APCERT Annual Report 2012

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

APCERT
Asia Pacific Computer Emergency Response Team

CONTENTS

Chair's Message 2012

The history of CERTs began in 1989 as a result of the Morris worm. As Internet expanded globally, CERTs began to form within the Asia Pacific region and quickly it became clear that collaboration to address challenges that went beyond individual national borders would become essential. Technical coordination was needed to help keep the growing global network running and free from malicious activity. APCERT was originally formed in 2003 with 15 teams from 12 economies with a vision that by working together the people and the nations in the region would benefit from sharing information and skills in building a more useable cyberspace.

After 10 years since its formation, APCERT is now comprised of 30 teams from 20 economies, geographically covering the region served by APNIC. Increasingly we have become one big team working together, responding to incidents, exercising our ability to collaborate and building the capabilities of the member teams to provide a Cleaner, Safer and Reliable cyberspace. We have reached out to partners around the world in participating in dialogues and establishing coordination to improve Internet security.

Over the last 10 years, challenges have continued to mount as well – more, faster spreading malware, bigger botnets and more competition and national security involvement by governments. Today more technology waves have emerged – mobile, social media, cloud. We face more sophisticated threats – APT, Stuxnet and DDOS against many APCERT member economies, especially their financial sectors. Governments are engaging in cyber war/conflict discussions, taking sides on who is conducting attacks and creating risks. States view cyberspace seen as competitive environment. This situation challenges APCERT with the possible break down in trust within CERT/technical community if member teams are seen as instruments of government national security competition. However, we have successfully bonded ourselves by focusing our role building the regional level of cyber risk reduction.

APCERT sees the opportunity to collaborate on cyberspace safety, cleanliness and health – clean up malware and cooperate in removing botnets, focus on measurement and enabling remediation through education, tools and information sharing. I strongly believe APCERT efforts should go further in this area.

APCERT's continued success as a collaborative team will come from staying focused on improving condition of the infrastructure and making cyberspace better for all people and nations. We will continue to lead in establishing global collaboration and bringing the message to the rest of the world in pursing the vision of a clean, safe and reliable Internet. We must assist all stakeholders in a focus on collaborative clean up to reducing cyber risks and avoid being bogged down in competition between government.

I am proud to serve as your Chair and hope to help enable the excellent teams and people that make up APCERT in continuing to make the globe's cyberspace a better place.

Yurie Ito
Chair, APCERT
Director, Global Coordination Division, 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 organization was established in February 2003 with the objective of encouraging and supporting the activities of CERTs/CSIRTs in the region.

APCERT maintains a trusted network of cyber security experts in the Asia Pacific region to improve the region's awareness of malicious cyber activity and its collective ability to detect, prevent and mitigate such activity through:

1. enhancing the Asia Pacific's regional and international cooperation on cyber security;
2. jointly developing measures to mitigate large-scale or regional network security incidents;
3. facilitating information sharing and technology exchange on cyber security and threats among its members;
4. promoting collaborative research and development on subjects of interest to its members;
5. assisting other CERTs and CSIRTs in the region to conduct efficient and effective computer emergency response; and
6. providing inputs and/or recommendations to help address legal issues related to cyber security and incident response across regional boundaries.

The formation of CERTs/CSIRTs at the organizational, 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 organizations, such as the Forum of Incident Response and Security Teams (FIRST – *www.first.org*), the Trans-European Research and Education Networking Association (TERENA)

task force (TF-CSIRT – *www.terena.nl/tech/task-forces/tf-csirt/*), a task force that promotes collaboration and coordination between CSIRTs in Europe, and the Organisation of the Islamic Cooperation – Computer Emergency Response Team (OIC-CERT – www.oic-cert.net), a collaboration of information security organizations among the OIC member countries.

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

In March 2012, 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. JPCERT/CC continued to serve as the APCERT secretariat.

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 2012, **Taiwan E-Commerce Computer Emergency Response Team (EC-CERT)** of Chinese Taipei and **New Zealand National Cyber Security Centre (NCSC)** of New Zealand were approved as General Members. Furthermore, **CERT Australia** of Australia and **TechCERT** of Sri Lanka were approved as Full Members.
As of December 2012, APCERT consists of 30 teams from 20 economies across the Asia Pacific region, of which 21 teams are Full Members and 9 teams are General Members.

Full Members (21 Teams)

Team	Official Team Name	Economy
AusCERT	Australian Computer Emergency Response Team	Australia
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
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
MyCERT	Malaysian Computer Emergency Response Team	Malaysia
PHCERT	Philippine Computer Emergency Response Team	Philippine
SingCERT	Singapore Computer Emergency Response Team	Singapore
Sri Lanka CERT|CC	Sri Lanka Computer Emergency Readiness Team Coordination Centre	Sri Lanka
ThaiCERT	Thailand Computer Emergency Response Team	Thailand
TechCERT	TechCERT	Sri Lanka
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

General Members (9 Teams)

Team	Official Team Name	Economy
BDCERT	Bangladesh Computer Emergency Response Team	Bangladesh
BP DSIRT	BP Digital Security Incident Response Team	Singapore
EC-CERT	Taiwan E-Commerce Computer Emergency Response Team	Chinese Taipei
GCSIRT	Government Computer Security and Incident Response Team	Philippines
mmCERT	Myanmar Computer Emergency Response Team	Myanmar

MOCERT	Macau Computer Emergency Response Team Coordination Centre	Macao
MonCIRT	Mongolian Cyber Incident Response Team	Mongolia
NCSC	New Zealand National Cyber Security Centre	New Zealand
NUSCERT	National University of Singapore Computer Emergency Response Team	Singapore

3. Steering Committee (SC)

The following teams were elected to the APCERT Steering Committee (SC) at the APCERT Annual General Meeting (AGM) held in March 2012, in Bali, Indonesia.

- AusCERT
- CERT Australia
- CNCERT/CC
- ID-SIRTII/CC
- JPCERT/CC (Chair/Secretariat)
- KrCERT/CC (Deputy Chair)
- MyCERT

4. Working Groups (WG)

There are currently five (5) Working Groups (WG) in APCERT.

1) 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 Visualization features to the common platform.
- Secretariat: JPCERT/CC
- Members: TSUBAME project members
- Status: Active; TSUBAME Workshop held in March 2012

2) Information Classification WG (formed in 2011)

- Objective:
  - To devise an appropriate information classification and handling system to be adopted for use by APCERT Teamsfor communicating or sharing information.
- Convener: Kathryn Kerr (AusCERT)
- Status: Active.

3) Information Sharing WG (formed in 2011)

- Objective:
  - To identify different types of information that is regarded as useful for APCERT Teams to share with each other.
- Convener: Yonglin Zhou (CNCERT/CC)
- S t a t u s : Active.

4) 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 the new membership should be structured.
- Convener: Jinhyun Cho (KrCERT/CC)
- S t a t u s : Active.

5) Operational Framework WG (formed in 2011)

- Objective:
  - To identify the changes that need to be made to the existing APCERT Operational Framework
- Convener: Roy Ko (HKCERT)
- S t a t u s : Active.

5. APCERT Website

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

II. APCERT Activity Report 2012

1. International Activities and Engagements

APCERT has been active in representing and promoting APCERT in various international forums and activities. From January to December 2012, APCERT Teams have hosted, participated and/or contributed in the following events:

- **APCERT Drill 2012 (14 February 2012)**

  http://apcert.jpcert.or.jp/documents/pdf/APCERTDrill2012PressRelease_AP.pdf

  APCERT Drill 2012, the 8th APCERT Cyber Exercise Drill, was successfully conducted to test the response capabilities of the participating APCERT Teams. Following the signing of a Memorandum of Understanding on collaboration between APCERT and the Organisation of the Islamic Cooperation – Computer Emergency Response Team (OIC-CERT) in September 2011, for the first time APCERT invited the participation from Teams of the OIC-CERT. 22 teams from 17 economies of APCERT (Australia, Bangladesh, Brunei Darussalam, People's Republic of China, Chinese Taipei, Hong Kong, India, Indonesia, Japan, Korea, Macao, Malaysia, Myanmar, Singapore, Sri Lanka, Thailand and Vietnam) and 3 teams from 3 economies of OIC-CERT (Tunisia, Egypt and Pakistan) participated in the Drill. The theme of the drill was "Advance Persistent Threats and Global Coordination."

- **APCERT Annual General Meeting (AGM) & Conference 2012 (25-28 March 2012, Bali, Indonesia)**

  http://apcert2012.idsirtii.or.id/apcert-2012/

  The APCERT Annual General Meeting (AGM) & Conference 2012 was held from 25-28 March 2012 at Padma Hotel Bali, Bali, Indonesia, hosted by ID-SIRTII/CC. The event brought APCERT Teams together, as well as other CERTs/CSIRTs in the Asia Pacific region, as well as closely related organizations, invited guests and speakers.

  Program Overview:

25 March (Sun)	AM:	APCERT Steering Committee Meeting, APCERT Working Group Meetings TSUBAME Workshop

		(Closed to APCERT members)
	PM:	Pre-Annual General Meeting
		(Closed to APCERT members)
26 March (Mon)	AM:	APCERT Annual General Meeting
		(Closed to APCERT members)
	PM:	APCERT Closed Conference
		(Closed to APCERT members and invited guests)
27 March (Tue)	All day:	APCERT Open Conference *(Open to public)*
28 March (Wed)	All day:	The Amazing Trace *(Closed by invitation)*

The event delivered productive discussions on developing strategic planning for APCERT operations. In pursuit of APCERT's vision stating "APCERT will work to help create a Safe, Clean and Reliable cyber space in the Asia Pacific region through global collaboration" (approved at APCERT AGM & Conference 2011), the program included panel discussions on clean-up efforts of local networks, as well as effective global collaboration on Internet clean-up, involving teams from within and outside the region. The annual event also provided opportunities to share information security trends and best practices among various CERTs/CSIRTs.

- **TSUBAME Workshop 2012 (25 March 2012, Bali, Indonesia)**

  The APCERT TSUBAME Workshop 2012 on Network Traffic Monitoring Project was held on 25 March 2012, in conjunction with APCERT AGM & Conference 2012. The workshop was organized by JPCERT/CC to enhance the TSUBAME project and the cooperation among its members.

- **APEC TEL 45 (5-11 April 2012, Da Nang, Vietnam)**

  APCERT Teams participated in APEC TEL 45 SPSG (Security and Prosperity Steering Group) and co-hosted a "CSIRT Workshop," and presented on APCERT activities. APCERT also had its status as an APEC TEL guest renewed for a further three years and will continue to provide advice and expertise to SPSG as the security expert community in the Asia Pacific region.

- **NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) (12-16 April 2012, Vienna, Austria)**

  APCERT Chair, Ms. Yurie Ito (JPCERT/CC), participated in the event and presented on APCERT activities, as well as security trends in the Asia Pacific

region.

- **OECD Working Party on Information Security and Privacy (WPISP) Meeting (9-10 May 2012, Paris, France)**

  APCERT Chair, Ms. Yurie Ito (JPCERT/CC), participated in the event and discussed the possibility of future collaborative activities with OECD.

- **24th Annual FIRST Conference Malta (17-22 June 2012)**

  http://conference.first.org/2012/

  APCERT Teams attended the Annual FIRST Conference and shared valuable experience and expertise through various presentations, as well as holding an APCERT meeting.

- **National CSIRT Meeting (23-24 June 2012, Malta)**

  APCERT Teams attended the National CSIRT Meeting, hosted by CERT/CC, and exchanged various activity updates as well as recent projects and research studies. JPCERT/CC, as the APCERT Chair and Secretariat, also presented on recent APCERT activities.

- **AP*Retreat Meeting (17 July 2012, Tokyo, Japan)**

  http://www.apstar.org/ap_retreat.php

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

  JPCERT/CC, as the APCERT Secretariat, attended the AP*Retreat Meeting (held twice a year) and presented an update on APCERT activities.

- **APEC TEL 46 (30 July - 4 August 2012, St. Petersburg, Russia)**

  APCERT Chair, Ms. Yurie Ito (JPCERT/CC), participated in APEC TEL 46 SPSG (Security and Prosperity Steering Group) via video conference, and presented on recent APCERT activities.

- **ASEAN Regional Forum "Cyber Incident Response Workshop" (6 - 7 September 2012, Singapore)**

  A "Cyber Incident Response Workshop" was organized by SingCERT and CERT Australia with the aim to discuss large-scale, cross-border incidents impacting

the ASEAN region. The Workshop was attended by various sectors including CERTs/CSIRTs, law enforcements and government agencies. APCERT was recognized as an effective community within the existing information sharing frameworks.

- **ACID (ASEAN CERT Incident Drill) 2012 (12 September 2012)**

  ACID 2012, led and coordinated by SingCERT, entered its seventh iteration with participation from ASEAN CERTs and APCERT Teams. The drill was completed successfully with the focus on investigating and responding to android malware targeting online banking applications.

- **The 3rd APT Cybersecurity Forum (25 - 27 September 2012, Macao, China)**

  http://www.apt.int/2012-CSF3

  The 3rd APT Cybersecurity Forum was organized by the Asia Pacific Telecommunity and hosted by the Bureau of Telecommunications Regulation (DSRT) of Macao, Special Administrative Region, People's Republic of China.
  Mr. Geoffroy Thonon (MOCERT) represented APCERT at this forum and presented on APCERT activities to relevant participants.

- **CSIRT Trainings for Africa**

  JPCERT/CC organized training for CERTs/CSIRTs in Africa and introduced APCERT activities during the training on behalf of APCERT.
  - 7 - 12 May 2012, Gambia
  - 25 - 27 November 2012, Sudan

- **Memorandum of Understanding (MOU) between APCERT and the STOP. THINK. CONNECT. Messaging Convention**

  http://www.apcert.org/documents/pdf/Joint-media-release-STC-APCERT.pdf

  APCERT and the STOP. THINK. CONNECT. Messaging Convention joined forces to propagate the global STOP. THINK. CONNECT. online safety awareness campaign to the 20 economies represented by APCERT's membership.

Other International Activities and Engagements

- **DotAsia**

  APCERT serves as a member of the Advisory Council of DotAsia, to assist DotAsia 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 (JPCERT/CC) serves as a Steering Committee member of FIRST from June 2011.

2. Approval of New General Members / Full Members

From January to December 2012, the following teams were approved as APCERT General Members / Full Members.

- CERT Australia (Australia) was approved as Full Member as of 14 March
- TechCERT (Sri Lanka) was approved as Full Member as of 14 March
- NCSC (New Zealand) was approved as General Member as of 14 March
- EC-CERT (Chinese Taipei) was approved as General Member as of 16 August

3. APCERT SC Meetings

From January to December 2012, SC members held seven (7) teleconferences and one (1) face-to-face meeting to discuss on APCERT operations and activities.

31 January	Teleconference
22 February	Teleconference
14 March	Teleconference
25 March	Face-to-face meeting at APCERT AGM & Conference 2012, Bali
23 May	Teleconference
16 August	Teleconference
2 October	Teleconference
4 December	Teleconference

4. APCERT Study Calls

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

Date: 11th July 2012

Topic: "Reversing Malicious Flash"

Speaker: Mr. Mahmud Abdul Rahman

Organized by: MyCERT, CyberSecurity Malaysia

5. APCERT Information Classification Policy

On 15 October 2012, APCERT published its Information Classification Policy, based on the Traffic Light Protocol (TLP) used widely by the international CERT/CSIRT community. The project was led by the APCERT Information Classification Working Group (Convenor: AusCERT).

The policy was developed for APCERT members to:

build trust and confidence that sensitive information will be handled appropriately by APCERT members by allowing APCERT recipients to better understand the sensitivity and/or restrictions which may apply to some types of information; and through increased trust and confidence, enable more effective and useful communication and assistance to occur between APCERT teams.

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

Full Members

1. AusCERT Activity Report

Australian Computer Emergency Response Team – Australia

About AusCERT

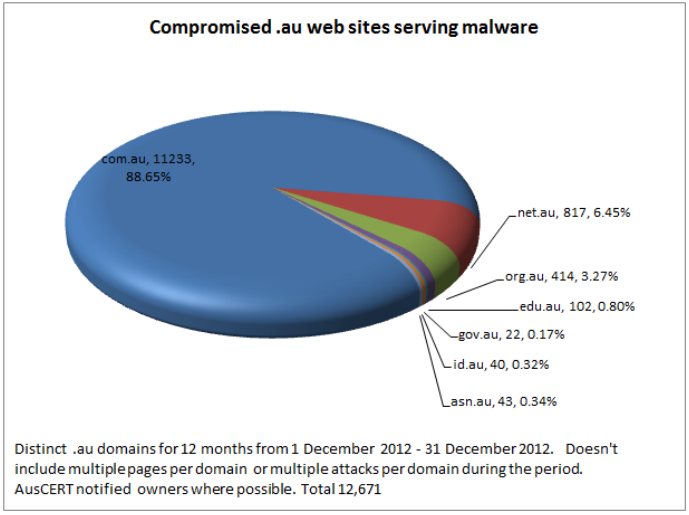
AusCERT is the premier Computer Emergency Response Team (CERT) established in Australia in 1993 and a leading CERT in the Asia/Pacific region. AusCERT operates within a worldwide network of information security experts to provide computer incident prevention, response and mitigation strategies for members and assistance to affected parties in Australia. 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 a member of FIRST.

Security advisories and bulletins

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

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.



Compromise evidence collection and data distribution

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

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.

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 Sydney and Melbourne.

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. BKIS Activity Report

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

Internet security in enterprises and agencies has not been improved
According to statistics by Bkis, in 2012, there were about 2,203 websites of enterprises and agencies attacked in Vietnam, mainly through vulnerabilities in network system. Comparing to 2011 (about 2,245 websites attacked), the number almost does not decrease.

This shows that Internet security has got enough concern in enterprises and agencies. According to Bkis experts, most Vietnamese enterprises haven't been able to assign staffs specializing in Internet security, while ability of such personnel, if yes, does not meet the reality's requirements. These are the main reasons.

Spyware – New strategy of cybercriminals
In 2012, attacking, spreading spyware in enterprises and agencies is a new kind of national cybercriminals. Last year, the world was impinged by Flame and Duqu, the viruses which steal confidential information from the computing system in the Middle East. Bkis experts state, similar cases are beginning in Vietnam.

You may be surprised at the above information, however in Vietnam, Bkis honeypot system detected a series of emails sent to agencies, enterprises that

were attached with document files containing spyware. Because document files have always been considered as safe ones, most receivers did open the attachments and got infected with spyware exploiting holes on Microsoft Office (including Word, Excel and PowerPoint). Upon infection, the viruses silently control the victim computers, open backdoor to let the hackers remotely control the victims. They also get commands from the hackers to download other viruses onto the computers to log keystrokes, print screen, steal data.

One again, the case raises the alarm about Internet security in enterprises and agencies in Vietnam, especially in the context of a potential cyber-war in the world.

Virus on mobile phone is no longer a theory

In the previous years, virus on mobile phone was only at the starting point, mainly under trail. In 2012, they become the real threat to users. Bkis honeypot system detected 34,094 virus samples spreading on mobile phones, 9 times greater than that of 2011 (3,700 samples).

Bkis researches show that, in order to spread, mobile phone viruses use similar method with their peers on computers. Taking advantage of the need for smartphone famous softwares, hackers created bogus softwares with malicious code, then pushed them onto unofficial application markets on the Internet, cheated users to download. From April 2012, consecutive softwares such as Instagram or Angry Bird were faked by virus to target users.

The trend of faking softwares to inject virus will continue in the next years, when each day there are thousands of smart phone applications updated on the Internet.

Facebook - fertile environment for hackers

The number of Facebook users explored, following was change in computer viruses' target. Instead of aiming Yahoo! Messenger as before, malware moved to take advantage the social networks to infect users' computers.

One of virus spreading methods that trap most Facebook users is currently creating fake YouTube plugin containing viruses. Then, bad guys cheat users to download the plugin to view the video clip, but the fact is downloading virus to

spread malicious links to the victim's friends. The clips often contain sexual pictures of famous singers, actors, or footballers such as Rihanna, Emma Watson, Ronaldo…to attract users.

Subjectiveness is the reason why many users are cheated by bad guys to download virus onto their computers. Users' awareness when joining social networks on the Internet is an alarming issue in 2012.

Smartphone security became hot issue by the end of year

In the panorama of cyber security in 2012, mobile phone security emerged with many fluctuations at the end of year. It is easy to understand because smartphone is replacing old-fashioned phones with the increasing rate of 47% (according to the Gartner's newest statistics of the world's mobile phone in 3rd quarter of 2012).

The rapid increasing of smartphone is followed by the risk of losing information security on mobile devices which are replacing computers. Risks such as: wiretapping, cheating by SMS on iPhone, cheating for cost of telecommunications and so on causes damages and fear for users. In 2012, Bkis spam statistic system reported that, each day, there were about 9.8 millions of SMS spam in Vietnam and network providers earned about 3 billion Vietnamese dong from SMS spam.

Most threatening are the mobile eavesdropping softwares widely sold on the Internet. The softwares permit bad guys to take control of in-coming and out-coming calls and other important data such as: calling logs, message content, victim's location. This means that personal life of user will be violated.

By the end of December, Bkis provided the solution that prevented wiretapping on mobile. The solution is integrated on Bkis Mobile Security software, and gave strong warning: Mobile phone is important device, and user should not permit others, even acquaintances, use it.

2.2 Threat landscape in 2013 in Vietnam

Spy activities via spreading virus will become an "industry" in 2013. Most users think that document files (Word, Excel, PowerPoint) are safe and have no virus. It is not easy to change the mind in the near future, and this is an "ideal" condition for cybercriminals to develop spy network.

The methods of spreading malicious code which used to be seen on computer environment only will explode on smartphone in 2013. Famous softwares, security softwares for smartphone will be the main targets for faking. The increasing need of installing security software for smartphone is good bait for cybercriminals.

3. Events organized / co-organized

3.1 Training Courses

Network Security Training Courses:

July 2012, Dec 2012: For Network Administrators from companies and banks

Security Awareness Training Courses:

November 2012: 2 classes for VSD: Vietnam Securities Depository

3.2 Security Articles

In 2012, Bkis sent Vietnamese press 12 researches on the Internet security.

3.3 Seminar

May 2012: Organized a seminar about security for banking system.

March 2013: Organized a seminar on spyware in Security World 2013 conference in Vietnam.

4. International Collaboration

February 2013: Bkis took part in the APCERT Drill as a member of the organizing committee and a member of the exercise control group

3. BruCERT Activity Report

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 provides 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)* welcomes 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

2. BruCERT Operation in 2012

2.1 Incidents response

In 2012, BruCERT receives quite a high numbers of security incidents reports from both the public and the private sector. There were an increasing number of incidents that had been reported to BruCERT, which show positive feedbacks from the Brunei community. On the down side, there is also an increase number of website that had been defaced in Brunei. Most of the defacement are due to lack of security controls being placed and install security patches on the victims' sides. The statistic of the security incident is shown as Figure 1.

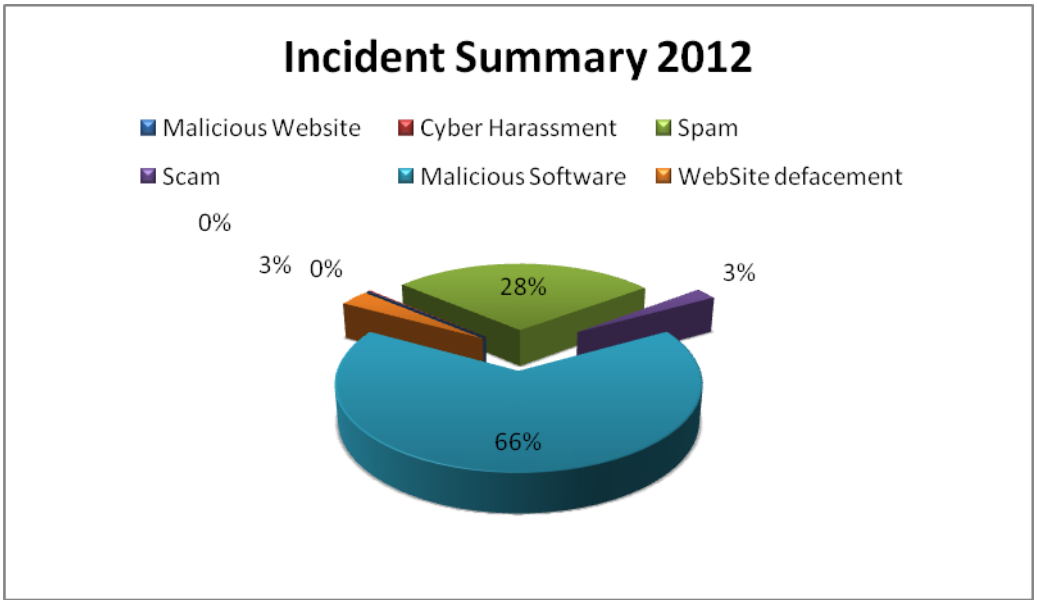


Figure 1

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

3. BruCERT Activities in 2012

3.1 Seminars/Conferences/Meetings/Visits

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

- On 25th March until 28th 2012 - Three BruCERT delegates attended the APCERT 2012 Annual General Meeting which takes place at Bali Island Indonesia, hosted by ID-SIRTII.

- On 26th until 28th September 2011, BruCERT Attended the OIC-CERT Annual Conference 2011 and the 3rd Annual General Meeting.

- In February 14th 2012, BruCERT joined the APCERT Drill as one of the

organizer.

- In September 27th 2012, BruCERT joined the ASEAN CERT Incident Response Drill, where the main objective is to simulate realistic cross-border incidents handling and promote collaboration among national CERTs in the region

3.2 Awareness Campaign

- On11th Feb Until 7th May 2012 – BruCERT was involved with Brunei Law Enforcement Agencies visiting 44 primary schools, promoting Security awareness by providing security magazines and quizzes to students.

- On November 9th until 11th 2012 – BruCERT joint the "Cyber Security Awareness Week" and organized the password challenge competition at one of the malls. BruCERT also release "Parents' Guide On Online Safety for children" book for the public.

- On November 20th Until 22th 2012 – BruCERT co-sponsored the "Universal Day" for the Ministry of Culture, Youth and Sport

3.3 Training and Seminars

- Since 2011 until 2012, BruCERT continuously provide security awareness training to the Government Civil Servant as part of BruCERT Awareness program.

- On 23rd April 2012, BruCERT and other relevant Brunei government agencies was involved in the developing of the Child Online Protection (COP) framework with International Telecommunication Unit (ITU) and IMPACT.

- From November 21st until November 25th, BruCERT hosted the OIC-CERT Technical Training which was conducted by MYCERT. It is the first time such an event had been organized in Brunei Darussalam.

- On December 12th, BruCERT will be co-hosting with Microsoft a Public Safety Day for relevant Government Agencies in Brunei Darussalam.

4. Conclusion

In 2012, 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.

4. CERT Australia Activity Report

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 and Critical Infrastructure. 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.

1.2 Establishment

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

1.3 Activities

CERT Australia assists in building Australia's strategic cyber security capability and co-ordinates the national operational response to cyber security events for the private sector, which in turn impact on all Australians.

CERT Australia works with other Australian Government agencies to contribute to a shared understanding of major cyber events. It provides a pathway to the national crisis management arrangements and alerts and guidance to the private sector.

CERT Australia incorporates a range of current 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 the owners and operators of critical infrastructure and other systems of national interest 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.

1.4 Workforce power

CERT Australia currently employs 23 core staff.

1.5 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 Systems of National Interest or Critical Infrastructure providers.

2. Activities & Operations

Throughout 2012, CERT Australia:

- Provided unique cyber security threat and vulnerability information relevant to the Australian private sector; specifically those organisations identified as Systems of National Interest and Critical Infrastructure, the purpose of which is to assist the private sector to protect their networks.
- Co-hosted and delivered an ASEAN Regional Forum workshop on cyber incident response with the Government of Singapore in Singapore to ASEAN Regional Forum economies.
- 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 two national information exchanges which included members of the

banking and finance, control systems and telecommunications sectors. These exchanges enable government and business to share sensitive cyber-security technical information and experiences in a trusted environment, which enhances 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.
- Participated in academic research projects related to cyber components of Australian internet security on topics including BGP monitoring and trend analysis.
- Responded to incidents involving targeted and untargeted Australian organisations.

2.1 Incident handling reports

In 2012, CERT Australia had almost 7,300 cyber incidents reported to it, which required a range of responses depending on the nature of the incident. CERT Australia also produced and disseminated 93 sensitive advisories on cyber vulnerabilities affecting systems of national interest.

2.2 Data repatriation

CERT Australia repatriated more than 750,000 stolen records in 2012 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 and IDA/SingCERT jointly hosted the ASEAN Regional Forum (ARF) Incident Response Workshop 2012 in Singapore in September. The workshop was conducted as a table-top discussion, with the participants working on three different cyber security scenarios. There were a total of 68 delegates from 18 countries.

3.2 Drills

CERT Australia participated in the APCERT Drill in February 2012.

3.3 Seminars

CERT Australia organised and co-hosted a CERT 'Birds of a Feather' session at the AusCERT 2012 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

4.1 Presentations

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

- APCERT AGM and conference, March – Indonesia
- Multilateral Network Security Information Exchange, September – Canada
- AusCERT 2012 conference, May – Australia
- FIRST conference, June – Malta
- Idaho National Laboratories control systems training workshop, April – USA
- Blackhat, DefCon & GFIRST, 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 2012 are:

- CERT Australia, along with IDA/SingCERT hosted the 2012 ASEAN Regional Forum (ARF) Incident Response Workshop in Singapore in September.
- CERT Australia participated in the 2012 APCERT Drill held in February.

5. CERT-In Activity Report

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 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 2012 is given in the following table:

Activities	Year 2012
Security Incidents handled	22060
Security Alerts issued	10
Advisories Published	56
Vulnerability Notes Published	122
Security Guidelines Published	1
White papers/Case Studies Published	5
Trainings Organized	26
Indian Website Defacements tracked	23014
Open Proxy Servers tracked	2759
Bot Infected Systems tracked	6494717

Table 1. CERT-In Activities during year 2012

2.2 Abuse Statistics

In the year 2012, CERT-In handled more than 22000 incidents. The types of incidents handled were mostly of Spam, Website compromise & malware

propagation, Malicious Code, Phishing and Network Scanning & Probing.

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

Security Incidents	2004	2005	2006	2007	2008	2009	2010	2011	2012
Phishing	3	101	339	392	604	374	508	674	887
Network Scanning / Probing	11	40	177	223	265	303	277	1748	2866
Virus / Malicious Code	5	95	19	358	408	596	2817	2765	3149
Spam	-	-	-	-	305	285	181	2480	8150
Website Compromise & Malware Propagation	-	-	-	-	835	6548	6344	4394	4591
Others	4	18	17	264	148	160	188	1240	2417
Total	**23**	**254**	**552**	**1237**	**2565**	**8266**	**10315**	**13301**	**22060**

Table 2. Year-wise summary of Security Incidents handled

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

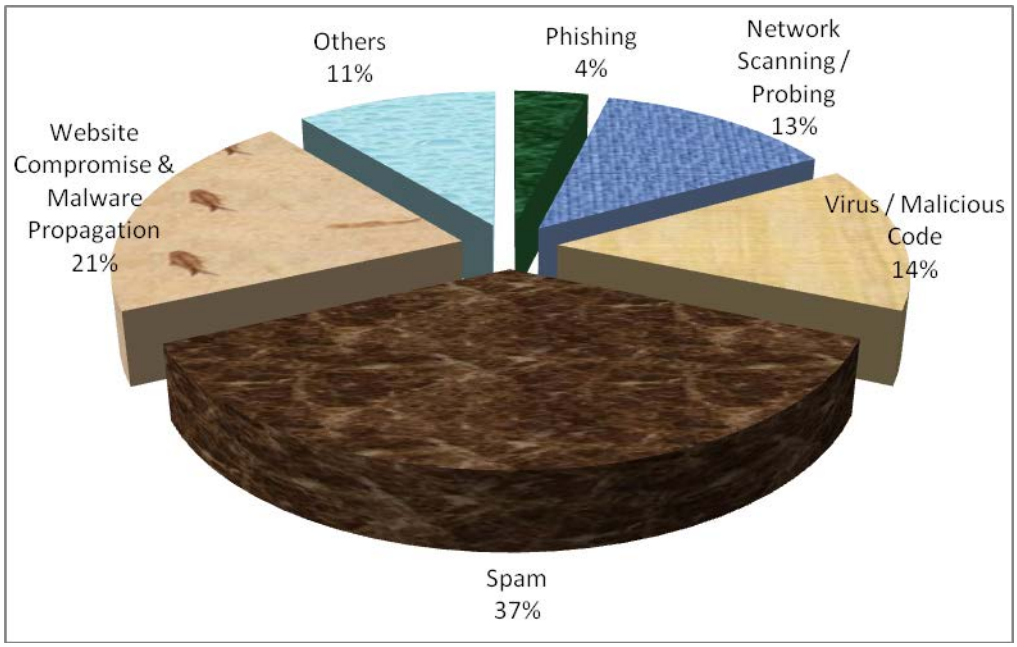


Figure 1. Summary of incidents handled by CERT-In during 2012

2.3 Incident Trends

The trends of incidents reported to and handled by CERT-In and cyber attack trends during the year 2012 are as follows:

- **Website compromise and Malware Propagations**

  These are website intrusions and drive-by-download attacks through compromised websites. Around 4591 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 end-systems to deliver malware such as key loggers and information stealers. The attackers targeted web browser plug-ins lavishly to deliver malicious contents. The code injected into the websites are heavily obfuscated and polymorphic making them harder to detect.

- **Surge of Exploit Kits**

  Significant increase in the exploit tool kits were observed in this year. An exploit kit/ exploit pack, is a toolkit that facilitates the automation of client-side vulnerability exploitation. The modus operandi normally revolves around targeting browsers and programs that a website can invoke through the browser. The exploit kits are typically concealed with client side software vulnerabilities in Adobe reader, JRE, Adobe flash Player, Media Players etc. (non-exhaustive list).

- **Persistent and complex PC malware**

  The major and notable malware families observed were Autorun, dorkbot, Nitol, Ramnit, Sality (new variants), Vobfus, Win32/CplLnk, Conficker, Rimecud.

- **Information and Banking Trojans - New trends and methods in the arsenal**

  The most notable information stealer Trojans were Zeus and Spyeye, which among other capacities, are able to inject code onto the webpages returned from the banking sites and also having immense stealth mechanisms. Three derivates of Zeus have been reported such as Citadel, Ice IX, P2P version. Additionally threats into the banking malware family, Carberp and Tinba were observed.

- **DNS Changer**

  The malware initially infects the Windows or Apple computers and subsequently gain access to routers connected to those systems to exploit weakness like default factory configurations, easily guessable passwords etc. Once exploited or accessed, changes the DNS settings in the said computers and devices and make them point to rouge foreign DNS servers, which are forced to connect to the rogue network rather than to legitimate Internet Service Providers (ISPs). Users surfing the Web on infected computers would be redirected from legitimate sites to fraudulent or malicious ones.

- **Mobile malware and Mobile Botnets**

  Malware trends indicate that malware affecting mobile platforms largely Android was on the rise due to the high prevalence of Android enabled mobile devices. The android malware families prevalent were Opfake, Android Kungfu, Plangton, FakeInst, SMSreg, GAMEX, RootSmart, Lotoor capable of performing premium based texting/subscribe the user to expensive services, install backdoors, exfiltrated confidential data, reading and intercepting SMSs and send it to remote servers and wait for the command from cybercriminals and effectively becoming part of botnets.

- **Mobile Botnets**

  Botnet that targets mobile devices such as smart phones, attempting to gain complete access to the device and its contents as well as providing control to the botnet creator. Mobile botnets take advantage of unpatched exploits to provide hackers with root permissions over the compromised mobile device, enabling hackers to send e-mail or text messages, make phone calls, access contacts and photos, and more. Most mobile botnets go undetected and are able to spread by sending copies of themselves from compromised devices to other devices via text messages or e-mail messages.

- **Malicious Spam and identity theft schemes were leveraging Social networking sites**.

  Several campaigns hit the deck spreading virally such as clickjacking, LIKE

jacking. Additionally series of malware attacks creates pandemonium on the SNS sites such as My Webcam Thingy (Twitter), FireFoxed (click jacking intrusions), Dislike Scam (Facebook), Over The rainbow (Twitter).

- **Distributed Denial of Service (DDoS) Attacks**

  A no. of websites in the Government and Corporate sectors were targeted with Distributed Denial of Service attacks during May - June, 2012. These attacks were carried out by the well known hacktivist group 'Anonymous'.

- **Other Trends observed in 2012**

  CERT-In has observed that Content Management System vulnerabilities (especially Joomla! and Wordpress) were widely getting exploited for Wesbsite Defacements and launching Distributed Denial of Services attacks. Sophisticated tools(web versions also) capable of launching flood attacks have been used for Denial of Service attacks against Govt., Financial and private sector organizations. There has been a rise in the spamming incidents targeting genuine users for financial frauds.

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 23014 numbers of defacements have been tracked. Most of the defacements were under '.in' domain, in which a total 11304 '.in' domain websites were defaced.

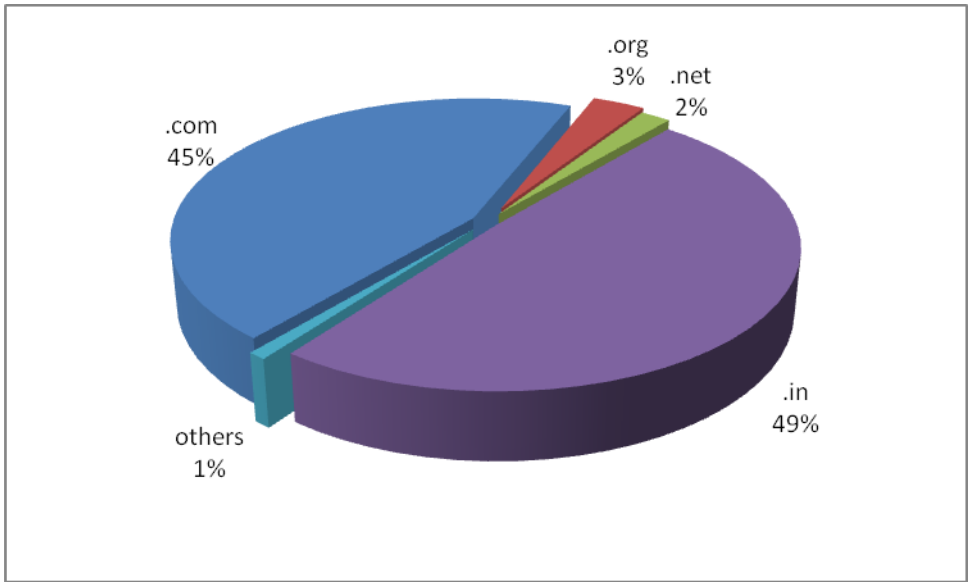


Figure 2. Indian websites defaced during 2012 (Top Level Domains)

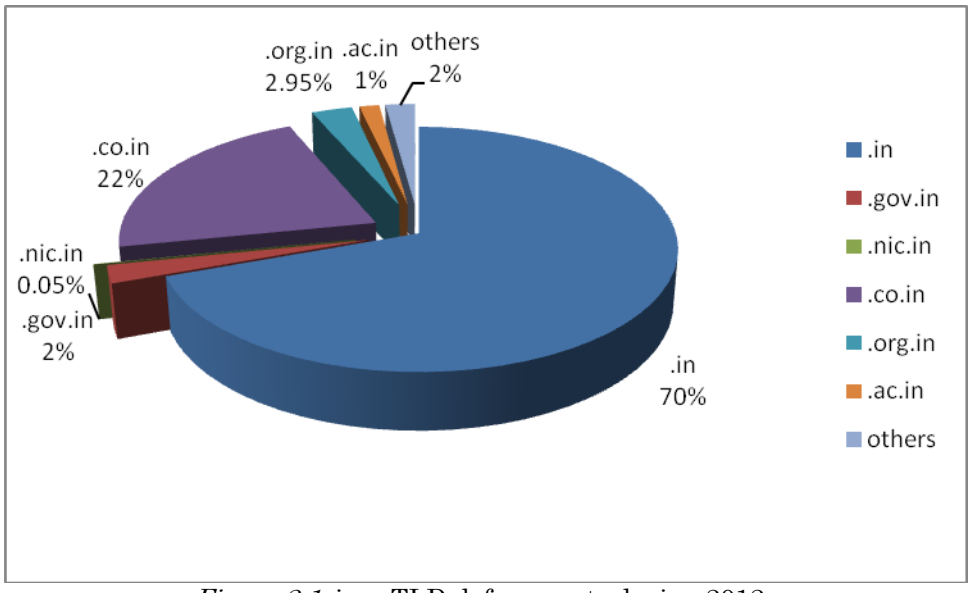


Figure 2.1 .in ccTLD defacements during 2012

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 2759 open proxy servers were tracked in the year 2012. The month-wise distribution of open proxy servers tracked during this year is shown in the figure 3.

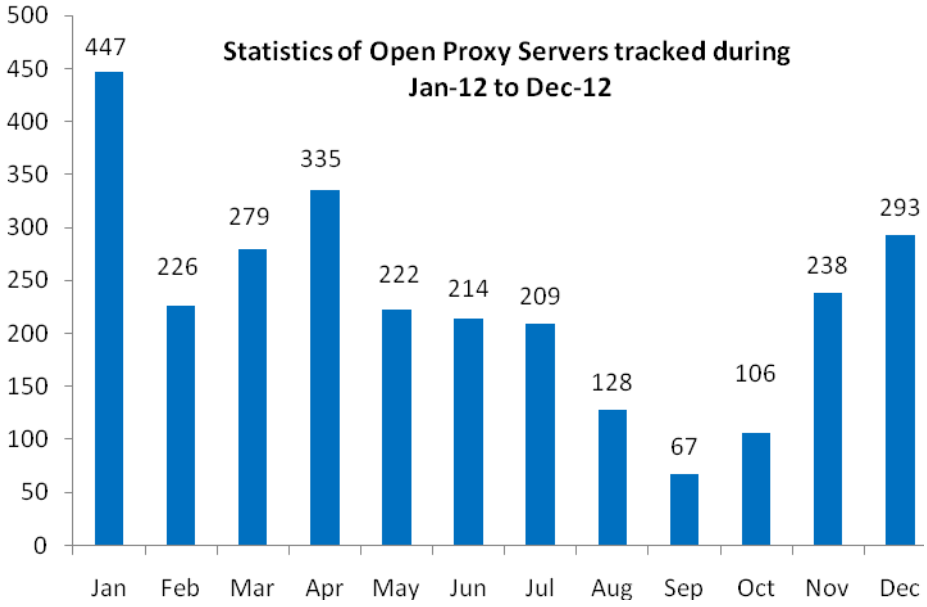


Figure 3. Monthly statistics of Open Proxy Servers in 2012

2.6 Botnet Tracking and Mitigation

CERT-In is tracking Bots and Botnets involving Indian systems. After tracking the IP addresses of Command and Control servers and Bots operating within India, actions are being taken to clean the respective systems and prevent malicious activities. Figure 4 shows the number of Bot infected systems and Command & Control servers tracked in 2012.

Month	Number of Bot Infected Systems	C&C Servers
January	977043	3
February	809164	1
March	835255	6
April	725003	4
May	779566	5
June	555274	5
July	485776	2
August	705660	1
September	1234512	5
October	1261631	4

November	3188652	6
December	2907292	6

Figure 4. Botnet statistics in 2012

2.7 Collaborative Incident resolution

During the year 2012, CERT-In worked in collaboration with Microsoft and Internet Service Providers in India to detect and clean the botnet infected systems, specifically the ZeuS variants and Nitol Botnet. The outcome was very encouraging.

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.

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 2012:

- Workshop on "Identity and Access Management" on January 06, 2012
- Workshop on "Network Perimeter Defence in Depth" on January 20, 2012
- Workshop on "Linux Security" on February 03, 2012
- Workshop on "Current Security Trends" on February 09, 2012
- Workshop on "Intrusion Detection in Depth" on March 02, 2012
- Workshop on "Mobile Forensics" on March 23, 2012
- Workshop on "Cyber crime & Computer Forensics" on April 26, 2012
- Workshop on "Network Penetration Testing" on April 30, 2012
- Workshop on "Cyber Espionage, Infiltration & Combating techniques" on May 09, 2012
- Workshop on "Information Security for Railway officers" on May 14, 2012
- Workshop on " IPv6 Essentials, Implementation and Security" on June 11, 2012
- Workshop on "Virtualization & Cloud Security" on July 18, 2012
- Workshop on "Cyber Forensics" on July 19, 2012
- Workshop on "Web Application Security & Penetration Testing Basics" on July 31, 2012
- Workshop on "Securing Critical Information Infrastructure" on August 06, 2012
- Workshop on "Advanced Information Security" on August 24, 2012
- Workshop on "DDoS Attacks & Mitigation" on August 28, 2012
- Workshop on "Threat & Vulnerability Management" on September 21, 2012
- Workshop on "Windows Security" on September 28, 2012
- Workshop on "Wireless Security" on October 17, 2012
- Workshop on "Advanced Application Security" on October 30, 2012
- Workshop on "Information Security Policy, Compliance and Auditing" on November 09, 2012
- Workshop on "MS SQL Database Security" on November 27, 2012
- Workshop on "ORACLE Database Security" on December 07, 2012
- Workshop on "MySQL Database Security" on December 14, 2012

3.2 Cyber Security Drills

CERT-In successfully participated in the APCERT Incident Handling drill conducted in February 2012 and ASEAN CERTs Incident Handling Drill (ACID 2012) held in September 2012.

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 7 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. 7th Cyber Security Drill Mock Drill was conducted on 19th and 20th December 2012. This time, cyber security drill involved simulated cyber attacks as well as simulated cyber crisis scenarios.

4. Achievements

4.1 Publications

The following were published by CERT-In in the year 2012:

1. **Enterprise Wireless Fidelity Implementations Using Port Based Network Access Control (IEEE 802.1X)** - International Journal of Computer Science and Telecommunications [Volume 3, Issue 7, July 2012] - Noorul Ameen, Vincy Salam and Anil Sagar
2. **Integrated approach to prevent SQL injection attack and reflected cross site scripting attack**, International Journal of System Assurance Engineering and Management, December 2012, Volume 3, Issue 4, pp 343-351 - Pankaj Sharma, Rahul Johari, S. S. Sarma,
3. **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.

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).

India-US Joint Cyber Security Exercise (CSE) was conducted for first time between CERT-In, India and National Cyber Security Division (NCSD), Department of Homeland Security(DHS), USA on 11th, 12th and 17th September 2012 in order to build increased operational collaboration between CERTs as part of the MoU. Indian Computer Emergency Response Team (CERT-In), United States Computer Emergency Response Team (US-CERT) and Industrial Control CERT-US (ICS-CERT) were the participants of Joint CSE. The exercise was appreciated highly by both sides to build a workable path forward for joint cyber security cooperation between USA and India.

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.

6. CNCERT/CC Activity Report

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

1. About CNCERT

1.1 Introduction

CNCERT (or CNCERT/CC) is a National level CERT organization under the leadership of MIIT (Ministry of Industry and Information Technology of the People's Republic of China). It serves as the national network security monitoring, early warning and emergency response center, as well as the key technical coordination body for public network security issues. Therefore, the vital roles it plays are as follows:

- Monitoring public network security,
- Collecting, analyzing and publishing network security threats,
- Notifying the communication industry of network security incidents,
- Receiving and handling network security incidents home and abroad,
- Exchanging network security information and cooperating with international security organizations.

1.2 Establishment

CNCERT was founded in Sep., 1999, 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

The constituency of CNCERT includes the general public, government departments, the communication industry and businesses in mainland China. It supports the governmental departments in fulfilling their network security-related social management and public service functions, ensures safe

operation of the national information infrastructure and assists the critical information systems in network security monitoring, early warning and emergency response. Besides, it also cooperates with international internet organizations to resolve cross-border network security incidents.

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 2012, CNCERT received a total of about 19 thousand incident complaints, a 24.5% increase from the previous year. And among these incident complaints, 1,200 were reported by overseas organizations, making a 42.9% drop from the year of 2011. As shown in Figure 2-1, most of the victims were plagued by phishing (49.5%), vulnerability (39.4%) and malware (5.4%). Different from the previous year, phishing overtook vulnerability to become the most frequent incident complained about. And malware still ranked the third place with a considerable decrease of 71.2% from 2011 because of CNCERT's Trojan and Botnet clean-up campaigns in 2012.

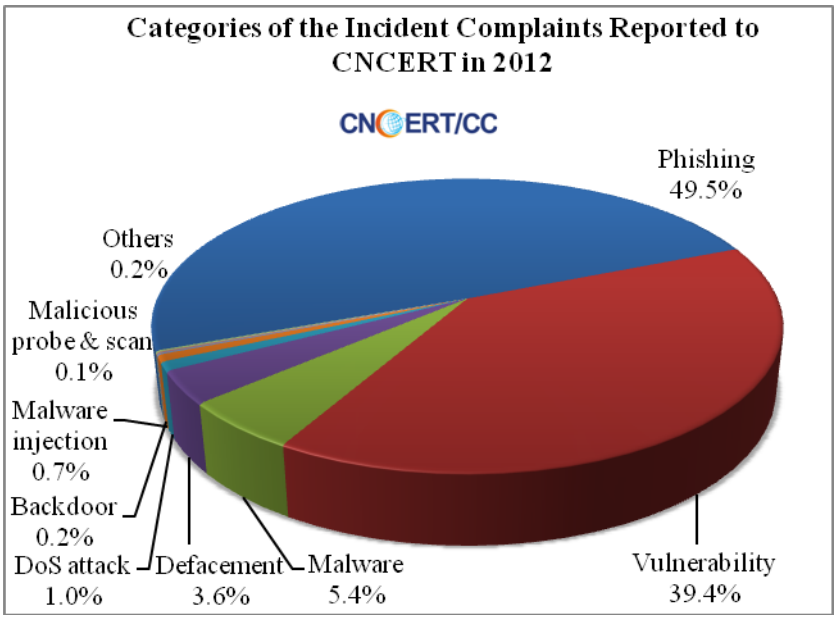


Figure 2-1 Categories of the Incident Reported to CNCERT in 2012

In 2012, CNCERT handled almost 19 thousand incidents, a significant rise of 72.1% compare with that in 2011. Besides, CNCERT has carried out 14 clean-up campaign against Trojans and Botnets as well as 6 clean-up campaigns against mobile malware in 2012. As illustrated in Figure 2-2, vulnerability (40.7%) dominated the categories of the incidents handled by CNCERT In 2012, followed by phishing (35%) and website defacement (11.7%).

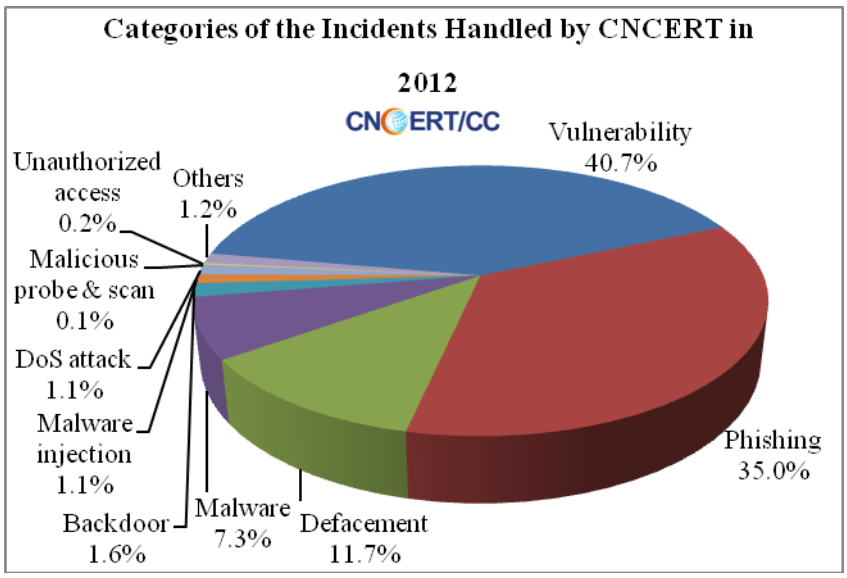


Figure 2-2 Categories of the Incidents Handled by CNCERT in 2012

2.2 Internet Monitoring

2.2.1 Compromised Hosts and Websites

In 2012, CNCERT monitored and discovered about 7.4 million incidents spreading known-type malware, which involved about 7 thousand domain names, about 8 thousand IP addresses and 38 thousand malware download links. Figure 2-3 depicts the monthly statistics of malware spreading incidents in 2012, with the most rampant malware activity in June.

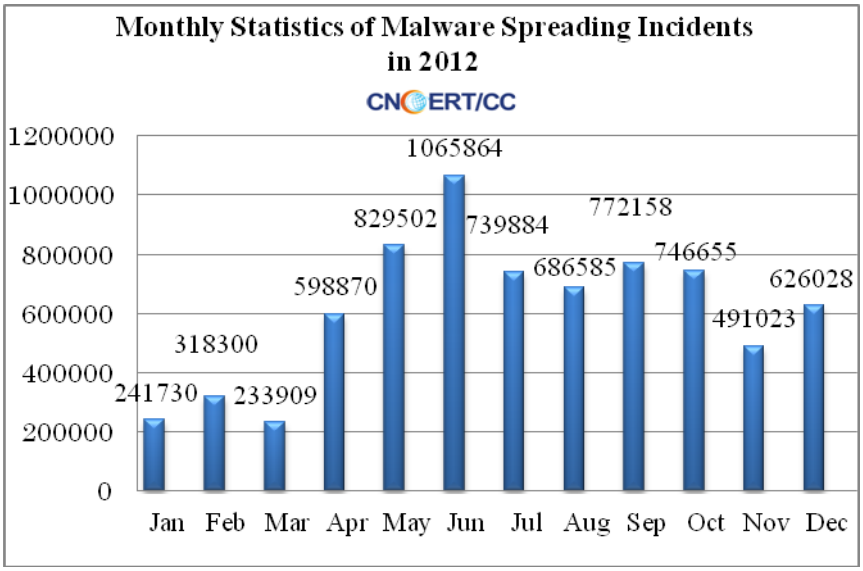


Figure 2-3 Monthly Statistics of Malware Spreading Incidents in 2012

In mainland China, IPs of the hosts infected with Trojan or Botnet reached about 14 million, which increased by 64.7% compared with that in 2011.

By CNCERT's Conficker Sinkhole system, over 28 million hosts per month on average were suspected to be infected all over the world. And 3.25 million compromised hosts per month were located in mainland China. As shown in Figure 2-4, mainland China (14.3%) had the most infection, followed by Brazil (10.9%), and Russia (6.5%).

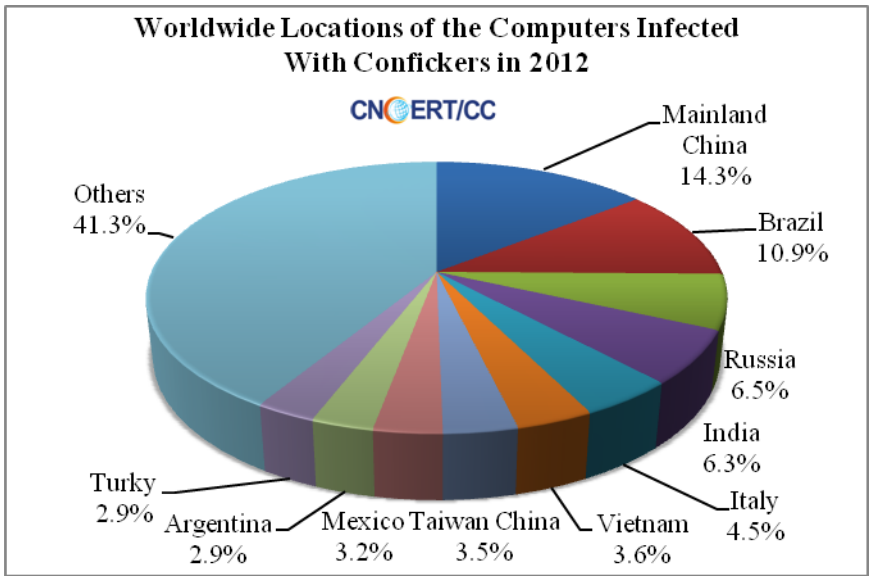


Figure 2-4 Worldwide Locations of the Computers Infected With Confickers in 2012

About 16 thousand websites in mainland China were defaced, a slight increase of 6.1% compare with that in 2011, including 1802 government sites. Besides, about

52 thousand websites were detected to be planted with backdoors and secretly controlled, including 3016 government sites.

2.2.2 Location of Malicious IPs

Because CNCERT's monitoring systems are all located in mainland China, most IPs of Trojan or Botnet C&C servers we detected were identified in local networks. But we still saw more than 73 thousand oversea C&C servers which increased 56.9% from 2011. The USA hosted the largest number of oversea Trojan or Botnet C&C servers' IPs, followed by Japan and Taiwan China.

In 2012, CNCERT detected about 22 thousand phishing sites targeting the banks in mainland China. About 2576 IPs were used to host those fake pages. 3.8% of those IPs were in mainland China and 96.2% were out of mainland China. The USA network hosted most of the phishing servers (80%).

CNCERT detected almost 58 thousand backdoor control IPs. Besides about 26 thousand were located in mainland China, 7370 (12.8%) were located in the USA, followed with 4362 (7.6%) in Taiwan China and 2590 (4.5%) in HongKong China.

2.3 Mobile Internet Monitoring

In 2012, CNCERT captured and collected about 163 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 (39.8%). Rogue malware (27.7%) rose to the second place. And followed it were those intended for fee consumption and remote control, accounting for 11% and 8.5% respectively.

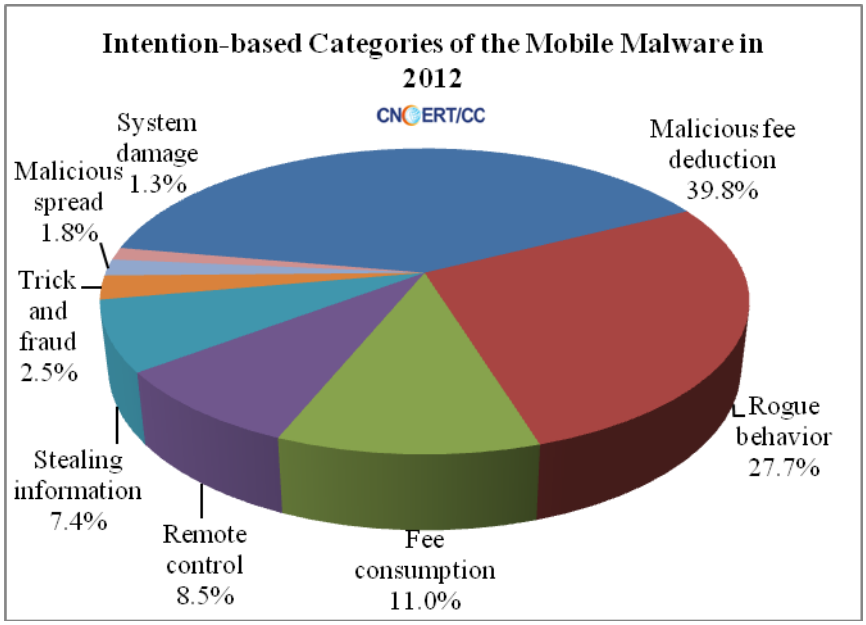


Figure 2-5 Intention-based Categories of the Mobile Malware in 2012

The majority of these mobile malware identified by CNCERT ran on Android and Symbian platform, recording about 134 thousand (82.5%) and about 28 thousand (17.5%) respectively.

3. Events organized/co-organized

3.1 Conferences

CNCERT 2012 Annual Conference

CNCERT organized CNCERT 2012 Annual Conference-"Build up Secure and Harmonious Network Environment" from 3rd to 5th July 2012 at Xi'an city, Shannxi province, China. Four tracks were designed for subject presentations at the annual conference, including New Challenge and New technology, Vulnerabilities and Personal Information Protection, E-Government and Important Information System Security, and Analysis on Underground Industry and Corresponding Response.

Press Briefing of Report on 2011 China Network Security Landscape

CNCERT hosted the Press Briefing of Report on 2011 China Network Security Landscape on 19 March 2012 in Beijing which attracted 50 experts from over 40 relevant organizations. The report summarized new trends and features of network security in China in 2011 and predicated security trends in 2012 with some countermeasures offered.

4. 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 2012

Name	Issues	Description
Weekly Report of CNCERT (Chinese)	52	Emailed to over 430 organizations and individuals and published on CNCERT's Chinese-version website (http://www.cert.org.cn/)
Weekly Report of CNCERT (English)	52	Emailed to relevant organizations and individuals and published on CNCERT's English-version website (http://www.cert.org.cn/english_web/documents.htm)
CNCERT Monthly Report on Internet Security Threats (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 on Network Security (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 Network Security Data	24	Published on journals and magazines.

5. Conferences attended & speeches delivered

APCERT 2012 Drill-"Advance Persistent Threats and Global Coordination",

CNCERT participated in the APCERT 2012 Drill -"Advance Persistent Threats and Global Coordination" as a participant on 29 January 2012 and completed it successfully.

1ST China and Korea Internet Roundtable-"Development and Cooperation"

CNCERT took part in the First Internet Roundtable between China and Korea which was kicked off on 5 December 2012 in Beijing. This two-day conference covered the Internet economy, network infrastructure construction and cybercrime. At the conference, CNCERT presented a report on landscape of China internet security and countermeasures, as well as exchanged views on international cooperation on network security and other issues with the Korean delegates.

2012 APCERT Annual Conference-"Cleaning the Cyber Environment"

Four Delegates from CNCERT attended the APCERT Annual General Meeting and Conference 2012 which was held from March 25 to 28 in 2012 in Indonesia with the theme of "Cleaning the Cyber Environment". At the conference, CNCERT introduced its network security services in 2012, and gave a keynote speech of "New Challenges to Security of the Public Network Environment" as invited.

The 45th Meeting of APEC Telecommunications and Information Working Group

From 5th to 11th April 2012, CNCERT attended the 45th Meeting of APEC Telecommunications and Information Working Group (APEC TEL 45) held in Da Nang city, Vietnam. At the meeting, the Chinese delegates introduced their efforts and achievements in improving the internet security, shared experience and methods in incident handling and information sharing.

ARF Workshop on Cyber Incident Response

CNCERT, together with 59 delegates from 17 countries, took part in the ARF (ASEAN Regional Forum) Workshop on Cyber Incident Response in Singapore from 6th to 8th September 2012. The CNCERT delegate presented a speech focusing on vulnerabilities of the industry controlling system and DDoS attacks.

7. HKCERT Activity Report

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 Mission and Constituency

HKCERT is the centre of coordination of computer security incident response for 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

1.3 Organization

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 a group of computer security specialists.

2. Operations and Activities

2.1 Incident Handling

During the period from January to December of 2012, HKCERT had handled 1,189 incidents, including 1,050 security incidents and 108 virus incidents. Security incident reports continue to overtake virus incident reports (See Figure 1).

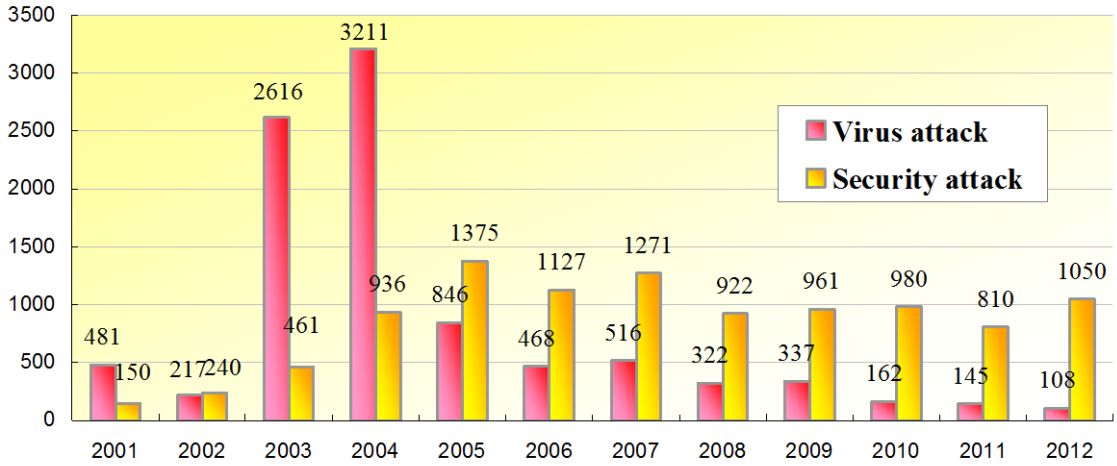


Figure 1. HKCERT Incident Reports in 2012

The total number of incidents handled by HKCERT in 2012 has increased by 22%, compared to 2011. This is mainly caused by the increase in the proactive discovery cases, in particular web defacement cases. The increase in proactive discovery cases may be caused by our improvement in the discovery process and additional resources put into proactive discovery. It also reflected the seriousness and resilience of modern malware infection and active intrusion, and the inadequacy of organizations in securing their systems.

We started to accept incident reports relating to smartphone in April 2012. During this period, we have received 18 reports in this area and most of them were relating to phishing messages.

2.2 Information Gathering and Dissemination

HKCERT collected security-related information from security organizations, made judgments on the impact to Hong Kong, and decided whether to disseminate the information. During the period from January to December of 2012, HKCERT published 429 security bulletins (See Figure 2) which is a 25.1% increase from previous year's number. All security bulletins were related to vulnerabilities and no malware alert was published during this period. In

addition, we have also published 58 blogs and advisories, including security advice on the use of smartphone and the best security reads of the week.

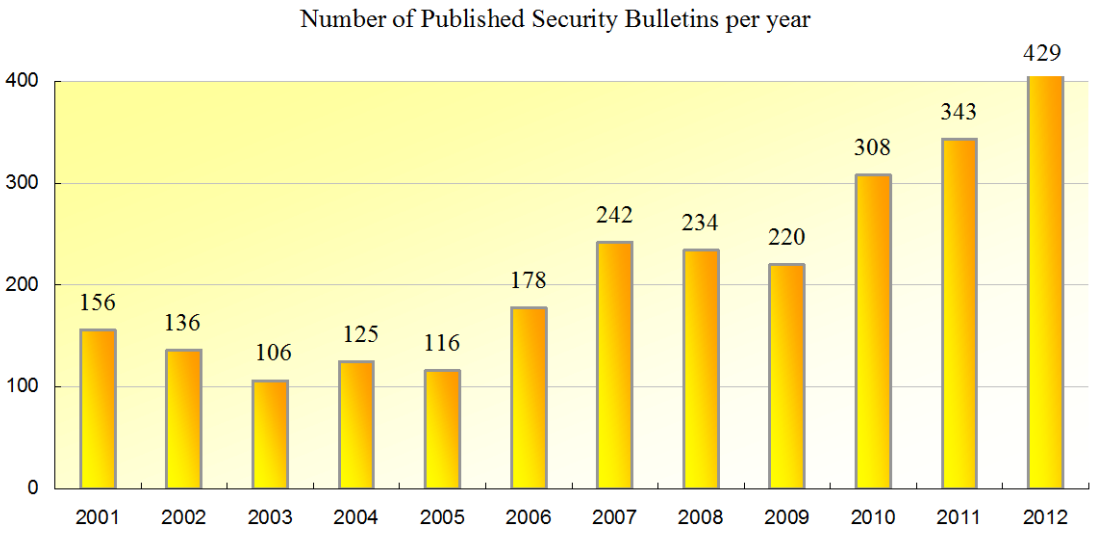


Figure 2. HKCERT Published Security Bulletins in 2012

2.3 Publications

We had published 12 issues of monthly e-Newsletter in the period.

3. Security Awareness and Training

3.1 Seminars, Conference and Meetings

HKCERT jointly organized the "Build A Secure Cyberspace" campaign with the Government and HK Police. The campaign involved public seminars, a cyber security symposium for ISPs, and a poster design contest. Four public seminars were organized in March, May, August and December 2012.

We organized the Information Security Summit 2012 with other information security organizations and associations in November 2012, 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. Coordination and collaboration

4.1 International Collaboration

HKCERT participated in a number of international coordination and collaboration events:

- Participated in the APCERT AGM and Conference in Bali, Indonesia; the FIRST AGM and Conference in Malta; and the Annual Meeting for CSIRTs with National Responsibility in Malta.
- Participated in the APCERT Drill (February 2012) and acted as the Exercise Control team member. The theme of the drill this year was "Advance Persistent Threats and Global Coordination". The drill was a great success with 22 APCERT teams from 17 economies 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 2012, HKCERT had worked with ISPs to clean up DNS Changer infected machines in Hong Kong.
- Co-organized a local drill with HK Police and OGCIO on 31st October 2012 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

- Organized an industry networking session with information security organizations in Hong Kong.

5. Other Activities

5.1 Year Ender press briefing

HKCERT organizes 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 2012 year ender briefing was held on 5th January 2012 to talk on the security status of 2011 and trends of 2012.

5.2 Three Year Strategic Plan

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

6. Future Plans

6.1 Funding

HKCERT would secure Government funding to provide the basic CERT services in 2013/2014. 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.

6.2 Enhancement Areas

- HKCERT is working on adding critical security bulletins messages to the GovHK Notifications mobile application (a one-stop platform for citizens to receive Hong Kong Government notifications.)
- HKCERT is working on an Information Feed Analysis System to collect intelligence of compromised machines in Hong Kong. The system will provide a better picture of security status of Hong Kong and help clean up the botnets and C&C servers in Hong Kong.
- HKCERT is also developing a new Incident Report Management System which will help improve the efficiency of our incident response activities.
- HKCERT is enhancing the liaison and information sharing with the critical

infrastructure sector to better protect the security environment of Hong Kong.

8. ID-CERT Activity Report

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 2011 complaints received by ID-CERT were still handled by Budi Rahardjo, MSc., PhD. and Andika Triwidada. January 2011, Ahmad Alkazimy was recruited after being volunteer in research activity since March, 2007. Then, Rahmadian L. Arbianita joined the team since January 2012.

Volunteers :

1. Budi Rahardjo, MSc., PhD. ***(ID-CERT Chair)***
2. Andika Triwidada ***(ID-CERT Co-Chair)***
   Finger print: 5568 7C7D E898 4F33 A594 A996 DA4B C29F E22D FEE7

3. Maman Sutarman
4. Ikhlasul Amal
5. Rizky Ariestiyansyah
6. Other volunteers

Professional Staffs :

1. 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
2. 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 this 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

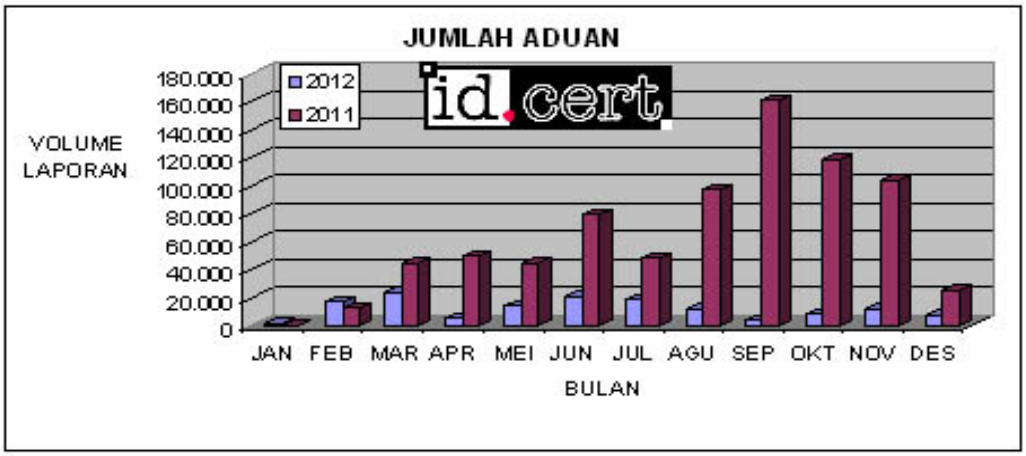
ID-CERT is a reactive CERT. From all complaints received by ID-CERT, Network Incident is the biggest amount reported. These reports/complaints which were once received by individuals - usually received by Budi Rahardjo, MSc., PhD., Andika Triwidada, and Ahmad Alkazimy - in the year 2012 has begun received on a particular email and handled by a professional staff of ID-CERT, which is then forwarded to the sites reported problems or to the related service provider.

Additionally, other media used to describe the case and its development is the mailing list.

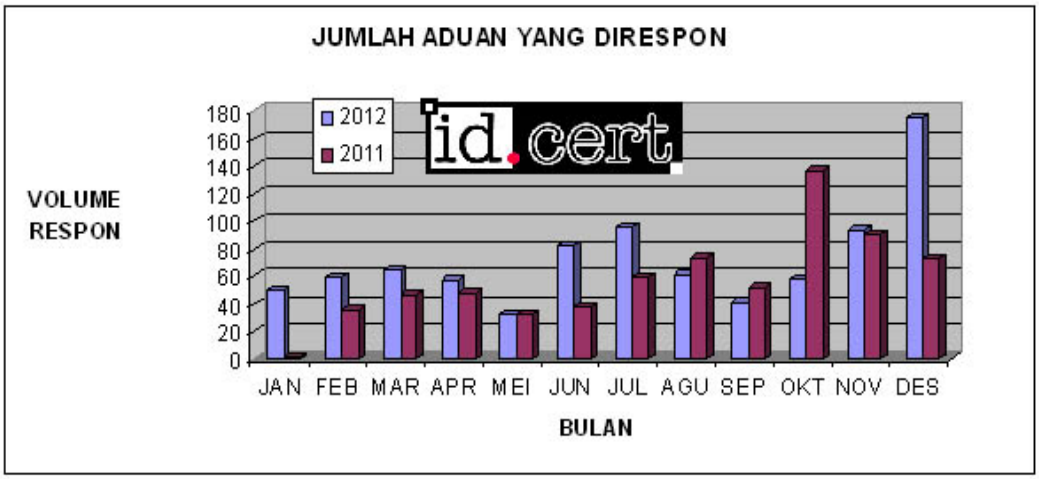
Now, ID-CERT has a HelpDesk that manages the received reports/complaints and the progress report completion. Currently, ID-CERT is run by professionals and supported by volunteers. The demand for the HelpDesk is related to service and handle the complaints of incident, as well as the statistical purposes to display cases handled, which is always presented at APCERT AGM.

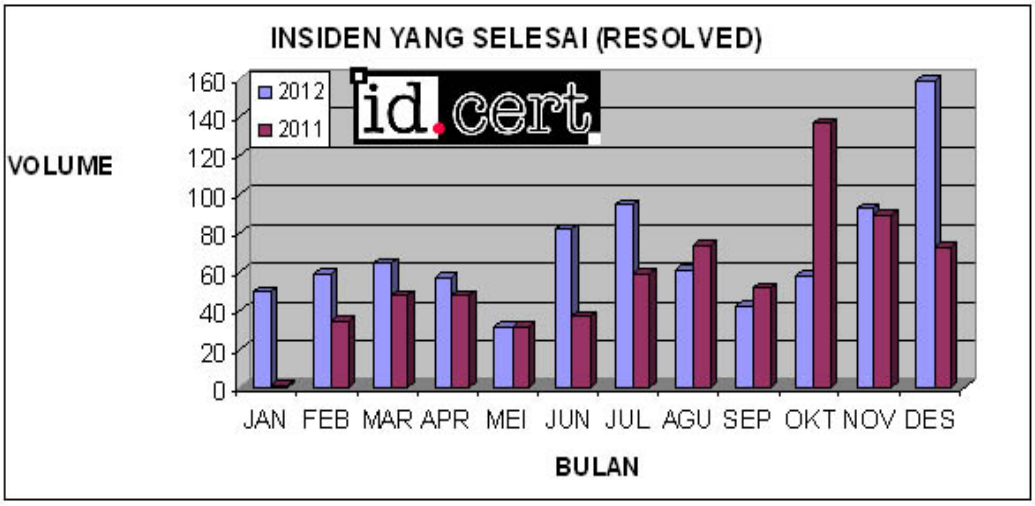
3.1 Incident Handling

At December 31, 2012 ID-CERT had received 141,616 incident complaints during the year 2012.



ID-CERT had proceed 868 incidents and 852 of them had successfully handled and solved.





ID-CERT has made Standard Operation Procedures (SOP) relating to the incident handling with priority: the complaints that come from local and the international complaints that request for assistance. While the complaint incidents in the sent as a copy/cc (already addressed directly to the ISP) ID-CERT will not process it further.

Effective as of November 1, 2012, ID-CERT has handled fully all incidents according the SOP, which was previously only focused on Phishing/Spoofing complaints and government agencies complaints.

In order to expedite the handling and incident documentation process of complaints, effective on November 1, 2012 ID-CERT had also successfully operate the documentation and e-mail ticket system using RTIR.

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 the last 2 years, ID-CERT has conducted research related to the handling of incidents based on complaints or it's called Incident Monitoring Report (IMR) by involving ISPs, NAPs, Telecommunication Operators, and non-ISPs, such as government and corporate institutions. Starting with the Internet Abuse Research in 2010, now as of March 2012, the research has become one of the ID-CERT routine activities and become permanent that expected to be sustainable, so that Indonesia can have a primary data on Incident Monitoring

Report occurred in Indonesia.

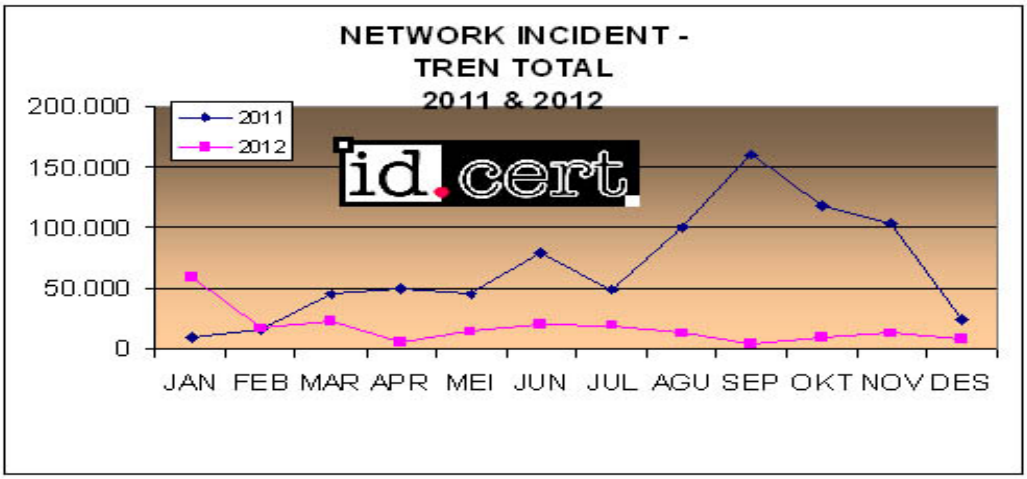
In contrast to the reports ID-CERT received above, reports received through IMR in the year 2012, when averaged over a number of reports of complaints are 290,297 reports per month. While the number of reports received during the year 2011 was reported as 1,057,333 or an average of 88,111 per month. And total number of reports received in 2012 is only 265,194.

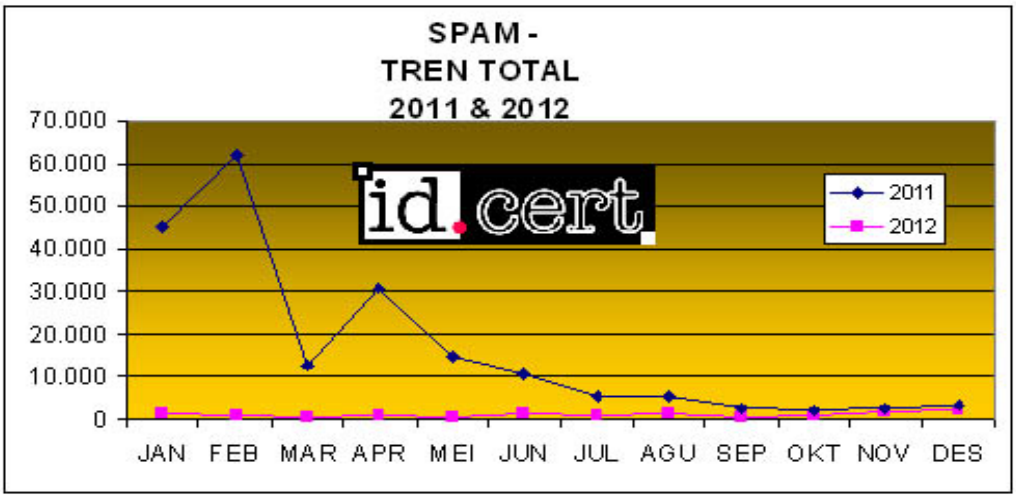
2012		
No.	Category	Rating (%)
1.	Network Incident	76,53
2.	**Malware**	8,63
3.	**Intellectual Property Rights/HaKI**	6,99
4.	**Spam**	4,78
5.	**Spam Complaint**	1,94
6.	**Spoofing/Phishing**	0,64
7.	**Response**	0,48

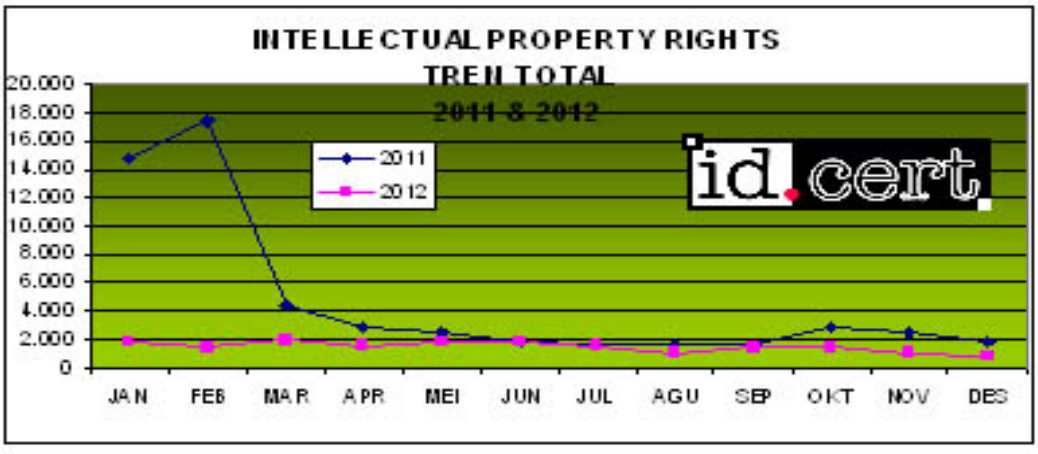
2011		
No.	Category	Rating (%)
1.	Network Incident	75,45
2.	Spam	17,40
3.	Intellectual Property Rights/HaKI	5,33
4.	Malware	1,62
5.	Spoofing/Phishing	0,11
6.	Response	0,07
7.	Spam Complaint	0,03

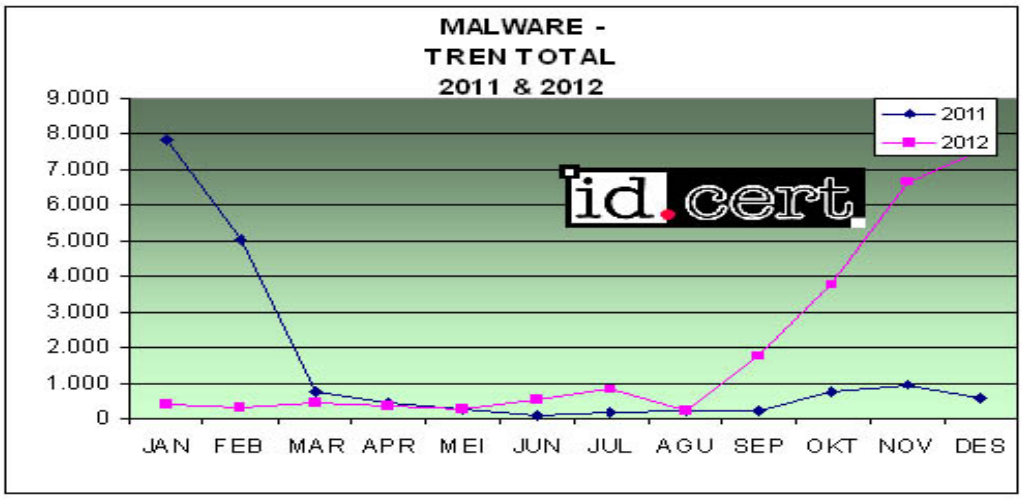
*Note: **in Bold:** position rating changing in 2012 compared to 2011*

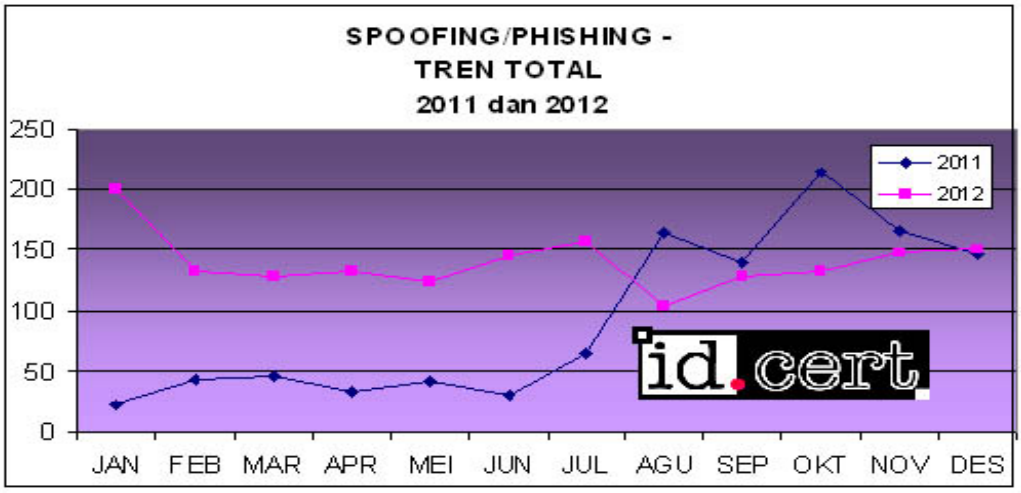
Here are comparison of trend graphs total in 2011 and 2012 for Network Incident, Spam, Intellectual Property Rights /IPR, Malware, Spoofing/Phishing, Response, and Spam Complaints:

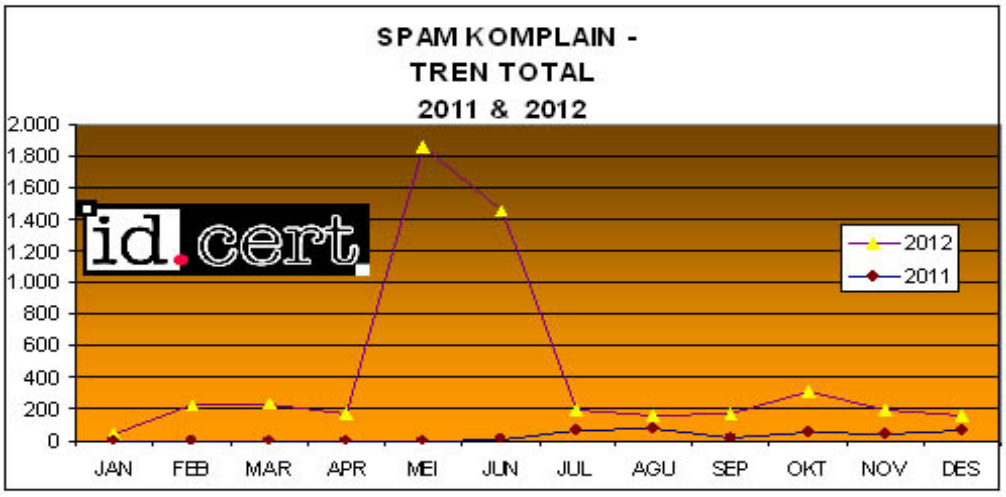

NETWORK INCIDENT -
TREN TOTAL
2011 & 2012
200.000
150.000
100.000
50.000
0
2011
2012
id.cert
JAN FEB MAR APR MEI JUN JUL AGU SEP OKT NOV DES


SPAM -
TREN TOTAL
2011 & 2012
70.000
60.000
50.000
40.000
30.000
20.000
10.000
0
id.cert
2011
2012
JAN FEB MAR APR MEI JUN JUL AGU SEP OKT NOV DES


INTELLECTUAL PROPERTY RIGHTS
TREN TOTAL
2011 & 2012
20.000
18.000
16.000
14.000
12.000
10.000
8.000
6.000
4.000
2.000
0
2011
2012
id.cert
JAN FEB MAR APR MEI JUN JUL AGU SEP OKT NOV DES







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

Since November 2012, on the advice of a number of CERTs when occuring the Outbreak Malware Grumbot, the ID-CERT began issuing warnings in the Security Advisory form. This is the latest achievement of ID-CERT after all this time trying to find the right formula and type of Security Warning/Advisory/Notice which suitable for ID-CERT constituents.

By December 2012, ID-CERT has issued 5 (five) Security Warning/Advisory/Notice in Bahasa Indonesia.

3.4 Events

There are three major events attended by ID-CERT in 2012:

1. February 14, 2012 – APCERT Drill
2. February 29, 2012 – ID-CERT Gathering IV in Jakarta
3. March 25-28, 2012 – APCERT Annual General Meeting 2012 in Bali

4. Achievement

ID-CERT achievements in 2012 are:

1. ID-CERT has built a Standard Operation Procedures (SOP) and detail job desk to conduct staff development and personnel additions, at least for a response helpdesk.
2. ID-CERT has made the development of hardware and software associated with building a systemic mechanism email responder and updated ID-CERT website www.cert.or.id
3. ID-CERT has been conducting research required by the Internet community in Indonesia.
4. Since November 2012 ID-CERT officially began releasing Security Warning/Advisory/Notice on ID-CERT website and mailing list.
5. ID-CERT has published a research report on a regular basis: per bi-monthly, per semester, and annual report on the ID-CERT website.
6. ID-CERT got involved in the establishment of GovCSIRT from Roadmap to operational implementation.

5. Agenda

ID-CERT main concern is what actually expected by the public from ID-CERT.

1. ID-CERT plans to continue to conduct various researches and studies required by the Internet community in Indonesia. For that, the ID-CERT also plans to add personnel in the research/study and collaborate with leading universities in developing any needed research.
2. ID-CERT keeps periodically publish research reports per month, bi-monthly, per semester and annual/final report.
3. ID-CERT also wants the support of the constituents of public education in various sectors of internet security.

9. ID-SIRTII/CC Activity Report

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

1. About Id-SIRTII/CC

1.1 Introduction

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

1.2 Establishment

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

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

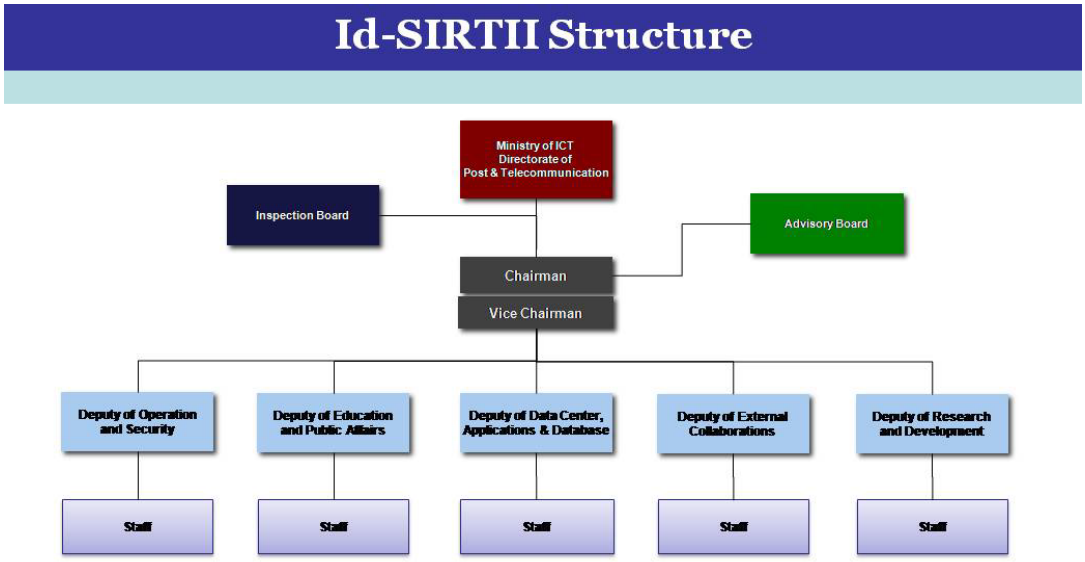
- Act No.36/1999 regarding National Telecommunication Industry
- Government Regulation No.52/2000 regarding Telecommunication Practices
- Ministry of Communication and Information Technology Regulation No.27/PER/M.KOMINFO/9/2006 regarding Telecommunication Network Management Security based on internet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

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

1.3 Workforce Power

Id-SIRTII/CC now has 6-team member Board of Directors, which is Chairman

and 5 deputy (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

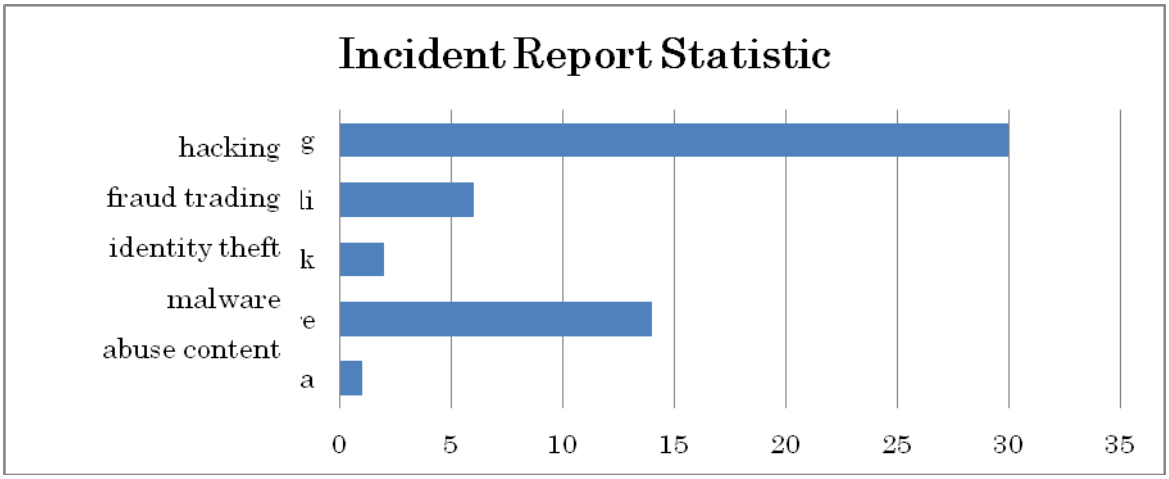
transactions (log files) for supporting the law enforcement process

- 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

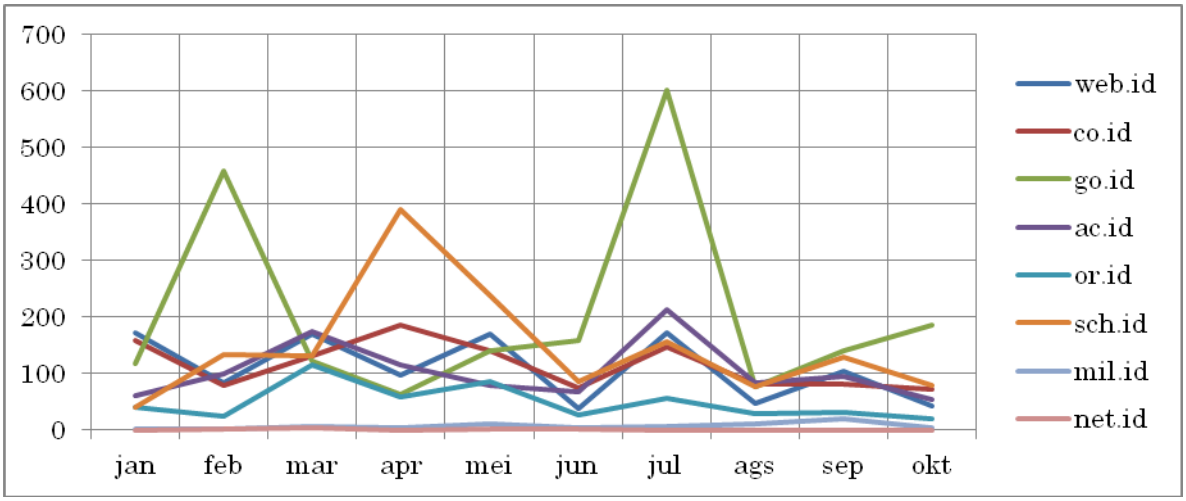
2.1 Incident Reports

We provide Incident Reporting Service for public in the first quarter of year 2012. 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 keep our constituency informed of potential vulnerabilities, and where possible, will inform this community of such vulnerabilities before they are actively exploited. The statistic during 2012 is shown as follow:



Web Defacement

Id-SIRTII/CC also conducted an intensive monitoring on critical websites especially the government institutions. During year 2012, government website (go.id) dominated the number of web defacement case, following by school websites (sch.id). The statistic can be shown on the following graph:



2.2 Incident Handling

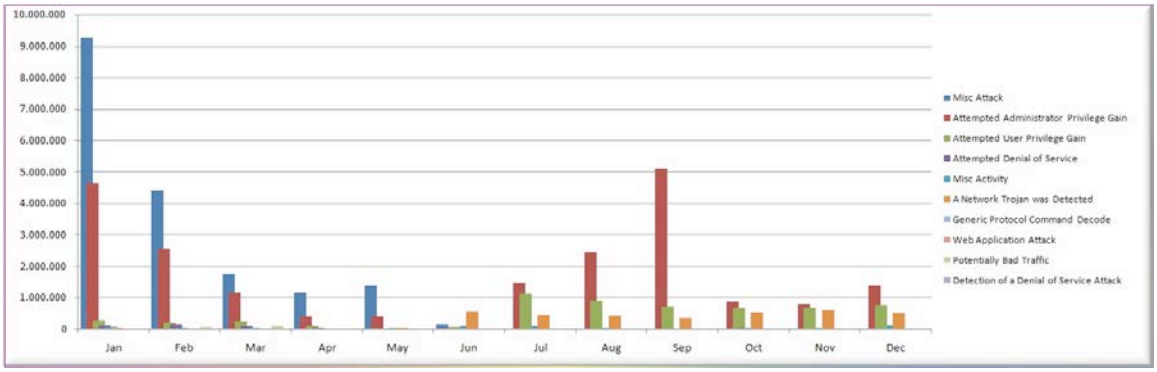
Assisting +20 Cyber Crime case with INP as an expert witness and +50 technical support and incident analysis/handling.

2.3 Incident Statistic

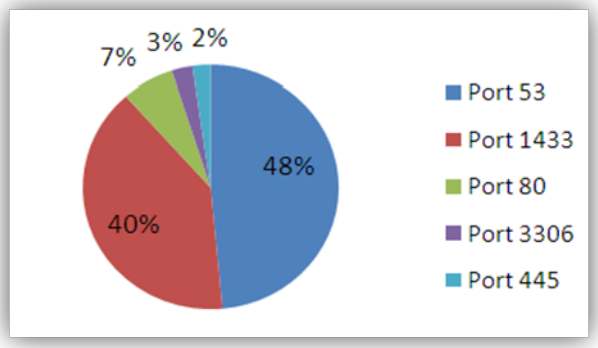
Based on our Monitoring Systems below is 10 Most Active events:

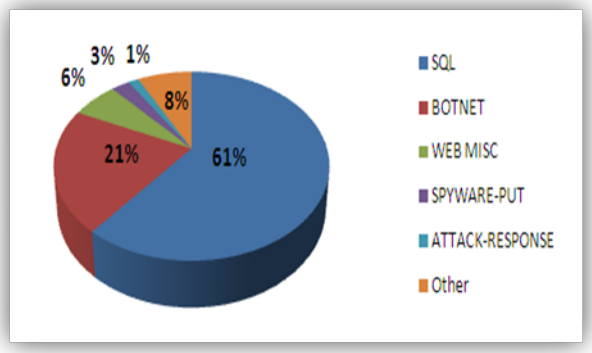
Classification	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
Misc Attack	9.265.759	4.412.183	1.751.258	1.161.333	1.407.615	154.060	406	2.081	1.539	6.984	10.808	4.770
Attempted Administrator Privilege Gain	4.653.292	2.549.203	1.161.362	416.932	402.630	40.867	1.463.948	2.461.394	5.127.160	884.703	800.065	1.402.242
Attempted User Privilege Gain	287.568	215.619	257.479	96.806	31.501	68.107	1.135.140	892.301	732.629	683.432	667.075	769.397
Attempted Denial of Service	118.416	154.191	106.304	42.294	140	29.588	19.351	24.342	26.192	38.960	16.079	20.893
Misc Activity	68.331	50.031	62.414	32.951	39.218	105.934	91.734	56.537	37.710	40.912	44.256	120.638
A Network Trojan was Detected	47.333	32.968	35.562	24.906	40.089	559.356	464.261	434.749	352.842	540.480	624.202	507.928
Generic Protocol Command Decode	11.631	8.263	5.625	716	557	281	0	58	11	1.480	1.673	305
Web Application Attack	3.839	64	409	397	814	258	3.633	2.774	1.845	2.449	1.911	6.633
Potentially Bad Traffic	3.530	73.150	97.307	9.285	6.896	37	2.289	1.380	1.514	1.314	131	1.004
Detection of a Denial of Service Attack	642	546	303	0	0	0	0	0	1	0	81	0
TOTAL	14.460.341	7.496.218	3.478.023	1.785.620	1.929.460	958.488	3.180.762	3.875.616	6.281.443	2.200.714	2.166.281	2.833.810

* 10 Active Events Classification



The following figures show the top 5 incident based on Port and Events during 2012:





2.4 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.

3. Event Organized/Co-Organized Achievement

3.1 International Membership

- FIRST, Full Member (2011)

- National CSIRT Forum (2010)
- APCERT, Full Member (2010)
- OIC-CERT, Full Member (2009)

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).

3.4 Organizing Conference and Workshop/Training

- Become a host for APCERT AGM and Conference 2012 frm 25-28 March 2012 in Bali. Following by FIRST Technical Colloquium event from 29-31 March 2012 on the same venue.
- A number of national seminar and workshop, such as: Incident Handling, Creating & Managing CSIRT and Forensics.
- National Drill Test in Jogjakarta, 13-14 July 2013 with 100 participants from various sectors such as government, banking, law enforcement, ISPs and communities.
- We conduct +50 various security training in 2012 i.e. Secure Coding and Secure Programming, Cyber Crime and Digital Forensic for LEA.

4. International Cooperation

4.1 Memorandum of Understanding with other int'l institution

MYCERT/CC, JPCERT/CC, Telcom-ISAC Japan, KRCERT/CC (on progress), CNCERT/CC

4.2 Joining Int'l Conference and Events

- AOTS/HIDA Training 2012, Tokyo – Japan
- APCERT AGM 2012, Bali – Indonesia
- FIRST TC 2012, Bali (Indonesia) and Buenos Aires (Argentina)
- OIC-CERT AGM 2012, Oman
- ASEAN-Japan Security Forum 2012, Brunei

- ASEAN CERTs Incident Drill (ACID) 2012
- APCERT Drill Test 2012

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

In 2012, 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, Sociaties, 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.

10. JPCERT/CC Activity Report

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 2012, JPCERT/CC received 17,265 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	2,699	4,072	5,430	5,064	17,265

Figure 1. Incident reports to JPCERT/CC (2012)

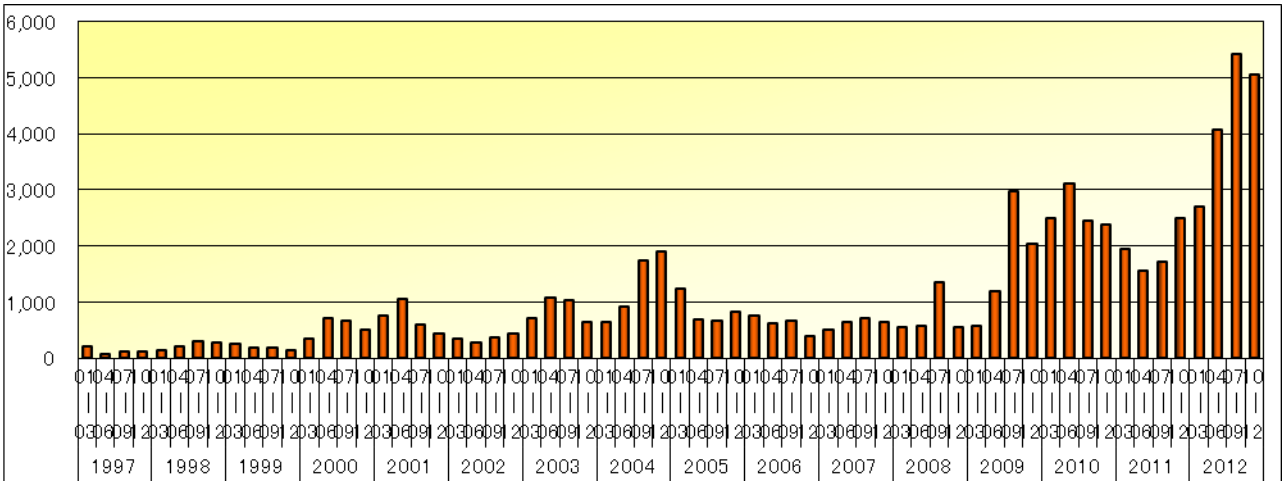


Figure 2. Incident reports to JPCERT/CC (1997-2012)

2.2 Abuse statistics

The incident reports to JPCERT/CC in 2012 were categorized as in Figure 3. About 60% of the incident reports were on scan, followed by website defacement and phishing.

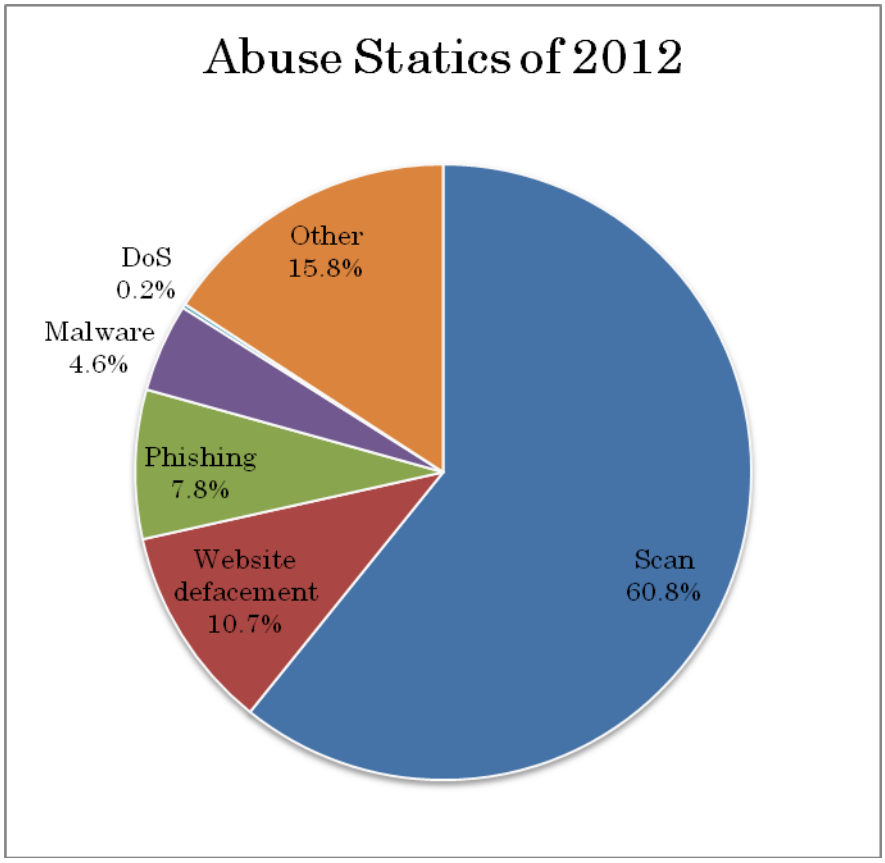


Figure 3. Abuse Statistics of 2012

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 2012, 45 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 information 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 (including information on affected products, workarounds and solutions, such as updates and patches) on each vulnerability.

  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 2012, 262 vulnerabilities coordinated by JPCERT/CC were published on JVN. Among them, 112 cases were reported through IPA in Japan, 2 cases were published in cooperation with CERT-FI, and 148 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 Becomes CVE Numbering Authority (Japanese)
  https://www.jpcert.or.jp/press/2010/PR20100624_cna.pdf
  - JPCERT/CC Becomes CVE Numbering Authority (English)

https://cve.mitre.org/news/archives/2010_news.html#jun232010a

- **JPCERT/CC Weekly Report**

  JPCERT/CC publishes weekly reports on selected security information of the preceding week that is regarded as high importance by JPCERT/CC. Weekly reports also contain a relevant security tip every week.

- **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. Starting from January 2013, we will extend our services on incident handling for ICS operators for ICS. We've started to distribute ICS security assessment tools for our constituents.

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.

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)

  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 2012 are as follows:

Invitational Training	- Training for ThaiCERT staff (September) - Training for PacCERT staff (September)

On-site Training/Seminar	-TSUBAME Workshop (March) -Java/ Android Secure Coding Seminars (May) -CSIRT Training Course for Africa (May and November) - Incident Response Training for LaoCERT (September) - Incident Response Training for mmCERT (November) -Advanced Malware Analysis Training for mmCERT (November)
Domestic Seminars/Conference	-Control System Security Conference (February, December) -Java Secure Coding Seminar (February, August, September, December) -Workshop on Information Sharing for Cyber Security (February) -Malware Analysis Workshop (MWS 2012) (October) …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	-Support of PacCERT establishment (March, July)
Dispatch of Speakers	-24th Annual FIRST Conference Malta (June) -ASEAN Regional Forum (ARF) Cyber Incident Response Workshop (September) -Cyber Security UAE Summit 2012 (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 2012:

RSA Conference 2012 (February)

APCERT AGM and Conference2012 (Bali)

APWG Conference (April, November)

Industrial Control Systems Joint Working Group (ICSJWG) Conference (May, October)

24th Annual FIRST Conference Malta (June)

National CSIRT Meeting (June)

Workshop on the Economics of Information Security (WEIS) (June)

RECON 2012 (June)

APISC 2012 (July)

Black Hat USA 2012 (July)

USENIX Security Symposium (August)

Control Systems Cyber Security Advance Training and Workshop (September)

Society of Instrument and Control Engineers (SICE) Annual Conference (September)

AVAR 2012 (November)

The 2012 International Conference on Network Computing and Information Security (December)

…and many more

3.4 Drills

JPCERT/CC participated in the following drills in 2012 to test our incident response capability:

- APCERT Drill 2012 (14 February)
- ASEAN CERT Incident Drill (ACID) 2012 (12 September)

4. MoU

To further strengthen cooperation, JPCERT/CC has been signing a Memorandum of Understanding (MoU) with various security organizations. For 2012, we have newly signed the MOU with BDCERT, CERT Australia and CERT.GOV.AZ, IT-ISAC, MOCERT, ThaiCERT.

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 the member of FIRST.

- **ISO International Standard**

  (ISO/IEC JTC 1/SC 27 Information technology – Security techniques)

  JPCERT/CC contributes to the following ISO International Standards being developed under ISO/IEC JTC 1/SC 27:

  ISO/IEC 29147: "Vulnerability Disclosure"

  ISO/IEC 27035: "Information Security Incident Management"

  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 the 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 & analyses within the region.

7. JPCERT/CC Contact Information

URL: https://www.jpcert.or.jp/
E-mail: global-cc@jpcert.or.jp
Phone: +81-3-3518-4600
Fax: +81-3-3518-4602

11. KrCERT/CC Activity Report

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 cybersecurity 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.

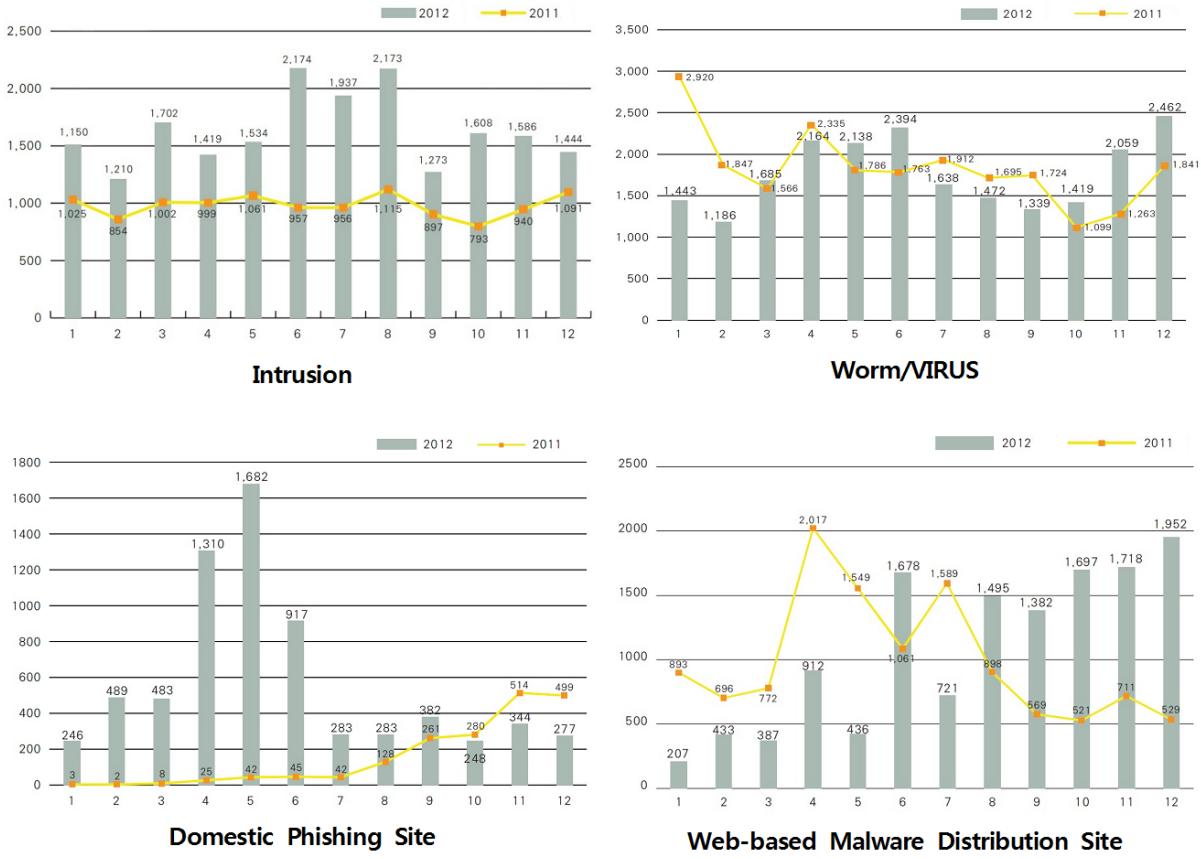
KrCERT/CC has responded to many security challenges and evolved itself to meet those challenges. The first major challenge was the breakdown of Internet infrastructure over several hours caused by slammer worm outbreak on 25th January 2003. At that time, KrCERT/CC didn't have the effective communication 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.

Distributed Denial of Service(DDoS) attack targeting Korea and US government in July 2009 was another big challenge from KrCERT/CC. Response experience with this DDoS attack enabled KrCERT/CC to improve its capability and operation. To do so, much budget was approved for CSIRT operation improvement and new staffs were hired. As a result, new services, such as DDoS shelter, cyber remediation service and so on, were introduced.

2. Activities in Year 2012

2.1 Incident handling reports

Internet incidents reported to KrCERT/CC are classified into the following 4 categories: worm/virus, hacking incident, domestic phishing site and web-based malware.



2012 KrCERT/CC incident report statistics

The number of incident reports on worm/virus to KrCERT/CC in 2012 is 21,399. , which shows almost no difference compared to that of 2011(21,751). The number of hacking incident reported to KrCERT/CC increased is from 11,690 in 2011 to 19,570 in 2012. The number of phishing sites targeting domestic brans is increased from 1,849 in 2011 to 6,944 in 2012. The number of web-based malware distribution site is also increased from 11,805 in 2011 to 13,018 in 2012.

2.1.1 Worm/Virus

The number of worm/virus incidents reported to KrCERT/CC in 2012 is 21,399. The number of this worm/virus incidents reportshows almost no difference compared to that of 2011. The most reported malware in 2012 is ONLINE

GAMEHACK, which steals online game credential, such as ID and Password. This particular malware was also ranked the top in 2011. Bad guys or hackers are trying to gain financial benefit by selling expensive online game items collected from stolen game accounts. This information can be traded in online black market. End users need to make efforts to prevent the damage from malware by installing up-to-date patches and scanning computers with the updated anti-virus softwares.

2.1.2 Hacking Incident

The number of hacking incidents reported to KrCERT/CC in 2012 is 19,570. It is increased by 67.4% compared to that of 2011(11,690).

KrCERT/CC observed a new trend in phishing incidents. 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 New service

2.2.1 Phone Keeper

Phone Keeper is the application developed and distributed by the KrCERT/CC in 2012 with the purpose of providing a security measure to users with Android platform based smart devices. The features of the Phone Keeper includes; checking the device's security configuration to let the users aware the level of security of own devices and allow to make any improvements required, and providing an easy guide to users facilitate a mobile anti-virus application if it is not already installed for checking and removal of the known malicious applications.

3. Events organized

3.1 2012 APISC Training Course

KrCERT/CC hosted the 2012 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 9th to 13th July in Ibis Seoul Hotel, Seoul, Korea. 20 trainees from 17 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 2012, KrCERT/CC has concluded the memorandum of understanding (MoU) with a foreign national CSIRT and a leading security company. The MoU with CERT-RO was signed to broaden the cooperation boundary to Europe. The MoU with Symantec 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

12. MyCERT Activity Report

Malaysian Computer Emergency Response Team – Malaysia

1. INTRODUCTION

1.1 CyberSecurity Malaysia

CyberSecurity Malaysia (www.cybersecurity.my) is the national cyber security specialist centre under the Ministry of Science, Technology and Innovation (**MOSTI**) of Malaysia. Previously known as the National ICT Security and Emergency Response Centre (**NISER**), CyberSecurity Malaysia became an agency under the purview of MOSTI in 2005 as the national body to monitor aspects of National e-Security. This is in line with the gazetted role by the Government for this agency to provide cyber security specialist services and continuous monitoring of cyber threats that have devastating impact to national security.

In essence, CyberSecurity Malaysia provides specialised cyber security services such as:

i. Cyber security emergency response, incident handling, and digital forensics.
ii. Cyber security quality management.
iii. Cyber security capability and capacity development.
iv. Cyber security outreach and acculturation.
v. Cyber security research and risk assessment.
vi. Cyber security evaluation and certification.

With all these services, CyberSecurity Malaysia has the vision of becoming a globally recognized national cyber security reference and specialist centre by 2020 while having the mission to create and sustain a safer cyberspace that promotes national sustainability, social well-being and wealth creation.

In delivering the services, CyberSecurity Malaysia has various departments with various expertises in cyber security. However, for the APCERT Annual Report, CyberSecurity Malaysia will give emphasis on services provided by the Malaysian Computer Emergency Response Team (**MyCERT**) Department.

1.2 The Malaysian Computer Emergency Response Team

MyCERT, a Department within CyberSecurity Malaysia, is the pioneering entity in providing incident handling services in Malaysia. It started in 1997 with 5 staff and presently has grown to 20 specialists. This Department serves as the point of reference for the country's Internet users in incidents handling 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 Centre

The Cyber999 Help Centre provides assistance for the Malaysian Internet users in detection, interpretation and response to computer security incidents.

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

i. Responded and resolved 9986 incidents in which 85% of the cases were resolved.
ii. Testified to court cases as Expert Witnesses.
iii. Published articles related to cyber security in newsletter.

1.2.2 The Malware Research Centre

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

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

1.3 Constituency

MyCERT 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, MyCERT will request assistance from its counterpart or trusted parties in resolving the matter.

2. ACTIVITIES AND OPERATION

2.1 Incident Handling Reports And Abuse Statistics

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

In 2012, MyCERT had produced:

i. 31 advisories
ii. 6 alerts
iii. 9 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/2012/main/index.html*

No	Type of incidents	Percentage (%)
1	Intrusion	43.3
2	Fraud	40.1
3	Malicious Codes	6.5
4	Spam	5.3
5	Cyber Harassment	3.0
6	Vulnerabilities Report	0.8
7	Intrusion Attempts	0.7
8	Denial of Service	0.2
9	Content Related	0.2

Figure 1: Type of incidents Handled by MyCERT in year 2012

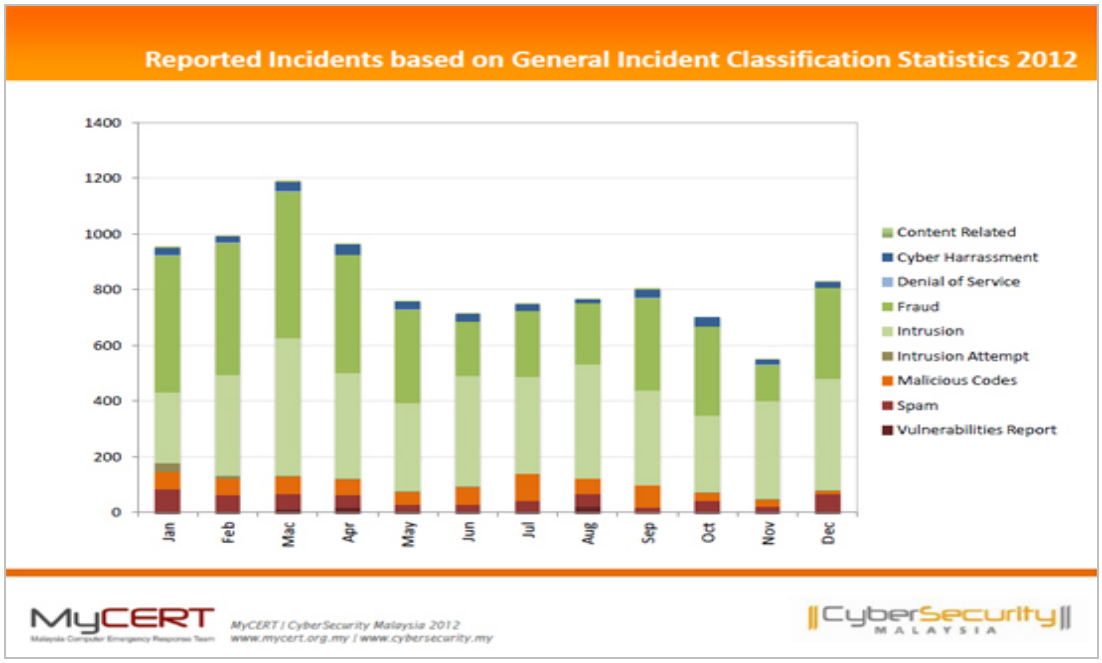


Figure 2: Reported Incidents Handled by MyCERT in 2012

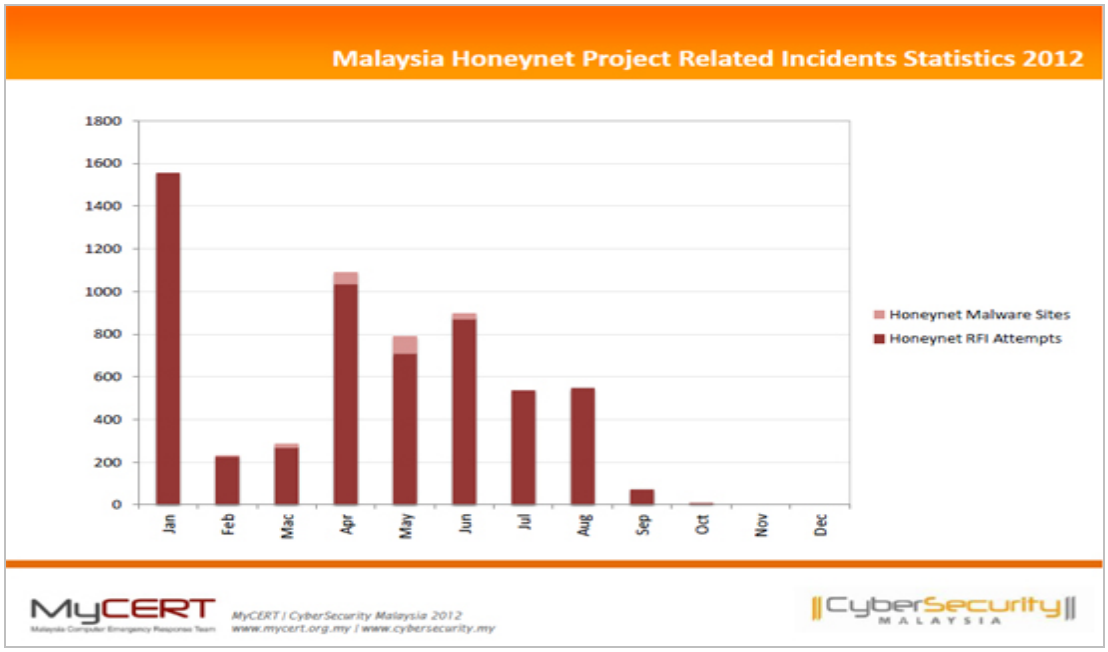


Figure 3 : Honeynet Project Related Incident Statistics in 2012

More information on Cyber999 statistics can be viewed at:
http://www.mycert.org.my/en/services/statistic/mycert/2012/main/detail/836/index.html

3. EVENTS INVOLVEMENT AND ACHIEVEMENTS

CyberSecurity Malaysia's MyCERT provides assistance in the area of cyber security by attending various information security activities training, seminars/conferences and meetings. Following are some of the activities:

3.1 Cyber Drills

MyCERT was involved in three major multinational Cyber Drills.

The cyber drills are:

i. APCERT Drill, 14 February 2012
ii. OIC-CERT Drill, 21 February 2012
iii. ASEAN CERT Incident Drill (ACID), 12 September 2012

3.2 APCERT Wiki

APCERT Wiki is a platform for communication and discussion among the APCERT members which currently hosted and maintained by MyCERT. More information of APCERT Wiki can be found at: *https://wiki.apcert.org*

3.3 Training

MyCERT staff attended various information security trainings. Several CERT specific workshops and hands-on training attended in 2012 include:

i. Malware Reversing Laboratory, HackInParis June, Paris (France)
ii. Reversing Android Malware, Honeynet Project, San Francisco (USA)
iii. Analyzing Malicious PDF, Taipei (Taiwan)

3.4 Presentations

CyberSecurity Malaysia through the MyCERT Department had been invited to various talks at international conferences or seminars as speakers. Among the distinguished events were:

i. BlackHat Euro, Amsterdam (Netherland)
ii. PacSEC, Tokyo (Japan)
iii. Reversing Malicious Flash, APCERT Knowledge Sharing
iv. Reversing Android Malware, Taipei (Taiwan)
v. Vulnerability Score in First TC, Tokyo (Japan)
vi. OIC-CERT Conference in Oman

3.5 Tools Developed

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

NO	Tool name	Description
1	DNSChanger Malware Detector:	Identify of DNSChanger malware infection machine in Malaysia.
2	Kelihos.B Malware Detector	Detector for Kelihos.B infection for Malaysian IP addresses.
3	MalShare (Beta)	Malware collection and classification.
4	TrueType Font Fuzzer	Research on security advisories MS11-077, MS11-087
5	rKaji	Return Oriented Programming (ROP) shellcode Analyzer
6	G-Decoder (Beta)	Universal JavaScript decoder for obfuscated JavaScript
7	WhoisHammer	Multiple domains whois information gathering
8	DontPhishME Terbang (v1.7.5)	Signature based and fully automated extension compilation
9	Metaware	MOSTI eScienceFund Project
10	MyLipas	provides web defacement feed scraped from many sources
11	BrowserInception	Experimental project demonstrating capability of PhantomJS and provides web page screenshot service to MyLipas

3.6 Articles

Year 2012 has displayed few articles by 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. GDI Font Fuzzing in Windows Kernel for Fun, BlackHat Euro 2012
ii. Code & Platform Level SQL Injections Defenses, Hakin9 Magazine

4. INTERNATIONAL COLLABORATION

4.1 Memorandum of Understanding (MoU)

Following are some of the official collaborations in matters of cyber security by CyberSecurity Malaysia:

i. MoU between CyberSecurity Malaysia and Japan Computer Emergency Response Team
ii. MoU between CyberSecurity Malaysia and Taiwan Information Security Centre National Cheng-Kung University
iii. MoU between CyberSecurity Malaysia and United Arab Emirates Computer Emergency Response Team (aeCERT)

4.2 New Partnership and Existing Cooperation

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

i. Chair and 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 are not OIC-CERT members.

5. FUTURE PLANS

For 2013, the main role of CyberSecurity Malaysia will be to secure the country's cyberspace. The agency is optimistic in expanding its services and explores new opportunities locally and internationally which will initiates awareness and understanding on issues and challenges in the area of cyber security.

Moreover, CyberSecurity Malaysia foresees more collaboration initiatives with foreign ministries, organizations, and CERTs/CSIRT for broader engagement in indentifying the latest technology and strategic approach toward securing the cyber space.

CyberSecurity Malaysia also look forward to enhancing the capability and capacity of the local cyber security industry. Internally, the agency is sending the staffs for training and certification in various security fields to acquire the appropriate skill sets in order to support the cyber security initiatives of the country.

On the international front, CyberSecurity Malaysia will continue to participate in international events such as conference, training and technical colloquium for knowledge sharing and interact with global technical expert from various areas of the cyber security domain. The agency will continue to drive the OIC-CERT

collaboration and to pursue cross border cyber security initiatives by establishing formal relationships focusing on collaborative activities.

6. CONCLUSION

The Malaysia's 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.

As the cyber environment does not conform to the physical boundary of the countries, international relations will remain as an important initiative. Therefore, 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.

13. SingCERT Activity Report

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 Trend

There is a increase in the total number of incidents reported to SingCERT in the year 2012 as compared to the year 2011.The significant increase in the reported incidents were due to the reported phishing incidents. The incidents included phishing emails targeting users and also phishing 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.

2.2 DNS Changer Incident

SingCERT collaborated with Internet Systems Consortium (ISC) on the DNSchanger incident and we monitored the situation closely till the shut down date (9th July 2012) of the compromised DNS servers. On top of that, SingCERT sent out advisory and worked with Singapore's major Internet Service Providers to inform the public about the incident and providing them with mitigation procedures.

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 2 seminars and workshops for the year 2012. 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 2012

The ASEAN CERTs Incident Drill (ACID) 2012 was conducted successfully on 12 September 2012. 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 Android Malware targeting online banking application. 12 CERTs from 10 countries from ASEAN and Asia took part in the drill, and good feedbacks were received from all the participants.

3.3 ASEAN Regional Forum (ARF) Incident Response Workshop 2012

The ASEAN Regional Forum (ARF) Incident Response Workshop 2012 was held in Singapore and it was jointly hosted by IDA/SingCERT and CERT Australia. The workshop was conducted in a table-top discussion manner, where the participants were provided with different sets of scenarios related to Cyber Security. There were a total of 68 delegates from 18 countries. Good feedbacks were received from the participants.

4. International Collaboration

4.1 Incident Drill

- SingCERT organised the ASEAN CERT Incident Drill (ACID) in September

2012

- SingCERT participated in the APCERT Annual incident drill in January 2013.

5. Future Plans and Projects

SingCERT will be organising the 8th ASEAN CERTs Incident Drill for the year 2013. Discussions are in progress to work out the scope and coverage.

14. Sri Lanka CERT | CC Activity Report

Sri Lanka Computer Emergency Readiness Team Coordination Centre – Sri Lanka

1. About Sri Lanka CERT

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 nine team members consisting of the Chief Executive Officer, a Principal Information Security Engineer, an Administrative Officer, five Information Security Engineers and an IT Assistant.

This team is supported by four undergraduate interns. All the staff are highly skilled and experienced in different areas of information security and have achieved corresponding Information security certifications which are widely recognized in the industry, such as SANS GCIH, Microsoft MCSE, EC-Council Certified Ethical Hacker (CEH) and Certified Hacking Forensics Investigator (CHFI), Cisco CCNA and CCSP and (ISC)² CISSP.

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

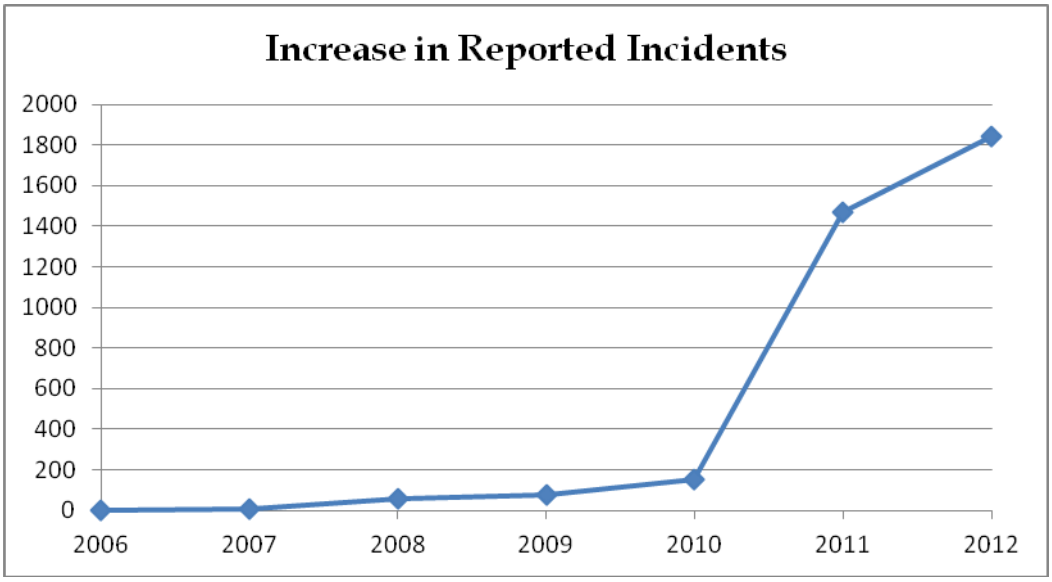
2.1 Incident Handling Statistics

Incidents reported to Sri Lanka CERT increased to 1,840 in the year 2012. In the year 2011, it was 1,469 incidents were reported. This is a 25% increase in reported incidents compared to the year 2011. 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	3
Abuse/Privacy	16
Scams	3
Malware	0
Defacements	15
Hate/Threat Mail	1
Unauthorized Access	1
Intellectual property	0

violation	
DoS/DDoS	1
Fake Accounts	1,800
Total	**1,840**

The following graph depicts the increase in the number of incidents since the inception of Sri Lanka CERT in mid-2006.



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. The Bank CSIRT is already operational while the Defence CSIRT is in its implementation stage and 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 has now transformed 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 implements security standards to ensure a minimum level of security compliance within the industry.

2.2.2 Incident handling - blocking Phishing sites

Since it takes considerable time to take down the phishing sites targeting local banks of Sri Lanka, a process was established to block the sites locally with the help of TRC (Telecommunication Regulatory Commission) Sri Lanka and the ISPs. This will minimize the damage caused to on-line banking customers during the time of taking down those phishing sites with the help of international CERTs and ISPs.

2.2.3 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 the first 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.

2.2.4 Vulnerability Assessments – Formal procedure for security testing government websites

In year 2012 all of the government website assessments were carried out according to the formal procedure which was established in year 2011 by Sri Lanka CERT with ICTA and GIDC NOC involvement. ICTA was the primary

contact point when dealing with website security assessments for government sites which are hosted at GIDC NOC. Sri Lanka CERT produced all of the assessment reports and final approval for website hosting documents based on a format which was agreed by both ICTA and Sri Lanka CERT.

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 2012 Sri Lanka CERT conducted the following training and education programs successfully:

a. Presentation on "First Responders responsibility on computer related crimes"
b. Seminar series on "Internet safety for School Children" for School Children

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 2012 included;

a. Security Policy development workshops for government organizations
b. Forensics investigation support for Law enforcement
c. Configuration reviews for critical government organization information systems

d. Network Security assessments for several banks
e. Application security assessments for financial institutions
f. Investigation of a financial fraud in a leading bank

3.3 Seminars & Workshops

a. Cyber Security Week 2012

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.

The objectives of this program are to:

- Build awareness and update knowledge on key security areas that matter both locally and globally, commercially and personally
- Understand emerging technologies and the security issues pertinent to those technologies
- Provide a meeting ground for like minded individuals with a special interest in information security to forge alliances, share knowledge and experience and build consensus on security issues of the day

The flagship event of CSW each year is the Annual National Conference on Cyber Security.

Cyber Security Week 2012 was held in the month of December, and featured a series of events:

- Annual National Conference on Cyber Security

- Two full-day Workshops for professionals, namely:
  - Technical workshop on "OWASP ESAPI: making it work for you"
  - Technical workshop on "Practical secured software security testing"

- 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.

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-2011 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;

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

Sri Lanka CERT is represented on the board and steering committee of the Information Systems Security Association (ISSA) Sri Lanka Chapter, and is

involved in the planning its membership drive and strategic partnership formation efforts

Sri Lanka CERT is also actively supporting the formation of SLSEC, a proposed online forum where security enthusiasts can get help from fellow security enthusiasts. The forum will be managed by a governing body consisting of Sri Lankan representatives in Sri Lanka as well as overseas. The site will be hosted and managed, by Sri Lankan expatriates.

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, 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 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 25th -28th, 2012

APCERT AGM & Conference
Bali-Indonesia

April 20th - May 5th, 2012
USTTI training on cyber security
Washington, USA

June 16th -25th, 2012
FIRST AGM & Conference
Malta

July 6th –8th, 2012
CISSP Asian item writing workshop
Singapore

July 7th –14th, 2012
APISC training (KrCERT | CC)
Seoul, Korea

October 24th – November 3rd, 2012
CyberLympics at HackerHalted
Miami, USA

October 19th – 31st, 2012
USTTI training on cyber security
Washington, USA

November 16th, 2012
Asian Oceanian Computing Industry Organization (ASOCIO) International Conference 2012, Cyberjaya, Malaysia

5.3 International incident coordination

Sri Lanka CERT | CC actively participated in the APCERT Drill 2012 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, 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;

a. Development and Implementation of the National Certification Authority
b. Implementation of the Telco CSIRT
c. Development and implementation of the Defense CSIRT
d. Conceptualization, development and implementation of the Edu-CSIRT
e. Cyber Security Week 2013

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:

a. Recruitment of undergraduate students on internships on an annual basis to enhance the information security capabilities of the younger generation.
b. 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 starting Sri Lanka CERT in year 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 increase in number of incidents reported and handled by Sri Lanka CERT in the past consecutive years.

During this year most of the incidents reported to Sri Lanka CERT were related to phishing sites and various activities conducted through social networking sites, 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 2012 were very successful and had huge demand. We will continue to conduct the Annual Computer 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.

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.

15. TechCERT Activity Report

TechCERT – 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. Companies 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 programmes on safe use of computers and the internet.

1.2 TechCERT Technical Team

The present technical staff strength of TechCERT is 17 personnel and their professional qualification status is listed below (please note that most staff members have multiple qualifications in different areas of information security, computer systems security, network security specializations):

PhD	3
MEng/MSc/MPhil	7
PG Diploma	3
BSc Eng/BSc/BIT	16
C|EH	4
C|HFI	1
Certified ISMS Auditor (ISO27000)	2
MCSE/MCSA	1
MCP	1
BCS	1
CCNA / CCNA Security	5
Chartered Engineers	3

1.3 Constituency

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

2. Activities & Operations

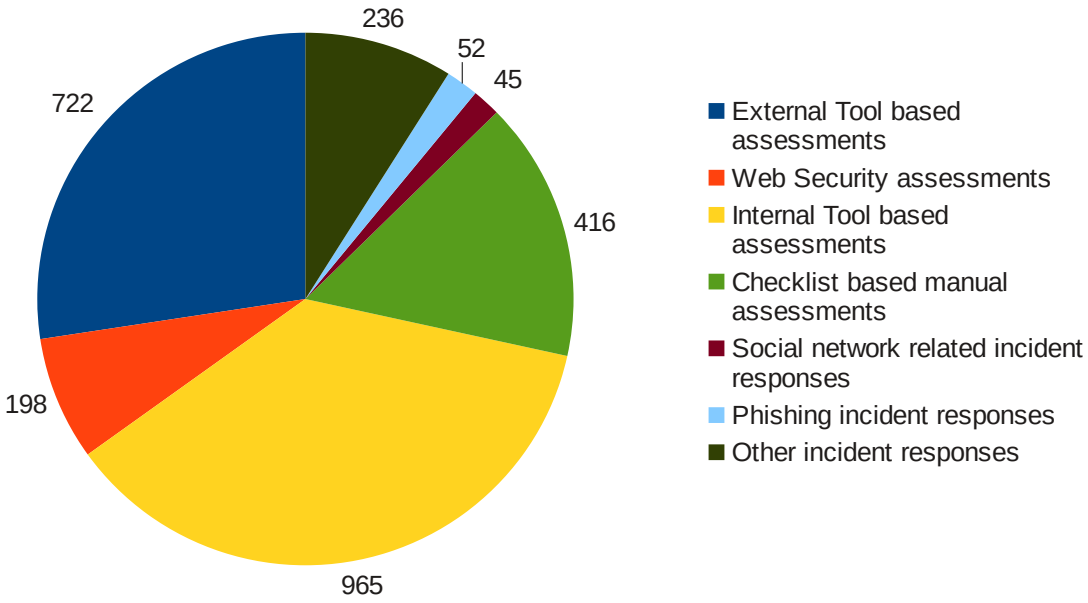
The TechCERT Managed Security Services include a range of engineering and consultancy services:

- 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
- 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 Activity Chart for 2012

Activity Type	Count
External Tool based assessments	722
Web Security assessments	198
Internal Tool based assessments	965
Checklist based manual assessments	416
Social network related incident responses	45
Phishing incident responses	52
Other incident responses	236



2.2 Organizing of Training Seminars, Workshops and Demonstrations

10th May 2012 **CBSL (Central Bank of Sri Lanka) Workshop**

TechCERT conducted a workshop on information security concepts, Policies, security threats and APT for the Financial sector officials in Sri Lanka on 10th May 2012 at CBSL Training center

25th/31st January 2012 **Forensic Training to Sri Lanka Army**

TechCERT conducted a series of training sessions for the Sri Lanka Army on Digital Forensic Investigations

21-22nd February 2012 **Internet Forensics and Malware Analysis Workshop - Team Cymru**

TechCERT organized a workshop on Internet forensics and malware analysis together with Team Cymru

18th May 2012 **Cyber Security Awareness Program for the Governor Central Province**

TechCERT conducted an awareness program on cyber security for the personnels at the office of Governor Central Province

05th June 2012 **Information Security Wokshop at Elizebeth Moir School**

TechCERT conducted a workshop on Information Security at the Elizebeth Moir School, Colombo, Sri Lanka.

09th January 2012 **Seminar on "Safe Use of Internet" at Sabaragamuwa University**

12th July 2012 **Technical Presentation & Demonstration at NITC Conference 2012**

TechCERT conducted a technical presentation on "Insider Threat The Nightmare Scenario of a good Employee Gone Bad" and a demonstration at the workshop organized parallel to the NITC Conference 2012

13th July 2012 **Technical Workshop on "Defending against Digital Zombies on Cyber Space" at CSSL**

TechCERT team conducted a full-day workshop on "Defending against Digital Zombies on Cyber Space" for the general public at the National IT Conference Workshop organized by Computer Society of Sri Lanka

24th October 2012 **Technical Presentation at Bank CIO Forum**

TechCERT conducted an awareness program on Phishing Attacks & introduced 'PhishHOOK' to government & private banks of Sri Lanka

March 2012 **Technical Presentation at the Terrorist Investigation Department (TID)**

Dr. Chandana Gamage of TechCERT conducted a technical presentation for the TID Officers of the Sri Lanka Police on SAARC Regional Terrorism

Offense Information Systems

March 2012 **Seminar on desktop application security**

A seminar was conducted on 'Desktop Application Security' for the Information Technology Officers at Ministry of Education, Sri Lanka under eMIS project

8th February 2012 **Quiz Competition on Cyber Security**

TechCERT conducted a quiz competition on Cyber Security at Anula Vidyalaya, Colombo, concurrent to the IT Day of the College

19th June 2012 **Seminar on Cyber Security**

TechCERT conducted a seminar on 'Cyber Security' at Museaus College, Colombo 7

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

22nd June 2012	Sangamiththa Vidyalaya, Galle
26th June 2012	Southland College, Galle
20th September 2012	Kekirawa Central College, Anuradhapura
21st September 2012	Ganthiriyagama Vidyalaya, Anuradhapura
15th October 2012	Samudradevi Vidyalaya, Colombo
17th October 2012	Nalanda College, Colombo

17/22nd October 2012	Malabe Sri Rahula Vidyalaya, Colombo
17th January 2013	Bomiriya Central College, Colombo
17th January 2013	Ananda Shasthralaya, Colombo

2.3 Participation in Conferences, Workshops and Training Programmes

1. Dileepa Lathsara, COO TechCERT participated for the, FIRST, 24th Annual Computer Security Conference: "Security is not an island." Held in the Portomaso, St. Julian's, Malta, 17-22 June 2012
2. Kushan Sharma and Nalinda Herath participated for the APCERT AGM and Conference 2012 held at Bali, Indonesia, 25-29 March 2012
3. Kushan Sharma participated in ERU Conference 2012, organized by University of Moratuwa, Sri Lanka.

2.4 Cyber Security Drills

14th February 2012	**APCERT Cyber Security Drill 2012** TechCERT participated in the Drill as a member of the Organizing Committee and acted as the head of EXCON
28th August 2012	**Cyber Security Drill for Sri Lanka Bank** TechCERT conducted a cyber security drill for the Sri Lankan Banking Sector on 'APT and Coordination within Sri Lanka'
05th September 2012	**Cyber Security Drill for Sri Lanka Financial and Manufacturers** TechCERT conducted a cyber security drill for the major financial organizations within Sri Lanka on 'APT and Coordination within Sri Lanka'

3. Achievements

3.1 Technological Achievements

- Improvements for the "PhishHook" Phishing Early warning system and increase in number of deployments within Sri Lanka
- Development of a Knowledge base for Incident response support
- Improvements for the DNSSEC integration project in to LK Domain
- Establishment of an inhouse R&D division

3.2 Technical Publications

- Kushan Sharma and Chandana Gamage, "Building Sand Castles within IaaS-based Cloud Instances", 18th ERU Research Symposium 2012, Faculty of Engineering, University of Moratuwa, Sri Lanka, December 2012. (ISSN: 1391– 999)

- Asanka Balasooriya and Dr. Shantha Fernando, "Next Generation Security Framework to Detect Botnets on Computer Network", in the proceedings of the 2nd International Conference on Security Science and Technology, Singapore.

4. 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

5. 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 other Financial Organizations in Sri Lanka.

Similar to year 2011, there was a significant increase in phishing attacks and web site hacking incidents in Sri Lanka in 2012. 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.

16. ThaiCERT Activity Report

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.

ThaiCERT
Thailand Computer Emergency Response Team
a member of ETDA

ETDA

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 11 full-time staffs consisting of 1 director, 2 security specialists and 8 computer engineers.

Activities & Operations

Abuse statistics

Reported Incidents Received from E-mail

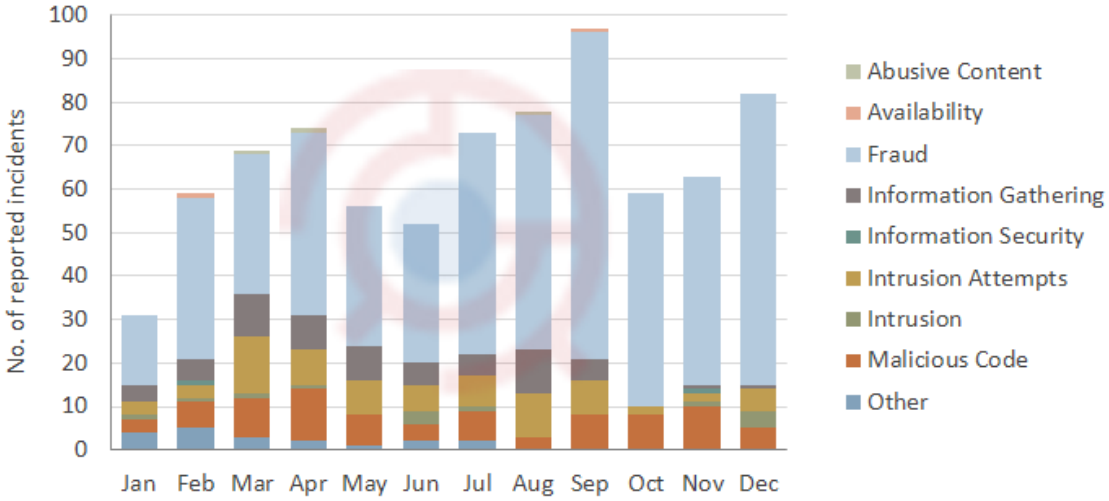


Figure 1: The number of reported incidents in 2012

In 2012, ThaiCERT received a total of 792 reported incident cases (tickets) through the official e-mail address. The received tickets per month varied approximately between 30 to 100 tickets as shown in Figure 1, relatively lower than the second half of the previous year.

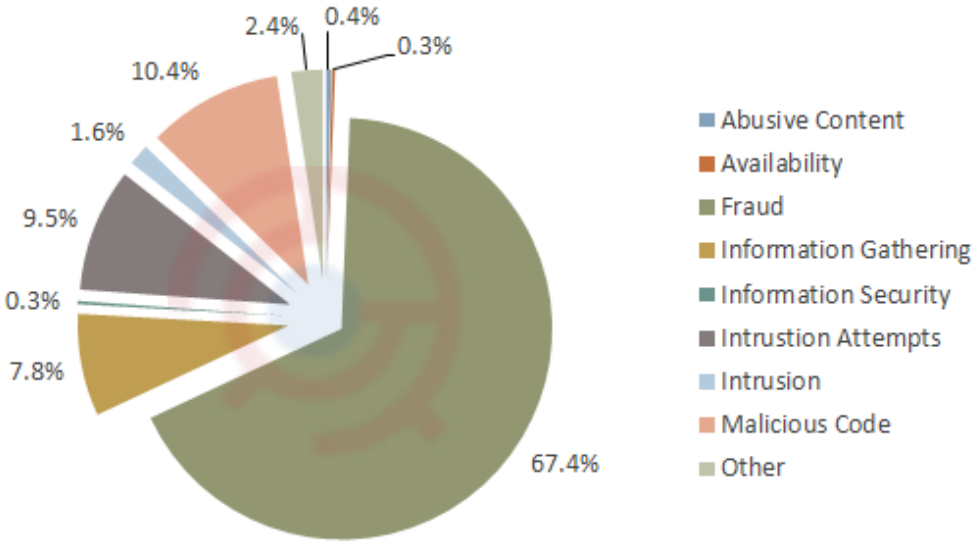


Figure 2: The proportion of reported incidents by incident type in 2012

In reference to the received tickets classified according to eCSIRT incident

classification[1], it was obviously that Fraud, dominated in reported incident types with 67.4%, where all Fraud cases in this statistics were phishing. Malicious Code was the follow-up incident type with 10.4%. Intrusion Attempts and Information Gathering, which was mostly in relationship with unauthorized scans and login attempts on remote access services such as SSH, were ranked in the third and fourth with 9.5% and 7.8% respectively. In brief, the ranking of incident types was similar comparing with the previous year, where Malicious Code went up to the second position while Intrusion Attempts and Information Gathering remained in the top four reported incident types.

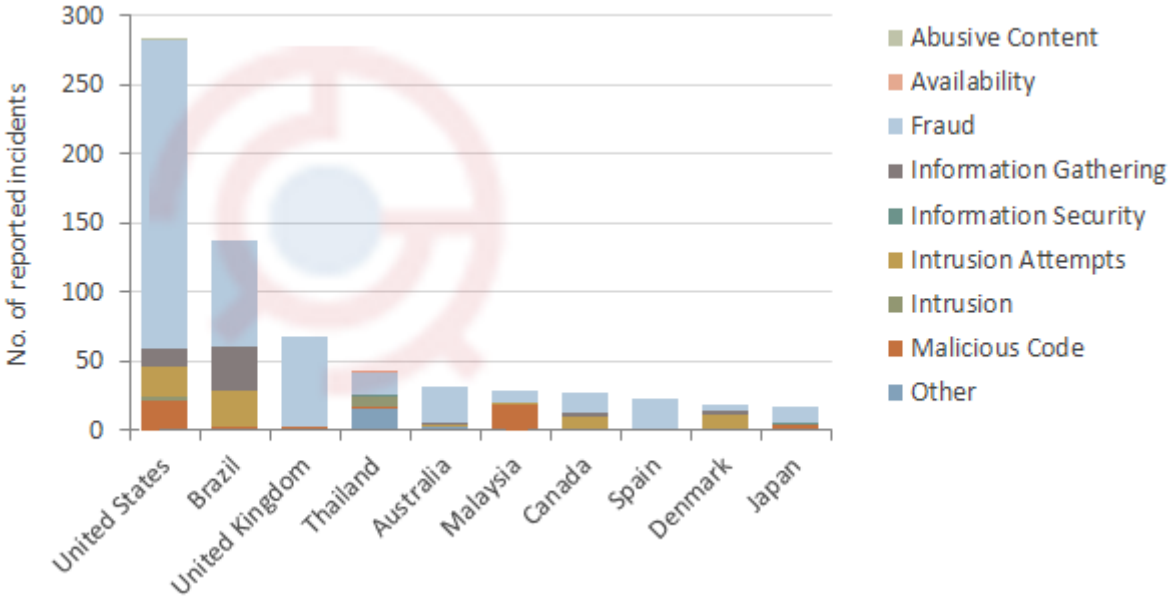


Figure 3: Top 10 incident reporters by country in 2012

Regarding the incident reporters classified by country, Figure 3 shows that most of the security incidents were reported by the United States with 36%. Brazil came in the second position with 17%, followed by United Kingdom with 9%. When the incident type (excluding Fraud) was taken into consideration, it can be seen that Brazil reported most of the Intrusion Attempts and Information Gathering incidents; while United States and Malaysia reported most of the Malicious Code incidents.

Reported Incidents Received from Automatic Feeds

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

As of early August 2012 after ThaiCERT had collaboration with APWG and Team Cymru, ThaiCERT received information consisting 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, also are going to provide our own automatic feeds to other relevant Internet Service Providers (ISP) as well. An overview of the received information can be seen in the following figure.

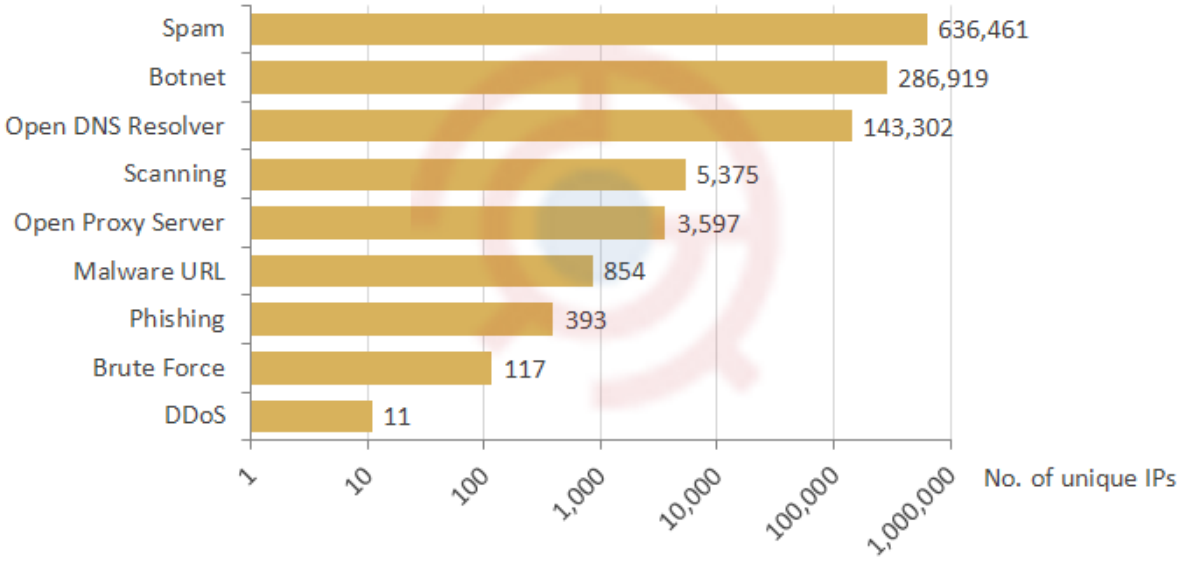


Figure 4: Top incident types by number of unique IPs between early August and December 2012

Approximately a million unique IP addresses were reported from the feeds within less than five months. It can be seen from Figure 4 that most systems were compromised and were used as a base for spreading spam messages with 59% followed by the systems being a part of botnet with 27% in which 11% of them shared between both categories. Open DNS resolver, a DNS server that was improperly configured to allow recursive queries from the public, was ranked in the third with 13%. Other interesting statistics, for example, a top five malwares relevant to botnet were Zeus (40%), Kelihos (13%), irc-botnet (12%), Feodo (8%), and Conficker (6%).

Rustock and Zeus Botnets

In the late of 2011, ThaiCERT had an effort to coordinate with Microsoft to support the operation after taking down the Rustock botnet by analyzing information received from Microsoft about Rustock-infected computers located in

Thailand and contacting with relevant parties in order to deal with infected hosts under their control. Moreover, Microsoft also reported information related to Zeus-infected computers in late of June 2012 and operated in the same approach as the previous case.

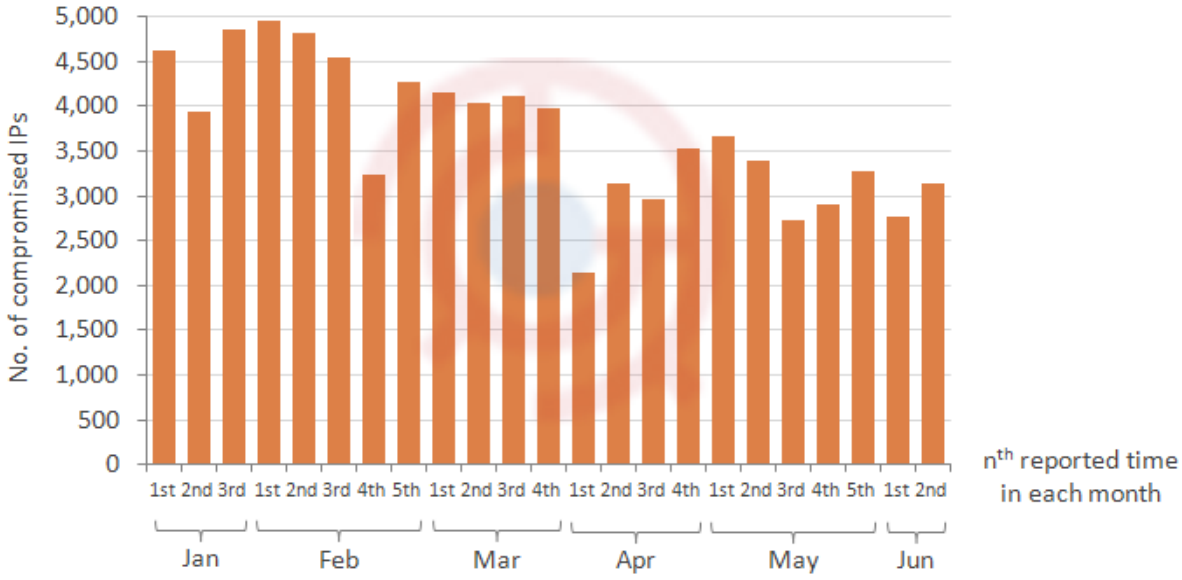


Figure 5: Number of reported compromised IPs by Rustock between January and June 2012

In regard to the reported Rustock-infected hosts information as shown in Figure 5, almost 90,000 IP addresses were received in total and between 2,000 - 5,000 IP addresses each time. The average number of reported IP addresses slowly decreased month by month since ThaiCERT continuously contacted with affected organizations asking for collaboration to deal with compromised IP addresses, until any Rustock report was received from Microsoft.

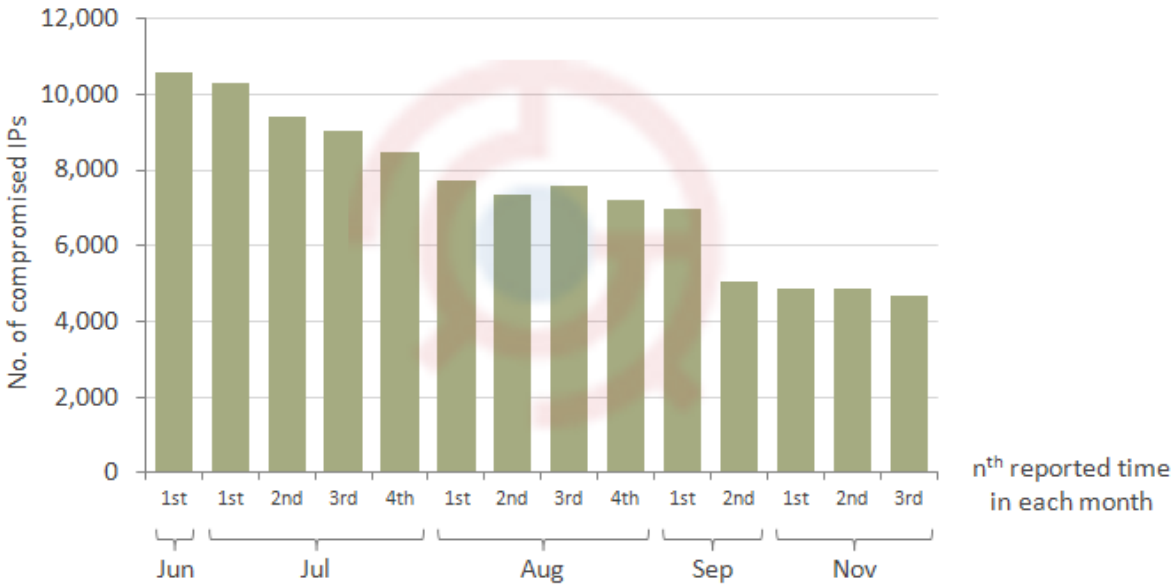


Figure 6: Number of reported compromised IPs by Zeus between June and November 2012

Apart from the Rustock malware, in the same period of 2012, ThaiCERT received a report of compromised hosts by Zeus with approximately 10,000 IP addresses as seen in Figure 6 and decreased down to approximately 4,700 IP addresses in late November, the last time ThaiCERT received a report. ThaiCERT followed the procedure as done in the Rustock case by contacting with relevant ISPs to handle with those reported IP addresses.

New Operation

Digital Forensics

Digital forensics became one of ThaiCERT main operations since January 2012 for the purpose of establishing a digital forensics lab to support an investigation process which was normally done by law enforcement agencies. Since it was a new emerging operation, coordination with relevant parties in order to create a collaboration network with local and international organizations, became the first priority to be achieved. With regards to knowledge and skill development, our staffs participated in a number of seminars and trainings organized by Thailand's Department of Special Investigation (DSI), Asian Forensic Sciences Network (AFSN), and INTERPOL. They currently hold international digital forensics-related certificates liked IACIS Certified Forensic Computer Examiner (CFCE) and more.

Activities

Training

Co-organized:

- Java and Android Secure Coding training (co-organized with JPCERT/CC), Bangkok, Thailand, April 2012
- Securing Networks training (co-organized with ITU-IMPACT), Bangkok, Thailand, September 2012
- Participated:
- 6th INTERPOL Train-the-Trainer Workshop on Computer Forensics training, Thailand, August 2012
- Etc:
- Invited to be a trainer of Basic Understanding of CSIRT and Incident Response training co-organized by JPCERT/CC and LaoCERT, Vientiane, Laos, October 2012

Drill

Participated:

- APCERT Drill 2012 under the theme "Advanced Persistent Threats and Global Coordination", February 2012
- ASEAN CERT Incident Drill (ACID) 2012, September 2012
- International Cyber Defense Workshop (ICDW) 2012-2, November 2012

Seminars

Participated:

- 45th TEL Working Group Meeting, Da Nang, Vietnam, April 2012
- 1st Meeting of ASEAN Network Security Action Council, Brunei, June 2012
- ASEAN-Japan Workshop on International Security, Brunei, June 2012
- 24th Annual FIRST Conference 2012, Malta, June 2012
- Annual Technical Meeting for CSIRTs with National Responsibility, Malta, June 2012
- Security and Prosperity Steering Group (SPSG), Russia, July 2012
- ASEAN Regional Forum (ARF) Cyber Incident Response Workshop, Singapore, September 2012
- 3rd APT Cybersecurity Forum, Macau, September 2012
- Asian Forensic Sciences Network 4th Annual Meeting & Symposium,

Thailand, November 2012

- Kyoto 2012 FIRST Technical Colloquium, Kyoto, Japan, November 2012

Certifications

ThaiCERT staffs currently hold the following professional security certificates:

- (ISC)² CISSP
- GIAC GSEC
- GIAC GPEN
- IRCA ISO/IEC 27001 ISMS Lead Auditor
- IACIS CFCE
- EnCase EnCE
- CompTIA Security+

International Collaboration

MoU

JPCERT/CC

ThaiCERT signed an MoU with JPCERT/CC for collaboration and support on information security development, along with exchanging knowledge between both teams and co-organizing academic trainings. In addition, JPCERT/CC also organized on-the-job, incident response and malware analysis trainings for ThaiCERT staffs at JPCERT/CC headquarters, Japan in September 2012.

Symantec

Enhancing the capability to deal with cybersecurity threats, ThaiCERT and Symantec had an agreement to establish a system for detecting unauthorized attempts and analyzing gathered information.

APWG

After signing an MoU with Anti-Phishing Working Group (APWG), a non-profit research firm, for collaboration on resolving the phishing issue; APWG then provides information of real-time phishing websites for ThaiCERT to be able to use in order to coordinate with any impacted entity and resolve the problem efficiently.

Team Cymru

By joining Team Cymru's CSIRT assistance program, ThaiCERT received such a

useful information to analyze the impacted ISPs; then coordinate with the team for the purpose of reducing an amount of infected and vulnerable hosts in Thailand.

17. TWCERT/CC Activity Report

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

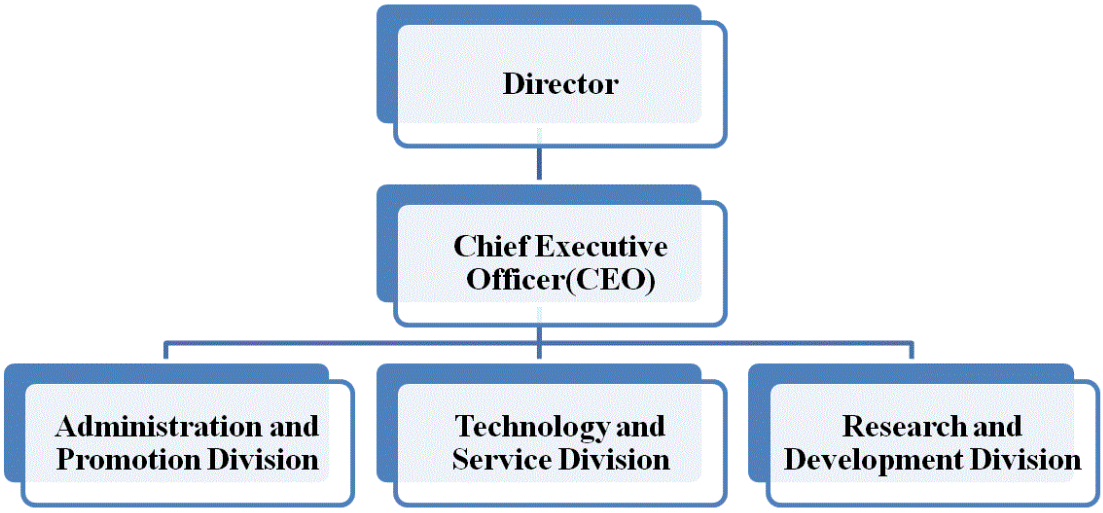
TWCERT/CC formally established since 1998. The major purposes of TWCERT/CC are to prevent and actively assist the computer and network security incidents in Taiwan, to analyze the system vulnerabilities, to provide computer and network security tools and related documents for the system administrators 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	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012
Total	1260	5318	2874	1824	788	660	1087	679	1094	6666	8,126

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.

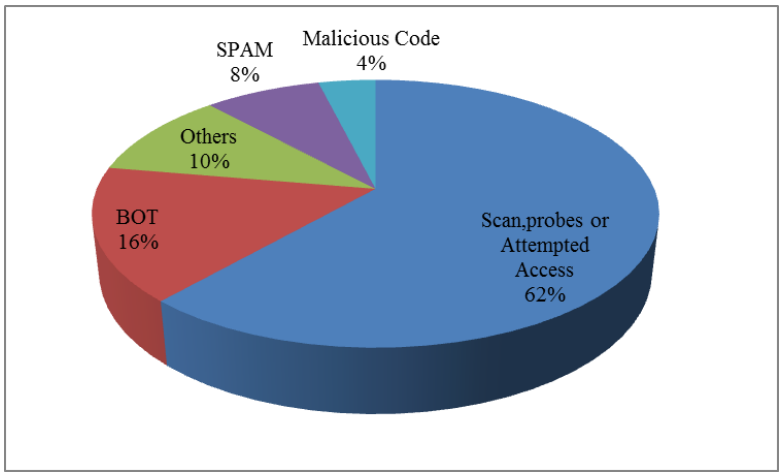


Figure 1. TWCERT/CC incident response classification statistics

■ **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	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012
Advisory	258	142	197	140	138	119	49	44	234	98	115

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.

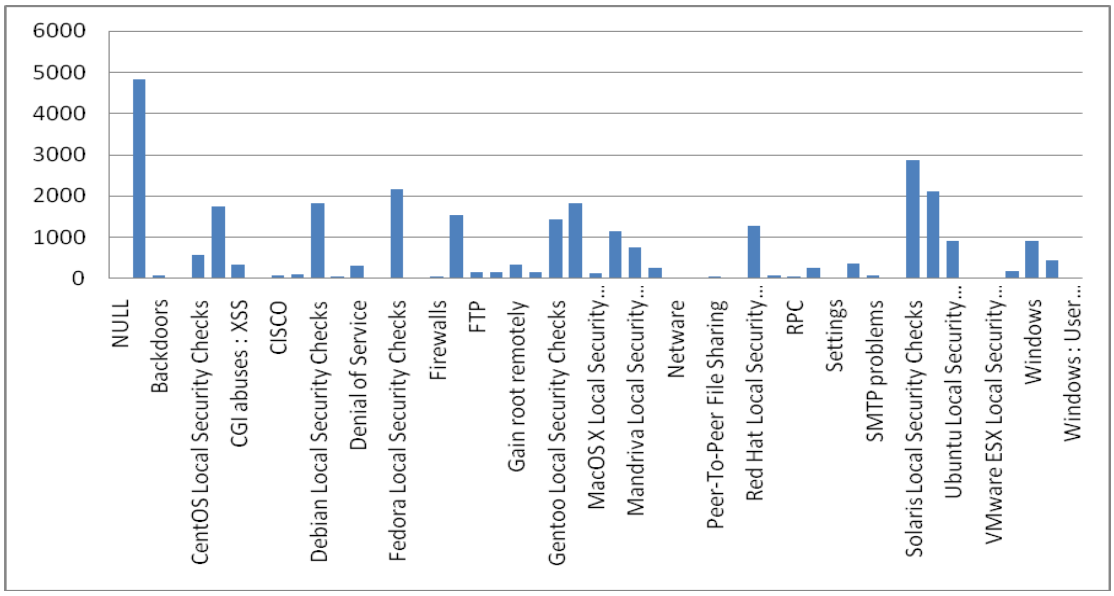


Figure 2. Categories of TWCERT/CC Vulnerability Database

■ 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 2012 and originated from 136 countries. The geographic distribution of the spam sources is shown in Figure 3 and the amount of the spam over the year of 2012 in Figure 4.

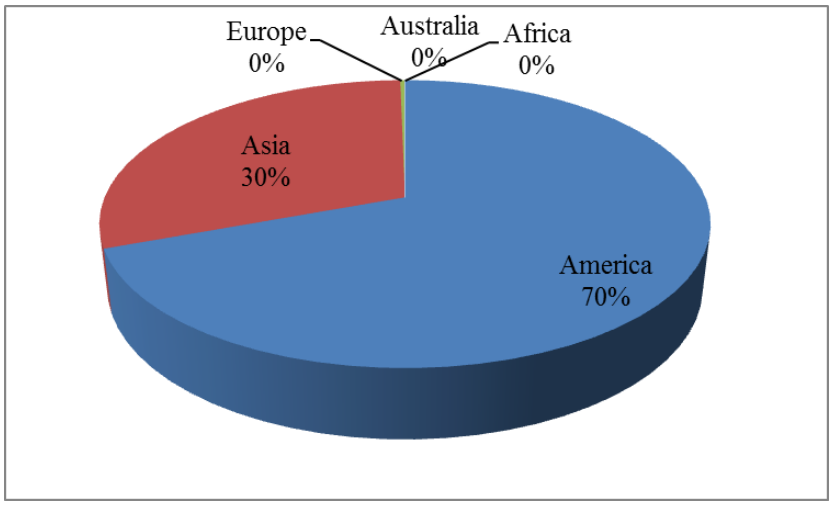
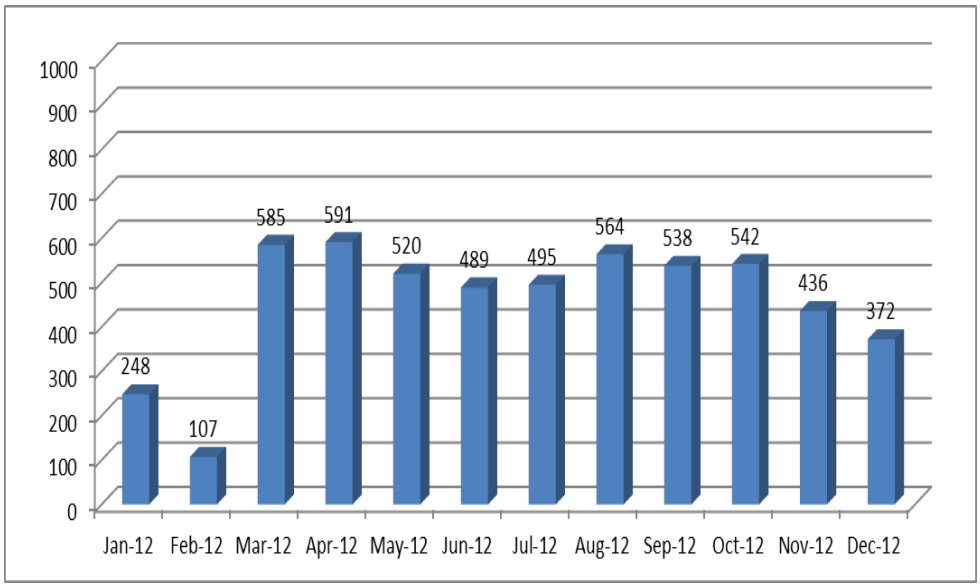


Figure 3. Geographic distribution of the spam sources.



Unit : One Hundred

Figure 4. The amount of spam each month in 2012.

2.3 New Service: 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
2012/11/15	Penetration Testing
2012/11/13	Penetration Testing
2012/11/09	Penetration Testing

2012/10/24	DDOS Attacks and Defense
2012/10/23	Wireless Network Security
2012/09/07	Web Application Security
2012/08/20	DNSSEC – Linux /BIND
2012/08/12	The analysis of Malicious code and Digital Forensic
2012/07/11	DNSSEC – Linux /BIND
2012/06/12	The analysis of Malicious code and Digital Forensic
2012/06/10	Wireless Network Security
2012/05/18	Network Traffic Analysis
2012/05/17	Network Traffic Analysis
2012/04/16	The analysis of Malicious code and Digital Forensic

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 2012. Total of 4,077 educational institutions and over ten thousands of security officers were involved in this drill program with a high completion rate of 99%.

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 2003 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.

18. VNCERT Activity Report

Vietnam Computer Emergency Response Team – Vietnam

1. About VNCERT

1.1 Introduction

VNCERT is an agency under Ministry of Information and Communications of Vietnam, established by decision of Vietnam's Prime minister in December, 2005. In Vietnam, VNCERT is responsible for state management of information security area.

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.
- Guide deploying process of the Anti-spam Law in Vietnam.

1.2 Staff and structure

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 Da Nang city.

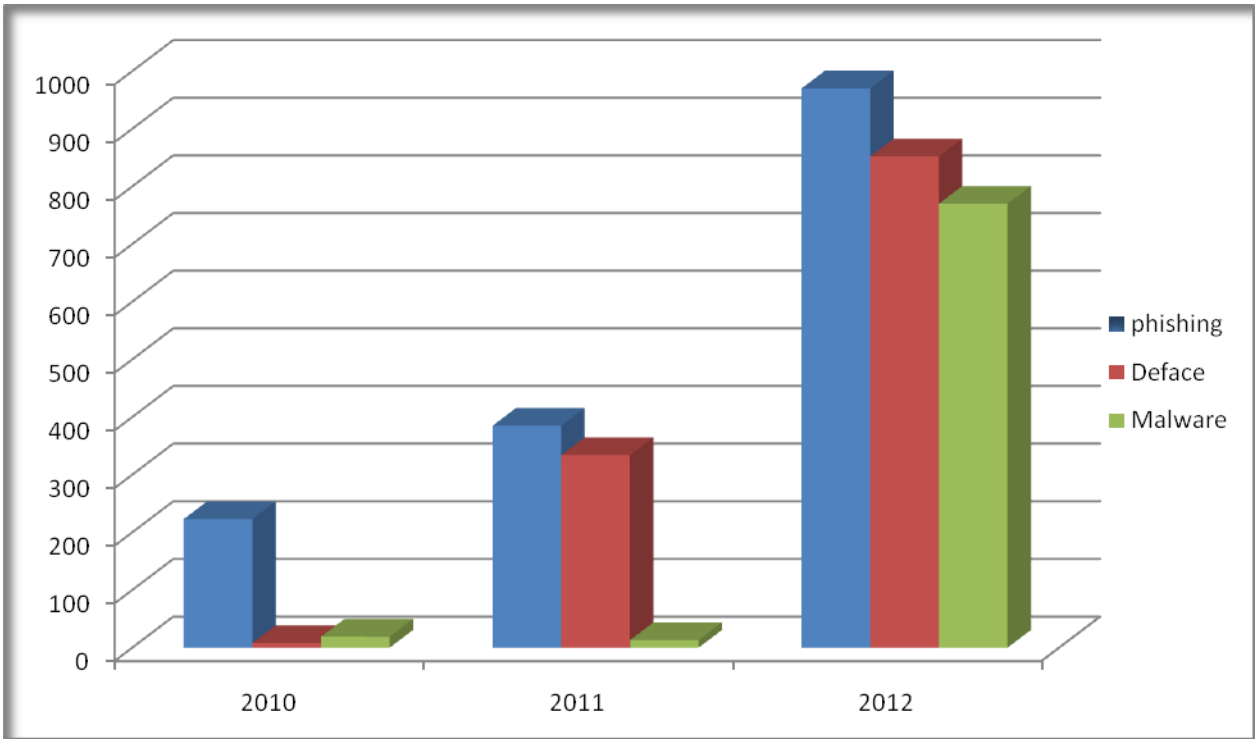
Current number of employees in VNCERT is about sixty.

2. Activities & Operations

2.1 Incident reports & handling

In 2012 the total number of incidents were reported to VNCERT was 2179 in

which there are 970 phishing cases, 852 malwares, 770 defaces. Almost of phishing cases related to finance, commonly forging banks' website. On 2012, number of malwares that spread by email on office files raised, they stole passwords of email accounts, documents and other personal information.



Picture 1: Incidents in Viet Nam since 2010, 2011 and 2012.

2.2 Coordinating, warning and supporting activities

We are collecting security news from many sources including international organizations, NGO or Internet users, and make thousands warning to organizer in Vietnam.

We supported 254 agencies and organizers to audit information security.

From 2012, we have started warning government agencies about malwares on their information system.

We supported 64 organizations to handle incidents.

We are doing research and analysis to make alerts to communities about new vulnerabilities, threads and new dangerous malwares.

We are protecting online programs of government and supported LAOCERT to ensure network of ASEM event.

2.3 Anti-spam activities

Release the new Decree 77/2012/ND-CP about Anti-spam, Amending and Supplementing Decree for Decree 90/2008/ND-CP that focus on Anti SMS spam.

2.4 Legal environment improvement

VNCERT is drafting the Information Security Law.

3. Events organized / Co-organized

3.1 Training & Drills

In 2012 VNCERT arranged some training courses for raising information security awareness as well as working experience in Information Security field to staff in some organizations and an expert training program in malware code analysis

We have organized some training courses about information security (including CHFI, ICSA/LPT, and CISSP) for employees.

We participated in 02 international drills: ASEAN CERTs Incident Drill (ACID 2012) and APCERT Annual Drill 2012.

We cooperated with VNISA to organize the Information Security Contest for Students that is one of the activities of the Vietnam Information Security Day 2012.

3.2 Seminars & Etc

We co-operated with Ministry of Public Security and IDG Vietnam Corporation to organize annual event "Security World 2012", CSO Conference & Award 2012

We co-operated with VNISA to organize the conference “Information Security in E-government” and to organize the annual event “National Information Security Day 2012” with theme “together to build secure information infrastructure for the national sovereignty of the country".

4. International Collaboration.

We renewed the MOU with JPCERT.

We supported international organizers to remove the phishing sites in Vietnam.

We participated in some annual conferences such as APCERT Meeting 2012, MERIDIAN Conference 2012, APECTEL 45, National CERT Meeting 2012…

We participated in the events of ASEAN-Japan cooperation program on IS awareness raise for communities.

We supported some foreign partners to research information security current status in Vietnam.

5. Future Plans

Finish the Information Security Law to Submit to Government.

Deploy the anti-botnet project that will remove the biggest botnet on the cyberspace in Vietnam.

Organize the drill for government agencies in Vietnam with participation of ISP and information security companies.

Build botnet database and IP database of organizers to early warn about infected malware computers in government agencies.

Strengthen information sharing channels to deliver and receive cyber security information nation-wide.

Organize the conference on coordinate and incident response.

Build mechanism to sharing spam information with countries (Japan).

Participate actively in the collaboration activities among APCERT and ASEAN CERTs, improving exchange experiences activities;

6. Conclusion

For better protecting the cyberspace in Vietnam, in 2013 we focus on:

- Completing the legal framework on information security, especially the draft of Information Security Law,
- Building mechanism to sharing network security information between VNCERT and local or oversea organizations.
- Enhancing the cooperation among the CSIRTs network in Vietnam
- Building the Network Monitoring System and starting to collect and monitor information security.

General Members

19. bdCERT Activity Report

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 2012 as compare to the year 2011. In year 2012, bdCERT has received 276867 incident reports, which has been originated from 37885 unique IP. Taxonomy statistics of incidents report are shown in figure 1. Majority of incidents are related with Spam, Open Resolvers and bots.

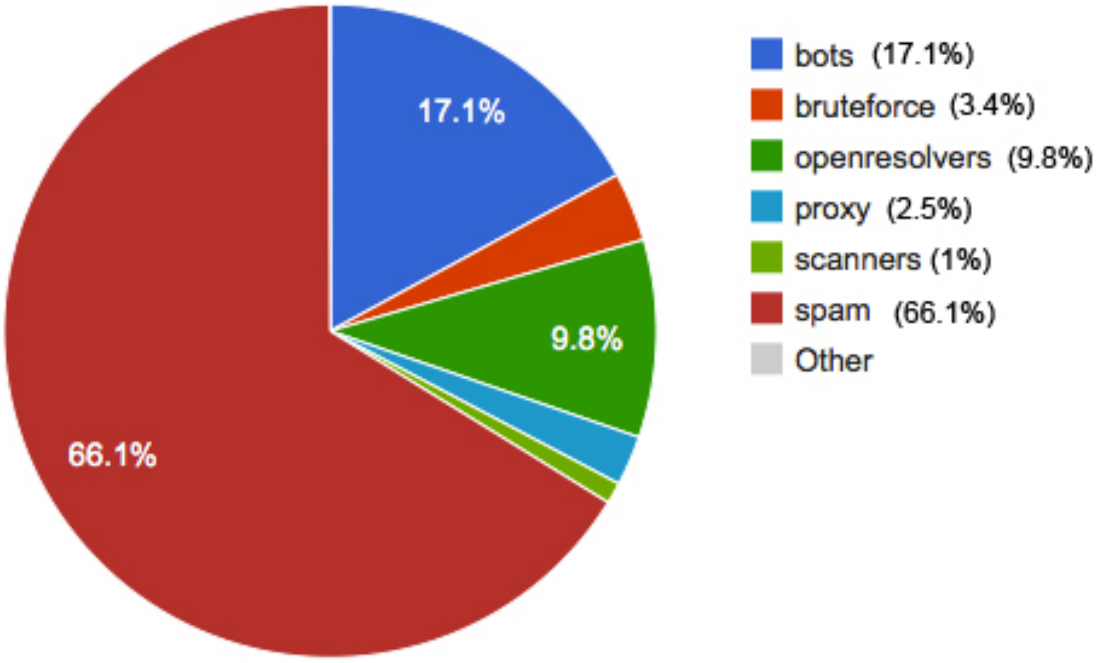


Figure 1 : Taxonomy statics of Incident Response.

2.2. New Services

a) In year 2012, bdCERT introduce ASN based abuse report for the ISP. From bdCERT ASN Portal; ISP can get abuse report based on their Autonomus System or IP Block.

b) bdCERT introduce SMS based incident reporting for there constituencies.

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 Cyber Attack & Network Forensic

  3 days (11th June 2012 to 13th June 2012) long training program on Cyber Attack & Network Forensic organized by ISPAB in collaboration with bdCERT. This training program is supported by ICT Business Promotion Council. Participants come from all area which includes Financial Institute, Law enforce agencies, Government Officials, ISP, Telecommunication Industry.

- Digital World 2012

  bdCERT representative participate in Digital World 2012 organized by Ministry of Information & Communication Technology, Bangladesh. The session "Cyber Security & Cyber Crime" was conducted by bdCERT with other security experts from home and abroad.

3.2 Trainings & Seminars Participated

- 2012 APISC Security Training Course

  bdCERT representative participate in 2012 APISC Security Training Course held by KCC at Korea and supported by KrCERT/CC.

4. INTERNATIONAL COLLABORATION

- bdCERT signed MOU with Team Cymru to facilitates security related services and enhance knowledge of local resources.

5. FUTURE PLANS & Projects

a) Government Endorsement for BDCERT

b) Full Membership of APCERT

c) Full Membership of OIC-CERT

d) Building Awareness

e) Fund Raising

f) Consulting to form other CERTs within the constituents

20. EC-CERT Activity Report

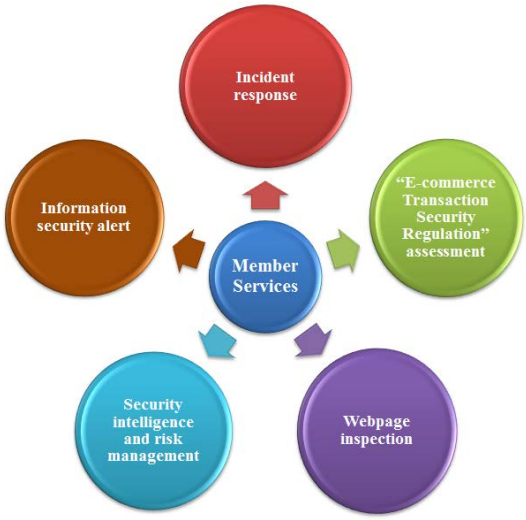
Taiwan E-Commerce Computer Emergency Response Team – Chinese Taipei

1. About EC-CERT

1.1 Introduction

EC-CERT is the abbreviation for "Electronic Commerce - Computer Emergency Response Team". It is the first CERT for EC industry in the world. The purpose of EC-CERT is to apply a reliable and confidential communicating channel to notify, exchange, and analyze information security events that occur within the e-commerce network, and further activate early prevention, solving methods and optimal operations against threatening vulnerabilities and attack patterns; In addition when an unexpected situation occurs, EC-CERT provides emergency responses and handling suggestions to effectively reduce losses, have rapid recovery, and ensure smooth operations of Taiwan's e-commerce websites and systems.

1.2 EC-CERT Services



- Incident response

  E-commerce members can report information security breach according to the "Regulations and Procedures for E-commerce Computer Emergency Incident Response Reporting Mechanism." The team will respond and manage the incident according to the "E-commerce Computer Emergency Standard Operation Procedure", and provide necessary information and technical assistances to the reporter of the incident.

- Information security alert

  Gather various data on security threats, exchange security information with domestic and foreign information security organizations, then compile, analyze, and interpret these data. Then provide through e-mails and cellphone text messages the latest news of information security threat such as security leaks, malicious websites, hackings and phishing, and recommend defensive measures so that e-commerce operators can take early precautionary measures to reduce their information security threats and to avoid potential loss.

- Security intelligence and risk management

  Integrate resources of information security service providers. For members with Internet information security defense facilities (firewall, IPS), collect real time log and provide them with a 24-7 information security monitoring service, including real-time monitoring, reporting, online emergency response and management, and defense recommendations for intrusions and hackings.

- Webpage inspection

  Based on the IP addresses provided by e-commerce members, regularly scan webpages for Trojans and specific malicious codes, and then issue immediate security warnings for unusual webpage activities to reduce the risk of e-commerce websites becoming zombie sites with malicious code.

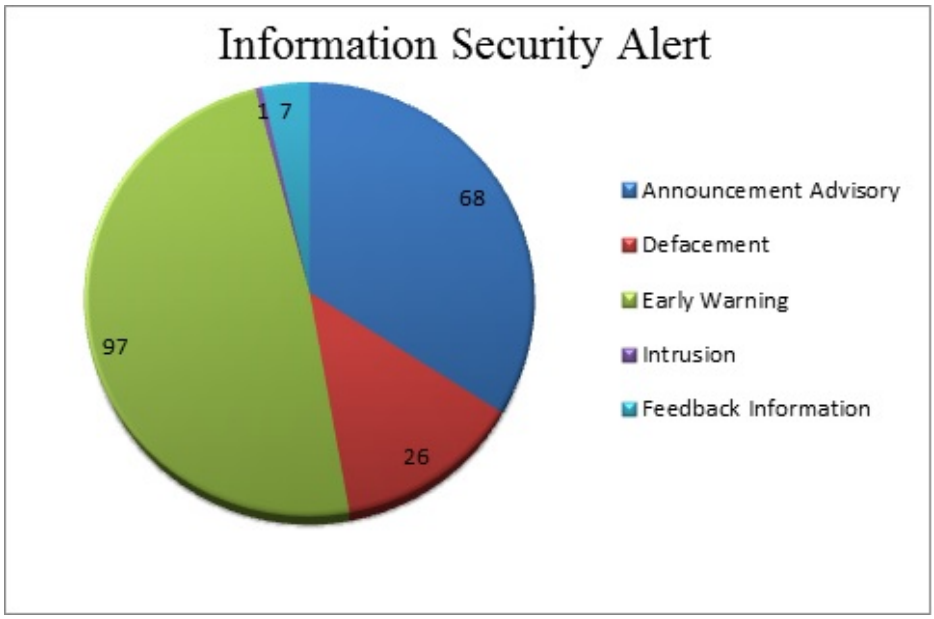
- "E-commerce Transaction Security Regulation" assessment

  Based on the team's e-commerce transaction security regulations, integrate information safety management consultants to provide e-commerce operators with free on-site regulation assessments in order to promote understanding and compliance with regulations.

2. EC-CERT Activities and Operations in 2012

- Communication and cooperation with other security unites
  - Connect with 4 domestic information security institutions for real time security information exchange.
  - EC-CERT organized 6 events including information exchange meetings, seminars and hearings in Taiwan.

- Information security alert service
  - EC-CERT provided members with a total of 199 notices regarding the latest information security threat warnings and Internet vulnerabilities.

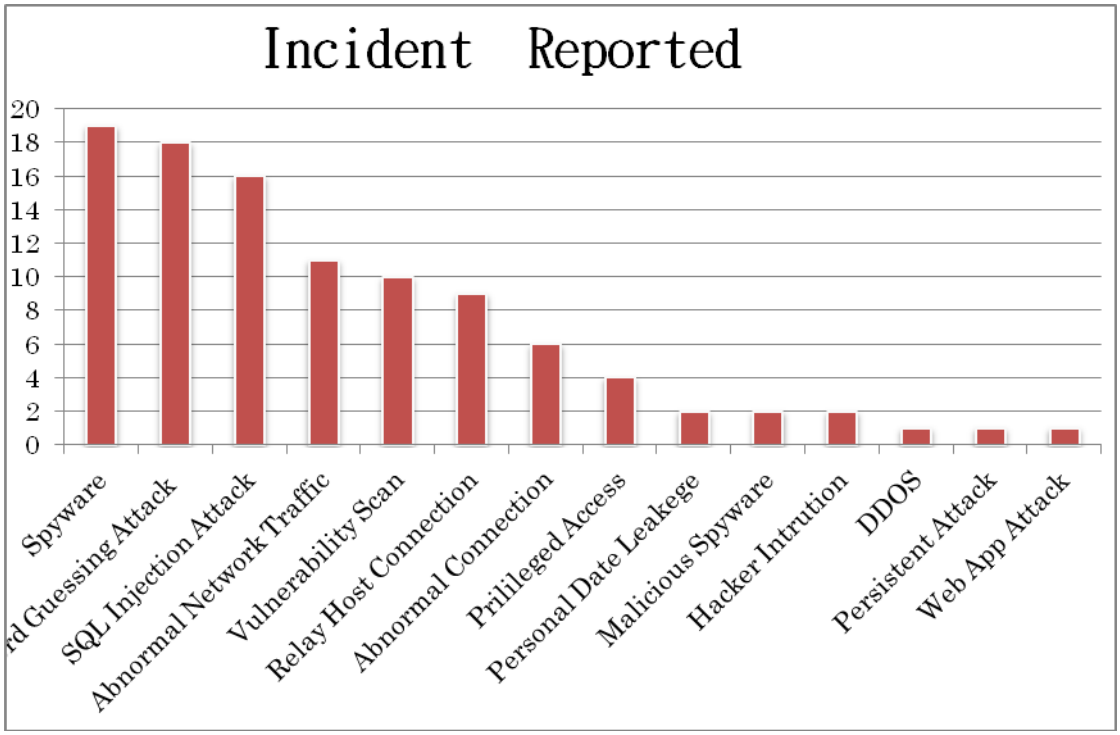


- Formulation of mechanism regulations
  - EC-CERT formulated "E-Commerce Information Security Incident Reporting Regulations and Operation Guidelines".
  - EC-CERT implemented E-Commerce trading security indicator survey.

- Website and system development
  - EC-CERT Official Website.
  - Information Security Incident Reporting and Response Website.
  - Information Security Information Exchange System.
  - Warning Issuing System.
  - Information Security Database.
  - Information Security Regulation Evaluation System.
  - Information Security Regulation Health Check System.

- Incident Report and Response
  - EC-CERT received 102 incidents reported and supported 73 times of e-commerce information security telephone consulting and referral service.

- EC-CERT has over 130 members include e-commerce vendors, information security experts and financial sectors.



3. Conclusion

As the E-Commerce market value growth in Taiwan, EC-CERT plays an important role to upgrade security ability of E-Commerce industry. In 2012, EC-CERT help observed an improvement in network security response in E-Commerce industry comparing to years before. Also EC-CERT continues to provide members with latest information security service such as real time alerts, incident monitoring, information exchange, consulting service, 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.

EC-CERT Contact Information :

Website : http://ec-cert.org.tw/?str=en

Telephone : +886-2-66396620

Facsimile : +886-2-66398963

E-Mail : service@ec-cert.org.tw

21. mmCERT Activity Report

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 to support the incident handling in Myanmar. In the National Cyber Security Framework, mmCERT is under the Cyber Security Incident Handling Committee. mmCERT serves cyber security incident handling not only for Myanmar internet users but Myanmar government agencies' websites also.

1.2 History

mmCERT was established as a national computer emergency response team in Myanmar on 23rd July 2004 and mmCERT coordination center (mmCERT/cc) was opened in December 2010 under the Ministry of Communication and Information Technology (MCIT). mmCERT was joined as the General Member of the APCERT in December 2011.

mmCERT is the first CSIRT (Computer Security Incident Response Team) established in Myanmar and it's a government-funded organization. mmCERT/cc consists of 11 members as of 2012. The Members of mmCERT are MCIT and MOST (Ministry of Science and Technology).

1.3 Contact Information

Email: technicalteam@mmcert.org.mm, infoteam@mmcert.org.mm

Phone: +95 1 650891, +95 1 652372

1.4 Constituency

mmCERT's constituents are Myanmar internet users in the public and private sector, business and home. During two years experiences, mmCERT mostly related with internet service providers and application service providers in Myanmar.

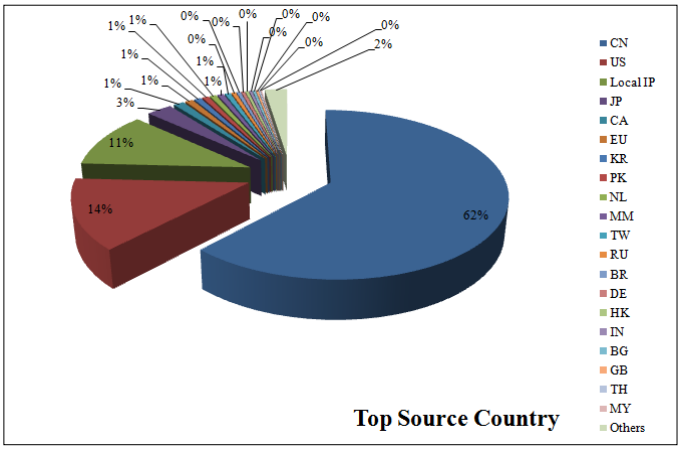
2. Activities and Operations

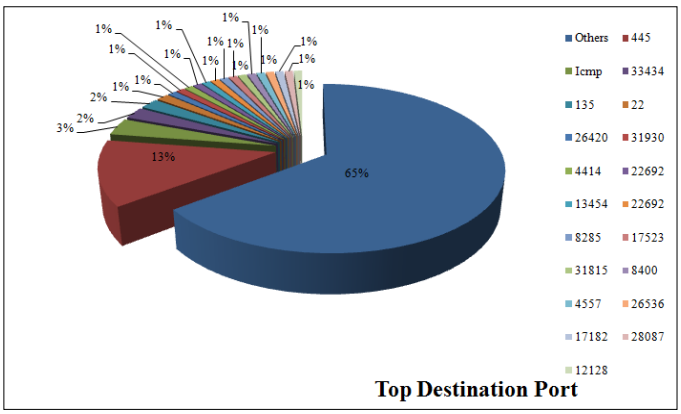
2.1 Weekly Email Newsletters

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 security organizations.

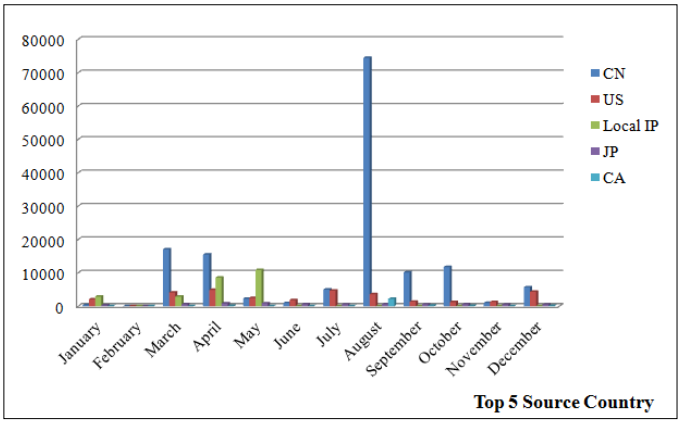
2.2 TSUBAME Statistics

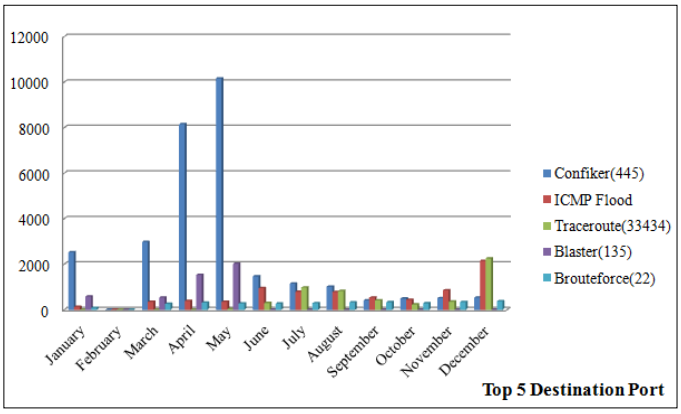
The following graph shows the top source country and top destination ports statistics obtained from TSUBAME Sensor in 2012.





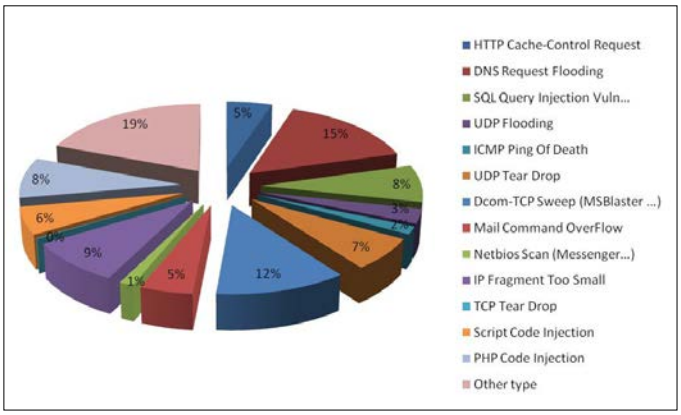
The following graphs show the top five countries and top five destination ports statistics per month in 2012.



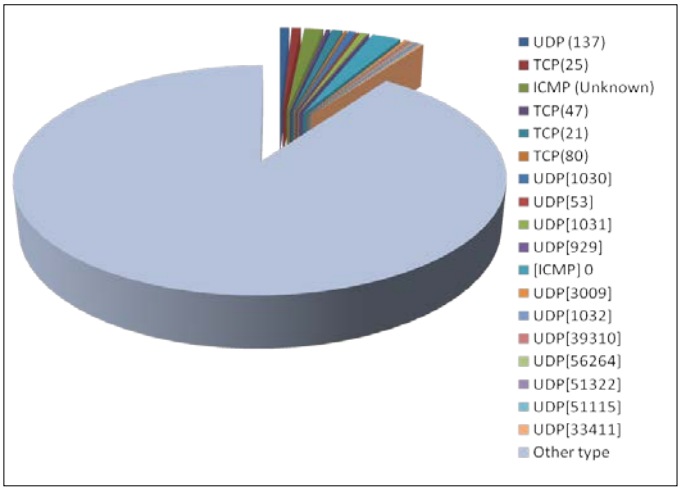


2.3 Intrusion Prevention System statistic

According to IPS system result of local ISPs, the most common attack types in 2012 are shown below.

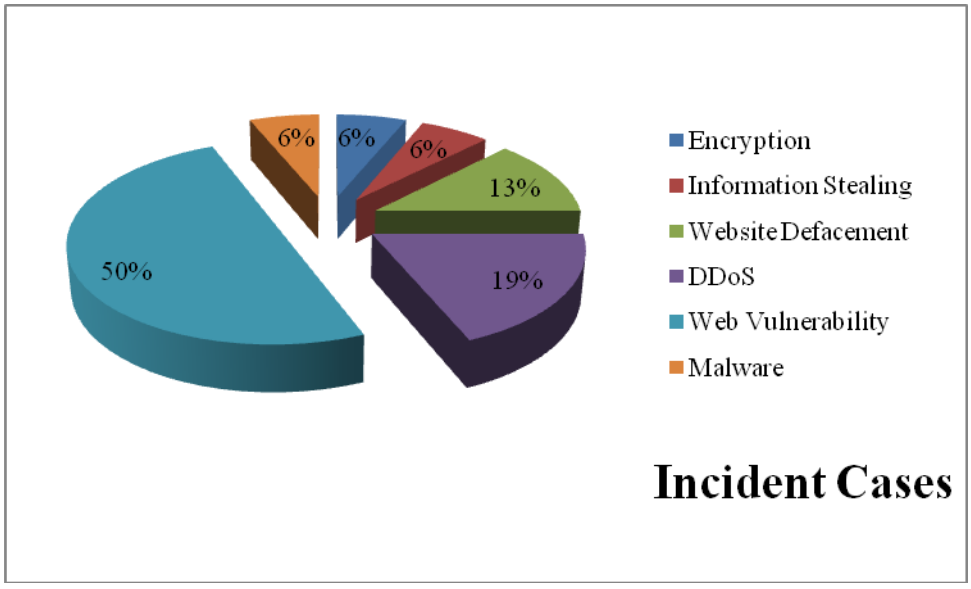


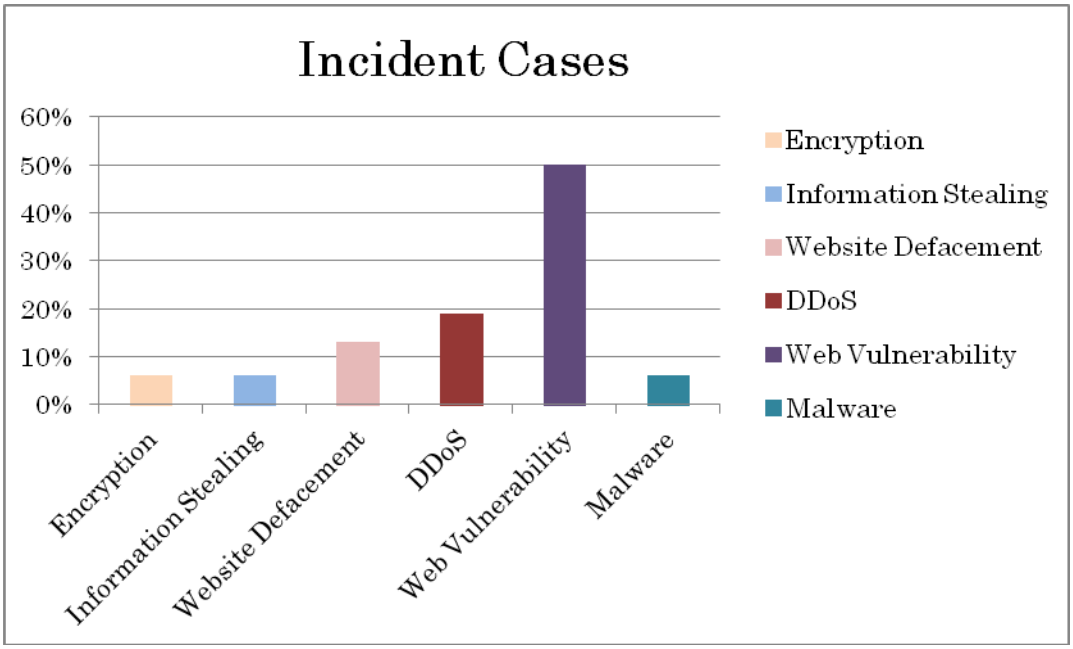
The following figure shows the summary of IPS by customer network from September to December, 2012. These are the most infected ports: ICMP, TCP (25), UDP (137), UDP (1030), UDP (1031) and TCP (21).



2.4 Incident Handling Report

The following graph shows the incidents that were solved by mmCERT in 2012. According to our incident analysis, Web Vulnerability and DDoS attack are most prominent incident cases happened in 2012. In addition, mmCERT gave the technical advisories for all these incident cases to its constituency.





3. Events Organized/Co-organized

3.1 Training

- Providing Network Forensic Training to Local Service Providers (LSP) (March 21, 2012)
- Providing Network Forensic Training to Government and Private Banks (May 18, 2012)
- Providing Network Forensic Training at TPTC (Telecommunications & Postal Training Center) which is a training center of MCIT. (June 6, 2012)

3.2 Meeting

mmCERT/cc organized face to face meeting among technical staffs from two major ISPs, constituents and mmCERT members.

3.3 Workshop

- Provide IT security Workshop to M.C.Tech Students from University of Computer Studies Yangon, Myanmar. (October 26, 2012)

3.4 Seminar

- Provide Website Security Seminar to Government official from Ministries and IT persons from Private Company. (August 8, 2012).

3.5 Drill

- Participated in Asia Pacific (APCERT) Drill (February 14, 2012).
- Participated in ASEAN CERT Android Malware Incident Drill (ACID 2012) (September 12, 2012).

4. International Collaboration

- Advanced Malware Training provided by JPCERT/CC (November 5-9, 2012).
- Incident Handling Training provided by JPCERT/CC (November 12-16, 2012).
- Visiting Mitsubishi Research Institute (MRI), JICA, JPCERT/cc to mmCERT/cc (June 6, 2012).

5. Conclusion

As being mmCERT is a developing team, mmCERT technical staff development activities such as giving seminars, writing technical advisories and practicing and preparation for Incident Handling Activities were done throughout the year 2012. mmCERT looks forward National IT image by cooperating with international CERTs for cyber security and cybercrime in 2013.

22. MOCERT Activity Report

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 2012 there are three (3) staff providing the service with two (2) additional support staff.

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 2012 MOCERT has provided the following activities

Support the Early Waning through

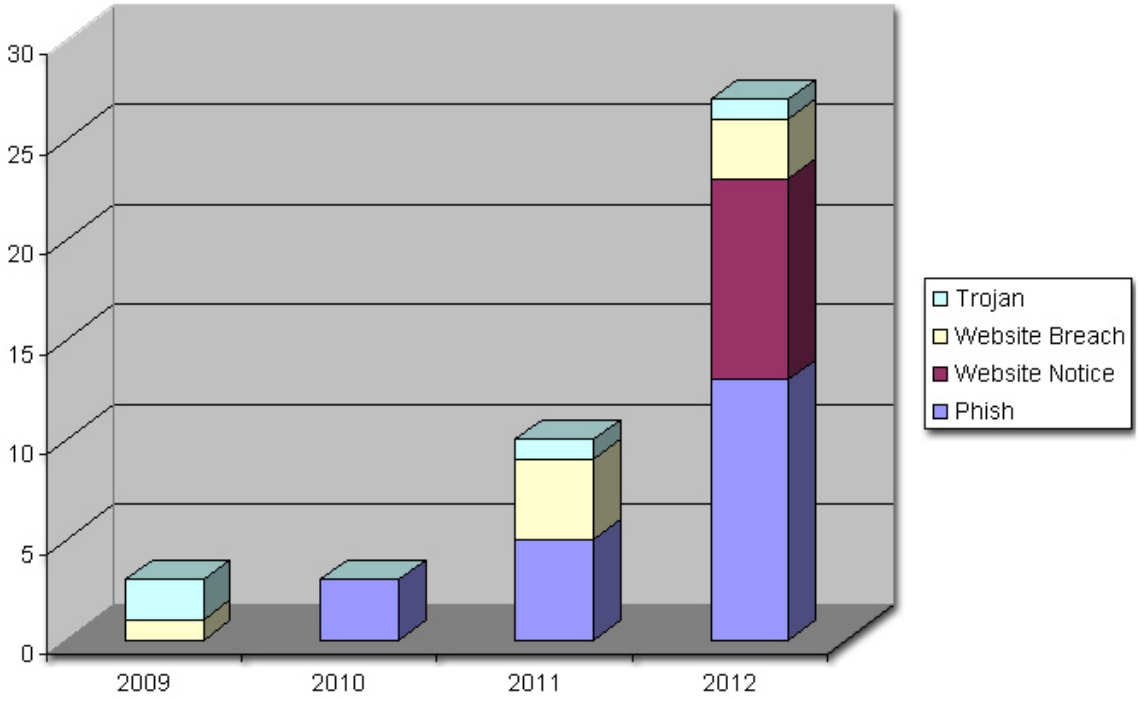
- Publication of industry specific notification of potential information security issues
- Publication of broadly affecting issues that affect web servers of Macau origin be they government, industry or other
- Conducted publicly available seminars on the computer security
- Conducted workshops at the public, tertiary education and secondary education institutes on computer security
- Maintenance of a website as point of reference for MOCERT services
- Inclusion of tertiary level interns in computer security related projects.
- Assisted in the delivery of a course in Computer security topics at university and high schools.
- Performed a web server from page search of infectious code, twice a year, yielding incidents.
- Actively taking part in the computer security community through conferences
- Speech to government IT staff at a local event called Clean PC Day
- Speech representing APCERT at the 3rd APT Cybersecurity Forum
- Speech representing MOCERT at the 3rd APT Cybersecurity Forum
- Assisted in the APCERT Membership Working Group
- Assisted in the TSUBAME Working Group
- 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. There still is reluctance from reporting issues which provides a natural shy stance to computer security.

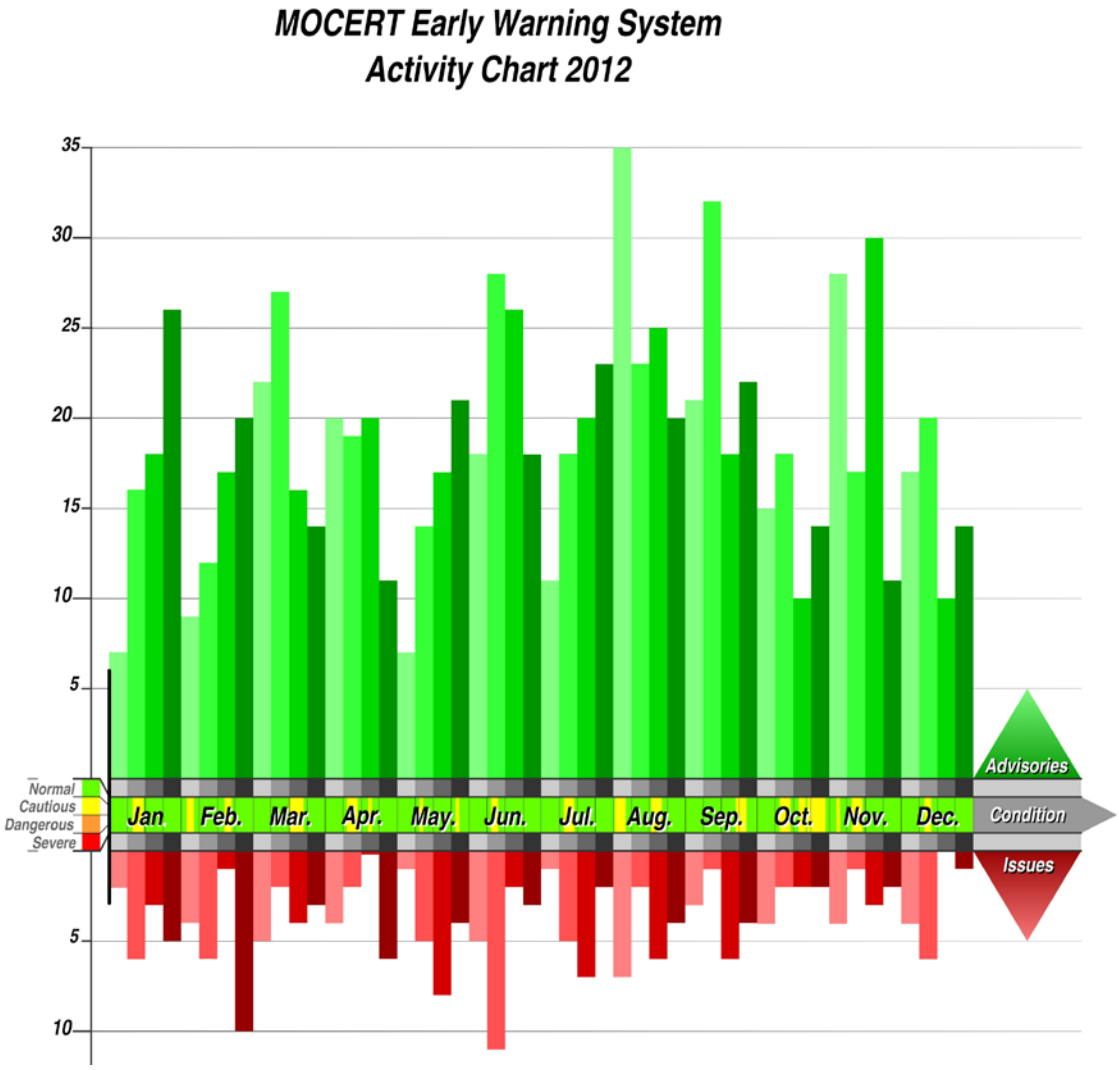
Sources of incidents are from three distinct channels.

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.

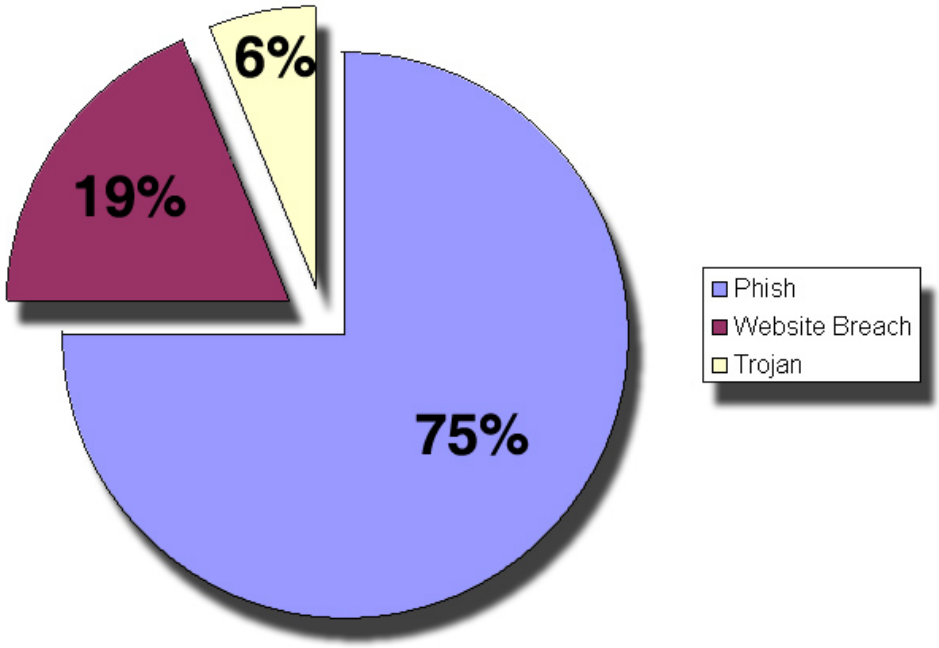
The notifications are then classified to Issues and Advisories and then posted. The following diagram shows the distribution of postings were in 2012, 1076 postings were made with 895 Advisories, and 181 Issues.



DNS Changer – Notices were issued to the public and website link made from the MOCERT website about how users could check their systems. Also remedial actions were notified on the website so that users were able correct their problems before the DNS servers were shutdown on the 9th of July. The efforts alleviated the impact of the shutdown to the point that no appreciable disruptions occurred.

2.2 Abuse statistics

The following pie graph denotes the abuse distribution as noted for the year 2012. 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

13th-16th February 2012 - "Clean PC Day for schools"

Spanning four days, a Clean PC Day activity was held in Colégio Diocesano de Sao José (CDSJ) for the high school students of Form 5 from 13th to 16th February. Attendees were explained about the reasons why, and the methods of how to keep their PC clean. Alerts of current cyber attacks were also introduced and useful anti-virus tools and software were demonstrated. The highlight of the activity showed that indeed the best approach to a clean PC from cyber attacks rests on the user's awareness and ability when using their computer and Internet. After the activity, CDSJ students of Form 5 are now better prepared and able to keep a clean PC.

25th July 2012 - "Data Management and Social Networking Risks" "Clean PC Day"

Titled "Data Management and Social Networking Risks" 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 25th July 2012, at Macau New Technologies Incubation Centre (MANETIC)

1st June 2012 - "Phishing Attacks – Biting back HARD"

This was a community awareness seminar addressing the current issue of Phishing. The focus is on bank fraudulent websites being hosted outside of Macau or fraudulent foreign bank websites unwittingly being hosted in Macau. Insights of the economics of Webfraud and Phishing highlighted its main weakness. Also methods and techniques on how user can act, as well as more advanced techniques of how these sites are handled and ultimately brought down are shared with the community.

8th October 2012 -"Surviving Computer Attacks" seminar

A series of seminars centred around computer attacks and avoiding them were compiled in a single afternoon on 8th October 2012. Speakers from Hong Kong, experienced in a range of attacks on computer system from Distributed Denial of Service (DDoS) to Advanced Persistent Threat (APT) as well as issues with Cloud Computing, were brought together to provide attendees an opportunity to better assess their organizations' risk exposure and the available controls to mitigate these risks

19th November 2012 "Cryptoparty – a start to online privacy" Seminar

Technical Director of Central Technology Limited and MOCERT introduced the use of open source encryption software and techniques that are available for attendees to better control on their private information security both at enterprise and at home, including how to store, transfer and discard the information.

3.1 Training

Staff in MOCERT service is 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 2012 was as a player. The event was instrumental in reshaping some of the services provided for 2012. The drill allowed for a better understanding of issues facing the CERT community and skill sets required to

solve them. Involvement in the Organizing Committee for the 2013 drill has been sought.

3.3 Seminars

MOCERT attend both APCERT Bali and FIRST Malta meeting in the year 2012.

4. Achievements

4.1 Presentation

25th-27th September 2012 – Speeches at the 3rd APT Cybersecurity Forum

Two speeches were delivered by MOCERT in front of related industry as well as Ministries of Telecommunication of economies from the Asia Pacific region. The first speech centred around the computer incidents handled in Macau by MOCERT. The second speech was delivered by MOCERT on behalf of Asia Pacific Computer Emergency Response Teams (APCERT), an association of CERT, about their activities and the vision of the APCERT group. Both presentations together demonstrated that indeed as innovation drives the telecommunications industry forward, this benefit may be on borrowed time should security issues in cyberspace not be resolved

4.2 Publication

The five (5) leaflet publications that were made the previous year is still 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

5.2 Mentor

Dec 2012

Internship

One (1) Student from the University of Saint Jose was taken in for internship. This student is assisting tin the implementation of the Cuckoo Sandbox analysis tool.

6. Future Plans

MOCERT is still reviewing its services after a positive result from being more proactive in finding problems in the cyber landscape of Macau. Initiatives that allow further sweeps of AS4609 both in depth and frequency will be investigated along with correlation of external use of data such as from the sensors and Shadow server which can be capitalized even further.

7. Conclusion

2012 has been a year full of change that was catalyzed by membership in APCERT. The major changes occurred is the active search of problems that are on the cyber landscape of Macau. These changes complements the in services of a computer emergency response team, by which instead of being reactive, further proactive measure are taken. This approach has been beneficial due to the current culture of the constituency. These changes are done progressively and ongoing for the next few years as new services are devised and tailored for the needs of the Macau constituency to make a clean and safe Internet.

23. MonCIRT Activity Report

Mongolian Cyber Incident Response Team – Mongolia

1. About MonCIRT

1.1 Introduction

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

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

MonCIRT services are available for all business entities, personals.

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

- Telephone and email
  - hotline: + 976 - 70113151
  - email: info@moncirt.org.mn
- World Wide Web: http://www.moncirt.org.mn/

1.1.1 Establishment

MonCIRT was established in 2006 as NGO. From 2006 till 2013 MonCIRT operate as sole national CSIRT of Mongolia. As the sole CERT of Mongolia at this moment, MonCIRT acts as the focal point for cyber security for the nation, especially business sector.

In December 2011 the Government of Mongolia approved decree on creation of National Cyber Security Department and in frame of this initiative plan to establish MNCERT.

In December of 2011 the MonCIRT signed MOU with National Data Center on support of MonCIRT and collaborating in the field of Incident Responses, using of NDC monitoring and Intrusion Prevention capabilities. National Data Center plan to establish CSIRT based on their Information Security Department and Monitoring Center.

1.1.2 Workforce

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

1.1.3 Constituency

Currently MonCIRT‘s constituency encompasses the Business Sector of Mongolia because government organizations plan to establish Government CSIRTs. In case of establishment and start of expected government MNCERT, Data Center CERT our constituency will be narrowed and it will be formed from business companies, private sector organizations, NGO and general public. We started to works closely with Chief Information Officers and system administrators of business sector’s and organizational networks of its constituency. In addition we drafted MonCIRT’s new regulations.

2. Activities & Operations

2.1 Activities

The summary of activities carried out by MonCIRT during the year 2012 is given in the following table:

Activities	Year 2012
Security Incidents handled	58
Security Alerts issued	195
Advisories Published	10
Vulnerability Notes Published	89
Security Guidelines Published	0
Trainings Organized	4
Mongolian Website Defacements tracked and advised	146
Open Proxy Servers tracked	6
Bot Infected Systems tracked	482
Phishing (mirror) web sites tracked and removed	4
Projects	0

The majority of web threats in Mongolia in 2012 are delivered from previously trusted and popular web sites that have been hacked for use by cybercrime. For this reason, reputation defenses become less effective. The once obscure link farm for search engine poisoning now resides within popular web sites. The exception for link farms is now a rogue domain or remote web location. Phishing attacks overwhelmingly come from popular and trusted web sites hacked by cybercrime. From January through December 2012, the MonCIRT received 351 email messages and more than 110 hotline calls reporting computer security incidents or requesting information. 184 of these messages, information was related with real incidents and we provided with recommendations. We received 16 vulnerability reports and handled 37 computer security incidents during this period. We cannot retrieve incident handling statistics from organizations, administrators due to executive's restriction.

We continue to provide advice to computer system administrators in the Internet community who report security problems. 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

Malware and the malicious web

- In 2012, near daily leaks of private information about victims were announced like game scoreboards through tweets and other social media.

Personal details, such as email addresses, passwords (both encrypted and clear text), and even national ID numbers were put on public display.

- Based on data for 2012, it is not surprising that the bulk of the security incidents disclosed were carried out with the majority of attackers going after a broad target base while using off-the-shelf tools and techniques. We attribute this to the wide public availability of toolkits and to the large number of vulnerable web applications that exist on the Internet.
- The year began and ended with a high-profile DDoS attacks against the Mongolian cell phone operators.

  This technique assisted in much higher connected uptime as well as having more bandwidth than home PC's to carry out the attacks.
- In the sampling of security incidents from 2012, the Mongolia had the most breaches, at 6%.
- The relative volume of the various alerts can help to describe how attacks are established and launched. They also frequently provide hints about how methods have evolved. Based on this, the main focus in 2012 may have been the subversion of systems, with larger coordinated attacks being executed across fairly broad swaths of the Internet.

2.3. Incident trends

From 2012 we trying to become a major reporting center for incidents and vulnerabilities and establish MonCIRT reputation for discretion and objectivity among business organizations, general public. Based on our experience the National Data Center start to handle incidents. As a result of connection with NDC's monitoring system, IPS and Tsubame system and sharing of attack data we able to obtain a broad view of incident and vulnerability trends and characteristics.

During the year 2012 MonCIRT handled several incidents of intrusions into websites using SQL and PHP injection and injecting Java script to redirect visitors to malicious websites. By exploiting vulnerabilities in web applications trusted websites are infected with links to malicious websites serving content that contains client side exploits. Most of incidents handled was web site defacements. We tracked and advised in 146 defacement cases from which 18 is handled by our team.

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

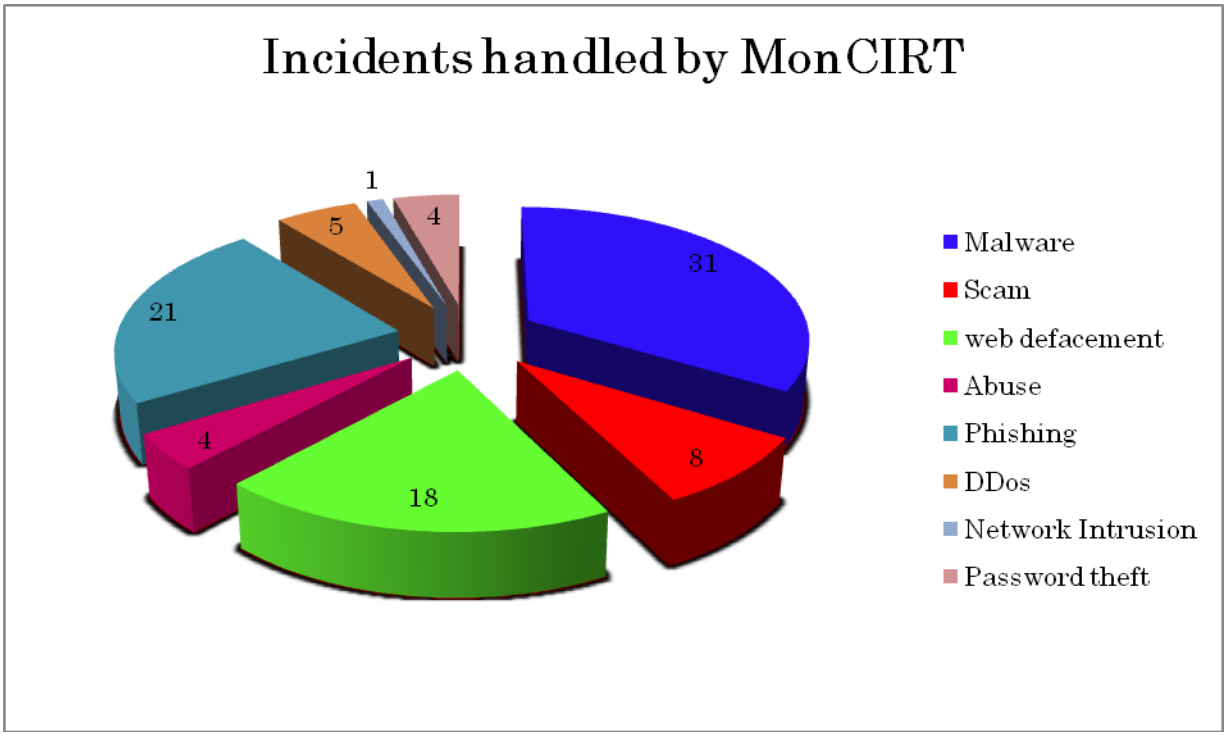
below the leading categories for hosting malware (versus delivery) for the 2012 in Mongolian Internet segment.

1. Online Storage
2. Software Downloads
3. Pornography
4. Open/Mixed Content
5. Computers/Internet
6. Placeholders
7. Phishing
8. Hacking
9. Online Games

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

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

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



2.4 Tracking and advise of/on Mongolian Website Defacements

MonCIRT is tracking the defacements of websites on Mongolian languages and suggesting suitable measures to harden the web servers to concerned organizations. In all 146 numbers of defacements were tracked in the year 2012 most of the defacements were done for the websites under .mn domain. In total 118 .mn domain websites were defaced.

2.5 Tracking of Open Proxy Servers

MonCIRT is tracking the open proxy servers existing in Mongolia and proactively alerting concerned system administrators to properly configure the same in order to reduce spamming and other malicious activities originating from Mongolia. 15 open proxy servers were tracked in the year 2012 in Mongolia.

2.6 Botnet Tracking, Mitigation

MonCIRT is tracking Bots and Botnets involving Mongolian systems. Users were advised on suitable measures for disinfection. As show our survey in Mongolia operate one Command & Control server tracked from 2011. Result of our survey shows 1089 Bot infected in Mongolia in 2012.

2.7. New services

2.7.1 Network secure administration

Our founders Professor Khaltar T and Mr Anar S (CISCO certified professional, network auditor) organized 2 trainings on network secure administration for system administrators of business organizations. In addition MonCIRT continue the project together with Forensic Analyze Center of Mongolia named "National Digital Forensic Analyse Capacity Building".

2.7.2 Setting up new CSIRT

We initiated the reformation of MonCIRT as MonCIRT NGO and National Data Center joint CSIRT from 2011. But new government decide to stop these activities and create NDC separate CSIRT. Therefore we now assist in this activities and support NDC CSIRT creation processes.

3. Events organized / co-organized

3.1 Training / Education

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

The MonCIRT offers different training courses. These courses derive from the practical work of the MonCIRT staffs, providing introductory and advanced training for technical staff and the management of network security management, configuration, incident response and are centered around broader Internet security issues and security practices. One course offering are geared toward educating policymakers, managers, and senior executives who are responsible for the security of information assets and based in MNS ISO/IEC 27001, 27002, 27005, 27033.

Courses offered in 2012 included the following:

- *Network security management and configuration*
- *Information Security for Managers*
- *Internal Information Security audit and Self evaluation*
- *Network Monitoring*
- *Fundamentals of Incident Handling and Management*
- *Fundamentals of Ethical Hacking*

In addition MonCIRT organized following workshops:

« Workshop on "Network monitoring" on September 13, 2012

« Workshop on "New Cyber threats" on August 24, 2012

3.2 Drills

In 2012 MonCIRT cannot organize local network security drill-III due to financial limitation, new parliament election and the Government was changed.

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 2012 and participated in conference edicated to this event. The governing board director of MonCIRT prof Khaltar Togtuun was one of key speaker of this conference.
b. With sponsorship of Security Solution Service LLC and National Data Center organized annual “Security Open Day Mongolia 2012” in November. Within these days it is successfully hold scientific & practical conference, fair and workshop.
c. Together with National Data Center organized ethical hacking contest “Kharuul Zangi 2012”.

4. Achievements

4.1 Presentations

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

a. Conducted presentations during the Annual “Security Open Day” and ICTPA expo 2012 conference on themes “IPS implementation” and “Importance of Information security audits”.

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 8 advisories and 64 vulnerability notes in 2012. Among the criteria for developing an advisory are the urgency of the problem, potential impact of intruder exploitation, and existence of a software patch or workaround. On the day of release, we send advisories to a mailing list of MOSA and network

administrators mailing list.

MonCIRT Security Practices

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

- *Outsourcing Managed Security Services*
- *Securing Desktop Workstations*
- *Monitoring the Network*
- *Deploying next generation Firewalls*

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 2012:

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 refused our offer.

5.2 Event participation

July 7th – 12th, 2012, Seoul

APISC 2012 training

5.3 International incident coordination

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

6. Future Plans

6.1 Future projects

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

6.2 Future plan

In relation with creation of new CSIRTs it is planned to reorganize board structure, management staffs and expand our operation, establish new services aimed on Business sector's networks, public networks.

7. Conclusion

For MonCIRTs' constant and developing activity we ask for financial support from Cyber Security Office of Mongolia. 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.

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

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 (after start of new CSIRTs) 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 2013" while finding new ways to reach an even wider audience.

MonCIRT shall continue to participate in regional events such as the Annual APCERT drill and will begin to participate in FIRST events and join to FIRST.

Contact Information

Postal Address: Mongolian Cyber Incident Response Team (MonCIRT).

Tokyo street 3-12. Bayanzurkh District. Ulaanbaatar, Mongolia, 13381.

Incident Response Help Desk

Phone: +976-70113151

Fax: +976-70153286

24. NCSC Activity Report

New Zealand National Cyber Security Centre – New Zealand

1. About NZ NCSC

1.1 Introduction

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

1.1.1 Establishment

The NCSC was formally established following the release of New Zealand's Cyber Security Strategy in June 2011, and became operational in September 2011. It has absorbed its predecessor organisation, the Centre for Critical Infrastructure Protection (CCIP), in doing so adopting an expanded scope and responsibilities for coordinating and responding to cyber security issues, including;

- Incident coordination and response;
- Provision of policy advice and publications;
- Engagement with the public and private sectors to develop and improve awareness and appreciations of cyber security threats;
- Provide a single point of contact for enquiries;
- Liaise with the international CERT community and global partners to promote greater cooperation; and
- Coordination with other organisations acting in the domestic cyber security space.

1.1.2 Workforce power

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

1.1.3 Constituency

Primarily New Zealand government agencies, law enforcement, Critical National Infrastructure (CNI) operators and other key industry stake holders, in addition to wider engagement with the entities in the private sector.

2. Activities & Operations

2.1 Incident handling reports

In 2012, the NCSC received a total of 134 incident reports which met the appropriate reporting criteria. The largest category of Incident Report types (Fig 1.1) was scam & spam related incidents which made up 31% of the incidents captured. Denial of service (DoS) attacks and Botnet/Malware activity were the second largest categories making up 16% and 14% of incidents respectively. Other significant issues include website compromises, hijacking & defacement (10%), Spear Phishing (7%) and attempted network intrusions (which includes malicious scanning) (6%).

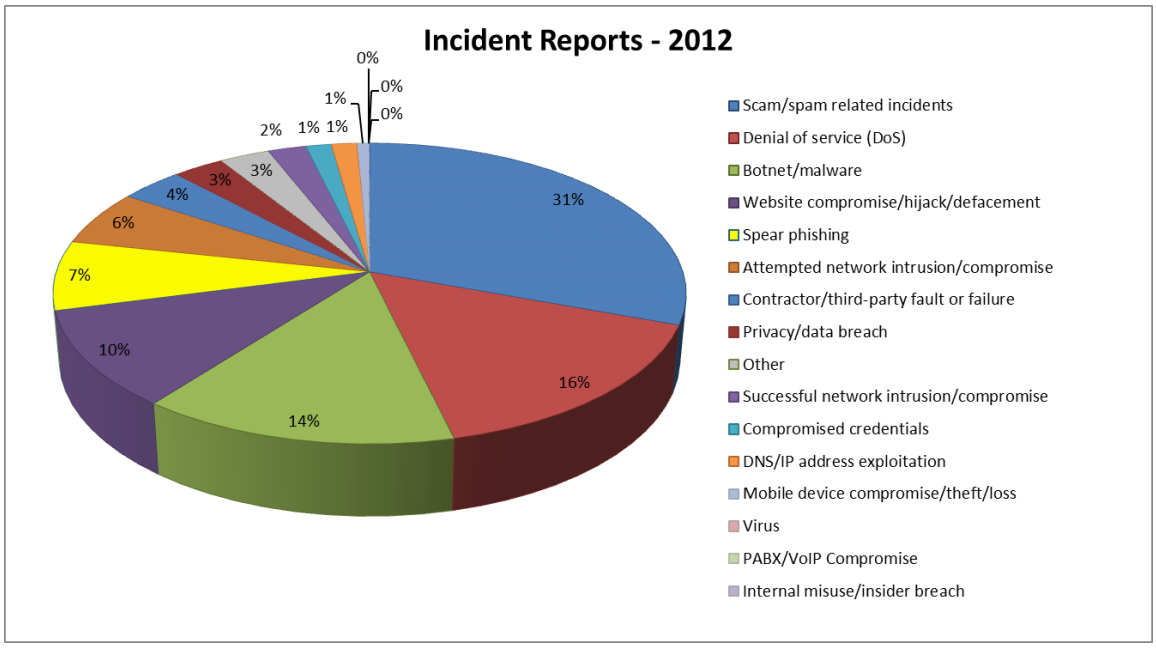


Fig 1.1

The attribution of the incidents (Fig 1.2) revealed that the bulk (60%) of incidents reported originated from an overseas source. Nearly a third of the incidents reported (31%) involved incidents originating from domestic sources. 9% of incidents were unable to be attributed to a specific origin.

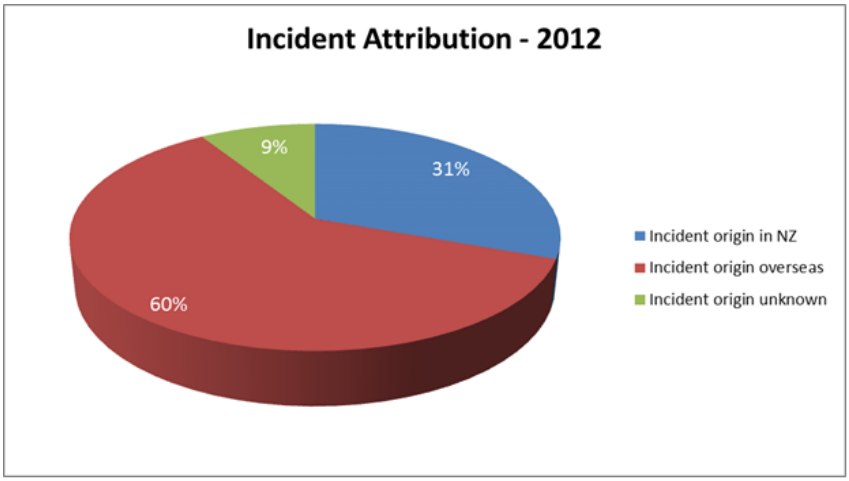


Fig 1.2

Of the organisations and individuals targeted (Fig 1.3) the private sector (47%) represented the largest category. Incidents targeted at individuals were the second largest group (26%), while government (16%) and critical national infrastructure providers (6%) also reported significant numbers of incidents.

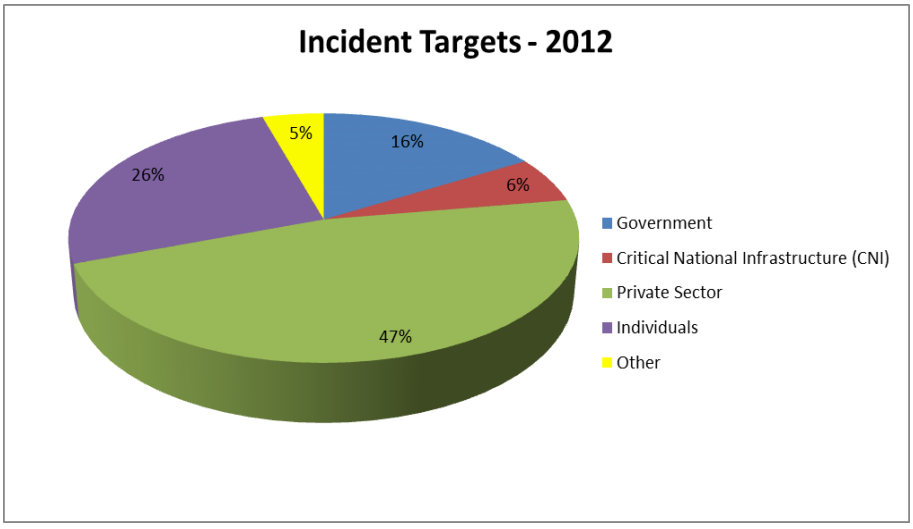


Fig 1.3

2.2 Additional activities

In addition to receiving incident reports, the NCSC:

- Issued unique advisories to key partners;
- Produced content for & highlighted significant issues via the NCSC website;
- Coordinated & hosted industry engagement forums;
- Participated in the NZ Internet Task Force (NZITF), a domestic security community, to promote collaborative approaches to security issues;

- Released public reports on the NCSC activities and provided policy guidance; and
- Undertook the preparation of a CSIRT training programme to build resilience among public & private partners.

3. Events organized / co-organized

Organised and hosted several industry & government engagement forums, held at regular intervals throughout the year.

3.1 Training

Helped prepare & participate in a number of training activities through the NZITF and other fora.

3.2 Drills

In 2012, NCSC coordinated and participated in the NZITF communications drill in October and also coordinated a governmental response exercise. NCSC also joined the 2013 APCERT communications drill in February.

4. Presentations

Throughout 2012, NCSC presented at and / or participated in several international forums including:
AusCERT Conference, Australia
GovIS Conference, New Zealand
Kiwicon, New Zealand
NZITF Conference, New Zealand
ISACA Oceania Conference (CACS) and local chapter meetings, New Zealand
ASIS International (American Society for Industrial Security) New Zealand Chapter, New Zealand

4.1 Publications

NCSC publishes a number of security alerts & advisories via its website, through direct exchanges with partners and on a bi-lateral basis where appropriate. Additionally, NCSC is involved in the publication of:

- Application Whitelisting guidance (website release);

- Skype implementation guidance (website release); and
- Incident Report Summaries 2011, 2012 (website release)
- Produced & presented a paper on Cloud Security at the ISACA Oceania (CACS)& ASIS International conferences

5. International Collaboration

The NCSC participates in the APCERT forum.

6. Future projects

- Extending services offered
- Expand engagement with domestic & international partners
- Planning training & awareness programmes

7. Conclusion

The NCSC has spent 2012 developing the foundational groundwork into sustained, strategic and systematic engagement across a number of sectors. It has focused on engaging on both technical and policy issues, and will seek to grow engagement at the international level in 2013.