations, and discussed topics such as international collaboration on projects and operations.

4. Achievements

In March 2013, CERT Australia hosted the 10th Anniversary APCERT Annual General Meeting and Conference in Brisbane, Australia.

In August, CERT Australia co-hosted the first Panoply Cyber Security Competition to be held in Australia. CERT Australia, in conjunction with the US Department of Homeland Security and the Center for Infrastructure Assurance and Security, hosted the event at the Annual Security in Government Conference in Canberra.

4.1 Presentations

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

- APCERT AGM and Conference, March – Australia
- International Watch and Warning Network (IWWN) Annual Meeting, May – Switzerland
- FIRST conference, June – Thailand
- Blackhat & DefCon, July – USA
- 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 2013 are:

- CERT Australia participated in the 2013 APCERT Drill held in January
- Hosted APCERT 10th Anniversary AGM & Conference in March
- CERT Australia participated in the 2013 ASEAN CERT Incident Drill (ACID) held in October.

6. 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 2013 is given in the following table:

Activities	Year 2013
Security Incidents handled	71780
Security Alerts issued	12
Advisories Published	92
Vulnerability Notes Published	223
Trainings Organized	25
Indian Website Defacements tracked	24216

Open Proxy Servers tracked	**2224**
Bot Infected Systems tracked	**7457024**

Table 1. CERT-In Activities during year 2013

2.2 Abuse Statistics

In the year 2013, CERT-In handled more than 71000 incidents. The types of incidents handled were mostly of Spam, Website intrusion & malware propagation, Malicious Code, Phishing and Network Scanning & Probing.

The year-wise summary of various types of incidents handled is given below:

Security Incidents	2005	2006	2007	2008	2009	2010	2011	2012	2013
Phishing	101	339	392	604	374	508	674	887	755
Network Scanning / Probing	40	177	223	265	303	277	1748	2866	239
Virus / Malicious Code	95	19	358	408	596	2817	2765	3149	160
Spam	-	-	-	305	285	181	2480	8150	65877
Website Intrusion & Malware Propagation	-	-	-	835	6548	6344	4394	4591	4265
Others	18	17	264	148	160	188	1240	2417	484
Total	**254**	**552**	**1237**	**2565**	**8266**	**10315**	**13301**	**22060**	**71780**

Table 2. Year-wise summary of Security Incidents handled

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

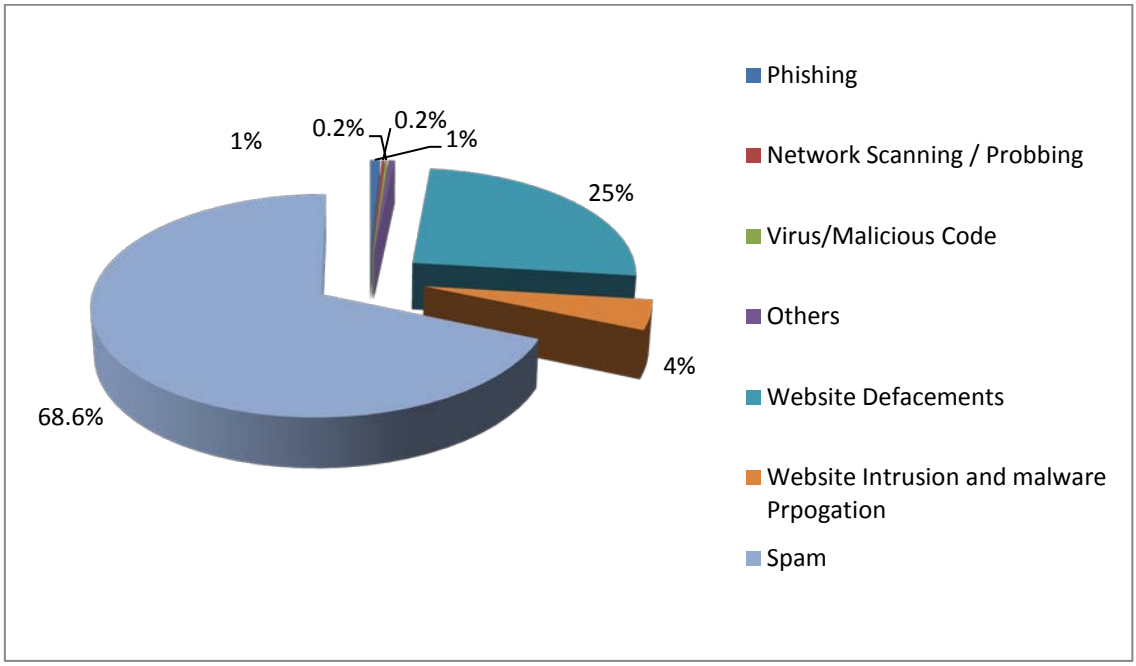


Figure 1. **Summary of incidents handled by CERT-In during 2013**

2.3 Incident Trends

The trends of incidents reported to and handled by CERT-In and cyber attack trends during the year 2013 are as follows:

- **Website Intrusion and Malware Propagations**

  These are website intrusions and drive-by-download attacks through compromised websites. Around 4265 malicious URLs were tracked in the ".in" space. The legitimate web sites which are compromised resulting in redirection of visitors to malicious websites that exploit vulnerabilities in client side applications to deliver malware such as key loggers and information stealers. The malicious websites comprise attack tool kits such as blackhole, RedKit, Nuclear, Darkleech etc. The malicious code on the exploit kits included shellcode and Java scripts besides exploits for vulnerabilities in Internet Explorer, Java SE/SDK, Adobe Flash, Silverlight etc.

- **Vulnerabilites and Malware affecting Android mobile devices**

  Critical vulnerabilities were reported in Android based systems such as "Master key vulnerability", "PRNG initialization vulnerability" etc. Exploitation of

master key vulnerability enables attackers to bypass verification process to install malicious files on the affected device.

The malware affecting Androd mobile platform rose exponentially. Android.Adrd is a trojan horse that arrives bundled with legitimate Android applications and infects Android based smart phones. The malware seems to be created by downloading an application from a marketplace, modifying the legitimate application and then redistributing via marketplace or other separate channels. The Trojan may change mobile device settings and steal device information. Other prominent Android malware reported are Superclean/DroidCleaner, USB cleaver etc.

- **Trojan.Cryptolocker**

  Trojan Cryptolocker is spreading via malicious hyperlinks shared via spam emails, social media, malicious email attachments (fake FedEx and UPS tracking notices), drive-by-download or as a part of dropped file from other malwares. Cryptolocker encrypts files located within local drives, shared network drives, USB drives, external hard drives, network file shares and even some cloud storage drives using RSA public-key cryptography (2048-bit), with the private key stored only on the malware's control servers.

- **ZeroAccess Botnet**

  Win32/Sirefef a.k.a "Zero Access" is a widespread multi-component malware family of rootkits which is affecting the windows operating systems. The threat spreads majorly by exploit kits, use of pirated softwares and other malware downloaders. It uses disk-level hooking to hide itself (hide processes, related files, network activites,) in order to hinder its detection and removal on infected computer. Large number of infected systems are tracked and notifications issued to concerned Internet Service Providers.

- **DDoS attack trends**

  Multiple websites in the Government and Corporate sectors were targeted with Distributed Denial of Service attacks during 2013. It has been observed that vulnerabilities in Content Management Systems (Joomla!, Wordpress, etc.) are being exploited and attack scripts are embedded on compromised websites/servers which utilizes resources of web servers to launch Distributed

Denial of Services attacks.

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 24216 numbers of defacements have been tracked. Most of the defacements were under '.in' domain, in which a total 15490 '.in' domain websites were defaced.

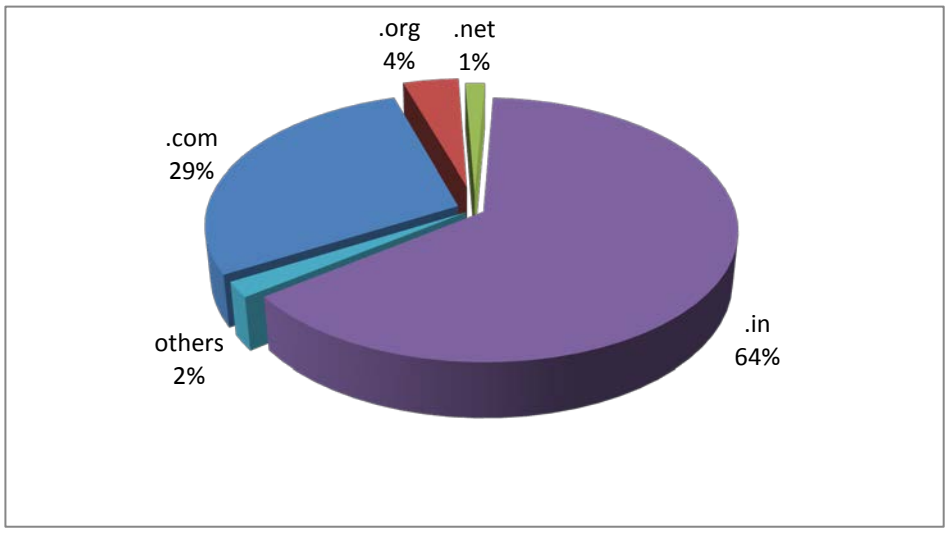


Figure 2. Indian websites defaced during 2013 (Top Level Domains)

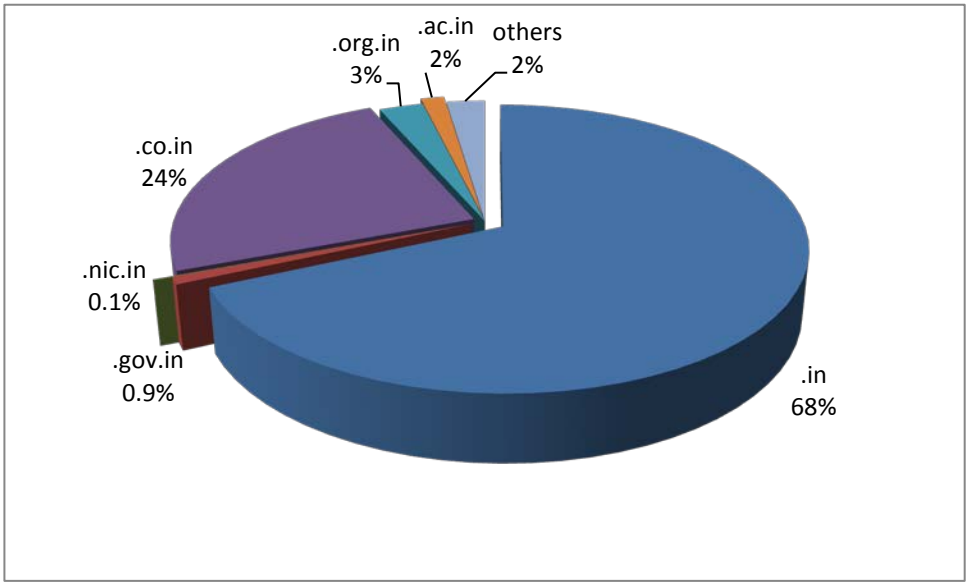


Figure 2.1 .in ccTLD defacements during 2013

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 2224 open proxy servers were tracked in the year 2013. The month-wise distribution of open proxy servers tracked during this year is shown in the figure 3.

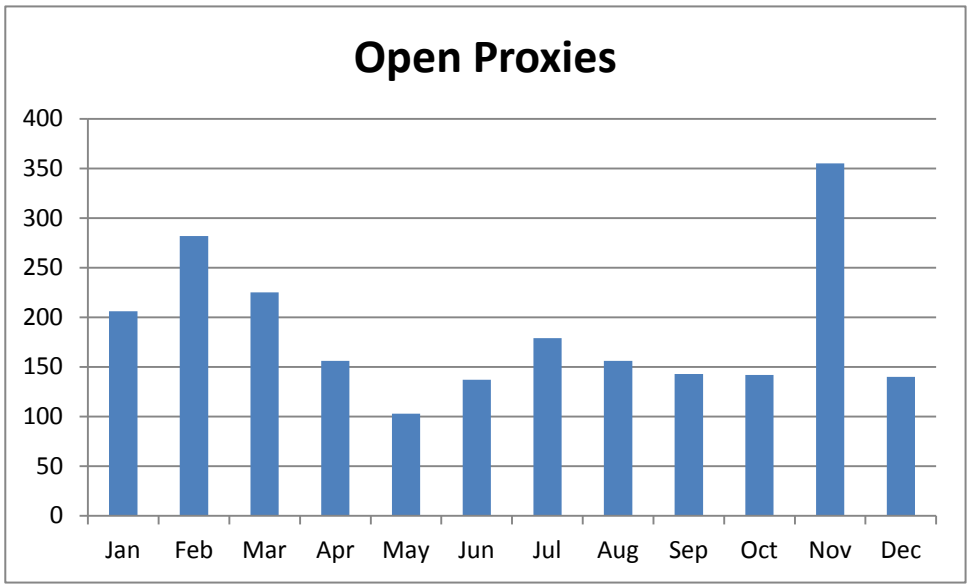


Figure 3. Monthly statistics of Open Proxy Servers in 2013

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 2013.

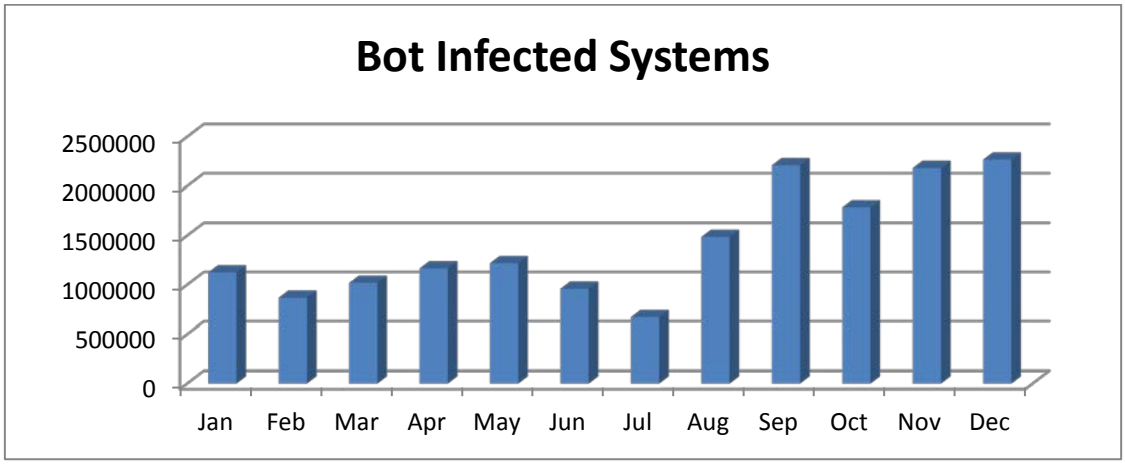


Figure 4. Botnet statistics in 2013

2.7 Collaborative Incident resolution

During the year 2013, CERT-In worked in collaboration with security/product vendors and Internet Service Providers in India to detect the botnet infected systems by tracking the Command & Control servers. Botnets such as Bamital, Citadel and ZeroAccess 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 22 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 2013:

- Workshop on "Data Centre Security " on January 11, 2013
- Workshop on "Linux Security" on January 24, 2013
- Workshop on "Introduction to Cyber Security and Cyber Forensics" on February 18, 2013
- Workshop on "Network Security" on February 22, 2013
- Workshop on "Web Application Security: Current trends" on March 07, 2013
- Workshop on "Mobile Forensics" on March 22, 2013
- Workshop on "Advanced Web Application Security " on April 29, 2013
- Workshop on "Introduction to Cyber Security & Crisis Management Plan(CMP) " on April 30, 2013
- Workshop on "Network Security : Perimeter Defence in Depth" on May 24, 2013
- Workshop on "Virtualisation & Cloud Security " on May 31, 2013
- Workshop on "Cyber Crime Investigation & Cyber Forensics" on June 14, 2013

- Workshop on "Vulnerability Assessment & Penetration Testing " on June 18, 2013
- Workshop on "Cyber Espionage, Infiltration and Combating Techniques" on July 11, 2013
- Workshop on "Windows 8 Security " on August 12, 2013
- Workshop on "Information Security Compliance, Assurance and Crisis Management Plan" on August 27, 2013
- Workshop on "Latest Security Trends " on September 24, 2013
- Workshop on "Cyber Security: Threats & Mitigation" on September 30, 2013
- Workshop on "Cyber Security and Cyber Forensics" on October 14, 2013
- Workshop on "Network Penetration Testing" on October 25, 2013
- Workshop on "Wireless Network Security" on October 31, 2013
- Workshop on "Advanced Persistent Threats" on November 12, 2013
- Workshop on "Cyber Security Policy and Crisis Management Plan" on November 22, 2013
- Workshop on "Advanced Computer Forensics" on December 05, 2013

3.2 Cyber Security Drills

CERT-In successfully participated in the APCERT Incident Handling drill conducted in January 2013 and ASEAN CERTs Incident Handling Drill (ACID 2013) held in October 2013.

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 8 Cyber security drills of different complexities with 115 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. 8th Cyber Security Drill Mock Drill was conducted on 20th December

2013. This time, cyber security drill involved simulated cyber attacks as well as simulated cyber crisis scenarios.

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.

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, 9 implementation enabling workshops have been conducted. Services of CERT-In empanelled IT security auditors are being used to verify compliance.

- 21 auditors were empanelled for audit of IT infrastructure after a fresh round of skill assessment in the year 2013, in addition to existing 22 auditors.

- 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.
- MoU is being signed with KISA 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

7. CNCERT/CC

National Computer network Emergency Response technical Team / Coordination Center of China – People's Republic of China

1. About CNCERT

1.1 Introduction

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

1.2 Establishment

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

1.3 Workforce power

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

1.4 Constituency

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

1.5 Contact

E-mail：cncert@cert.org.cn

Hotline：+8610 82990999（Chinese）, 82991000（English）

Fax：+8610 82990375

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

2. Activities & Operations

2.1 Incident handling

In 2013, CNCERT received a total of about 31.7 thousand incident complaints, a 65.5% increase from the previous year. And among these incident complaints, 971 were reported by overseas organizations, making a 19.1% drop from the year of 2012. As shown in Figure 2-1, most of the victims were plagued by vulnerability (34.5%), phishing (33.4%) and website defacement (14.4%). Different from the previous year, vulnerability overtook phishing to become the most frequent incident complained about. And website defacement ranked the third place with a considerable increase of 569.4% from 2012.

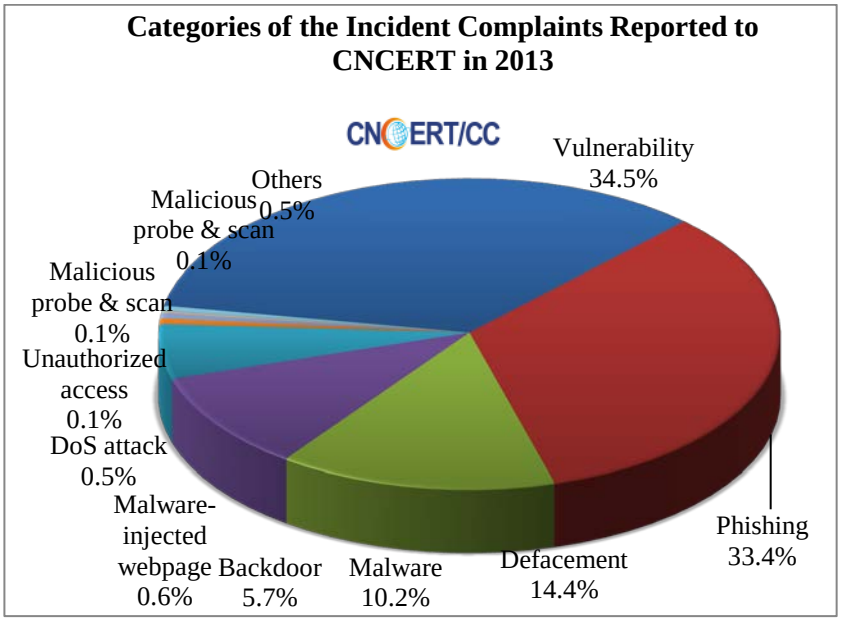


Figure 2-1Categories of the Incident Reported to CNCERT in 2013

In 2013, CNCERT handled almost 31.2 thousand incidents, a significant rise of 65.8% compare with that in 2012. Besides, CNCERT has carried out 8 clean-up campaign against Trojan and Botnet as well as 8 clean-up campaigns against mobile malware in 2013. As illustrated in Figure 2-2, vulnerability (34.9%) dominated the categories of the incidents handled by CNCERT In 2013, followed by phishing (32.7%) and website defacement (14.6%).

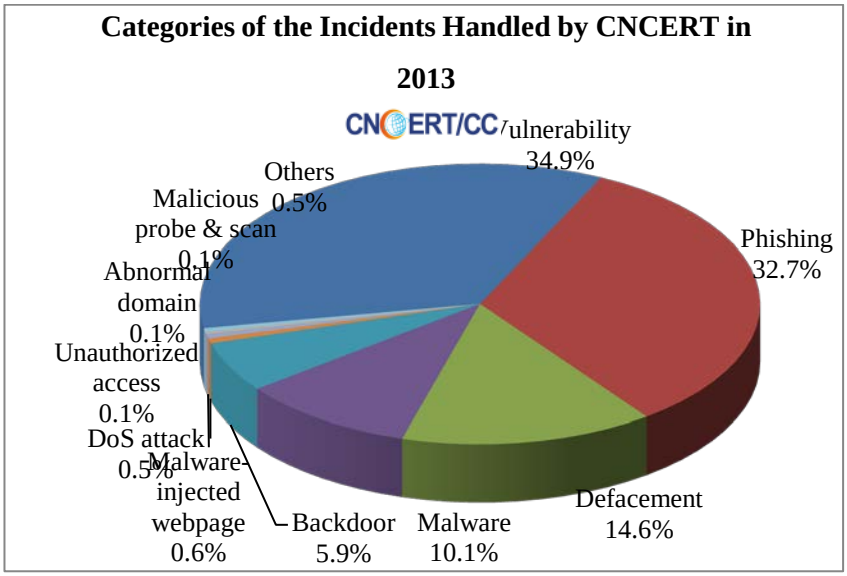


Figure 2-2 Categories of the Incidents Handled by CNCERT in 2013

2.2 Internet Awareness

2.2.1 Compromised Hosts and Websites

In 2013, CNCERT monitored and discovered about 4.0 million incidents spreading known-type malware, which involved about 2.6 thousand domain names, about 4.8 thousand IP addresses and 17.6 thousand malware download links. Figure 2-3 depicts the monthly statistics of malware spreading incidents in 2013, with the most rampant malware activity in the last two months.

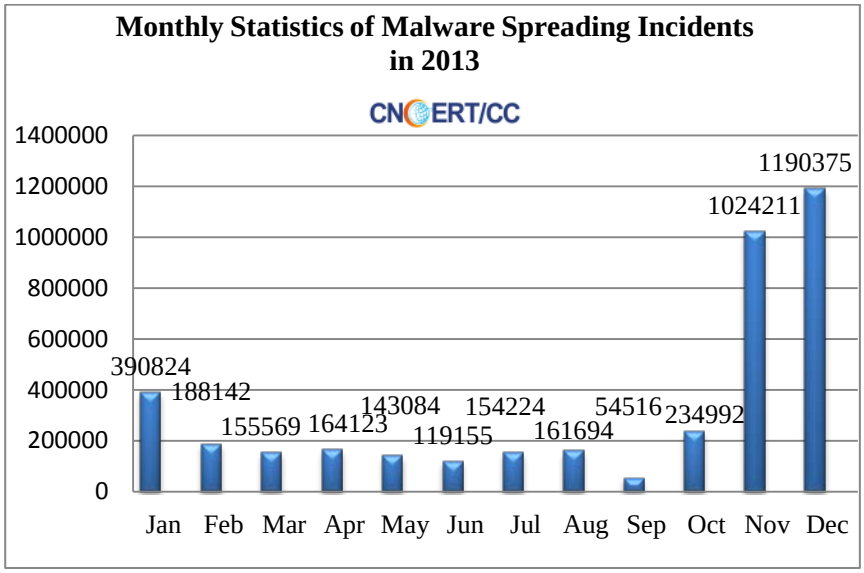


Figure 2-3 Monthly Statistics of Malware Spreading Incidents in 2013

In mainland China, IPs of the hosts infected with Trojan or Botnet reached about 11.4 million, which decreased by 22.5% compared with that in 2012.

By CNCERT's Conficker Sinkhole, over 1.8 million hosts per month on average were suspected to be infected all over the world. And 17.2 million compromised hosts per month were located in mainland China. As shown in Figure 2-4, mainland China (13.7%) had the most infection, followed by Brazil (10.0%), and India (6.5%).

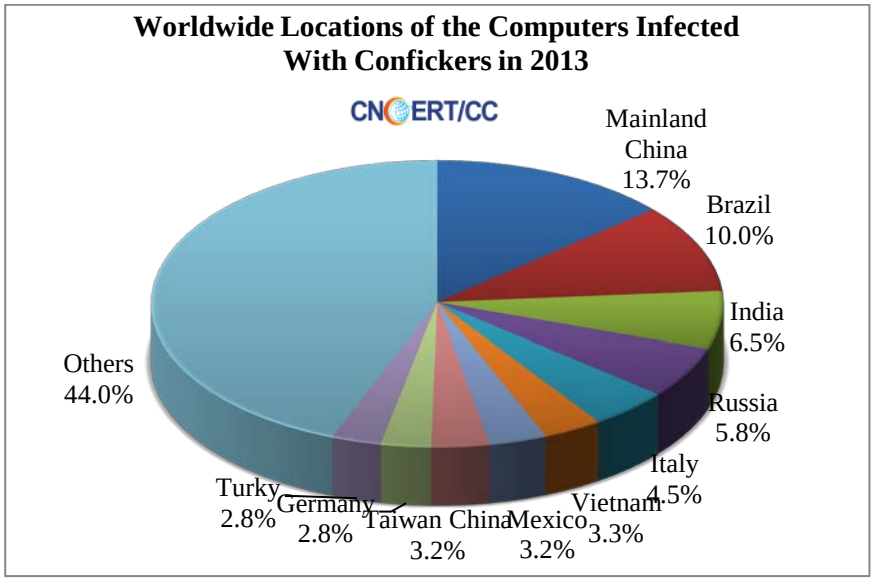


Figure 2-4 Worldwide Locations of the Computers Infected With Confickers in 2013

About 24.0 thousand websites in mainland China were defaced, a considerable increase of 46.7% compare with that in 2012, including 2430 government sites. Besides, about 76.2 thousand websites were detected to be planted with backdoors and secretly controlled, including 2425 government sites.

2.2.2 Location of Malicious IPs

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 29.1 thousand oversea C&C servers which decreased 60.2% from 2012. The US hosted the largest number of oversea C&C servers' IPs of Trojan or Botnet, followed by Korea and HongKong China.

In 2013, CNCERT found about 30.2 thousand phishing sites targeting the websites in mainland China. About 4240 IPs were used to host those fake pages. About 90.2% were out of mainland China. Most of the phishing servers (53.4%) were located in US.

CNCERT found almost 47.3 thousand backdoor controlled IPs. Besides, about 16.4 thousand were located in mainland China, 6215 (13.1%) were located in the US, followed with 3505 (7.4%) in Indonesia and 2007 (4.2%) in Korea.

2.3 Mobile Awareness

In 2013, CNCERT collected about 702.8 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 (71.5%), fee consumption (15.1%) rose to the second place. And followed it were those intended for system damage and stealing information, both accounting for 3.2%.

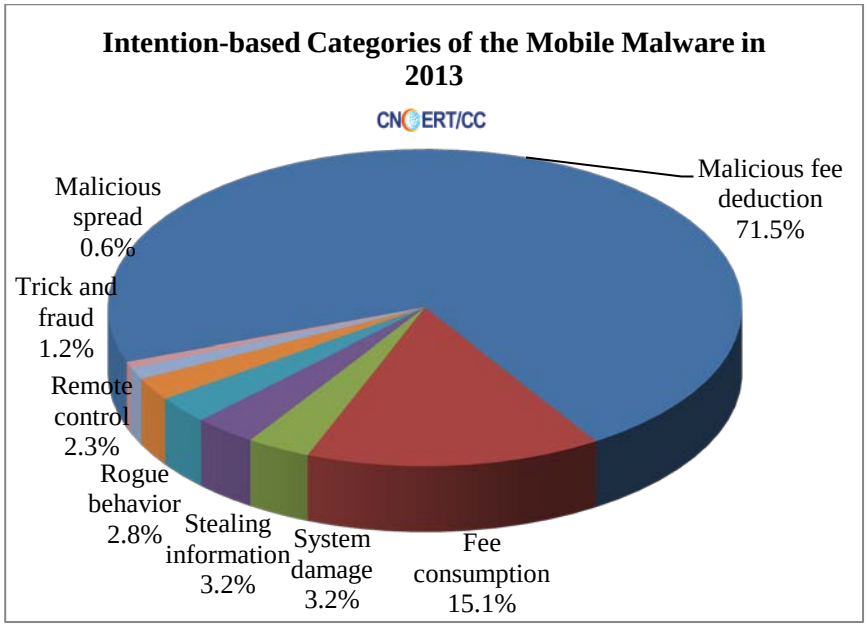


Figure 2-5 Intention-based Categories of the Mobile Malware in 2013

The majority of these mobile malware identified by CNCERT ran on Android platform, recording about 699.5 thousand (99.5%).

3. Events organized/co-organized

Press Briefing of Report on 2012 China Network Security Landscape

CNCERT hosted the Press Briefing of Report on 2012 China Network Security Landscape on 19 March 2013 in Beijing which attracted 97 experts from over 73 relevant organizations. The report summarized new trends and features of network security in China in 2012 and predicated security trends in 2013 with some countermeasures offered.

CNCERT2013 Annual Conference

CNCERT organized CNCERT 2013 Annual Conference on July 4 2013 at Hohhot, Inner Mongolia Autonomous Region, China. The theme of the conference is " Network Create Value·Security Guarantee Economy ". Four tracks will be designed for subject presentations, including National Economic Security, Mobile Internet Security, Data and Application Security, and Academic Network Security Seminar.

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

On July 30, 2013, the leaders and operational level delegates of the national CERTs/CSIRTs of China, Japan and Korea, gathered in Shanghai, China, to hold the first China-Japan-Korea Annual Meeting for Cyber Security Incident Response. The Parties reviewed cooperative activities for times of significant incidents affecting their respective countries, an operation standard in effect since 2005, and confirmed to enhance the existing cooperation with the goal of coordinating critical incidents in a more effective and efficient manner.

The Fifth China-ASEAN Network Security Seminar

CNCERT organized the Fifth China-ASEAN Network Security Seminar in Chengdu, China on October15th -17th 2013 which attracted 20 delegates from national CERTs and ICT authorities from 8 ASEAN countries. At the conference, all nations reported the general situation and development of cybersecurity of their own country, and made detailed plans to further cooperation.

Besides, Cybercrime Investigations and Forensics Technology Training was held during the same period. Cybersecurity experts from organizations like IMPACT and Microsoft introduced various cybercrime investigations and forensics technologies. This was the first cooperation between CNCERT and IMPACT and the training achieved good results.

4. Drills/Conferences attended

APCERT 2013 Drill - "Countering Large Scale Denial of Service Attack"

CNCERT participated in the APCERT 2013 Drill -"Countering Large Scale Denial of Service Attack" as a participant on January 29th 2013 and completed it successfully.

ASEAN CERT Incident Drill (ACID) 2013

CNCERT participated in the ASEAN CERT Incident Drill (ACID) 2013 on October 9th 2013 and completed it successfully. About 16th CERTs from 13 countries and areas joined the drill in total.

2013 APCERT Annual Conference-"APCERT & Cyber Security : Then, Now and Beyond"

Four Delegates from CNCERT attended the APCERT Annual General Meeting and Conference 2013 which was held from March 24th to 27th in 2013 in Brisbane with the theme of "APCERT & Cyber Security : Then, Now and Beyond". At the conference, CNCERT introduced its work on cleaning public network environment and preventing DDoS attacks.

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)	51	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)	51	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	20	Published on journals and magazines.

8. EC-CERT

Taiwan E-Commerce Computer Emergency Response Team – Chinese Taipei

1. About EC-CERT

1.1 Introduction

EC-CERT is the abbreviation for "Electronic Commerce - Computer Emergency Response Team". The purpose of EC-CERT is an organization offer reliable and confidential communicating channel to notify, exchange, and analyze information security events take place within the e-commerce network, and further activate early prevention, solving SOP against threatening vulnerabilities and attack patterns; if an unexpected situation happen, EC-CERT takes emergency response with rescue and recovery procedure to prevent further losses ensure smoothly developing of Taiwan's e-commerce market.

Figure 1.EC-CERT Official Website

Website：http://ec-cert.org.tw/?str=en

Telephone：886-2-66396620

Facsimile：886-2-66398963

E-Mail：service@ec-cert.org.tw

1.2 Taiwan E-Commerce Computer Emergency Response Team

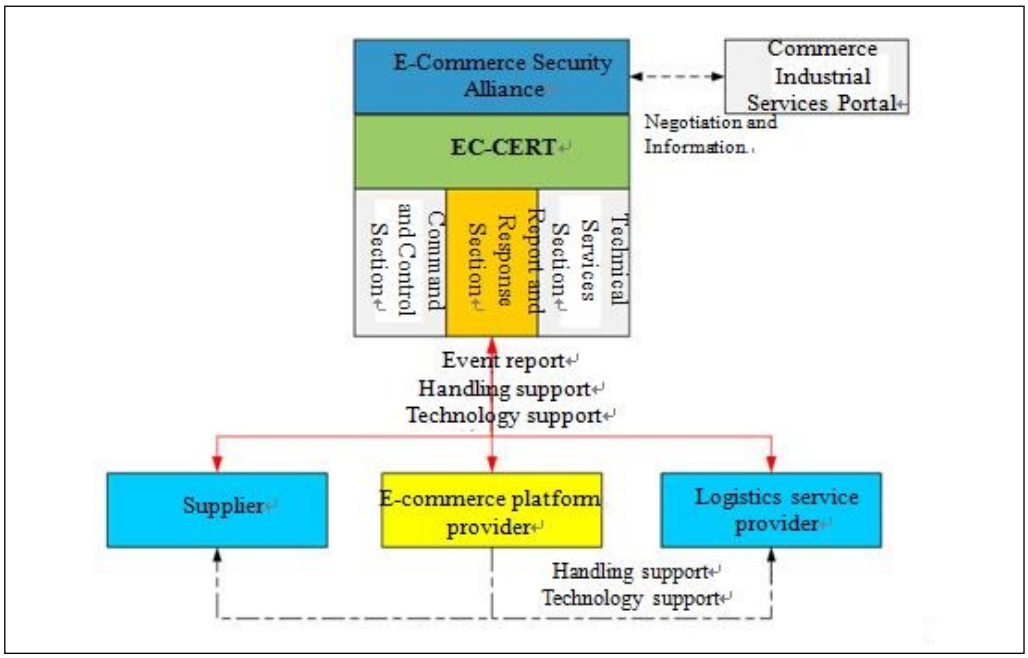


Figure 2.Organization Structure

(1) Information Security Director

The position is held by the Chairman of the "E-commerce Reliable Security Alliance". The Director is to supervise the overall issues in notification, response and handling of information security events.

(2) Command and Control Section; composed by EC-CERT, with the main responsibilities as follow:

A. Command and control the matter of information security incidents;

B. Convene the "Information Security Incident Response and Handling" meeting;

C. Responsible of contact issues of information security.

(3) Report and Response Section; composed by EC-CERT, with the main responsibilities as follow:

A. Operation, management, maintenance and monitoring of the EC-CERT Information Security Incident Notification System (including notification

phone lines, fax, and backup support systems);

B. Process management, auditing and examination of notification events.

C. Issuing of information security alerts and announcements.

(4) Technical Services Section; composed by EC-CERT and information security consulting firms. The Section is responsible for handling, identifying and technical support towards information security events.

(5) E-commerce Information Security Event Handling Group; task-force based, the Group is composed by the Information Security Director and different Sections. If an event is categorized as level "4" of "3", the Group activates immediately for response and handling of the event.

2. Activities & Operations

2.1 Incident handling reports

(1) Communication and cooperation with other security unites

(2) Connect with 6 domestic information security institutions for real time security information exchange counting for 241.

2.2 Information security alert services

The EC-CERT provided members notices regarding the latest information security threat warnings and Internet vulnerabilities as in Figure 3. About 49% of the Alert reports were on Early Warning, flowed by Announcement Advisory and Feedback Information.

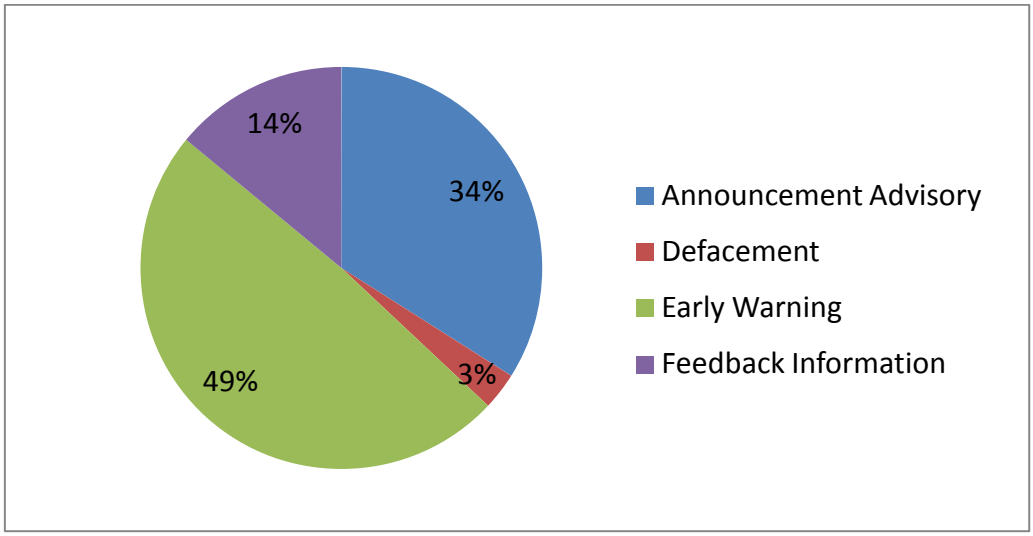


Figure 3. Information Security Alert Reports

2.3 Information Security Incident Monitoring Services

EC-CERT deployed monitoring stations to detect abnormal network traffics. The incident reports were categorized as in Figure 4. We did inform the members, gave advice and consultation.

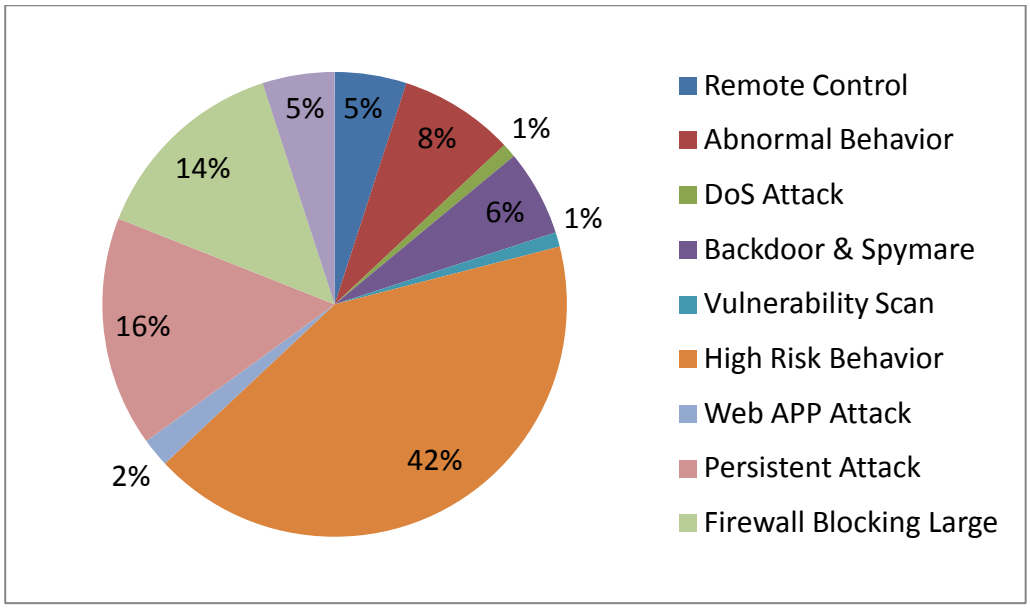


Figure 4.Incident Reports

2.4 Incident Report and Response

(1) EC-CERT supported 28 times of E-Commerce information security telephone consulting and referral service.

(2) EC-CERT has over 154 members include e-commerce vendors, information security experts and financial sectors.

2.5 New services

EC-CERT has provided E-Commerce Information Security Regulation Evaluation service for five E-Commerce company. The service evaluates target company if is able to provide safe transaction environment in information security, once results is up to 80%. EC-CERT would award to a certificates. We encourage E-commerce vendor accept this service freely. We hope it effectively reduce dispute in this field.

3. Events organized / co-organized

3.1 Training

EC-CERT organized three seminars for E-Commerce Industry and counseled ten E-Commerce Industries on E-Commerce Trading Security Regulation.

3.2 Seminars & Etc

EC-CERT organized one seminar E-commerce Reliable Security Alliance Annual Meeting, inviting security experts to share the up to date hacker assaulting practice, to assist IT industry early prevent.

4. Conclusion

In order to strengthen the security of e-commerce network transaction, EC-CERT plays an important role as a wide range of e-commerce industry information security services provider. Such as real time alerts, incident monitoring, information exchange, consulting service, regulation evaluation and personal information prevention. In the future, EC-CERT glad to exchange any security information with other units and cooperate with. EC-CERT will dedicate the security of E-Commerce transaction.

9. 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 computer security incident reporting and responses; to provide a focal point in Hong Kong for cooperation and coordination with other Computer Emergency Response Teams, 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 2013, HKCERT had handled 1,593 security incidents which was 52% increase of the previous year. (See Figure 1).

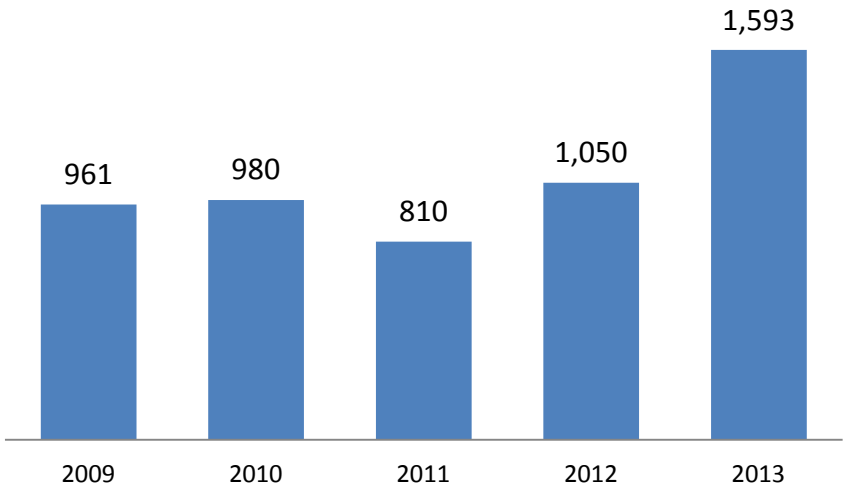


Figure 1. Incident Reports Handled by HKCERT

This increase was mainly caused by the increase in the botnet incidents. In 2012, HKCERT handled 120 botnet incidents. In 2013, it has been increased to 423 cases. (See Figure 2). During the period, HKCERT has participated in several global botnet take down operations against Citadel, Brobot, ZeroAccess and Pushdo.

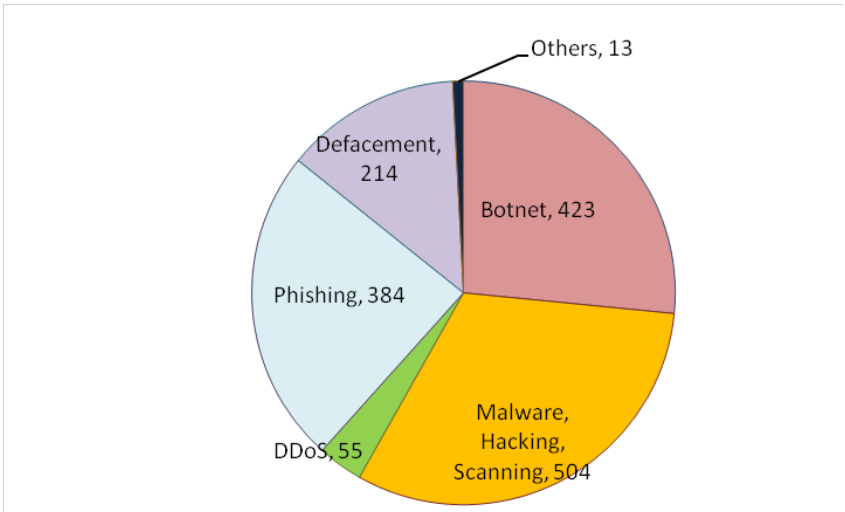


Figure 2. Distribution of Incident Reports in 2013

2.2 Information Gathering and Dissemination

During the period from January to December of 2013, HKCERT published 471 security bulletins (See Figure 3) on the website. This was a 10% increase from the previous year. In addition, we have also published 97 blogs and advisories, including security advice on the use of smartphone and the best security reads of the week.

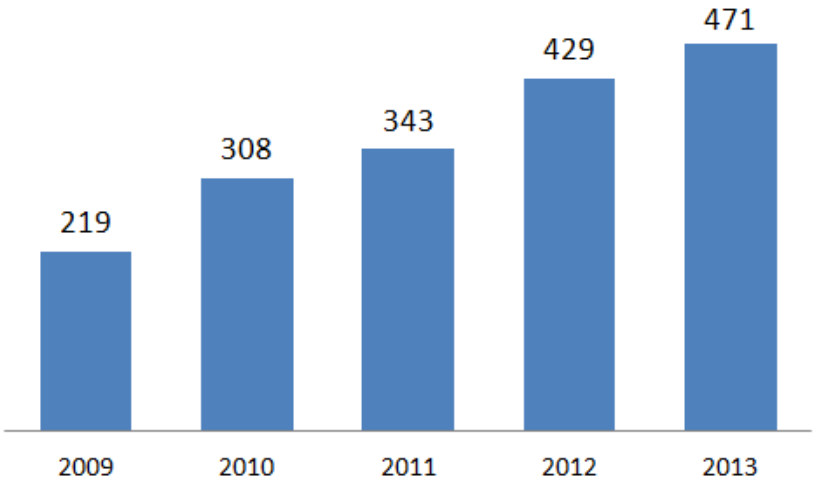


Figure 3. HKCERT Published Security Bulletins

HKCERT used the HKCERT website, RSS, HKCERT mobile app, and Hong Kong Government Notification mobile app (starting July 2013) to publish security bulletins, blogs and news. HKCERT also used email and SMS to publish selected security bulletins to subscribers.

2.3 Publications

- HKCERT had published 12 issues of monthly e-Newsletter in the period.
- HKCERT had published Hong Kong Google Play Store's Apps Security Risk Report since July 2013 (six reports). The Report is a cooperation with National Institute of Network and Information Security (NINIS) of China.

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 video creation contest. Four public seminars were organized in January, April, August and December 2013.

We organized the Information Security Summit 2013 with other information security organizations and associations in November 2013, 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 briefings and responses

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 Brisbane, Australia; the FIRST AGM and Conference in Bangkok; and the Annual Meeting for CSIRTs with National Responsibility in Bangkok.
- Participated in the APCERT Drill (January 2013) and acted as leader of the Organizing Committee and the Exercise Control team. The theme of the drill this year was "Countering Large Scale Denial of Service Attack". The drill was a great success with 22 APCERT teams from 18 economies, and 4 economies of OIC-CERT participating.
- Participated in International honeypot initiatives, including joining the Tsubame project of JPCERT/CC and The Honeynet Project.
- Represented APCERT in the Advisory Council of DotAsia Organization

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 2013, HKCERT had worked with ISPs to clean up Citadel, Brobot, ZeroAccess and Pushdo botnet machines in Hong Kong.
- Co-organized a local drill with HK Police and OGCIO on 8th November 2013 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 the financial sector and promoted cyber security drill to members of Hong Kong Association of Banks
- Liaised with critical infrastructure sector and had delivered awareness briefings to these organizations for better protecting the security environment of Hong Kong.

5. Other Achievements

5.1 Strategy and Service Review

HKCERT had conducted a review of the strategy and service in October 2013. The review was undertaken by AusCERT at the request of HKCERT for the Hong Kong SAR Government to review the operation of HKCERT as well as its future direction to evaluate its ability to meet the current and future needs.

5.2 Three Year Strategic Plan

HKCERT prepared its second rolling Three Year Strategic Plan and presented to the government. The plan will be updated annually.

5.3 Smartphone incident response service

HKCERT started the service in 2012 and gradually developed the security analysis skills and process, accompanying with public awareness blog articles and security guidelines.

HKCERT added critical security bulletins messages to the GovHK Notifications mobile application (a one-stop platform for citizens to receive Hong Kong Government notifications) since July 2013.

5.4 Global intelligence collection and follow up

HKCERT implemented the Information Feed Analysis System (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.

5.5 Incident Management System revamp

HKCERT implemented a new Incident Report Management System which helped improving the efficiency of our incident response activities and providing useful statistics.

5.6 Year Ender press briefing

HKCERT organized a year ender press briefing to media at the beginning of each year, to report on information security status in the past year, and to give perspective of the trends of security attacks in the coming year to warn the public for better awareness and preparedness. The 2013 year ender briefing was held on 20th January 2013 to brief on the security status of 2013 and trends of 2014.

6. Future Plans

6.1 Strategy

"Proactivity", "Share to Win" and "Security is not an Island" are three directions

of HKCERT. We 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 2014/2015. 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 a Decision Support System, an add-on to the Information Feed Analysis System (IFAS) to select prioritized incidents and collect intelligence about compromised machines in Hong Kong to follow up.

HKCERT is assessing the feasibility of an Automated Malware Analysis System to help automating the analysis of malicious software and URL to streamline security analysis process.

7. Conclusion

Year 2013 was a year with many changes and challenges in HKCERT. We had some changes in personnel. We had new services and projects implemented, and we were much more involved in global botnet takedown operations.

With the Internet security facing more crises from cyber conflicts, ransomware, exposure of Internet devices and new security challenges arising from adoption of emerging technologies like Cloud Computing, Mobile Payment and Internet of Things, we expect a more challenging year 2014. HKCERT is committed to working with international and local partners to assist the assurance of the security of the Internet. 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.

10. 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.

1.2 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.

1.3 Workforce Power

During 2013 complaints received were handled by Ahmad K. Alkazimy and Rahmadian L. Arbianita on the Help Desk.

In February, Ikhlasul Amal joined ID-CERT as Technical Editor.
In October, Wayan Achadiana joined to support on RBL (RealTime Block List).

Internship for Malware Laboratory:

1. Ade Yoseman
2. Ardy
3. Hadi Rasyid Sono

Volunteers:

1. Budi Rahardjo, MSc., PhD. ***(ID-CERT Chair)***
2. Andika Triwidada ***(ID-CERT Co-Chair)***
3. Maman Sutarman
4. Betha
5. Other volunteers

Professional Staffs:

- Ahmad Alkazimy (***ID-CERT Manager***)
  e-Mail: ahmad@cert.or.id
  Mobile: +62-838-74-9292-15
  Finger print: 39B2 87BA 3DD6 7832 D56F 0344 FCE4 3A7C FE38 CC96
- Rahmadian L. Arbianita (***Incident Response Officer – HelpDesk***)
  e-Mail: rahmadian@cert.or.id
  Mobile: +62-811-22-77-03
  Finger print: 414A 1183 199E 8BA5 E0D1 C234 08BF 8BDE 1766 2CC7

1.4 Community Support

ID-CERT wishes that more respondents will be participated in the various studies conducted by ID-CERT, in order to make a better internet in Indonesia in the future. ID-CERT also wishes that the efforts in building all of these can have support in ID-CERT operations.

1.4.1 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.

1.4.2 Respondent

Now ID-CERT has 38 organization respondents participating in Internet Abuse Research. ID-CERT still welcome to new respondents who wish to join in the various researches/studies conducted by ID-CERT.

1.4.3 Affiliation

ID-CERT defines that ID-CERT supporter or affiliate is the organization that have supported in ID-CERT research.

ID-CERT still welcome and invite Indonesia Internet community to support ID-CERT in a way of sponsorship, donations or through the mechanism of Membership Fees (to be determined later).

1.4.4 Volunteer

From the start, 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.

ID-CERT also welcome a wide opportunity for individuals who want to contribute to Indonesia internet security by being one of ID-CERT researchers or help desk officers.

2 Mission

ID-CERT missions are:

1. ID-CERT does not have operational authority to its constituency, either in Indonesia or abroad, but only to inform the various complaints of network incidents, and relies entirely on the cooperation with the parties involved in the incident related networks.
2. ID-CERT is built by the community and the results will be given back to the community.
3. ID-CERT helps to socialize the importance/awareness of internet security in Indonesia.
4. ID-CERT is undertaking various researches in internet security required by the

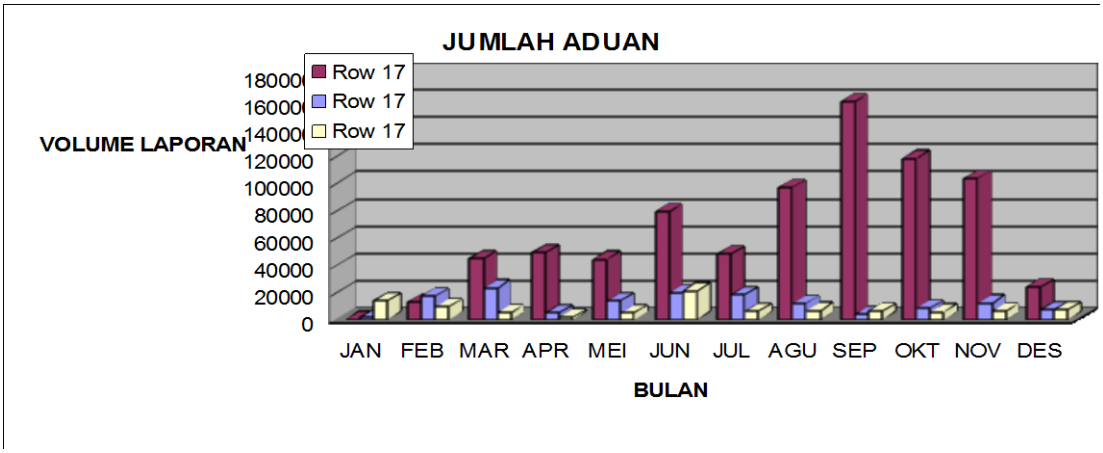
internet community in Indonesia.

5. ID-CERT mission is to coordinate the incident handling involving local and international communities.

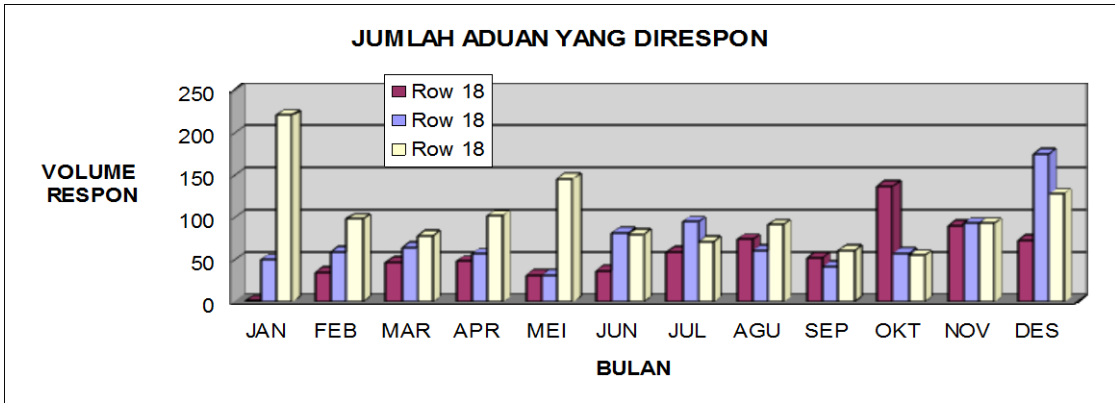
3 Activities

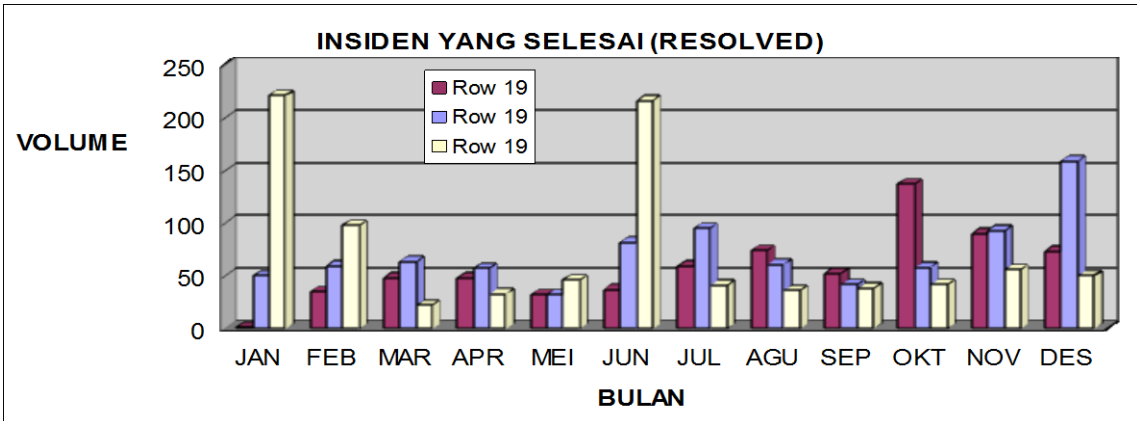
3.1. Incident Handling

By December 31, 2013 ID-CERT had received 94,035 incident complaints during the year 2013.



ID-CERT had proceed 1,224 incidents and 899 of them had successfully handled and solved.





3.2. Incident Monitoring Report (IMR)

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

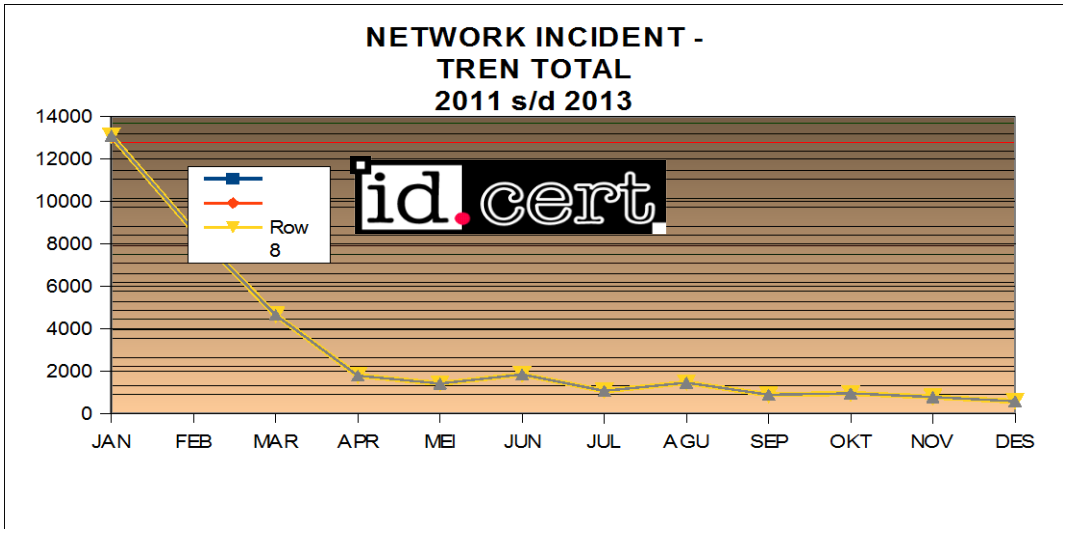
In contrast to the reports ID-CERT received above, reports received through IMR in the year 2013, when averaged over a number of reports of complaints are 11,108 reports per month. While the number of reports received during the year 2012 was reported as average of 290,297 per month. And total number of reports received in 2013 is only 133,297.

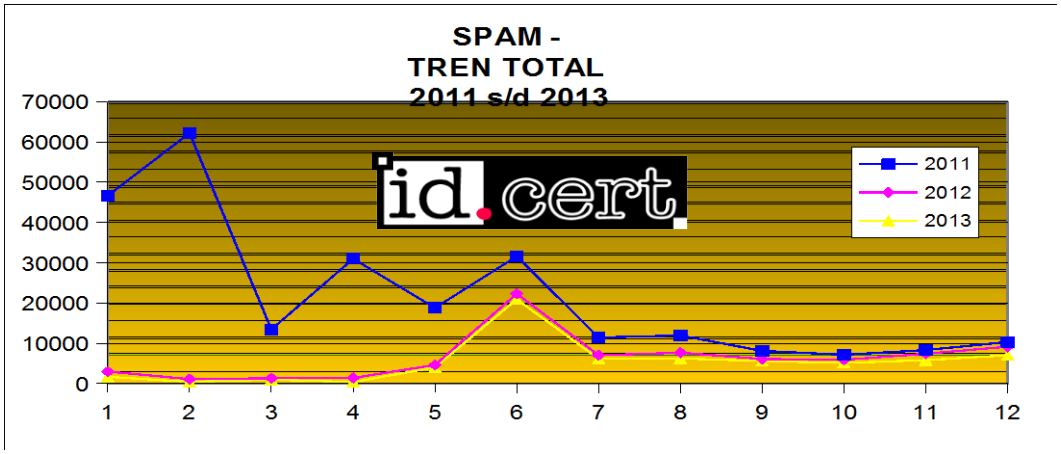
2012		
No.	Category	Rating (%)
1.	Network Incident	76,53
2.	Malware	8,63
3.	Intellectual Property Rights/HaKI	6,99
4.	Spam	4,78
5.	Spam Complaint	1,94
6.	Spoofing/Phishing	0,64
7.	Response	0,48

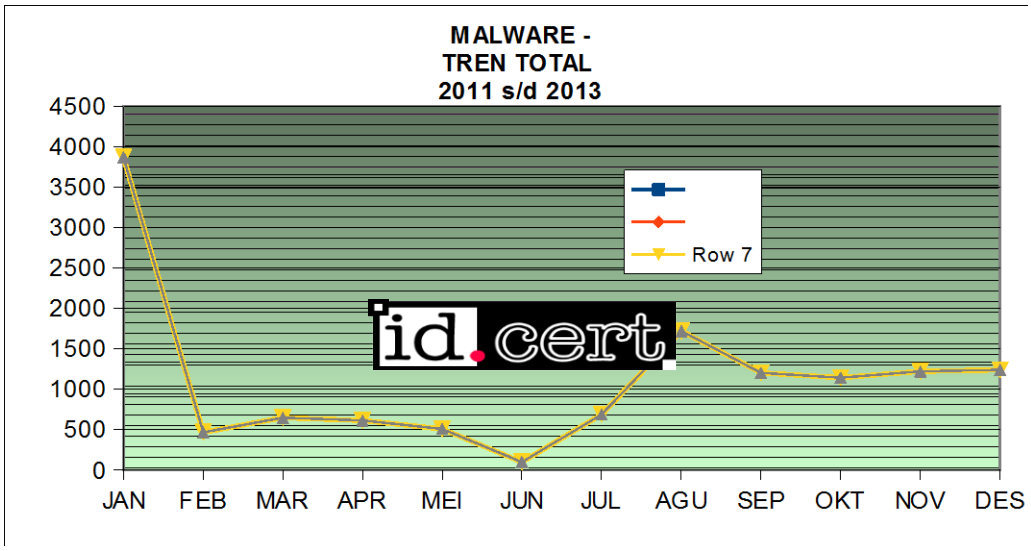
2013		
No.	Category	Rating (%)
1.	Network Incident	51,48
2.	**Spam**	36,07
3.	**Other**	9,29
4.	**Malware**	3,05
5.	**Spoofing/Phishing**	0,05
6.	**Response**	0,05
7.	**Spam Complaint**	0,01

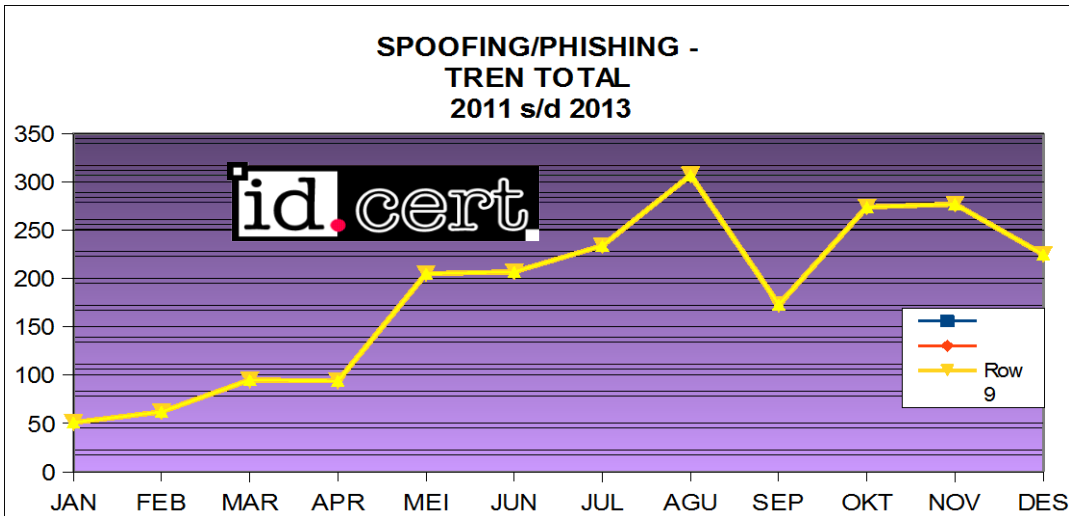
*Note: **in Bold:** position rating changing in 2013 compared to 2012*

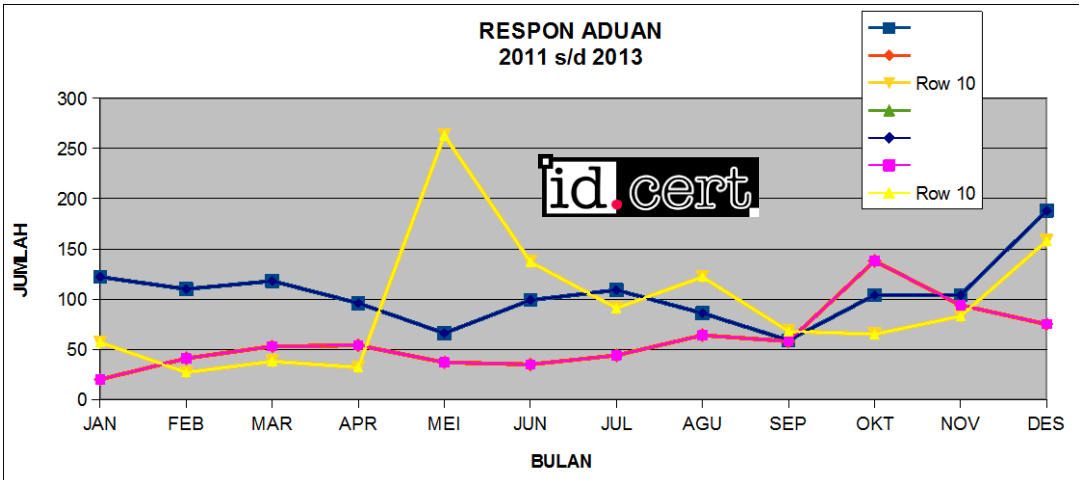
Here are trend graphs in total from 2011 to 2012 for Network Incident, Spam, Malware, Spoofing/Phishing, Response, and Spam Complaints:

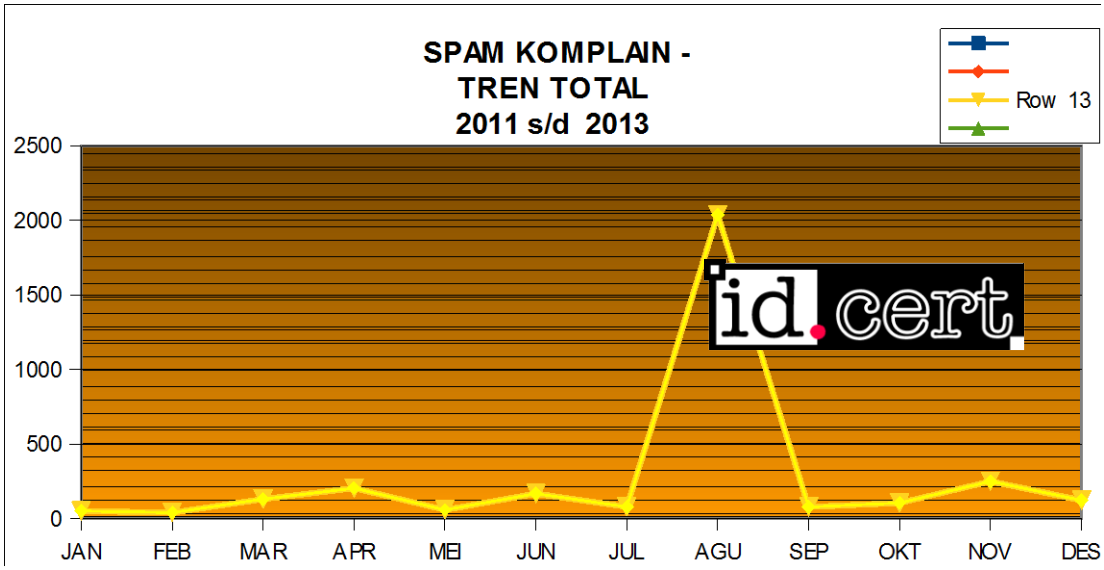





MALWARE -
TREN TOTAL
2011 s/d 2013
4500
4000
3500
3000
2500
2000
1500
1000
500
0
JAN
FEB
MAR
APR
MEI
JUN
JUL
AGU
SEP
OKT
NOV
DES
Row 7
id.cert


SPOOFING/PHISHING -
TREN TOTAL
2011 s/d 2013
350
300
250
200
150
100
50
0
JAN
FEB
MAR
APR
MEI
JUN
JUL
AGU
SEP
OKT
NOV
DES
Row 9
id.cert


RESPON ADUAN
2011 s/d 2013
300
250
200
150
100
50
0
JUMLAH
JAN
FEB
MAR
APR
MEI
JUN
JUL
AGU
SEP
OKT
NOV
DES
BULAN
Row 10
Row 10
id.cert



Complaints/Cases received by ID-CERT most of them are from other countries, after they found difficulty in contacting the administrator of the problematic website. ID-CERT is being a trusted party to report the case because ID-CERT has established good relationships with neighboring countries.

3.3. Security Warning/Advisory/Notice

In 2013 ID-CERT has issued 3 Security Alerts/Warning in Bahasa Indonesia:

1. Malware CMS yang mengakibatkan Spam (CMS Malware resulted in Spam)
December 4, 2013
http://www.cert.or.id/index-berita/en/berita/39/

2. Ancaman DDoS yang berkolaborasi dengan Malware (DDoS Collaborated with Malware Threat)
May 25, 2013
http://www.cert.or.id/index-berita/en/berita/31/

3. Ancaman DDoS dan Langkah Antisipasi (DDoS Threat and Anticipation)
March 28, 2013
http://www.cert.or.id/index-berita/en/berita/28/

3.4. Events

There are several events attended by ID-CERT in 2013:

1. January 29, 2013 – APCERT Drill
2. February 7-8, 2013 - ASEAN-Japan Cyber Security Workshop, Bangkok
3. February 14, 2013 – ID-CERT Gathering V, Jakarta
4. March 12-15, 2013 - Cyber Intelligence Asia, Kuala Lumpur
5. March 24-27, 2013 – APCERT Annual General Meeting 2013, Brisbane
6. April 12-14, 2013 – TRACEROUTE Party, Jakarta

4 Achievement

ID-CERT achievements in 2013 are:

1. Foundation Member Award at APCERT 10th Anniversary
2. New layout ID-CERT website, www.cert.or.id
3. Build ID-CERT Malware Team
4. Collaboration with APJII to have Anti Spam RBL (RealTime Block List)
5. November 7, 2013: First ID-CERT – APJII Cyber Incident Simulation Drill. 18 ISPs participated in this Drill.

11. ID-SIRTII/CC

Indonesia Security Incident Response Team of Internet Infrastructure - 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.

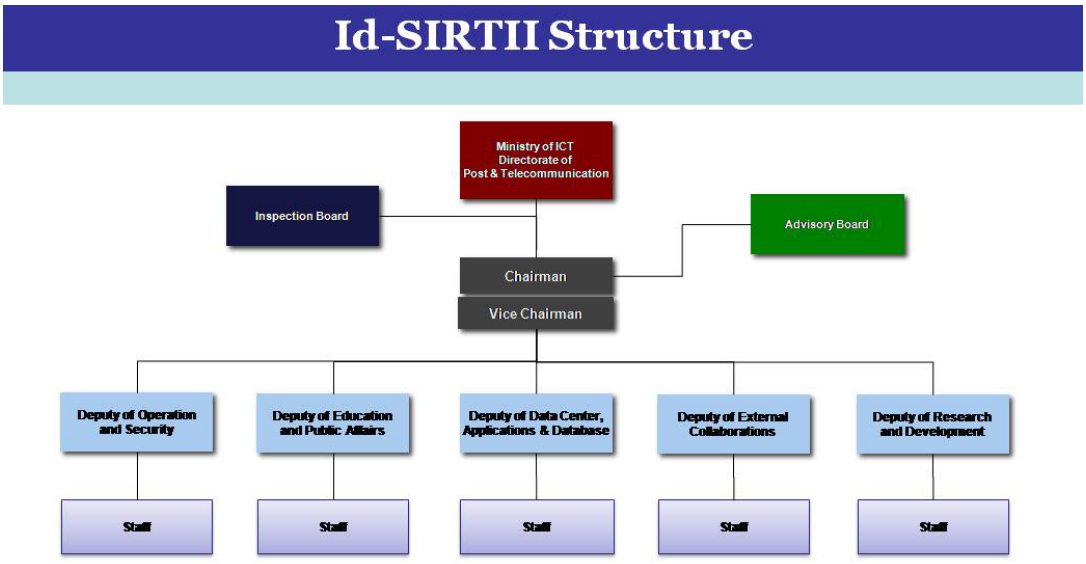
ID-SIRTII as a legal institution which has been granted the right and authority to conduct Internet traffic monitoring in Indonesia refers to the rule of law as follows below:

- 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. Workforce Power

Id-SIRTII/CC now has 6-team 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.



1.4. Constituency etc.

Our constituencies are:

- 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.

Our main activities are:

- Socializing to related parties to conduct security activities of the telecommunications network utilization of IP-based
- Monitoring, detection and early warning of threats and disturbance of the telecommunications network of IP-based in Indonesia
- Developing and / or providing, operating, maintaining and developing 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 2013. 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 give 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 keepour constituency informed of potential vulnerabilities, and where possible, will inform this community of such vulnerabilities before they are actively exploited. The statistic during 2013 is shown as follow:

The following figure shows internet traffic monitoring result conducted by ID-SIRTII Monitoring division between January and December 2013, there are 74.199.628 incidents reported. The graphic tells that there is a escalation of incidents, allegedly associated with the several national issues against other

countries.

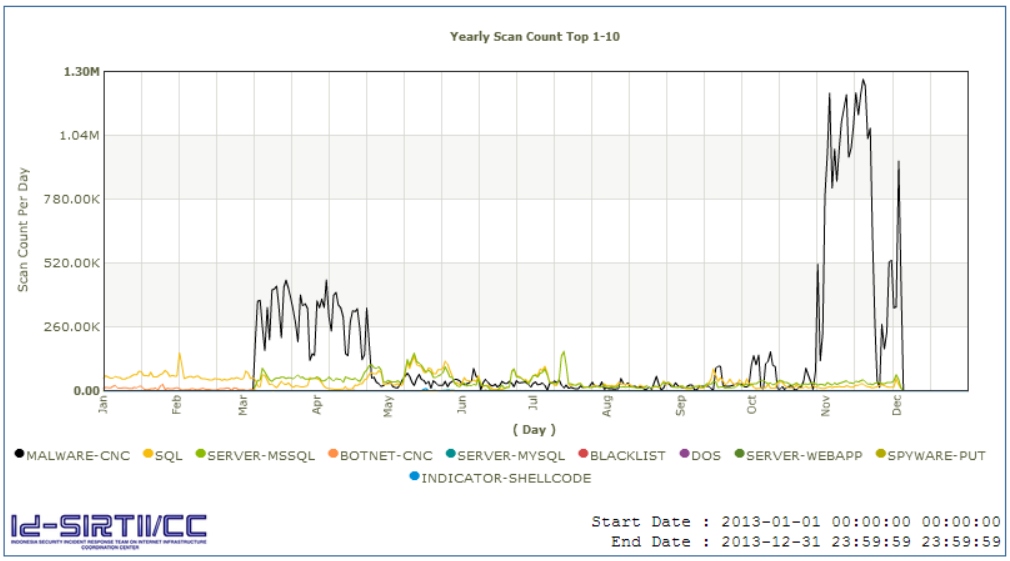


Figure 1: Graphic of Incident Categorized by Incident Classification

CLASIFICAITON	TOTAL
MALWARE-CNC	47.864.568
SQL	13.211.947
SERVER-MSSQL	10.985.929
BOTNET-CNC	718.328
SERVER-MYSQL	324.264
BLACKLIST	208.557
DOS	184.487
SERVER-WEBAPP	118.203
SPYWARE-PUT	114.723

INDICATOR-SHELLCODE	76.752
Other	391.870
Total	74.199.628

Figure 2: Incident Table Categorized by Incident Classification

The following figures show the top 10 incident based on destination port 2013

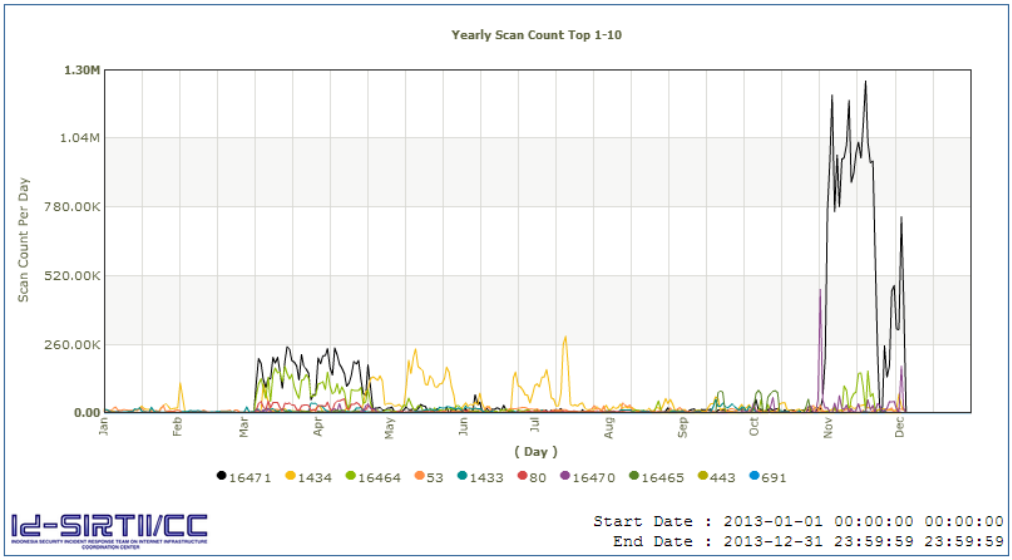


Figure 3: Incident Graphic Categorized by Destination Port

Destination Port	Total
16471	33,618,332.00
1434	11,038,697.00
16464	7,194,577.00
53	2,516,317.00
1433	2,455,304.00
80	2,278,375.00
16470	1,970,944.00
16465	1,189,973.00
443	253,919.00
691	189,731.00
Other	11,493,875.00
Total	74,200,044.00

Figure 4: Incident Table Categorized by Destination Port

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 2013 ID-SIRTII receipt 1.087 incident reports. The following table is summary of public incident reports categorized by Incident Classification:

No	Category	Sub Category
1	Malware	Botnet CNC
		Bot
		Worm
		Backdoor
		Trojan
2	Fraud	Phising
		Scam
		Spam

3	DOS	DOS
		DDOS
4	Vulnerability	SQL injection
		Web Defacement
		Missconfiguration
		0-Day
		Data Leak
5	Intrusion	SSH attack
		Brute Force
		Snifing
		Scan Probe

List of Sub Category

Category	Jan	Feb	March	April	May	June	July	Augst	Sept	Nov	Des
Malware	29	44	34	66	83	65	75	68	64	74	60
Fraud	13	18	10	32	25	16	14	19	20	16	11
Vulnerability	11	33	13	16	13	8	7	10	13	11	16
Intrusion	0	7	5	2	1	7	2	6	4	13	11
Dos	2	3	0	1	0	0	2	0	1	12	1
Count	55	105	62	117	122	96	100	103	102	126	99

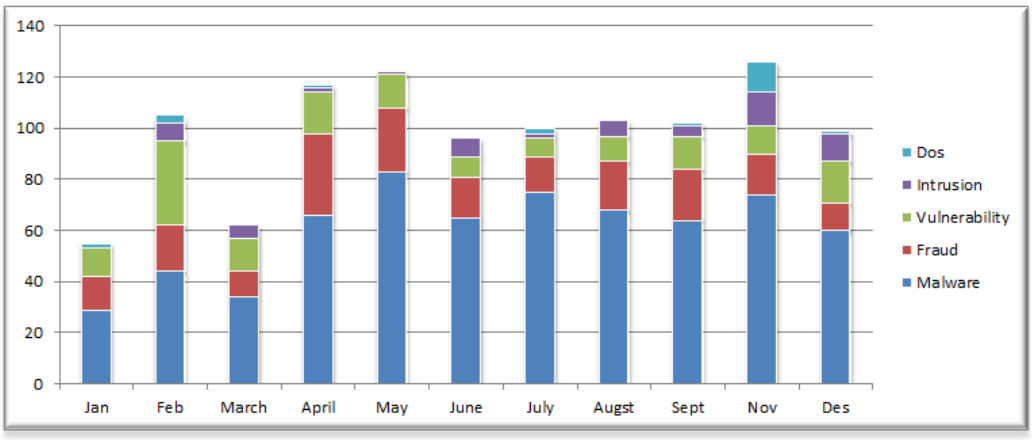


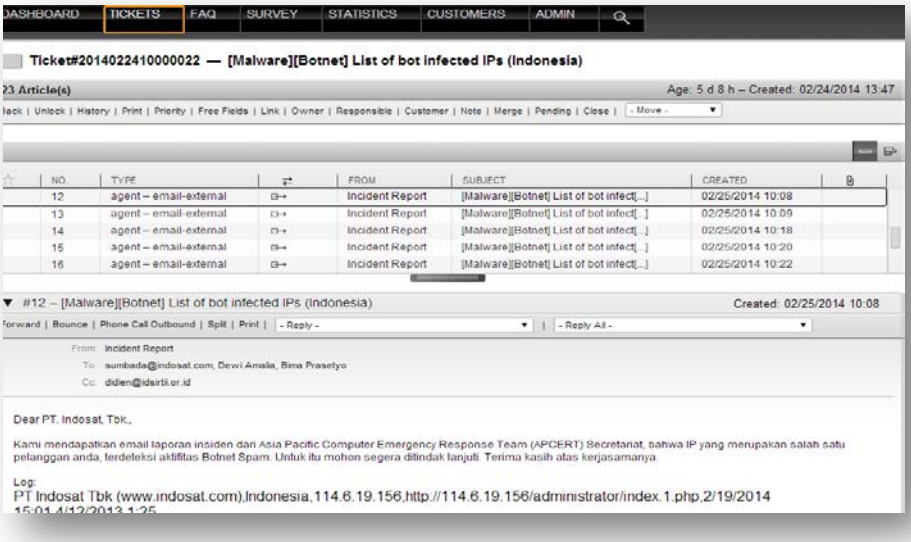
Figure 6: Monthly Table of Incidents Categorized by Incident Classification

APCERT-Team Report

ID-SIRTII also accepts incident report from APCERT-team. During 2013, 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. Below is the screenshot of OTRS system used by ID-SIRTII.



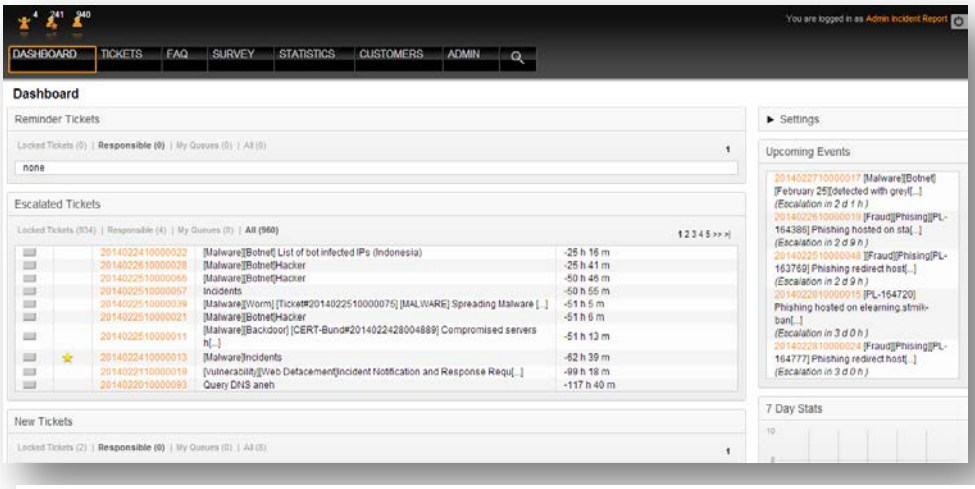
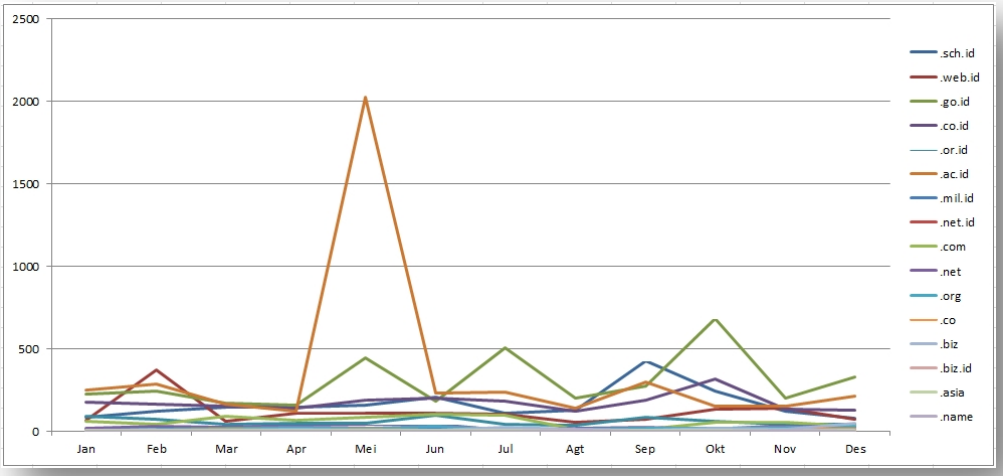


Figure 7: Communication and coordination activity with stakeholder via OTRS system.

Web Defacement

Id-SIRTII/CC also conducted an intensive monitoring on critical websites especially the government institutions. During year 2013, there are 15448 incident in total. School websites (sch.id) dominated the number of web defacement case, following by n government website (go.id). The statistic can be shown on the following graph:



2.2. Establishing and Supporting Sector based CSIRTs

As the cleaning cyber environment need more strategic partnership with other institutions we have establishing sector based CSIRT such as Academic CSIRT, Gov-CSIRT. Now APJII-CSIRT (ISPs association) is still under preparation. In

2013, sector CSIRT which are successfully established are: West Java Province CSIRT (under GovCSIRT) and Defence CSIRT (under Ministry of Defence)

3. Event Organized/Co-Organized Achievement

3.1. International Membership

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

3.2. Presentation and Publication

Security Awareness and Workshop Road Show in 5 major cities within the country and +20 seminars invitation.

3.3. Community Cooperation

Research and Development Project with APTIKOM – Academic CERT, National Honey Net, ID-X. Special Program with SANS, EC-COUNCIL, KKI and SGU (Swiss German University), APJII (ISPs Association), AOSI (Association of Indonesia Open Source), FTII (Federation of Indonesia Information Technology)

3.4. Organizing Conference and Workshop/Training

- Become a host for APCERT TWS (Technical Workshop in Security) 2013 and FIRST Technical Colloquium 2013 on 23-24 September 2013 in Yogyakarta. The face-to-face Steering Committee meeting is also conducted back to back with the event.
- Become a host for OIC-Cert AGM, Worskshop and Conference on 18-20 November 2013 in Bandung.
- A number of national seminar and workshop, such as: Incident Handling, Creating & Managing CSIRT and Forensics.
- National Drill Test in Bandung, 18-20 September 2013 with almost 100 participants from various sectors such as government, banking, law enforcement, ISPs and communities.
- We conduct +50 various security training in 2013 i.e. Secure Coding and Secure Programming, Cyber Crime and Digital Forensic for LEA.

- Conducting National Cyber Defence Competition (CDC) and Cyber Jawara 2013 which consist of CND, Pentest, CTF and Forensics.

4. International Cooperation

4.1. Joining Int'l Conference and Events

- AOTS/HIDA Training 2013, Tokyo – Japan
- APCERT AGM 2013, Brisbane – Australia
- FIRST AGM 2013, in Bangkok - Thailand
- OIC-CERT AGM 2013, in Yogyakarta – Indonesia (as a host)
- ASEAN-Japan Security Forum 2013, Manila - Phillipine
- ASEAN CERTs Incident Drill (ACID) 2013 as OC and Participant
- APCERT Drill Test 2013 as a CoEx, OC and Participant

5. Future Plans

- Improving the system for Public Incident Reporting Service
- More Research and Development Cooperation
- More 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.

12. 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 2013, JPCERT/CC received 29,746 computer security incident reports from Japan and overseas. A ticket number is assigned to each incident report to keep track of the status.

	1st Qtr	2nd Qtr	3rd Qtr	4th Qtr	Total
Incident Reports	5,453	9,386	10,095	4,812	29,746

Figure 1. Incident reports to JPCERT/CC (2013)

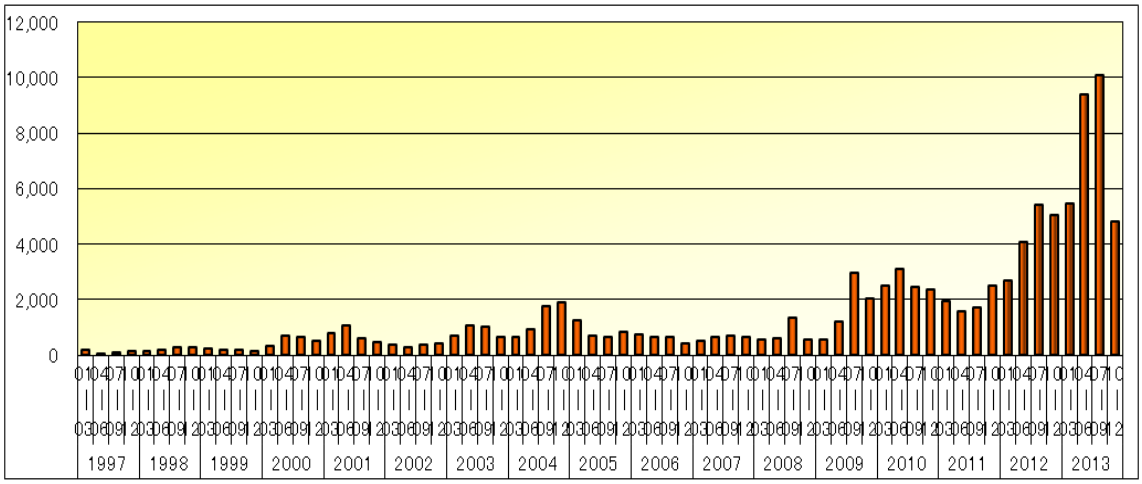


Figure 2. Incident reports to JPCERT/CC (1997-2013)

2.2 Abuse statistics

The incident reports to JPCERT/CC in 2013 were categorized as in Figure 3. About 45% of the incident reports were on scan, followed by website defacement and phishing.

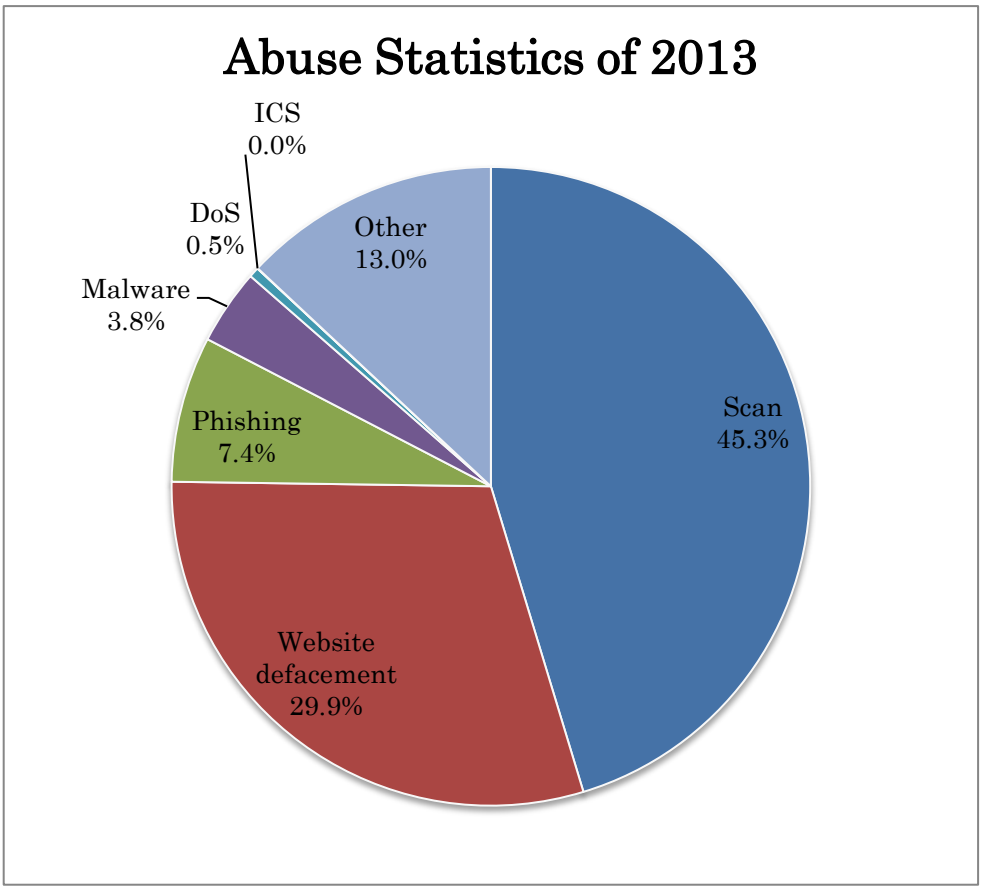


Figure 3. Abuse Statistics of 2013

2.3 Security Alerts and Advisories

- **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 2013, 55 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 their 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 CERT-FI (https://www.cert.fi/en/).

  In 2013, 261 vulnerabilities coordinated by JPCERT/CC were published on JVN. Among them, 127 cases were reported through IPA in Japan, and 134 cases were published in cooperation with some overseas vendors and CERT/CC.

  In June 2010, JPCERT/CC became a CVE Numbering Authority (CNA). Since then, JPCERT/CC is 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 is providing information security related alerts via Twitter.

- **JPCERT/CC Official Blog**

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

  Since September 2010, JPCERT/CC is providing security news regarding Japan as well as activities happening at JPCERT/CC on an English blog.

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 an 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 center for conducting technical examination and analysis of artifacts. The artifacts include not only viruses and bots but also tools which can potentially be used with malicious intent. As the findings through the analysis are incorporated into the incident response and the information provision that forms the basis of JPCERT/CC, our research center is pursuing the sophistication of 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.

- **Technical Notes**

  JPCERT/CC publishes documents that provide general technical information and/or instructions for incident handling.

- **Library**

  The library provides security materials targeting both security professionals and beginners, such as information security materials for new employees, security setup of e-mail software, professional security review, etc. (Japanese only)

- **Open DNS Resolver Check Site**

  JPCERT/CC released the "Open DNS Resolver Check Site" on 31st of 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.

  http://www.openresolver.jp/ (Japanese)

  http://www.openresolver.jp/en/ (English)

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 understand the Internet threat situation 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/ (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 by JPCERT/CC in 2013 are as follows:

On-site Training/Seminar	-TSUBAME Network Monitoring Workshop (March) -C/C++ Secure Coding Seminar (May) -Incident Handling, Network Forensics Training for MNDC (August) -Incident Response, Handling Training for LaoCERT (October) -CSIRT Training Course for AfricaCERT (June, November)
Domestic Seminars/Conference	-Control System Security Conference (January) -Open Source Conference 2013 Kansai @Kyoto (August) -SICE Annual Conference 2013 (September) …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	-Information Security 2013 Conference and Training (August) -APCERT Technical Workshop (September)
Dispatch of Speakers	-International Conference on Information Security (July)

	-ASEAN Cybersecurity Seminar for Policy Makers (September) -Building Domestic and International Coordination Mechanism in Computer Incident Response in Vietnam(October) …and many more

3.3 Participation to International Events

JPCERT/CC participates in the many international events. Below are some of the events we joined in 2013:

RSA Conference US 2013 (February)
APCERT AGM and Conference 2013 (March)
APEC TEL SPSG (April, September)
Multi-stakeholder Consultation for the Review of the OECD 2002 Security Guidelines (June)
25th Annual FIRST Conference Bangkok (June)
National CSIRT Meeting (June)
2013 APISC Security Training Course (July)
Black Hat USA 2013 (July)
DEFCON 21 Hacking Conference (August)
The First China-Japan-Korea CSIRT Annual Meeting for Cybersecurity Incident Response (August)
AP* Retreat Meeting (August)
First Technical Colloquium in Yogyakarta (September)
Seoul Conference on Cyberspace 2013 (October)
OIC-CERT Annual Conference 2013 (November)
…and many more

3.4 Drills

JPCERT/CC participated in the following drills in 2013 to test our incident response capability:

- APCERT Drill 2013 (29 January)
- ASEAN CERT Incident Drill (ACID) 2013 (4 October)

4. MoU

To further strengthen cooperation, JPCERT/CC has been signing a Memorandum of Understanding (MOU) with various security organizations. For 2013, we have newly signed the MOU with CERT-RO, MECIRT, HKCERT, PacCERT, New Zealand Government Communications Security Bureau and Team Cymru.

5. Other Publications

JPCERT/CC also publishes quarterly activity reports and study/research reports.

6. 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 Steering Committee member of the FIRST organization since 2005. JPCERT/CC is offering sponsorship support 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 acting as a steering committee member and secretariat for the organization. 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 is aimed to establish a common

platform for Internet threat monitoring, information sharing & analysis within the region.

7. JPCERT/CC Contact Information

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

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

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

Phone: +81-3-3518-4600

Fax: +81-3-3518-4602

13. KrCERT/CC

Korea Internet Security Center - Korea

1. About KrCERT/CC

1.1 Introduction

Korea Computer Emergency Response Team/Coordination Center(KrCERT/CC) serves as the focal point to coordinate security incidents on all Korean constituency. In the national cyber security framework, KrCERT/CC, covers the incident handling and security of information systems and networks in 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.

1.2 History

KrCERT/CC was established in 1996 and joined in 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 evolved itself to meet those challenges. The first major challenge was the breakdown of Internet infrastructure over several hours caused by slammer worm outbreak on 25th January 2003. At that time, KrCERT/CC didn't have the effective communication and coordination system in place yet. Korean government recognized that the close collaboration between CERT and ISP is a key success factor for major incidents. Korea Internet Security Center(KISC), 24/7 security operation center, started the operation in December 2003.

2. ACTIVITIES IN YEAR 2013

2.1 Incident handling reports

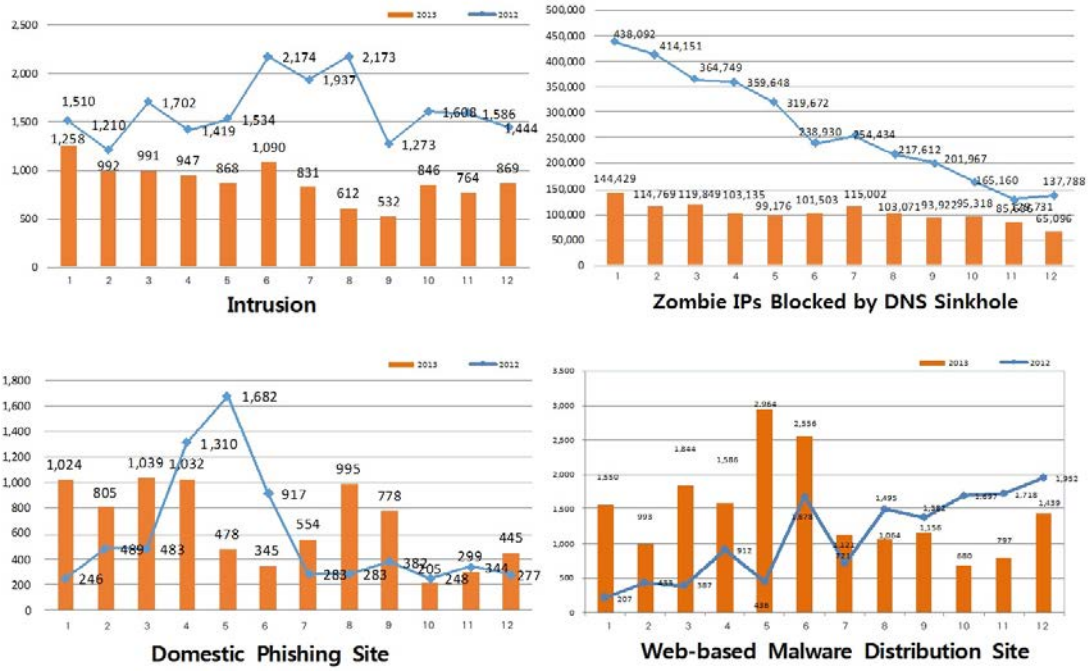
Internet incidents reported to KrCERT/CC are classified into the following 4 categories: hacking intrusion, zombie IPs blocked by DNS sinkhole, domestic phishing site and web-based malware distribution site.

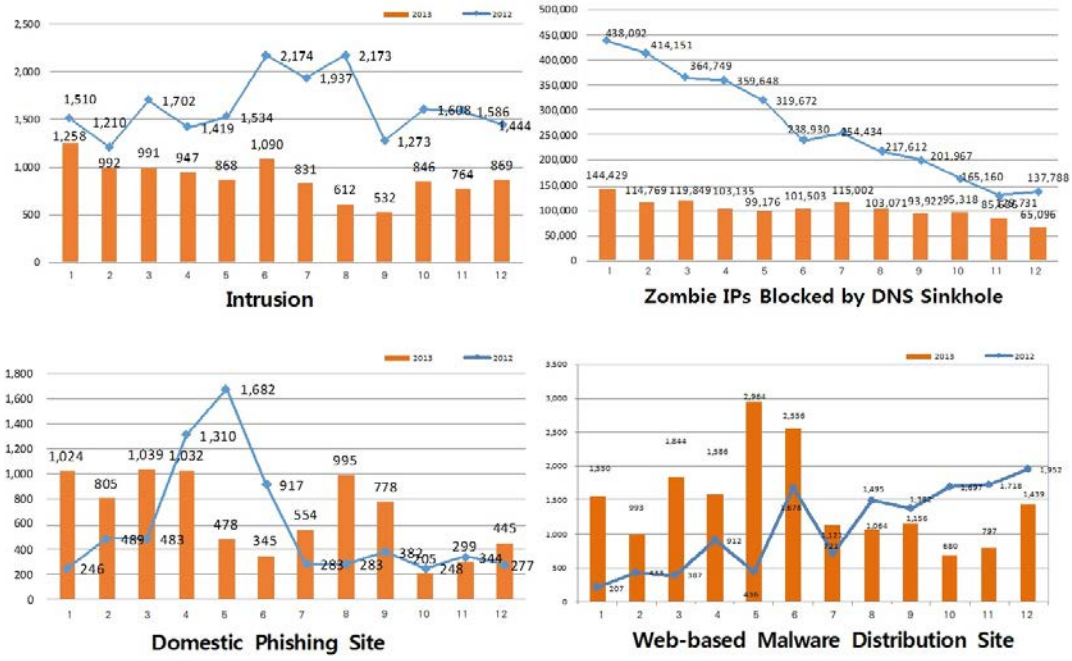
The number of hacking incidents reported by KrCERT/CC decreased from 19,570 in

2012 to 10,600 in 2013. The number of incident reports on Zombie PCs by DNS sinkhole is 1,240,906 in 2013, which shows a sharp decrease compared to that of 2012(3,241,924). The number of phishing sites targeting domestic site is increased from 6,944 in 2012 to 7,999 in 2013. The number of web-based malware distribution sites is also increased from 13,018 in 2012 to 17,750 in 2013.

2.1.1 Hacking Intrusion

The number of hacking incidents reported to KrCERT/CC is 10,600 in 2013. It is decreased by 46% compared to that of 19,570 in 2012.





2013 KrCERT/CC incident report statistics

2.1.2 Zombie IPs

The number of Zombie PCs blocked by DNS Sinkhole in 2013 is 1,240,906. The number of this Zombie PCs reports shows almost a decrease of nearly 60% compared to that of 2012.

KrCERT/CC observed an increase in phishing incidents and malware distribution sites. Especially, phishing reports targeting Korean organizations such as financial institutions and so on hosted in foreign countries are setting increased. To protect our citizen, KrCERT/CC blocks the access to those foreign phishing hosts in cooperation with ISPs and requests for takedown of phishing hosts to the relevant CSIRTs or ISPs.

2.2 Massive cyber attack

KrCERT/CC encountered two kinds of the massive cyber attack in 2013.

First of all, the cyber attack which targeted 6 broadcasters and financial institutions happened on 20th March. 48,700 PCs and several ATMs were destroyed through vulnerabilities in the software update server.

Secondly, the website of Blue House that is executive office of the Republic of Korea,

the ruling party and major media companies were attacked by hackers on 25th June. The international hackers group, Anonymous launched a cyber attack on 40 North Korean websites on 26th June. About 130 internet servers were terminated, four homepages were defaced and two sites came under DDoS attack.

KrCERT/CC organized a joint response team, operated an emergency response system, analyzed malware codes collected from damaged systems, developed and distributed dedicated vaccines to remove the malicious codes and reinforced monitoring of homepages in provision against additional attack.

2.3 New service

2.3.1 Cyber Threat & Incident Information Analysis · Sharing System

Cyber Threat & Incident Information Analysis Sharing System is the system developed by the KrCERT/CC in 2013 with the purpose of collecting recent cyber threats and cyber incident information to manage them effectively, and find correlations between them. And National Security Vulnerability Database established by the sharing system provides well-used software vulnerability information for S/W venders and security companies before being abused by hackers.

3. Events organized

3.1 2013 APISC Training Course

KrCERT/CC hosted the 2013 APISC Security Training Course to support strengthening response capabilities of developing economies from Asia Pacific Region. The training has been annually held since 2005. The main objective is to assist developing economies who are interested in establishing Internet response capabilities, such as a CSIRT, while providing training opportunities for establishing and managing CSIRT in their own economy. The course was held from 8th to 12th July in Somerset Palace, Seoul, Korea. 20 trainees from 19 economies and 5 trainers from 4 economies attended 5 days of training course. On the first day of the course, all participants had a chance to share their domestic snapshot and experience on information security. The session helped to identify where each CSIRT is positioned and its future steps in consideration of the training curriculum.

From second day of the course, the Training of Network Security Incident Teams Staff (TRANSITS) educational materials were delivered for training. The active interaction between trainers and sharing responsibilities among trainers made the course more successful and fruitful.

4. International Collaboration

In 2013, KrCERT/CC has concluded the memorandum of understanding (MoU) and the framework for operational collaboration(FOC) with a foreign national CSIRT and a leading security company. The MoU with China, Kazakhstan and the FOC with Australia were signed to broaden the cooperation boundary to foreign countries. The MoU with McAfee, Fireeye would enable KrCERT/CC to share cyber threat information with the leading security company.

5. Future Plans

KrCERT/CC is planning to resume the hosting of the APISC training course to support capacity building for CERT/CSIRTs from developing economies. KrCERT/CC continues working with foreign partners actively on diverse issues on

cyber security.

KrCERT/CC Contact Information

Website : http://eng.krcert.or.kr

E-mail : first-team@krcert.or.kr

Phone : +82-2-118

14. 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 2013 there are three (3) staff providing the service with two (2) additional support staff. Staffing will need to be reviewed 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 2013 MOCERT has provided the following activities in addition to the base Incident Response and Early Waning through

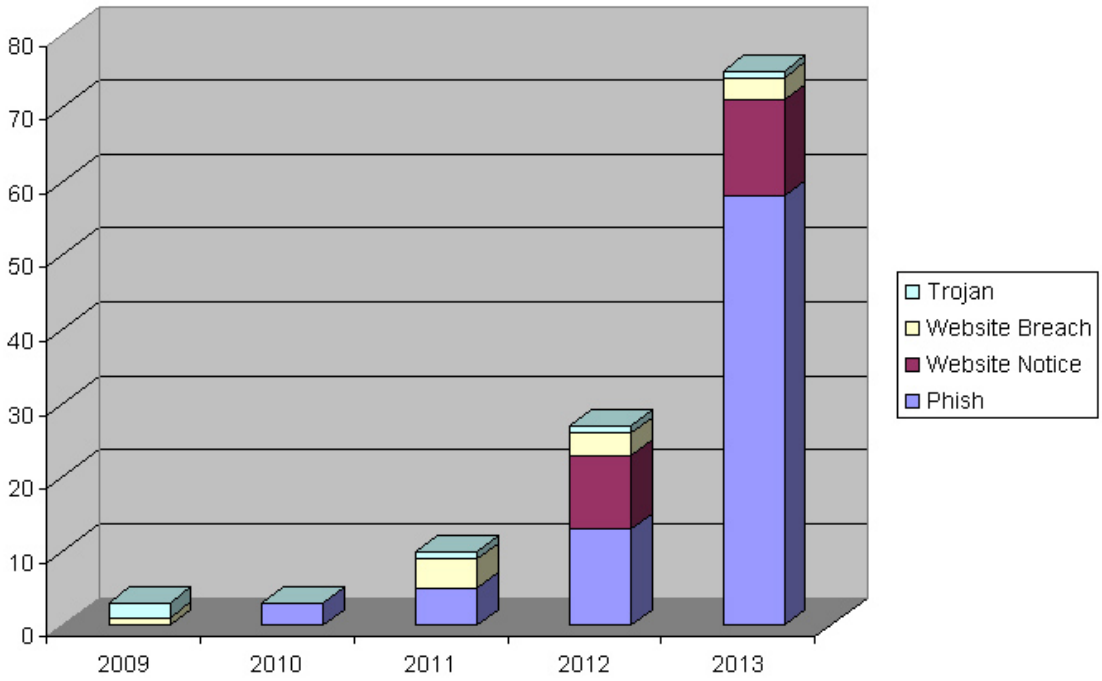
- Publication of industry specific notification of potential information security issues;
- Publication of broadly affecting issues that affect web servers of Macau origin be they government, industry or other;
- Conducted publicly available seminars on cyber security;
- Conducted workshops at the public, 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
- Assisted in the TSUBAME Working Group
- Assisted in the APCERT Drill 2013 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.

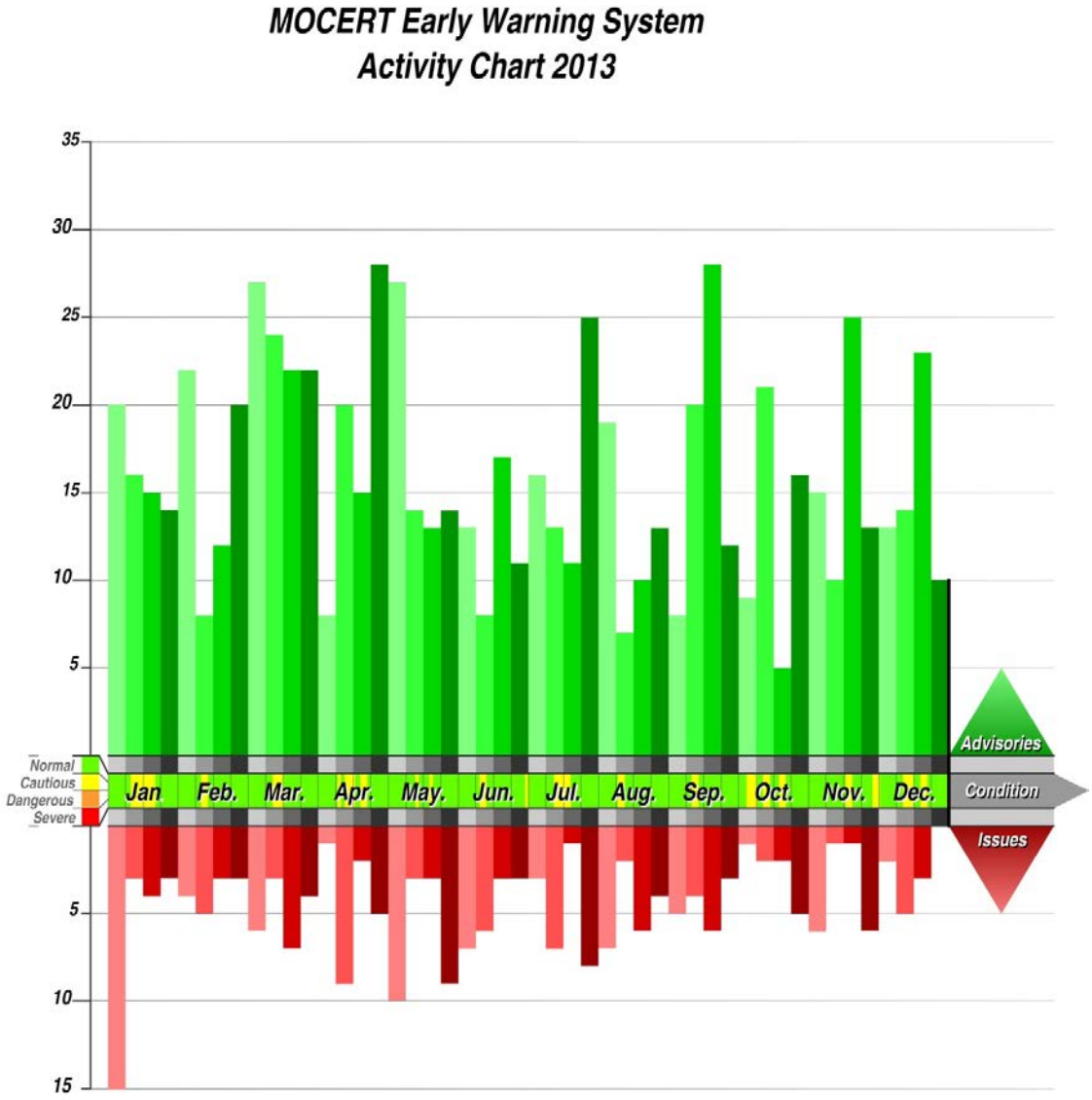
Sources of incidents are from three distinct channels.

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



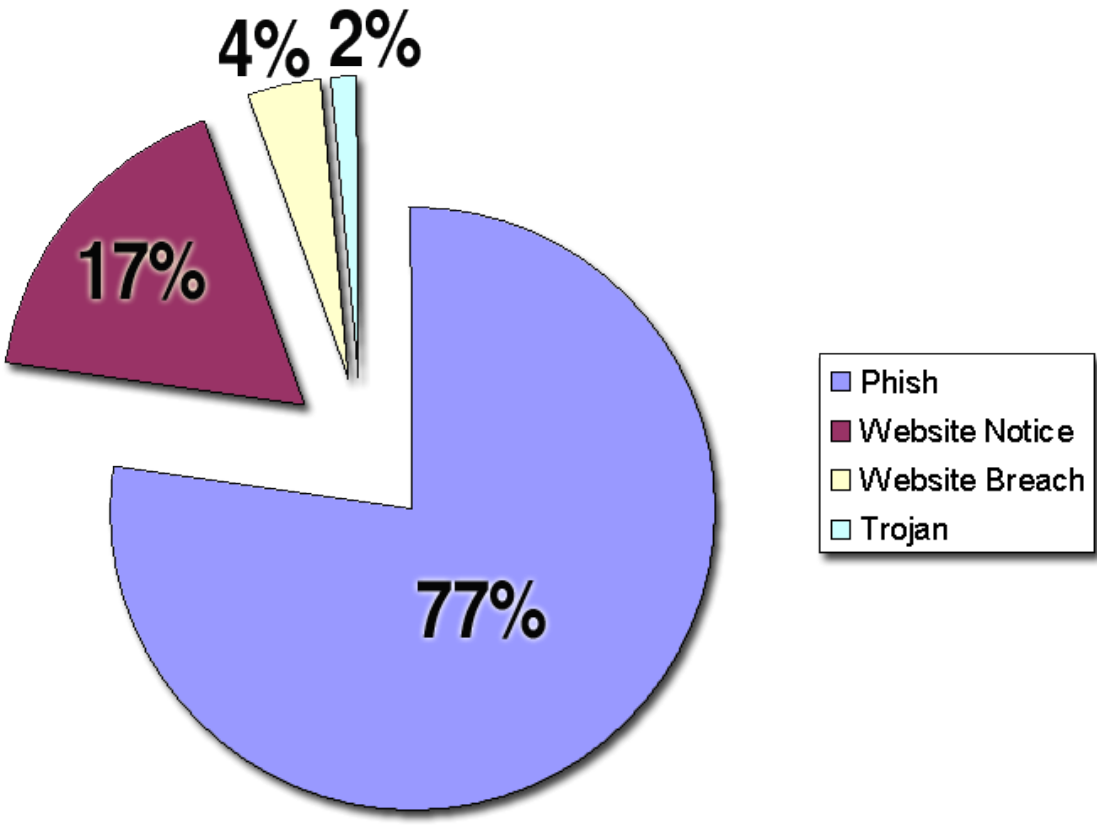
Early Warning Notices - A website collects notifications related to computer security, where all notifications are reviewed by staff to determine the impact to Macao constituency.

The notifications are then classified to Issues and Advisories and then posted. The following diagram shows the distribution of postings were in 2013, 981 postings were made with 776 Advisories, and 205 Issues.



2.2 Abuse statistics

The following pie graph denotes the abuse distribution as noted for the year 2013. The numbers are drawn from the incidents handled with the removal of the "web notices" as they do not constitute an abuse.



3. Events organized / co-organized

29th July 2013 - "Not IF but WHEN" "Clean PC Day"

Titled "Not IF but WHEN" 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 29th July 2013, at Macau Science Center

30-31 Jul and 1-2nd Aug 2013 – Master Classes

Titled "Reverse Engineering and Analysis of Malware"

Titled "Vulnerability Testing"

Two (2) master classes were run just after the Clean PC Day event, each delivering fourteen hours of experience back to the Macau community.

22nd January 2013 - "The Problem with Drive-by Downloads"

The seminar provided, through demonstration, the effect of a drive by download exploit. This seminar was designed as a high impact demonstration of the extreme effect of a successful exploitation as well as the relative little awareness the user has to such a successful attack. The event then goes on to show how frequent these attacks can be.

23rd May 2013 - "Smart Moves on Smart Devices"

This seminar focuses on smart choices that may be preformed in using popular communication applications on smart phones and to be able to align the expected level of trust to the past and current realities of the application's ability to deliver on that trust. As these applications change versions so rapidly, topics of the software's developer's business and software development strategies will be covered in the same detail as technical reviews of the application on mobile phone operating systems.

23rd October 2013 - "Practical G_PG_P"

This seminar focuses on the use of encryption using the PGP/GPG programs that are available. It covers not only the technical side of set up and running of these types of encryption but also talks about the operational challenges of using such a system. The seminar is aimed at transferring the skills to the Macau community

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 2013 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 2013. 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 2014 drill has been sought.

3.3 Seminars

MOCERT attend both APCERT Brisbane and FIRST Bangkok meeting in the year 2013.

4. Achievements

4.1 Publication.

The five (5) 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 is still investigating further cooperation with industry in handling and reducing the impact of phishing. Also, tied into this effort is performing malware analysis. Although the malware analysis team will take a significant amount of time to develop this is seen as a very important development of the MOCERT.

7. Conclusion

2013 has been a year where our services have touched saturation briefly in May of this year. The major challenges up ahead are restructuring the team to expand service in 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.

15. 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. In 2013 MonCIRT paid more attention on following functions because new malwares and attacks activated:

- Collection, analysis and dissemination of information on cyber incidents, internet threats
- Forecast and alerts of cyber security incidents
- Issue guidelines, advisories, vulnerability notes and white papers on information security practices, procedures, prevention, response and reporting of cyber incidents
- Provide information on incident and vulnerability trends and characteristics

MonCIRT aimed mainly on mining and energy sector business entities in 2013. 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:

1.1.1 Establishment

MonCIRT was established in 2006 as NGO. From 2006 till 2013 MonCIRT operate as sole national CSIRT of Mongolia. From 2013 the CERT at National Data Center was established and operate as Government entities CSIRT. From December of 2011 the MonCIRT assist in creation of this CERT based on MOU with National Data Center.

1.1.2 Workforce

MonCIRT currently has a total of 8 constant staffs such as: executive director-1, experts -3, the bookkeeper -1, system administrator-1 and watchers -2 .

1.1.3 Constituency

Currently MonCIRT's constituency are business companies, private sector organizations, NGO and general public. The NDC (Government) CERT encompasses all government bodies and critical inftrastructure organizations. We works closely with Chief Information Officers and system administrators of business sector's entities.

2. Activities & Operations

2.1 Activities

The summary of activities carried out by MonCIRT during the year 2013 is given in the following table:

Activities	Year 2013
Security Incidents handled	65
Security Alerts issued	216
Advisories Published	6
Vulnerability Notes Published	45
Security Guidelines Published	1
Trainings Organized	2
Mongolian Website Defacements tracked and advised	92
Open Proxy Servers tracked	6
Bot Infected Systems tracked	253
Phishing (mirror) web sites tracked and removed	6
Monitored targeted attacks and cyber espionage	3
Nation-state-sponsored cyber-attacks	1

In 2012 increased Mobile threats such as NFC worms, DroidDream, ZeaHace, TrojanSMS Agents, DroidKungFu. Phishing attacks overwhelmingly come from popular and trusted web sites hacked by cybercrime. In addition malware propagation through websites was observed constantly. Main methods of malware propagation was email, chat, social networks and malicious websites. Percentage of growth rates of Autorun and signatures to detect compromised websites 2012 vs. 2013 was 5,3%.

In 2013 MonCIRT observed first Industrial Espionage attempts and Nation-state-sponsored cyber attack attempt. For the reason of National Security

we cannot show IP addresses and these cases now under investigation of Government bodies.

From January through December 2013, the MonCIRT received 495 email messages and 196 hotline calls reporting computer security incidents or requesting information. 237 of these messages, information was related with real incidents and we provided with recommendations. We received 42 vulnerability reports and handled 65 computer security incidents during this period. We cannot retrieve incident handling statistics from most of organizations, administrators due to executive's restriction. From 2014 we plan to establish regular dialog with system administrators of organizations and to offer information on state of Internet security to the system administrators, network managers, and others in the Internet community.

2.2 Threats

Reflecting on the security and threat landscape of 2013, one trend that stands out is the growing ability of malware authors to camouflage their attacks. Widespread dissemination of advanced botnet and exploit kit source code allows more malware authors to create innovative and diverse new attacks.

Cybercriminals have started to leverage online marketing as a way to promote and sell their services on the black market. In 2012, the Blackhole exploit kit broke new ground. But in 2013, Blackhole was replaced by several new exploit kits that grew out of it, borrowing some of its code.

Modern malware is all about stealth. Advanced persistent threats (APTs), one of the most vicious examples of a stealth threat, precisely target individuals, businesses, governments and their data. APTs are a sophisticated weapon to carry out targeted missions in cyber space. Data leaks—including espionage and exposure of corporate data—was a primary theme this past year. APT attacks in 2013 were well-planned and well-funded; carried out by highly-motivated, technologically advanced, and skilled adversaries.

The growing popularity of the "Internet of Things" (e.g., mobile devices, applications, social networks, and interconnected gadgets and devices) makes the threat landscape a moving target. New threats arise with emerging technologies like near field communications (NFC) being integrated into mobile platforms. Innovative

uses of GPS services to connect our digital and physical lives present new opportunities for cybercriminals to compromise our security and privacy.

2.3 Incident trends

During the year 2013 MonCIRT handled several incidents related to botnet, web based malware, Android attacks and injecting Java script to redirect visitors to malicious websites. By exploiting vulnerabilities in web applications trusted websites are infected with links to malicious websites serving content that contains client side exploits. Most of incidents handled was web site defacements. We tracked and advised in 129 defacement cases from which 21 is handled by our team.

As show our monitoring, the malware delivery networks are now hiding in legitimate sites that are typically allowed by acceptable use policies.

In the past 12 months, botnets have become more widespread, resilient and camouflaged—and they seem to be finding some dangerous new targets.

In summer of 2013 the number of ZeroAccess infected endpoints reduced but ZeroAccess trend increased from September. Botnets are increasingly relying on the darknet. Based on bot infection alerts from APCERT we removed zombie infections and analyzed reasons. As revealed our analyze some C&C check-in address an infected client tries to contact isn't part of a botnet: it's a legitimate (but compromised) domain that can't conveniently be blocked.

Android malware continues to grow and evolve, following paths first blazed by Windows. But there is progress to report in securing the platform.

While no single Android malware family is currently dominant, today's most widely detected Android malware is Andr/BBridge-A. This Trojan uses a privilege escalation exploit to install additional malicious apps on your device.

Dangerous, difficult-to-detect web server attacks and exploit kits broadened in 2013, leading to more drive-by attacks against vulnerable web clients.

In 2012, Blackhole was the dominant exploit kit, but in 2013, newer kits such as Neutrino and Redkit became far more prevalent.

We are seeing more persistent, targeted attack and many seem to be aimed at compromising financial accounts

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

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

2.4 New services

2.4.1 Network secure administration

Excecutive director of MonCIRT Dr Esbold U and Mr Anar S (CISCO certified professional, network auditor) organized 2 trainings on network secure administration for system administrators of business organizations.

2.4.2 Setting up new CSIRT

We supported and assisted in creation of NDC's CERT and developed and provided 4 documents such as CSIRT establishment manual, CERT manual, Incident handling manual.

3. Events organized / co-organized

3.1 Training / Education

To create awareness and to enable users to implement best practices, MonCIRT is organizing workshops and training programs on focused topics for targeted audience such as mining, energy, financial and banking sector officers, System Administrators. Experts from industry are delivering lectures in these workshops apart from MonCIRT staff.

The MonCIRT offering different training courses. These courses derive from the practical work of the MonCIRT staffs, providing introductory and advanced training for technical staff and the management of network security management, configuration, incident response and are centered around broader Internet security issues and security practices.

We also organized Workshop "Mobile threats" in September 19, 2013.

3.2 Drills

In 2013 MonCIRT organized local network security drill-IV together with National Data Center CERT and this event covered about 28 entities.

3.3 Seminars

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

a. MonCIRT was one of the partner in organization of ICTPA expo 2013 and participated in conference dedicated to this event.

b. With sponsorship of Security Solution Service LLC and National Data Center organized annual "Security Open Day Mongolia 2013" in November. Within these days it is successfully hold scientific & practical conference, fair and workshop.

c. In addition MonCIRT co-organized third ethical hackers competition "Kharuul Zangi 2013" together with NDC in November of 2013 during "Security Open Day Mongolia 2013".

4. Achievements

4.1 Presentations

MonCIRT's board members participated and presented in local conferences as key speakers.

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 6 advisories and 45 vulnerability notes in 2013.

On the day of release, we sent advisories to a mailing list of MOSA and network administrators mailing list.

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 2013

5. International and Domestic Collaboration

5.1 MoU

We tried to sign MOU with National Cyber Security Office and NDC on establishment of MonCIRT/CC, but new management of these organizations delayed our offer .

5.2 Event participation

July 7th – 12th, 2012, Seoul

APISC 2013 training

5.3 International incident coordination

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

6. Future Plans

6.1 Future projects

Together with SecureShield Co.Ltd (USA) we plan to start project on establishment of National Threat monitoring center .

7. Conclusion

Despite difficulties in financings MonCIRT handled many incidents related with Business organizations and MonCIRT's awareness campaigns was successful. The awareness and knowledge of the public on information security have increased considerably thanking these awareness campaigns.

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.

In support of establishment of NDC CERT MonCIRT develops methodological guides, incident handling guide, CSIRT setting up guide on Mongolian and updated CERT handbook.

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 public and private sector oriented CSIRT and in future intend to act as Coordination Center and a national point of contact, for its international counterparts.

We will continue to conduct the Annual "Security Open Day" and will organize National Conference on Cyber Security under name "InfoSec Mongolia 2014".

MonCIRT shall continue to participate in regional events such as the Annual APCERT AGM, Technical workshops and will begin to participate in FIRST events and join FIRST.

Contact Information

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

.

Incident Response Help Desk

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

16. mmCERT

Myanmar Computer Emergency Response Team - Myanmar

1. About mmCERT

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 among IT Industries and government agencies in Myanmar. This annual report includes activities and operations which have been conducted in mmCERT during last year, 2013.

1.2 History

mmCERT was established as a national computer emergency response team in Myanmar on 23rd July 2004. The Ministry of Communication and Information Technology (MCIT) is a leading ministry of national cyber security in Myanmar and MCIT provides funding to mmCERT/cc (mmCERT coordination center) since it was formed last 3 years.

mmCERT/cc consisted of 10 members in 2013 and the Members of mmCERT/cc are from MCIT and MOST (Ministry of Science and Technology).

1.3 Constituency

mmCERT/cc has been enhancing for disseminating security information and advisories and providing technical assistance to his constituencies. These are financial, governmental, research and education, internet service provider, vendor and economy. Some government agencies, IT industries and service providers were closely dealing with mmCERT in 2013.

2. Activities and Operations

2.1 Weekly Email Newsletter

Every Friday, mmCERT Email Newsletter was published and distributed to all local ISPs and constituencies starting from August 24, 2012. Resources of Email

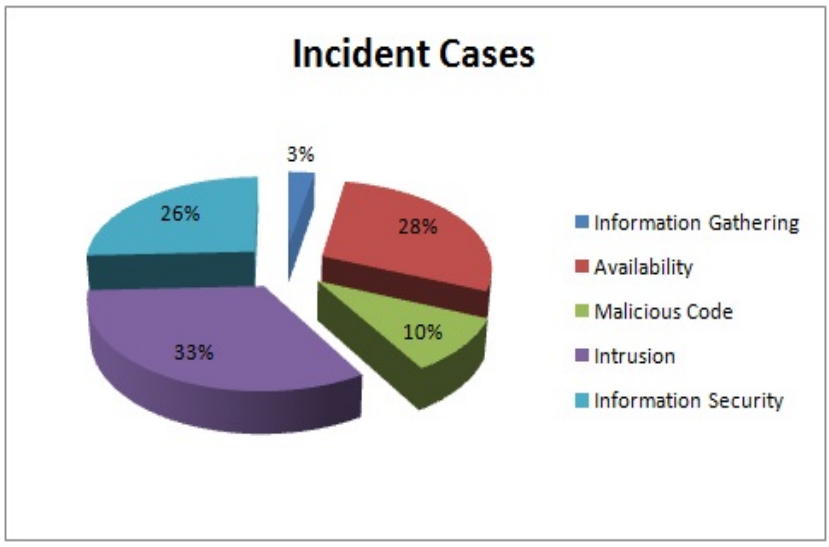
Newsletters are the report from APCERT members monthly, weekly and daily based and other security related information from internet and security organizations.

2.2 Weekly Technical Article

Every Thursday, mmCERT Technical Article was written in Myanmar and posted on mmCERT website (www.mmcert.org.mm) since May 2013.

2.3 Incident Handling Report

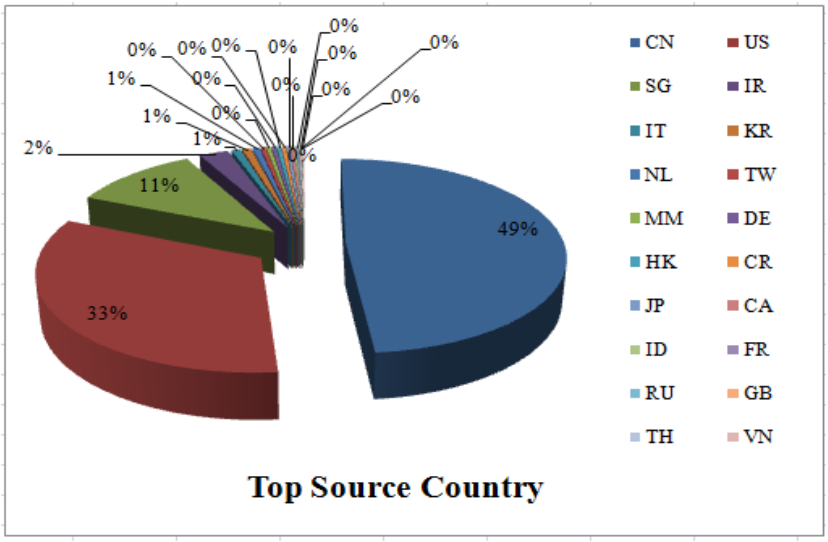
The following graph shows the incidents that were solved by mmCERT in 2013. According to our incident analysis, Intrusion and Availability incident cases were prominent happened in 2013.

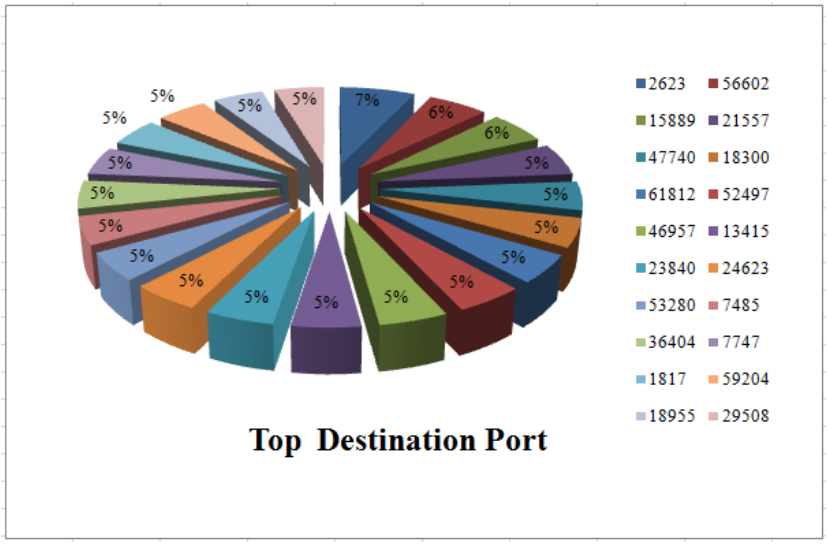


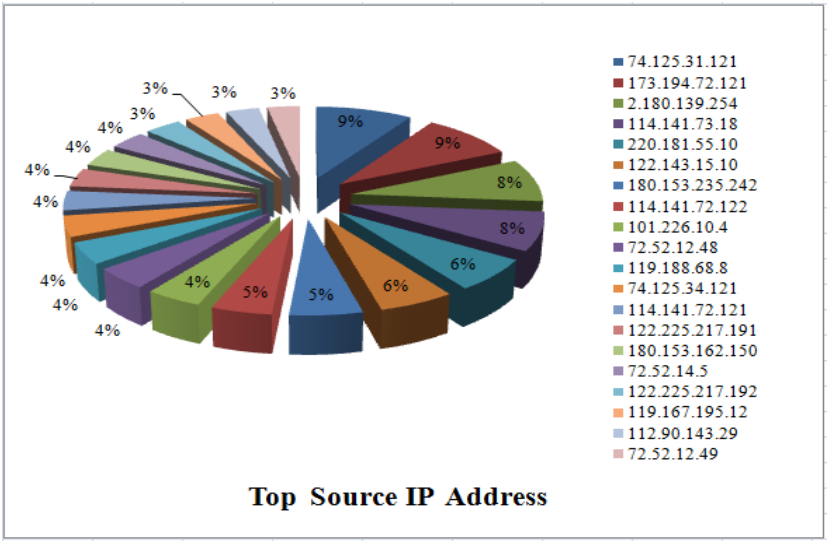
In addition, mmCERT gave technical advisories for all these incident cases to its constituency.

2.4 TSUBAME Statistics

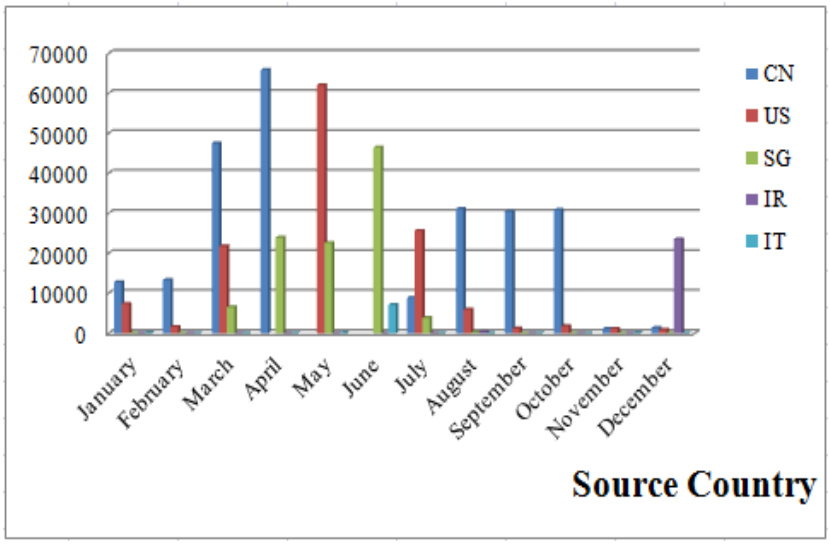
The following graph shows the top source country, top destination port and top source ip address statistics obtained from TSUBAME Sensor in 2013.

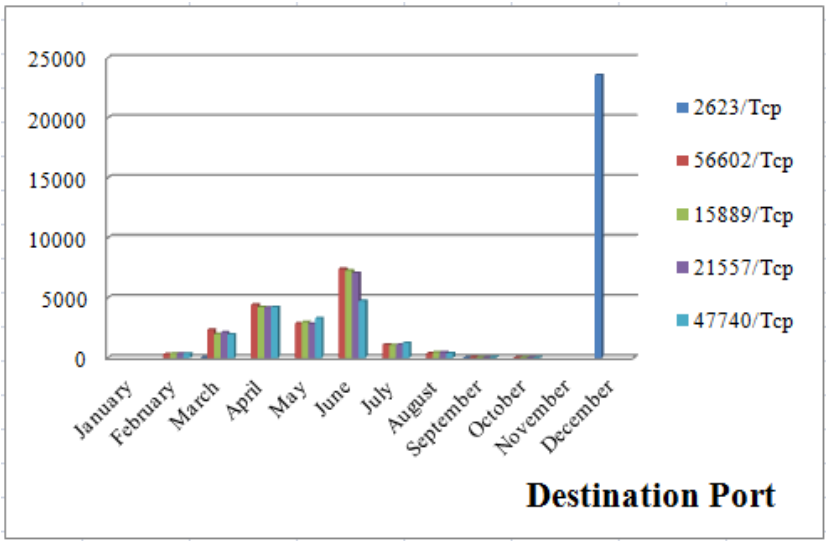


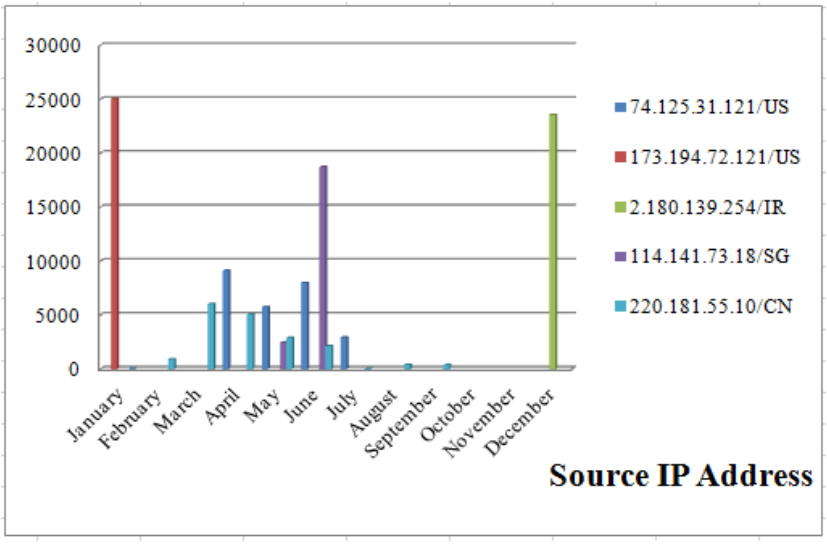




The following graphs show the top five countries, top five destination ports and top five source ip addresses statistics per month in 2013.


70000
60000
50000
40000
30000
20000
10000
0
January
February
March
April
May
June
July
August
September
October
November
December
CN
US
SG
IR
IT
Source Country


25000
20000
15000
10000
5000
0
January
February
March
April
May
June
July
August
September
October
November
December
2623/Tcp
56602/Tcp
15889/Tcp
21557/Tcp
47740/Tcp
Destination Port


30000
25000
20000
15000
10000
5000
0
January
February
March
April
May
June
July
August
September
October
November
December
74.125.31.121/US
173.194.72.121/US
2.180.139.254/IR
114.141.73.18/SG
220.181.55.10/CN
Source IP Address

3. Events Organized/Co-organized

3.1 Training

- Providing Network Forensic Training to government staffs and law enforcement agencies at Training Center, MCIT in Yangon on September 9-13, 2013.
- Providing Network Forensic Training to government staffs at Training Center, MCIT in Nay Pyi Taw on December 2-6, 2013.
- Providing Onsite Training to M.E Students from Technological University of Hmawbi, Myanmar on December 18 -19, 2013.
- Attending Specialized Program on Reducing Cyber Crime through Knowledge Exchange And Capacity Building provide by ITEC, CDAC at Noida, India from October 28 to December 23, 2014.

3.2 Workshop

- Participating in 4th APT Community Forum (CSF-4) at Kuala Lumpur, Malaysia on December 3-5, 2013.
- Participating in Cooperation against Cybercrime: Octopus Conference 2013 at Strasbourg, France on December 4-6, 2013.
- ITU Cyberdrill Workshop for CLMV on December 9-11, 2013 in Lao, PDR.

3.3 Seminar

- Providing Website Security Seminar to Government official from Ministries and IT persons from Private Company on August 8, 2012.
- Providing Seminar to government official from Law enforcement agency with following titles on October 2-3, 2013.
    - Current Cyber Security Status & Case Study
    - Cyber Crime
    - Computer Forensics
- Providing Seminar to public at Myanmar Info Tech on October 15, 2013
    - Cyber Security & Malware Analysis
    - Web Application Attacks

3.4 Drill

- Participating in APCERT Drill on January 29, 2013

- Participating in ASEAN CERT Incident Drill (ACID 2013) on October 9, 2013.
- Participated in Cyber Security Forum and Cyber Drill (CLMV) at Laos PDR. on December 9-11, 2013

4. International Collaboration

- Discussing on providing information security training proposed by Cyber Security, Malaysia with MOST, Malaysia.

5. Conclusion

As being mmCERT is a developing team, we are trying very much for our team in terms of organization framework; roles and responsibility; capacity building and etc. mmCERT/cc expect to be a developed and matured team among the APCERT members by doing incident handling and efficiently providing technical advisories to our constituencies in 2014. Moreover we are strongly willing to promote international and national cooperation on incident handling and information sharing as much as we can.

17. MyCERT

Malaysia Computer Emergency Response Team - Malaysia

1. Introduction

1.1 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 determine cyber threats to the nation. This agency beginings as the Malaysian Computer Emergency Response Team (**MyCERT**) in 1997 and with the establishment of CyberSecurity Malaysia in 2009, had expanded its services in the area of Digital Forensics, Cyber Security Assurance, Information Security Best Practises, Security Policies, Outreach Programs and Information Security Professional Development. Cybersecurity Malaysia now have more than 150 staffs and MyCERT is a department within this agency that provides cyber security incident handling, network monitoring services and malware research and analysis.

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 capability and capacity in the field of cyber security (Training) and to create awareness and a culture of cyber security (Outreach).

In order to execute the roles above, various services were introduced by

CyberSecurity Malaysia 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. InfoSecurity Professional Development;
ix. Outreach Programmes; and
x. Cyber Security Policy Research.

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

1.2 The Malaysian Computer Emergency Response Team

MyCERT, a department within CyberSecurity Malaysia, was the pioneer entity in providing incident handling services in Malaysia. It started in 1997 with 5 staff and presently has grown to 20 specialists of various CERT related areas. MyCERT serve as the point of reference for the Internet community in Malaysia dealing with computer security incidents such as intrusion, identity theft, malware infection, cyber harassment and other computer security related incidents.

Currently MyCERT offers 2 main services:

i. The Cyber999 Help Centre; and
ii. The Malware Research Centre

1.2.1 The Cyber999 Help Center

The Cyber999 Help center is for Internet users and organizations to report or escalate computer security incidents that threatens their on line security, safety or privacy. It is a public service that provides emergency response to computer security related emergencies as well as assistance in handling incidents such as computer abuses, hack attempts and other information security breaches.

The MyCERT website at: *http://www.mycert.org.my/en/* display the channels to report internet abuse and grievances to the Cyber999 Help Centre. The achievements of the centre to date are :

i. Responded and resolved 9986 incidents which is about 85% case resolution;
ii. Expert Witness for court cases that had been highlighted in the media; and
iii. Articles contribution related to web security in the Hackin9 newsletter.

1.2.2 The Malware Research Centre

The CyberSecurity Malaysia Malware Research Centre managed by MyCERT was launched on 2 December 2009. The centre operates a distributed research network for analysing malware and computer security threats. The centre collaborates with trusted parties and researchers in sharing security threat research information to further strengthen the capability of understanding cyber security treat levels. Other activities at this centre include:

i. Conducting research and development work in mitigating malware threats;
ii. Producing advisories on the latest malware threats;
iii. Monitoring threat through the distributed honeynet project; and
iv. Establishing partnership with universities, CERT's and international organizations.

1.3 Constituency

CyberSecurity Malaysia's constituency is the Malaysian Internet Users. Incidents within Malaysia that are reported by the Malaysian public and organizations will be resolved by assisting the complainants on cyber security technical matters. For cases involving international parties, CyberSecurity Malaysia will work with its foreign counterpart or trusted parties in resolving the matter.

2. ACTIVITIES & OPERATION

2.1 Incident Handling Reports And Abuse Statistics

CyberSecurity Malaysia through MyCERT receives reports from various parties within the constituency as well as foreign correspondents. These include home

users, private and government sectors, security teams from abroad (foreign CERTs), Special Interest Groups, and from internal proactive monitoring by CyberSecurity Malaysia's staff.

In 2013, MyCERT had produced:

i. 13 advisories;
ii. 7 alerts; and
iii. 5 summary reports.

The specific list of the advisory, alerts and summary reports can be viewed at:
http://www.mycert.org.my/en/services/advisories/mycert/2013/main/index.html

The Cyber999 Help Center had successfully resolved more than 93.55% of the incidents reported. There were about 10,636 cases reported of which the bulk of the incidents were related to:

No	Type of incidents	Percentage (%)
1	Intrusion	26
2	Fraud	42.2
3	Malicious Codes	16.5
4	Spam	8.9
5	Cyber Harassment	4.8
6	Vulnerabilities Report	0.2
7	Intrusion Attempts	0.7
8	Denial of Service	0.2
9	Content Related	0.5

Figures below shows reported cases that were handled by MyCERT for the year under review:

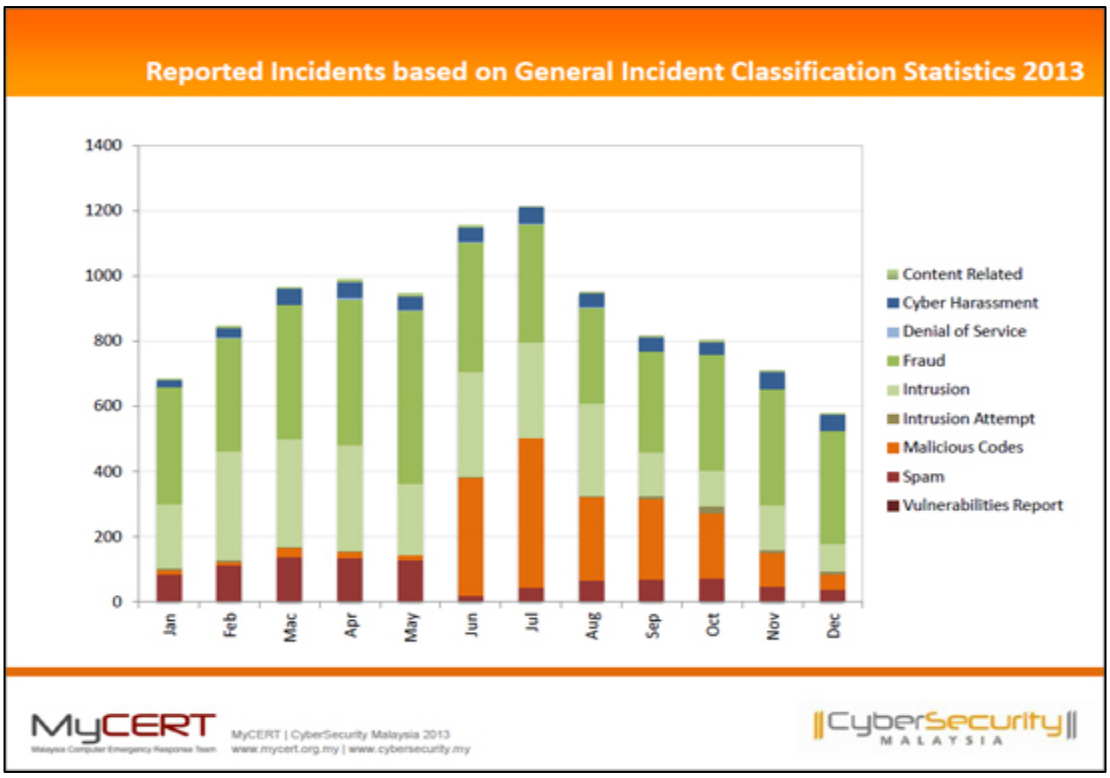


Figure #1: Reported Incidents Handled by MyCERT in 2013

Further information on Cyber999 statistics can be viewed at: http://www.mycert.org.my/en/services/statistic/mycert/2013/main/detail/914/index.html

3. EVENTS INVOLVEMENT AND ACHIEVEMENTS

CyberSecurity Malaysia's staffs actively provide assistance in the area of IT security by attending various training, seminars/conferences and meetings. MyCERT's staff has attended the following:

3.1 Cyber Drills

In 2013, CyberSecurity Malaysia was involved in three major multinational Cyber Drills.

The cyber drills are :

i. The 5th National drill, 25th November 2013;
CyberSecurity Malaysia was involved in co-organizing the drill called

X-Maya 5 with the National Security Council. The agency acts as the drill exercise coordinator which was participated by 80 organizations from law enforcement agencies, ISPs, local CERTs, banks, and relevant security organizations.

ii. The APCERT Drill, 29th January 2013;

iii. OIC-CERT Drill, 14th May 2013;
CyberSecurity Malaysia as the Chair of the OIC-CERT lead the drill as the organizer and exercise coordinator.

iv. The ASEAN CERT Incident Drill (ACID), 9th Oct 2013.

3.2 Trainings

CyberSecurity Malaysia conduct various information security training and hands-on training conducted in 2013 which among them are:

i. IHNS Training for National Cyber Crisis (X-Maya 5);

ii. CSIRT Training for Malaysia *Securities Commission; and*

iii. Incident Handling and Network Security Training for Government Agencies and Energy Sectors.

3.3 Presentations

CyberSecurity Malaysia through MyCERT had been invited to participate in various international conferences and seminars as speakers. Among the distinguished events were:

i. APCERT Conference, Brisbane, Australia
ii. FIRST TC, Amsterdam, Netherland
iii. OWASP, Kuala Lumpur, Malaysia
iv. National CSIRT Meetings, Bangkok, Thailand
v. OIC-CERT Annual Conference, Bandung, Indonesia

3.4 Tools developed

Following is a list of CERT specific tools developed by MyCERT:

i. G-Decoder (Javascript Deobfuscator)
ii. Malshare

iii. DontPhishMe IE (Browser Addons for Phishing Detection)

3.5 Paper Publication

Year 2013 has displayed few articles by the MyCERT with the objective of sharing their knowledge as well as improving their capability in expressing knowledge in the form of literature. The articles published are as follows:

i. Title : Automated Enhancement Tool for Malware Incident Handling
ii. Published : Artificial Intelligent Computer System (AICS 2013) Proceedings

3.6 Social Media

CyberSecurity Malaysia actively participated in disseminating security concerns to the mass media. Through social media such as Facebook and twitter, CyberSecurity Malaysia is able to address issues related to cyber security to its constituency. As of now, there are 1287 likes to Facebook and 686 followers to Twitter.

In addition, CyberSecurity Malaysia attends talking session on the local radio as well as television to address issues on security matters.

4. INTERNATIONAL COLLABORATION

4.1 Memorandum of Understanding (MoU)

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

i. China
ii. Egypt
iii. Indonesia
iv. Japan
v. Morocco
vi. Singapore
vii. Tunisia
viii. Turkey

4.2 New Partnership and Existing Cooperation

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

i. As the Permanent Secretariat of the Organization of Islamic Cooperation - Computer Emergency Response Team (**OIC-CERT**);

ii. Exploring the possibility of collaboration with AfricaCERT;

iii. Reaching out to OIC countries that is not an OIC-CERT members; and

iv. Participation in the Verizon Inc DBIR project by providing yearly security incident statistics.

5. FUTURE PLANS

CyberSecurity Malaysia, through MYCERT, will strive to enhance awareness to its constituency and encourage security incidents be reported to it Cyber999 help centre. There are plans to expand MyCERT reporting channels and promote of its services through the mass media.

CyberSecurity Malaysia also looks forward to new collaboration with local and international security organization and hope to encourage more formation of CSIRT within an organization. It is inspired to work closely with other security organization and CERT community by holding bilateral agreement through MoUs.

Encouragement of skilled and certified staff who would be able to contribute in the international security arena is the agency's aspiration. Staff would be supported to provide training, presentation and publication in international security events. CyberSecurity Malaysia, through MyCERT, will develop in-house tools to assist in mitigating security issues to be used by the stakeholders. Development Projects are planned to develop tools that will assist the public and banking industry to secure their online activities.

6. CONCLUSION

CyberSecurity Malaysia, through MyCERT, observed a slight increase in computer incidents reported to its Cyber999 Help Centre in 2013 compared to the previous

year. The agency will work with the constituencies and international allies to generate useful cooperation in safe guarding the cyber environment.

As the cyber environment does not conform to the physical boundary of the countries, international relations will remain an important initiative. CyberSecurity Malaysia will continue to establish and support cross border collaboration either through bilateral or multilateral platforms such as the APCERT and the OIC-CERT. New cooperation between CyberSecurity Malaysia and other security organization had been created especially concerning mobile security and malware threats.

The Malaysian National Cyber Security Policy provides emphasis on capacity and capability building, mitigation of cyber threats and international collaboration. In line with this, CyberSecurity Malaysia will continue to develop new and enhance existing cyber security processes, human capability and technology. CyberSecurity Malaysia will continue its commitment to seek for new edges in cyber security and to be a catalyst in developing the industry

18. 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 2013 as compared to the year 2012.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 2013. 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 2013

The ASEAN CERTs Incident Drill (ACID) 2013 was conducted successfully on 9 October 2013. In order to develop scenarios which reflected prevailing cyber threats that were confronting the CERTs, the theme selected for the drill was focused on threats from investigating and responding to a cyber espionage scenario in a company. 14 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 9 October 2013
- SingCERT participated in the APCERT Annual incident drill in 29 January 2013.

5. Future Plans and Projects

5.1 ACID Drill

SingCERT will be organising the 9th ASEAN CERTs Incident Drill for the year 2014. Discussions are in progress to work out the scope and coverage.

19. 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 responses to cyber security threats and vulnerabilities.

1.1.1 Establishment

As the national CERT of Sri Lanka, Sri Lanka CERT 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 ICT revenue generation activities. 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 the 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, the ICTA was brought under the purview of the newly formed Ministry of Telecommunications and ICT.

1.1.2 Workforce

Sri Lanka CERT currently has a total strength of eight team members consisting

of the Chief Executive Officer, Manager Operations and Principal Information Security Engineer, two Senior Information Security Engineers, two Information Security Engineers, an Information Security Analyst and an Administrative Officer. This team is supported by five undergraduate interns. All the staff are highly skilled and experienced in different areas of information security and have achieved corresponding Information security certifications which are widely recognized in the industry, such as SANS GCIH, Microsoft MCSE, EC-Council Certified Ethical Hacker (CEH) and Certified Hacking Forensics Investigator (CHFI), Cisco CCNA and CCSP and CISSP by International Information Systems Security Certification Consortium; (ISC)[2].

1.1.3 Constituency

Sri Lanka CERT's Constituency encompasses the whole of the cyber community of Sri Lanka (private & public sector organizations, and the general public). Sri Lanka CERT maintains a good rapport with government and private sector establishments, and extends assistance to the general public as permitted by available resources. In accordance with its mandate, Sri Lanka CERT | CC gives priority to requests for assistance from government. Based on availability of human resources and necessary skills, requests from private sector are handled free of charge or on a paid basis, depending on the type of service provided.

2. Activities & Operations

2.1 Incident Handling Statistics

Incidents reported to Sri Lanka CERT decreased to 1,375 in the year 2013. In the year 2012, 1,840 incidents were reported. This is a 33% decrease in reported incidents compared to the year 2012. This decrease may be a testimony to the awareness that Sri Lanka CERT has succeeded in creating among the general public with regard to taking protective measures as well as finding solutions for themselves due to the awareness that has been created. Another reason could be the establishment of a cyber crime unit by the Sri Lanka Police with the assistance of Sri Lanka CERT. Some constituents may as a result report incidents directly to the Police. We have not as yet been able to collate these statistics.

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

Type of Incident	No
Phishing	8
Abuse/Privacy	8
Scams	18
Malware	2
Defacements	16
Hate/Threat Mail	8
Unauthorized Access/Attempts	11
Intellectual property violation	3
DoS/DDoS	1
Fake Accounts	1,300
Total	**1,375**

2.2 New services

2.2.1 Setting up sector based CSIRTs

Sri Lanka CERT initiated the setting up of sector-based CSIRTs in 2010. Typical sectors are Banking, Telecom, Defence and Education. All the preparatory work relating to the setting up of the Bank CSIRT have been done, and suitable launch date will be fixed during the course of the year, while the Defence CSIRT is also in its formation stage. The Telco CSIRT concept paper is awaiting approval from the Telecom Regulatory Commission (TRC) Board, which the intended host body. The Education CSIRT is in the concept phase.

The rationale for sector based CSIRT's is to ensure that Sri Lanka CERT 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.

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.

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.

2.2.2 National Certification Authority

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

To address this issue, Sri Lanka CERT, ICTA (the apex body for ICT in Sri Lanka) and various stakeholders have come together to form a task force to determine the policies, procedures, governance and service models of the national CA. The end objective is to have a national level body which will effectively regulate the issuing of a number digital certificate classes at affordable prices that are in accordance with the local legislation and international standards.

Sri Lanka CERT expects to launch the National CA in the year 2014.

3. Events organized / co-organized

3.1 Training / Education

In order to fulfill its mandate to create awareness and build IS skills within the constituency; Sri Lanka CERT continues to organize training programs and education sessions targeting various audiences including CIOs, Engineers,

System Administrators, Banking and Telecom Sector Staff, Students, and General Public.

During the year 2013 Sri Lanka CERT conducted the following training and education programs successfully:

- Regular press releases to the media about incidents and impending vulnerabilities
- Awareness programs for School Teachers.
- Bank CEO's forum organized by Central Bank of Sri Lanka
- SEARCC2013 International conference organized by Computer Society of Sri Lanka
- Seminar for Child and Women's Bureau
- CISSP certification awareness event in collaboration with ISC(2).
- Cyber Guardian e-newsletters distributed monthly through SchoolNet. This is the third consecutive year of this circulation which is widely accepted and read.
- Train-the-trainer on-line safety awareness programs island wide with the assistance of the Ministry of Education for IT Teachers of schools
- Child on-line safety awareness presentations at private and government schools
- Participated in a one hour radio program called "Subarathi" in Sri Lanka Broadcasting Cooperation and two hour radio program in "Sinha Sakkshiya" in 'SinhaFM' popular private radio channel as part of CERT's awareness creation campaign
- Conducted a training program for SOCO officers at police training college 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.

3.2 Consultancy

Sri Lanka CERT 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 organizations
- Application and network security vulnerability assessments for e-Government applications
- Credit card fraud investigations for a local banks
- Conducted information security assessments to secure the website and Registration Management System of the Commonwealth Heads of Government Meeting (CHOGM 2013).
- Carried out technical forensic investigations for the Criminal Investigations Division (CIS) 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
- 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
- Preparing an RFP for the procurement of an Internet Payment Gateway for a government bank as a paid consultancy service.
- Developed a Baseline Security Standard for Banks with the assistance of SLSI (Sri Lanka Standards Institution) and Central Bank of Sri Lanka

3.3 Seminars & Workshops

- Cyber Security Week 2013: Since 2008, Sri Lanka CERT | CC has been conducting an annual security awareness program titled Cyber Security Week (CSW). This international event draws attention of the local as well as regional information security professionals.

  Cyber Security Week 2013 was held in the month of September, and featured a

series of events:

- Annual National Conference on Cyber Security
- Workshop for law enforcement agencies by APNIC
- Three full-day Workshops for professionals, namely:
    - Technical workshop on "Network forensics using netflow and botnet traffic analysis"
    - Technical workshop on "Socio-technical assessment of access and insider threats"
    - Technical workshop on " Network security focusing on router and DNS 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 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 the Council of Europe Workshop on Cyber Crime and Cybercrime Legislation, including the adaption of the Budapest Convention.
- CIO Forum in collaboration with (ISC)2 Sri Lanka Chapter.
- Carrying out Presentations on Information security for SLAS (Sri Lanka Administrative Services) officers at SLIDA

4. Achievements

4.1 Publications & Other media

a. Website

The Sri Lanka CERT 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.

b. 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.

c. Newspapers/media

Sri Lanka CERT 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 against these attacks.

4.2 Certification & Membership

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

- Microsoft SCP (Security Cooperation Program)
- Collaborative agreement with "IMPACT", where Sri Lanka CERT will benefit from receiving threat intelligence from the region and also form part of the global incident response team.

The most important achievement to-date in this respect is Sri Lanka CERT's role in the setting up of the Sri Lanka Chapter of the International Information Systems Security Certification Consortium, Inc., commonly referred to as the (ISC)², and widely accepted as the global, non-profit leader in educating and certifying information security professionals throughout their careers.

The Sri Lankan Chapter was formed with the objective of disseminating knowledge and providing a common forum for the information security professionals and the (ISC)² credential holders. In addition, the Chapter encourages Information Security certifications among professionals in Sri Lanka. This has now evolved to being a fully fledged association that serves as the main 'focus' group for Information Security Professionals in the country and Sri Lanka CERT continues to facilitate it's growth.

5. International Collaboration

5.1 MoU's

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 and Shadowserver; as a result of above MoUs Sri Lanka CERT gets daily statistics for its "Threat Visualization System" which is used for alerting ISPs about possible suspicious network traffic.

5.2 Event participation

March 24th -27th
2013-APCERT AGM & Conference, Brisbane-Australia

June 16th-21st
2013- FIRST AGM & Conference, Bangkok- Thailand

June 22nd -23rd
CERT | CC conference for CERTs with National responsibility

5.3 International incident coordination

Sri Lanka CERT | CC actively participated in the APCERT Drill 2013 as a player.

In addition to the engagements with CERTs the Asia Pacific region, Sri Lanka CERT has regular operational engagements with CERTs/Information security organizations in other regions of the world and commercial organizations (such as Facebook, Google, Yahoo) to handle phishing and identity theft incidents.

6. Future Plans

6.1 Future projects

The following projects are either in the conceptual stage or just being initiated,

and are intended to serve the constituency directly;

- Development and Implementation of a security operations center (SOC)
- Establishment of the National Certification Authority
- Establishment of sector based CSIRT's
- Cyber Security Week 2014

6.2 Framework

6.2.1 Future Operations

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

- Recruitment of undergraduate 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.

6.2.2 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, it is planned to place the sensors at all ISP networks to cover the IP blocks in order to gather data on attack traffic generating to and from the country. The 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.

All this information, coupled with the Automated Threat Analysis and Visualization tool will enable Sri Lanka CERT to spot potentially vulnerable incidents at a glance and proceed to take remedial measures.

7. Conclusion

After establishing Sri Lanka CERT in 2006, it was necessary to conduct awareness campaigns to notify the public about our presence and the activities. 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 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 2013 were very successful 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 shall continue to participate in regional events such as the Annual APCERT 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 with the help of all the CERTs and information security organizations through APCERT.

20. TechCERT

Tech CERT – Sri Lanka

1. About TechCERT

1.1 Introduction

The information-driven and highly networked economy of the modern day requires organizations to operate complex information systems and be interconnected through local and international networks that span geographical, legal and cultural boundaries. Organizations that store and process sensitive and valuable trade and market information, client information and transaction history data, continues to be at the top of potential targets for cyber criminals who probe, scan and penetrate the IT infrastructure of these organizations to carry out massive thefts of proprietary data, customer information and transaction data.

The aftermath of a cyber-attack is not only the direct revenue losses but also the tremendous indirect costs to rebuild the IT infrastructure and re-establish its security. TechCERT assists the general public of Sri Lanka and its members secure the proverbial stable doors before the horses get an opportunity to bolt. While individuals and organizations in Sri Lanka have been provided with expanded legal cover under the Electronic Transactions Act No 19 of 2006 and Computer Crimes Act No 24 of 2007, it also imposes a heavy burden on corporations to secure the private and confidential information that they store and transmit on public unsecured IT infrastructure.

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	2
MEng/MSc/MPhil/MISM	11
PG Diploma	3
BSc Eng/BSc/BIT	13
CISSP	1
CISA	1
C|EH	6
C|HFI	1
Certified ISMS Auditor (ISO27000)	2
MCP/MCSA	4
MCSE/MCTS	2
CCNA / CCNA Security/CISCO FWL	4
ITIL V3	2
Qualys Guard Certified Specialists	2
CISE	1
ACE	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.

2. Activities & Operations

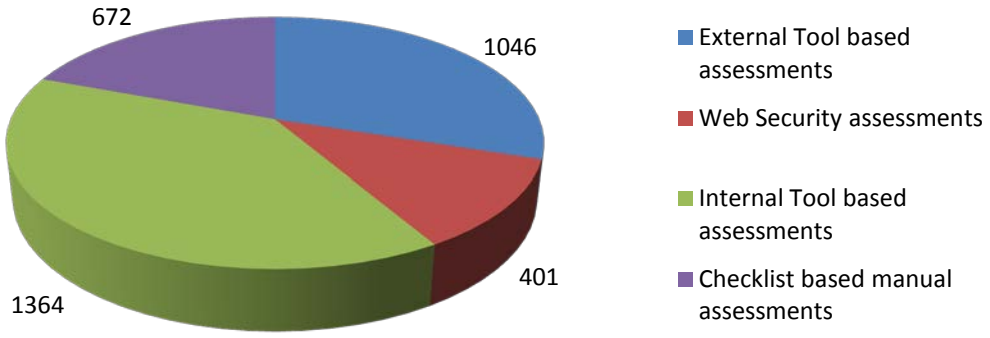
The TechCERT Managed Security Services include a range of engineering and consultancy services:

- 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 audits
- 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 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

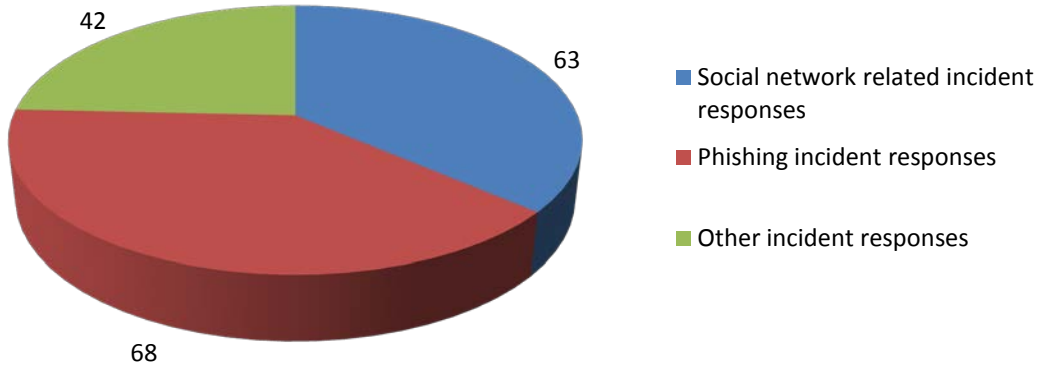
Security Assessments

Activity Type	Count
External Tool based assessments	1046
Web Security assessments	401
Internal Tool based assessments	1364
Checklist based manual assessments	672



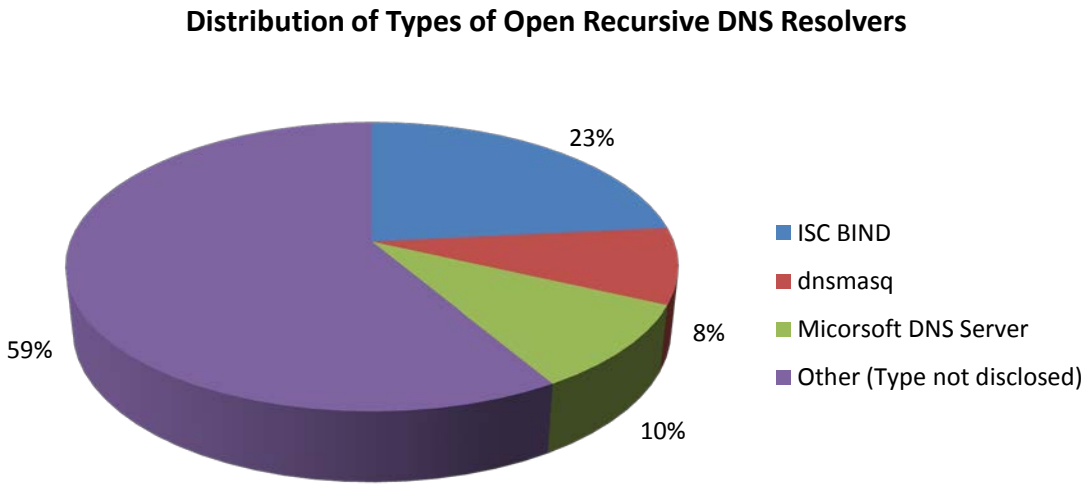
Incident Response

Type of Incident Response	Count
Social network related incident responses	63
Phishing incident responses	68
Other incident responses	42



DNS Buster Project (Open Recursive DNS Server Detections)

Total assessments	25400 *(100 IP blocks of 24 net mask)*
Number of Total detections	94



3. Events

3.1 Organizing of Training Seminars, Workshops and Demonstrations

2nd February 2013	**Public Seminar and Demonstration – Safe Use of Computers – Sabaragamuwa Province** TechCERT conducted a public seminar and demonstration session enhancing knowledge about common pit falls in internet. This seminar was conducted in Sri Lanka Telecom auditorium in Rathnapura.
8th March 2013	**Public Seminar and Demonstration – Information Security Modern Workplace – North Province** TechCERT conducted a public seminar and demonstration session enhancing knowledge about information security aspects in work environment. This seminar was conducted in Jaffna Library.

14th March 2013	**Seminar and Demonstration – Safe Internet Browsing – Southern Province** TechCERT conducted a seminar and demonstration session enhancing knowledge for university students and lecturers about common pit falls in internet. This seminar was conducted in Agriculture Engineering Department, University of Ruhuna.
21st March 2013	**Public Seminar and Demonstration – Safe Use of Computers – North West Province** TechCERT conducted a public seminar and demonstration session enhancing knowledge about common pit falls in internet. This seminar was conducted in Sri Lanka Telecom auditorium in Kurunegala.
9th May 2013	**Public Seminar and Demonstration – Safe Use of Computers – Central Province** TechCERT conducted a public seminar and demonstration session enhancing knowledge about common pit falls in internet. This seminar was conducted in faculty of engineering university of Peradeniya.
3rd September 2013	**Public Seminar and Demonstration – Safe Use of Computers – North Central Province** TechCERT conducted a public seminar and demonstration session enhancing knowledge about common pit falls in internet. This seminar was conducted in Post-Harvest Technology Institute, Anurdapura.
5th November 2013	**Seminar and Demonstration – Cyber Safety – Western Province** TechCERT conducted a seminar and demonstration session enhancing knowledge for students and lecturers about common pit falls in internet. This seminar was conducted in Sri Lanka Institute of Advance Technological Education.

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

Program Name	Date	Audience	Venue
Safe internet Browsing	18th January 2013	Students	Malabe Rahula Vidyalaya, Talahena, Sri Jayawardenepura Kotte
Safe Internet Browsing	24th January 2013	Students	Gothami Balika Vidyalaya, Colombo 10.
Safe Internet Browsing	15th March 2013	Students	St Aloysius College, Galle.
Safe Internet Browsing	5th May 2013	Teachers/Students	Nalanda College, Colombo 10.
Cyber Safety	11th October 2013	Students	Royal College, Colombo 7
Cyber Safety	7th November 2013	Students	Kottawa Dharmapala Vidyalaya, Kottawa
Safe Internet Browsing	11th February 2014	Students/Teachers	Bandarawela Educational Zone
Stay Safe on Internet	11th February 2014	Students	St Joseph Girls College, Nugegoda

Safe Internet Browsing	12th February 2014	Students/Teachers	Sri. Devananda Vidyala, Bandarawela
Cyber Safety	13th February 2014	Teachers	Welimada Educational Zone

3.3 Participation in Conferences, Workshops and Training Programs

1. Dr. Shantha Fernando, Chief Consultant / Co-Founder of TechCERT participated for the, FIRST, 25th Annual FIRST Conference 'Incident Response: Sharing to Win' held on 16-21 June 2013 at Bangkok, Thailand

2. Nalinda Herath participated for the APCERT AGM and Conference 2013 held on 24-27 March 2013 at Brisbane, Australia

3. Dileepa Lathsara, COO TechCERT and Amila Perera participated for the workshop 'Capacity Building Workshop on Electronic Evidence Conducted' conducted by Council of Europe held on 4-5 October 2013 at Colombo, Sri Lanka

4. Asanka Balasooriya participated in '2nd International Conference on Security Science and Technology ICSST 2013 and International Journal of Engineering and Technology (IJET)' held on 1-2 April 2013 at Singapore.

5. Kushan Sharma and Kasun Chathuranga participated for the workshop 'Qualys Guard Vulnerability Management & Policy Compliance' conducted by Qualys Inc on 24-25 October 2013 at Colombo, Sri Lanka

6. Kushan Sharma participated in 'ERU Conference 2013' held on 27 February 2013 organized by University of Moratuwa, Sri Lanka.

7. Asanka Balasooriya participated in '19th ERU Symposium 2013' held on 26 November 2013 organized by University of Moratuwa, Sri Lanka.

8. Dileepa Lathsara and Nalinda Herath participated for the training of 'National Root Certificate System' conducted by Epiphany Consulting Co Ltd, Thailand on 17-19 December 2013 at Colombo, Sri Lanka

9. Nalinda Herath and Asanka Abeyrathne participated for the training of 'Red Hat Certificate System' conducted by Open Ed Consulting (Private) Limited on 20-23 January 2013 at Colombo, Sri Lanka

3.4 Cyber Security Drills

29th January 2013	**APCERT Cyber Security Drill 2013** TechCERT participated in the Drill as a member of the Organizing Committee and member of EXCON
27th June 2013	**Cyber Security Drill for Sri Lankan Banks** TechCERT conducted a cyber-security drill for the Sri Lankan Banking Sector on 'Countering Large Scale Denial of Service Attacks and Coordination within Sri Lanka"
29th July 2013	**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 "Countering Large Scale Denial of Service Attacks and Coordination within Sri Lanka"

4. Achievements

4.1 Technological Achievements

- Deployment of the project "DNS Buster" with cooperation with Sri Lankan ISPs to detect open recursive DNS resolvers and remediate. Open recursive DNS servers can be used DNS Amplification DDoS attacks.

- Deployment of Incident Response Hot-Line
- Deployment of free web site security assessment program for Sri Lankan sites
- 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
- Improvements for the DNSSEC integration project in to LK Domain

4.2 Technical Publications

1. Kushan Sharma And Chandana Gamage, "Building Sand Castles Within IAAS-Based Cloud Instances", 18th ERU Research Symposium, 2013: Faculty Of Engineering, University Of Moratuwa, Sri Lanka

2. Asanka Balasooriya & Shantha Fernando, " Generalized Extensions for Botnet Detection", in the proceeding of National Engineering Conference, 19th ERU Symposium, Faculty of Engineering, University of Moratuwa, Moratuwa, Sri Lanka., November 26th 2013.

3. Asanka Balasooriya & Shantha Fernando, "Next Generation Security Framework to Detect Botnets on Computer Networks", in the proceeding of 2nd International Conference on Security Science & Technology ICSST 2013), April 1-2, 2013, Singapore.

5. Future Plans

- Improve proactive IT security response strategies
- 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 several cyber drills for the Banking Sector and conduct the first ever cyber drill Telcos and ISPs in Sri Lanka.

Similar to year 2012, there was a significant increase in phishing attacks and web site defacement/hacking incidents in Sri Lanka in 2013. TechCERT successfully responded to most of the incidents reported and assisted the relevant authorities to mitigate the threats. 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.

21. ThaiCERT

Thailand Computer Emergency Response Team - Thailand

About ThaiCERT

Introduction

ThaiCERT, a non-profit government funded, is a Computer Security Response Team (CSIRT) for Thailand, providing an official point of contact for dealing with computer security incidents in Internet Community of Thailand. Further from to coordinating and handling with the reported incidents, ThaiCERT also provides an advisory service to both the organizations and individuals, releasing cybersecurity alerts and news, and organizing academic trainings for the public to enhance knowledge and raise awareness of people on information security. With the emerging of various security incidents in the Internet Community of Thailand, ThaiCERT then expanded its service not only to the government units but also to the private organizations as well. Currently, ThaiCERT is a security operation unit in a public organization named Electronic Transactions Development Agency (ETDA), under the supervision of Ministry of Information and Communication Technology, Thailand.

Constituency

The constituents of ThaiCERT are public, private and home sectors of internet users in Thailand. ThaiCERT provides the incident coordination service to other international entities, where the sources of attacks were originated within Thailand as well.

Staffing

ThaiCERT currently employs 13 full-time technical staffs consisting of 6 senior security specialists and 7 IR and forensics engineers.

Activities & Operations

Abuse statistics

Reported Incidents Received from E-mail

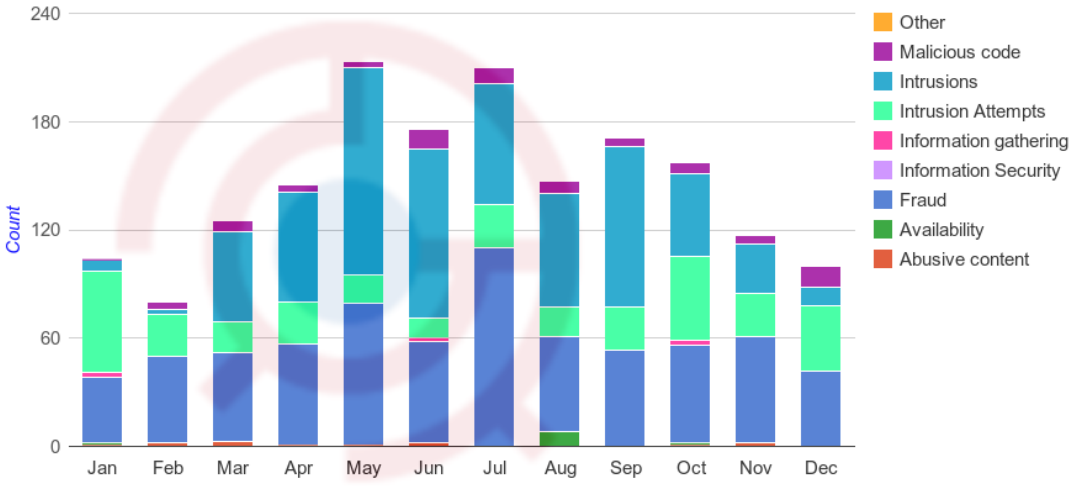


Figure 5: The number of reported incidents in 2013

Through the official e-mail address, ThaiCERT received a total of 1,745 reported incident cases (tickets) in 2013, which were increased by 120% compared to those of 2012 (792 cases). The received reports per month varied approximately between 80 to 210 cases as shown in Figure 1, relatively higher than the previous year (30 to 100 cases per month).

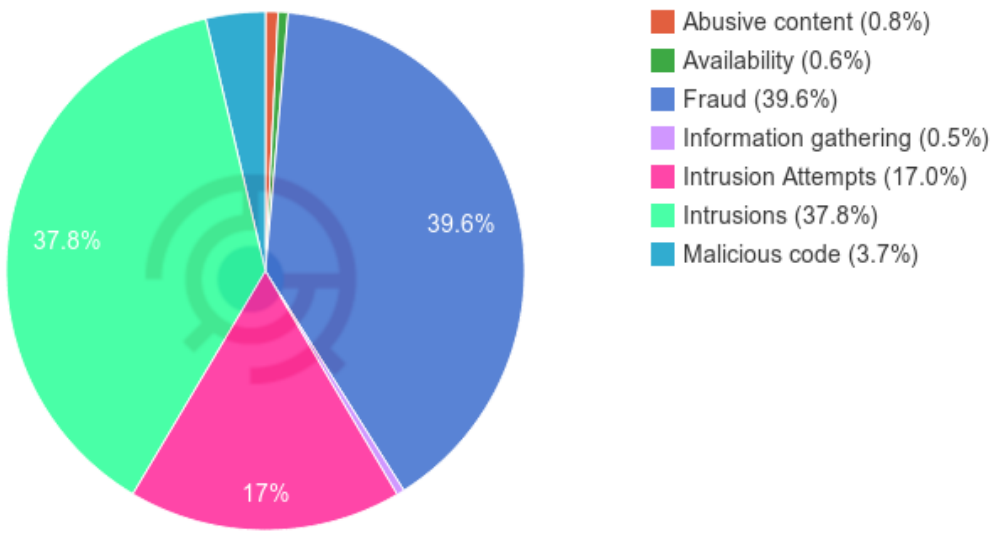


Figure 6: The proportion of reported incidents by incident type in 2013

In reference to the received tickets classified according to eCSIRT incident classification[1], 39.6 % of incident reports were on fraud, where most fraud cases in these statistics were phishing. The number was followed by intrusions (37.8%), where most of the cases were website defacement, and intrusion attempts (17.0%).

While in the previous year, the number of fraud incidents dominated in reported incident types with 67.4%, the numbers of fraud and intrusion incidents were almost the same in 2013 due to increasing intrusion incidents. Compared to the previous year, the number of intrusion incidents was increased significantly from 13 cases in 2012 to 632 cases in 2013 because ThaiCERT decided to handle defacement incidents reported from our automatic feed system which collected incident reports from our global security partners.

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

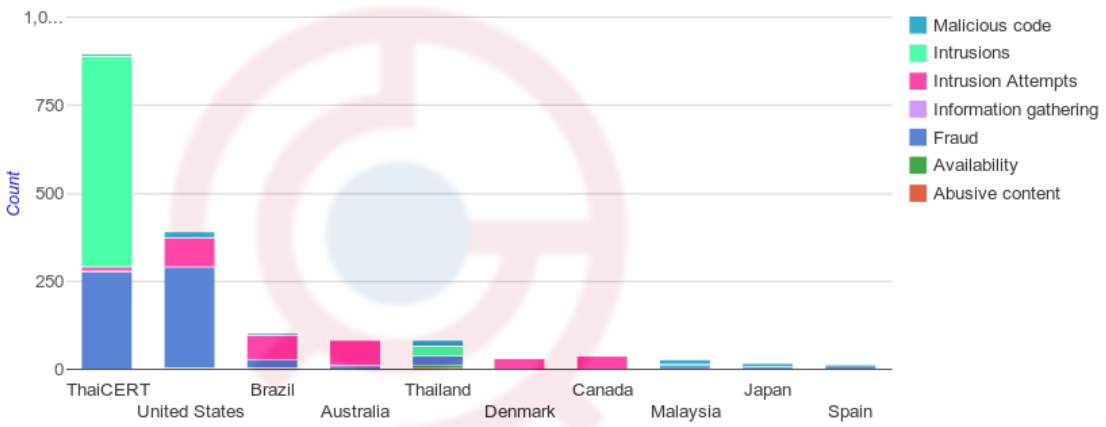


Figure 7: Top 10 incident reporters by country in 2013

Regarding the incident reporters classified by country, Figure 3 shows that most of the security incidents were reported by ThaiCERT security watch system with 895 cases or 51.28% of all reports, which were increased significantly from those of the previous year (43 cases) because in 2013, ThaiCERT decided to handle phishing and defacement incidents reported from automatic feed system. United States came in the second position with 392 cases, which were increased from those in 2011 (67 cases). Brazil, which was in the second position in 2011, came down to the third position with 102 cases, which were slightly decreased from those in the previous year (137 cases).

Reported Incidents Received from Automatic Feeds

With collaboration with our global security partners, ThaiCERT received information consisting of a global list of phishing URLs and a huge list of unauthorized activities originated from Thailand toward foreign hosts and misconfigured systems located in Thailand through their provided automatic feeds. ThaiCERT implemented the system to automatically collect, normalize and analyze any information, and then distributed these data through our own automatic feeds to other relevant Internet Service Providers (ISPs) tas part of our incident coordination service. An overview of the received information can be seen in the following figure.

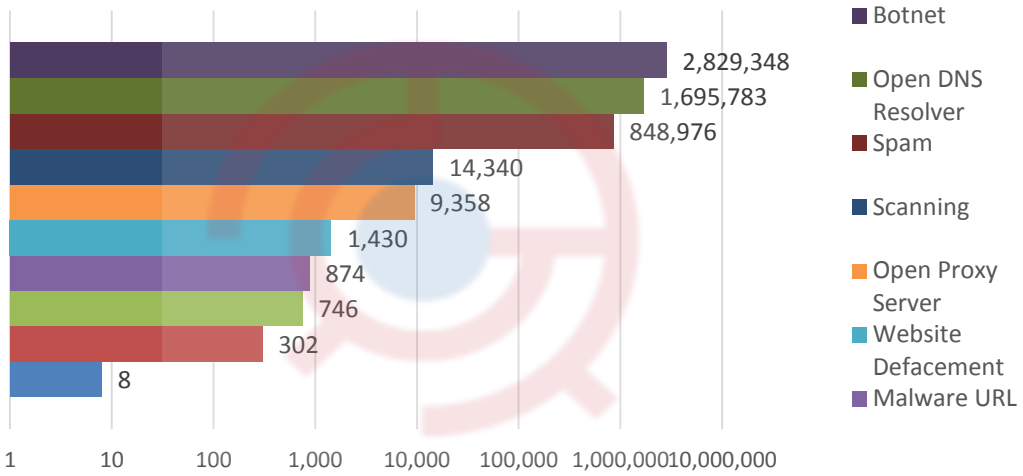


Figure 8: Top incident types by number of unique IPs in 2013

Figure 4 shows that there was a total of 5,401,165 unique IP addresses reported, which could be concluded that these were at least 5,401,165 unique IP addresses in Thailand having cybersecurity issues. It could clearly be seen that Botnet had the highest number of reported IP addresses with a total number of 2,829,348 or 52.38% of all reports, followed by open DNS resolver and spam with 1,695,783 and 848,976 IP addresses respectively. Whereas the number of reported IP addresses from other types of reports was less than 30,000 IP addresses.

Botnet, open DNS resolver and spam were also in top 3 in 2012, which means these types of threats are one of major concerns that need to be addressed in Thailand.

New Operation

Vulnerability Assessment

A single successful penetration by a malicious hacker can result in a compromise of an organization's confidentiality, integrity, and availability. Vulnerability assessment became one of ThaiCERT main operations for the purpose to prevent such a compromise for organizations. With regards to knowledge and skill development, our staffs hold international penetration testing certificates including GIAC penetration tester (GPEN) and GIAC Web Application Penetration Tester (GWAPT). In 2013, ThaiCERT had been provided vulnerability assessment and penetration testing service to 31 government agencies including web application and system testing.

Activities

Training

Co-organized:

- Certified Ethical Hacker training (co-organized with EC-Council), Bangkok, Thailand, August 2013
- Open Web and Application Security training (co-organized with OWASP), Bangkok, Thailand, July 2013

Participated:

- Mobile Forensics training, Dixie State College of Utah, Utah, United States of America, February 2013
- The Training Program on Enhancing Information Security for ASEAN, Japan, February 2013
- 2013 APISC Security Training Course, South Korea, July 2013

Etc:

- Invited to be a trainer of Incident Response training co-organized by JPCERT/CC and LaoCERT, Lao PDR, October 2013

Drill

Participated:

- APCERT Drill 2013 under the theme "Countering Large Scale Denial of Service Attack", January 2013
- ASEAN CERT Incident Drill (ACID) 2013, October 2013

Seminars

Participated:

- RSA Conference 2013, San Francisco, USA, February 2013
- APCERT AGM 2013, Brisbane, Australia, March 2013
- 47th APEC TEL, Bali, Indonesia, April 2013
- 4th ASEAN-Japan Information Security Workshop, Tokyo, Japan, August 2013
- 2nd ASEAN Network Security Action Council (ANSAC), Manado, Indonesia, August 2013
- 48th APEC TEL, Honolulu, United States of America, September 2013
- ASEAN Regional Forum (ARF) Workshop on Measures to Enhance Cyber Security - Legal and Cultural Aspects, Beijing, China, September 2013
- The 5th China Network Security Seminar, Chengdu, China, October 2013

Certifications

ThaiCERT staffs currently hold the following professional security certificates:

- (ISC)² CISSP
- GIAC GSEC
- GIAC GPEN
- GIAC GWAPT
- GIAC GCIA
- EC-Council Certified Ethical Hacker
- IRCA ISO/IEC 27001 ISMS Lead Auditor
- IACIS CFCE
- EnCase EnCE
- Access Data Mobile Examiner
- Access Data Certified Examiner
- CompTIA Security+

International Collaboration

MoU

Ministry of Internal Affairs and Communication of Japan

By signing MoU with Ministry of Internal Affairs and Communication of Japan for collaboration on project called PRACTICE (Proactive Response Against Cyber-Attacks Through International Collaborative Exchange Project), ThaiCERT was able to gain cyber attack trend forecast based on monitoring and analysis to protect users from malware infection and malicious activities in cyberspace proactively and reduce the damage.

Dixie State College of Utah's Southwest Regional Computer Crime Institute (SWRCCI)

After establish a partnership with Dixie State College of Utah's Southwest Regional Computer Crime Institute (SWRCCI) to exchange information, experience and knowledge with a goal to facilitate digital forensic competency development in organizations, ThaiCERT participated in mobile forensic training and seminar which were held by SWRCCI in February 2013.

The International Council of Electronic Commerce Consultants (EC-Council)

To develop cybersecurity capability in main government agency and critical infrastructure to prepare their IT security professionals for real-world attack and how to react when a breach occurs, ThaiCERT and EC-Council had collaboration and organized Certified Ethical Hacker training to their IT experts in August 2013. Furthermore, Computer Hacking Forensic Investigator (CHFI) training program was scheduled to be held in 2014.

Royal Thai Police

By signing MoU with Royal Thai Police, main police organization in Thailand, ThaiCERT had been closely working with digital forensic investigation unit of Royal Thai Police in order to develop common standard for digital forensic operation. The standard was used by various digital forensic agencies in Thailand.

Lao Computer Emergency Response Team (LaoCERT), Ministry of Posts and Telecommunications (MPT)

After signing MoU with LaoCERT, ThaiCERT and LaoCERT had been exchanged information and knowledge of IT Security. In October 2013, ThaiCERT, JPCERT and LaoCERT organized incident response training and experience sharing event held in Lao PDR.

SANS institute

In October 2013, SANS Institute and ThaiCERT announced the establishment of a partnership to facilitate Thailand's national cybersecurity competency development with a goal to defend and prevent compromise in Thailand's critical information infrastructure. Selection of potential candidates and the training was planned to be held in 2014.

22. 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:

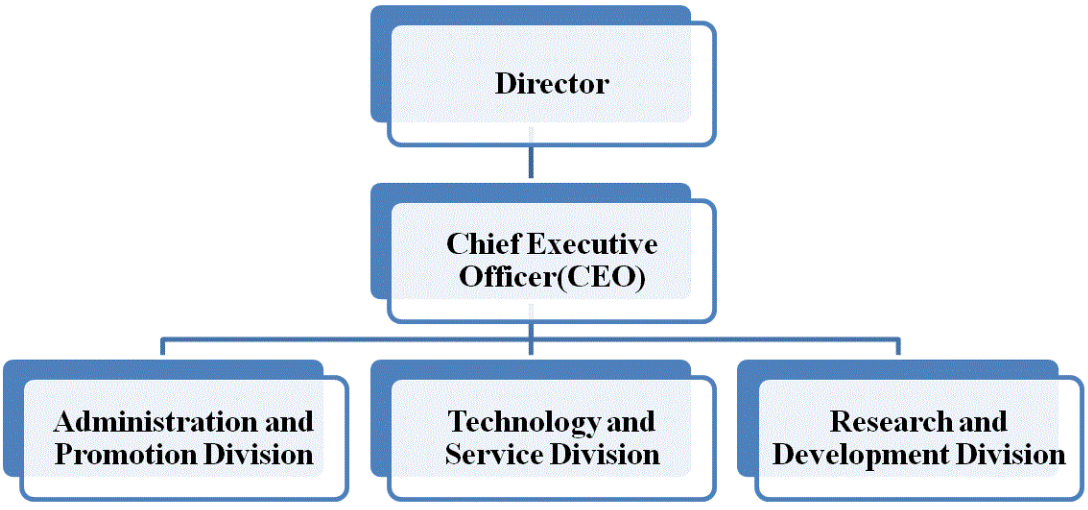
(1). To assist the handling of the intrusion incidents in the constituency, .tw domain.
(2). To announce the system vulnerability information.
(3). To provide security training and education on protection and defending technologies and skills.
(4). To assess periodically the national-wide security level 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



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	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013
Total	5318	2874	1824	788	660	1087	679	1094	6666	8,126	140,250

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.

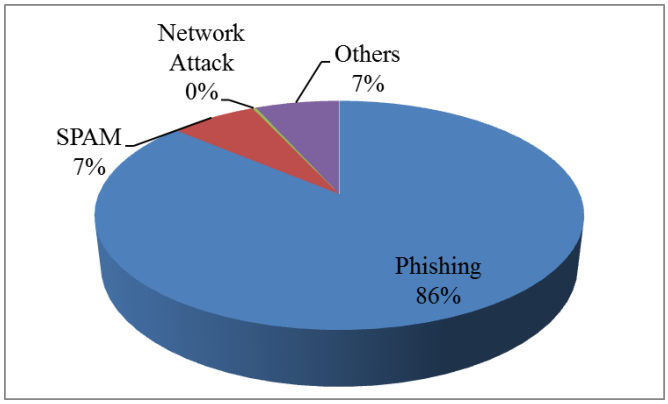


Figure 1 TWCERT/CC incident response classification statistics

■ **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	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013
Advisory	142	197	140	138	119	49	44	234	98	115	154

Table 2. TWCERT/CC advisory statistics

■ **Mailing List and Newsletter Service**

TWCERT/CC has collected and compiled security documentations and the advisories from various foreign hardware and software companies. The information has been evaluated and translated into the localized language, the staff dispatches to the Taiwan publicity to achieve the synchronicity of worldwide circulating information as soon as possible. In addition, the monthly TWCERT/CC Newsletters include special columns on the latest network security information and technologies that can raise the network security awareness in Taiwan.

■ **Information Security News Update**

TWCERT/CC researches, analyzes and develops technology and training aimed at helping administrators to secure their systems and networks. TWCERT/CC irregularly provides security related information, such as security tools, advisory, vulnerability remediation, technology documents, for the multitude and security-conscious users to enhance security education and consciousness.

■ **Localized Vulnerability Database**

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.

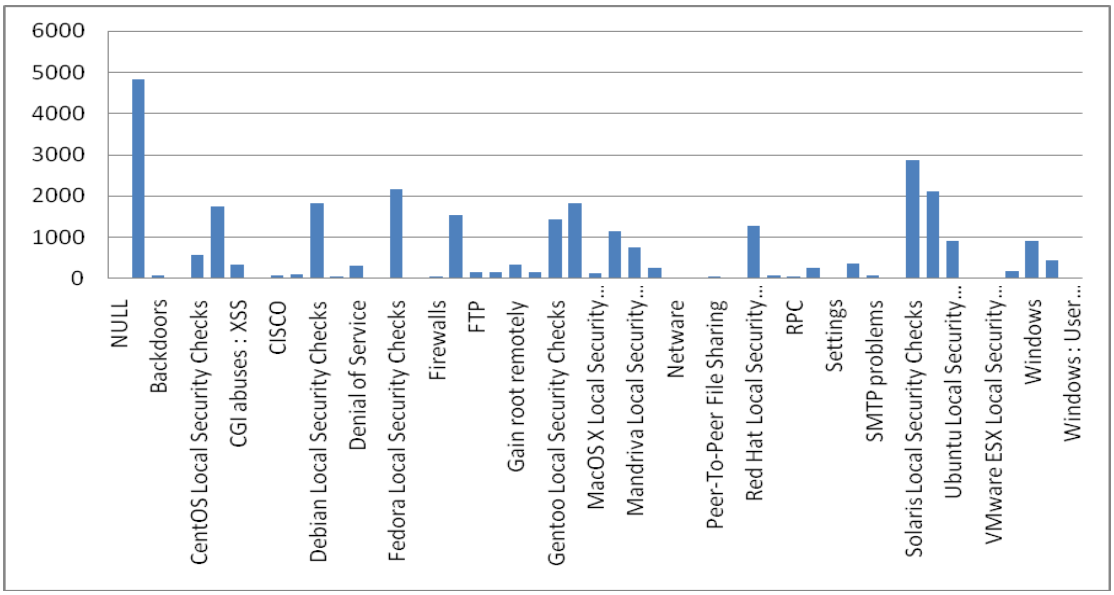


Figure 2. Categories of TWCERT/CC Vulnerability Database

- **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.

- **Member Services**

TWCERT/CC offers products, service and resources to help registered members find the best approach to security and continuously researching various aspects of computer security to benefit our members.

2.2 Abuse statistics

- **Spam analysis report**

TWCERT/CC handles and analyzes spam reported from online. Over five hundred millions of spam received in 2013 and originated from 93 countries. The geographic distribution of the spam sources is shown in Figure 3 and the amount of the spam over the year of 2013 in Figure 4.

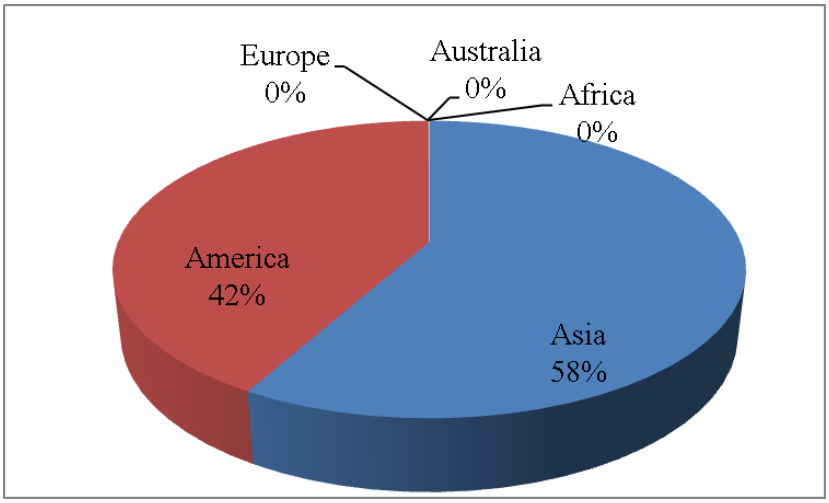


Figure 3 Geographic distribution of the spam sources.

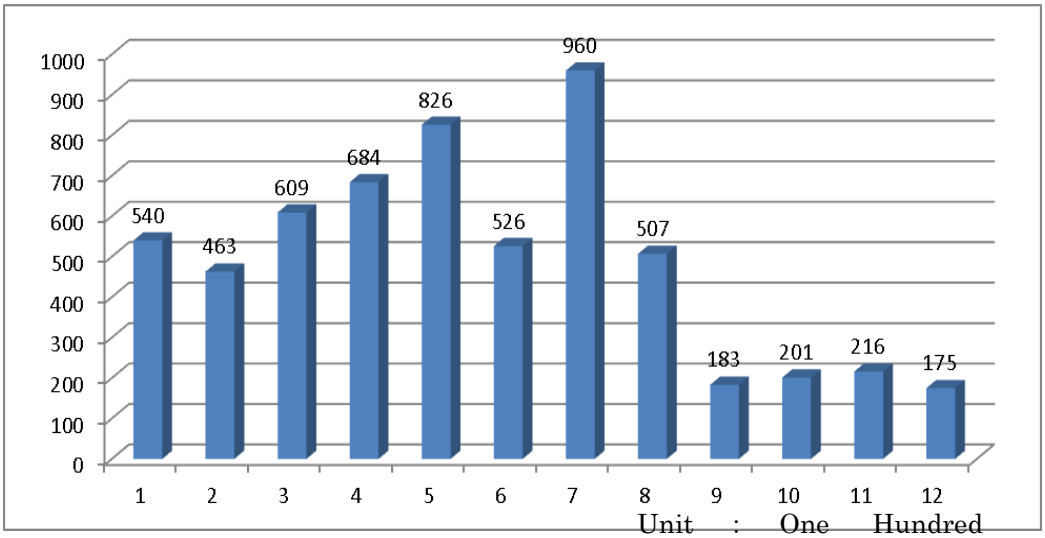


Figure 4 The amount of spam each month in 2013.

2.3 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 websiste 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 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
2013/12/12	Advanced Persistent Threat
2013/12/09	Information Security & Personal Data Protection
2013/11/09	Unix/Linux Security
2013/11/08	Penetration Testing
2013/10/09	DNSSEC
2013/09/09	Web Security and Penetration Testing
2013/08/16	The analysis of Malicious code and Digital Forensic
2013/08/12	Web Security and Penetration Testing
2013/07/09	Social Engineering

Table 3 list of TWCERT/CC workshops and training courses

3.2 Drill

TWCERT/CC supports TANet (Taiwan Academic Network) to operate an incident handling drill in the fourth quarter of 2013. Total of 4,069 educational institutions and over ten thousands of security officers were involved in this drill program with a high completion rate of 99.9%.

4. Achievements

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

safeguard to protect against the increasing intrusion and attack.

- **Enhance domestic network security**

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

- **Encourage and coordinate incident response**

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

- **Security promotion**

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

- **Security training**

  Recently frequent incidents encourage security awareness and professional demand. Personal training is the major work in technology development. TWCERT/CC offers many introductory and advanced training for executive, managers, educators, engineers, cyber administrators/operators and so on.

TWCERT/CC has trained many good talent of security field who are responsible for the security of information assets in different organizations. Hope to enhance domestic research and development capacity by mutual support and cooperation.

- **International relationship**

TWCERT/CC actively participates in international organizations and activities, and improves our capabilities and services. We have joined in FIRST, APCERT 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
- 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.

■ **Seoul-Melbourne Multilateral Memorandum of Understanding on Cooperation in SPAM Prevention**

E-mail becomes a major application with the population of computer and network,

however, the following spam abuse is getting more and more rampant. Spam not only wastes individual and enterprise cost, but also endangers information and network security. Enterprises and the government have to face and restrain the spam threat which is a global authorized problem. In addition to legislation and management, the most important is to set up a transnational and trans-organizational cooperation to effectively stop spam persecution.

Seoul-Melbourne Multilateral Memorandum of Understanding on Cooperation in Counting SPAM is an agreement signed by Australian Communications and Media Authority (ACMA) and Korea Information Security Agency (KISA) in 2003. Participates in Seoul-Melbourne MoU are part of a network of computer security incident response and security teams that work together voluntarily to deal with spam problem and prevention.

TWCERT/CC has been promoting the training of computer-network security response for years. Since 2005, TWCERT/CC has officially joined Seoul-Melbourne MoU member, and played the contact agent for sharing the experiences on dealing Taiwan's spam issues and exchange the anti-spam jurisdiction process with other members.

The key points of our missions are:

- To cope Taiwan's network security incidents with other nations, and take the part as a coordination center;
- To assist in handling the transnational spam problems;
- To exchange the related security intelligence with each member;
- To participate in international forums and meetings related to network security, and to uplift Taiwan's international image and position.

6. Future work and Conclusion

In order to improve the international involvement, TWCERT wishes to participate in transnational incident investigation and response assistance and to enhance Taiwan's visibility. As the personal privacy legislation is going to be effective soon, different sectors put more attention on security. Beside international coordination, horizontal collaboration on incident response is essential, too. Government

organized CIIP (Critical Information Infrastructure Protection) drill initiates collaboration among different agencies and organizations. The future work 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.
- Jointly developing measures to world-scale network security incidents and know well the international security tendency and development to advance global internet environment.
- Train the awareness and capability in information security and risk management through information sharing and international cooperation.

23. TWNCERT

Taiwan National Computer Emergency Response Team – Chinese Taipei

1. About TWNCERT

TWNCERT (Taiwan National CERT) was built in 2001. TWNCERT is intended for improving incident response and information security awareness and sharing in Taiwan. 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.
- Providing an 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 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.

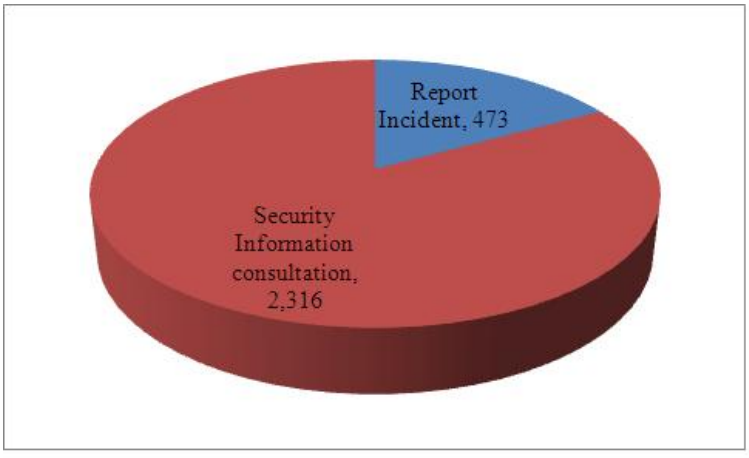
- Risk analysis: Undertaking risk assessment.

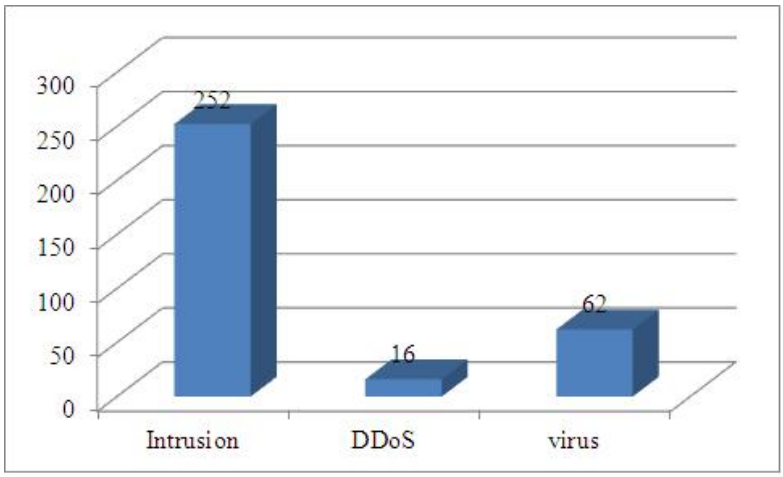
- Collaboration: Building collaborative relationship with legal community, information security business and ISP.

- Coordination: Building coordination and communication channels with domestic and foreign incident response organizations.

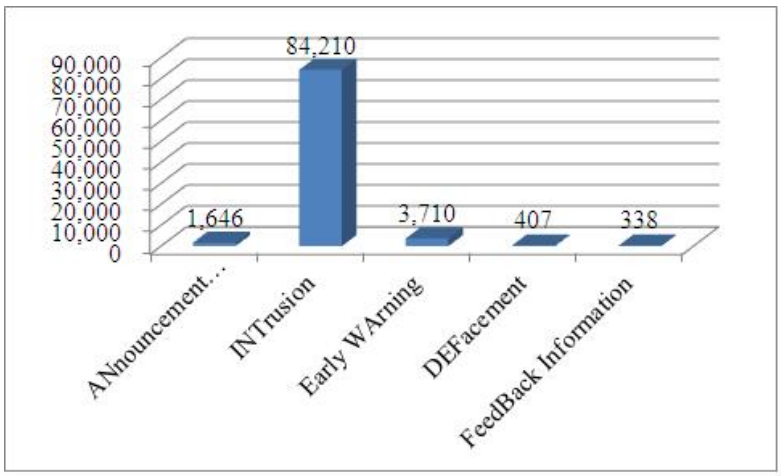
2. Operations & Activities

- In 2013, TWNCERT received 473 reports on computer information security incidents from Taiwan government sectors. The top 3 incident categories are Intrusion, DDoS and Virus. TWNCERT also had offered 2,316 information security consulting services in 2013.



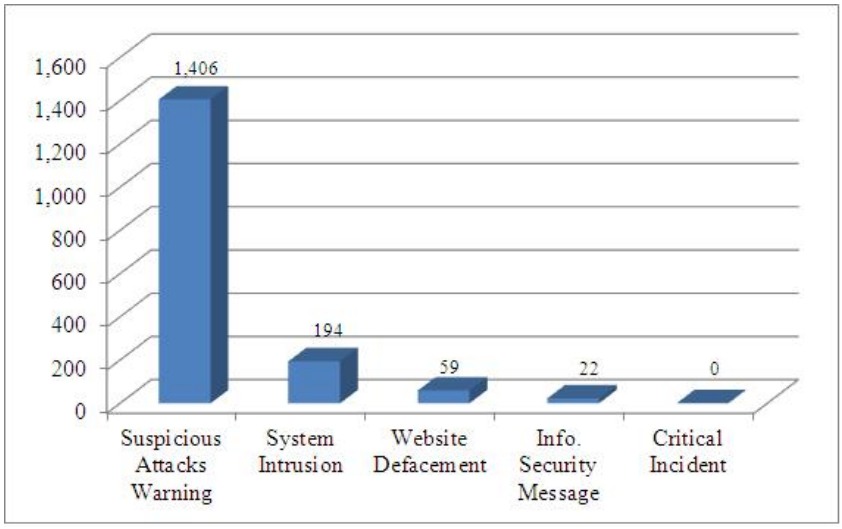


- TWNCERT started operating the government ISAC since 2009, called G-ISAC (Government Information Sharing and Analysis Center). TWNCERT began not only deal with government sectors information security relevant, but also sharing security information with Academic ISAC (A-ISAC), National Communications Commission ISAC (NCC-ISAC), which includes most major ISPs in Taiwan. In addition, major SOCs, 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. Currently, G-ISAC has covered over 99.001% IPs in Taiwan, and has shared thousands of security incident and critical information each year. G-ISAC members shared a total of 90,311 security information in 2013.



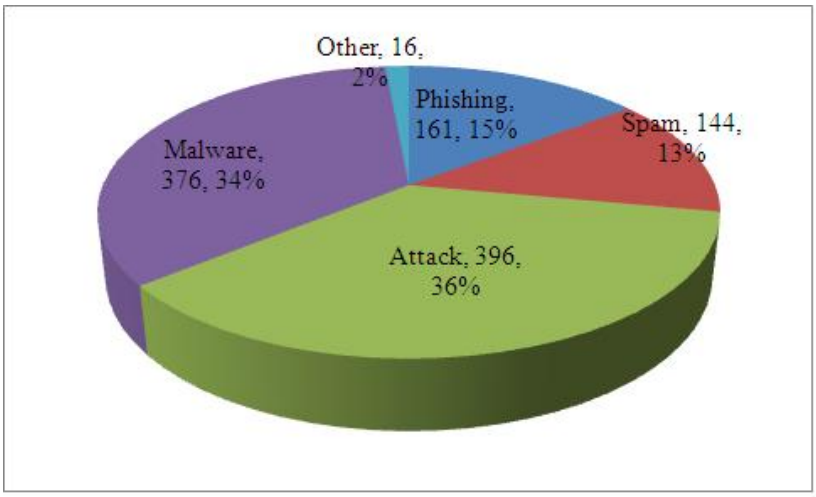
- In 2013, TWNCERT published 1,681 advisories to government sectors:

  - Suspicious Attacks Warning: 1,406
  - System Intrusion: 194
  - Website Defacement: 59
  - Info. Security Message: 22
  - Critical Incident: 0



3. International Collaboration

- In 2013, TWNCERT received more than 1,093 international information security incident reports, provided assistance and cooperation to other CSIRTs and governments. Chart below is the classification of the incident reports:



- TWNCERT has reported Botnet Information to 18 countries, including Australia, Belgium, Brazil, China, France, Germany, Indonesia, India, Japan, Malaysia, Netherlands, Philippines, USA, Russia, Spain, Singapore, South Korea and Thailand.

- Attended 25th Annual FIRST Conference in June 2013
- Attended Blackhat USA in July 2013
- Attended APEC TEL 48 in September 2013
- Attended the 13th RAISE in November 2013
- Attended AVAR 2013 in December 2013
- Signed MOU with Team Cymru for CSIRT Assistance Program in October 2013

24. VNCERT

Vietnam Computer Emergency Response Team - Vietnam

1. About VNCERT

1.1 Introduction

1.1.1. Establishment

VNCERT is belong 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.

Roles of VNCERT:

- Coordinating national computer incident response activities.
- Watching and warning computer network security problems.
- Building and coordinating to build computer network security technical standard.
- Promoting to build CERTs in the organizations, enterprises, and agencies in Vietnam.
- VNCERT is the point of contact of Vietnam with the oversea CERTs in this area.
- Support Ministry of Information and Communications with activities in state management about Information Security.
- Implementing and Deploying the Anti-spam activities.

1.1.2. Workforce power

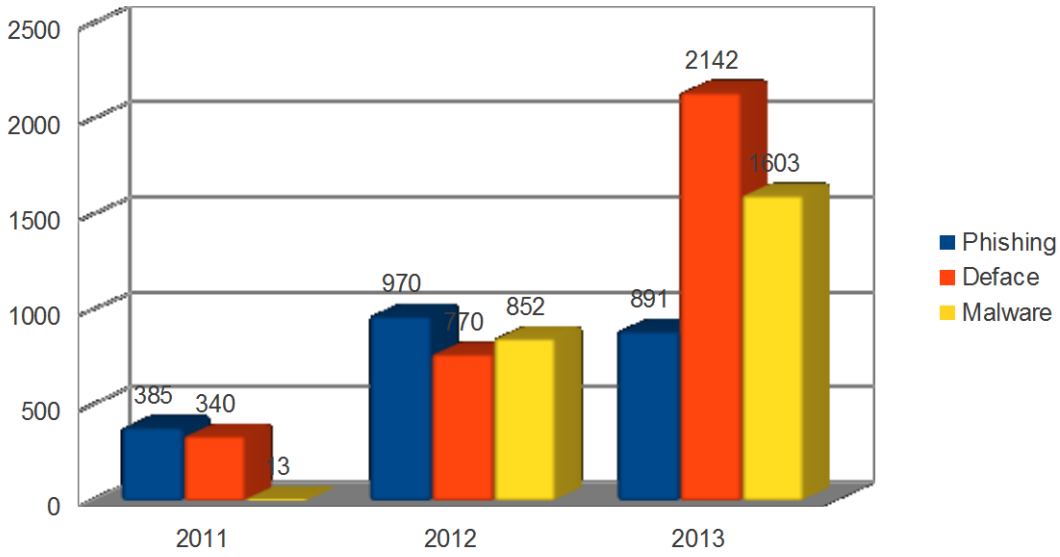
VNCERT has four specialized divisions: Division of Operation, Division of System technique, Division of Training & Consultancy and Division of Research and Development. VNCERT also has two branches, one in Ho Chi Minh City and another in Danang City.

Current number of employees in VNCERT is 60.

2. Activities & Operations

2.1 Incident handling reports

On 2013, VNCERT processed 4636 information security incidents (including 2469 phishings, 1603 Malwares, 2142 Defaces).



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

2.2 Abuse statistics

Security Incidents	2009	2010	2011	2012	2013
Phishing	136	233	385	970	2469
Deface	35	19	340	770	1603
Malware	10	8	13	852	2142
Other	25	11	17	----	165
Total	**206**	**271**	**757**	**2179**	**4810**

2.3 Incident Coordinating, warning and supporting activities

Supported 82 government agencies and organizasions to pen test and audit information security.

Removed botnet malwares from thousands of computers in government agencies.

Participated the Microsoft removing botnet operations focused on Conficker, Sality,

Traficonverter and Downadup, etc.

Supported USCERT and US Banks to remove malicious code on 2322 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.

2.4 Anti-spam activities

Coordinated mobile operators and SMS content providers to process 157 incidents in SMS Spam.

Participated in inspection activities at 27 content providers of SMS spam activities and content provider services.

2.5 Legal Framework Update on Information Security

Decree No. 72/2013/ND-CP dated July 15, 2013 of the Government on management, provision and use of Internet services and online information.

Decree No. 77/2012/ND-CP dated October 05, 2012 of the Government on amendment and supplement for the Government's Decree No. 90/2008/ND-CP dated August 13, 2008 on anti-spams.

Decree No. 197/2013/ND-CP dated November 13, 2013, of the Government on sanctioning of administrative violations in the field of telecommunication, post, radio frequency and Information Technology.

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 for the Decree 77/2012/ND-CP on Amendment and Supplement for the Decree 90/2008/ND-CP on Anti spam, that will be released on second quarter of 2014.

3. Events organized / Co-organized

3.1 Training

Organized training a course about information security (LPI-Linux Professional Institute) for 15 employees.

Organized training courses and sharing experience about CERT activities and Incident Response for LaoCERT.

Organized training information security courses for government agencies.

Cooperate with VNISA to organize the Information Security Contest for students on universities.

3.2 Seminars & Etc

Cooperate with Ministry of Public Security and IDG Vietnam Corporation to organize annual event "Security World 2013".

Cooperate with VNISA to organize the annual event “National Information Security Day 2013”.

Organized the conference about Coordinate and Incident Response of CSIRT network in Vietnam.

4. International Collaboration

4.1 Incident Drill

Participate in 03 international drills: APCERT Annual Drill 2013, ASEAN-JAPAN Drill and ASEAN CERTs Incident Drill (ACID 2013).

Organized the VNCSIRT Drills for 80 government agencies with participating of ISPs and information security companies.

4.2 MoU

No MoU signed in 2013.

4.3 Presentation

In 2013, VNCERT presented at and/or participated in 19 international conferences and forums.

5 Future Plans

Finish the drafting of Information Security Law and submit to the National Assembly at the end of 2014.

Deploy the incident monitoring project for incident in VietNam.

Organize the VNCSIRT Drill 2014.

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.