APCERT Annual Report 2010

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

CONTENTS

Chair's Message 2010 3

I. About APCERT 5

II. APCERT Activity Report 2010... 10

1. International Activities and Engagements 10
2. Approval of New General Members / Full Members 16
3. APCERT SC Meetings 16

III. Activity Reports from APCERT Members 17

Full Members 17

1. AusCERT Activity Report 17
2. BKIS Activity Report 28
3. CERT-In Activity Report 36
4. CNCERT/CC Activity Report 45
5. HKCERT Activity Report 54
6. ID-CERT Activity Report 61
7. JPCERT/CC Activity Report 67
8. KrCERT/CC Activity Report 75
9. MyCERT Activity Report 80
10. PHCERT Activity Report 89
11. SingCERT Activity Report 95
12. SLCERT Activity Report 97
13. ThaiCERT Activity Report 106
14. TWCERT Activity Report 109
15. TWNCERT /CC Activity Report 120
16. VNCERT Activity Report 125

General Members 130

17. BDCERT Activity Report 130
18. CERT Australia Activity Report 135
19. MonCIRT Activity Report 140
20. TechCERT Activity Report 150

Chair’s Message 2010

APCERT had a very good start last year. In May 2010, APCERT was awarded the "AusCERT's Annual Award for Organizational Excellence in Information Security". The award was one of the SC Magazine Awards Australia held at the AusCERT 2010 conference. The award was presented to " .. the organization that in the past year most contributed to information security in the areas of community service, innovation, education, liaison, law enforcement, governance or leadership.." This award was presented to recognize the contributions of ALL team members in making APCERT an outstanding organization.

Our coordination and collaboration in tackling incidents, the commitment and participation of teams in the annual drill, and the efforts in contributing to the information security community by different teams, etc. were good illustrations of what APCERT has achieved. And all these would not have been possible without the contribution from our members.

The participation and results from the APCERT Drill this year were encouraging. 20 teams, that is nearly 80% of all member teams, participated in the drill and some teams joined this meaningful event the first time. The coordination network that has been built up within the Asia-Pacific region was once again verified on its effectiveness and prompt response to latest threats. Other than participating as a “player” of the drill, many teams participated in organizing the event, including designing the scenario and developing the artifacts and scripts in the exercise. All these involvement will definitely help upgrade the skills and capabilities of the teams concerned. I encourage teams to actively participate in organizing the drill in future.

The Code of Conduct working group has developed a document for member teams to follow. With the approval of this document, the Steering Committee will review the Operational Framework to link the documents together, including defining the actions to take in case of infringement of these rules.

Four new teams joined the APCERT family this year and furthered our objective in enhancing the regional coordination.

I would like to take this opportunity to thank the steering committee members for their contribution last year. I look forward to the continual support from our members to make the APCERT very successful organization in the years to come.

Roy Ko
Chair, APCERT
Centre Manager, HKCERT

I. About APCERT

1. Objectives and Scope of Activities

APCERT *(Asia Pacific Computer Emergency Response Team)* is a coalition of the forum of CERTs *(Computer Emergency Response Teams)* and CSIRTs *(Computer Security Incident Response Teams)*. The organization was established on February 2003 to encourage and support the activities of CERTs/CSIRTs in the Asia Pacific region.

APCERT will maintain a trusted contact network of computer security experts in the Asia-pacific region to improve the regions' awareness and competency in relation to computer security incidents through:

1. enhancing Asia-Pacific regional and international cooperation on information security;
2. jointly developing measures to deal with large-scale or regional network security incidents;
3. facilitating information sharing and technology exchange, including information security, computer virus and malicious code, among its members;
4. promoting collaborative research and development on subjects of interest to its members;
5. assisting other CERTs and CSIRTs in the region to conduct efficient and effective computer emergency response;
6. providing inputs and/or recommendations to help address legal issues related to information security and emergency 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 computer security incidents, widespread security vulnerabilities and incident coordination throughout the region. One important role of CERTs/CSIRTs is education and training to raise awareness and encourage best practice. APCERT coordinates activities with other regional and global organizations, such as the Forum of incident Response and Security Teams (FIRST) <www.first.org>, and TF-CSIRT, a task force that promotes collaboration between CSIRTs at the European level <www.terena.nl/tech/task-forces/tf-csirt/>.

The geographical boundary of APCERT activities are the same as that of 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

At present, APCERT Chair is HKCERT (Hong Kong Computer Emergency Response Team Coordination Centre). Deputy Chair is SingCERT (Singapore Computer Emergency Response Team). JPCERT/CC (Japan Computer Emergency Response Team/Coordination Center) serves as secretariat.

URL: http://www.apcert.org
Email: apcert-sec@apcert.org.

2. APCERT Members

APCERT was formed in 2003 by 15 teams from 12 economies across the Asia-Pacific region, and has increased its membership since then. In 2010, TechCERT, MonCIRT and CERT Australia have been approved as General Member of APCERT. Also, BruCERT has upgraded its membership to Full Member of APCERT.

As of December 2010, APCERT consists of 26 teams from 17 economies across the AP region, of which 18 teams are full members and 8 teams are general members.

Full Members

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

General Members

Team	Official Team Name	Economy
BDCERT	Bangladesh Computer Emergency Response Team	Bangladesh
BP DSIRT	BP Digital Security Incident Response Team	Singapore
CERT Australia	CERT Australia	Australia
GCSIRT	Government Computer Security and Incident Response Team	Philippine
ID-SIRTII	Indonesia Security Incident Response Team of Internet Infrastructure	Indonesia
MonCIRT	Mongolian Cyber Incident Response Team	Mongolia
NUSCERT	National University of Singapore Computer Emergency Response Team	Singapore
TechCERT	TechCERT	Sri Lanka

3. Steering Committee (SC)

Since the last APCERT AGM held in March 2009, Chinese Taipei, the following members served as APCERT Steering Committee (SC).

- HKCERT (Chair)
- SingCERT (Deputy Chair)
- AusCERT
- KrCERT/CC
- JPCERT/CC (Secretariat)
- MyCERT
- ThaiCERT

4. Working Groups (WG)

There are 5 Working Groups in APCERT.

1) Accreditation Rule WG

- Objective: To develop an accreditation scheme for APCERT members
- Members: JPCERT/CC (Chair), AusCERT, HKCERT, KrCERT/CC and MyCERT
- Status: Inactive; Work completed

2) Training & Communication WG

- Objective: To discuss a training mechanism within APCERT (i.e. information exchange, CERT/CSIRT training)
- Members: TWCERT/CC (Chair), AusCERT, KrCERT/CC, MyCERT and SingCERT
- Status: Inactive; Work completed with no further follow up actions

3) Finance WG

- Objective: To discuss membership fee in the short run and develop a concrete scheme in the long run
- Members: JPCERT/CC (Chair), AusCERT, HKCERT, KrCERT/CC, TWCERT/CC and TWNCERT
- Status: Inactive; Work completed in 2009 following AusCERT proposal to Steering Committee and Annual General Meeting.

4) **TSUBAME WG** (formed in 2009)

- Objectives：
  - Establish a common platform for Internet threat monitoring, information sharing & analyses in Asia-Pacific region
  - Promote collaboration among CSIRT in Asia-Pacific region by using the common platform
  - Enhance capability of global threat analyses by incorporating 3D Visualization features to the common platform
- Members： JPCERT/CC (secretariat) and TSUBAME project members
- Status： Active； Held Tsubame Workshop in 2010

5) **Code of Conduct WG** (formed in 2009)

- Objective： To review the existing practices and to define the responsibilities of APCERT members in areas of APCERT as a community
- Members： Steering Committee, BKIS and SLCERT
- Status： Active； Draft Code of Conduct to be submitted to Steering Committee and Annual General Meeting.

5. APCERT Website

JPCERT/CC manages and updates the APCERT website <www.apcert.org>.
On a temporary basis, AusCERT hosts the Point of Contact (POC) information for APCERT POC teams.　Access is by password only for APCERT teams.

II. APCERT Activity Report 2010

1. International Activities and Engagements

APCERT has been active in representing and promoting APCERT in various international events. From January 2010 to December2010, APCERT members have hosted, participated and/or contributed in the following events:

- **APCERT Drill 2010**

  http://www.apcert.org/documents/pdf/Drill2010_PressRelease.pdf

  On 28th January, 2010, APCERT Drill 2010, the 6th APCERT Cyber Exercise Drill, was successfully held with participation from 16 teams of 14 economies (Australia, Brunei, China, Chinese Taipei, Hong Kong China, India, Indonesia, Japan, Korea, Malaysia, Singapore, Sri Lanka, Thailand and Vietnam). The theme of the drill was "Fighting Cyber Crimes with Financial Incentives" and was coordinated by HKCERT, CNCERT/CC, MyCERT with scenarios designers of BKIS and SLCERT.

- **2nd PacCERT Working Group Meeting**

  http://www.itu.int/ITU-D/asp/CMS/Events/2009/PACCERT/index.asp

  The International Telecommunication Union (ITU) with support from the Department of Broadband, Communications and the Digital Economy (DBCDE), Australian Government, commissioned AusCERT to undertake a readiness assessment for establishing a Pacific regional CERT (PacCERT).

  APCERT secretariat shared a presentation on APCERT activities in the 2nd PacCERT Working Group Meeting held on 11-12 February 2010, Suva, Fiji Islands.

- **AP* Retreat meeting**

  http://www.apstar.org/apstar_agenda.php?p_content_category_id=2&p_meeting_id=30

  MyCERT shared a presentation on APCERT activity updates at the AP* Retreat Meeting held on 28 February 2010, Kuala Lumpur, Malaysia. AP* Retreat Meeting gathers Internet-related organizations from the Asia Pacific region, to share their respective activities and to discuss issues that need to be considered as Asia-Pacific community, as well as to establish a trust relationship among the organizations. The meeting is held every once or twice a year.

- **APCERT AGM & Conference 2010**

http://apcert2010.thaicert.org/

APCERT AGM & Conference 2010 took place in Phuket "Pearl of the Orient", Thailand between 3-4 March 2010, hosted by Thai Computer Emergency Response Team (ThaiCERT). As the countries in Asia Pacific region focus on the development and adoption of "Web 2.0", the next generation of the cyber world including web-based communities, web applications, social networking sites, video-sharing sites, wikis, and blogs, the theme of APCERT 2010 is "security on social networks". The conference consisted of three parts:

(1) A meeting of the Steering Committee members;

(2) The Annual General Meeting (AGM) of all APCERT members; and

(3) Open conference sessions for all parties.

The event was a great opportunity for people who are interested in information security, Web 2.0 and related issues to share knowledge and experiences among each other within a casual environment. Phuket was proud to extend its hospitality to the international community in the field of information technology with the focus on security, bringing valuable knowledge and of course unforgettable memories and experiences.

- **APCERT Workshop 2010 - TSUBAME Network Traffic Monitoring Project**

APCERT Workshop 2010 on TSUBAME Network Traffic Monitoring Project, held in conjunction with APCERT AGM & Conference 2010, was organized by JPCERT/CC to enhance the TSUBAME project and the cooperation among its members.

The morning session was open to the public for understanding and exchanging information about TSUBAME. The afternoon session was closed to TSUBAME project members, including a hands-on class on TSUBAME data analysis, and discussions on future plans.

- **Support for Network Security of Expo 2010 Shanghai China**

http://en.expo2010.cn/

Expo 2010 was held from 1 May to 31 October 2010 in Shanghai, China, with more than 200 countries/regions and international organizations to give their exhibitions, and more than 70 million audience from all over the world. As during the Beijing 2008 Olympic Games, CNCERT/CC joined the network security work of Expo 2010, mainly safeguarding its systems as well as watching the Internet security around them. CNCERT/CC asked all APCERT Teams to assist on the network security of Expo 2010, especially on threat warning, attack monitoring, incident handling, as well as data and sample sharing. With APCERT Teams' cooperation, CNCERT/CC successfully accomplished its mission.

- **AusCERT's Annual Award for Organisational Excellence in Information Security awarded to APCERT at AusCERT 2010**

http://awards.scmagazine.com.au/winners-finalists-2010#annual

As part of the IT Security industry leading global awards program, the SC Magazine Awards Australia was organized to recognize the professionals, organizations and products that repulse threats confronted by users on a daily basis. An expert judging panel <http://awards.scmagazine.com.au/judging-panel/> of Australian security experts honoured outstanding work by their peers in the trenches, the innovations happening in the vendor and service provider communities and excellence from governments, businesses and charities.

This is the second consecutive year for these awards and follows the footsteps of the SC Awards in Europe and the US, now in its 13th year. These awards were run in the lead up to the AusCERT2010 Conference <http://conference.auscert.org.au/conf2010/>, Australia's premier event for the IT security community, now in its 8th year, where the awards were presented at a gala dinner.

APCERT was declared the winner of the Annual Award for Organizational Excellence in Information Security. This was presented to the organization that in the past year contributed most to information security in the areas of community service, innovation, education, liaison, law enforcement, governance or leadership. Lal Dias of SLCERT who was present at the conference accepted the award on behalf of APCERT.

Photo gallery;

http://www.itnews.com.au/Gallery/175337,photo-gallery-sc-awards-2010-at-auscert-gala-dinner.aspx/1

- **APEC TEL 41**

"Several APCERT Teams participated in APEC TEL (APEC Telecommunications and Information Working Group) 41, where HKCERT, on behalf of APCERT, presented on ""APCERT Drill 2010 (summary report)"" and APCERT perspectives on ""Emerging Security Threat Landscape"" of the region. In the SPSG (Security and Prosperity Steering Group) meeting, there were also other useful presentations from APCERT teams and economies: Gumblar incident analysis by JPCERT/CC, Cyber Security Awareness Raising Activities by Japan and Korea, International PKI and e-Authentication Training Program by Chinese Taipei, and Australian Cyber Security Strategy by CERT Australia.

- **Internet Summit Africa - CSIRT Training (CERT Instructor Training Course for Managers)**

http://africaasia.net/index.html
http://africaasia.net/2010-6-CERT.html

JPCERT/CC participated in the Internet Summit Africa (30 May-10 June 2010, Kigali, Rwanda), and lectured a CERT Instructor Training Course for Managers, organized by AAF (Africa Asia Forum on Network Research & Engineering). The training contents included 1) Internet security trends, 2) overview of CSIRT and fundamentals of computer security incident handling, 3) creating a CSIRT, and 4) international CERT activities, where JPCERT/CC introduced activities of APCERT as the CSIRT community in the Asia Pacific region.

- **AP* Retreat meeting**

http://www.apstar.org/apstar_agenda.php?p_content_category_id=2&p_meeting_id=31

AP* is the community of Asia Pacific Internet organisations, 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. The AP* Retreat meeting is held every once or twice a year, which provides an opportunity to share activities, discuss trends, and to establish a trust relationship.
AusCERT represented APCERT in this meeting and presented APCERT activity updates.

- **ACID (ASEAN CERT Incident Drill) 2010**

ACID (ASEAN CERT Incident Drill) 2010, lead and coordinated by SingCERT, entered its fifth iteration this year with participation from ASEAN CERTs and APCERT Teams. The drill was completed successfully with focus on detection and investigation of attacks using common file formats as transmission vectors for exploit.

- **Support for XIX Commonwealth Games 2010 Delhi**

http://www.cwgdelhi2010.org/

The XIX Commonwealth Games 2010 Delhi was completed successfully without any major security incidents. CERT-In extended appreciation to the support and cooperation extended by APCERT Teams for meeting any eventuality during the Commonwealth Games.

- **APCERT as supporting organization for CSM-ACE 2010**

http://www.csm-ace.my/event2010/event2010-main.html

CSM-ACE (Cyber Security Malaysia Awards, Conference & Exhibition) 2010, endorsed by MOSTI (Ministry of Science, Technology and Innovation) and organized by CyberSecurity Malaysia, was held as an annual industry conference that shapes the regional information security landscape. Expected to draw over 1,000 participants from around the world, the CSM-ACE 2010 brought together some of the most influential and innovative minds in business, government, academia and key information security players to exchange policies, ideas and technology. Themed as "Securing Our Digital City", it was a proactive initiative to address national security concerns and to build community confidence by mitigating the multi-dimensional cyber security challenges in critical

infrastructure, economic and cyber crimes. The vision is to create a cyber-secured community that is engaged at the local, state, national and international levels.

APCERT served as a supporting organization for CSM-ACE 2010.

- **Support for APEC 2010 in Yokohama, Japan**

http://www.mofa.go.jp/policy/economy/apec/2010/

The APEC 2010 meetings were completed successfully without any major security incidents. JPCERT/CC extended appreciation to the support and cooperation extended by APCERT Teams concerning any potential information to secure against cyber attacks targeting the IT infrastructure of the event.

- **APT Cybersecurity Forum**

http://www.apt.int/2010-CSF

The APT Cybersecurity Forum, organized by the Asia Pacific Telecommunity (APT) and hosted by the Department of Broadband, Communications and the Digital Economy (DBCDE), Government of Australia, was held with invitations also extended to CERTs including APCERT and the newly formed PacCERT. AusCERT represented APCERT at this forum and presented on APCERT activities to share its expertise to the relevant participants.

- **AfriNIC-13 - CSIRT Training (CERT Workshop for Trainers)**

http://meeting.afrinic.net/afrinic-13/index.php/the-meeting/agenda

JPCERT/CC participated in AfriNIC-13 (20-26 November 2010, Johannesburg, South Africa), and lectured a CERT Workshop for Trainers, organized by AAF (Africa Asia Forum on Network Research & Engineering). The training contents included 1) overview of CSIRTs (operational and technical), 2) overview of information security from a technical perspective, 3) OS programming, 4) basics of incident analysis including hands-on sessions, 5) information gathering and analysis, 6) publishing technical documents, 7) advanced analysis on websites and malware, and 8) how to conduct incident handling drills.

JPCERT/CC introduced APCERT activities and the APCERT Drill in this training on behalf of APCERT.

- **APCERT's status as APEC TEL General Guest terminates**

APCERT had participated and contributed to APEC TEL as General Guest in the past few years and fulfilled its term as of December 2010.

Other International Activities and Engagements

- **APEC TEL SPSG (Security and Prosperity Steering Group)**

  Mr. Jinhyun Cho of KrCERT/CC served as convener of APEC TEL SPSG (Term of service was fulfilled at APEC TEL 41 (6-12 May 2010). APCERT would like to thank Mr. Jinhyun Cho for his contribution in bridging APCERT with APEC TEL SPSG in the past few years.)

- **FIRST Technical Colloquium and CNCERT/CC Conference 2010**

  The APCERT Chair attended the September 2010 FIRST Technical

Colloquium and CNCERT/CC Conference 2010 in Beijing on 12-15 September 2010, and spoke on the topic "APCERT Cyber Drill". APCERT members that attended the conference had a dinner meeting hosted by CNCERT/CC.

- **DotAsia**

  APCERT was invited to be 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.

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

  Ms. Yurie Ito of JPCERT/CC serves as Steering Committee member and Board of Director of FIRST

2. Approval of New General Members / Full Members

From the last APCERT AGM in March 2010 to December 2010, the following teams newly joined APCERT General Member / Full Member.

- TechCERT (Sri Lanka) was approved as General Member as of 2 March 2010
- MonCIRT (Mongolia) was approved as General Member as of 2 March 2010
- BruCERT (Brunei) was approved as Full Member as of 2 March 2010
- CERT Australia (Australia) was approved as General Member as of 1 November 2010

3. APCERT SC Meetings

Since the last APCERT AGM held in March 2010 to December 2010, SC members held 1 face-to-face meeting and 3 teleconferences to discuss on APCERT operations and activities.

III. Activity Reports from APCERT Members

Full Members

1. AusCERT Activity Report

Australian Computer Emergency Response Team - Australia

The following information contains information about AusCERT's activities during 2010.

1. ABOUT AusCERT

1.1 Introduction

AusCERT (Australian Computer Emergency Response Team) is an independent, non-government, self-funded, not-for-profit team of information and technical security professionals based at the University of Queensland. The University of Queensland is one of Australia's premier learning and research institutions.

In addition to supporting its members, AusCERT provides assistance to a broad section of the community affected by cyber attacks in Australia and overseas and responds to requests for assistance from its CERT counterparts.

AusCERT's core services are to:

collect, analyse and provide advice about computer network threats and vulnerabilities; help to mitigate Internet attacks directed at Australian Internet users and networks; and provide advice about issues affecting Internet security in Australia and globally.

1.2 Establishment

AusCERT was officially established on 8 March 1993 through the collaboration of three Brisbane based universities, including the University of Queensland. Over time, as the Internet grew and government, business and ordinary users began to use the Internet for daily communications and business, AusCERT's focus changed from being university centric to include the interests of all sectors.

1.3 Staffing

AusCERT currently employs 14 staff.

1.4 Constituency

AusCERT's constituents are its members and Australian Internet users in the public and private sector, home and business.

AusCERT works closely with Australian government agencies, industry and technology vendors and provides computer security and incident handling advice to a range of subscribers throughout Australia, New Zealand and the Asia-Pacific region. All Australian universities and the majority of New Zealand universities are members of AusCERT and there is a strong relationship with the Council of Australian University Directors of Information Technology (CAUDIT).

AusCERT participates in the Australian government's IT Security Experts' Advisory Group (ITSEAG).

2. ACTIVITIES AND OPERATIONS

During 2010, AusCERT:

- provided incident response to help organisations mitigate Internet based attacks against their networks (see figure 1-7) ;
- mitigated online attacks that have compromised personal identity information (PII) by notifying the public and private sector organisations whose customers or clients have been affected (see figure 4);
- published security bulletins,[1] (including security bulletins about specific cyber threats affecting Australian networks and Internet users) (see figure 8);
- provided public outreach, education and awareness raising about Internet security issues by maintaining the Stay Smart Online Alert Service,2 on behalf of the Australian government, and through the media;
- provided a secure and trusted certificate issuing service for the education and research sector;
- provided information and expertise to law enforcement about specific cyber attacks affecting or emanating from Australian networks;
- participated in government, CERT and industry multi-lateral meetings including cyber security exercises with a range of global partners;
- communicated, cooperated and built relationships with industry, domain name registries, telecommunication providers and national CERT

[1] https://www.auscert.org.au/1.

[2] www.ssoalertservice.net.au

counterparts overseas.

2.1 Incident Handling

The majority of AusCERT's work as a computer security incident response team involves proactively looking for evidence of Internet attacks directed at Australian Internet users and organisations with an online presence. AusCERT uses a number of methods to locate, analyse and mitigate these attacks. While these are not the only incidents handled by AusCERT, they represent common forms of cyber attack.

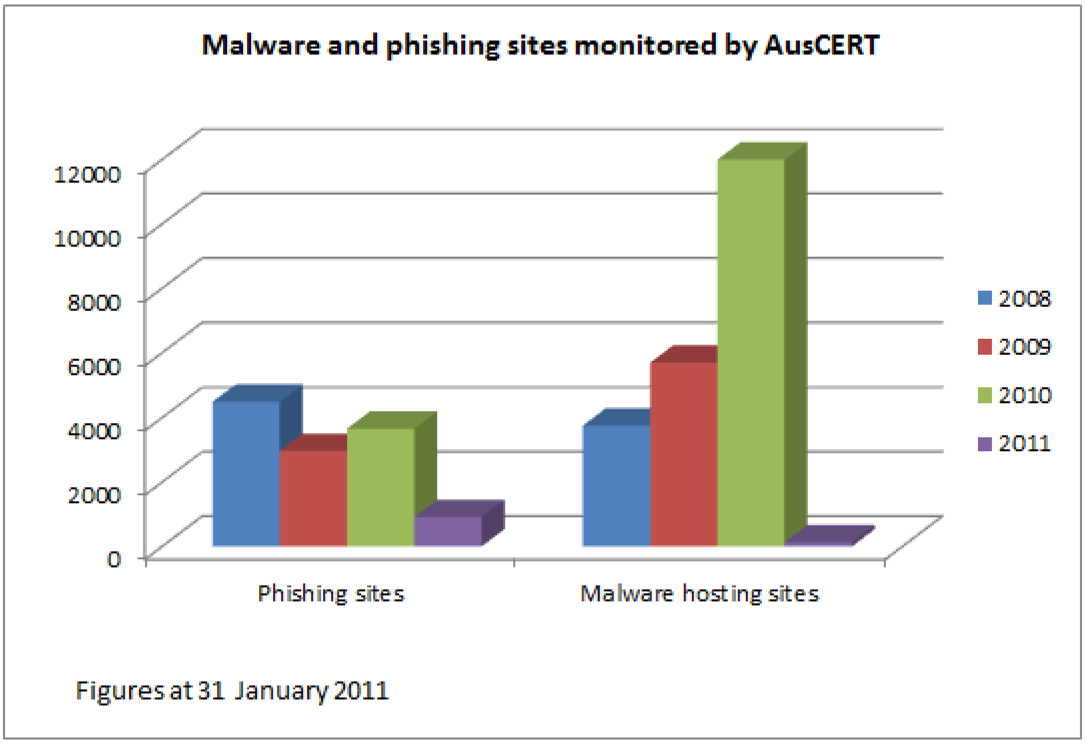
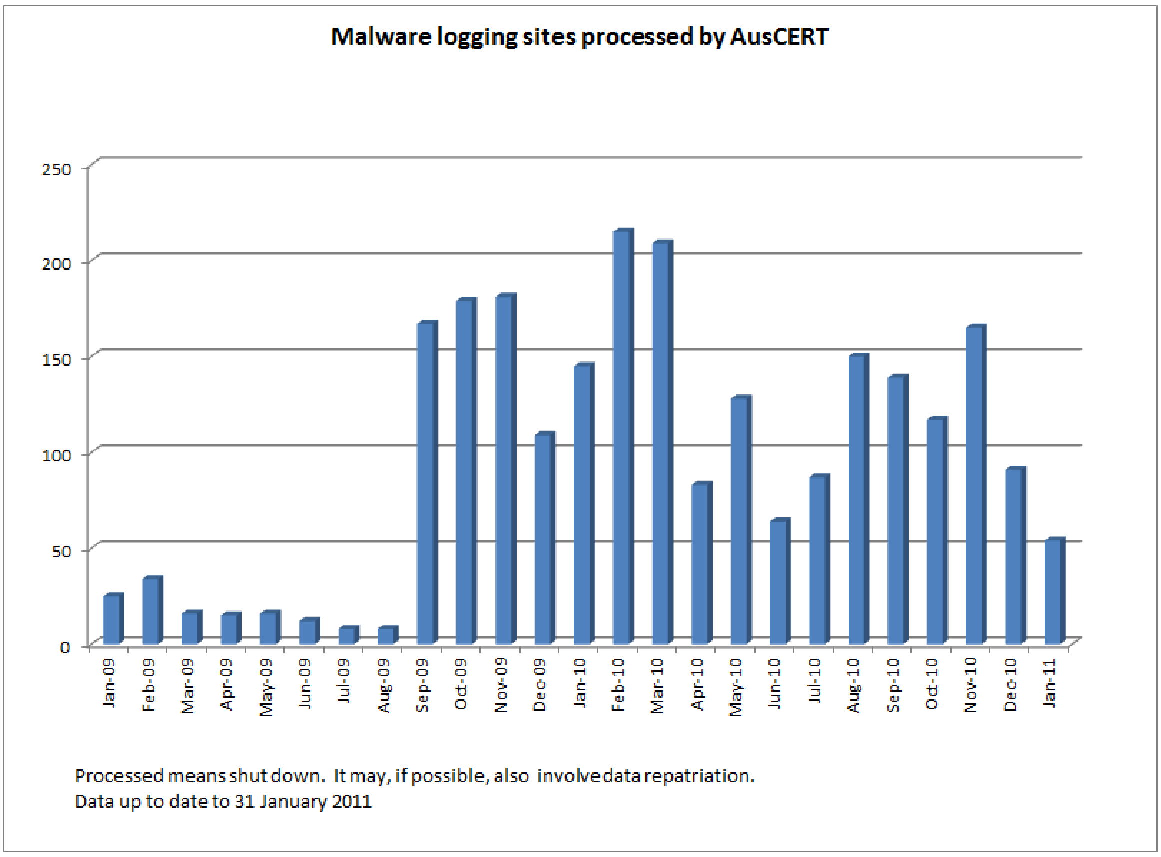


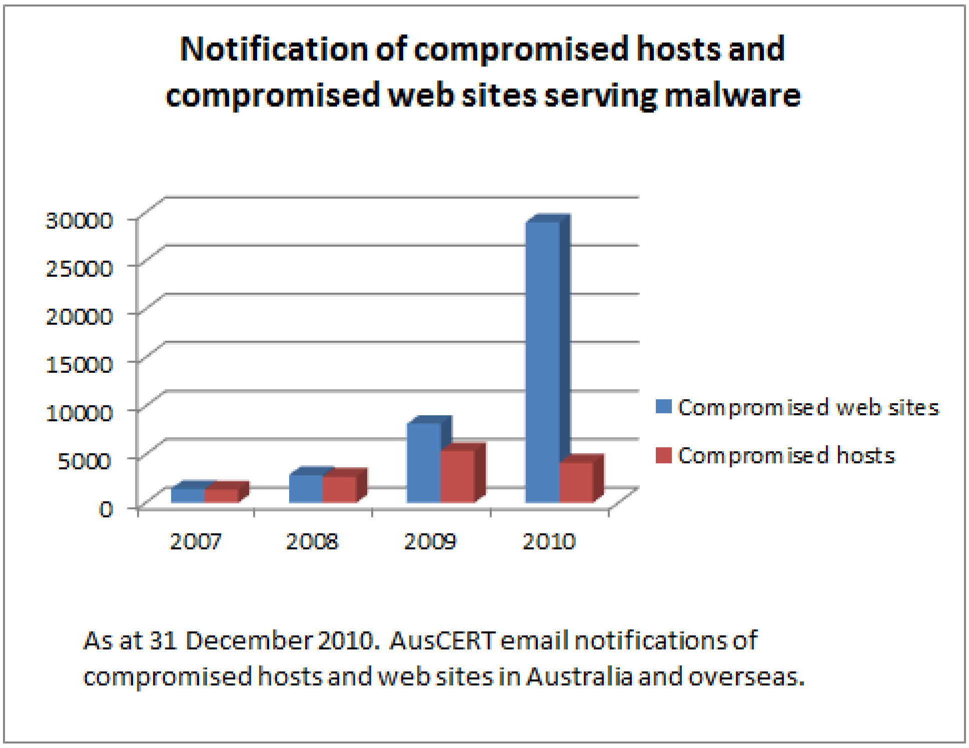
Figure 1



Malware logging sites processed by AusCERT

Processed means shut down. It may, if possible, also involve data repatriation.
Data up to date to 31 January 2011

Figure 2



Notification of compromised hosts and compromised web sites serving malware

As at 31 December 2010. AusCERT email notifications of compromised hosts and web sites in Australia and overseas.

Figure 3

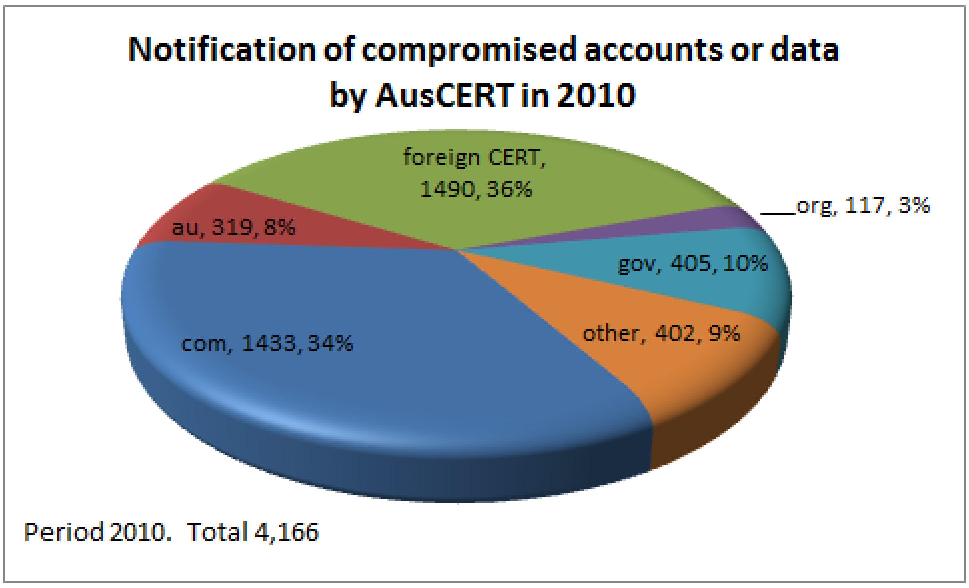


Figure 4

Figure 4 shows the number of email notifications made by AusCERT including information about compromised accounts and data in Australia and overseas repatriated from malware logging sites as at 31 December 2010.

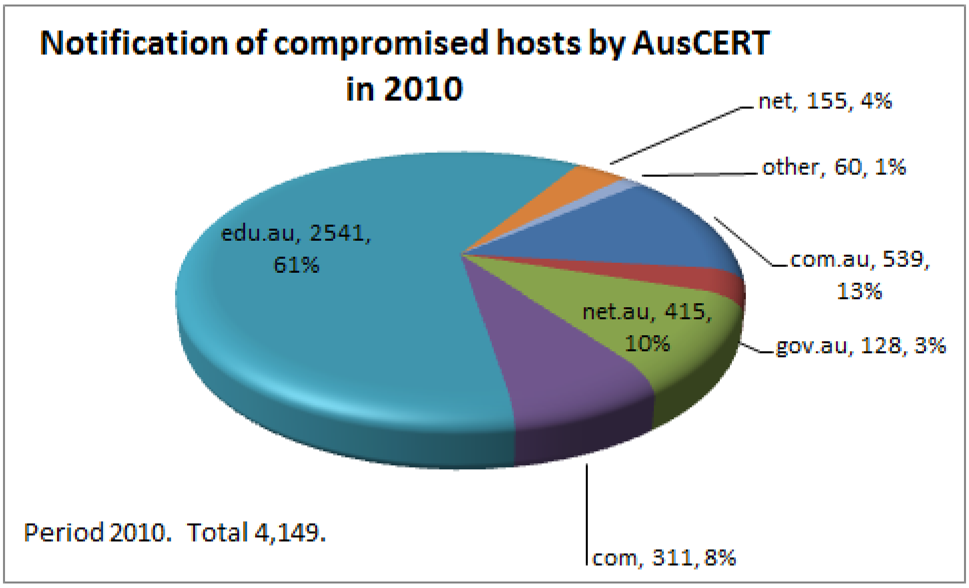


Figure 5

Figure 5 shows the number of email notifications made by AusCERT regarding compromised hosts in Australia and overseas as at 31 December 2010.

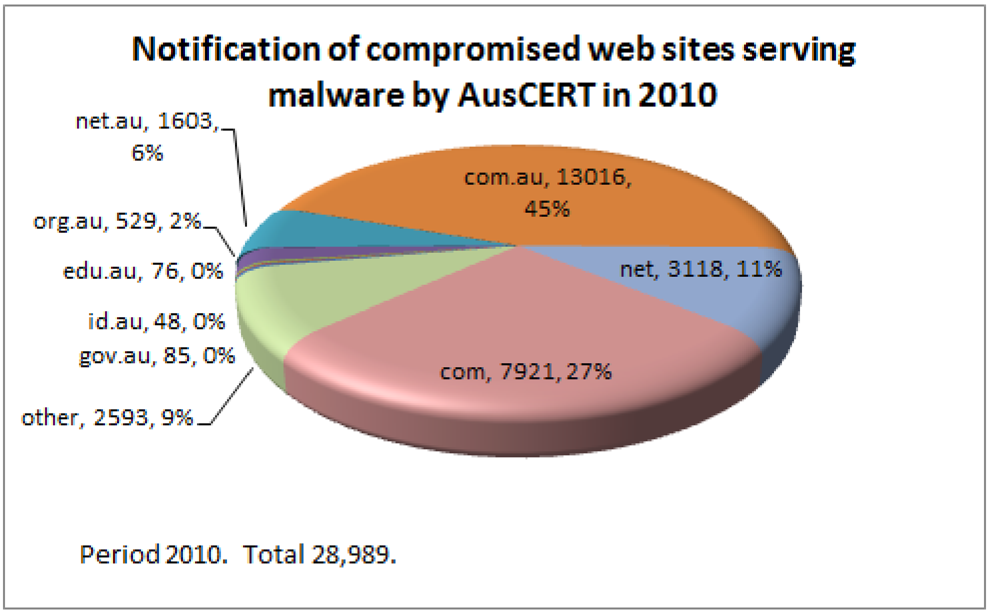
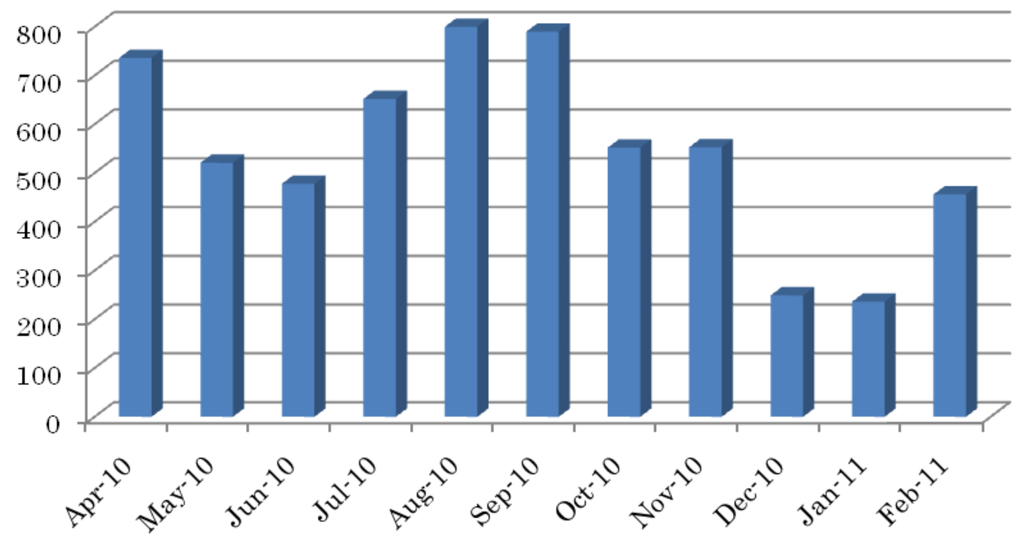


Figure 6

Figure 6 shows the number of email notifications made by AusCERT regarding compromised web sites in Australia and overseas as at 31 December 2010.

Compromised .au web sites serving malware



Distinct .au domains *per month* between 1 April to 28 February 2011. Doesn't include multiple pages per domain or multiple attacks per month. AusCERT notified owners where possible. Total 6,023.

Figure 7

2.2 Security bulletins and blogs

AusCERT publishes security bulletins as part of its services. During 2010, AusCERT published 1,179 external security bulletins (ESB), and 254 AusCERT bulletins. Sixty-eight blogs were published.

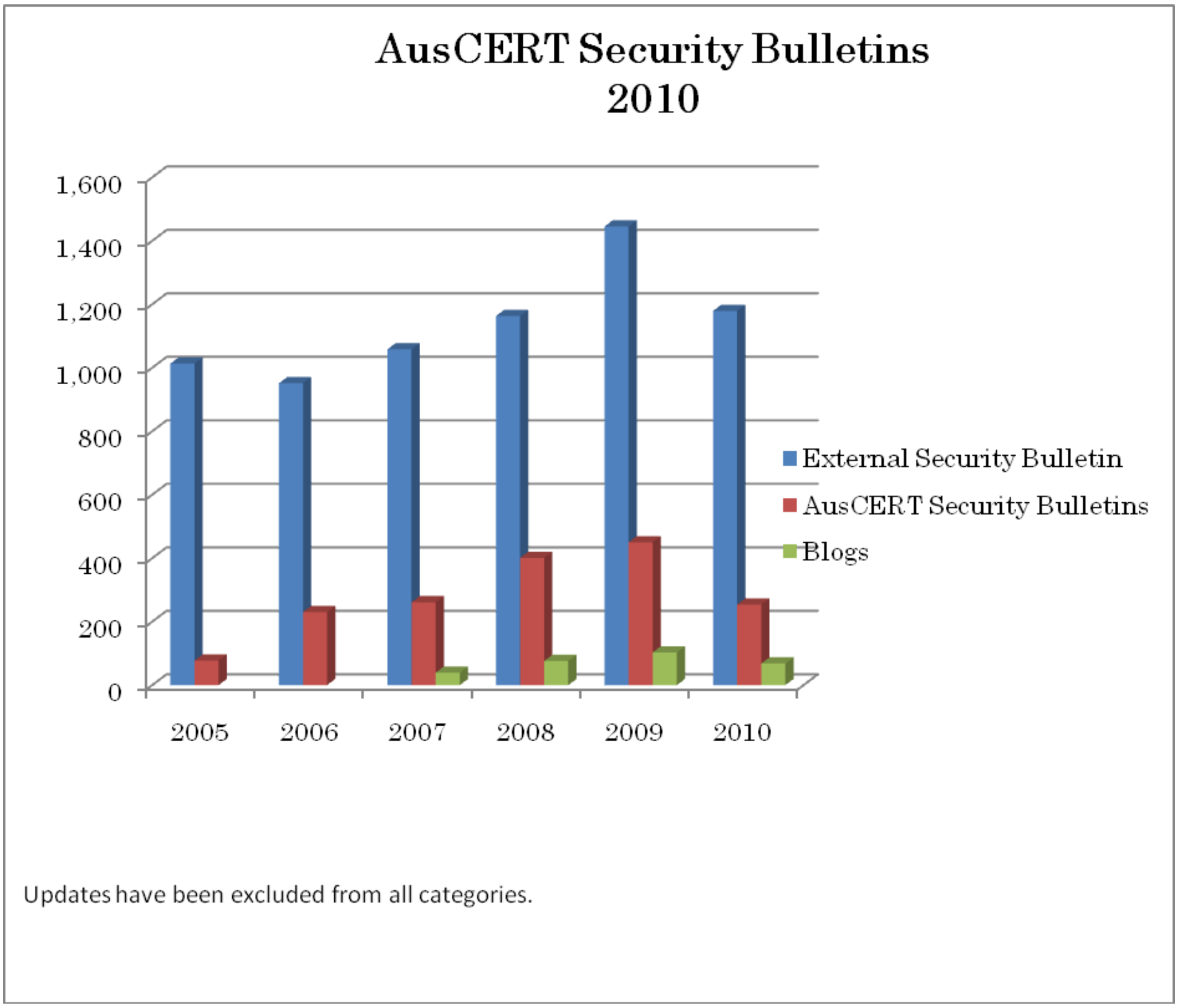


Figure 8

2.3 Network monitoring

AusCERT collaborates with a number of international partners operating monitoring projects by hosting sensors for the purposes of detecting compromised hosts and analysing cyber attacks.

2.4 Stay Smart Online Alert Service

In 2010 AusCERT continued to provide a service under contract from the Australian government, which is part of the Australian government's broader Stay Smart Online initiative.[3] The Stay Smart Online Alert Service is a free service aimed at home users and SMEs with little or no technical knowledge. The service provides access to email, web and RSS feeds and includes a

[3] www.staysmartonline.gov.au

monthly newsletter and fact sheets. [4] AusCERT published 57 alerts and 25 advisories during 2010.

2.5 AusCERT Certificate Services (AusCERT-CS)

The AusCERT Certificate Service, which utilises Comodo certificate services, provides Australia's education and research community with SSL server certificates that are widely recognised by popular web browsers, mobile devices and other user applications.

Server, personal and code-signing certificates are available. More information about the AusCERT Certificate Services is available from:
http://cs.auscert.org.au

3. EVENTS ORGANISED / CO-ORGANISED

3.1 Conferences

AusCERT held its annual Asia-Pacific Information Security Conference at the Gold Coast Australia in May 2010 with around 1,200 delegates.[5] Coinciding with the annual AusCERT conference, AusCERT helped facilitate an Australian law enforcement workshop and hosted other networking and information sharing events for CERTs and ISPs. Also, AusCERT hosted an online crime symposium for key stakeholders and organisations whose customers or users are at risk of being affected by cybercrime and/or are in a position to prevent or mitigate cybercrime.

During 2010, AusCERT participated in a number of international conferences and events, including:

- APCERT2010, Phuket Thailand
- FIRST conference and technical colloquium
- APT Cybersecurity Forum for Asia Pacific
- Underground Economy, Lyon
- GovCERT.nl Symposium in Rotterdam

4. ACHIEVEMENTS

4.1 Presentations and awareness raising

AusCERT has given presentations at several conferences throughout 2010. These include presentations at APAN29 conference in Sydney, ITU Working

[4] www.ssoalertservice.net.au
[5] conference.auscert.org.au/conf2010/

Group Meeting in Suva, Fiji and the Underground Economy conference in France.

For the most part, these presentations have sought to give various communities knowledge of the cyber threat environment and allow them to consider whether their own preparations or strategic plans – be they at organisational, national or at international level are adequate to meet the needs of the current threat environment and future anticipated threats.

4.2 Best security initiative award winner

In 2010, AusCERT won the 2010 Australia and New Zealand Internet Best Practice Awards[6] for its work to repatriate data stolen from malware infected computers so the affected parties can mitigate the harm. The initiative has allowed many thousands of victims all around the world to minimise subsequent harm arising from the compromise of their computers by malware.

.auDA & InternetNZ
Internet Best Practice Awards 2010
Best Security Initiative Award WINNER

4.3 Publications

As part of its efforts to distribute relevant information in an efficient manner, AusCERT continued to publish a web log and a twitter feed.[7]

This provides a platform for AusCERT to informally discuss current activity and interesting developments in the security threat environment and promote articles from other information security professionals or the media of interest.

5. INTERNATIONAL COLLABORATION

AusCERT continues to be actively involved with APCERT, serving on the Steering Committee again during 2010. AusCERT also manages the APCERT mailing lists and restricted web access to the APCERT Point of Contacts.

[6] http://www.auscert.org.au/13352
[7] http://twitter.com/auscert

AusCERT also works closely with the UK Payments Administration (previously APACS), FIRST, Digital Phishnet, Anti Phishing Working Group, IMPACT, the ITU and European government CERTs and many open and closed information security groups.

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 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

The year 2010 saw a sudden rise in the number of fake antivirus programs, with 2.2 million computers infected. Virus spread for systems intrusion and DDoS attacks, as well as the return of data destroying virus and the new trend of malware faking data files, etc. are also the dominant virus issues in the past year.

Below is the summary of virus condition in 2010, as well as some predictions for the year 2011.

- **The explosion of Fake AV**

  In last year's report, Bkis predicted: "2010 will see the sudden rise in the number of fake antivirus programs". The explosion in the number of computers infected with fake AV did happen in 2010. In fact, 2.2 million computers fell victims to Fake AV, 5.5 times more than the figure 258,000 of 2009.

  The common trick of Fake AVs is inducing users to websites of fake online virus scanning services to install malwares on users' computers. According to Bkis research, the primary reason many computers in Vietnam are infected with this kind of virus is the habit of using unlicensed or cracked software. With this habit, even already warned by experts, users still unaffectedly click every unknown link. This is the fatal weakness that leads to the infection of Fake AV.

- **Faking data files, the new trend of virus**

  More than 1.4 million computers were infected with virus faking folders, image files, word files, excel files, etc. According to Bkis analysis, this family of virus will make up a new trend in the near future.

With the disguising icon, the virus' execution file looks exactly like a folder or an image, word, excel file. Thus, users or even experts are easily fooled to open malicious file without any suspicion. This is also the explanation for the breakneck spread of this virus family despite its new emergence.

- **The return of data destroying viruses**

  In the previous year, our virus monitoring system detected two waves of newly emerging data destroying virus. These families of virus are named W32.Delfile.Worm and W32.FakeStuxer.Trojan by Bkav. Even though the consequence was not serious and widespread, the return of data destroying virus is expected to be a big threat to users' data in the coming time.

  In accordance with the helical growth model, the coming back of this kind of virus in new forms will bring about more sophisticated behaviours compared with the data destroying viruses in the 90s. These new viruses are equipped with techniques for quickly spreading through the Internet; therefore, they can propagate much faster than their silently spreading predecessors. That's why the new viruses are thousand times more dangerous.

  Today, users tend to store lots of important data on their computers, so the return of data destroying virus with rapid spread will cause serious consequence once these viruses propagate in large scale. To protect computers from this kind of virus, users are recommended to use licensed antivirus software and scan for virus on a regular basis. They should back up their important data on other storage devices to ensure the data's safety upon incidents.

- **Alarm sounding about virus spread for system intrusion and DDoS attacks**

  Recently, many big websites in Vietnam have continuously been intruded by virus, or hit by DDoS attacks. Such attacks together with the disclosure of the classified information of some websites have raised great concern among community.

Bkis have discovered some hacker groups who installed virus on network security systems in Vietnam to steal internal classified information of some organizations. Besides, they also control some software download websites to install virus on computers which download software from these websites. The botnet consisting of the infected computers becomes the jumping-off- point for hacker to perform DDoS attacks against big systems in Vietnam. This is an alarming situation because not only big systems can be attacked any time, but there are also thousands of computers nationwide are controlled by hackers, which affects the whole national security.

Thus, users should be cautious upon software download. Users are recommended to download software from vendor's website, and curtail downloading from intermediate sites, even popular sources. At the same time, users need to update their antivirus software on a regular basis for timely virus prevention.

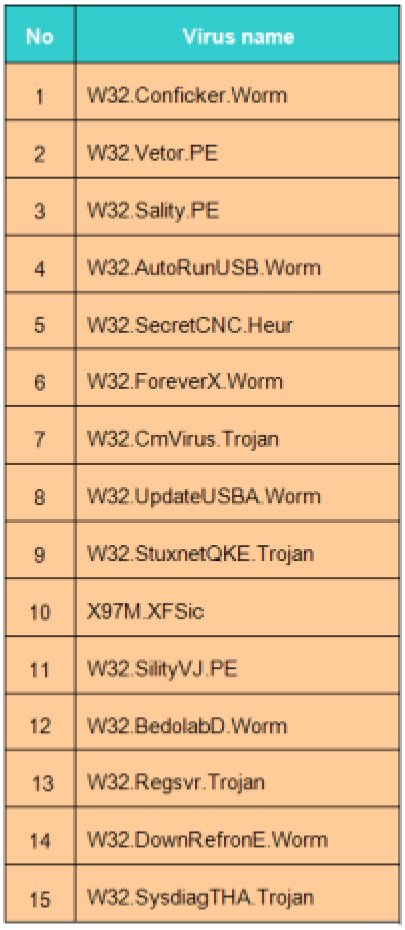
- **General virus statistics in 2010**

According to our monitoring virus system, there were 58.6 millions of computers infected with virus in 2010. On average, there were over 160 thousands of virus infected machines, which is an alarming figure in Vietnam.

There were 57,835 new virus families emerging, but the most widely spread virus is an old virus family, W32.Conficker.Worm. This virus has been rampant worldwide since the end of 2008. However, according to our statistics, there were more than 6.5 million computers infected with Conficker in 2010.

Metamorphic virus continued to occupy top 3 widespread viruses in the year, and became the obsession of Vietnamese users. With the capacity of transformation to hide themselves, two virus families, namely Vetor and Sality, have infected more than 5.9 million computers.

List of top 15 widespread viruses in 2010:



No	Virus name
1	W32.Conficker.Worm
2	W32.Vetor.PE
3	W32.Sality.PE
4	W32.AutoRunUSB.Worm
5	W32.SecretCNC.Heur
6	W32.ForeverX.Worm
7	W32.CmVirus.Trojan
8	W32.UpdateUSBA.Worm
9	W32.StuxnetQKE.Trojan
10	X97M.XFSic
11	W32.SilityVJ.PE
12	W32.BedolabD.Worm
13	W32.Regsvr.Trojan
14	W32.DownRefronE.Worm
15	W32.SysdiagTHA.Trojan

2.2 Threat landscape in 2011 in Vietnam

Rootkit will not be a privilege of some hackers like before, but will become a new trend once this tool is publicized. Metamorphic virus will employ more new techniques to prolong the spread for years.

Due to the popularity of Windows 7 which is able to ensure high security level, the important execution decision is up to the users. Thus, there would be an in increasing growth of virus designed to fool users' sense. Fake-icon virus is the first generation; and this trend is expected to continue in 2011.

Virus with socio-political motivation is to emerge more, taking advantage of popular software download websites to spread. Botnet which consists of the infected computers are used to perform attacks against targeted objects to steal confidential information from individuals and organizations.

More frauds and attacks against cell phones will occur in 2011. There may be first assaults on cell phones to spread malicious codes, mainly in the form of hidden Trojan to steal users' personal information.

3. Events organized / co-organized

3.1 Training Courses

- Network Security Training Courses:
  April 2010: For Engineers of Ministry of Public Security
  July 2010: For Network Administrators from companies (Banks...)

- Security Awareness Training Courses:
  September 2010: 2 classes for PetroVietnam Construction joint stock corporation (PVC)

3.2 Security Advisories

In 2010, we have discovered and published 05 advisories of the software vulnerabilities. For reference, here is the list of advisories:

No	Advisory
	Libxml2 vulnerability in Google Chrome and Apple Safari
	Multiple Vulnerabilities in OpenBlog 1.2.1
	Vulnerability in Flash Slideshow Maker
	Multiple Vulnerabilities in CMS Made Simple
	Multiple Vulnerabilities in BigAce

3.3 Security survey program in Vietnam 2010

An independent research of Bkis shows that virus situation in 2010 has been improved but not much. In 2010, virus resulted in a 5,900 billion VND (~ 282,770,189 USD) loss in Vietnam. This figure is drawn from the survey carried out in January 2011.

The damage is calculated based on the income of computer users and the value of their interrupted working time due to virus related troubles. Accordingly, on average, a single computer user in Vietnam suffers a loss of 1,192,000 VND in 2010. With at least 5 million of regularly used computers nationwide, the total loss in 2010 amounted to as much as 5,900 billion VND.

Below are some judgments about virus situation and users' security awareness in 2010:

- **Slight decline in the rate of infected computers**

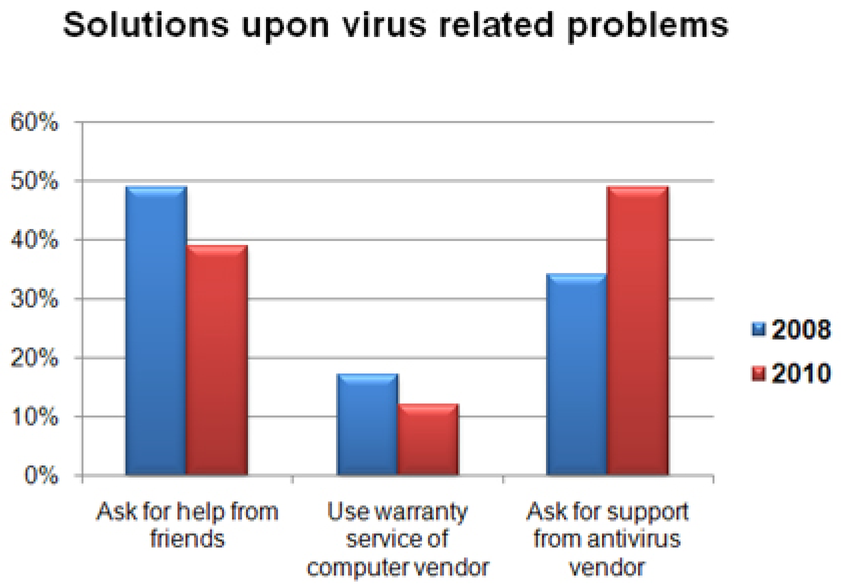
  In 2010, 93 percent of computers in Vietnam were infected with virus at least once. This situation has been improved, but not much, compared with the previous years of around 97 percent. More than one

  USB stick memory continued to be the most common infection vector. Nearly 96 percent of the people surveyed say that their USB drives were infected with virus in 2010.

- **Further improvement in users' security awareness**

  Most of the surveyed people (93 percent) think that a licensed antivirus software is necessary for effective virus removal. If users use unlicensed software, they will meet difficulty dealing with virus related problems since they do not get technical support from the antivirus vendor.

  The ways that users handle with virus related issues have been changed considerably compared with 2008. In 2010, 49 percent of the users said that they would ask for support from antivirus vendor upon such incidents; meanwhile this figure was only 34 percent in 2008. So gradually, users know how to better protect themselves against virus and how to employ technical support professionally.



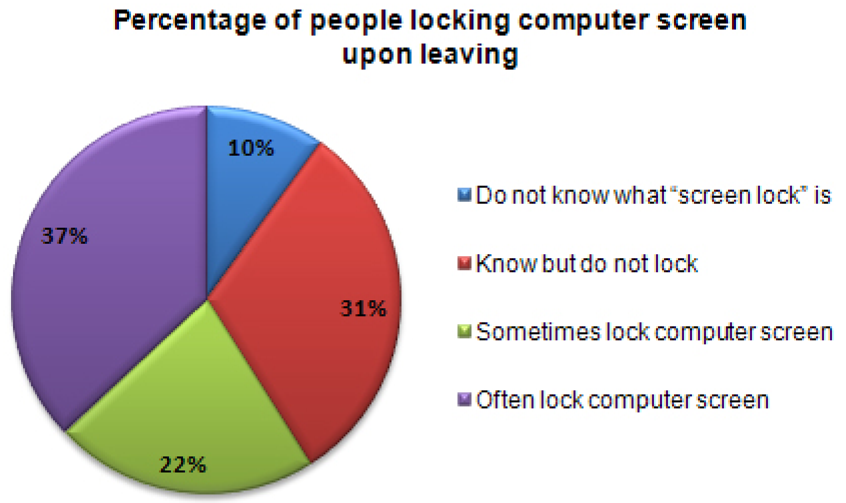
A good sign is that users are now cautious with links sent via chat programs or emails. The survey shows that there were only 10 percent of users who easily click the strange links. Nearly 67 percent of them say that they will confirm the link' source if it is sent from an acquaintance and ignore it if it is from a stranger. This is also the safest way to deal with the case.

- Good awareness but actual action does not live to expectation

  Private password may open a whole world of an individual, for instance, working computer, email, etc. but there were still 53 percent of users who do not pay due attention to protect their password.

  Users need to create a strong password to avoid password theft or disclosure. A strong password is the one which has at least 9 characters, consisting of number, letter, capital letter and symbols like @#$%^&*, etc. Besides, passwords must not be disclosed to anyone or written somewhere. Users should also change their password regularly.

  Another simple technique to ensure the security of your computer is to lock the screen when it is not in use. Up to 63 percent of the users do not lock their screen regularly or have never performed screen lock when they leave their computer; though this can be simply done with "Windows + L" keystroke.



Businesses should apply screen lock policy to all their staff. This is also one of the essential requirements when developing Information Security Management standard ISO 27001.

3.4 Seminar

- April 2010: Organized an seminar about the Vulnerabilities in Internet Banking Systems in Vietnam
- June 2010: co-organized with VINSA (Vietnam Information Security Association) a seminar about the vulnerabilities in 3G network in Vietnam.

4. Achievements

- June 2010: Bkis honored for outstanding achievement in implementing Resolution No 09/CP, National program of crime prevention in businesses and organizations, period 1998 – 2010 by Ministry of Public Security
- November 2010: Bkis security researcher awarded by Google for vulnerability discovery

5. International Collaboration

- July 2010: developed a tool to detect all kinds of viruses exploiting .lnk vulnerability (example: Stuxnet) and shared tool in the security community.
- February 2011: Bkis took part in the APCERT Drill as a member of the organizing committee and a member of the exercise control group

3. 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 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.

In the Information Technology (Amendment) Act 2008, CERT-In has been designated 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 was operational since January 2004. The constituency of CERT-In is the Indian cyber community. In the Information Technology (Amendment) Act 2008, CERT-In has been designated to serve as the national agency in the area of cyber security.

1.1.2 Workforce power

CERT-In has a 30 member technical staff.

1.1.3 Constituency

The constituency of CERT-In is the Indian cyber community. CERT-In works cooperatively with Chief Information Officers and system administrators of various sectoral and organisational networks of its constituency.

2. Activities and Operations of CERT-In

- 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
- Promotion best practices and periodic security assessment through Security Assurance Framework

2.1 Incident handling Reports

The summary of activities carried out by CERT-In during the year 2010 is given in the following table:

Activities	Year 2010
Security Incidents handled	10315
Security Alerts issued	43
Advisories Published	72
Vulnerability Notes Published	274
Security Guidelines Published	1
White papers/Case Studies Published	1
Trainings Organized	26
Indian Website Defacements tracked	14348
Open Proxy Servers tracked	2492
Bot Infected Systems tracked	6893814

Table 1. CERT-In Activities during year 2010

In the year 2010, CERT-In handled more than 10000 incidents. The types of incidents handled were mostly of Phishing, Malicious Code, Website compromise & propagation of malware and Network Scanning & Probing.

2.1.1 Incident Trends

During the year 2010 CERT-In handled several incidents of intrusions into websites and injecting iFrame and 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. The return of the attack toolkit Asprox has also been witnessed with a slightly different SQL injection method to penetrate into the web applications.

A rise in the malware infections was observed. Prominent botnet infections were due to Conficker and Mariposa (Rimecud) worms. On the crimeware front, Zeus (the infamous password stealing trojan) was the most effective botnet. Trojan SymbOS/Zitmo - Symbian malware was also propagated by the ZeuS botnet. It is named as Zeus In The MObile. The backdoor trojan acts as a spyware and forwards some of the victims SMS messages to another phone number controlled by the malware. Bot families like Pushdo, Taterf, were in the wild. Malware families like Waledac, Mebroot, Rustock were also observed as part of malicious code incidents.

One of the prominent malware with high damage potential is Stuxnet targets industrial control systems (ICS) by modifying the Programmable Logic Controllers (PLC). The threat made use of Windows rootkits , Antivirus evasion techniques, intriguing process injection and hooking, network infection routines, and a command and control interface.

It has been observed that Mariposa Botnet showed large number of infections. This botnet uses blended malwares for fast spread and due to download and execution of arbitrary malicious executables the functionality of botnet is extended effectively.

Rise of WEB 2.0 attacks had been witnessed largely. The social networking sites were used largely to send spam mails (normally a link shortened with *tinyurl* facility) and trick unsuspecting users to fall victim to malware infection. Koobface botnet targeted Facebook users disguising as fake video player/ application.

Fake Antivirus programs posed a rising threat using SEO poisoning techniques to entice users to visit malicious websites and deliver malicious scareware.

Vulnerabilities in Adobe products and Flash player were actively exploited in targeted attacks. Malware targeting mobile platforms also were reported.

2.1.2 Tracking of Indian Website Defacements

CERT-In is tracking the defacements of Indian websites and suggesting suitable measures to harden the web servers to concerned organizations. In all 14348 numbers of defacements were tracked in the year 2010. Most of the defacements were done for the websites under *.in* domain. In total 9772 *.in* domain websites were defaced.

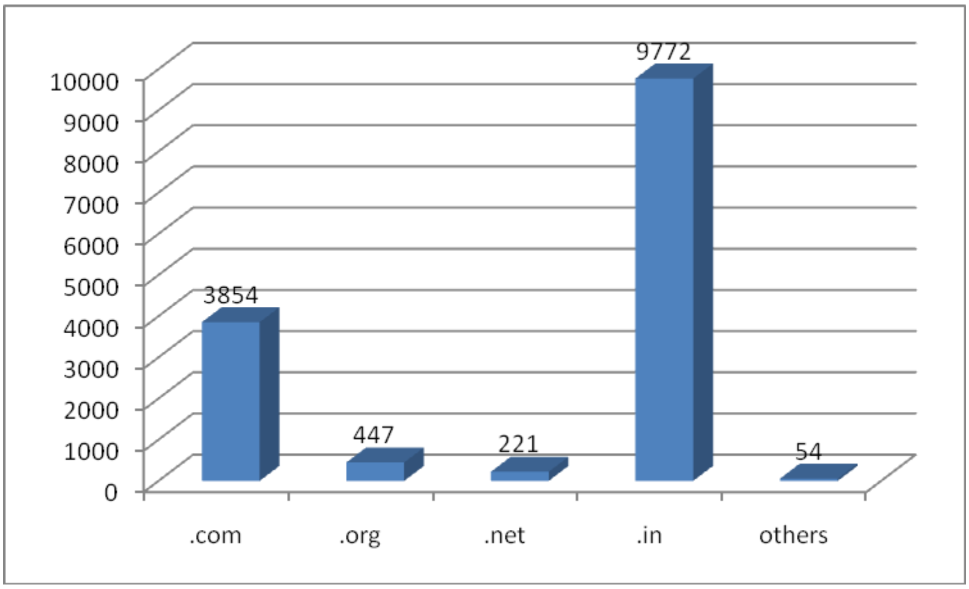


Figure 2. Indian websites defaced during 2010 (Top level domains)

2.1.3 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 2492 open proxy servers were tracked in the year 2010. The month-wise distribution of open proxy servers tracked during this year is shown in the figure 3.

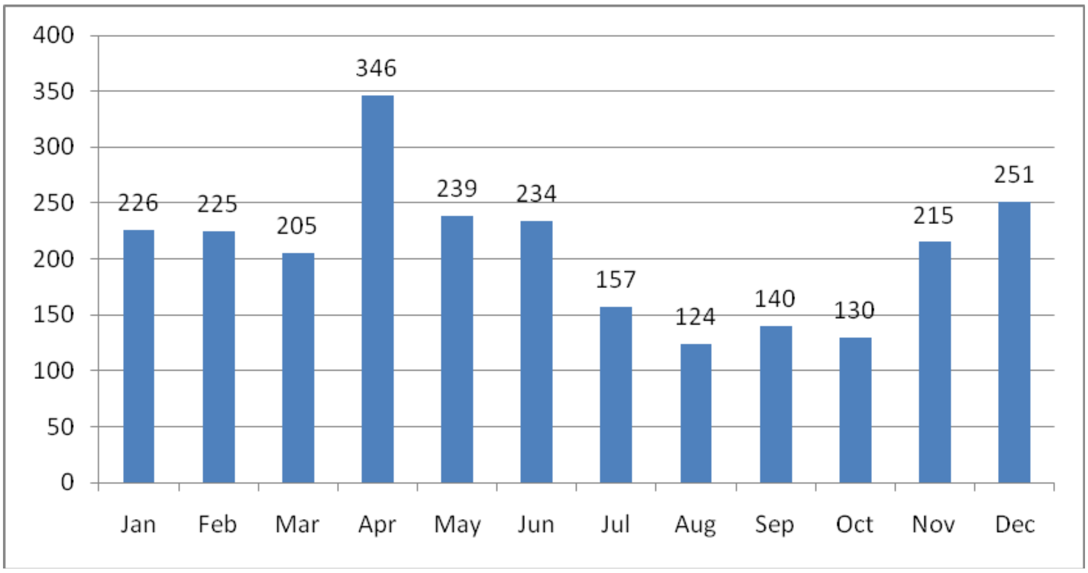


Figure 3. Monthly statistics of Open Proxy Servers in 2010

2.1.4 Botnet Tracking and Mitigation

CERT-In is tracking Bots and Botnets involving Indian systems. Users were advised on suitable measures for dis-infection. Figure 4 shows the number of Bot infected systems and Command & Control servers tracked in 2010.

Month	Number of Bot Infected Systems	C&C Servers
January	35659	19
February	158851	16
March	69183	-
April	1736353	07
May	2116482	-
June	39600	-
July	32242	13
August	263196	9
September	153196	3
October	274224	11
November	617365	13
December	1661156	16

Figure 4. Botnet statistics in 2010

2.2 Abuse statistics

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

Security Incidents	2004	2005	2006	2007	2008	2009	2010
Phishing	3	101	339	392	604	374	508
Network Scanning / Probing	11	40	177	223	265	303	477
Virus / Malicious Code	5	95	19	358	408	596	1817
Spam	-	-	-	-	305	285	981
Website Compromise & Malware Propagation	-	-	-	-	835	6548	6344
Others	4	18	17	264	148	160	188
Total	23	254	552	1237	2565	8266	10315

Table 2. Year-wise summary of Security Incidents handled

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. The following training programmes were conducted during 2010.

- Workshop on "Stuxnet Malware Threats and Response Measures" on December 15, 2010
- Workshop on "Information Security and Cloud Computing" on December 08, 2010
- Workshop on "Web Server Security" on November 29, 2010
- Workshop on "Intrusion Detection and Mitigation" on November 12, 2010
- Two Workshops on "Secure Coding in C/C++" on October 26-29, 2010 in association with JPCERT/CC
- Workshop on "Windows Security" on October 20, 2010
- Workshop on "Mail Server Security" on October 08, 2010
- Workshop on "Secure coding in .NET" on September 24, 2010
- Workshop on "DDoS Attacks & Mitigation" on September 03, 2010

- Workshop on "Information Security Policy Compliance for CISOs" on September 01, 2010
- Workshop on "DNS Security" on August 20, 2010
- Workshop on "VoIP Security" on August 06, 2010
- Workshop on "Vulnerability Assessment & Penetration Testing" on July 21, 2010
- Workshop on "Crimeware and Financial Frauds" on June 30, 2010
- Workshop on "Secure Code Development in PHP" on June 24, 2010
- Workshop on "Wireless Security" on May 06, 2010
- Workshop on "Virtualization Security and Challenges" on April 23, 2010
- Workshop on "Computer Forensics : Seizing & Imaging of Digital Evidence" on April 07, 2010
- Workshop on "Secure Architecture for System Administrators" on February 26, 2010
- Workshop on "Security Information and Event Management" on February 17, 2010
- Workshop on "Network Security" on January 28, 2010
- Workshop on "Data Centre Security" on January 15, 2010
- Workshop on "Computer Forensics: Seizing and Imaging of Digital Evidence" on January 04, 2010

3.2 Drills

Cyber Security Mock Drills are being conducted to assess preparedness of organizations in critical sectors to withstand cyber attacks. First Cyber security mock drill was conducted in November 2009, the second mock drill was conducted in March 2010 and the third mock drill was conducted on 11th December 2010.

4. Achievements

4.1 Presentation

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

4.2 Publications

The following were published by CERT-In in the year 2010:

- CERT-In Guide for Securing IIS 7.0 Web Server: The purpose of the guideline is to recommend security practices for designing, implementing and operating publicly accessible Microsoft Internet Information Services (IIS) 7.0 Web servers, including related network infrastructure issues

- Case study on Mariposa Botnet (CICS-2010-01): The case study discusses the propagation and damage capabilities of Mariposa Botnet which is detected as Autorun/Palevo/Rimecud/Pilleuz by different Antivirus systems.
- 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).

CERT-In has successfully participated in ASEAN CERTs Incident Handling Drill (**ACID 2010**) held in September 2010 and **APCERT Drill 2010** held in January 2010.

One of CERT-In member participated in **APISC Training Course 2010** sponsored by **KrCERT/CC** scheduled during 27 September – 1 October, 2010 at Seoul, Korea.

One senior official from CERT-In participated in **Digital Crimes Consortium Conference 2010**, being hosted and sponsored by **Microsoft** at Montreal, Canada during 12 -15 October, 2010.

Two Training programmes on **"Secure C/C++ Programming"** were conducted in collaboration with **JPCERT/CC** in October 2010.

6. Future Plans/Projects

CERT-In has been evolved as the most trusted referral agency in the area of information security in the country. Following are the future plans:

- Development and implementation of a framework to enable organisations to respond to cyber incidents and assess the preparedness of organisations to withstand cyber attacks. Continuous assessment and improving the security posture of Critical Infrastructure Organisations through regular interaction with CISOs and sectorial CERTs.

- Implementation of projects in the areas of attack detection & prevention
- Promotion of research and development in malware detection & prevention and Cyber Forensics.

4. 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 is a National level CERT organization, which is responsible for the coordination of activities among all CERTs within China concerning incidents in national public networks.

1.2 Establishment

CNCERT was founded in Oct., 2000, and became a member of FIRST in Aug 2002. CNCERT took an active part in the establishment of APCERT as a founding member.

1.3 Workforce power

CNCERT, which is headquartered in Beijing, the capital of P.R.China, has 31 provincial branch offices in 31 provinces of China mainland.

1.4 Constituency & Etc

CNCERT provides computer network security services and technology support in the handling of security incidents for national public networks, important national application systems and key organizations, involving detection, prediction, response and prevention. It collects, verifies, accumulates and publishes authoritative information on the Internet security issues. It is also responsible for the exchange of information, coordination of action with International Security Organizations.

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 reports

In 2010, CNCERT received 10,433 incidents reports[8] and 5070 of them were from international users and agencies. Most incident reports were about vulnerability (33.04%), malicious code (29.61%), webpage malicious code (21.35%) and phishing (15.01%).

In 2010, CNCERT handled 3,236 incidents. Malicious code (1,463), Webpage malicious code (649), phishing (631) and web defacement (410) were 4 main incidents handled.

TOP 10 Phishing Reporters	
From	Number
s21sec.com	196
ebay.com	125
hsbc.com.cn	110
brandprotect.com	107
phishlabs.com	106
bradesco.com.br	86
cert.br	62
telefonica.es	61
irs.gov	58
rsa.com	57

TOP 10 Phishing Targets	
Target	Number
bbva.com	170
ebay.com	134
bradesco.com.br	127
Hsbc.com.cn	115

[8] In 2010, CNCERT had not estimated spam incident reports in its data collection, instead, suggested users turn to Anti-spam center of ISC for incident report. Meanwhile, CNCERT sent all related reports to Anti-spam center for them to handle.

I irs.gov	73
wachovia.com	71
alliance-leicester.co.uk	57
Icbc.com.cn	51
cctv.com	51
ceca.es	37

2.2 Abuse Statistics

2.2.1 Trojan & Botnet Monitoring

According to CNCERT's sample monitoring, in 2010, there were 479,626 IPs of Trojan C&C server discovered with 21.3% reduction compared with 2009, and 10,317,169 IPs of Trojan clients discovered with a big increase of 274.9% than 2009. Meanwhile, about 220,000 IPs of Trojan C&C servers were outside of Chinese mainland. Top 3 countries or regions are USA, India and Chinese Taipei China.

As for Botnet, there were about 14,000 IPs of Botnet C&C server discovered with 39.6% reduction than 2009, and about 5,620,000 IPs of Bot discovered with 52.% reduction. Meanwhile, 6,531 IPs of Botnet C&C servers were outside of Chinese mainland. Top 3 countries or regions are USA, India and Turkey. In general, the size of IRC Botnets is going on to become smaller, localized and specialized. The Botnet with less than 1,000 bots is much more favorable to attackers.

2.2.2 Conficker Monitoring

By Dec 2010, there was over 60,000,000 IPs of computer infected with Conficker in the world. China mainland was still No.1'severe disaster area'with over 9,000,000 IPs of infected computer. Other severe disaster area includes USA(15%) and Brazil(7%).

2.2.3 Stuxnet Worm Monitoring

As the first worm infecting industrial controlling system, Stuxnet caused a worldwide concerning in 2010. By the end of 2010, 578 IPs of computers have been infected in China mainland. The number is very few if comparing with other normal worms.

2.2.4 Mobile Virus Monitoring

In 2010, CNCERT discovered that there had been 2,003,515 cell phones infected with 'DuMusicPlay', 831,843 cell phones infected with 'Skulls', 216,147 infected with 'FC.MapUp.A' and 1431 infected with 'Boothelper.A'.

Symbian was still the primary target for mobile virus and more than 69% mobile viruses compromised Symbian OS cell phone. J2ME(27%) was the second largest infected target. Android (3%) ranked No.3 and kept a fast growth.

2.2.5 Web Defacement Monitoring

In 2010, CNCERT discovered about 34,845 defaced websites in China mainland. 4,635 are governmental websites, a large proportion.

2.2.6 Malicious Domain Name Monitoring

In 2010, top 10 malicious domain names are as follows.

Rank	Domain Name
1	www.w22rt.com
2	annil.8866.org
3	a.ppmmoo.cn
4	lsrc.cn
5	vod123.8866.org
6	ferrari10.7766.org
7	jjeffyfc19.info
8	web.9bic.net
9	ghtoto.3322.org
10	ada.bij.pl

2.3 New services

In 2010, CNCERT had put more effort into the establishment of CNVD[9] and ANVA[10], which are 2 platforms for information sharing among all related members, aiming to provide constituency and users with richer information and data. Besides public information services, CNCERT also delivered more

[9] China National Vulnerability Database

[10] Anti-Network Virus Alliance

customized information reports to its contracted users.

Large event network security assistance is always the task of CNCERT. CNCERT provided monitoring and alert services for EXPO 2010 in Shanghai and 16th Asia Games in Guangzhou.

3. Events organized/co-organized

3.1 Training

N/A

3.2 Drills

APCERT 2010 Drill held on 28 Jan 2010, as the organizing committee member with HKCERT and MyCERT.

3.3 Seminars & Etc

- **Seminar on Network Security Terminology**
  The Seminar was held in Beijing, 23 Mar 2010, aiming to regulate the terminology of network security and make common sense among IT organizations.
- **Press Conference on 2009 China Netizen Network Security Investigation Report**
  The meeting was held in Beijing, 30 Mar 2010.
- **2010 CNVD[11] Spring Working Conference**
  The meeting was held in Beijing, 20 Apr 2010.
- **2010 ANVA[12] Working Conference**
  The meeting was held in Beijing, 6 Aug 2010.
- **September 2010 FIRST Technical Colloquium & CNCERT Annual Conference**
  The Conference was held in Beijing from 12 to 14 Sep 2010. Nearly 400 delegates from 10 countries and regions attended the conference. Mr. Yang Xueshan, the Minister of the Ministry of Industry and Information Technology of PRC addressed on the plenary meeting. This event was open to FIRST members and invited guests. It’s a three day event comprising of 1 day hands-on workshop, 1day plenary meeting and 1 day breakout

[11] China National Vulnerability Database
[12] Anti-Network Virus Alliance

sessions.

For the hands-on workshop on 12th, there were 6 hands-on sessions and 6 instructors from FIRST members. Totally about 151 people attended the classes. For the plenary meeting on 13th and breakout sessions on 14th, 41 speakers delivered the speeches or presentations. 3 topics of high-level panel discussions were included in the plenary meeting. At the same time, 7 exhibition booths were provided for all delegates to visit on site.

- China-USA Network Security Dialog Ongoing

  Since Mar 2010, CNCERT had already organized 14 conferences on China-USA Network Security Dialog Mechanism Anti-spam Subject including both parties' face-face conferences, teleconferences and China side internal conferences. Members of China side are from Anti-spam Center of ISC, Beijing Post & Telecommunication University, China Telecom, China Unicom, Sina, Netease, 263.com, Tencent, HiChina, NSFocus and etc. Members of USA side are from Switch NAP、Google、Northrop Grumman、Bell Labs、Comcast Cable Communications、VeriSign、Pennsylvania State University、George Washington University、CERT at CMU Software Engineering Institute、AT&T、Global Cyber Risk、San Jose State University、Cox Communications and etc. By the end of 2010, both parties had completed a draft on Anti-spam Proposal Joint Report based on sufficient view exchange.

4. Achievements

4.1 Presentation

- Network Threat VS Financial & Economic Security, 7th Worldwide Security Conference, Belgium, Feb 2010
- CNCERT Activity Update & China-Japan Cooperation Proposal, China-Japan ICT & Industrial Policy Seminar, Beijing China, Apr 9 2010
- China Update on Network Security Activity, 41st/42nd APEC-TEL Conferences, May/Aug 2010.
- China Update on Internet Situation Awareness, 2nd Microsoft Anti Digital Crime Cooperation Conference, Montreal Canada, Oct 12-15 2010.

4.2 Publication

“2009 China Internet Security Report” (in Chinese, ISBN: 9787121115646).

4.3 Certification & Etc

By Dec 2010, as the Network Security Information Notification Center of Communication Industry, CNCERT had already built up a stable information notification working systems with 262 working units.

As the operation and administration organization, CNCERT developed 25 CNVD members and 22 ANVA members since its establishment in 2009.

5. International Collaboration

5.1 MoU

N/A

5.2 Conferences and Events

- 22nd Annual FIRST Conference
  CNCERT delegation attended the FIRST Conference in Miami, USA, June 13-18 2010.
- ACID 2010
  CNCERT participated in ACID 2010 on 21 Sep 2010.
- China-ASEAN Telecommunication Regulation Round Table Symposium
  CNCERT participated in the Symposium in Vietnam, July 8 2010.

6. Future Plans

6.1 Future projects

N/A

6.2 Framework

6.2.1 Future operation

To better handle cross border incidents and exchanging necessary important information, CNCERT/CC is going to update or sign MOUs with more CERTs/CSIRTs teams around the world.

6.2.2 Tracking

Conficker worm, Mobile virus, and Stuxnet worm.

6.3 Etc

N/A

7. Conclusion

In 2010, the national Internet infrastructure generally ran good, and the level of network security got improved significantly. There was no severe security event like 5.19 event in 2009 (several provincial Internet failure) happened.

Baidu event tell us that the domain name systems security was relatively weak. 3Q event (conflict between 360.cn and QQ) indicates that there was urgent need to strengthen privacy protection for users, regulation on Internet value-added services competition and supervision/administration of Internet value-added service providers' network security. Government website security remains weak and vulnerable. Large E-commerce websites, large financial websites, third-party online payment websites and large social networking websites became the main target of online fraud. Industrial control systems faced new challenges because of Stuxnet worm.

Continuous efforts of combating Trojan horse and botnet resulted in public network environment improved. DoS attack shows 2 signs of transferring and large amount of flow. Some underground game service websites redirected its domain name to those large public websites to avoid attacks. More and more large-flow DDoS attacks increasingly became the serious threat to Internet infrastructure and important online applications, so it is recommended for the communication industry to further improve source address authentication mechanism.

Mobile virus grows fast, spreads wide, and harms big. Mobile Internet network environment should be in good governance urgently. More and more high-risk vulnerabilities exposes out of network devices, operating systems, server systems, database software, application software and even security products. Base on CNVD 2010 vulnerabilities statistics, top 3 types of vulnerability are on application software (62%), operating system (16%) and Web application (9%).

Cross-border network security incidents have become increasingly prominent. Attackers are very fond of utilizing foreign resources to implement attacks, which calls for more international cooperation.

5. 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. Her missions are to handle computer security incident reports, gather and disseminate information relating to security issues, advise on preventive measures against security threats, promote information security awareness, and maintain network with other computer emergency response teams (CERT) and security organizations to facilitate coordination and collaboration.

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, two consultants and a group of computer security specialists.

2. Operations and Activities

2.1 Incident Handling

HKCERT serves as a coordination centre for information security incidents of Hong Kong. HKCERT is recognized as the national CERT for the economy of Hong Kong and the point of contact in cross border information security incidents.

During the period from January to December of 2010, HKCERT had handled 1153 incidents, including 980 security incidents, 162 virus incidents and 11 other incidents. Security incident reports continue to overtake virus incident reports (See Figure 1).

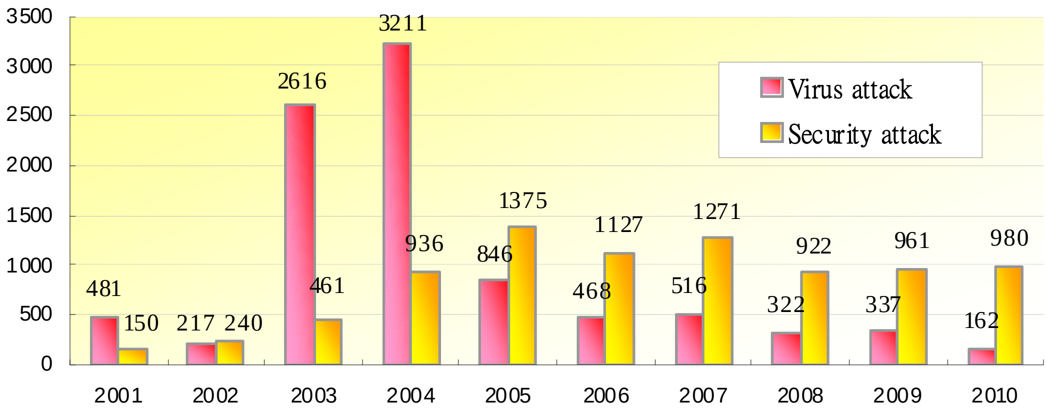


Figure 1. HKCERT Incident Reports in 2010

The number of incidents reported by local parties was 360 (26.3%), by overseas parties was 554 (40.6%) and by proactive discovery was 452 (33.1%). The figures indicated several critical points.

- The low local reports indicated that malware nowadays are more stealth than before. We have to do more awareness promotion to educate the general public. HKCERT has to build up a stronger malware collection and analysis capability.
- The significant number of cross border incidents reflected the globalization of cyber attacks. A strong international collaboration is essential to success in security assurance.
- The number of incidents we proactively discovered was more than that of locally reported incidents. We have to conduct proactively research to effectively discover previous unreported incidents.

For proactively discovered incident reports, we mean those incidents which are not reported by any other, but by discovery research of HKCERT staff. Our staff kept track of third party sources of malware hosting websites and command and control centres. We also monitor security researcher information sources and use the keywords of active exploit script names and related domains as keywords in search engine to locate suspicious websites. Out of all 452 proactively discovered incident reports, 33.4% were defacement websites, 31.6% were phishing sites and 14.8% were SQL injection. Code injected websites usually contained links redirecting users to exploit hosting websites. These sites have potential to cause financial loss to users. However, due to limited resources in HKCERT, proactive discovery of incidents was given a lower priority. We could have identified more cases if more resources were available.

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 2010, HKCERT published 308 security bulletins and advisories (See Figure 2) which is a 40% increase from previous year's number (i.e. 220). All security bulletins were related to vulnerabilities and no malware alert was published during this period.

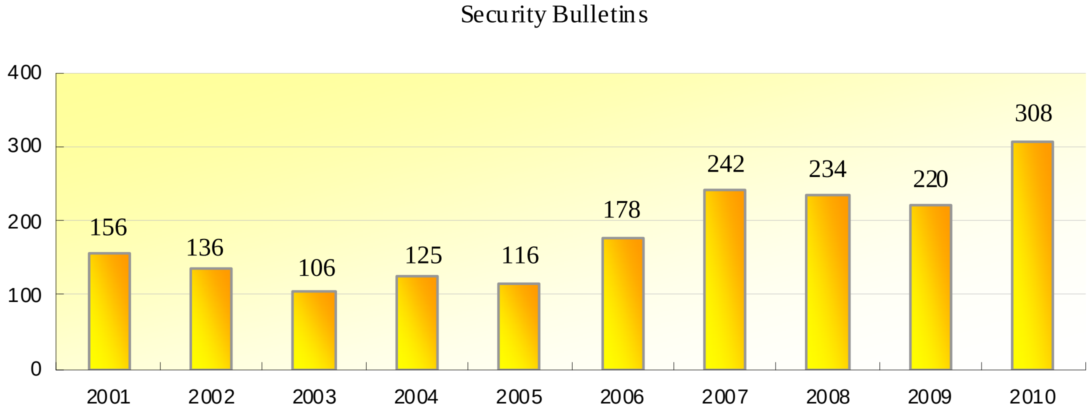


Figure 2. HKCERT Published Security Bulletins in 2010

The major software vendors (Microsoft, Adobe and Oracle) have adopted a practice to disclose vulnerabilities on a specific date each month. This was a good practice for enterprise patch management. However it had also put great pressure on HKCERT's capability to disseminate the large number of security bulletins within a short period of time.

2.3 Publications

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

The **Information Express RSS feed services** continued to be well received.

There were 579,809 RSS visitors in 2010, representing **a 42% increment compared with the previous year**.

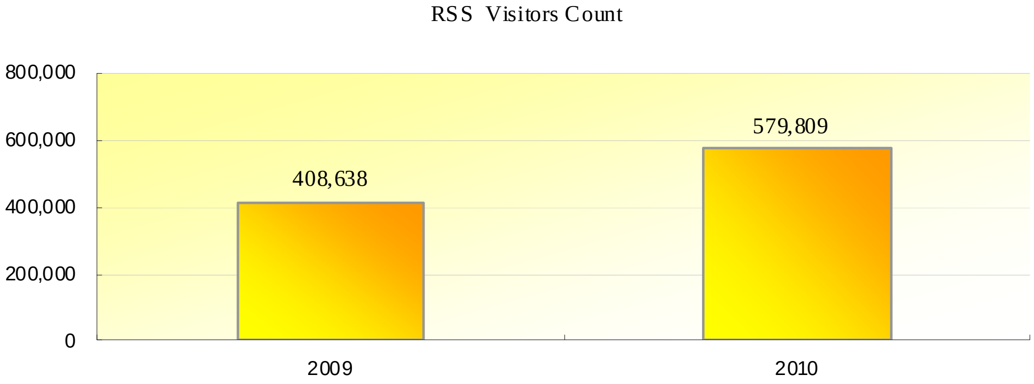


Figure 3. HKCERT RSS Visitors Count in 2010

3. Security Awareness and Training

3.1 Seminars, Conference and Meetings

HKCERT jointly organized the Hong Kong Clean PC Day 2010 campaign with the Government and Police. The campaign involved public seminars, ISP symposium and a logo design competition. Four public seminars were organized in March May, July and November 2010.

We organized the Information Security Summit 2010 with other organizations and associations in November 2010, inviting local and international speakers to provide insights and updates to local corporate users.

3.2 Training

We coordinated one overseas expert and two local experts to deliver three speeches and one hands-on workshop on “Penetration Test Kungfu with BackTrack” in the training workshops of the Information Security Summit.

3.3 Speeches and Presentations

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

3.4 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 March 2010 in Thailand.
- Served as member of APCERT Steering Committee in 2010.
- Elected as chair of APCERT
- Participated in the Microsoft Security Cooperation Program to share information
- Represented APCERT in the Advisory Council of DotAsia Organization
- Joined the Tsubame distributed honeypot project of JPCERT/CC
- Participated in the APCERT Drill in January 2010. HKCERT was leader of organizing committee and acted as the Exercise Control team member. The theme of the drill this year was "Fighting Cyber Crimes with Financial Incentives." The drill was a great success with 16 teams from 14 economies participating.
- Participated in panel discussion "What's Next for Corporate Security Incidents" in the INTERPOL Information Security Conference 2010 in Hong Kong in September 2010
- Participated in FIRST TC and CNCERT/CC Conference in September 2010 in Beijing, China and delivered a talk on APCERT Drill
- Participated in the SecureAsia@Singapore Conference of (ISC2) in July 2010 and acted as a panelist.
- Delivered speech in the Macau CERT and Manetic "Botnets, DDoS Trends and Security Countermeasures“ seminar in July 2010
- Participated in the APEC TEL41 Working Group Meeting held in Taipei in May 2010. As the chair of APCERT, HKCERT delivered two speeches on "APCERT Drill 2010 (summary report)" and "Emerging Security Threat Landscape of the region."
- Participated in the FIRST AGM and Conference, and CERT/CC's Collaboration Meeting for CSIRT with National Responsibility in June 2010 in Miami, Florida.
- Participated in other international conferences: Digital Crime Consortium Conference in Montreal, Canada in October 2010.

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".
- Co-organized a local drill with HK Police and OGCIO in October 2010. Some critical information infrastructure (HKIX, HKIRC, HKISPA) and ISPs were involved. 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 Information Security Task Force and provided security status reporting during Internet traffic impact by Japan earthquake, and important events such as the policy address of CE and the budget speech
- Established a Information Security Advisory and Collaboration (ISAC) Mailing list and advised on latest information security issues through the list
- Organized a round table discussion meeting with information security organizations
- Liaised with Macao CERT in her application to APCERT and FIRST

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.

In 2010, the year ender briefing was held on 7th January.

5.2 Website revamp

HKCERT started to re-design and revamp its website in 2010, to replace the old design that has been in existence for nearly ten years. The website supports mobile device and has social network feature. The security of the HKCERT website would be enhanced by adopting SSL protection for all pages. In the new website, security bulletins would be given severity rating to help users to prioritize their mitigation measures.

The new website will be official launched in early 2011.

6. Future Plans

6.1 Funding

HKCERT would secure Government funding to provide the basic CERT services in 2011/2012. 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 had conducted a strategic review of services by JPCERT/CC in late 2009. The review had pointed out areas for improvement which we are working on an implementation plan on these recommendations.

From the incident report statistics we found that strengthening proactive discovery could probably generate good results. We plan to invest more resources to allow tracking of more information sources and automation the process. Furthermore, malware analysis capabilities and public awareness education could directly address the threat of new malware.

A lot of global cooperation is required in incident response and we depended on Internet infrastructure players and security organizations as our strategic partners to speed up the take downs. HKCERT shall continue to work closely with local ISPs and Domain Name Registries. We shall enhance our local and international coordination and collaboration work.

6. ID-CERT Activity Report

Indonesia Computer Emergency Response Team - Indonesia

1. About ID-CERT

1.1 Introduction

ID-CERT or Indonesia Computer Emergency Response Team CERT is a forum which was born in Indonesia on 1998. ID-CERT is a coordination forum for community-based and independent communities.

Founded by Dr. DR. Budi Rahardjo, 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

Establishment of ID-CERT begins with "reckless", based on considerations there has been no CERT in Indonesia at that time, in 1998. With its informal and important listed first. At that time the countries around us also begin to seek CERT and this continues into the Asia-Pacific forum, which later became the forerunner of APCERT.

From an organizational standpoint, ID-CERT wish to remain standing as a non-governmental organizations, independent, but received an allocation of government funding as a contribution to the CERT. With the current form of ID-CERT be reactive (not active) to a case of incoming or reported by others. ID-CERT also does not have the authority to investigate a case thoroughly, but a liaison who can be trusted, especially by those who reported incident.

1.3 Workforce power

Currently, complaints received by ID-CERT are still handled by Dr. Budi Rahardjo, Andika Triwidada and Ahmad Alkazimy (who recently joined thru research activity) and active since 2010.

Since January 2010, ID-CERT has recruited a professional staff named Ahmad Alkazimy. He has been previously in ID-CERT as a volunteer since March 2007. His own background: had worked at the Indonesian ISP Associations (APJII) from 2001 to 2007 and also in APIA (Asia & Pacific Internet Association) since 2007 to 2009 in supporting the APRICOT (Asia Pacific Regional Internet Conference on Operational Technologies)

Gradually, in line with the need to develop the role of ID-CERT, SOP and so the future ofID-CERT will begin to recruit professionals and also collaborating with some campus.

1.4 Constituency

At this time, we have successfully expanded our constituents ISP, NAP , Government bodies, ccTLD-ID Registry, Corporates, Professional Associations and individuals.

In addition, we also have succeeded in formulating our mission together with the community and our constituents are as follows:

- The purpose ID-CERT is to coordinate the incidents handling involving Indonesia and abroad.
- ID-CERT does not have operational authority to his constituency in both Indonesia and abroad, but only inform a variety of complaints to network incidents, and depend entirely on the cooperation with all those involved in incidents related networks.
- ID-CERT was built by the community and the results will be return to the community.
- Build the internet security awareness in Indonesia.
- Undertakes research in the field of Internet security needed by the Indonesian Internet community.

2. Activities and Operation

2.1 Incident handling reports

Abuse category consists of:

Spam	spam complaints received from abroad to the network in Indonesia
Spam Complaint	spam complaints received from domestic to the network in Indonesia and abroad.
Response	The response provided by all parties on incoming reports
Network Incident	Activities carried out on other people's networks as well as all activities related to network abuse.
Fraud	Report misuse of credit cards. This definition is based on reports police / law enforcement.
Spoofing / Phishing	e-mail scams and websites to deceive users
Malware	A computer program created with malicious intent
Others	Reports of abuse are received apart from the existing category above

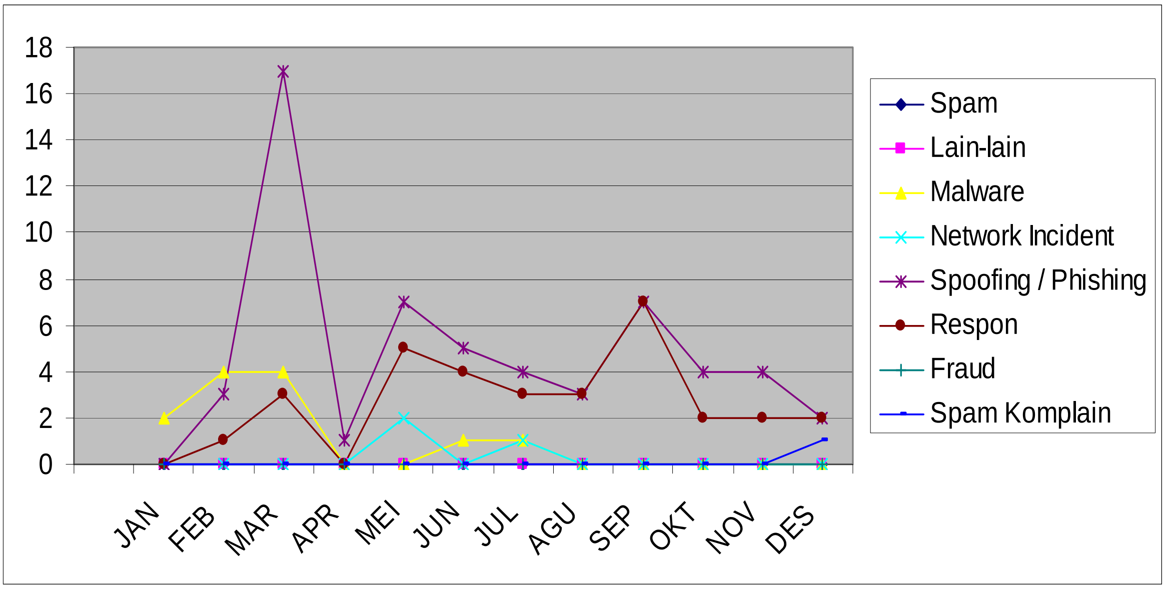


Figure 1: Incident Handling Reports 2010

Most of the complaints that we received on 2010 from the communities are Spoofing/ Phishing, followed by the Response from the community and also Malware.

2.2 Research on Indonesia internet abuse statistics 2010

The research initiated several years ago on creating Internet Security statistics based on reports received by ID-CERT only.

Since 2010, we add more respondents besides the current data from ID-CERT. Currently, 13 respondents had joint the Internet Abuse research on 2010, including: ID-CERT, PANDI, three telecommunication operators, two NAP's and six ISP's.

The type of data that we get from the respondents are Summaries of Abuse reports received by each respondents or we accept copies email of Abuse reports received by each respondents

We are also targeting for more respondents in this year onwards.

In contrast to reports received by the ID-CERT itself, the amount of average consolidated complaint received through Internet research Abuse of the year 2010amounted to 290,297 reports.

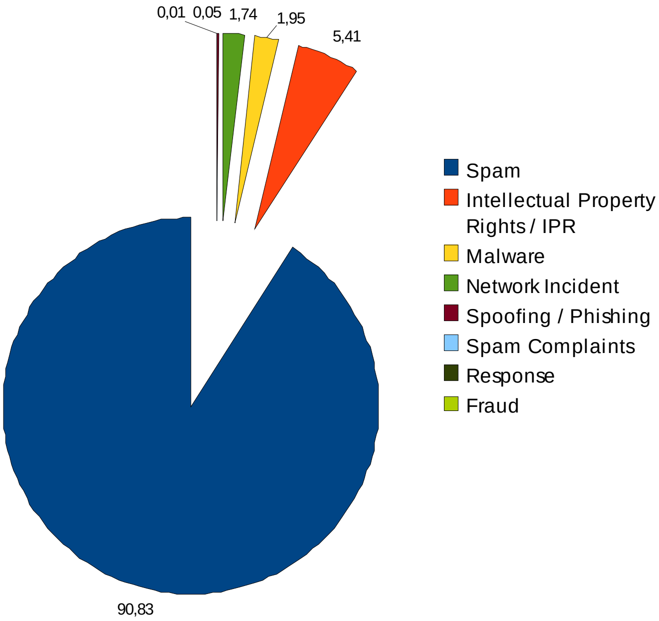


Figure 2:
Research on Indonesia Internet Abuse Statistics 2010 (Monthly average, in %)

Figures shown above are the average abuse complaints that we received from the 13 respondents. The biggest level is the spam. Followed by the second large complaints are the Intellectual Property Rights for movies, music and software.

3. Events Organised

Since 2007, we had done 3 ID-CERT Public Gathering, as follows:

(1) ID-CERT Public Gathering I on 28 Nov 2007 in Jakarta.

(2) ID-CERT Public Gathering II on 28 July 2010 in Jakarta.

(3) ID-CERT Public Gathering III on 28 Feb 2011 in Jakarta.

A number of topics that we discussed in the gathering include the following:

(1) Current and future services;

(2) Abuse Research update;

(3) Funding;

4. Future Plan

ID-CERT is preparing a number of plans related to future development of ID-CERT.

ID-CERT has plans to send its staff for an internship to another CERT. This meant that the employee of ID-CERT can have a complete picture of CERT services in general. More specifically at the same time, ID-CERT is preparing the workflow and SOP.

In addition, research activities such as Abuse Research which is a local product of ID-CERT for the needs of their constituents will continue to work on. ID-CERT plans to maintain the data until the next few years.ID-CERT is preparing several other research that will be run this year as well.

It is important that the attention of ID-CERT for the next step is: what exactly is expected by society to ID-CERT.

(1) ID-CERT plans to build Standard Operation Procedures (SOPs) along with a clear jobdesk to conduct staff development and additional personnel, at least to make the response helpdesk.

(2) ID-CERT plans to develop hardware and software associated with tracking system and email management reporting for abuse reports.

(3) ID-CERT plans to continue conduct various studies required by the Indonesian Internet community. ID-CERT is also planning to add personnel in the field of research and collaboration with leading universities in developing any necessary research. One who has been running now is an Internet Abuse Research Indonesia 2010 & 2011.

(4) ID-CERT will publish regular research reports each month, bi monthly, one semester each year until the final report.

(5) ID-CERT would like to have some supports from their constituency for public education on Internet security.

5. ID-CERT PGP Key's

Mr. Ahmad Alkazimy
e-Mail address: ahmad@cert.or.id
Fingerprint=39B2 87BA 3DD6 7832 D56F 0344 FCE4 3A7C FE38 CC96

Mr. Andika Triwidada
e-Mail address: andika@cert.or.id
Fingerprint=5568 7C7D E898 4F33 A594 A996 DA4B C29F E22D FEE7

6. Conclusion

After facing the hard times, now ID-CERT tried to rise again as a community-based CERT.

As for the future based on ID-CERT's views: in Indonesia, will appear more sectors CERT such as banking CERT, government CERT, education CERT, etc based on the need of their own community to coordinating each other.

In the year 2010, though only a few abuse reports that come in, we plan to continue enhance the ability of our personnel through training and plan for internship.

Another issue that we found is the difficulties to contact the content provider/social networking providers such as Facebook, Twitter, Yahoo and Google.

7. 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 2010, JPCERT/CC received 10,417 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	2,488	3,113	2,441	2,375	**10,417**

Figure 1. Incident reports to JPCERT/CC (2010)

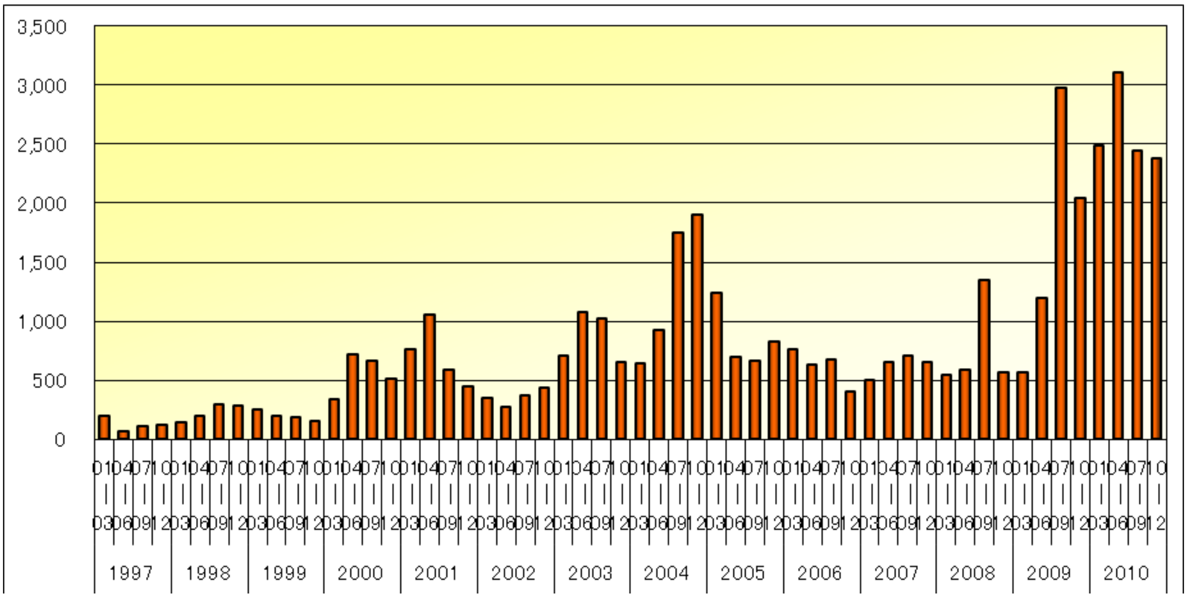


Figure 2. Incident reports to JPCERT/CC (1997-2010)

2.2 Abuse statistics

The incident reports to JPCERT/CC in 2010 were categorized as in Figure 3. More than half of the incident reports were on malware, followed by scan, website defacement and phishing.

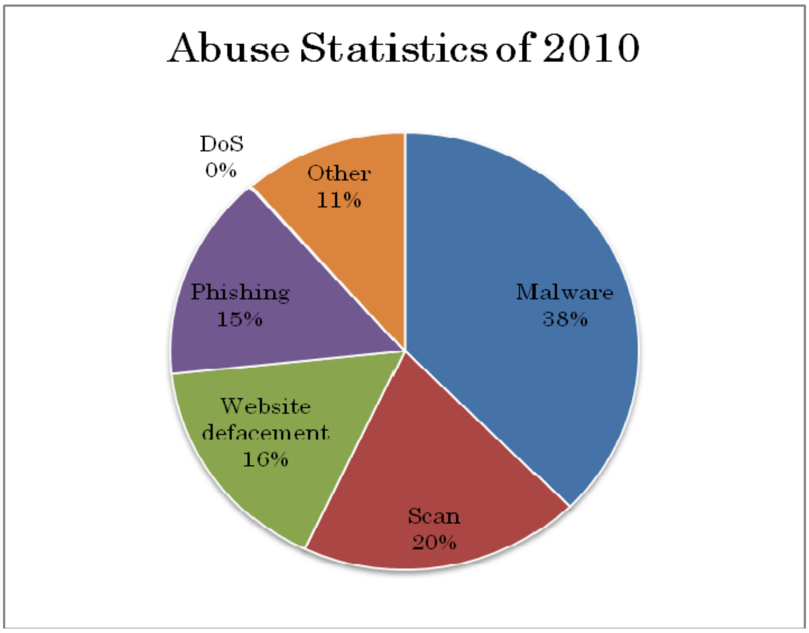


Figure 3. Abuse Statistics of 2010

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 2010, 33 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 (http://www.cert.org/), CPNI (http://www.cpni.gov.uk/) and
  CERT-FI (http://www.cert.fi/en/).
  In 2010, 181 vulnerabilities coordinated by JPCERT/CC were published on JVN. Among them, 66 cases were reported through IPA in Japan, and 115 cases were published in cooperation with 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)
  http://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**

  http://twitter.com/jpcert (Japanese)
  http://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 language blog.

2.4 Control System Security

JPCERT/CC coordinates control system security with relevant organizations in Japan. It provides information on vulnerabilities and solutions regarding control systems, lists of recommended reading materials, as well as reports and documents.

2.5 Education / Public Awareness

- Secure Coding

  JPCERT/CC provides C/C++ secure coding seminars, CERT C Secure Coding Standards, books and materials on secure software development and secure coding rules.

- 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.

2.6 Internet Scan Acquisition System (ISDAS)

https://www.jpcert.or.jp/english/isdas/

ISDAS monitors the Internet traffic in Japan in order to detect threat activities such as worm and scan. The project was initiated in November 2003 with the objective of improving Internet security by providing up-to-date graphs and reports.

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.

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 secretariat for the association.

- **Cyber Clean Center (CCC)**

  https://www.ccc.go.jp/en_index.html

  CCC is active in analyzing characteristics of BOTs, and providing information on disinfection of BOTs from users' computers. In addition, CCC is a core organization taking a role to promote BOT cleaning and prevention of re-infection of users' computers which are once infected by BOTs, based on cooperation with ISPs (Internet Service Providers).

  CCC is a project coordinated by the Ministry of Internal Affairs and Communications (MIC) and Ministry of Economy, Trade and Industry

(METI). JPCERT/CC contributes to the project by analyzing malware and developing disinfection tools for infected users.

- **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 2010 are as follows:

Invitational Training	-CSIRT Training Course for Asia Pacific
On-site Training/Seminar	-Malware Analysis Training -C/C++ Secure Coding Seminars -Tsubame Workshop - CSIRT Training Course for Africa
On-the-job Training	-Malware Analysis Training
Domestic Seminars	-C/C++ Secure Coding Seminars -Control System Security Conference

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 establishing Malware Analysis Laboratory
Dispatch of Speakers	-Information Security Seminar (Philippines) -Regional Collaboration in Cyber Security (Singapore) -OIC-Summit 2010 (Malaysia) …and many more

3.3 Participation to International Events

JPCERT/CC participates in the many international conferences. Below are the events we joined in 2010:

- 29th TF-CSIRT Meeting
- APEC TEL 41 (Chinese Taipei)
- 22nd Annual FIRST Conference (U.S.)
- National CSIRT Meeting (U.S.)
- CIP-Forum (U.S.)
- APISC Security Training Course (Korea)
- GOVCERT.NL Symposium 2010 (Netherlands)

…and many more

3.4 Drills

JPCERT/CC participated in the following drills in 2010 to test our incident response capability:

- ASEAN CERT Incident Drill (ACID) 2010
- APCERT Drill 2010

4. Other Publications

JPCERT/CC also publishes quarterly activity reports, study/research reports, and CSIRT related materials.

5. International Contribution

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

  http://www.first.org

  JPCERT/CC contributes to the international CSIRT community by serving as a Director and 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: "Responsible Vulnerability Disclosure"
  ISO/IEC 27035: "Information Security Incident Management"

6. JPCERT/CC Contact Information

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

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

Phone: +81-3-3518-4600

Fax: +81-3-3518-4602

8. 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 was established in July 1996 with aim of setting up single point of contact for international incident handling, supporting the response activities on information systems and networks in Korea and unifying coordination framework among network operators. KrCERT/CC, under Korea Communications Commission(KCC), covers private sector in the national cybersecurity framework.

1.2 History

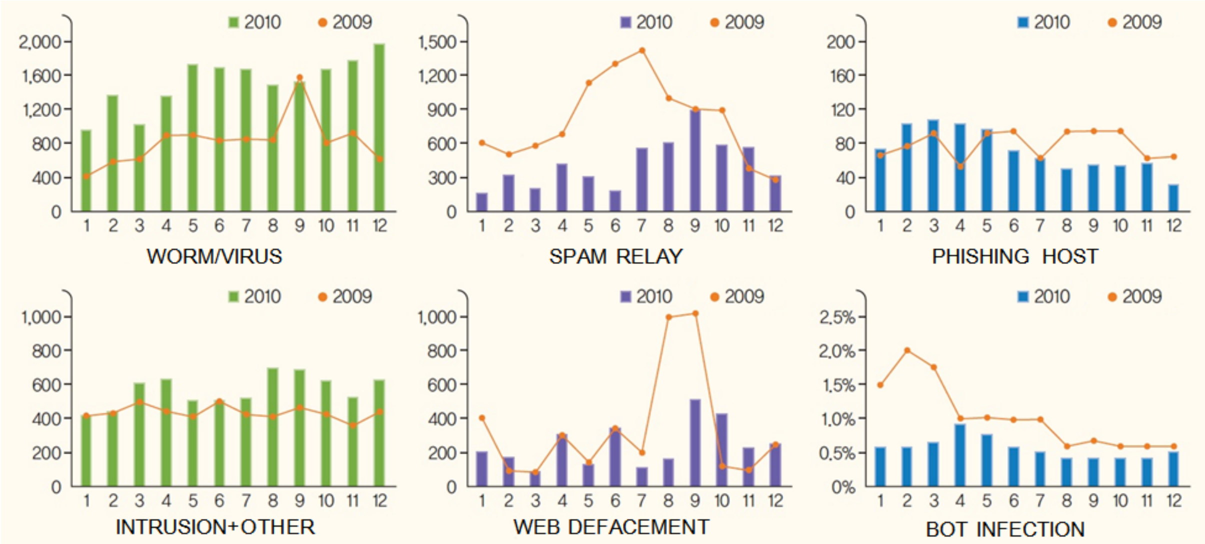
The major changes of KrCERT/CC occurred in 2003 and 2010. The first major change for KrCERT/CC was after the slammer worm outbreak dated back to 25th January 2003. Korean government decided to set up the network monitoring center, called as Korea Internet Security Center(KISC), in collaboration with major Internet Service Providers.

Second major changes in KrCERT/CC occurred after DDoS attacks targeting Korea and US government and major businesses in July 2009. To protect users from cyber threats, much more security budget was approved for KrCERT/CC and many staffs were newly hired. The focus of KrCERT/CC moved from the response focused activities to the balanced activities between prevention and response. KrCERT/CC created a new division for internet incident prevention consisting of 3 teams, PC security team, web security team and spam response team.

2. ACTIVITIES IN YEAR 2010

2.1 Incident handling reports

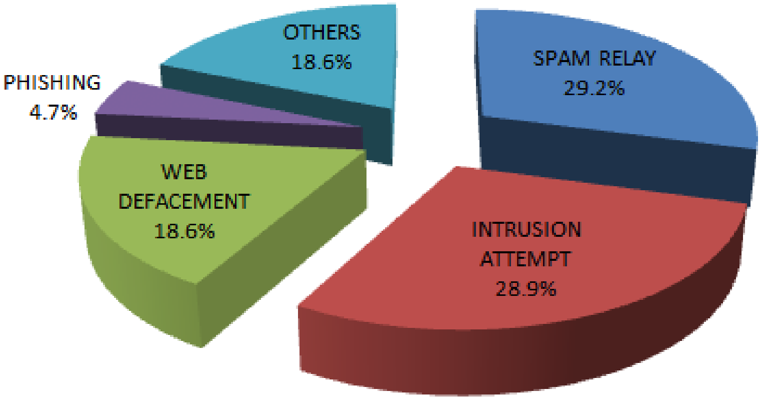
Internet incidents reported to KrCERT/CC are classified into the following 3 categories: worm/virus, hacking incident and bot infection. Hacking Incident. Hacking incident is classified into 4 sub-categories : spam relay, phishing host, intrusion attempt and web defacement.



2010 KrCERT/CC incident report graph

The number of incident reports on worm/virus to KrCERT/CC in 2010 is 17,930. It is around 69 percent increase, compared to that of 2009(10,395). The monthly average number of incident reporting increased from 865 in 2009 to 1,495 in 2010.

The number of hacking incident reported to KrCERT/CC decreased from 21,230 in 2009 to 16,295 in 2010. The number of spam relay subcategory decreased dramatically from 10,148 in 2009 to 5,216 in 2010.



2010 KrCERT/CC incident report ratio

2.1.1 Worm/Virus

The number of worm/virus incidents reported to KrCERT/CC in 2010 is

17,930. The incident reports gradually increased last year. The number of reports in December, with the highest reports, is 1,987,. The most reported malware in 2010 is ONLINE GAMEHACK, which steals the online game credential, such as ID and Password. Users need to make efforts to prevent the damage from malware by installing up-to-date windows patches and scanning computers with the anti-virus vaccines.

2.1.2 Hacking Incident

The number of hacking incident reported to KrCERT/CC in 2010 is 16,295. Dramatic decrease of hacking incidents in 2010 is due to spam relay. The reports of spam replay decreased 48.6 percent, compared to that of 2009. Even with this, among hacking incident reports, spam relay takes the highest ranking with 32 percent. Intrusion attempts take the second rank with 25.3 percent.

2.2 New services

2.2.1 24/7 toll-free call service, 118

KrCERT/CC started 24/7 toll-free call service to handle inquiries on hacking/virus, spam report, privacy infringement and all other Internet related issues, even for smart phone. Korean users can consult with the specialist on cyber incidents. If user can't solve the problem just by call, KrCERT/CC provides the remote management service, such as malware cleanup, with consent from users.

2.2.2 Cyber Remediation Service

Cyber remediation service consists mainly of two parts, user notification system and dedicated vaccines for major incidents, such as DDoS attacks occurred in July 2009. This is one of public and private partnership projects to combat malware infection. KrCERT/CC installed specialized notification devices in 3 major domestic ISPs and have funded the collaboration project with 3 domestic anti-virus vendors to develop the dedicated vaccine for major incidents. KrCERT/CC collects and provides the information on infected machines, such as the IP, timestamp and malware involved, to the relevant ISPs. When users turn on computer, the pop-up window appears just after the computer is connected to Internet. The pop-up notifies that the computer is infected with malware and asks users to run the dedicated vaccine or malware disinfection tool. The window also provides the links to dedicated vaccine developed by domestic KrCERT/CC vaccine partners

2.2.3 Free DDoS shelter service for SME

KrCERT/CC started the protection service, with the support from Korean government, for small and medium enterprises(SME) under cyber attack such as Distributed Denial of Service(DDoS) Attack. Victims of DDoS Attacks can report to KrCERT/CC for DDoS Shelther service. KrCERT/CC updates Domain Records to the shelter server IPs with the consent from site owner. All DDoS traffics are rerouted to DDoS shelter zone. The DDoS shelter filters out attack traffics and sends the normal traffics to the original site. The service is only available to SMEs who don't have enough resource to subscribe to the premium protection hosting.

3. Events organized

3.1 2010 APISC Training Course

KrCERT/CC hosted the 2010 APISC Security Training Course to support strengthening response capabilities of developing economies from Asia Pacific Region. The training has been annually held from 2005. The main objectives is to assist developing economies who are interested in establishing Internet response capabilities, such as CSIRT, while providing a training opportunities for establishing and managing CSIRT in their own economy. The course was held from 27th September to 1st October in Ibis Myeong-dong Hotel, Seoul, Korea. 23 trainees from 15 economies and 5 trainers from 4 economies attended 5 days training course, consisting of one day for introduction of information security in Korea, one day for economy updates and 3 days for CSIRT training for business and technical perspective, including CSIRT operational exercise.

The CSIRT training is based on the material of Training of Network Security Incident Teams Staff (TRANSITS) from TERENA. The active interaction between trainers and trainees and sharing responsibilities among trainers made the course more successful and fruitful.

4. International Collaboration

Jinhyun CHO, an international cooperation staff of KrCERT/CC, successfully finished his two year term for SPSG Convenor at APECTEL41, held at Chinese

Taipei in May 2010. During his term, he tried to liaison between policy makers and CSIRT communities including APCERT.

5. Future Plans

KrCERT/CC has the responsibility to host 2011 APCERT AGM & Annual Conference in Jeju Korea with the warm support of APCERT members. The event would be a great chance to contribute to APCERT activities and promote Korea's leading information security activities.

KrCERT/CC Contact Information

Website : http://www.krcert.or.kr/english_www
E-mail : first-team@krcert.or.kr
Phone : +82-2-118

9. MyCERT Activity Report

Malaysian Computer Emergency Response Team - Malaysia

1. About MyCERT

1.1 Introduction

The Malaysian Computer Emergency Response Team (MyCERT) was established in 1997 to address the computer security concerns in Malaysia. With the number of computer users in Malaysia increasing rapidly each day, MyCERT has seen an increase of reports relating to computer incident ever since its operation. The nature of such incidents had transformed from merely virus attachments, spamming and web defacement to a more delicate type of attacks such as malware attacks, account compromise and online fraud which effects monetary losses to victims of individual, corporate, and nation stature.

Besides its primary role in maintaining computer and cyber security as well as advisory services to domestic Internet users, MyCERT actively assist other international computer security incident response teams (CSIRTs) around the world through cooperation, knowledge sharing, and capability development.

1.2 Establishment

MyCERT operates under CyberSecurity Malaysia, a non-profit organization under the purview of the Ministry of Science, Technology and Innovation (MOSTI), Malaysia. CyberSecurity Malaysia main roles can be summarized as follows:

- To assist MOSTI in the implementation of the National Cyber Security Policy (NCSP)
- To provide Cyber Security Emergency Services and act as the national technical coordination centre
- To conduct Cyber Threat Research & Risk Assessment
- To provide Cyber Security Quality Management Services
- To build capability in the field of cyber security (Training) and to create awareness and a culture of cyber security (Outreach)

Further information about CyberSecurity Malaysia can be viewed at:
http://www.cybersecurity.my/en/

1.3 Workforce

As of December 2010, MyCERT has 21 staff operating its two main services, the Cyber999 Security Incident Help Centre and the Malware Research Centre.

The Malaysia Computer Emergency Response TEAM (MyCERT)

1.4 Constituency

MyCERT's primary constituency is the Malaysian Internet Users. Therefore, MyCERT handles security incidents reported by the Malaysian public as well as provide assistance to international organizations in resolving security incidents when the sources or target of incidents are within Malaysia.

2. ACTIVITIES IN YEAR 2010

In 2010, MyCERT had observed a growing number of targeted attacks such as intrusion, online fraud and malware leading to identity theft. In dealing with these incidents, collaboration and coordination with various parties such as law enforcement agencies, corporate IT departments and legal departments were sought to resolve such incident and attacks.

2.1 Incident Handling Reports

For the year under review, the Cyber999© Help Centre had handled a total of 8,090 security incident cases reported to it. About 97% incidents were resolved according to the centre's service level agreements (SLAs). In addition, MyCERT had also processed about 24,187 incidents related to malware, intrusion attempts, infection attempts and remote file inclusion (RFI) attacks transpired in its research network project operated by the Malware Research Centre.

More information on the incidents can be viewed at:
http://www.mycert.org.my/en/services/statistic/mycert/2010/main/detail/725/index.html

Additionally, the centre issued two (2) security advisories, 47 security alerts related to various vulnerabilities in applications and security incidents in 2010.

The list of advisories and alerts can be viewed at:
http://www.mycert.org.my/en/services/advisories/mycert/2010/main/index.html

The Malware Research Centre maintains a blog in sharing information on malware analysis that had produced not less than 15 articles. More information of the blog can be viewed at:
http://blog.honeynet.org.my/

It is worth mentioning that highlights of the increase in incidents in 2010 were of fraud, scam and network harassment in nature. MyCERT also saw an increase of social network harassment such as online extortion, cyber bullying and social network accounts being compromised.

2.2 Abuse Statistics

MyCERT's 2010 abuse statistics and security incidents are generally categorized as intrusion, malicious code, fraud, harassment and spam. The incidents statistics are as shown below:

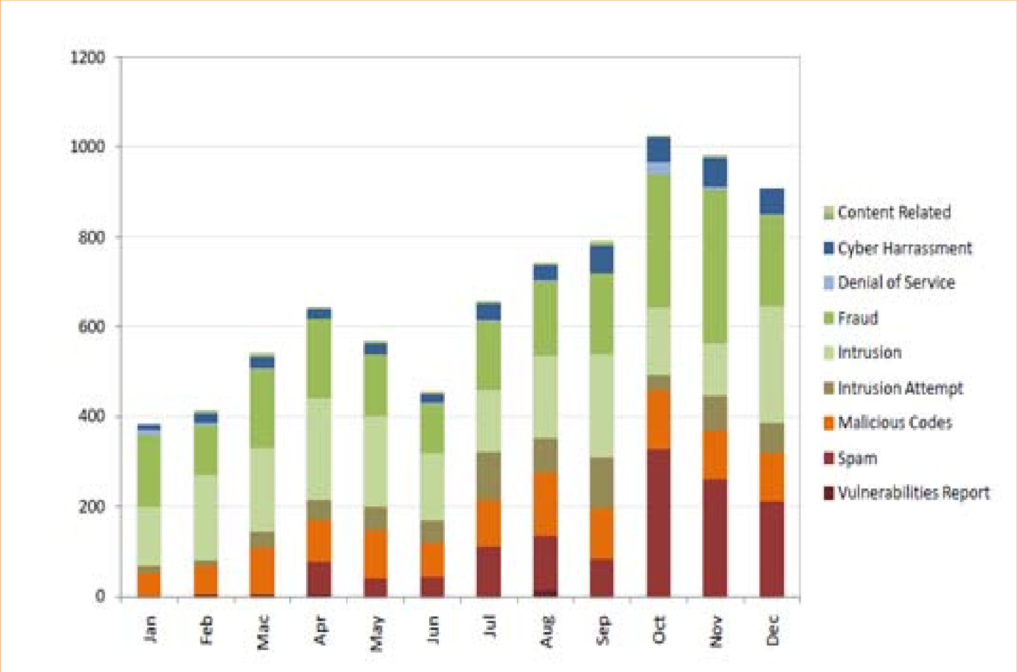


Figure #1: Reported Incidents Handled by MyCERT in 2010

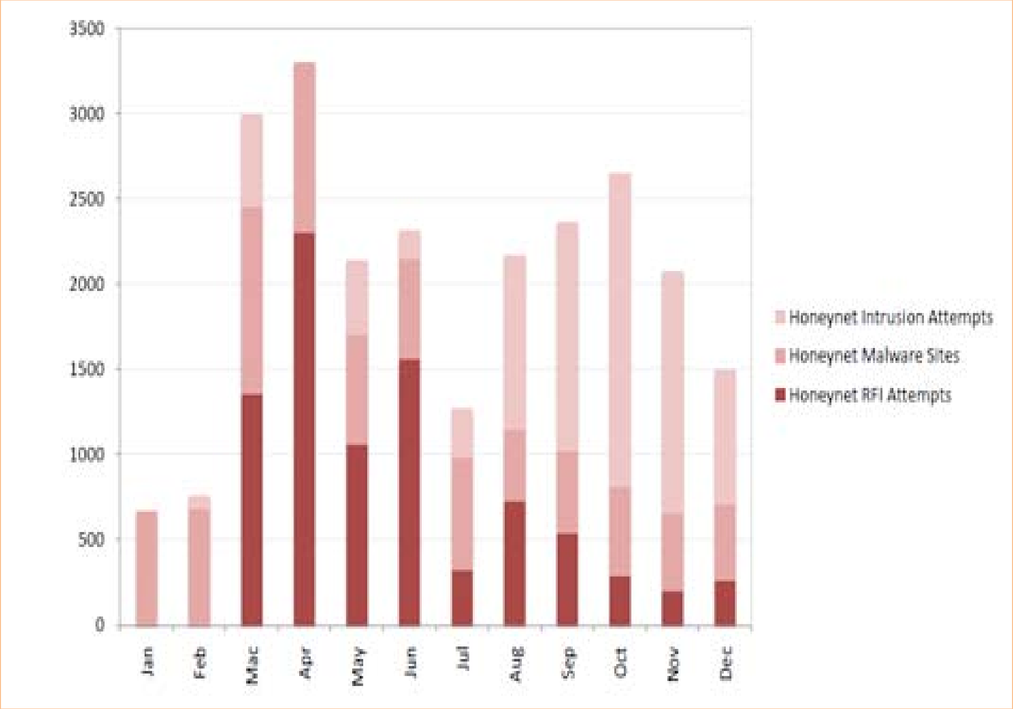


Figure #2: Honeynet Project Related Incident Statistics in 2010

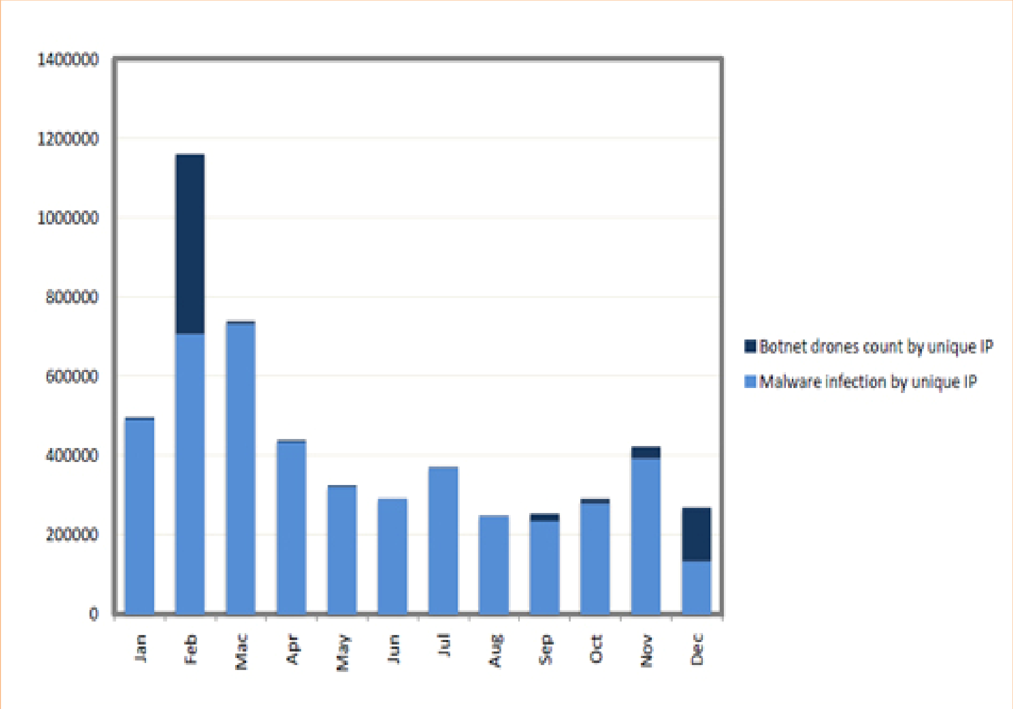


Figure #3: Botnet Drones and Malware Infection in 2010

Detailed information of the abuse statistics and trends are available in MyCERT website.

2.3 Events Organized

In order to be recognized as a cyber security specialist centre, MyCERT has been active in participating in numerous local and international security events. The team had prescribed to the need of sharing knowledge through actively participating in various trainings and talks in the area of incident handling, malware analysis, and security trends for different kinds of audience. Under its parent company CyberSecurity Malaysia, it had assisted to organize national and international events beneficial to Internet users worldwide.

2.4 Trainings

There were several workshops or hands-on training conducted by MyCERT in year 2010 which include:

- Log Analysis & Web Security, OIC-CERT Regional Workshop (Middle East), Cairo, Egypt

- Incident Handling & Response + Mini Drill training for participants of the National Cyber Security Exercise, Kuala Lumpur, Malaysia
- Incident Handling Analysis, OIC-CERT Regional Workshop (Africa Region), Rabat, Morocco
- Analyzing Malicious PDF with Open Source Tools, MSCMOSC2010, Kuala Lumpur, Malaysia
- Log analysis hands-on training & Analyzing Malicious PDF File, CSM-ACE 2010 / OICCERT Regional Workshop (Asia), Kuala Lumpur, Malaysia

2.5 Cyber Security Exercises

MyCERT had participated and assisted in coordinating three cyber-drills of national and international significant in 2010. They were:

- Asia Pacific CERT (APCERT) Drill
  MyCERT participated as a player as well as taking the role of as the exercise advisor drill.

- ASEAN CERT Incident Drill (ACID)
  MyCERT participated as a player in the drill organized by SingCERT.

- National Cyber Drill (X-Maya 3)
  MyCERT coordinated and developed the drill scenarios and artifacts for X-Maya 3, which was organized under the initiative of the National Security Council (NSC). A total of 21 agencies from 10 Critical National Information Infrastructure (CNII) sectors took part in X-Maya 3 and engaged in incident handling activities to further strengthen their capabilities as well as cooperating among the agencies.

2.6 Seminars & Conferences

In 2010, CyberSecurity Malaysia had organized its premier annual information security event on 25-to-29 October 2010 at the Kuala Lumpur Convention Centre. The conference called Cyber Security Malaysia Awards, Conference and Exhibition (CSM-ACE) 2010, was an initiative to promote the information security agenda in the region and the world.

3. ACHIEVEMENTS

3.1 Presentation

MyCERT representatives had been invited to various talks at international conferences or seminars as speaker. Among the distinguished events were:

- ISAC and Botnet Prevention Conference, Taipei, Chinese Taipei
- APCERT Annual Conference and Annual General Meeting, Phuket, Thailand
- The Honeynet Project 9th Annual workshop, Mexico
- APWG - The fourth annual Counter-eCrime Operations Summit (CeCOS IV), Brazil
- 5th ENISA Workshop, Heraklion, Crete Greece (via Skype)
- SIGINT 2010, Chaos Computer Club (CCC), Cologne, Germany
- 22nd Annual FIRST Conference, Miami, USA

In addition to the above, MyCERT had spoken at not less than 50 different occasions at local events throughout the year.

3.2 Publications

3.2.1 Alerts and Advisories

Alerts, advisories and publications produced by MyCERT's are available at MyCERT's website that can be viewed at: http//www.mycert.org.my/

3.3 Certification

2010 saw four (4) of MyCERT members being certified the prestigious SysAdmin, Audit, Network, Security (SANS) Institute for SANS GPEN (Penetration Testing), and SANS GREM (Reverse Engineering). This adds to 13 team members that had been certified by SANS so far, as an addition to other certifications received by other team members.

3.4 Security Tools Development

MyCERT registered three significant achievements in 2010 with the launch of its in-house security tools development. On 4th August 2010, the MyKotakPasir, and Gallus were launched during the National Drill (X-Maya3). These web-based tools allow automatic analysis of malicious executables and PDFs.

Furthermore, an addon for Mozilla Firefox called DontPhishme was launched on 3rd July 2010. DontPhishme alerts Internet users when they visit a fraudulent banking website.

4. INTERNATIONAL COLLABORATION

To strengthen the capability in mitigating the nation's cyber security, it is crucial for existing collaboration be enhanced, in addition to new affiliation being made with national and international organizations.

4.1 Memorandum of Understanding (MoU)

To further strengthen cooperation with other security organizations, MyCERT through CyberSecurity Malaysia had signed a Memorandum of Understanding (MoU) with two security institutions:

- United Arab Emirates Computer Emergency Response Team (*aeCERT*)
- Taiwan Information Security Center National Cheng-Kung University (TWISC)

4.2 Membership Support

Through its work with various teams, MyCERT had the opportunity to vouch for other teams intending to be recognized within the Computer Incident Response bodies especially in FIRST, APCERT, and OIC-CERT.

Teams supported to become FIRST member were:

- United Arab Emirates Computer Emergency Response Team (*aeCERT*), UAE
- Education Cyber Security Center (ECSC) Republic of Korea, and
- Indonesia Security Incident Response Team (IdSIRTII), Republic of Indonesia

Teams supported to become OIC-CERT member were:

- Academic Protection Awareness Isfahan University of Technology CERT (APA-IUTcert), Islamic Republic of Iran, and
- Amirkabir University of Technology, Islamic Republic of Iran

4.3 New Partnership and Existing Cooperation

Last year saw new partnerships made with 10 critical national infrastructure organizations for its Enterprise Honeynet Project. MyCERT had also expanded its data sharing efforts to various numerous strategic partners.

MyCERT through CyberSecurity Malaysia also strengthened its existing international cooperation with the Asia Pacific Computer Emergency Response Teams (APCERT) and Organization of the Islamic Conference – Computer Emergency Response Teams (OIC-CERT) as a Steering Committee (SC) member. It maintains its membership as a Full Member in the Forum of Incident Response Security Team (FIRST).

5. FUTURE PLANS

5.1 Future projects

MyCERT is currently looking at new development and innovation of security tools to support the nation and the Internet users from being a victim to cyber attacks. It is also actively seeking to improve its collaboration with new partners that have the same mission to insure that the cyberspace is secured and safe for everyone.

6. CONCLUSION

2010 had been another busy year in terms of reactive and proactive services. MyCERT's past experience and initiatives had somewhat assisted it in providing the required service to its important stakeholders within and outside Malaysia.

2011 meanwhile is seen to be a challenging time for MyCERT with an expected high rate of incidents reporting to be encountered from the Malaysian public. The team is also expected to engross its time in producing newly improved security tools under the Malware Research Centre.

With support from other services offered by CyberSecurity Malaysia, MyCERT will continue to position itself at the forefront in safeguarding the nation from cyber security threats. MyCERT looks forward to the challenges and interesting engagements in 2011 with other APCERT and international incident security community.

10. PHCERT Activity Report

Philippine Computer Emergency Response Team - Philippines

1. About PHCERT

1.1 Introduction

The Philippine Computer Emergency Response Team (PHCERT) is a member-based non-stock, non-profit organization composed of information security professionals and practitioners committed to ensuring that the internet and electronic environment is secure and trustworthy.

PHCERT coordinates resolution of information security incidents with reporting entities and possible sources or hosts of security malware, fraudulent websites, and other avenues of fraudulent and/or disruptive activities.

PHCERT receives advisories and alerts and in turn issues such advisories and alerts to its members on reported vulnerabilities and actions that may be taken by its members to preserve and protect the integrity of information system infrastructure of the organizations where they are employed.

PHCERT promotes best information security practices and standards through its awareness and education programs.

PHCERT serves as point of contact for information security incidents.

PHCERT maintains a healthy working relationship with the three branches of government:

- With the Executive Branch – by participating in various committees charged with the development of rules and regulations and the adoption of information security standards.
- With the Legislative Branch – by participating in technical working groups tasked with reviewing proposed legislation that seeks to promote a secure Philippine cyber environment and by providing expert advice to legislators.
- With the Judiciary – by participating in committees tasked with the development of rules that help in the judicial resolution of information security related incidents.

PHCERT also maintains a healthy working relationship with law enforcement agencies: the Department of Justice, the National Bureau of Investigation, the Philippine National Police, and the Criminal Investigation and Detection

Group.

1.2 Constituency

As a general rule, PHCERT's constituency includes the general public. The core constituency covers the individual members and, by extension, the private and public sector organizations where they are employed. Covered also are members of partner organizations listed in Item 4.2 below.

1.3 Members

The members serve on a purely voluntary basis, providing personal time and expertise to help in the resolution of incidents and promotion of information security practice.

1.4 Organization

PHCERT is managed by a Board of Trustees. The five members of the Board are elected by the members at large during its annual meeting. The members of the Board elect among themselves who shall serve as officers – President, Treasurer, Secretary, Vice President for Incident Management, Vice President for Awareness and Education Programs, Vice President for Membership Affairs.

2. Activities

2.1 Incidents Handling

Incident Handling is one of the major tasks performed by PHCERT. On receipt of an abuse report, the report is immediately acknowledged, logged, and monitored. Coordination with concerned parties is then initiated. Communications is done primarily via email. Landline and mobile phone are secondary modes of communication. Upon resolution, a Incident Closing Report is filed.

Abuse cases are also reported to law enforcement authorities for further action. Many reported cases have been successfully prosecuted.

2.2 2010 Statistics

Government website defacements dominated the reported incidents in 2010. 162 national and local government agency websites were defaced, although significantly down from 227 reported defacement incidents in 2009.

Defacements were reported prior to the National and Local Elections held on May 10, 2010, many of which were determined to have been cases of political hacktivism. Other defacement reports were related to the hostage taking of foreign nationals in August 2010 – hacked websites were reported within a two-week period of the incident.

Three cases of phishing sites and fraudulent email sources, two cases of cyberbullying, 38 cases of email (specifically yahoo email accounts) and social networking account hijacking, and 5 cases of fake email and social networking accounts were reported. The hijacked yahoo email accounts were used to generate unsolicited commercial communication (spam), targeting email addresses in the respective directories of the account owners.

A particular case of website spoofing reported by JPCERT/CC was traced to Cebu City located in central Philippines. It was found that the information provided in the DNS registry were all fictitious. The case was referred to the National Bureau of Investigation for resolution.

2.3 Consultancy

PHCERT provides consulting services requested by government agencies, in regard to security policy development and information system security review (and in some cases, vulnerability assessment.

PHCERT provides consulting services to the Department of Trade and Industry and the National Computer Center in the implementation of Executive Order 810 which mandates the use of digital signatures in e-government services.

PHCERT provides consulting services to the Chief Information Officers Forum (CIO Forum) for the development of plans and implementation of managed information security services for government agencies.

2.4 New Services

No new services were offered in 2010.

3. Events

3.1 Awareness, Training, and Education

- PHCERT sent 4 of its members to participate in the Training Program on Information Security: Strengthening of CSIRT (Computer Security Incident Response Team) conducted under the auspices of the Association of Overseas Technical Scholarships from 13-22 January 2010 in Tokyo, Japan. The training program was prepared and conducted by JPCERT/CC.

- A PHCERT delegate attended the APCERT Annual General Membership Meeting hosted by ThaiCERT held on 3-5 March 2010 in Phuket, Thailand made possible through the Fellowship Program
- The Secure Coding in C/C++ Training program, delivered by JPCERT/CC representatives, was held on 1-3 December 2010
- Various lectures and presentations on information security topics (best practice, standards, role of CERTs, setting up CSIRTs, certification, and others) were delivered by PHCERT members to different organizations including groups of information system auditors (ISACA), legal practitioners, electronic engineers (IECEP), IT professional organizations (PSIA, PCS, ITAP), government IT managers (CIO Forum), among others.
- PHCERT initiated the development of a training program for government agencies on the establishment of Incident Response Teams to be rolled out in 2011.
- PHCERT initiated contacts between the Commission on Information and Communications Technology and IMPACT.

3.2 Tsubame Project

PHCERT is a participant in the Tsubame Project of JPCERT. Negotiations for the hosting of Tsubame sensors were initiated with two telecoms companies following the installation of a sensor in December 2009.

3.3 Legislative Participation

PHCERT seats in the Technical Working Groups in both house of Congress to assist in the review of the proposed Cyber Crime Bill, seen to (1) strengthen information security awareness and practice in the country and (2) recognition of CERT/CSIRTS as coordination and collaboration is one of the highlighted provisions of the bill.

4. Collaboration

4.1 International

PHCERT received abuse reports from other CERTs of other countries, eg., Spain, Brazil, and India in 2010. The reported incidents were successfully resolved.

4.2 Local

PHCERT continues to nurture its relationships with the following organizations:

- Government Computer Security Incident Response Team (GCSIRT) which was organized and operated by the Criminal Investigation and Detection Group of the Philippine National Police. GCSIRT's focus is on criminal investigation and evidence gathering. GCSIRT is a general member of APCERT.
- National Cyber Security Office (NCSO) which operates under the Commission on Information and Communications Technology.
- The Incident Response Team of the Department of Social Welfare and Development
- The Information System Security Society of the Philippines, an organization of information system security professionals and practitioners.
- The Philippine Certified Information System Security Professionals.

4.3 Others

- PHCERT and the International Multilateral Partnership Against Cyber Threats (IMPACT) have started together in working with the Philippine Commission on Information and Communications Technology (CICT), for the CICT to avail of the programs offered by IMPACT and to connect to IMPACT's Global Resource Center.
- PHCERT has signed up with Microsoft's Security Cooperation Program.

5. Future Plans

5.1 In PHCERT's over 10 years existence, the organization had faced legal challenges in the performance of its self-appointed mandate. Information security incidents are expected to rise both in numbers and sophistication. This fact has not escaped notice of individual users and government and private sector organizations. Relationships with the greater number of government and private sector organizations are founded on relationships with personal contacts. In some cases, PHCERT had resorted to Memoranda of Agreement or Understanding with individual business organizations which define standard procedural protocols in address information security incidents. This set up, however, will prove to be unwieldy as the number of MOAs or MOUs grow in numbers. PHCERT is addressing this issue by:

- Espousing the passage of the Cyber Crime Bill which includes a provision on incident coordination and response
- Re-organizing PHCERT to allow public and private sector organization members

5.2 Roll out of a training program for the establishment of Incident Response Team in government agencies

5.3 Roll out of a plan for the establishment of industry sector and organizational incident response teams.

5.4 Implement the plan to deliver information security awareness programs at the national and local levels, drawing support from the public school system as initiated by Senator Edgardo J. Angara.

11. 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 an increase in the total number of incidents reported to SingCERT in the year 2010 as compared to the year 2009. Phishing websites especially of local banks were the major concerns in 2010. SingCERT continues to work with other CERTs and our Internet Service Providers (ISPs) to track down affected users and keep them informed on how to secure their systems. On the regional and international fronts, collaboration and cooperation among CERTs have proved effective in the resolution of our cross-border incidents.

3. Events organised / co-organised

3.1 Seminars and Workshops

In our continued efforts to keep our constituency updated on security trends and developments, SingCERT organised 4 seminars and workshops for the year 2010. 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 2010

The ASEAN CERTs Incident Drill (ACID) 2010 was conducted successfully on 21 September 2010. 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 PDF exploits. 12 CERTs from 10 countries from ASEAN and Asia took part in the drill, and good feedbacks were received from all the participants.

4. International Collaboration

4.1 Incident Drill

SingCERT organised the ASEAN CERT Incident Drill in September 2010 and participated in the APCERT Annual incident drill in February 2011.

5. Future Plans and Projects

SingCERT will be organising the 6th ASEAN CERTs Incident Drill for the year 2011. Discussions are in progress to work out the scope and coverage.

12. SLCERT Activity Report

Sri Lanka Computer Emergency Response Team – Sri Lanka

1. About SLCERT

1.1 Introduction

The Sri Lanka Computer Emergency Response Team (SLCERT) is the center 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, SLCERT 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.

In anticipation of increased cyber security incidents as Sri Lanka's IT infrastructure grows, SLCERT 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. SLCERT 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.

1.1.2 Workforce

SLCERT currently has a total of nine security team members including a Manager Operations and a Chief Operating Officer. All the staff is highly skilled and have been trained on various IT security certifications, such as GCIH, MCSE, CEH, CCNA, CCSP and CISSP.

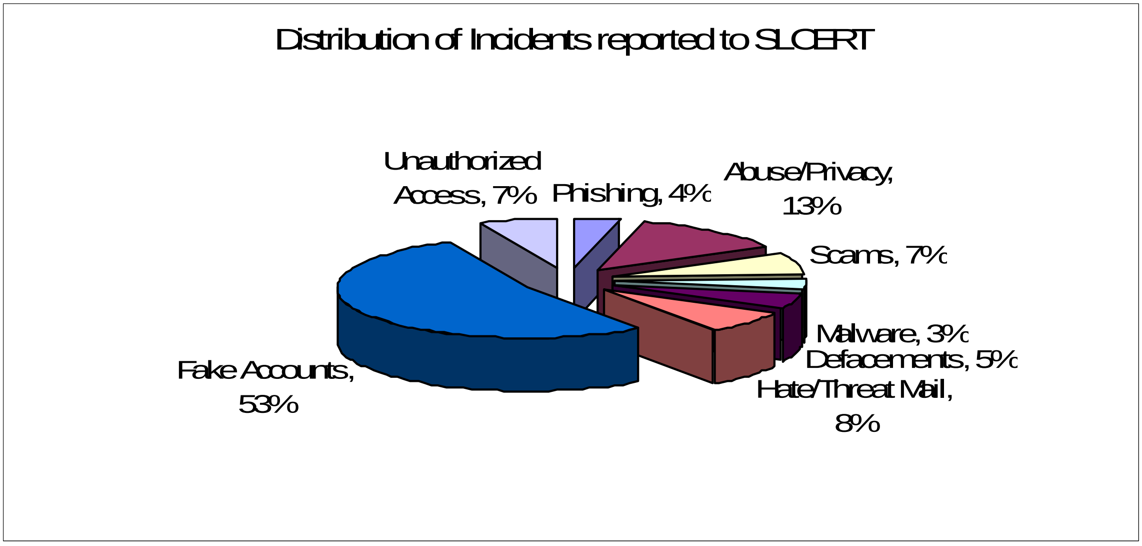
1.1.3 Constituency

SLCERT's Constituency encompasses the whole of the cyber community of Sri Lanka (private & public sector organizations, and the general public). SLCERT maintains a good rapport with government and private sector establishments, and extends assistance to the general public as permitted by available resources.

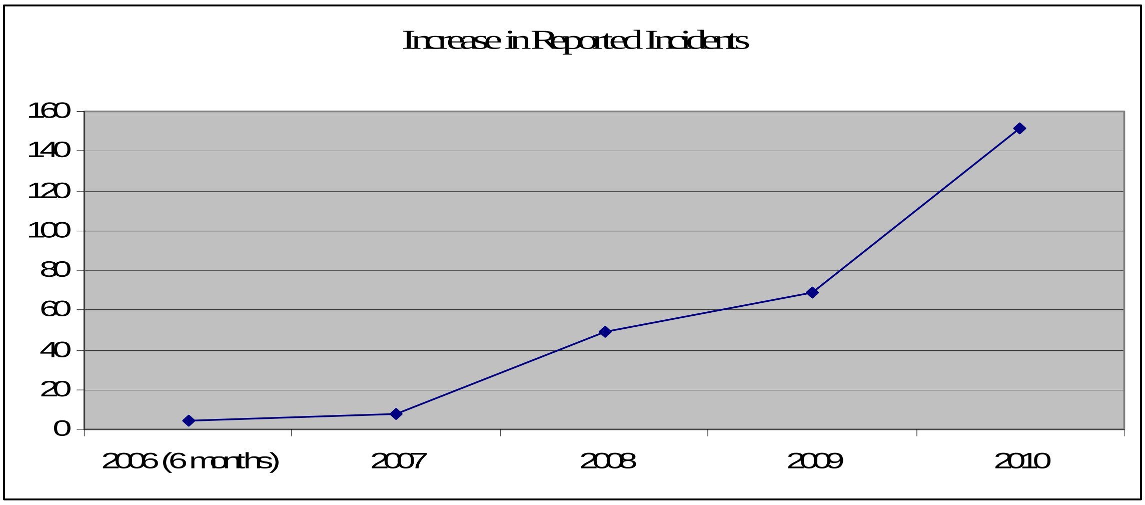
2. Activities & Operations

2.1 Incident Handling Statistics

Incidents reported to SLCERT increased to 151 in the year 2010. In the year 2009, only 69 incidents were reported. This can be seen as a major increase in the reported incidents compared to the year 2009. The following chart depicts the distribution of various types of incidents reported to SLCERT. All the incidents reported to SLCERT have been resolved satisfactorily.



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



2.2 New services

2.2.1 Setting up sector based CSIRTs

SLCERT has initiated the setting up of CSIRTs which are sector-based. Typical sectors are Banking, Telecom, Defence and education. The Bank CSIRT is already operational while the others are in the formulation stage.

The rationale for sector based CSIRT's is to ensure that SLCERT remains a small, focused national body that functions only as an incident escalation point and coordinates the incident responses and ensures national readiness to tackle large scale incidents effectively.

The net result of setting up sector based CSIRTs and accrediting and coordinating the activities of these CSIRTs is that SLCERT has now transformed itself to being a true coordinating body. The Board of Directors of SLCERT has therefore recently approved the re-alignment of SLCERT by re-naming itself as "Sri Lanka Computer Emergency Readiness Team" in addition to being the Coordinating Centre. This process is already underway and SLCERT will soon be known as SLCERT/CC.

Sectoral 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 software and implements security standards to ensure a minimum level of security compliance within the industry.

2.2.2 Digital Forensics

SLCERT was appointed as one of the expert panel members under the "Payments Devices Fraud Act No 30 of 2006" by the Ministry of Finance.

The Computer Crimes Act of 2007 enabled law enforcement officers to obtain technical expertise of recognized information security professionals and organizations to extract and present digital evidence in court. Accordingly, SLCERT continues to assist Sri Lankan law enforcement agencies in carrying out forensic investigations.

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; SLCERT 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 2010 SLCERT conducted the following training and education programs successfully:

a. Seminar on “Using Network science to enhance information security”
b. Seminar on “ICT security” for CIO’s of Government Departments
c. Seminar titled “Shadows in the Cloud “using resources provided by IBM.
d. Played the role of Strategic Partner for the “Cyber Security Summit” organised by the Sri Lankan partner of EC-Council where SLCERT also made presentations.
e. Workshop and Presentation on intelligence gathering to counter Cyber Crime and Cyber Warfare for the Defence Ministry.
f. Participated in a regular Radio Program on national Radio titled “Trends in Cyber Security” mainly focusing on Facebook and e-mail abuse issues.
g. Organized number of media conferences to educate the general public on IT Security.

3.2 Consultancy

SLCERT continues to provide consultancy services in response to requests made – particularly from government departments.

Typical consultancy services provided during the year 2010 included;

a. Network reviews for government departments/private organizations
b. Security Policy development workshops for government organizations
c. Forensics investigation support for Law enforcement
d. Implementation of a Digital Forensics Laboratory for the Police Department
e. Configuration reviews for critical government organization information systems

3.3 Seminars & Workshops

a. Work shop on “Network and Web Application Security”

This was conducted for the technical and information security staff of private and government sector organizations.

b. 3rd Annual National Conference on Cyber Security 2010

This "Annual National Conference on Cyber Security" is an annual program organized by SLCERT since 2008, held in the month of September, which featured a series of events:

- Two Workshops for professionals, namely:
  - Implementation of Secure Networks (two day workshop)
  - Making Web Applications Secure (two day workshop)
- One-day Conference

4. Achievements

4.1 Presentations

a. Conducted presentations on "IT Security" for Chief Information Officers (CIO) of government organizations.

b. Conducted Security demonstrations during the "3rd Annual National Conference on Cyber Security 2010"

4.2 Publications & Other media

a. Website

The SLCERT 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. The website was revamped in 2010, to allow for more effective presentation of information.

b. E-mails

Disseminating security related information via e-mail alerts to SLCERT Website subscribers.

c. Newspapers/media

SLCERT continues to educate the general public through the electronic and print media about SLCERT's role in combating cyber crime.

4.3 Certification & Membership

Memberships obtained in professional security organizations in the period 2010:

a. Microsoft SCP (Security Cooperation Program)

b. Collaborative agreement with "IMPACT". SLCERT will benefit from receiving a threat feeds from the region and also form part of the global incident response team

c. SLCERT is represented on the board and steering committee of the Information Systems Security Association (ISSA) Sri Lanka Chapter, and is involved in the planning of its inaugural event and strategic partnership formation efforts

5. International Collaboration

5.1 MoU

In addition to being members of FIRST and APCERT, SLCERT has signed Memorandum of Understandings with Microsoft, to be a member of Microsoft Security Cooperation Program (SCP) and with IMPACT.

A relationship with (ISC)2 has also been established with SLCERT becoming the master affiliate of (ISC)2 in Sri Lanka from 2011. This would make SLCERT the prime body responsible for administering CISSP and CSSLP training and certification efforts in the country.

5.2 Event participation

March 2nd -5th, 2010
APCERT AGM & Conference
Phuket, Thailand.

May 2nd – 7th, 2010
Network Forensics workshop
IMPACT
Cyberjaya, Malaysia

May 17th - 21st, 2010
AusCERT Annual Conference
Gold Coast, Australia
Participated in the Annual AusCERT Conference and collected an award for on behalf of APCERT for 'Organizational Excellence in Information Security'.

June 14th – 18th, 2010

FIRST AGM and Annual Conference
Miami, Florida

Sept 27th – Oct 1st
APISC Training
Seoul, South Korea

October 12th – 16th, 2010
Digital Crimes Consortium (Organized by the Microsoft Digital Crimes Unit)
Montreal, Canada.

5.3 International incident coordination

Active participant in the recently concluded APCERT Drill 2011, where SLCERT played the role of Organizing Committee (OC) Lead and was part of the Exercise Control (EXCON) team.

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. Implementation and setting up of the National Certificate Authority
b. Setting up more sectoral CSIRTs and organizational CSIRTs in the economy
c. Additional Sensor deployment for "Tsubame" project, to cover 32 IP Address ranges belonging to Sri Lanka
d. Active participation in the IMPACT Network Early Warning System (NEWS) honeypot based monitoring system
e. Changing status from SLCERT to SLCERT/CC to reflect the new role that SLCERT will play with the sector based CSIRT's
f. Rename SLCERT as Sri Lanka Computer Emergency Readiness Team
g. Implement ISO 27001 at SLCERT
h. Implement the provisions of the collaboration agreement with ISC^2 to provide additional training and certification opportunities to the constitution
i. Fully exploit benefits accruing from the Microsoft SCP Agreement and the

IMPACT Agreement

j. Develop e-Government Policy Guidelines for government organizations
k. Collaborating with the Defence Ministry to develop Web Intelligence capability and Critical Infrastructure Protection Strategies
l. ISSA Launch and development work as a forum for IS professionals

6.2 Framework

6.2.1 Future Operation

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

It is planned to purchase new hardware, software that is necessary to expand the operations of SLCERT. The staff will also be increased to handle the increasing number of security incidents.

6.2.2 Operational Support Projects

SLCERT collaborated with a project team from Sri Lanka Institute of Information Technology (SLIIT) to develop an Incident Management System for its internal use, which helps record and monitor incident response progress. It is to be deployed in the first half of 2011.

7. Conclusion

Being nearly five years old, SLCERT has faced an uphill task of raising Information Security awareness in Sri Lanka. The increase in the number of incidents reported and handled by SLCERT in consecutive years is a testament to the success of SLCERT's awareness campaigns both through the use of seminars and conferences and through the use of popular media.

Over the years, SLCERT has also witnessed a major shift in its efforts from incident response to proactive security, embracing the notion that it is far better to prevent security incidents than to respond to them. In that regard, SLCERT has strengthened its skills and manpower base to address proactive security measures such as Network and vulnerability assessment and penetration testing, Organizational Information Security policy formulation, Configuration reviews and system hardening, Internet traffic monitoring and development of secure, yet cost-effective solutions.

Henceforth, SLCERT shall focus on extending and empowering its CSIRT umbrella, with the intention of having dedicated sector-based CSIRTs performing the first level of incident response as well as serving as channels for proactive security measures such as dissemination of security alerts and development and enforcement of security standards. Thus, SLCERT will act as an escalation to the sector-based CISRT, and a national point of contact, for its international counterparts. As a result of this evolution, SLCERT will rename itself SLCERT Coordination Centre. At the same time SLCERT will streamline its existing services so as to achieve maximum effectiveness with its existing staff strength. Focus shall be redirected on training staff in the necessary competencies to ensure continued and effective operations in the coming years. Train the trainer concepts will be employed extensively to avoid duplication of training costs. At the same time SLCERT shall embark upon several new projects to increase its service offering, including but not limited to establishment of a National Certificate Authority, introduction of managed security services and accreditation of security vendors.

All the events organized by SLCERT during the year 2010 were very successful. We will continue to conduct 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

SLCERT 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.

We look forward to being a bigger part of APCERT in 2011 by contributing to various working groups and activities to build a secure information environment in the Asia Pacific region.

13. ThaiCERT Activity Report

Thai Computer Emergency Response Team– Thailand

1. About ThaiCERT

Responding to computer security's incidents is the main mission of ThaiCERT. ThaiCERT has been receiving a number of security incident reports since the year 2001 – the year of ThaiCERT establishment -- and coordinated related organizations to resolve them. In the beginning, ThaiCERT only provided response service to government organizations, but since the advent of phishing cases we expanded our service to several private organizations concerning those cases in order to expedite the closing of their compromised cases.

2. Abuse Report

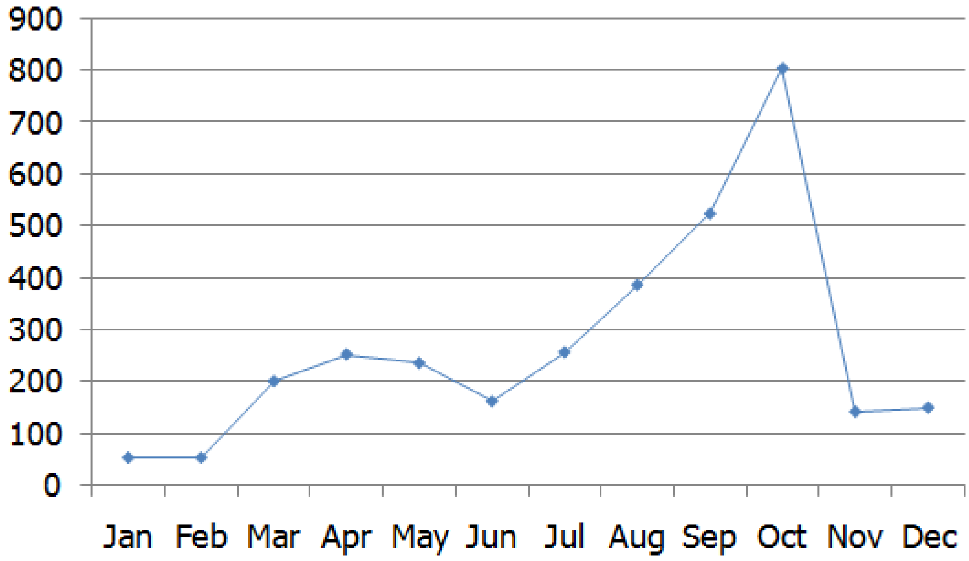


Figure 1 The number of incident reports each month in 2010

Focusing on incidents in the year 2010, the most 3 frequent types of incidents were Spam-related (1,612 cases – 50%), Malware-related (492 – 15%) and Phishing-related (451 – 14%) as show in Figure 2. The details of each type are shown below.

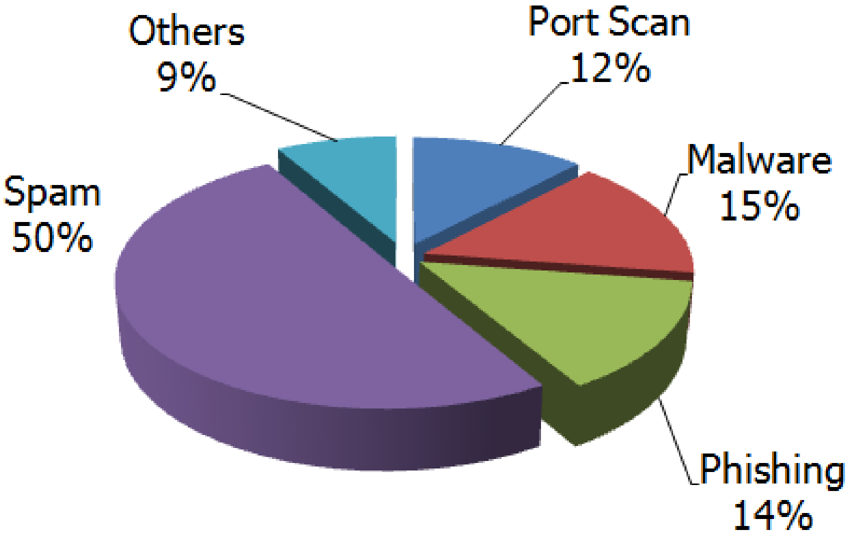


Figure 2 Ratio of each types of ThaiCERT's reported incidents in the year 2010

2.1 Spam cases

The sources of spam were either from regular Internet users or from spam servers used for sending advertisement email. The spam mails from regular Internet users were originated from home users' IP addresses, possibly associated with infected machines.

2.2 Malwares

The malware cases we handled were of two types. First, malwares were found on compromised servers used to spread malicious executable files or scripts (.js and .php). Second, Trojans were found on client's PCs. They stole personal information for fraudulent transactions

2.3 Phishing

There were two type phishing cases reported. First, the servers in Thailand were used as phishing hosts. In most of the reported phishing cases, compromised servers in Thailand were used to publish phishing web sites. Second, links to fake Thai banks were spread through spam emails as baits phishing for private information from Internet banking users. Phishers used visual deception techniques to mimic legitimate text, images and windows of the real Thai banks' web sites.

3. ThaiCERT Activities

3.1 APCERT AGM 2010 in Phuket

We hosted APCERT conference and AGM 2010 in Phuket, "Pearl of the Orient", Thailand between 3rd - 4th March 2010. The theme of the AGM2010 was "Security on Social Networks" to reflect on the current trends in the Asia Pacific region focusing on the development and adoption of "Web 2.0", the next generation of the cyber world including web-based communities, web applications, social networking sites, video-sharing sites, wikis, and blogs.

3.2 Incident Drills

We participated two online incident drills in 2010:

- APCERT Incident Handling Drill 2010
- ASEAN CERTs Incident Drill 2010

3.3 Training Courses

ThaiCERT arranged a variety of training courses in 2010 in Thailand. The main objective was to raise information security awareness and technical knowledge level of the general public. The courses include:

- IT Security awareness raising for users, executives, administrators or technicians
- Network Forensics
- Web security
- OS Hardening
- Dynamic Malware Analysis

In 2011, we plan to collaborate with JPCERT/CC to organize a C/C++ Secure Coding seminar in May in Thailand. We also consider organizing several IT security seminars and workshops.

14. TWCERT 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 Chinese Taipei 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

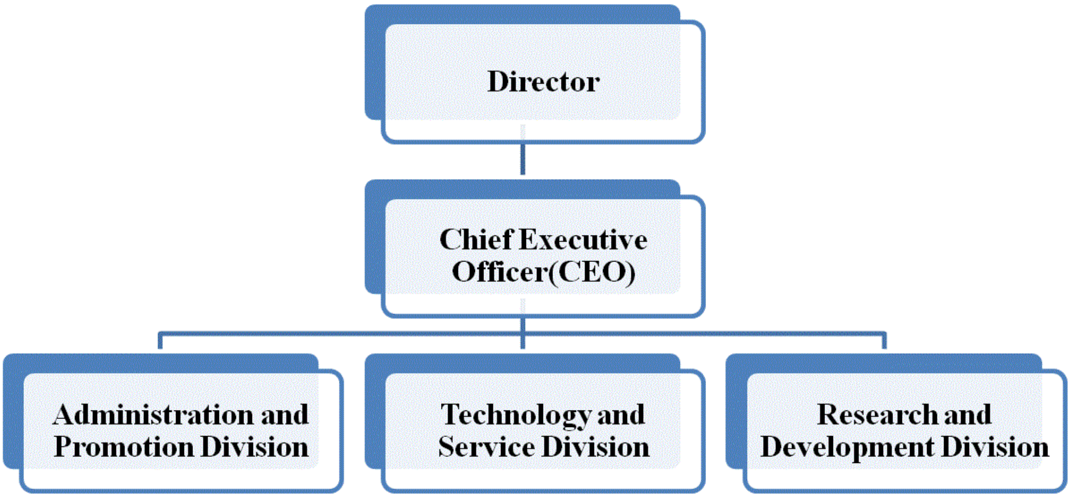
TWCERT/CC formally established since 1998. The major purposes of TWCERT/CC are to prevent and actively assist the computer and network security incidents in Chinese Taipei, to analyze the system vulnerabilities, to provide computer and network security tools and related documents for the system administrators and the programming guidelines for the developers, and conduct a series of training programs to raise the awareness of network security. TWCERT/CC is constantly reinforcing the organization functions and refining the network security services. With the dedicated devotion and seamless collaboration of the whole team, TWCERT/CC has accomplished several significant gradational goals and missions as follows:

- To assist the handling of the intrusion incidents in the constituency, .tw domain.
- To announce the system vulnerability information.
- To provide security training and education on protection and defending technologies and skills.
- To assess periodically the national-wide security level in the Internet.
- To be the point of contact of Chinese Taipei for international coordination.

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

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

1.1.2 Organization


Director
Chief Executive Officer(CEO)
Administration and Promotion Division
Technology and Service Division
Research and Development Division

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 Chinese Taipei's network security incidents with other CERTs. Expect to achieve the following goals:

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

- Real-time Incidents handling: offer an immediate warning and defense force to effectively restrain and control incidents extending.
- Recovery support: provide technological consultant and support to recovery operation and reduce damage.

Year	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010
Total	85	962	1260	5318	2874	1824	788	660	1087	679	1094

Table 1. TWCERT/CC incident response statistics

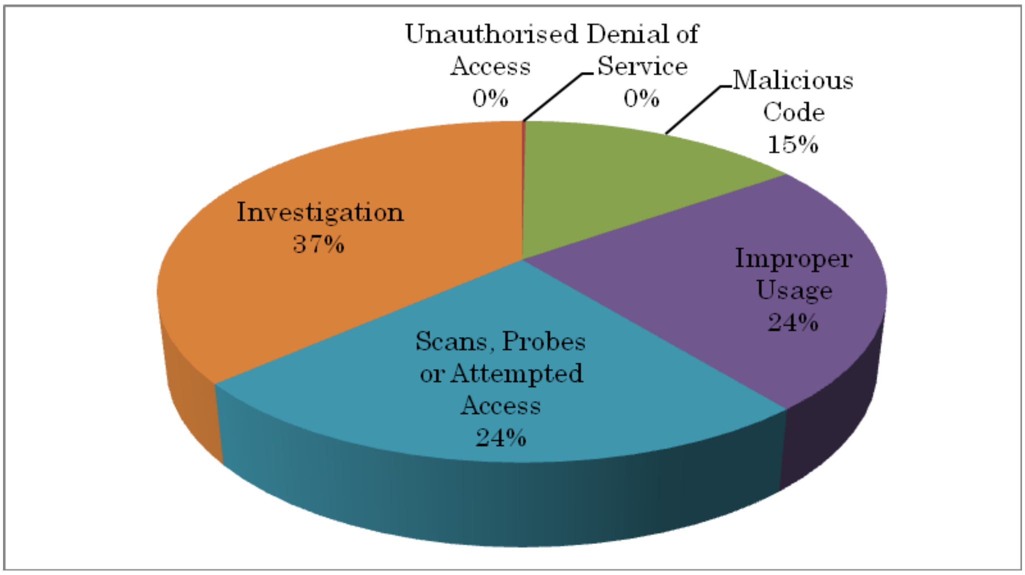


Figure2. TWCERT/CC incident response classification

2.2 Security Vulnerability Announcement

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

Year	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010
Advisory	178	172	258	142	197	140	138	119	49	44	234

Table 2. TWCERT/CC advisory statistics

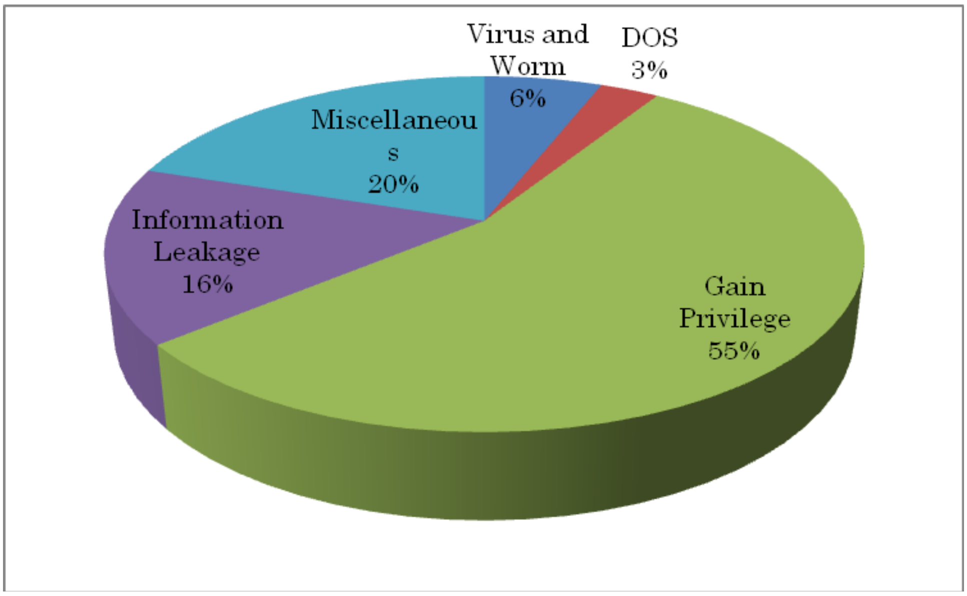


Figure 2. TWCERT/CC advisory classification

- **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 Chinese Taipei 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 Chinese Taipei.

- **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.

- **Remote Security Auditing System maintenance**

Systems or applications bugs and vulnerabilities are exploited to cause most incident events and unauthorized access. TWCERT/CC established an on-line Security Auditing System to provide customers self-check system vulnerabilities and patch without downloading/ installing/upgrading any software. Security Auditing System is a fortification of risk management tools, which is as important as firewall, anti-virus software and IDS. Security auditing system helps administrators understand the potential vulnerabilities and threats of their administrative domain. By continuing research and development, TWCERT/CC Security Auditing System will provide better and convenient service to accomplish the following design goals:

Convenience
User-friendly interface and easy-to-use
Flexible configuration and setup
Reliability
Reliable and efficient scan
Integrity
Graphical statistical report
Suggested and related advisories in the report

- **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. 3.

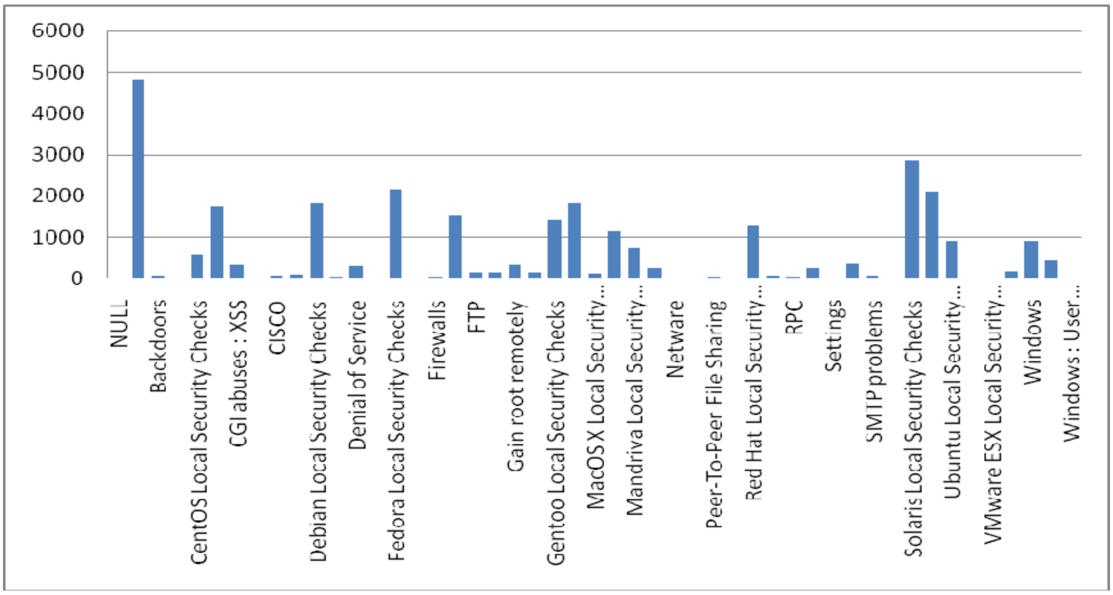


Figure 3. Categories of TWCERT/CC Vulnerability Database

- **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.

3. Events organized / co-organized

3.1 Information Security Training

TWCERT/CC hosts seminars or training regularly to popularize network security knowledge, to enhance system administrators' skills, and provides a good interaction channel for personal training and education promotion.

Date	Subject
2010/11/17	Network Security Countermeasures
2010/11/11	Web Application Security
2010/08/25	Network Attack and Defense-Phishing
2010/08/18	Personal Data Protection
2010/07/07	DNS Security
2010/06/11	Intrusion Detection and Prevention
2010/04/21	The analysis of Malicious code and Digital Forensic
2010/03/23	Unix-like System Security
2010/03/22	Cybercrime and Information Security

Table 3. Timetable of TWCERT/CC Training

3.2 Drill

TWCERT/CC helps TANet(Taiwan Academic Network) to run Information Security informative drill program during a period of two weeks, a total of 4,109 educational institutions involved in this successful program and the completion rate is 98%.

3.3 Collaboration Meetings

Date	Collaboration Meeting
2010/12/25	TWCERT/CC Network Security Technology Seminar
2010/12/24	TWCERT/CC Second Consultative Council
2010/09/23	Information Security Strategic Alliance Council
2010/09/16	TWCERT/CC First Consultative Council
2010/07/21	TWCERT/CC Network Security Technology Seminar
2010/05/12	TWCERT/CC Network Security Technology Seminar

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 Chinese Taipei 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.

- **Certification**

Staff 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 played 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.

5.1 Forum of Incident Response and Security Teams (FIRST)

FIRST is the Forum of Incident Response and Security Teams. It was clear from then on that information exchange and cooperation on issues of mutual interest like new vulnerabilities or wide ranging attacks - especially on core system like the DNS servers or the Internet as a critical infrastructure itself - were the key issues for security and incident response teams. FIRST 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 becomes the first official international coordination in Chinese Taipei by joining the FIRST in October 2001 to share the latest security information and technologies in FIRST forum with members, attends annual FIRT conference to establish a transnational security joint defense system and enhances incident-handling capability for integrated early-warning mechanism.

5.2 Asia Pacific Computer Emergency Response Team (APCERT)

Besides globalization organizations, Asia Pacific Computer Emergency Response Team is a regional coordination organization established by countries of the Asia Pacific region in 2002 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 Chinese Taipei much effort in security and help to understand the latest development and tendency in the Asia Pacific region.

5.3 Seoul-Melbourne Multilateral Memorandum of Understanding on Cooperation in Counting SPAM

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 Chinese Taipei's spam issues and exchange the anti-spam jurisdiction process with other members.

The key points of our missions are:

To cope Chinese Taipei'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 Chinese Taipei'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 Chinese Taipei'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.

15. TWNCERT /CC Activity Report

Taiwan National Computer Emergency Response Team - Chinese Taipei

1. About TWNCERT

TWNCERT domestically as known as ICST (Information & Communication Security Technology Center) is the leading CSIRT in Chinese Taipei public sector. TWNCERT is intended for improving incident response and information security awareness in Chinese Taipei. It is mainly dedicated to create a response center that can help optimize the capability of real-time monitoring, coordination, response and handing in the face of security incidents.

The missions of TWNCERT include:

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

TWNCERT services including:

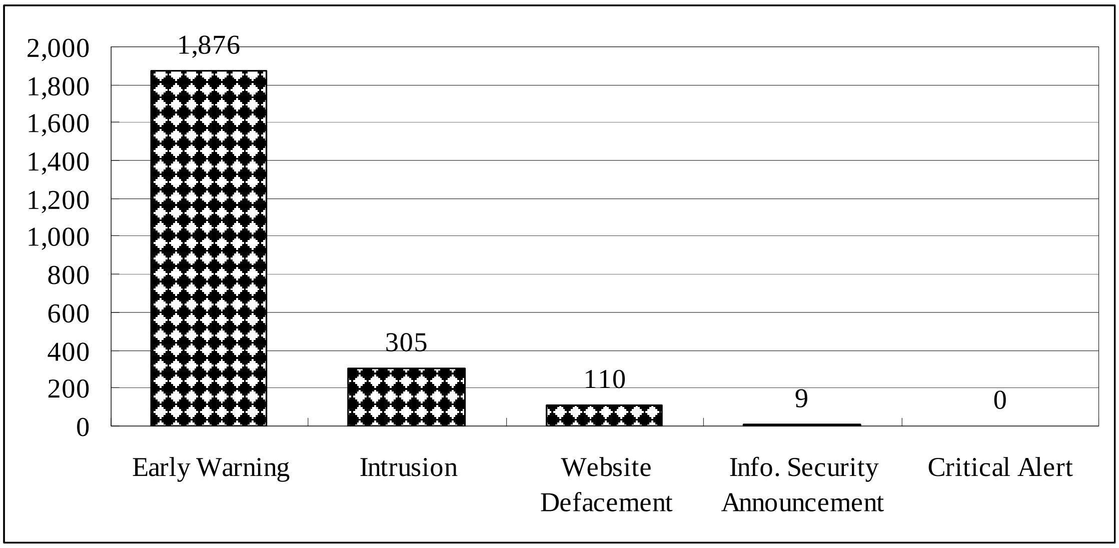
- Alert and publication: Guarding against and publishing probable security threats (e.g. vulnerability analysis).
- Technical service: Providing technical service to government agencies.
- Assistance in the setup of CERT: Assisting interested agencies to set up their own CERT.
- Consultation: Making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

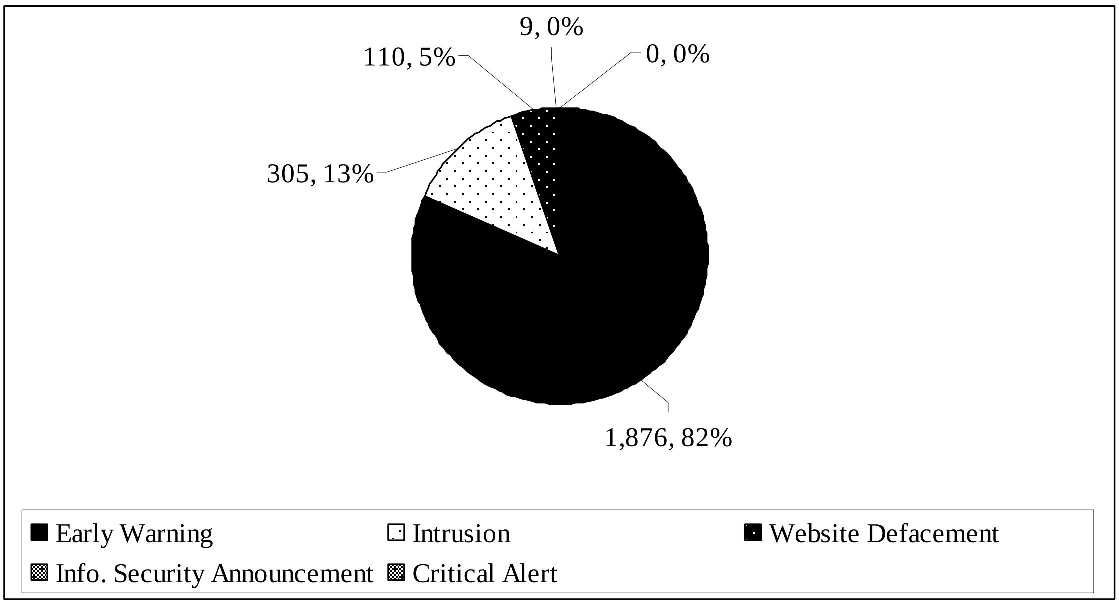
- Coordination: Building coordination and communication channels with domestic and foreign incident response organizations.

2. Operations & Activities

In 2010:

- TWNCERT received 732 information security incident reports from Chinese Taipei government and academic sectors
- TWNCERT offers 1,301information security consulting service
- TWNCERT offers 13 information security incident handlings for government sectors.
- TWNCERT held 10 government information security seminars、1 e-mail security seminar and 1 Web AP security seminar
- ITWNCERT held 3 training courses for government sectors: SSCP (25 people)、BS10012 (46 people) and computer forensics (50 people)
- 2010 Information Security Contest (including Catch-the Flag, Slogan, Poster and Animation Contest) starts from September to November.
  - Animation Contest: 115 attendees; 10 winners
  - Catch-the Flag :407 attendees(147 teams); 12 teams win
  - Slogan Contest: 2,242 competitions; 8 winners
  - Poster Contest: 593 competitions; 13 winners
- TWNCERT published totally 2,300 advisories ’ including:
  - Early Warning: 1,876
  - Intrusion: 305
  - Website Defacement: 110
  - Info. Security Announcement: 9
  - Critical Alert: 0





- In April, 2010, TWNCERT started to run the Government Information Sharing and Analysis Center (G-ISAC) and cooperated with its members:
  - Ministry of Education (Academic Information Sharing and Analysis Center, A-ISAC)
  - National Communication Commission (NCC Information Sharing and Analysis Center, NCC-ISAC)
  - Taiwan Network Information Center (TWNIC)

- ➢ Government Service Network (GSN)
- ➢ Ministry of Economic Affairs (EC-CERT)
- ➢ Private organizations SOCs (4 SOCs by 2010/12)

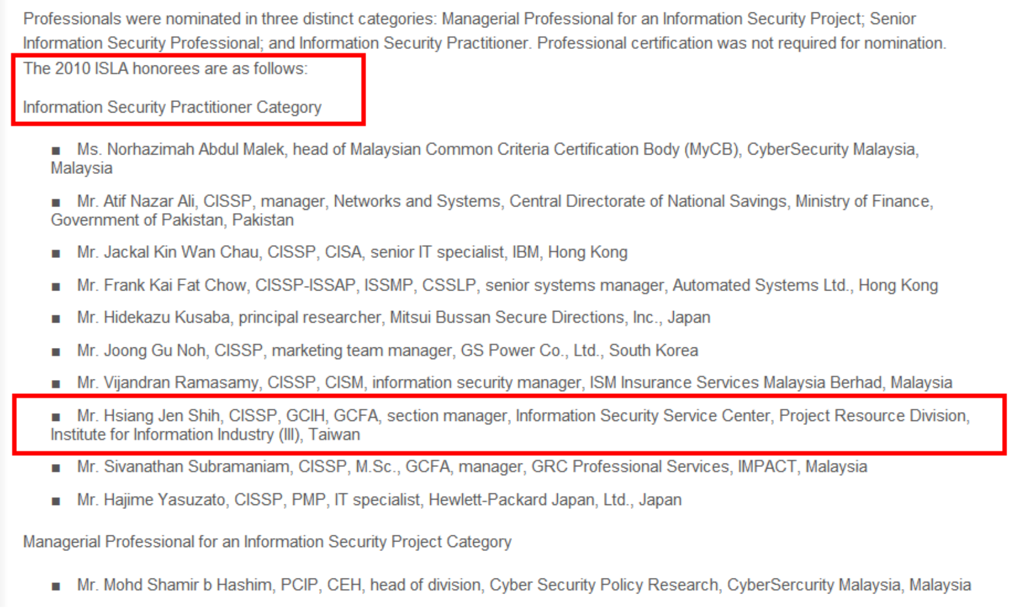
- G-ISAC mainly share 5 types of information among the members with its customized IODEF format: Announcement、Intrusion、Early Warning、Defacement、Feedback Information. G-ISAC members has shared 2,782 information.

3. Events

- Attended APCERT AGM as the full member in March
- Attended FIRST AGM as the full member in June.
- Attended AVAR AGM as the member in November
- Attended Microsoft Worldwide Public Safety Symposium in March
- Attended 2010 Conference on Cyber Conflict Conference in June
- Attended APECTEL 42 in August

4. Achievements

Our Engineer Mr. Hsiang Jen Shih is honored to gain (ISC)²® Announces Honorees for Annual Asia-Pacific Information Security Leadership Achievements Program in Information Security Practitioner Category.



Professionals were nominated in three distinct categories: Managerial Professional for an Information Security Project; Senior Information Security Professional; and Information Security Practitioner. Professional certification was not required for nomination.

The 2010 ISLA honorees are as follows:

Information Security Practitioner Category

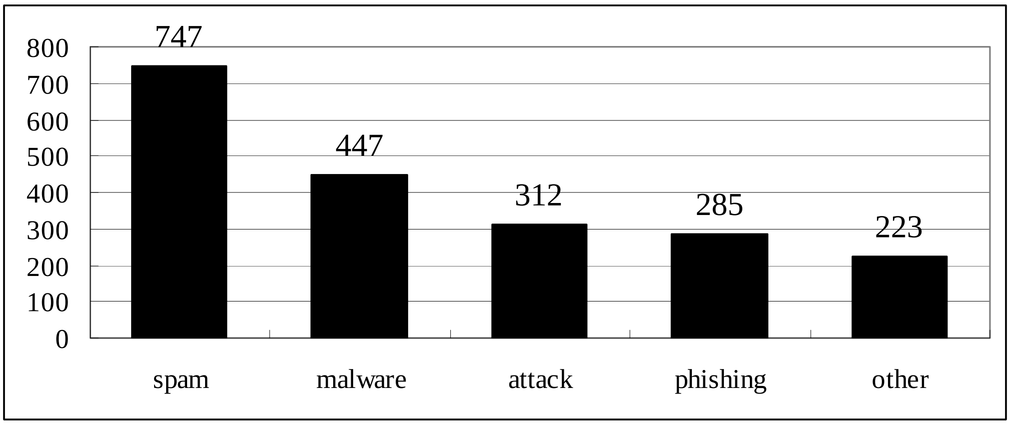
- ■ Ms. Norhazimah Abdul Malek, head of Malaysian Common Criteria Certification Body (MyCB), CyberSecurity Malaysia, Malaysia
- ■ Mr. Atif Nazar Ali, CISSP, manager, Networks and Systems, Central Directorate of National Savings, Ministry of Finance, Government of Pakistan, Pakistan
- ■ Mr. Jackal Kin Wan Chau, CISSP, CISA, senior IT specialist, IBM, Hong Kong
- ■ Mr. Frank Kai Fat Chow, CISSP-ISSAP, ISSMP, CSSLP, senior systems manager, Automated Systems Ltd., Hong Kong
- ■ Mr. Hidekazu Kusaba, principal researcher, Mitsui Bussan Secure Directions, Inc., Japan
- ■ Mr. Joong Gu Noh, CISSP, marketing team manager, GS Power Co., Ltd., South Korea
- ■ Mr. Vijandran Ramasamy, CISSP, CISM, information security manager, ISM Insurance Services Malaysia Berhad, Malaysia
- ■ Mr. Hsiang Jen Shih, CISSP, GCIH, GCFA, section manager, Information Security Service Center, Project Resource Division, Institute for Information Industry (III), Taiwan
- ■ Mr. Sivanathan Subramaniam, CISSP, M.Sc., GCFA, manager, GRC Professional Services, IMPACT, Malaysia
- ■ Mr. Hajime Yasuzato, CISSP, PMP, IT specialist, Hewlett-Packard Japan, Ltd., Japan

Managerial Professional for an Information Security Project Category

- ■ Mr. Mohd Shamir b Hashim, PCIP, CEH, head of division, Cyber Security Policy Research, CyberSercurity Malaysia, Malaysia

5. International Collaboration

- Started cooperate with IMPACT GRC in August and join its mailing list
- Totally received more than 3,000 information security incident reports and handled 2,076 reports in 2010. Below is the top 5 types of incident reported:



16. 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.

1.2 Roles of VNCERT

1.2.1 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.
- Lead the process of deploying the Anti-spam Law (Decree No.90 of the year 2008) in Vietnam.

1.2.2 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 fifty.

2. Activities & Operations

2.1 Incident reports & handling

In 2010, the total number of serious incidents reported to VNCERT was 249, which has increased more than 133% in comparison with 2009. Many reports were about phishing and defaced, some about malware and DoS attacks.

Almost phishing cases were related to finance, commonly forging banks' website to steal bank's account, and they were reported from outside Vietnam.

In 2010 there are 02 serious incidents in Viet Nam: Vietnamnet, the biggest e-newspaper, was attacked few times with deface, information stolen, and DDoS attack at last. Some incidents occurred on government agency systems, were handled by VNCERT quickly.

2.2 Watching and supporting activities

VNCERT also actively watched security news from many sources, and warned about security threats to organizations via private channels or to Internet users via media press. For examples, the threat of SSH scanning and some vulnerabilities of Microsoft products were warned early and widely.

VNCERT has supported some state organizations and industries to audit critical information systems and enhance system security.

VNCERT helped to secure all online important government events.

2.3 Anti-spam activities

- Request for composing new Circular that support Decree No.90/2008 (Against Spam).
- VNCERT has issued more than 60 certificates to Content Provider in total for providing advertising services on SMS, email and SMS over Internet.
- Building a system to manage certified Content Providers, SpamAlert system to monitor spam SMS by receiving reports from users.
- VNCERT has co-operated with MIC's Inspectorate to fine some companies that violated Anti-spam Law. At the end of the year, the number of spam messages decreased a lot.

2.4 Legal environment improvement

- Consider improving some aspects of Decree No.90 (Against Spam).
- Consider to request for building up Digital Information Security Law.
- Took part in composing Circular for Incident handling, and other Circulars to improve law system.

3. Events organized / Co-organized

3.1 Training & Drills

- In 2010, VNCERT arranged some training courses for raising information security awareness as well as working experience in Information Security field to staff in some organizations.

- VNCERT participated in 02 international drills: ASEAN CERTs Incident Drill and APCERT Annual Drill.
- Organize the course to study about Network designing. All attendees achieve CCDA certificate.

3.2 Seminars & Etc

- Co-operated with Ministry of Public Security and IDG Vietnam to organize annual event "Security World", the largest IT security conference in Vietnam. At this 5th anniversary, Security World 10 will feature the theme "Building a Practical and Effective Security Strategy in Today's Challenging business environment", focusing on high-efficient and cost-effective information security solutions to help enterprises maximize their ROI when budgets are tightened as consequences of the financial crisis.
- Co-operated with VNISA to organize the annual event "National Information Security Day 2010", the most important security conference of the year. The event was hosted by Ministry of Information and Communication. Main theme of 2010's is "Digital Information Security National Plan – A Road ahead".
- Co-organized the second event of ASEAN CSO Conference & Awards, featuring the theme "CSO – smart management, instant response", that focuses on effective strategic plan and information security management, awareness improvement of information security in enterprise community, network security and secure network security environment.

3.3 Consultancy

VNCERT supported the state and private organizations in the IS area and helped the Government to develop the national strategy to secure cyber-space. Besides, VNCERT provided assessment service to a some state agencies, helped them in auditing their system and procedures.

4. Achievements

VNCERT:

- Took part in the national and international conferences related IS, VNCERT always made detailed reports on network security, actively expressed the idea and enthusiasm to the conference programs.

- Had a good communication with the press and other means of communication to inform the VNCERT's activities to the public, aiming to raise prestige and state management role of Ministry of Information and Communication.
- Deployed RD project on building Internet information security monitoring and management system, support in watching and early warning about information security threats.
- Improved state macro-management model of the email-spam and SMS spam to the law system, took part in organizing activities to prevent spam messages.

5. International Collaboration

- VNCERT has signed MoUs with Laos' DTI (Department of Telecommunications and Internet) for co-operation in building LaosCERT.
- Take part in the "On-Job-Training" course of Malware Analysis that provided by JPCERT/CC.
- Take part in IMPACT co-operate program to study SANS' course and achieve certificates of GSEC (GIAC Security Essential Certification).
- Co-operated with oversea organizations to exchange experiences, study new technology and product that used for network monitoring.
- VNCERT has joined annual conference of APCERT, national CERTs conference, and many others.
- Organized a trip to visit Japan companies to study and exchange experiences about Information Security for Government.

6. Future Plans

VNCERT will:

- Coordinate the "Master plan of national developing digital information security of Vietnam in period from 2010 to 2020", in the roadmap from now to 2020, will have 6 major projects which are given as top priority to improve information security infrastructure and human resource training.
- Adjust some policies in law system for better suiting with current context.
- Develop and publish some new national standards on information security management and build up the National Network Security Technical Center in VNCERT.
- Strengthen information channels to deliver and receive cyber security

information nation-wide.

- Organize the national workshops/events on cyber security.
- Continue improving official websites of VNCERT for cyber security and for anti-spam management.
- Finish the RD projects on building the technical system for watch, warning and incident response and taking part in some international collaboration research projects.
- Participate actively in the collaboration activities among APCERT and ASEAN CERTs, improving exchange experiences activities; support Laos on building LaosCERT.
- Co-operate with TrustSphere on developing and maintaining a national database of senders of legitimate commercial email (that called "Vietnamese TrustCloud")
- Take part in cyber security activities following co-operation framework of ITU and IMPACT.

7. Conclusion

As a Full Member of APCERT, VNCERT will do the best to fulfill all the responsibility to develop information sharing and cooperation framework within APCERT, aiming to improve Internet security level and the quality of Internet related emergency response in the Asia Pacific region, as well as to contribute to the world's information security development.

Particularly, VNCERT will fully participate in sharing data, research, response strategies, and early warning notifications with all other CERTs around the world.

Ministry of Information and Communication of Vietnam is willing to support the APCERT initiative and promise to support VNCERT to contribute actively to the activities of the APCERT.

17. 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

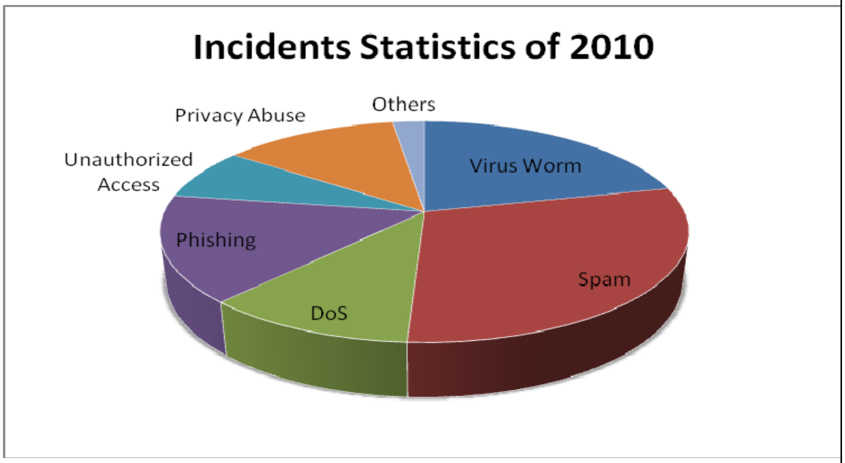
As a national CERT the constituencies of BDCERT are all the Internet users of Bangladesh. We work closely with all the ICT stake holders particularly with ISP Association of Bangladesh (ISPAB), Bangladesh Association of Software &

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

In year 2010, BDCERT has received 173 incident reports. Taxonomy statistics of incidents report are shown in figure 1. Majority of incidents are related with Phishing, Spam, DoS and Malware.



Taxonomy	Incident No
Virus / Worm	37
Spam	51
DoS	19
Phishing	27
Unauthorized Access	13
Privacy Abuse	22
Others	4

Figure 1 : Taxonomy statics of Incident

2.2 Incident Reports

The following graph shows the rise in incident reports received by BDCERT ever since its inception.

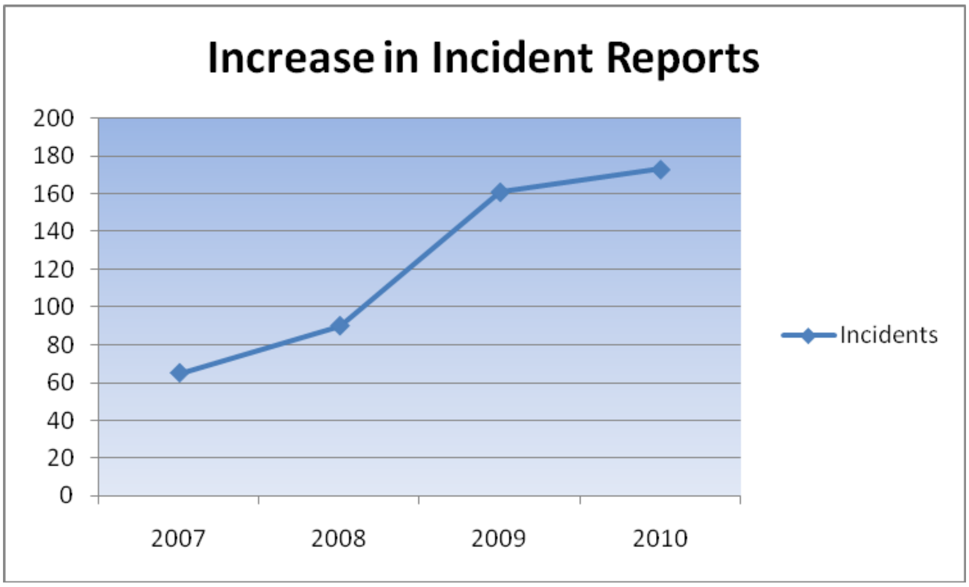


Figure 2: Increase in Incident Reports

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.

- 27 JAN-3 FEB SANOG XV:

  BDCERT collaborated with ISPAB to host the SANOG 15 Meet held at Dhaka. The meeting covers various discussions, conference, tutorials and workshops. A tutorial on Infrastructure Security Track was arranged for participants from the IT Sector to learn about the best practices for network core infrastructure security and layer 2 attacks and mitigation techniques.

- 14-17 September 2010 - Internet Governance Forum (IGF) 2010

  BDCERT collaborated with ISPAB and APNIC to arrange a Remote Participation to "IGF 2010 – developing the future together" which was live webcast from Vilnius Lithuania. It is the first time that Bangladesh had participated to this event from home. Some of the key issues covered in the IGF were Managing Critical Internet Resources; Security, Openness and Privacy; Access & Diversity; etc.

3.2 Trainings & Seminars Participated

- 29 Jan 2010 - Participated in SANOG training on "Network Core Infrastructure Security – Best Practices" and "Layer 2 Attack and Mitigation Techniques" which was conducted by Yusuf Bhaijii.
- 27Sept – 1Oct 2010 – "2010 APISC Security Training Course" held by KCC at Korea and supported by KrCERT/CC.
- 28-29 October 2010 - OIC-CERT Summit 2010 "Securing the Digital Ummah" held at Kuala Lumpur Malaysia

4. ACHIEVEMENTS

- Successfully conducted and participated in IGF 2010.
- Successfully co-hosted SANOG XV
- Supported WTISD 2010 fair organized by BTRC. Special speech and write up on Information security was provided by BDCERT.

4.1 Presentation

BDCERT has given presentations at several conferences throughout 2010 which includes:

a) APISC 2010, hosted by KrCERT/CC

b) OIC-CERT 2010, hosted by Cyber Security Malaysia

5. INTERNATIONAL COLLABORATION

BDCERT is collaborating with JPCERT/CC in Internet Traffic Monitoring Data Visualization Project "TSUBAME" project. In this project, sensors for the Internet traffic monitoring system are installed in the Asia Pacific region, and monitoring data acquired by these sensors are shared among participants of this project.

6. FUTURE PLANS & Projects

a) Government Endorsement for BDCERT

b) Full Membership of APCERT

c) Full Membership of OIC-CERT

e) Building Awareness

f) Fund Raising

g) Consulting to form other CERTs within the constituents

7. CONCLUSION

Internet users are growing exponentially since Bangladesh got connected to the global submarine cable system SEA-ME-WE-4 in May 2006. Though we have huge growth in Telecommunication and Internet but cyber security is not very familiar to general people except the nuisance of viruses and malwares. Thus BDCERT is working hard to make people aware of the risks of unsecured Internet. We are working closely with law enforcement agencies, government bodies and international CERTs to provide Incident response and mitigation to cyber threats.

18. CERT Australia Activity Report

CERT Australia - Australia

1. About CERT Australia

1.1 Introduction

CERT Australia is Australia's national computer emergency response team. It is the cyber security coordination point between the Australian Government and the Australian private sector, and represents Australia to the international internet security and incident response community – primarily the national CERT community.

1.2 Establishment

CERT Australia was announced in November 2009 and 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.

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.

1.3 Workforce power

CERT Australia currently employs 23 core staff.

1.4 Constituency

CERT Australia is the cyber security coordination point between the Australian Government and the Australian private sector. It seeks to improve cyber security for all Australian internet users by developing information about significant threats and vulnerabilities that may affect Australian systems, sharing it with key internet entities and assisting in mitigating these threats. CERT Australia does this in conjunction with other Australian government agencies.

2. Activities & Operations

Throughout 2010, CERT Australia:

- provided unique cyber security threat and vulnerability information relevant to the Australian private sector, the purpose of which is to assist the private sector to protect their networks.

- co-ordinated, facilitated and performed vulnerability analysis and disclosure, especially where vulnerabilities were identified by Australian stakeholders.
- provided a data repatriation capability to CERT Australia constituents.
- maintained three sector-specific information exchanges with the banking and finance, control systems and telecommunications sectors. These exchanges enabled 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.
- CERT Australia also participated in three academic research projects related to cyber components of Australian internet security.

2.1 Incident handling reports

In 2010, CERT Australia fielded 187 incidents and produced and disseminated 47 sensitive advisories on cyber vulnerabilities affecting systems of national interest.

2.2 Data repatriation

CERT Australia also processed approximately 250,000 stolen records, some including usernames and passwords, with 145,000 being repatriated to responsible organisations (including Australian businesses and peer national CERTs overseas).

3. Events organized / co-organized

3.1 Training

CERT Australia provided a trainer for the **TRANSITS CSIRTS**[13] training course in Korea in September 2010 as well as other parts of the **APISC**

[13] TRANSITS stands for 'Training of Network Security Incident Teams Staff' – originally, a European project to promote the establishment of Computer Security Incident Response Teams (CSIRTs) and the enhancement of existing CSIRTs by addressing the problem of the shortage of skilled CSIRT staff, the TRANSITS material has been further developed, expanded and adopted by various CERTs world-wide and remains in-use as part of training initiatives to date (Ref to original project: *http://www.ist-transits.org/*)

Training course[14], a yearly event organised by KrCERT.

3.2 Drills

Cyber Storm III (run in the third quarter of 2010) involved the United States, Australia, New Zealand, Canada, and the United Kingdom, Japan and nine European nations.

CERT Australia was actively involved in and took a leading role in the Australian component Cyber Storm III.

The Cyber storm framework was designed to test the effectiveness of response plans of both cross-border international communications between national CERTs, and locally between CERTs and the owners and operators of a nation's important IT systems and hardware.

Because the majority of Australia's important IT systems are owned and operated by the private sector, Cyber Storm III involved over 50 Australian organisations, including the communications, food, finance, transport, utilities and government sectors.

4. Achievements

4.1 Presentations/conferences

Throughout 2010, CERT Australia presented and participated in several international forums including:

- 41st APEC Telecommunications (APEC-TEL 41) conference, May 2010, Chinese Taipei.
- The 22nd annual Forum of Incident Response Security Teams (FIRST) conference, June 2010, USA.
- The 9th annual AusCERT conference, May 2010, Australia.
- Forum of Incident Response Security Teams – Technical Colloquium (FIRST-TC), September 2010, China.
- South East Asia Regional Centre for Counter-Terrorism (SEARCCT) cyber terrorism roundtable, April 2010, Malaysia.
- The World Computer Congress, August 2010, Australia.

[14] APISC Training is a yearly event organised by KrCERT. The week long event is aimed at providing CERT establishment training to (often developing) countries who have recently set up CERT teams or are intending to set up teams and may not have the specialist knowledge required. The core of the training is the TRANSITS training course as well as some other presentations by KrCERT.

4.2 Publications

4.2.1 Cyber alerts, advisories and strategies

CERT Australia makes cyber security alerts and advisories available to constituents via website, portal and direct contact. These alerts and advisories contain up-to-date information on cyber threats and software vulnerabilities and steps that can be taken to better secure computer systems.

CERT Australia continues to promote further development of the "Matrix of 35 strategies", rated by effectiveness, to assist organisations mitigate against targeted electronic intrusions, jointly developed by the Cyber Security Operations Centre in the Defence Signals Directorate and CERT Australia.

The abovementioned cyber alerts and advisories as well as documents supporting the Matrix of 35 strategies is publicly available from the CERT Australia website at URL:
http://www.cert.gov.au/www/cert/cert.nsf/Page/Alerts_and_Advisories

5. International Collaboration

Internationally, CERT Australia continues to establish and maintain contact with international CERTs and engage pro-actively in international forums. 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 more recent international activity include:

- CERT Australia was actively involved in the development of and playing in the 2011 APCERT Drill.
- Working with international counterparts on cyber incidents spread across a range of economies.

6. Future Plans

Some of the services and initiatives CERT Australia performs and will enhance in future include:

- Industry Briefings to raise awareness and build capability for Australian owners and operators of important IT systems
- Shutdown requests for sites hosting malicious software

- Notification of compromised Australian websites
- Improved vulnerability analysis and disclosure coordination
- Assessing emerging technologies and attack trends

19. MonCIRT Activity Report

Mongolian Cyber Incident Response Team– Mongolia

1. About MonCIRT

1.1 Introduction

A Mongolian Cyber Incident Response Team (MonCIRT) was formed by the lecturers of the Computer Science and Management School of Mongolian University of Science and Technology as Non Governmental, non profit organization in 2007 in response to the needs identified during an Internet security incident and operating as a service organization that is responsible for work with the Internet community in detecting and resolving computer security incidents as well as taking steps to prevent future incidents. MonCIRT services are available for all society,

Our specific mission is to

- Improve information security awareness, literacy, provide comprehensive trainings.
- Provide a comprehensive view of network security risks, attack methods, vulnerabilities, and the impact of attacks on information systems and networks;
- 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
- Provide methods to evaluate, improve, and maintain the security and survivability of networked systems

The MonCIRT helps the Internet community 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

Since 2002 prof Khaltar Togtuun developed the project “Mongolian Computer Emergency Response Team” and searched for supports in various instances. Finally in 2006, after approvement of "E-Mongolia" national program, when the government officials begin to understand importance of this organization a little some experts of information security was established MonCIRT as NGO. From 2006 till 2010 MonCIRT operate as sole national CSIRT of Mongolia. Only from 2010 the Government Communication Department has begun the initiative on creation of CSIRT of Government bodies.

As the national CERT of Mongolia, MonCIRT acts as the focal point for cyber security for the nation, especially business sector. Due to lack of knowledge, awareness, lack of incident response knowledge and capabilities of organizations the MonCIRT cannot becomes the single trusted source of advice about the latest threats and vulnerabilities affecting computer systems and networks yet, and a source of expertise.

1.1.2 Workforce

MonCIRT currently has a total of 6 constant staffs such as: executive director-1, experts 3 including watch and warning group leader, the bookkeeper 1, system administrator-1. Due to absence of government support and self financing we have dismissed 2 of our watch and warning staffs and our forensic analyst and botnet analyst has moved to the USA for study.

We constantly feel shortage of the qualified experts.

1.1.3 Constituency

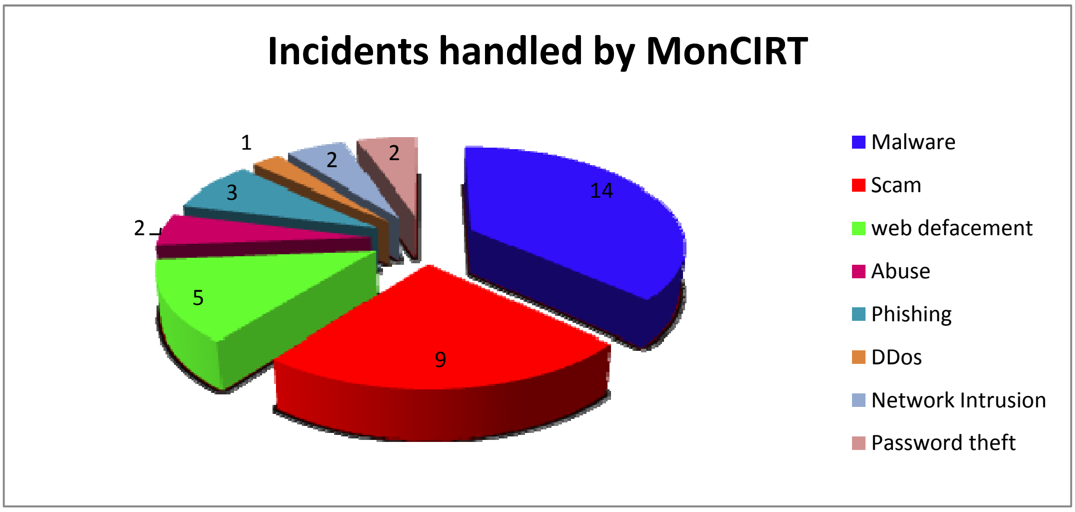
Currently MonCIRT‘s constituency encompasses the whole of the Internet community of Mongolia. In case of establishment and start of expected government MNCERT our constituency will be narrowed and it will be formed from business companies, private sector organizations, NGO and general public.

2. Activities & Operations

2.1 Incident Handling

From January through December 2010, the MonCIRT received 231 email messages and more than 30 hotline calls reporting computer security incidents or requesting information. Only 42 of these messages, information was related with real incidents. We received 9 vulnerability reports and handled 38 computer security incidents during this period. Because of lack of Information Security knowledge, misunderstanding of importance of network security the number of incident reports, requests not increase in comparison of 2009. We cannot retrieve incident handling statistics from organizations, administrators due to lack of security information sharing practice and mentality.

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



We continue to provide advice to computer system administrators in the Internet community who report security problems. From 2011 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 Incident and Vulnerability Analysis

We trying to become a major reporting center for incidents and vulnerabilities and establish MonCIRT reputation for discretion and objectivity. MonCIRT working to create organization's trust to us as reliable security center which can share sensitive information about security compromises and network vulnerabilities. Our connection with the Computer Science and Management School of Mongolian University of Science and Technology contributes to our ability to be neutral, enabling us to work with commercial competitors and government agencies without bias. As a result of the community's trust, we will be able to obtain a broad view of incident and vulnerability trends and characteristics.

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

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

2.3. New services

2.3.1 Botnet analyze

MonCIRT initiated the survey on botnet and the result of our survey shows that in Mongolia located one of Command and Control (CC) center of Botnet. We now working to investigate CC center's location. Further we plan to facilitate organizations in investigating of infected (zombie) computers.

2.3.2 Digital Forensics

One of founder of MonCIRT Mr Baasandorj N (SANS certified ethical hacker, forensic analyst) organize training on digital forensic for software engineers of law enforcement organizations, experts of Forensic Analyze Center of Mongolia. In addition MonCIRT plan to develop project together with Forensic Analyze Center of Mongolia named "National Digital Forensic Analyse Capacity Building".

2.3.3 Setting up sector based CSIRTs

MonCIRT has initiated the setting up of government CERT located in National Data Center and Military CERT which are sector-based. In addition we talking with Mongolian Bank Association to work closely with banking sector of Mongolia.

The our initiatives on establishment of sector based CSIRT's is aimed at ensuring that MonCIRT remains a small, focused national central body that functions only as an incident coordination center to handle large scale incidents effectively.

Sectoral CSIRTs will provide industry specific services to their constituents.

3. Events organized / co-organized

3.1 Training / Education

The MonCIRT offers six 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. All courses can be licensed.

Courses offered in 2010 included the following:

- *Concepts and Trends in Information Security*
- *Network security management and configuration*
- *Information Security for Managers*
- *Internal Information Security audit and Self evaluation*
- *Network Monitoring*
- *Fundamentals of Incident Handling*

3.2 Drills

In 2010 MonCIRT for the first time has tried to organize network security drill but due to financial limitation cannot to involve skilled experts and big audiences. Therefore was organized only small internal drill for school leavers.

In addition MonCIRT provide some consultancy on network security, security of Cloud Computing, digital forensic analyze, penetration test for government departments/private organizations

3.3 Seminars & Workshops

In order to create awareness and build IS skills within the constituency MonCIRT conducted the following conferences, seminars, workshops successfully during 2010:

- Together with National Security Council the MonCIRT organized conference named ‘Realization of Information Security Strategy within new National Security Strategy’. The governing board director of MonCIRT prof Khaltar Togtuun was one of leading developer of new “National Security Conception”. September 2010

- With sponsorship of Security Solution Service LLC and National Information Technology Park organized annual "Security Open Day Mongolia 2010". Within these days it is successfully hold scientific & practical conference, fair and workshop.
- Prof Khaltar T and Mr Ganbold T invited and participated in seminars, conferences organized both in Mongolia or abroad and made some presentations on behalf of MonCIRT.

4. Achievements

4.1 Presentations

MonCirt's board director and board members participated and presented in 3 local conferences and 2 conferences in abroad. In these conferences they have presented following presentations:

a. Conducted presentations in conference "National Security Conception and Globalism" for top officials of government organizations on theme "Information Security Issues in New National Security Conception".

b. Conducted presentations during the conference 'Realization of Information Security Strategy within new National Security Strategy' on themes "Cyber Security, Cyber warfare problems" and "Organizations' Network Security Policy, Procedures and Solutions"

c. Conducted presentations during the Annual "Security Open Day" on themes "Information Security Threats related with Mobile Devices", "Project Management in field of Corporate Information Security" and "Secure Computing Solutions for maintenance of security of Internet use in the corporate environment".

d. Conducted presentations during the Annual Information Security Conference in Moscow (Russia) on theme "Secure operation with web-applications in the Internet".

4.2 Publications

The MonCIRT published 5 advisories in 2010. 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, post them to the IT park and ICT mailing list.

a. Incident and Vulnerability Notes

The MonCIRT publishes incident notes and vulnerability notes as an informal means for giving the Internet community timely information relating to the security of its sites. Incident notes describe current intruder activities that have been reported to the ICTPA and Government Communication Department.

b. 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*

Some additional papers published in 2010 include

- "Information Security for Small and Medium Enterprises" Brochure, April 2010
- "Software Quality Requirements and Security Evaluations.
- “SaaS Security”

c. 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 2010.

5. International Collaboration

5.1 MoU

In addition to being member of APCERT, MonCirt has signed Memorandum of Understandings with ICTPA Mongolia and with IMPACT.

5.2 Event participation

March 2nd -5th, 2010
APCERT AGM & Conference
Phuket, Thailand.

March 16th – 18th, 2010
Asia Pacific Grid PMA conference.
Chinese Taipei

April 19th – 21th, 2010
InfoSec Europe
London, UK.

June 8th – 11th, 2010
Annual Information Security Conference
Moscow, Russia

Sept 27th – Oct 1st
APISC Training
Seoul, South Korea

5.3 International incident coordination

No participation in International Incident Coordination.

6. Future Plans

6.1 Future projects

As promised by Prime Minister of Mongolia the Government will delegate government functions to the NGOs and will support financially. If this promise is realised into lives and MonCIRT will be captured in frame of this program to appear possibilities initiate projects.

The following projects are in the conceptual stage and will be implemented in the case of Government support:

a. Development and training new staffs capable to handle incidents professionally, conduct log analyze.

b. Implementation and setting up the National Monitoring Center.

c. Setting up more sectoral CSIRTs.

d. Additional Sensor deployment for "Tsubame" project, to cover all IP Address ranges belonging to Mongolia.

e. To organize regular annual scientific - practical conference "InfoSec Mongolia"

f. Implement the provisions of the collaboration agreement with ICTPA to provide additional training and certification opportunities to the constitution

g. Develop Digital Forensic Analyze Capacity Building Project together with Forensic analyze Institute of Mongolia.

d. Develop conception and implement IT audit system.

6.2 Framework

6.2.1 Future Operation

It is planned to purchase new hardware, software that is necessary to expand the operations of MonCIRT in the case of Government support. We plan to reorganize board structure, management staffs. The staffs will be trained to handle the increasing number of security incidents.

7. Conclusion

For MonCIRTs' constant and developing activity it is necessary financial support. Despite difficulties in financings the number of incidents reported and handled by MonCIRT increased 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 job, awareness campaigns, presentations and publications.

In connection with the increased quantity of the Internet incidents MonCIRT offered to the Government and Government Communication Department to organise sectorial CSIRTs. To help new appearing CSIRTs MonCIRT develops methodological guides, incident handling guide, CSIRT setting up guide on Mongolian and updated CERT handbook (on Mongolian).

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 sectorial CSIRTs) act as Coordination Center and a national point of contact, for its international counterparts. As a result of this evolution, MonCIRT will rename itself MonCERT Coordination Centre.

All the events organized by MonCIRT during the year 2010 were very successful. We will continue to conduct the Annual "Security Open Day" and will organize National Conference on Cyber Security under name "InfoSec Mongolia" 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.

MonCIRT will be implemented in the case of Government support such significant projects as

Implementation and setting up the "National Monitoring Center", "Digital Forensic Analyze Capacity Building Project" together with Forensic analyze Institute of Mongolia and "Conception and implement IT audit system".

20. 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 internet in 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 16 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	5
PG Diploma	4
BSc Eng/BSc/BIT	14
C|EH	2
Certified ISMS Auditor (ISO27000)	2
MCSC	1
MCP	1
CCNA	5
Chartered Engineers	3

1.3 Constituency

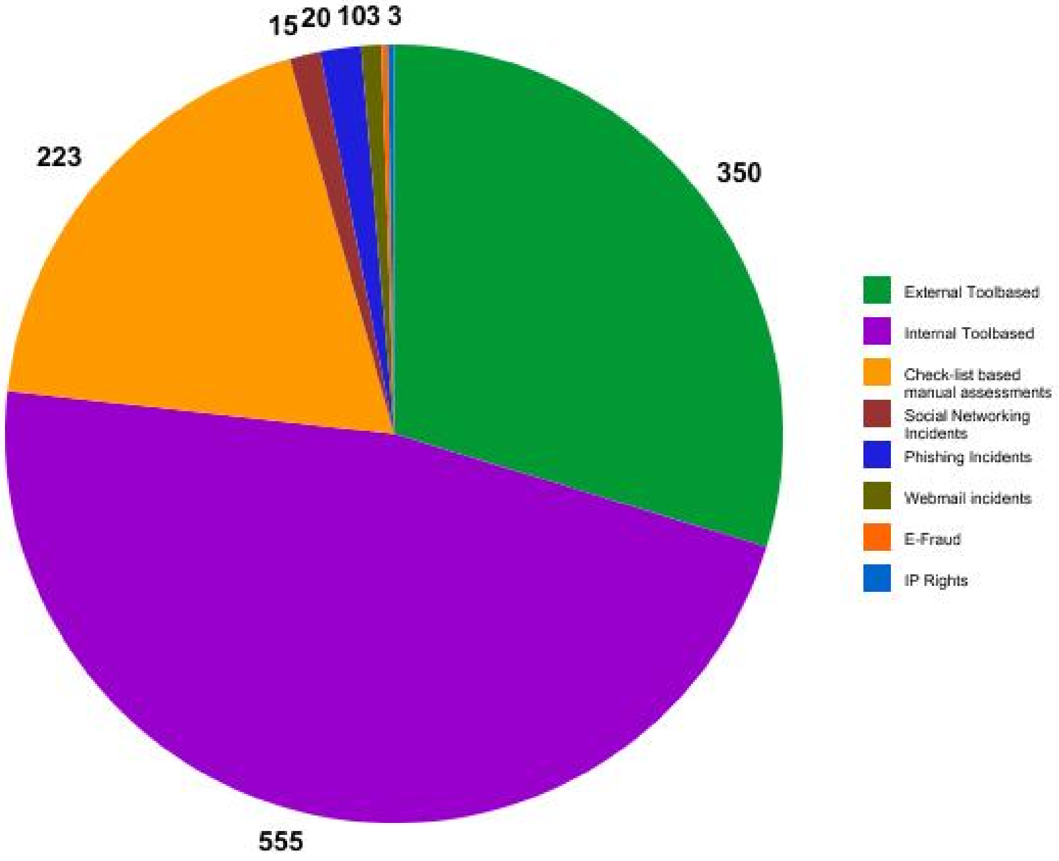
TechCERT works with its member organizations, selected governmental organizations as well as provide incident response services and awareness programmes for the general public of Sri Lanka.

2. Activities & Operations

TechCERT is currently engaged in the following operations

- Network Surveying and Vulnerability Assessments
- Responding to incidents received from the general public of Sri Lanka and TechCERT members
- Digital forensic investigations
- Firewall configuration testing
- Software code reviewing and security functionality audit
- Web Application penetration testing
- Routers and L3-Switches security assessment
- Wireless network security and penetration testing
- BCP and DRP planning and deployment

- Security Policy Evaluation in accordance with ISO 27001 standard
- Physical and Environment Security
- Implementation and maintenance of Certificate Authorities and related PKI services
- Advise on ISO 27001 implementation
- Vulnerability research and verification



TechCERT Activity Chart for 2010

2.1 Organizing of Training Seminars, Workshops and Demonstrations

- "Exploiting the weakest link in CMSs", Technical presentation by Janantha Marasinghe with Dr Chandana Gamage and Kasun Chathuranga at "Defence in Depth", TechCERT Technical Seminar held in collaboration with Symantec, 09 December 2010
- “Software based Agent Threats” by Athula Samarasinghe, with Pramith De Soysa and Nalinda Herath at "Defence in Depth", TechCERT Technical Seminar held in collaboration with Symantec, 09 December 2010

- "Enterprise E-mail Security at the Egress", Technical presentation by Dr Chandana Gamage with Dileepa Lathsara at the TechCERT Seminar on "Enterprise Applications Security in a Changing Environment" held in collaboration with Palo Alto Networks, 10 March 2010
- "Cryptographic Solutions to Information Security Problems", Technical Presentation by Dr. Chandana Gamage at the North-Western Provincial Centre seminar on "Safe Use of Computers" for the Institution of Engineers Sri Lanka, 18 March 2010
- "Infrastructure Support for a Secure Internet in Sri Lanka", Invited presentation by Dr. Chandana Gamage at 20 Years of Dot LK Conference by LK Domain Registry, 29 June 2010
- "Digital Signatures and its Applications", Technical Demonstration by Harshana Porawagama and Kushan Sharma (TechCERT team specialized in X.509 certificate authority implementation) at the North-Western Provincial Centre seminar on "Safe Use of Computers" for the Institution of Engineers Sri Lanka, 18 March 2010
- A demonstration on wireless based attacks were presented by Janantha Marasinghe, Athula Samarasinghe & Kushan Sharma at Cyber Security Conference 2010 organized by SLCERT, 01 September 2010
- "Digital Certificates and Email Signing", Technical Presentation and Demonstration by Dileepa Lathsara, Harshana Porawagama and Dr Chandana Gamage at the ICTA, Sri Lanka, 2010
- "Digital Certificates and Email Signing", Technical Presentation and Demonstration by Harshana Porawagama at the LK Domain Registry, Engineering Section, 2010
- "Technical issues of Digital Certificates and Digital Signing", Technical Presentation by Harshana Porawagama and Kushan Sharma at the Bar Association of Sri Lanka (BASL) at the invitation of IT and Law Sub Committee, 2010

2.2 Participation in Conferences, Workshops and Training Programmes

- APCERT Conference & AGM, Phuket, Thailand, 2010, participated by Dr. Shantha Fernando and Janantha Marasinghe
- FIRST Annual Conference, 2010, Miami, United States of America, 2010 participated by Dileepa Lathsara

- ISO/IEC 27001 ISMS training by Det Norske Veritas, 2010 participated by Dileepa Lathsara and Kushan Sharma
- CHFI Training, Colombo, Sri Lanka, 2010 participated by Kalana Guniyangoda
- CEH Training, Colombo, Sri Lanka, 2010 participated by Dileepa Lathsara
- Cyber Security 2010, Singapore participated by LtCol Athula Samarasinghe
- Symantec IT Security Seminar in Mumbai, India, Participated by LtCol Athula Samarasinghe
- Cyber Security Week 2010 organized by SLCERT , participated by Janantha Marasinghe, LtCol Athula Samarasinghe and Kushan Sharma

3. Achievements

3.1 Technical Publications

- "Chaos Theory based Cryptography in Digital Image Distribution" by Dr Chandana Gamage and Harshana Ranmuthugala, In Proceedings of the 2010 International Conference on Advances in ICT for Emerging Regions (ICTer), pages 32-39, Colombo, Sri Lanka, September 2010. IEEE Computer Society (ISBN: 978-1-4244-9041-7)
- "Countering Ambiguity Attacks Against Digital Image Watermarking Schemes" by Dr Chandana Gamage and Randima Hettiarachchi, In Proceedings of the 2010 CS&ES Conference (CSES 2010), pages 17-22, Moratuwa, Sri Lanka, September 2010 (ISBN: 978-955-9027-37-9)

3.2 General Articles for Public

- TechCERT provides weekly IT security related articles through its website. In addition to that TechCERT provides critical security updates relevant to Sri Lankan cyber space
- Facebook security tips leaflet produced by Janantha Marasinghe was distributed at InfoTel exhibition in 2010
- News article on first hand experience of a successful expatriate Facebook recovery story performed by TechCERT with the assistance of Facebook

Security Incident Response Team

3.3 Participation in Working Groups

- Janantha Marasinghe contributed to the ccNSO's Incident Response Working Group (IRWG) in its efforts to making incident handling procedures for DNS security
- TechCERT became a member of the Anti-Phishing Working Group (APWG) in 2010.

3.4 Obtaining of Certifications

- ISMS Lead Auditor "Provisional ISMS Auditors" title was obtained by two engineers at TechCERT
- CISSP certification was successfully completed by a TechCERT engineer

4. International Collaboration

- Conducted a workshop on digital forensics by teaming up with Team Cymru
- Conducted the workshop “Defence in depth” with Symantec Corporation
- Established a close working relationship with Facebook Security Incident Response Team to tackle local Facebook related incidents
- Continued the close working relationship with APCERT members when tackling cross border incidents, particularly phishing attacks

5. Future Plans

- TechCERT will be completing the first year of its general membership of APCERT and has already initiated plans to upgrade its membership status to full membership
- TechCERT will be providing X.509 v3 user certificates to the general public of Sri Lanka through LankaCertify for use in securing email communications and in integrity protection of publicly disclosed information
- TechCERT will be providing expert assistance to develop a FIPS 140-3 compliant product certification laboratory for security modules of local software products with testing and certification
- TechCERT will deploy an in-house developed Phishing detection and awareness programmes for public and the corporate sector
- TechCERT intends to expand the TSUBAME sensor nodes in Sri Lanka to better understand traffic patterns and gain expertise in attack prediction

- TechCERT intends to expand the public awareness campaign on information security for school children program it conducts with the collaboration of the Department of Computer Science and Engineering, University of Moratuwa, Sri Lanka
- TechCERT intends to expand the public awareness campaign on information security for engineering professionals program it conducts with the collaboration of the Institution of Engineers, Sri Lanka (IESL)

6. Conclusion

- TechCERT has consistently improved and expanded its capability to respond and assist its constituency in information security incidents and handle emergencies in a timely and professional manner.
- The year 2010 was marked by a significant increase in network probing attacks, web site hacking attacks and phishing attacks. The constituency was particularly impacted by attacks the involved social engineering approaches, social networking sites and use of spam mail.
- TechCERT is confident of its ability and readiness to successfully assist its constituency in computer emergencies. 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.