APCERT 2007 Annual Report

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

CONTENTS

Chair's Message 2007

In 2007, MyCERT was given the privilege to Chair the APCERT and with this trust, we have undertaken our best effort to emulate the achievements performed by the former APCERT Chair, AusCERT. As the current Chair, MyCERT is therefore pleased to report to members and concerned parties of activities and accomplishments made by APCERT throughout this year.

Security incidents are becoming more challenging to resolve which is evident from some of the security incidents that took place in 2007. Botnet propagation, coordinated attack on Root DNS servers, unprecedented attack on a nation (e.g.-Estonia), Stormworm (p2p based bot infrastructure using social engineering techniques to infect users), and the emergence of multiple web-based toolkits for client-based exploitation are some new examples of advanced incidents encountered this year.

Having majority of APCERT members consisting of National CERTs has provided greater opportunity to bring APCERT representation in APECTEL and ASEAN forums. Initiatives of APCERT members in cooperating, collaborating and communicating vital information sharing has transcended in improvement of each teams own economy and constituents in handling security incidents.

In 2007, APCERT members had shown a high level of commitment towards APCERT establishment through initiatives and activities conducted such as organizing the 6th APCERT AGM in Malaysia, coordination of APCERT Drill, members' participation in various events to promote APCERT (e.g. - conferences, forums, seminars, incident handling trainings), strategic collaborative visits, and so on. The commitments shown by APCERT members, has led to another new member joining APCERT, which is Vietnam CERT (VNCERT).

In moving through 2008, global cooperation with international security association such as FIRST, IMPACT, ENISA, TF-CSIRT, APECTEL and EGC, will be significantly enhanced as APCERT is transforming to become a major player in combating computer security threats.

MyCERT together with the Steering Committee members will try our utmost best to shoulder the effort in bringing APCERT to become major security organization trusted internationally.

Husin Jazri
CEO CyberSecurity Malaysia - MyCERT
Chair of APCERT
March 2008

I. About APCERT

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 to encourage and support the activities of CERTs/CSIRTs in the Asia Pacific region.

APCERT aims to:

- Enhance regional and international cooperation on information security in Asia,
- Jointly develop measures to deal with large-scale or regional network security incidents,
- Facilitate technology transfer and sharing of information about security, computer virus and malicious code, among its members,
- Promote collaborative research and development on subjects of interest to its members,
- Assist other CERTs/CSIRTs in the region to improve the efficiency and effectiveness of computer emergency responses,
- Provide inputs and/or recommendations to help address legal issues related to information security and emergency response across regional boundaries, and
- Organize an annual conference to raise awareness on computer security incident response and trends.

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 the 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 team of CSIRTs in Europe www.terena.nl/tech/task-forces/tf-csirt/.

The geographical boundary of APCERT activities are the same as that of APNIC. It comprises 62 economies in the Asia and Pacific region. The list of those economies is available at:
http://www.apnic.net/info/reference/lookup_codes_text.html
http://www.apnic.net/info/brochure/apnicbroc.pdf

At present, APCERT Chair is the Malaysian Computer Emergency Response Team (MyCERT). Deputy Chair is the National Computer network Emergency Response technical Team / Coordination Center of China (CNCERT/CC). Japan Computer Emergency Response Team/Coordination Center (JPCERT/CC) serves as Secretariat.

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

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. This year, Vietnam Computer Emergency Response Team (VNCERT) has been approved as General Member of the APCERT as of 19 April 2007. APCERT now consists of 20 teams from 14 economies across the AP region.

Full Members

Team	Official Team Name	Economy
AusCERT	Australian Computer Emergency Response Team	Australia
BKIS	Bach Khoa Internetwork Security Center	Vietnam
CCERT	CERNET Computer Emergency Response Team	People's Republic of China
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
KrCERTCC	Korea Internet Security Center	Korea
MyCERT	Malaysian Computer Emergency Response Team	Malaysia
PH-CERT	Philippine Computer Emergency Response Team	Philippine
SingCERT	Singapore Computer Emergency Response Team	Singapore
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

General Members

Team	Official Team Name	Economy
BP DSIRT	BP Digital Security Incident Response Team	Singapore
BruCERT	Brunei Computer Emergency Response Team	Negara Brunei Darussalam
CERT-In	Indian Computer Emergency Response Team	India
GCSIRT	Government Computer Security and Incident Response Team	Philippine
NUSCERT	National University of Singapore Computer Emergency Response Team	Singapore
VNCERT	Vietnam Computer Emergency Response Team	Vietnam

Steering Committee (SC)

The following APCERT members currently serve as Steering Committee (SC) for APCERT.
- AusCERT
- CNCERT/CC (Deputy Chair)
- HKCERT/CC
- JPCERT/CC (Secretariat)
- KrCERT/CC
- MyCERT (Chair)
- SingCERT

Working Groups (WG)

The following Working Groups are formed within APCERT.

1. Accreditation Rule WG

Objective: To develop an accreditation scheme for APCERT members
Members: JPCERT/CC (Chair), AusCERT, HKCERT, KrCERT/CC and MyCERT

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

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

II. APCERT Activity Report 2007

1. APCERT Activities & International Relationships/Engagements

APCERT has been active in terms of promoting and representing APCERT in various international government and non-government forums:

APCERT AGM 2007 – Hosted by MyCERT
7-9 February 2007 in Langkawi, Malaysia
http://www.cybersecurity.org.my/apcert/programs.html

The event was held in conjunction with the 6th APCERT AGM & conference which was attended by the APCERT members and invited guest. There were approximately 14 APCERT members and more than 100 participants that attended the two day conference. The event allowed participants to meet, discuss, learn and share issues of similar interest in improving the Internet security within each economies and throughout the Asia-Pacific region. (Report by MyCERT)

FIRST TC by Q-CERT
16 April 2007 in Doha, Qatar
http://www.first.org/events/colloquia/apr2007/

FIRST is an international confederation of trusted computer incident response teams who cooperatively handle computer security incidents and promote incident prevention programs. The Doha TC was held for five days with issues addressed ranging from Identity Theft, Privacy, Standards, Compliance (technical or legal), Cyber Crime and many more. MyCERT had presented on the topic of National & Regional CSIRTs from APCERT perspective and conducted a hands-on workshop for the Technical Colloquium session. (Report by MyCERT)

APEC TEL 35
22-27 April 2007 in Manila, Philippines
http://www.apectel35.org.ph/

The event was conducted with the objective to address the issues of malicious related activities or malwares spreading through computer networks. The APEC-OECD Malware Workshop allowed participants to discuss on ways to respond and find counter measures in handling and engaging with malware attack among the Asia Pacific region. (Report by MyCERT)

ASEAN CERT Incident Drill (ACID) 2007
16 July 2007
Coordinated by SingCERT

The ASEAN CERT Incident Drill (ACID) 2007 was held on 16 July 2007. The drill focused on the topic of handling cross-border incidents pertaining to malware. SingCERT, together with CNCERT, CERT-IN, MyCERT and VNCERT developed several non-malicious applications simulating malware.
(Report by SingCERT)

PacINET 2007
14-22 August 2007 in Solomon Islands
http://www.picisoc.org/tiki-index.php?page=PacInet+2007

AusCERT interacted with Pacific Islanders on CERT capability developments. (Report by AusCERT)

FIRST TC – Hosted by MyCERT, CyberSecurity Malaysia
22-24 August 2007 in Kuala Lumpur, Malaysia
http://www.first.org/events/colloquia/aug2007/

FIRST Technical Colloquia (TC) provides a discussion forum for FIRST member teams to share information effecting the operation of incident response and security teams. The event was held on the 22nd-24th August in Kuala Lumpur where FIRST members as well as invited guest attended the two days plenary session. A FIRST hands-on workshops was also held on 24th August for FIRST members only. In conjunction to the FIRST TC, a Critical National Information Infrastructure (CNII) workshop for local participants was also organized on 21st August. (Report by MyCERT)

AP* Retreat meeting
26 August 2007 in Xi'An, China
http://www.apstar.org/retreat/xian_2007/xian_agenda_2007.htm

On 26 August 2007, CNCERT on behalf of APCERT attended the AP* Retreat meeting held in Xi'An, China, and delivered a presentation titled with "APCERT Activity Updates" at the meeting. CNCERT's representative also answered some questions from attendee, and communicated with them about latest development of APCERT in details. (Report by CNCERT/CC)

ITU Regional Workshop
28-31 August 2007 in Hanoi, Vietnam
http://www.itu.int/ITU-D/cyb/events/2007/hanoi/

Presented on the overview of APCERT. (Report by AusCERT)

APEC TEL 36
22-26 October 2007 in San Diego, Chile
http://www.apectel36.cl/

Presentation and Workshops (Report by CNCERT/CC)

Site visit to IDSIRTII and IDCERT – MyCERT
2-3 October 2007 in Indonesia

The visit to the Indonesian Security Incident Response Team on Information Infrastructure (IDSIRTII) was made to understand the newly established Indonesian security organization. The visit was welcomed by the Chairman of IDSIRTII, Mr Eko Indradjit Wirjonoputro and Vice Chairman, Mr. Muhammaad Salahuddien where a briefing of the organization was provided. MyCERT was also invited to present during ID-SIRTII Seminar regarding Cyber Security on 31 October 2007.
A visit to IDCERT was made to to get updates of their latest operations and activities. The meeting was welcomed by the team's representative Mr. Andika and Mr. Amal at their office in Bandung, Indonesia. (Report by MyCERT)

Organization of American States Conference
6 November 2007 in Miami, USA
http://www.cicte.oas.org/Rev/EN/Events/Cyber_Events/II_Workshop_MIAMI-2007.asp

The overall objectives of this workshop increase awareness of the cyber threat to OAS Member States. MyCERT represented APCERT as Chairman to inform the OAS member state of the latest activities and operation of APCERT. (Report by MyCERT)

APCERT Drill 2007
22 November 2007
http://www.apcert.org/documents/pdf/APCERT-drill-2007.pdf

The APCERT drill was held on 22nd December 2007 with 12 teams participating in the drill. The drill was coordinated by MyCERT and AusCERT while SingCERT assisted in providing an IRC-server for real time coordination. The event main scenario was that of a cyber attack during the upcoming 2008 Beijing Olympics in China. (Report by MyCERT)

Site visit to SLCERT – by MyCERT and JPCERT/CC
4 December 2007, Sri Lanka

The visit was made with JPCERT/CC to further understand the newly established Sri Lanka CERT (SLCERT). SLCERT is a fully owned body supervised by the country's Information Communication Technology Agency. SLCERT had indicated to become a member of APCERT and had submitted their application form and relevant information to MyCERT where it will be processed by the APCERT Steering Committee.
(Report by MyCERT)

Site visit to BDCERT – by MyCERT and JPCERT/CC
6 December 2007, Bangladesh

The visit was made with MyCERT to further understand the newly established Bangladesh CERT (BDCERT). BDCERT is an initiative through voluntarily basis of members of the Internet Service providers Association of Bangladesh (ISPAB). BDCERT had indicated to become a member of APCERT and had submitted their application form and relevant information to JPCERT/CC where it will be processed by the APCERT Steering Committee. (Report by JPCERT/CC)

GOVCERT.NL
18-19 October 2007, Netherlands
http://www.govcertsymposium.com/index.asp

The 6th edition of the GOVCERT.NL symposium was organized to discuss on IT security and mastering our E-identity. MyCERT was invited to share our experience in participating in Cyber drills.
(Report by MyCERT)

AP* Retreat meeting
24 February 2008, Chinese Taipei
http://www.apstar.org/apstar_agenda.php?p_content_category_id=2&p_meeting_id=26

Deputy Director of TWNCERT (Chinese Taipei), Jia-Chyi Wu, had been on behalf of APCERT to speak APCERT activity update at AP* Retreat 2008 on February 24, 2008. The information about Drill 2007 is useful for several participants at the conference. (Report by TWNCERT)

***APEC TEL Security and Prosperity Steering Group (SPSG)**
Jinhyun Cho (KrCERT/CC) serves as Deputy Convenor of the SPSG.

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

Yurie Ito (JPCERT/CC) serves as FIRST Director & SC Member.

2. APCERT SC Meetings

Since the last APCERT AGM in Langkawi, Malaysia, the SC held 7 teleconference meetings to discuss on APCERT operations and activities.

Steering Committee

During 2007 the steering committee comprised the following members:

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

The two-year terms as members of the steering committee for CNCERT/CC, HKCERT, KrCERT/CC and SingCERT expire on 11 March 2008. These teams may nominate for election again. MyCERT's one-year term as Chair and CNCERT/CC's one-year term as Deputy Chair also expire on 11 March 2008, and may nominate for election again.

3. New Team Applications

VNCERT (Vietnam) was approved to join as General Member of APCERT as of 19 April 2007.

4. APCERT Website

JPCERT/CC manages and updates the apcert.org website. On a temporary basis, AusCERT hosts the POC contact details for each of the APCERT POCs. Access is by password only for APCERT teams. URL is: https://www.auscert.org.au/5642

III. Activity Reports from APCERT Members

The followings are the reports from APCERT members, which include their activity updates, incident response statistics, analysis, and trends as well as their future plans.

A. AusCERT Activity Report 2007

Australian Computer Emergency Response Team – Australia

The following information contains information about AusCERT's activities during 2007.

1. ABOUT AusCERT

1.1 Introduction

As the national CERT and a self-funded not-for-profit entity, AusCERT serves Australia's national interest by improving Internet security for Australian Internet users.
AusCERT does this by:

- collecting, analysing and providing advice about computer network threats and vulnerabilities;
- helping to mitigate Internet attacks directed at Australian Internet users and networks;
- and providing education and advice about issues affecting Internet security in Australia and globally.

AusCERT is the primary point of contact for handling incidents sourced from Australian networks or to provide information about threats and vulnerabilities that could affect Australian Internet users.
Increasingly, AusCERT has used its unique operational vantage monitoring, analysing and mitigating cyber attacks to advocate best practice in Internet security.

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, so too did AusCERT's focus change from being university centric to include the interests of all sectors.

AusCERT is an independent, non-government, self-funded not-for-profit team of IT security professionals, based at the University of Queensland. The University of Queensland is one of Australia's premier learning and research institutions.

AusCERT is recognised as the national CERT by the Australian government.

1.3 Workforce power

AusCERT employs 17 staff. Eight Coordination-Centre staff provide incident handling and security bulletins services to AusCERT members. Staff are on call on a 24 hour basis to help assist with emergency computer security incidents for members outside of core hours. Coordination Centre staff also monitor and initiate action to mitigate malware attacks, inter alia, directed at Australian Internet users in general as part of its national CERT role.

There are three managers who cover the Australian Access Federation project, Analysis and Assessments, and Training and Education. One team member provides infrastructure support; two cover administrative support for day to day operations. Daily business planning is covered by the Operations Manager and the General Manager. All managers contribute to the strategic direction of AusCERT.

1.4 Constituency

As the national CERT, AusCERT's constituents are Australian Internet users. As a self-funded entity that relies on revenue from its subscribers, member organisations remain AusCERT's highest priority. However, many of its activities done in support of its national CERT role provides general benefits to its membership by helping to contribute to increased level of security for Australia.

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).

2. ACTIVITIES AND OPERATIONS

AusCERT:

- provides incident response to help organisations mitigate Internet based attacks against their networks;
- mitigates online attacks that have compromised personal identity information (PII) by notifying the public and private sector organisations whose customers or clients have been affected;
- publishes security bulletins,[1] which are available from the AusCERT web site (including security bulletins about specific cyber threats affecting Australian networks and Internet users);
- publishes papers, policy submissions to government (relating to ICT and Internet security) and computer security and cyber crime surveys;[2]
- provides public outreach, education and awareness raising about Internet security issues including via the media;

---

[1] See AusCERT security bulletins: https://www.auscert.org.au/1
AusCERT restricts public access to a small selection of security bulletins and papers in order to retain member value. AusCERT relies on membership subscriptions to cover its operating costs – in the delivery of member services and national CERT functions.

[2] See AusCERT publications http://www.auscert.org.au/1920

- provides information and expertise to law enforcement about specific cyber attacks affecting or emanating from Australian networks;
- participates in government, CERT and industry multi-lateral meetings including actively participates in cyber security exercises with a range of global partners;
- communicates, cooperates and builds relationships with industry, domain name registries, telecommunication providers and AusCERT's many national CERT counterparts overseas which AusCERT relies upon to help provide assistance to Australian Internet users being attacked from sources in overseas constituencies.

2.1 Incident Handling

A large part of AusCERT's core business involves analysis of online cyber attacks. While these are not the only incidents handled by AusCERT, they represent a common form of cyber attack and show clear upward trends associated with these set of criminally-motivated activities.

Figure 1 shows the number of malware and phishing sites handled by AusCERT in 2007. The temporary drop in phishing attacks is due to a change in the reporting and handling arrangements that were previously in place, and are not a reflection of reduced activity of this nature. The peaks in malware activity are attributed to increased levels of storm botnet activity.

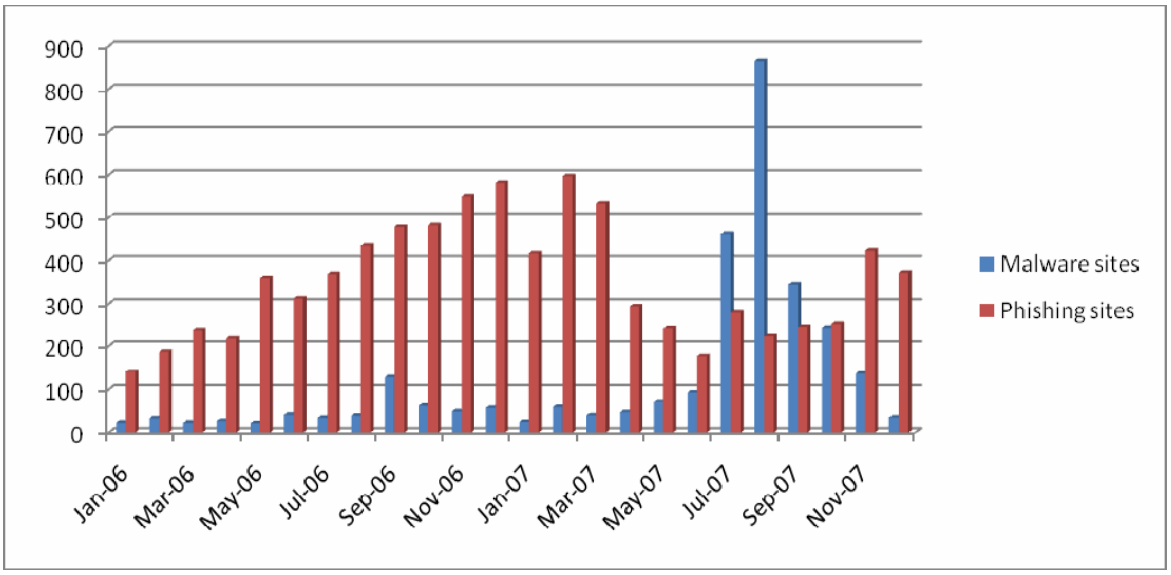


Figure 1

2.2 Security bulletins and blogs

AusCERT publishes security bulletins as part of its services. Security bulletins can be divided into four categories: Updates, Alerts, Advisories, and External Security Bulletins. Updates provide additional information or corrections to an existing Security Bulletin. They are a mechanism for quick release of important information in a less structured way. Alerts contain information about computer or network threats and vulnerabilities of a serious and urgent nature. Alerts may draw upon material already published by third parties. Advisories provide more detailed information about specific threats or vulnerabilities researched by AusCERT. External Security Bulletins are published by other computer security incident response teams, vendors that AusCERT redistributes or references (with permission).

During 2007, AusCERT published 1058 external security bulletins (ESB), 129 advisories, 132 alerts, and 28 updates and 39 blog items.

2.3 Network monitoring

AusCERT is collaborating with a number of partners operating monitoring projects, by hosting sensors. Data from these projects is returned to AusCERT for analysis.

2.4 Certification

AusCERT, in partnership with EWA Australia and the University of Queensland continues to support a community of IT practitioners with applicants from around the globe signing-up for certifications.

The International Systems Security Professional Certification Scheme (ISSPCS) is a global and open certification scheme for information and systems security professionals that address the shortfalls of traditional IT security certifications by founding the scheme on essential principles of security. The *International Systems Security Engineering Association* (ISSEA) is overseeing the development of the certification. See: www.isspcs.org/

2.5 New Services

Australian Access Federation

The Australian Access Federation (AAF) Project is implementing and deploying the infrastructure to facilitate trusted electronic communications and collaboration within and between higher education and research institutions both locally and internationally as well as with other organizations, in line with the NCRIS objective of providing researchers with access to an environment necessary to support world-class research.

The AAF project has three main components: the development of overarching governance and policies for the whole Federation, the development of specific policies, technical implementation and rollout of PKI for the Federation; and the development of specific policies, technical implementation and rollout of Shibboleth for the Federation. AusCERT is responsible for deploying the first two components of this project.

AusCERT's ability to include its Root Certificate into major vendor's browsers coupled with the deployment of a Public Key Infrastructure for the AAF will help reduce the barriers to increased use of PKI in the Higher Education and Research through:

- Provision of SSL server certificates, reducing overheads and the need to use self-signed certificates
- Provision of hosted Certificate Authority services enabling secure, low overhead issuing of end user certificates for our institution e.g. for access to sensitive/expensive resources and secure email .
- Quality validation services that we do not have to manage e.g. correctly implemented OCSP support

Further information about the AAF is available at www.aaf.edu.au.

AusCERT Blog

On 20 July 2008, AusCERT began a web log for members. The web log provides items of interest to members that may contain incomplete or uncorroborated information about security issues not suitable for publication in other formats but are worthy of timely release. Blog subjects have included follow ups on current malware activities, details of AusCERT participation in various forums, and the odd story of unusual happenings.

3. EVENTS ORGANISED / CO-ORGANISED

3.1 Training

AusCERT has worked closely with the CAUDIT to provide "hands on" workshops for Australian Universities throughout 2007. Web Infrastructure Security on Unix workshops were held in Brisbane, Canberra, Sydney, Melbourne, Adelaide, and Perth. The workshops were also provided to Universities in Auckland and Dunedin, New Zealand.

The workshops were also made open to the public during July and November 2007. These were well patronised by AusCERT members.

3.2 Drills

On 22 November 2007, APCERT ran its annual security exercise based on a scenario of cyber attacks aimed at disrupting the upcoming Beijing 2008 Olympic Games. As one of the organisers of the drill, AusCERT developed a list of objectives for the drill based on advice from APCERT teams, developed the Rules of Engagement, the scenario and played 'exercise control' on the day. Other parts of AusCERT participated in the drill exercise as responders.

3.3 Seminars

AusCERT held its annual Asia-Pacific Information Security Conference at the Gold Coast Australia in May 2007 with over 1,000 delegates. The conference continues to show itself to be the premier information security conference in Australia and the southern hemisphere conducted by information security professionals for information security professionals, IT managers and government decision makers in the field. See: http://conference.auscert.org.au/conf2007

Coinciding with the annual AusCERT conference, AusCERT also hosts an invitation only online crime symposium for key stakeholders and organisations that are most likely to be affected by this crime or are in a position to assist deal with the crimes. The purpose of the symposium is to bring speakers with particular insight into the problems to share their knowledge and experience with those who have the ability to help address the problems. Due to the potentially sensitive nature of the discussions, attendance is restricted.

Computer Security Day is an international event to raise awareness of computer security issues. To mark Computer Security Day in 2007, AusCERT organised a non-profit event in Brisbane.

In 2007, AusCERT participated in an APISC Security training course in Seoul, Korea, supported by Ministry of Information and Communication and KrCERT/CC. The course was well attended, with attendees from many countries.

AusCERT prepared consumer security advice and participated in the Australian government's scam watch week, coordinated by the Australian Competition and Consumer Commission.

4. ACHIEVEMENTS

4.1 Presentations

AusCERT has given presentations at several conferences throughout 2007 including keynote addresses and tutorials. These include presentations at International Telecommunication Union (ITU) Regional Workshop on Cybersecurity in Hanoi, London Action Plan Group, ISOC PacINET Conference in Solomon Islands, Oganisation for

Economic Co-operation and Development (OECD), and several workshops within Australia including local governments to name a few.

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 Publications

AusCERT made substantial contributions of content to and provided technical security advice on the OECD's paper on malware. The paper seeks to better inform OECD member countries about the effective use of malware by criminals, the challenges it poses in terms of prevention and response and seek to identify national and international strategies to help combat malware and botnets. The paper is awaiting public release.

During 2007, AusCERT produced papers on a DDoS attack directed at AusCERT, a security check list for Unix and Linux system administrators, and made submissions to public or government enquiries including on:

- Review of domain names policies to auDA
- Review of the Electronic Funds Transfer (EFT) Code of Conduct to ASIC
- Review of the Privacy Act to the Australian Law Reform Commission[3]

5. INTERNATIONAL COLLABORATION

5.1 Collaboration

AusCERT continues to be actively involved with APCERT, serving on the Steering Committee again during 2007. AusCERT also manages the APCERT mailing lists, and restricted web access to the APCERT Point of Contacts.

Other collaborations include the UK Association of Payments and Clearing Services (APACS), FIRST, Digital Phishnet, Anti Phishing Working Group, European Government CERTs and many open and closed information security groups.

6. FUTURE PLANS

6.1 Future Projects

AusCERT has a number of plans for projects in progress. Details will unfold when they are closer to implementation.

[3] All are publicly available from the AusCERT web site.

B. BKIS Activity Report 2007

Bach Khoa Internetwork Security Center – Vietnam

1.0 About Bkis - Vietnam

Bkis - Bach Khoa Internetwork Security Center is a Vietnam's leading Center in researching, deploying network security software and solution.

We have 5 technical departments: Antivirus, Application Security, Infrastructure Security, Security Devices, Software.

Bkis established on December 28th, 2001, and became full members of APCERT in 2002.

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

2.0 Activities & Operations

Security Statistic

Computer Virus 2007 (in Vietnam)	Quantity
Number of computers infected viruses	33,646,000
Number of new viruses appear in 2007	6,752
Number of new viruses per day	18,49 new virus / day
The most infected virus: **W32.Winib.Worm**	Infect 511,000 computers
Security 2007 (in Vietnam)	**Quantity**
Observed by Bkis:	
Number of websites hacked by Vietnamese hackers	118
Number of websites hacked by International hackers	224
Summary	**342**
Vulnerability Report:	
Number of important websites Bkis reports vulnerability	**140**

Top 15 viruses in 2007 in Vietnam

No	Virus	Pecentage
1	W32.Winib.Worm	1,51 %
2	W32.Ukuran.Worm	1,10 %
3	W32.SCkeylogA.Trojan	1,00 %
4	W32.Flashy.Trojan	0,88 %
5	W32.PerlovegaA.Worm	0,81 %
6	W32.USBNotify.Worm	0,68 %
7	W32.RavMonE.Worm	0,63 %
8	W32.TufikB.PE	0,60 %
9	W32.NotifyB.Worm	0,59 %
10	W32.CTFMonF.Trojan	0,56 %
11	W32.Dragon.Worm	0,56 %
12	W32.QQRobD.Trojan	0,54 %
13	W32.Hider.Trojan	0,51 %
14	W32.SandboxA.Adware	0,50 %
15	W32.OnlineGamesL.Worm	0,48 %

Security Training

Company	Quatity
Viettel Corporation, the largest Internet and communication provider in Vietnam.	40 leading engineers and managers
State Tresory	40 leading engineers and managers and 200 employees

Publishing

Objects	Quatity
Security News	12 for 12 months in 2007
Security Articles	50 for magazines
Security Advisory	40

C. CNCERT/CC Activity Report 2007

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

1.0 About CNCERT/CC

1.1 Introduction

CNCERT/CC is a functional organization under Internet Emergency Response Coordination Office of Ministry of Information Industry of China, who is responsible for the coordination of activities among all Computer Emergency Response Teams within China concerning incidents in national public networks.

1.1.1. Establishment

CNCERT/CC was founded in Oct., 2000, and became a member of FIRST (Forum of Incident Response and Security Teams) in Aug., 2002. CNCERT/CC took an active part in the establishment of APCERT as a member of the Steering Committee of APCERT.

1.1.2. Workforce power

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

1.1.3. Constituency & Etc

CNCERT/CC 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.

CNCERT/CC's activities are:

Information Collecting	collect various timely information on security events via various communication ways and cooperative system
Event Monitoring	detect various highly severe security problems and events in time, and deliver precaution and support for the related organizations.
Incident Handling	leverage domestic CERTs to handle various public network security incidents, and act as a premier window to accept and handle incident reports from homeland and world.
Data Analyzing	conduct comprehensive analysis with the data of security events, and produce trusted reports.
Resource Building	collect and maintain various basic information resources, including vulnerabilities, patches, defending tools and latest network security technologies for supporting purpose.
Security Research	research on various security issues and technologies as the basic work for security defense and emergency response.
Security Training	provide training courses on emergency response and handling technologies and the construction of CERT.
Technical Consulting	offer various technical consulting services on security incident handling.

International Exchanging organize domestic CERTs to conduct international cooperation and exchange.

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

2.0 Activities & Operations

2.1. Incident Reports

In 2007, CNCERT/CC received 4,390 incidents reports (excluding scanning attacks) from domestic and international users and agencies.

Most incident reports were about phishing (1,326), spam mail (1,197) and webpage embedded malicious code (1,151). The reports of these 3 types of incident were increased by 136%, 104% and 260% compared with that of last year respectively.

2.2. Incident Handling

In 2007, CNCERT/CC handled 1,057 incidents, including webpage defacement, phishing, webpage embedded malicious code, DoS and malware.

2.3. Abuse Statistics

Traffic Monitoring and Analysis
According to CNCERT/CC's data of Internet traffic sample monitoring, the top 4 applications of TCP traffic are http, P2P, email and instant messenger.

TCP Port	Rank	Percentage	Applications
80	1	29.39%	Http
4662	2	1.11%	eMule
25	3	0.66%	SMTP
443	4	0.56%	Https
8080	5	0.39%	Http
3077	6	0.35%	Xunlei (downloader)
8000	7	0.27%	QQ
1863	8	0.13%	MSN Messenger
6881	9	0.13%	BitTorrent
19101	10	0.10%	clubbox

Table 1 TCP Traffic Top 10 in 2007

The top 3 applications of UDP traffic are Xunlei, MS Messenger and Http.

UDP Port	Rank	Percentage	Applications
15000	1	2.80%	Xunlei (downloader)
1026	2	2.76%	MS Messenger
1027	3	2.40%	MS Messenger
80	4	1.70%	Http
53	5	1.30%	DNS
53124	6	0.95%	Unknown
3076	7	0.79%	Xunlei (downloader)
8000	8	0.75%	QQ
4672	9	0.65%	eMule
1434	10	0.64%	MSSQL

Table 2 UDP Traffic Top 10 in Year 2007

Trojan & Botnet Monitoring

In 2007, CNCERT/CC monitored some popular Trojans and discovered 995,154 IP addresses of computers embedded with Trojans in Chinese mainland, which was increased by 2125% compared with that of year 2006.

CNCERT/CC also kept on monitoring Botnet activities for a long time. In 2007, CNCERT/CC discovered over 3,624,665 IP addresses of computers embedded with Botnet clients in Chinese mainland. Meanwhile, 10,399 Botnet servers outside of Chinese mainland were discovered controlling Botnet clients in Chinese mainland. Among these Botnet servers, about 32% were in the United States, 13% in Chinese Taipei and 7% in South Korea.

Among ports used by Botnet based on IRC application, the top 3 ports are 6667 (40.1%), 1863 (5.2%) and 7000 (2.94%).

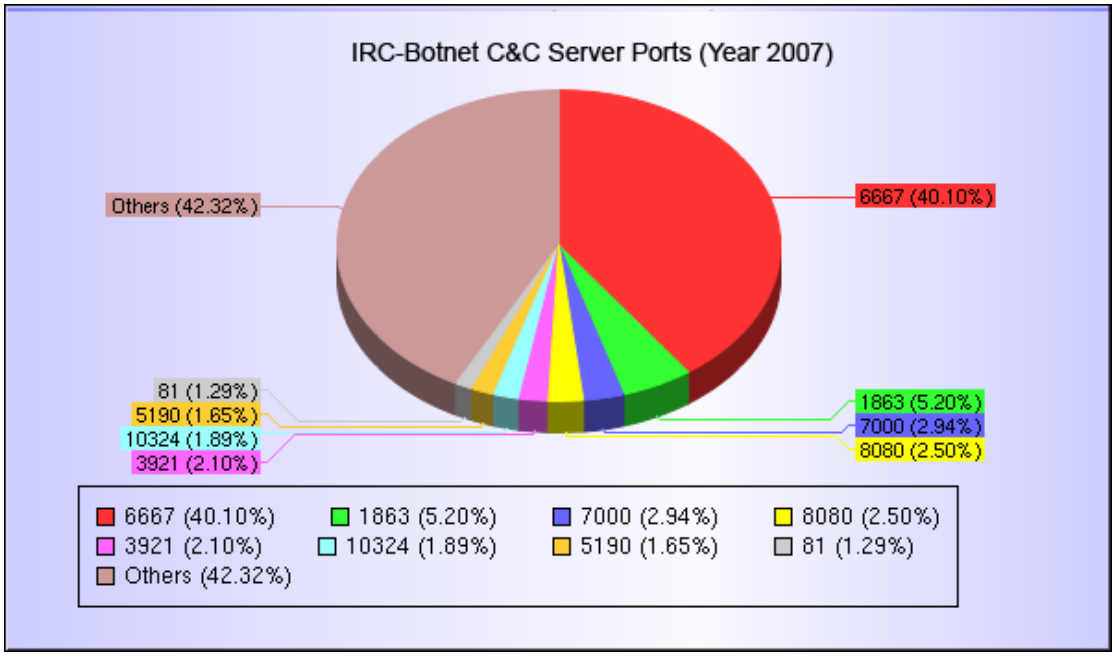


Figure 1 IRC-Botnet C&C Server Ports (Year 2007)

In general, the size of Botnets is going to become smaller, localized and specialized. The Botnet with less than 1 thousand Botnet clients is much more favorable to attackers.

Web Defacement Monitoring

In 2007, CNCERT/CC discovered totally 61,228 defaced websites in Chinese mainland, significantly increasing. According to monitoring data, the governmental websites seem to be much easier to be attacked due to their weak protection measures and maintenance.

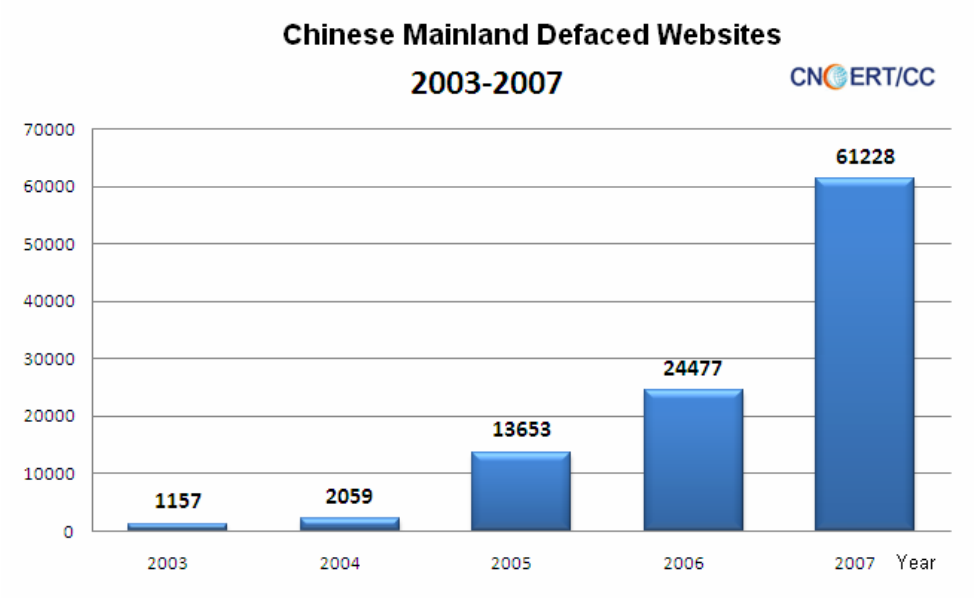


Figure 2 Chinese Mainland Defaced Websites Y2003-2007

Phishing Handling

In 2007, CNCERT/CC received 1,326 phishing reports and resolved 394 successfully. All of these phishing incidents were handled on the request of international CERTs or security organizations. The phishing sites are mostly famous international banking & finance systems.

Phishing Reporters	Number
VeriSign	259
eBay	255
RSA Cyota	128
Castlecops	143
Mark Mornitor	74

Table 3 Top 5 Phishing Reporters to CNCERT/CC in Year 2007

Malicious Code Capturing & Analysis

In order to enhance the capability of monitoring malicious code on Internet, CNCERT/CC started up its distributed honeynet project in 2006. The average times of sample capturing everyday reached 3,408 in 2007.

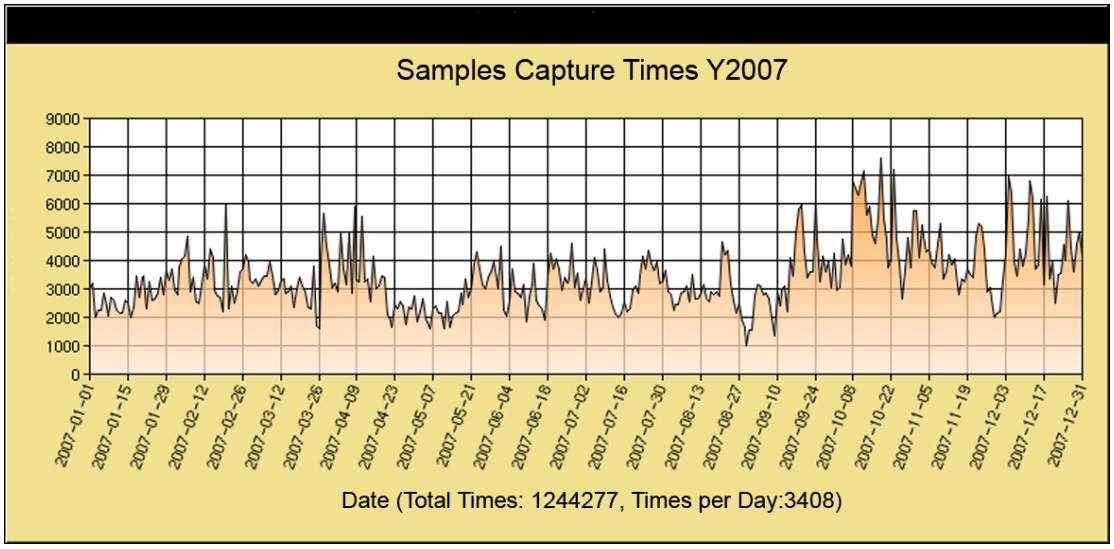


Figure 3 Samples Capturing Times Status

According to the data, the average number of new samples captured everyday is 496. That means new malicious codes were emerging endlessly.

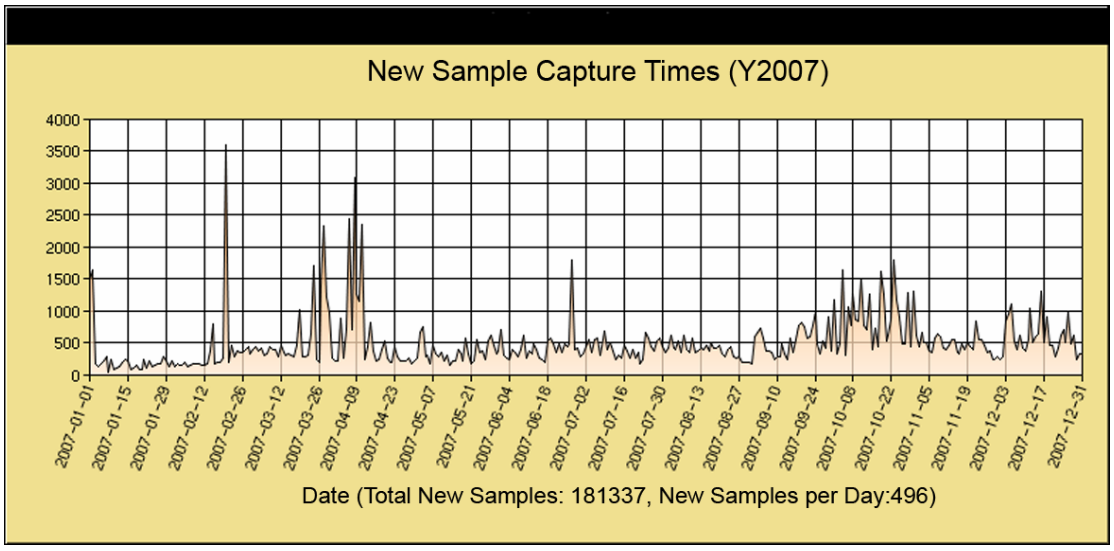


Figure 4 Number of Samples Captured Status

In 2007, 181,337 samples had been captured by CNCERT/CC's honeynet.

Rank	Malicious Code Name	Times of being Captured
1	Backdoor.Win32.VanBot.ax	82852
2	Net-Worm.Win32.Allaple.b	79196
3	Backdoor.Win32.PoeBot.c	69636
4	Net-Worm.Win32.Allaple.e	33712
5	Virus.Win32.Virut.b	33485
6	Backdoor.Win32.SdBot.aad	23998
7	Virus.Win32.Virut.a	21084
8	Backdoor.Win32.Rbot.bni	19348
9	Backdoor.Win32.Rbot.gen	18017
10	Backdoor.Win32.SdBot.xd	16891

Table 4 Top 10 Samples Captured by CNCERT/CC's honeynet

2.4. Security Information Services

CNCERT/CC's users of its security information services are ISPs, cooperative key infrastructures, and relevant government agencies as well. In 2007, 162 internal warnings and 5 critical vulnerability advisories had been delivered in time.

359 articles were published on CNCERT/CC's website, including security bulletins, vulnerability advisories, malware warnings, technical reports, security guide, and etc.

3.0. Events organized/co-organized

DDoS Seminar
The Seminar was held on 1st January, 2007 in Beijing. Delegates came from governments, security research organizations, enterprises and end users. The topics are the damage and prevention of DDoS attacks as well as how to mitigate its impact by technical and management means.

CNCERT/CC 2007 Annual Conference
The Conference was held in Wuxi from April 5 to 7, 2007. About 200 delegates attended the conference.

Computer Malicious Programs Handling Law Circumstance Seminar
The Seminar on law circumstance for handling computer malicious programs was held on 28 August, 2007, in Beijing.

Domain Name Abuse Handling Mechanism Seminar
The seminar on mechanism of handling network attack via domain name abuse was held on 12 September, 2007, in Beijing. It's sponsored by MII.

4.0. Achievement

4.1. Presentation and Publication

Introduction of Malware Issues, APEC-OECD Malware Workshop in APEC-TEL 35, 2007.4.22, Manila

National Network Security Capacity Building, ITU Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection, 2007.8, Hanoi

CERT/CSIRT's Role in Ensuring Olympic Cybersecurity, Information Security Summit 2007, 2007.12, Hong Kong

What Can National CERTs Contribute on Botnet Countermeasures, 2nd National CERT Meeting, 2007.6, Madrid

New Solution on New Threat: Learning from Botnet Incident Handling, MCMC 2nd Industry Talk, 2007.2, Malaysia

CNCERT/CC Annual Report 2006, APCERT 2007 Conference, 2007.2.7-9, Malaysia

Further Information Sharing on Botnet, APCERT 2007 Conference, 2007.2.7-9, Malaysia

Distributed Honeynet & Info Sharing on Malicious Server, CJK InfoSec WG 2007 meeting, 2007.5, Beijing.

12 monthly newsletters, 1 semiyearly special (in Chinese) were issued for high-end users in 2007.

4.2. Criteria

CNCERT/CC published "Incident Object Description and Exchange Format Criteria" (Chinese-edition).

5.0. International Cooperation

5.1. MoU

On June 14, 2007, CNCERT/CC signed Security Cooperation Protocol (SCP) with Microsoft China Corporation in Beijing.

5.2. Conference and Events

APCERT 2007 Annual Conference
CNCERT/CC delegation attended APCERT annual conference in Malaysia and was elected as the deputy chair of APCERT again.

4 CERTs Site Visit
During July 10-22, 2007, CNCERT/CC delegation visited VNCERT, LaoCERT, mmCERT and CamCERT successively.

ACID II 2007
CNCERT/CC participated in ACID II on 16th, July 2007.

APCERT Drill 2007
CNCERT/CC participated in the 4th APCERT incident handling drill on 21st, November 2007. CNCERT/CC appreciated that the Drill's scenario had been designed with Beijing 2008 Olympic Games as the background.

6.0 Future Plans

In 2008, Internet security during Beijing 2008 Olympic Games is the top priority to CNCERT/CC,

who will play an important role then. Therefore, CNCERT/CC expects to keep a stronger collaboration with APCERT members.

7.0 Conclusion

In 2007, the overall security status of Internet in China mainland was relatively calm in general. There was no large-scale network security incident happened with mass damage. With the Beijing 2008 Olympic Games upcoming, potential security risks and threats is increasing greatly. The possibility of large-scale network security incidents occurring cannot be neglected at the moment. Thus, it is necessary for government, ISPs, internet users, and so on, to pay much more attention and cooperate with each other more effectively. CNCERT/CC is also in need of the collaboration with CERTs community from all over the world to prevent and mitigate the impact of any cyber threat compromising Beijing 2008 Olympic Games.

D. HKCERT/CC Activity Report 2007

Hong Kong Computer Emergency Response Team/Coordination Center – Hong Kong, China

Activities in 2007

(a) Incident Report Statistics

In 2007, HKCERT received 1,797 incident reports, including 516 virus incident reports and 1,271 security reports (See Figure 1). Security incident reports continue to overtake virus incident reports.

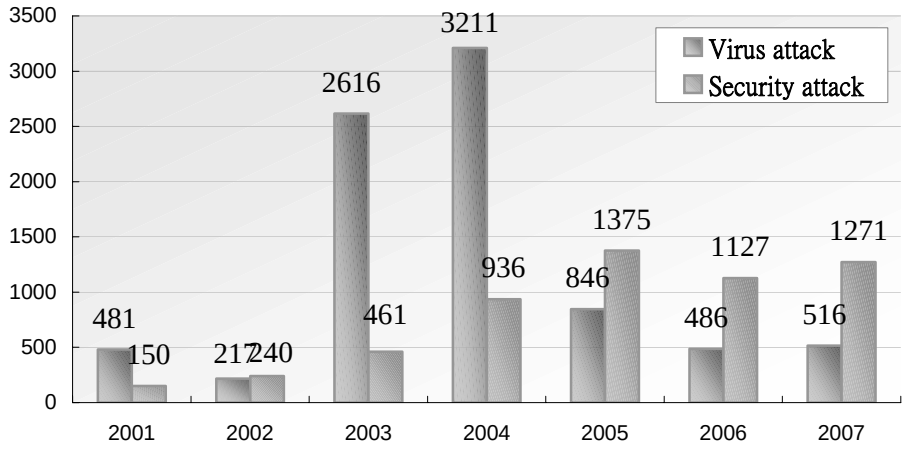


Figure 1. HKCERT incident report statistics 2001 - 2007

(b) Analysis of Composition of security alerts

Further analysis of the partitioning of security incident indicates that the number of phishing reports accounted for nearly 60% of all security incident reports. (See Table.1)

	2004	2005	2006	2007
Number of security incidents reported				
Hacking & Intrusion	783	206	416	416
Phishing	73	211	434	745
Spamming	80	82	47	32
Spyware		876	230	78
Total	936	1,375	1,127	1,271
Number of Computer Virus Incidents Reported	3,211	846	468	516
Virus Alerts Published	25	8	0	1
Security Alerts Published	100	108	178	241

Table 1. Distribution of security incident reports in 2007

(c) Activities Accomplished

In 2007, HKCERT had:

- published 1 virus alerts and 241 security alerts on our web site;
- published 12 issues of newsletter and sent out the alert summary two times each month;
- published the 3rd edition of Information Security Guide for Small and Medium Enterprise, in both English & Chinese;
- continued to work closely with the government and law enforcement agency, and held meetings to exchange information and to organize joint events regularly;
- participated in the government committees, including OFTA Wi-Fi Security Working Group, Information Infrastructure Liaison Group and Information Security Task Force;
- given advice on the Hong Kong Olympics 2008 and Equestrian 2007 web site security;
- worked closely with Hong Kong Police in pinning down phishing web sites;
- assisted HKDNR in identifying and shutting down malicious phishing websites;
- organized the Hong Kong Clean PC Day 2007 seminars in cooperation with government and police;
- served as a steering committee member of the Asia Pacific Computer Emergency Response Team (APCERT)
- participated in the APCERT annual drill in November 2007
- organized the Information Security Summit 2007 with other organizations and associations in December 2007

(d) Activities Planned

- Will host the APCERT Conference and AGM in March 2008

E. JPCERT/CC Activity Report 2007

Japan Computer Emergency Response Team/Coordination Center – Japan

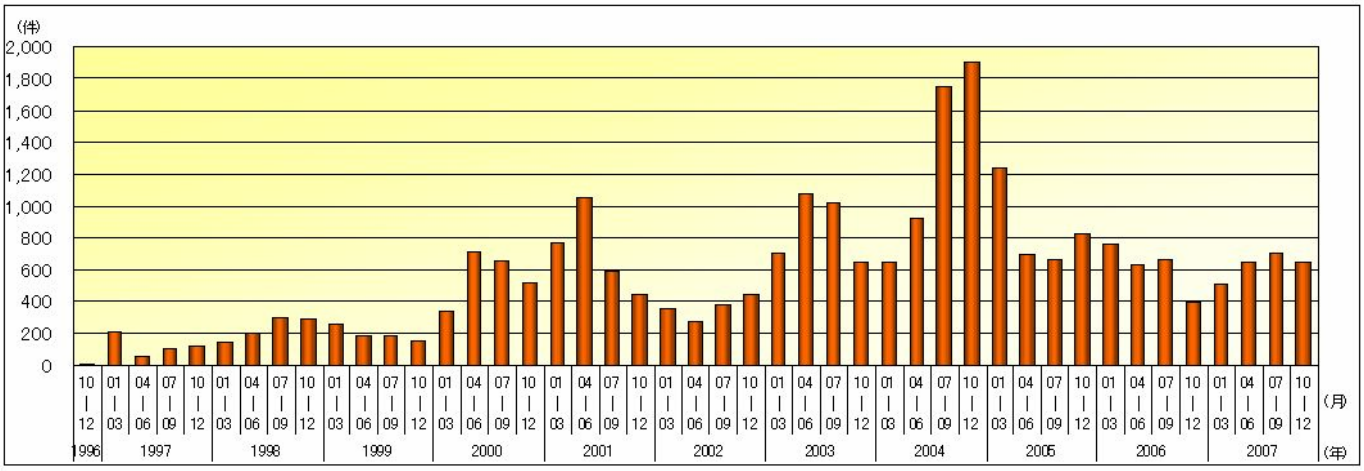
JPCERT/CC is the first CSIRT (Computer Emergency Response Team) established in Japan. It is an independent non-profit organization, acting as a national point of contact for the CSIRTs in Japan and worldwide. Since its inception in 1992, the center has been gathering computer incident and vulnerability information, issuing security alerts and advisories, providing incident responses, engaging research and development, and organizing forums and seminars to raise awareness of security issues.

Incident Statistics and Trends

In 2007, JPCERT/CC issued 2,513 tickets responding to computer security incident reports received from Japan and overseas. A ticket number is assigned to each incident report to keep track of the development. Among the 2,513 tickets, 1,611 tickets were related to probe, scan, and attempts that did not result in serious damages.

	1st Qtr	2nd Qtr	3rd Qtr	4th Qtr	Total
Tickets Issued	505	652	706	650	**2,513**

The incident reports that JPCERT/CC received since 1996:



*Our survey indicated that the sudden decrease in 2002 was caused by tightened security policy in many organizations. Consequently, reporting to external organizations like JPCERT/CC became difficult to do.
Also, most of security experts were too busy handling worms and other serious incidents to write a report during that year.

Source of Incident Reports

As the table below shows, JPCERT/CC received incident reports primarily from .jp, .com, and .org.

ISO Code	1st Qtr	2nd Qtr	3rd Qtr	4th Qtr	Total
.jp	184	186	263	193	826
.com	204	186	160	174	724
.org	0	158	114	0	272

Education and Training

We offer seminars, workshops, and internships targeting system administrators, network managers, and technical staffs who are interested in learning computer security. Some of the events organized or co-organized by JPCERT/CC in 2007 are listed below:

- Critical Information Infrastructure Protection Security Seminar (14 February 2007)
  A one day seminar co-organized by JPCERT/CC, Information-Technology Promotion Agency (IPA), Telecom Information Sharing and Analysis Center Japan (Telecom-ISAC Japan)

- CSIRT Training (12-16 March 2007)
  Incident Handling Workshop for Cambodia, Laos and Myanmar

- JPNIC, JPCERT/CC Security Seminar 2007 (13 March 2007)
  A one day seminar co-organized by JPCERT/CC and Japan Network Information Center (JPNIC)

- Security Day 2007 (18 December 2007)
  A one day seminar co-organized by JPCERT/CC, Japan Internet Providers Association (JAIPA), Telecom Information Sharing and Analysis Center Japan (Telecom-ISAC Japan), Japan Network Security Association (JNSA), Japan Certification Authority Forum (JCAF)

Projects

1. Internet Scan Acquisition System (ISDAS) Project

Internet Scan Data Acquisition System is similar to weather stations for monitoring barometric pressure, temperature, and humidity. Instead of monitoring weather, the system monitors Internet traffics. The project began in November 2003 with the objective of improving Internet security by providing up-to-date graphs and reports gathered by ISDAS.
http://www.jpcert.or.jp/isdas/index-en.html

2. JPCERT/CC Vendor Status Notes (JVN) Project

The project was initiated in 2001 with the objective to gather the vulnerability information about the

domestic products and to provide the information in Japanese on the Internet. The JVN website therefore lists a type of vulnerability, affected hardware or software, possible damage, technical tips, vendor information, and reference documents. This began as a joint project with JPCERT/CC and Keio University. The project team works closely with domestic vendors, including software/hardware/OS/router vendors, as well as network service providers. And now, JPCERT/CC and Information-technology Promotion Agency, Japan, The Information-technology Security Center (IPA/ISEC) operate this project.

http://jvn.jp/

In 2005, the vulnerability information published on JVN has also been distributed through RSS. RSS provides a brief summary, therefore enables people to obtain the latest information without accessing to JVN.

As JVN provides information from multiple vendors, JPCERT/CC has developed a vendor portal site that gathers there information using the web system. Currently, the system is used only to input information however JPCERT/CC plans to expand its service in the future.

Also, the following vulnerability information has been published on JVN in 2007.
-For vulnerability information reported within Japan, 107 cases were published.
-For information provided by CERT/CC, 42 Technical Alerts and 56 Vul Notes were translated and published.
-For information provided by NISCC, 2 cases were translated and published.

Activity Highlights

APCERT Secretariat

JPCERT/CC is supporting the security community in the Asia Pacific region by serving as the Secretariat for APCERT. Our contribution also includes financial support for holding its Annual General Meeting since 2001.

FIRST Related Activities

- The organization maintains a replica server for Forum of Incident Response and Security Teams (FIRST) in Japan. Yurie Ito, JPCERT/CC, also serves as Director and Steering Committee member of the FIRST organization since 2005.
http://www.first.org/

Incident Object Description and Exchange Format (IODEF)

IODEF is a standard XML data format for exchanging operational and statistical incident information among CSIRTs and other collaborators. JPCERT/CC presented an implementation model and the use of the information collected by IODEF at INCH Working Group meeting.

Security Industry Forum

Six years ago, JPCERT/CC created a forum called the SECOND, with objectives to build a trusted network among the major players in the industry and to coordinate in time of an emergency. The participants are the security experts from the major ISPs and vendors and meet regularly to exchange information. JPCERT/CC also provides a mailing list for the SECOND.

URL : http://www.jpcert.or.jp/
Email: info@jpcert.or.jp
Phone: +81 3 3518 4600
Fax: +81 3 3518 4602

F. KrCERT/CC Activity Report 2007

Korea Internet Security Center – Korea

1. Introduction on KrCERT/CC

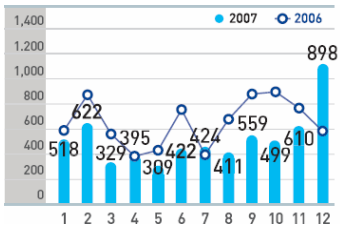
KrCERT/CC, also known as KISC, Korea Internet Security Center, serves as the nationwide coordination center in Korea, and is responsible for detecting, analyzing and responding all nationwide Internet incidents such as hacking, worm/virus, bot, phishing, and all other various Internet attacks. To mitigate the damage from those incidents occurred and to ensure more secure Internet environment, KrCERT/CC is seamlessly operating on 24/7 basis.

2. Latest Activities

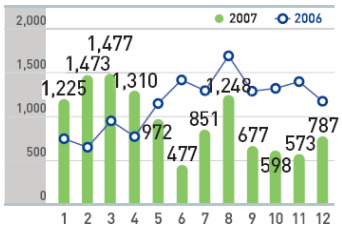
Overview

Internet incident reports[4] received by the KrCERT/CC are categorized into malicious code, hacking incident, and bot. Hacking incident has sub categories; spam relay, phishing[5], intrusion attempt, webpage defacement, and other. The number of malicious code reported to KrCERT/CC in 2007 is 5,996, which is 23% decrease compared with that of the last year (7,789 in 2006). The number of hacking incident reported to KrCERT/CC in 2007 is 21,732, which has 19% decrease compared with that of the last year (26,808 in 2006).

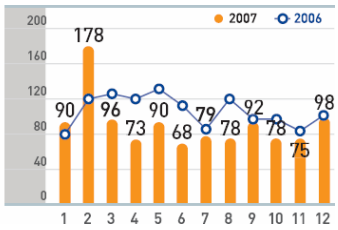
Worm/Virus



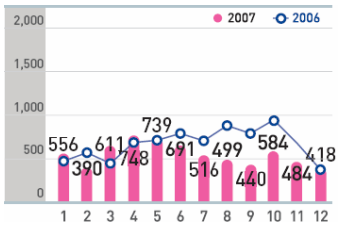
Spam Relay



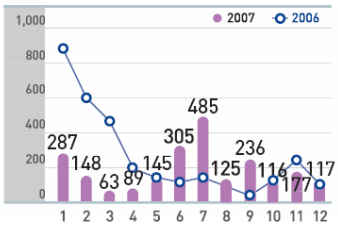
Phishing Host



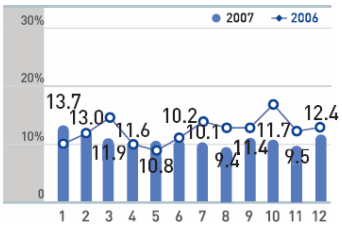
Intrusion + Other



Web Defacement



Bot Infection



However, this fact does not imply that damage caused by the malicious code and hacking incident is also decreased. Current trend shows that the attacks are targeting more narrowed scope and specific victim rather than the anonymous majority, and the victims can be vary from individuals to corporations, so how much the damage is severe is becoming something that cannot figure out easily, and difficult to scale or predict as the attack type is evolving.

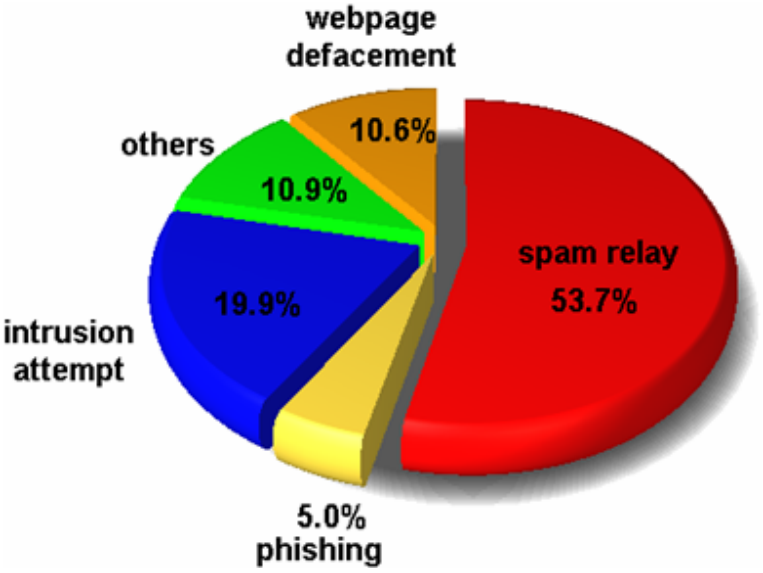
---

[4] Reported to KrCERT/CC via email and telephone

[5] Phishing incidents targeting Korean banks and financial institution are very rare; however, many Korean websites are abused as phishing host by the foreign hackers targeting foreign companies.

Hacking incident analysis

The total number of incident reports on hacking incident in year 2007 is 21,732. Among the reports on hacking incident, spam relay (11,668) takes over the half of the reports on hacking incident and it is decreased about 17% than that of the year 2006 (14,055).



Ratio of reports on hacking incident in 2007

The number of Phishing cases (1,095) is decreased compared with that of the last year (1,266). The number of webpage defacement is 2,293 and others 2,360. However, Intrusion attempt (4,316) is increased compared with that of the last year (3,711).

Rather simple hacking incidents such as webpage defacement is steadily decreasing, instead, spam relay steadily takes the top of all incidents. This fact might imply the current trend that the hackers are seeking the financial gain through their hacked servers using them as spam relay servers to send spam mails.

The number of reports on phishing is somewhat decreased but shows the steady number in recent years. This trend shows seeking the financial gain will not be easily abandoned by the hackers. Recent years are discovered several user-friendly phishing tool kits, which make more acceleration on the trend. Financial institutions are always the most targeting sector in phishing. One of the recent issues in Korea is that different aspects of phishing is surfacing that establishing the fake site of the famous online game and extorting the user identities, and forging the authentic site of the legal authorities and stealing the resident ID number, which can be compared with the social security number in the United States. The problem is that in Korea, only credentials of person's real name and resident ID number can be used for stealing the individual proprietary.

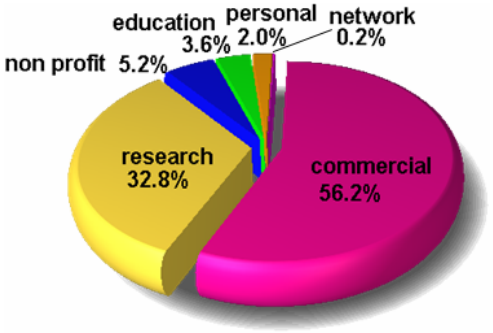
Efforts to reduce malware infected websites

KrCERT/CC operates a malware detection and response system, so-called MCFinder (malicious code finder), which enables to detect and manage malware infected systems. This detection system is crawling and hunting for websites infected with a malware, and links to malware in web pages. It has a pattern database for malware detection to determine whether the website is embedded with a malware and/or its link, and is being continuously updated.

Often a Trojan in the website inserted by a hacker spreads through Internet to users who connect

to. It then penetrates to users' PCs without any cognitive indication, to be abused as a Zombie or for stealing the personal data. Financial gain is often or mostly an objective for these incidents these days and this trend is rising than any moment before. This trend can be seen since many of the infected systems are eventually used as or connected to a phishing or identity theft.

To mitigate this trend, KrCERT/CC is putting an enormous effort by monitoring and handling the malware infected systems while taking down those sites, using the fore-mentioned system we developed. The number of detected malware websites in year 2007 is 5,551, which is 16% decrease compared with that (6,617) of the year 2006. We categorized them by business sectors as shown below.



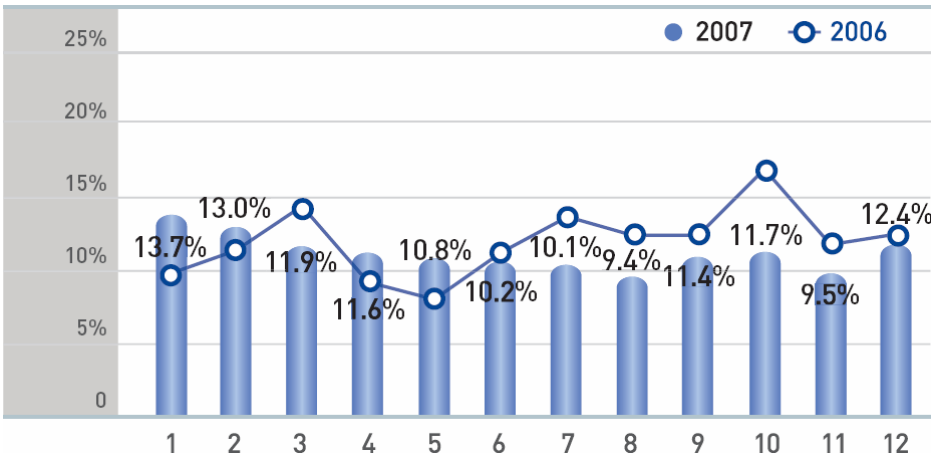
Most of the web server detected in the system is Microsoft IIS web server, which takes 57.3%, Apache takes 9%, and others 33.7%.

Efforts to reduce bot infection rate

Bot has been one of the worst threats for recent years and detected continuously that the domestic servers are exploited as bot C&C servers. It seems that domestic servers are continuously targeted because of its well-sorted infrastructure in Korea, since Bot C&C servers characteristically require fast network. KrCERT/CC is pouring a great effort to reduce the domestic bot infection rate, by monitoring and applying sinkhole method to the bot infected IPs, with the cooperation from ISPs in Korea.

Domestic bot infection rate has marked highest as 24.1% in January 2005, which gradually decreased month by month, and the monthly average rate of 2006 was 12.5%, which is decreased to 11.3% in 2007[6]. The graph of the domestic bot infection rate in 2007, shown below, has some ups and downs, but average rate is lower than that of the year 2006.

[6] This statistics is analyzed from KrCERT/CC's honeynet system located in Seoul, Korea. KrCERT/CC is operating Bot Detection System on real-time basis.



Monthly domestic bot infection rate in 2007

3. Event Activity

2007 APISC Security Training Course

KrCERT/CC hosted the 2007 APISC Security Training Course to support strengthening the response capabilities of the developing economies. The objective of this training course is to assist developing economies to establish Internet incident response capabilities while providing an education opportunity for establishing and managing CSIRT in their own country. This event was held on 10 - 14 September in Ibis Myeong-dong Hotel, with 33 trainees participated from 15 economies, 5 trainers from 3 economies, throughout the Asia Pacific region and Eastern Europe.

The contents of 5 days course includes general overview of the information security and KISA (Korea Information Security Agency) for one day, three days for TRANSITS (Training of Network Security Incident Teams Staff) course (lecture and case discussion), one half day for the business continuity planning workshop, and one half day for the tour. Active participation from the trainees benefited to all while active discussion and interaction of the trainees and trainers had been allocated for most of the time. The course was successful and fruitful as well as attendees have satisfied with the overall course.

International Incident Handling Drill

Internet is in the nature of borderless and seamless network, so as Internet incident. It is characteristically not limited to one economy or region. This reality put more meaning on the importance of having an incident handling drill among many economies, cooperation between CSIRTs for various sectors. KrCERT/CC has participated in the APCERT incident handling drill in 2007 which has ended with successful result.

The drill was to verify the coordination capabilities among CSIRTs on incident handling framework, deliver action plans to improve incident response system in each CSIRT, and give participants an experience of a coordination system, especially targeting the preparation of emergency on 2008 Beijing Olympics. For the preparation, 24/7 POCs were shared for rapid communication channel. 13 APCERT member teams from 12 economies have joined the drill, as the scenario was not revealed before the actual drill commenced. Some economies had their drill with the local ISPs involved and played with their own coordination system with the given version of scenario. MyCERT, AusCERT, and SingCERT has completed to coordinate the drill successfully, as whole other participated teams have successfully done their task. Yet another good drill was performed in 2007 by the APCERT members.

4. Achievements

KrCERT/CC has participated in National CSIRT meeting held in June 2007 in Madrid, Spain. The meeting is hosted by CERT/CC, with some local sponsors. We shared our experience presenting the national network monitoring system, effort to minimize the damage by detecting and handling the malware infected websites and DNS sinkhole system applied in the national level.

In APEC TEL 35 meeting held in Manila, Philippines, we have presented our experience of building an efficient nation-wide network coordination center, and the effort to reduce malware infection on websites by developing a special tool to detect the malicious website. In APEC TEL 36 meeting held in Santiago, Chile, KrCERT/CC co-hosted the cyber security drill workshop with the United States, and earned a successful outcome as it will undoubtedly develop to an actual joint drill in the future.

5. International Collaboration

KrCERT/CC has signed to the Joint Communiqué with MCMC[7] in Malaysia, for further cooperation on sharing the experience and strong and mutual working relationship. Both parties have agreed to facilitate the development of an effective working relationship with joint activities on matters of mutual benefit relating to their respective roles in the areas of network security, trust and governance in their respective countries, subject to the respective international obligations and the relevant laws and regulations of each country.

KrCERT/CC has also contributed to the project that providing the consultation on national

[7] Malaysian Communications and Multimedia Commission

information security implementation for Uzbekistan with the host organization, KISDI[8]. We have been participating in this project for two years since 2006, which we took a part in establishing a CSIRT in Philippines.

6. Future Plans

KrCERT/CC is planning to participate in a training program which is led by UN APCICT[9], located in Incheon, Korea. KrCERT/CC and UN APCICT concluded to the Letter of Understanding in February 2008, for promising a keen cooperation on the education for information security. Upon this agreement, KrCERT/CC is planning to develop a training material for government ICT leaders of Asia Pacific and developing economies and provide a resource person. Moreover, KrCERT/CC is planning to host 2008 APISC Security Training Course to be held with the keen cooperation with UN APCICT.

KrCERT/CC also plans to provide another good education opportunity in the year 2008 again, to many IT and security experts, by inviting them to provide an opportunity to attend security training course, through lectures and active discussions. This chance will give more skills and experiences in legal and technical way, not only to ones from developing economies who are or plans to building a CSIRT for their own constituencies, but also to leading teams by sharing the experiences and trends from all the economies from Asia Pacific region.

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

[8] Korea Information Society Development Institute
[9] United Nations Asian and Pacific Training Centre for Information and Communication Technology for Development

G. MyCERT Activity Report 2007

Malaysian Computer Emergency Response Team – Malaysia

1.0 MALAYSIAN COMPUTER EMERGENCY RESPONSE TEAM (MyCERT)

1.1 Introduction

In 1997, the Malaysian Computer Emergency Response Team (MyCERT) was established to address the internet security concerns in Malaysia. With the number of computer users in Malaysia increasing rapidly each day, more vulnerable computers are exposed to threats of abuse and criminal activities. This is the main essence of MyCERT's existence, providing a point of reference in resolving computer security incidents.

1.1.1 Establishment

MyCERT was first established in 1997, and now operates under CyberSecurity Malaysia (formerly known as NISER), a non-profit organization under the supervision of the Ministry of Science, Technology and Innovation (MOSTI), Malaysia. Further information about CyberSecurity Malaysia can be viewed at: http://www.cybersecurity.org.my/en/.

1.1.2 Constituency

Our constituency is the Malaysian Internet Users. We handle security incidents reported by Malaysian as well as foreign institutions where the sources or target of incidents are within Malaysia. Malaysian internet users are in the region of 11 to 12 million internet users.

2.0 ACTIVITIES AND OPERATIONS FOR 2007

In year 2007, MyCERT had received reports involving growing numbers of targeted attacks such as mass defacements and online fraud. In dealing with these incidents, collaboration and coordination with various parties such as law enforcement and corporate IT departments and legal departments were conducted to address the best means and mechanism in mitigating the attacks.

2.1 Incident Handling

MyCERT handled a total of 1038 incidents in 2007. Generally, the security incidents are categorized as intrusion, malicious code, fraud, harassment and spam. Fraud and intrusion related incidents makes up about 70% of total incidents handled. The majority of the cases for fraud are of phishing in nature. Incidents involving malware in particular botnet command and control, drop sites, and bot infection were also significant in 2007. On the other hand, spam related incidents continue to grow manifolds and dynamically subverting filters as well as employing various social engineering techniques.

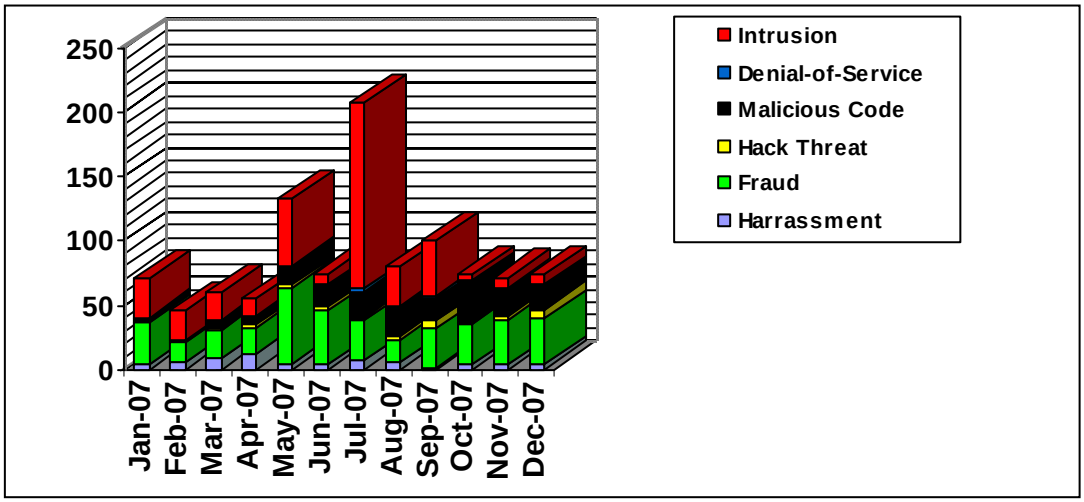
2.2 Trend in 2007

Abuse statistics and trends are available on MyCERT website. In addition, quarterly reports for 1999 to 2007 can also be viewed at *http://www.mycert.org.my/abuse-stat/index.html* and *http://www.mycert.org.my* respectively.

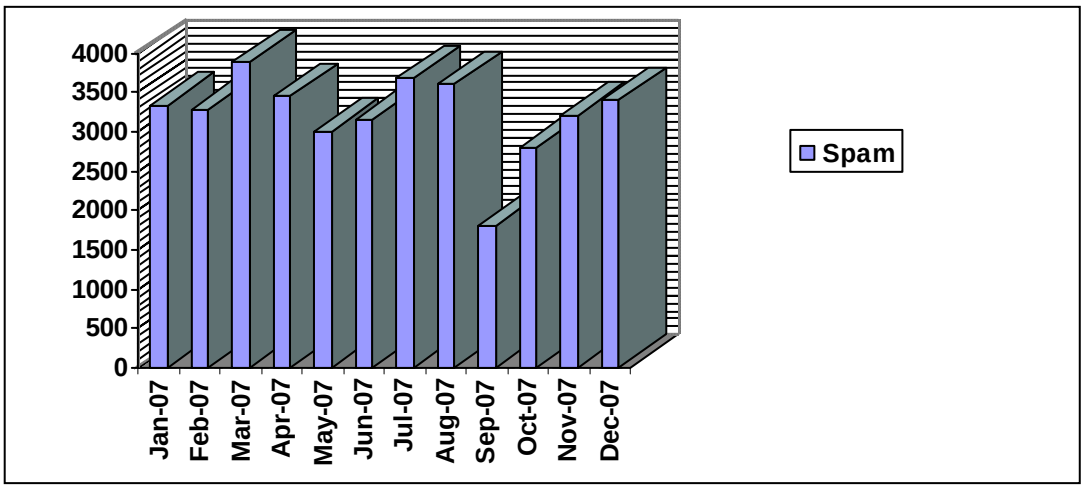
2.3 Abuse Statistics

The year 2007 abuse statistics and incidents chart are as shown below:

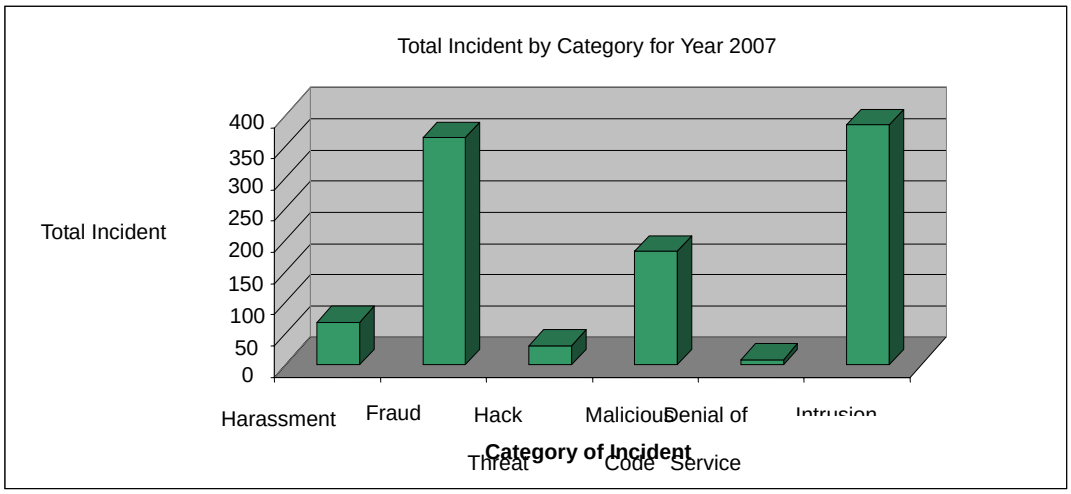
Incident Statistics for 2007



Spam Incident Statistics for 2007



Types of Incidents for 2007



3.0 EVENTS ORGANIZED, CO-ORGANIZED AND PARTICIPATED

MyCERT had participated and organized both national and international events throughout the year. On the local scene, MyCERT had been engaged to conduct trainings and talks in the area of incident handling, honeynet deployment and security trends for different types of audience. Internationally, MyCERT had been invited to share insights and case studies at various seminar and conferences on issues such as botnet, honeynet, cyber drills and malware analysis.

3.1 Major Events Organized

3.1.1 APCERT AGM & Conference 2007 (7th-9th February 2007).

The 6th APCERT AGM & Conference 2007 was held on 7th-9th February 2007 in Langkawi Island, Malaysia. In conjunction with the AGM, a two day conference was organized with more than 100 participants. Please visit http://www.cybersecurity.org.my/apcert/programs.html to get more information about the event.

3.1.2 FIRST TC 2007 (22nd-24th August 2007).

The Forum of Incident Response Security Team Technical Colloquia (FIRST TC) was organized by MyCERT on 22nd-24th August 2007 in Kuala Lumpur. The event consists of a two day plenary session which was opened to the invited guest among critical national organizations and one day hands-on session involving 4 workshops for FIRST members. The participation from FIRST, APCERT members and critical national organization were encouraging with a total of about 150 participants. Please visit http://www.first.org/events/colloquia/aug2007/ to get more information about the event.

3.2 Cyber Drill

In 2007, MyCERT had participated in three Cyber Drills of which two were international drills, ASEAN CERT Incident Drill (ACID2007) and APCERT

Drill 2007, and a national drill called MyDrill2007. MyCERT coordinated both APCERT Drill and MyDrill. The experience and knowledge gained through participating and coordinating the drills has resulted in lessons learned with the aim to improve incident handling procedures as well as strengthen cooperation and contacts among CERTs in ASEAN and Asia Pacific.

3.2.1 ASEAN CERT Incident Drill (ACID)

The ASEAN CERT Incident Drill (ACID) 2007 comprised of 13 CERTs from 11 economies conducted on 16th July 2007. The drill was coordinated by SingCERT. MyCERT meanwhile was one of the teams that had developed artifacts for the drill.

3.2.2 Asia Pacific CERT Drill (APCERT)

The APCERT Drill had 12 teams representing 12 economies in the Asia Pacific regions with MyCERT and AusCERT acting as joint developer and coordinator of the drill while SingCERT provided IRC service for real-time coordination. The event took place on 22nd November 2007 with the main scenario involving mitigation of cyber attacks during the 2008 Beijing Olympic in China.

3.2.3 Malaysian Cyber Drill (MyDrill)

Malaysian Cyber Drill (MyDrill) was a local drill organized by MyCERT, on 22nd November 2007 in conjunction with the 2007 APCERT Drill and involved six local organizations comprising of major ISP's, Domain Registrar and Anti-virus Company. The drill allowed local participants to prepare and test their response procedures through a carefully designed, multiple incident scenario which relate to the 2008 Beijing Olympics.

3.3 Training and Workshop

3.3.1 Workshops

There were several workshops or hands-on training conducted by MyCERT in 2007 which include:

a. Honeynet & Network Security Monitoring for Critical National Information Infrastructure (CNII) Hands-on Workshop.
b. Nepenthes and Honeypot Training for Higher Learning Institution Workshop.
c. Malware Capturing Technologies, Qatar FIRST TC.
d. Incident Handling Workshop for Cambodia, Laos and Myanmar.

4.0 ACHIEVEMENTS

4.1 National & International Presentation and Participation

In year 2007, MyCERT was actively involved in providing presentation at national and international events which includes:

a. Information Security Management Systems Awareness, Malaysia.
b. National Innovation Conference and Exhibition (NICE), Malaysia.
c. INFOSEC.my Special Interest Group, Malaysia.
d. APECTEL 35, Manila, Philippines.
e. FIRST TC (QCERT), Doha, Qatar.
f. APECTEL 36, Santiago, Chile.
g. Organization of American States Conference, Miami, USA.

h. AusCERT2007 IT Security Conference, Australia.
i. GOVCERT.nl, Netherland.

4.2 Publication

4.2.1 Alerts, Advisory and other publication

Alerts, Advisories and publications are available on MyCERT's website at http//www.mycert.org.my/.

5.0 INTERNATIONAL COLLABORATION

5.1 Engagement Session

As part of MyCERT initiatives to establish greater collaboration with National CERTs/CSIRTs, we have initiated face-to-face engagement session with new emerging National CERTs such as Sri Lanka CERT and IDSIRTII with the objective to foster greater collaboration and effective handling of incidents among CERTs.

5.2 Sponsor Team Application

For FIRST membership application, MyCERT had become sponsors for 2 teams who have now been successfully accepted as FIRST member. MyCERT was also involved in the sponsoring of Sri Lanka CERT application to become APCERT member.

6.0 FUTURE PLANS

In the future, MyCERT, via its host organization, CyberSecurity Malaysia, intends to expand its resources and capabilities to be able to play a proactive role in detection and alert on new cyber security threats as well as collaborating with other CERTs/CSIRTs as well as other leading organization on the global platform in combating phishing, botnet and other online crimes. MyCERT will also continue to assist organizations to establish incidents response capabilities in their respective constituency.

H. SingCERT Activity Report 2007

Singapore Computer Emergency Response Team – Singapore

1.0 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 frequent 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.

2.0 Activities & Operations

2.1 Incident Trend

For 2007, phishing and malicious software continued to be a concern. SingCERT handled on average 3 phishing incidents a month for FY07. SingCERT worked with our Internet Service Providers (ISPs) and other foreign CERTs to track down affected systems and users and informed them on how to secure their systems.

2.2 Participation in events

SingCERT participated in the APCERT Annual Drill 2007 and provided the IRC server that was used for co-ordination and communication by the drill participants.

3.0 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 3 seminars and 2 workshops for the year 2007.

4.0 International Collaboration

4.1 Incident Drill

SingCERT planned and led the ASEAN CERT Incident Drill (ACID) 2007 which expanded its scope to include not only the 10 ASEAN member countries, but also the dialogue partners and

representative from Europe. The drill was conducted successfully and received good feedback from the participants.

5.0 Future Plans and Projects

SingCERT, together with MyCERT, will be organising the 3rd ASEAN CERT Incident Drill for the year 2008. Discussions are in progress to work out the scope and coverage.

I. ThaiCERT Activity Report 2007

Thai Computer Emergency Response Team – Thai

Year 2007 Review and Comparative Incident Statistics

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

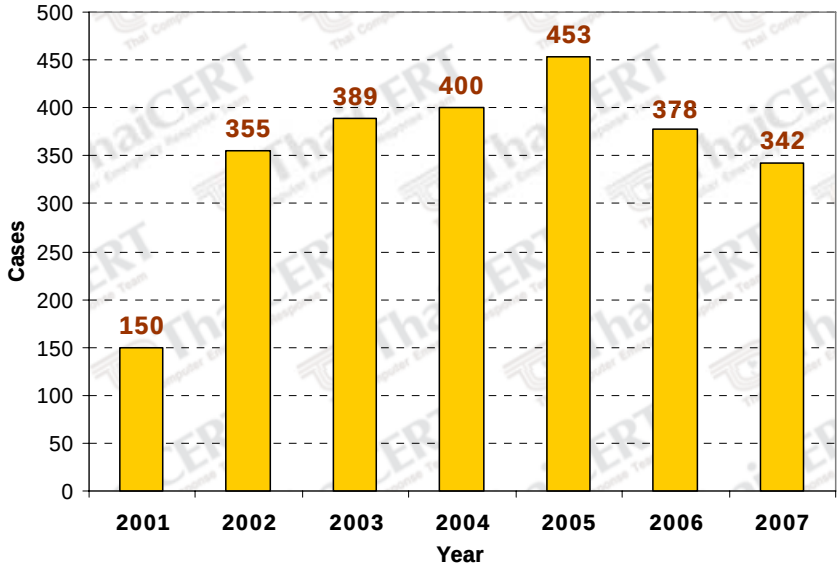


Chart 1: Number of ThaiCERT's handled incident in each year from 2001 to 2007.

According to the number of incidents in each year since 2001 in Chart 1 shown above, in year 2007 the total incident cases have been decreased from previous years. From the number of incidents categorized by types in Table 1 shown below, the phishing cases have been rapidly increased. They grew by 108 cases from year 2006 -- about 70-percent increase. On the contrary, malware (computer virus, internet worm, etc.) cases decreased to only 38 cases. Based on these data, one of possible reasons that can explain this situation -- in an optimistic way -- is that many users, especially non-administrative users, become more aware of computer threats than before. Consequentially, they might have improved their preparations to prevent those threats. The Chart 2 plotted from last table shown below depicts a clearer view.

Table 1: Number of ThaiCERT handled incident from 2001 categorized by incident types.

Year \ Type of Incident	Spam Mail	Port Scan and Probe	Malware	Phishing	Others (Hack, DDos etc.)
2001	66	38	34	-	12
2002	183	90	55	-	27
2003	31	170	171	-	17
2004	48	132	210	-	10
2005	24	56	307	20	46
2006	17	29	162	154	16
2007	**0**	**7**	**38**	**262**	**35**

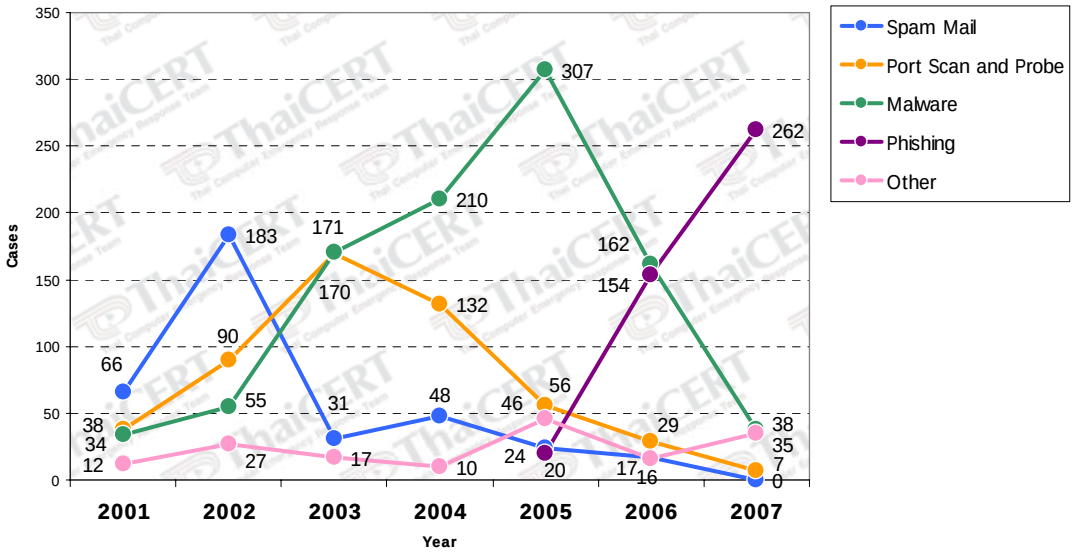


Chart 2: Number of ThaiCERT's handled incident from the year 2001 categorized by incident types.

Focusing on incidents in the year 2007, the most frequent type of incidents has changed from malware to phishing case. Approximate three-quarters of handled incidents seen by ThaiCERT are the phishing cases as shown by Chart 3 below. This evident implies that most of computer system threats have changed their theme to target personal monetary and e-commerce transaction. Note that the phishing is called based on the analogy that Internet scammers are using email lures to fish for passwords and financial data from the sea of Internet users [2]. Among all of the year 2007's phishing cases, there is one phishing case of a Thailand based bank. This fact indicates that Thai people have been the targets of the most popular computer threat too.

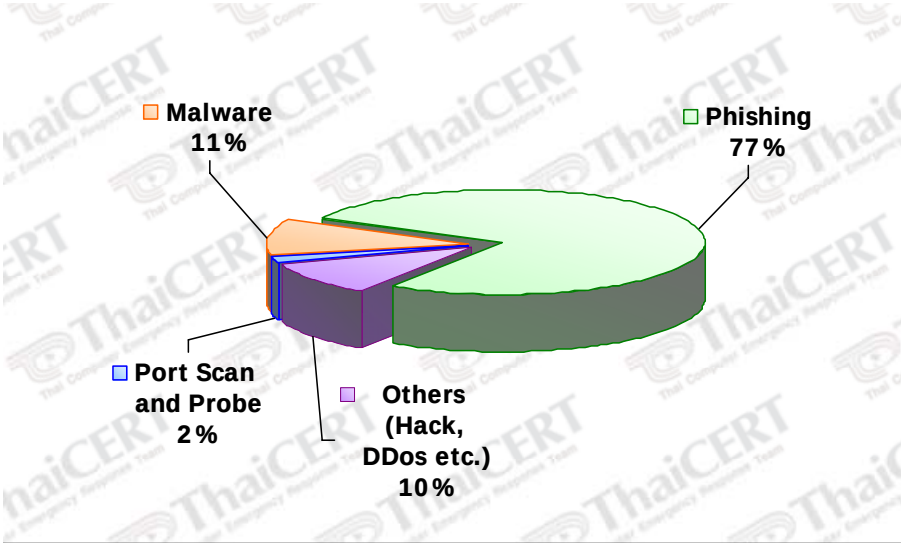


Chart 3: Ratio of each type of ThaiCERT's reported incidents in the year 2007.

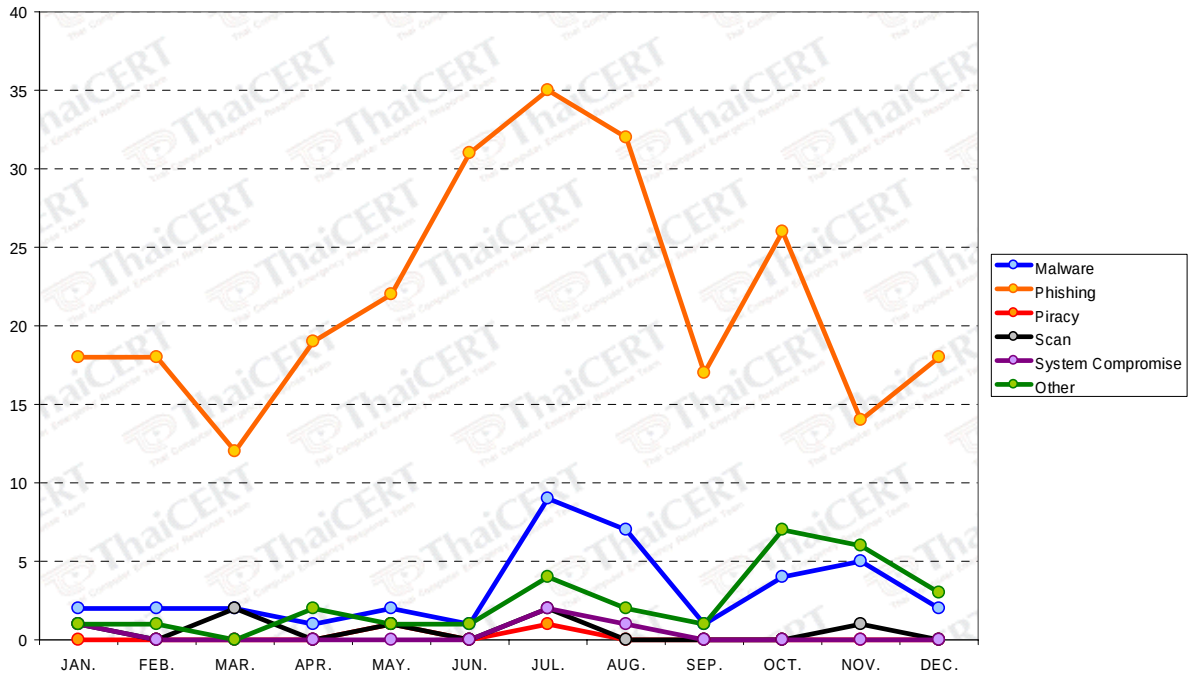


Chart 4: Number of incidents in each month during the year 2007, categorized by incident type.

Drilling down to the level of monthly statistics as shown in Chart 4, the most frequent threat type which was phishing had no fewer than 10 cases per month. In July which is the month with the highest number of phishing cases, there was on average one case per day. On the other hand, other types of incident had less than 10 cases even if they were in their busiest months. The largest numbers of incident cases were reported during the middle of the year from June to August while during the early and the late of the year 2007 there were fewer cases.

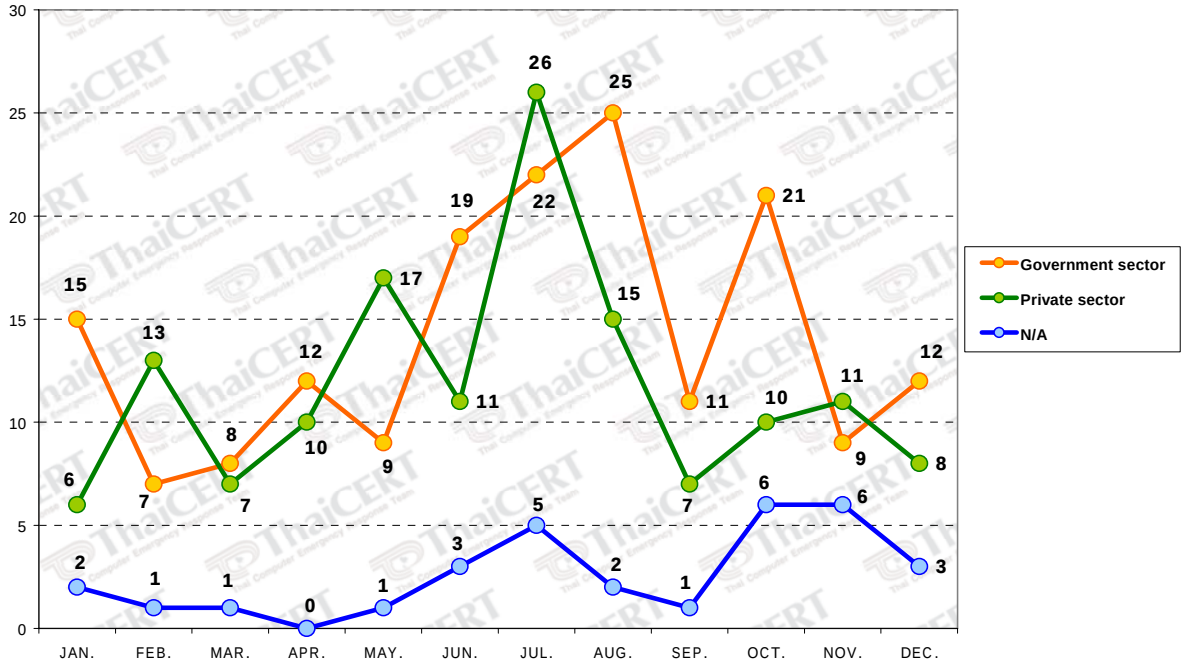


Chart 5: Number of incidents in each month of year 2007, categorized by incident source organization type.

When we considered the statistics of incidents based on their sources categorized as either government sector or private sector as shown in Chart 5, we found that the numbers of incidents coming from both sectors were almost equal. The government's incidents had 170 cases while the private's ones had 141 cases. Other 31 cases were the cases that we could not identify the sources or they were associated with both types of the source.

In the summary, there is a trend continued in the year 2007 from the previous year that the computer's incidents have changed their objectives from destroying valuable information to stealing valuable information especially personal information and e-commerce information. Even though over all number of incident cases was decreasing, the number of attacking related to the monetary and specific phishing targets was increasing. This trend is likely to grow in the year to come. The computer users including the ones who use e-commerce should prepare themselves to avoid this type of attacks.

Staff and Structure Update

Nowadays, ThaiCERT has 30 staff working in 4 security fields. Those 4 fields are

- Infrastructure Security Research and Development and ThaiCERT Services
- Wireless Broadband Security Research and Development
- Information Security Standard Research and Development
- National Security Technology Research and Development

Current certifications that our staff had gotten are such as CISSP, CWNA, RHCE, CCNA, CCNP, MCP, MCSA, CISA, GIAC and ISO27001 Auditor/Lead Auditor. We have planned to develop our staff's skill to get more certification.

ThaiCERT Services

1. **Incident Response**

   As told before, ThaiCERT has been receiving incident report to coordinate to related organizations. The more incident received, the more effort we have to spend. Therefore

ThaiCERT has developed new incident response system based on an open source project, RTIR -- Best Solution Practice's Request Ticket for Incident Response.

Many organizations in Thailand are interested in incident response. They cooperate with us when there are incidents which involved them. Some organizations join the first incident drill in Thailand.

2. Security Publications

Furthermore, there is a incident response service; ThaiCERT has provided security publications in other ways such as web page and hard copy. There are 55 web pages and 1 hard copy in 2007. All were translated into Thai.

Web page:	General articles	9	pages
	CERT advisory	41	pages
	Virus and vulnerabilities alert	4	pages
	Monthly news	1	pages
Hard copy:	ISO/IEC 27001 Standard version 2.0		

3. Security Course Training

ThaiCERT arrange a variety of training courses in 2007. The objective is to raise information security awareness to Thai people. There are many training courses such as

- Information security awareness for users/executives/administrators or technicians
- Malware Analysis Process for incident handlers
- Introduction to ISO/IEC 27001, ISO/IEC 17799 security standard
- OS hardening training and workshop
  - Microsoft Windows Workstation/Server
  - *nix in general-purpose/specific purpose
- DBMS hardening

4. Security Auditing

ThaiCERT provides an auditing service to the business companies and governments in Thailand to improve their IT security based on ISO/IEC 27001 and ISO/IEC 17799 standard.

ThaiCERT Activities

1. Seminar / Conference Participation

ThaiCERT has participated in some variant of regional and international conference in year 2007 such as

- APCERT Conference, Langkawi, Malaysia. (February 7th – 9th)
- FIRST TC Conference, Kuala Lumpur, Malaysia. (August 22nd – 24th)
- APISC Security Training Course, Seoul, Korea (September 8th – 15th)
- Etc.

2. Incident Drill

In year 2007, there are 3 on-line incident drills that were set in our region.

- Thailand Incident Drill 2007 on June 27th, held by ThaiCERT.
- ASEAN CERTs Incident Drill 2007 on July 4th, held by SingCERT.
- APCERT Incident Handling Drill 2007 on November 22nd, held by MyCERT.

ThaiCERT joined all of incident drills. These missions have shown readiness and responsiveness of local, ASEAN and Asia-Pacific incident response teams to handle incidents when they had occurred.

3. Information Security Alliance

Due to being a part of the Thailand Electronics Transaction Commission as a secretariat of security steering committee since last 3 years, ThaiCERT has contributed to govern the security standard and related issues to many organizations. Therefore, we become well

known in this field and we have much connection with the related parties. Then many critical infrastructure organizations in Thailand such as this list:

- telecommunications;
- electrical power systems
- gas and oil storage and transportation
- banking and finance
- transportation
- water supply systems
- emergency services (including medical, police, fire, and rescue) and continuity of government;

have been formed to be a club themselves as named “Information Security Alliances” or ISA. This forum is first target to enchant their information security systems to be more secure.

Secondly, it is easily to use ThaiCERT published book of the ISO/IEC 27001 standard – Information Security Management System (ISMS) in Thai language to apply to their information system.

Thirdly, this club composes of many big organizations and they devote their facilities to hold a seminar, panel discussion, exhibition or other security awareness activities in their places. These bring about their benefits such as they can share security vision, information security knowledge, security policies and procedure in their organization performed. For the activities hold in last year and recently, is listed below:

First times agenda;

“How to apply ISO/IEC 27001 to implement in your organization.”

Second times agenda;

“Phishing threat and electronic transaction in Thailand.”

Third times agenda;

“How to prepare the organization to comply with Computer Misuse Act, BE.2550.”

Fourth times agenda;

“Risk assessment and risk mitigation.”

Etc.

Lastly, as we are a CERT team, we can provide them with the new risks and new threats that be met to their organizations. Moreover, we can promote them to inform us about the incident coordination and response many incidents that we receive from our cooperation as quickly as possible. As, being in this part, we have more partners and more friends in the information security road in Thailand.

J. TWCERT/CC Activity Report 2007

Taiwan Computer Emergency Response Team/Coordination Center – Chinese Taipei

1. About TWCERT/CC

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 domestic security domain, 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.

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:

i. To assist the handling of the intrusion incidents around Chinese Taipei;
ii. To announce the system vulnerability information;
iii. To provide security training and education on protection and defending technologies and skills;
iv. To research and develop the Security Auditing System (SAS) which audits the subscribed client systems;
v. To assess periodically the general security level of Chinese Taipei in the Internet;
vi. To be the official international coordination in Chinese Taipei by joining international security organizations.

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 before hand. Following are our chief missions:

- 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 Chinese Taipei's 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.

2. Activities & Operations

■ Domestic and international security incidents advising and 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:

(1) Possible incidents prevention: provide an incident response channel and the prevent mechanism for the victims to avoid analogous events happening.
(2) Real-time Incidents handling: offer an immediate warning and defense force to effectively restrain and control incidents extending.
(3) Recovery support: provide technological consultant and support to recovery operation and reduce damage.

Year	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007
Total	2	9	85	962	1260	5318	2874	1824	788	660

Table 1. TWCERT/CC incident response statistics

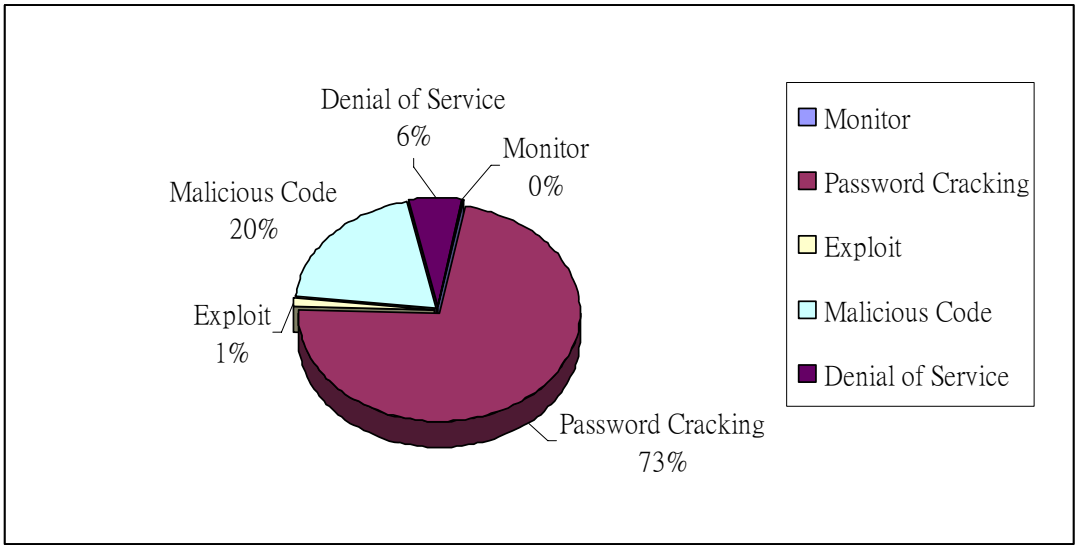


Fig 1. TWCERT/CC incident response classification

■ Research and provide vulnerability information

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	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007
Advisory	31	186	178	172	258	142	197	140	138	119

Table2. TWCERT/CC Advisory statistics

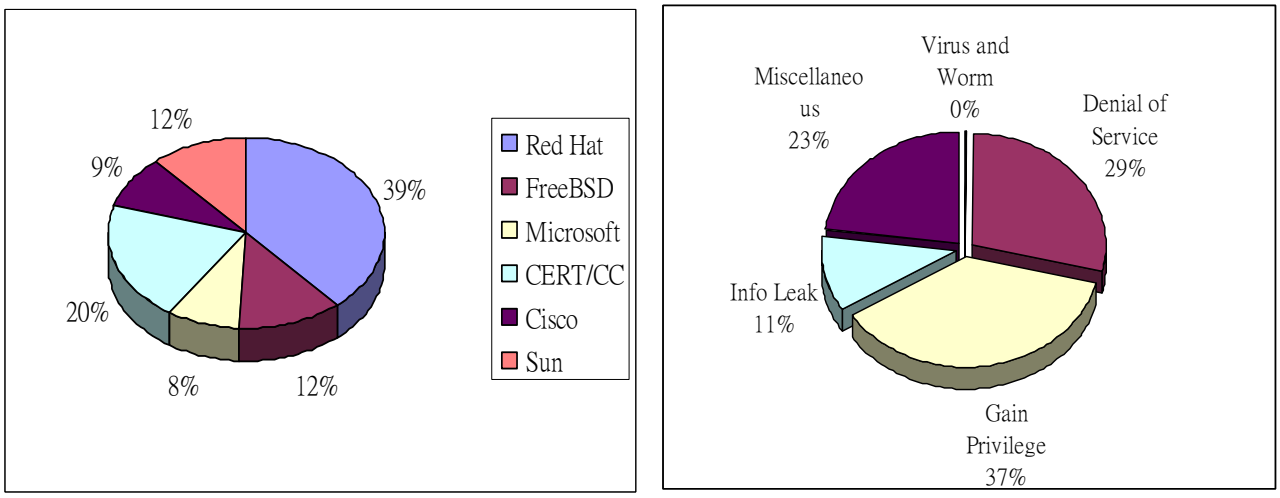


Fig 2. TWCERT/CC Advisory classification

- **Mailing list subscription**

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, technologies, or skills to raise the awareness of network security in Chinese Taipei.

- **Security related information providing**

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 maintain**

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:

A. Convenience
   - User-friendly interface and easy-to-use
   - Flexible configuration and setup

B. Reliability
   - Reliable and efficient scan

C. Integrity
- Graphical statistical report
- Suggested and related advisories in the report

■ **Localized Vulnerability Database maintaining**

The major purpose of the establishment of the vulnerability database in localized language is to collect the information of software vulnerabilities and system weaknesses. The vulnerability database contains 45 categories and up to 15 thousands records. We will continuously invest manpower to maintain and update. The major categories are shown in Fig. 3.

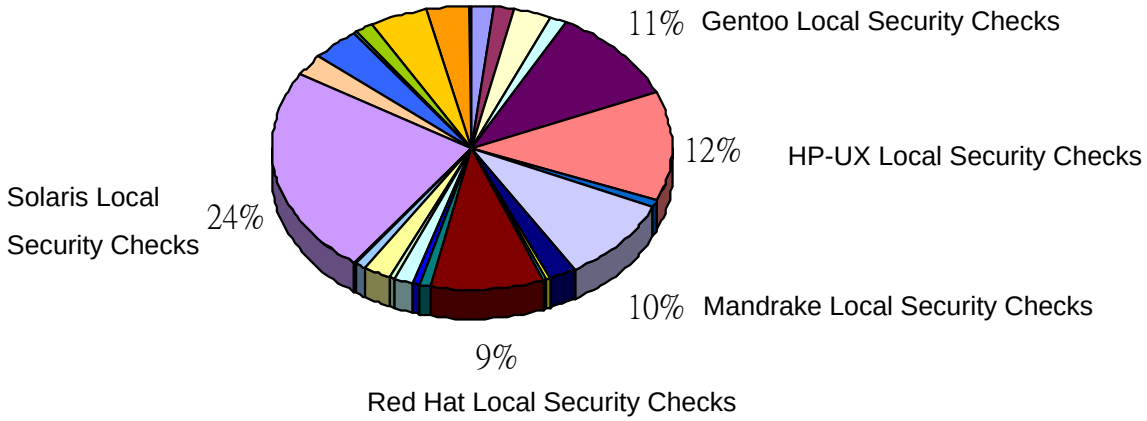


Fig 3. Categories of TWCERT/CC Vulnerability Database

■ **Security Training/Education**

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 service**

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 Training

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

Date	Subject
2007/03/15	A Key Predistribution Scheme for Sensor Networks Using Deployment
2007/03/20	Integrity Evidence for Chain of Custody in Signature Payload Embedding Systems
2007/10/29	Enterprise information security
2007/11/07	Information Sharing and Analysis Center (ISAC)
2007/11/19	Security threat and protection of VoIP
2007/11/30	Spam and Spyware
2007/12/28	Information Security in Telematics

3.2 Seminars

Date	Seminar	Sponsor	Location
2007/01/29	Info security white paper seminar	**Science and Technology Advisory Group of Executive Yuan**	**Chinese Taipei**
2007/02/08 | 2007/02/10	2007 APCERT Annual Meeting	APCERT	Langkawi, Malaysia
2007/04/16 | 2007/04/18	Info Security 2007	**Isecutech**	**Chinese Taipei**

4. Achievements

4.1 Services

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 before hand. 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 training/education 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 hold seminars and education training programs to publicize the network security information and to enhance the capability of the security administrators in a more active way. Such interactively training provides a great channel for information sharing as well as skill improvement.

- **Personnel 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 communication**

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.

4.2 Publication

Publication	Publish
An Alliance-based Anti-Spam Approach	Third International Conference on Natural Computing
A Key Predistribution Scheme for Wireless Sensor Networks Using the Small-World Concept	The 1st International Conference on Network-Based Information Systems
DoS Detection in Cluster-Based Sensor Networks	The Fourth IASTED International Conference on Communication, Network, and Information Security

Malicious DHTML Detection by Model-based Reasoning	2007 Information Security Conference

4.3 Certification

Information Security Management Systems Lead Auditor

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.

■ 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.

■ Asia Pacific Computer Emergency Response Team (APCERT)

Besides globalization organizations, Asia Pacific Computer Emergency Response Team is a regional coordination organization established by leading CERTs/CSIRTs 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.

■ 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:

1. To cope Chinese Taipei's network security incidents with other nations, and take the part as a coordination center;
2. To assist in handling the transnational spam problems;
3. To exchange the related security intelligence with each member;
4. 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

I order to keep the international influence, to participate in transnational operation and to ensure the basic right of the Internet users, TWCERT/CC wishes to enhance the international competitive ability and visibility of Chinese Taipei and practice in international communication by promoting security sense and transaction.

- 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.

K. TWNCERT Activity Report 2007

Taiwan National Computer Emergency Response Team - Chinese Taipei

Introduction

TWNECRT is a non-profit organization intended for improving incident response and IT 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 handling in the face of security incidents.

TWNCERT continues to provide many information security services, including promoting IT security awareness, engaging research and development, gathering computer incidents and vulnerability information, providing incident response service, IT security seminars and forums. TWNCERT is also willing to cooperate with other CSIRTs/CERTs computer security related organizations worldwide to deal with the computer incidents in Chinese Taipei and to share security information with each other.

2007 Highlights

1. Promote Security Awareness and Provide Training Course

TWNCERT offers IT security conferences, workshops, training courses, and exhibitions for technical staffs and security managers. The organized events in 2007 are listed below:

(1) Trainings
- ✓ ISMS lead auditor training courses.
- ✓ ISMS building training courses.
- ✓ Training courses for key area of ISMS auditing.

(2) Conferences and Workshops
- ✓ 6 workshops of information security technical issues are provided in 2007
- ✓ Chinese Taipei information security skill game for college students

2. Incident Response and Prevention

TWNCERT publishes advisories and alerts for preventing and responding to computer incidents. We collect information from many sources (e.g. real-time monitoring, incident handling and forensic, malicious code analysis) and try to integrate for announcing security trends. In 2007, TWNCERT published total 1429 advisories and alerts, including:

(1) 401 alerts for intrusion incidents.
(2) 9 advisories for system vulnerabilities or weakness.
(3) 213 alerts for web site defacement incidents.
(4) 805 advisories for warning the suspicious incidents and incident prevention.
(5) 1 alerts for emergency incident.

3. International Cooperation

TWNCERT is always glad to join in the international security organizations and share information with security communities. In 2007, TWNCERT continued to join in the following security communities and attended many important conferences and participate in related activities:

(1) APCERT
- ✓ Attend APCERT annual conference in Langkawi, Malaysia.
- ✓ Join in the APCERT Drill 2007

(2) FIRST
- ✓ Attend FIRST annual conference in Seville, Spain.

(3) APEC-TEL
- ✓ Attend APEC-TEL 35 meeting in Manila, Philippines.
- ✓ Attend APEC-TEL 36 meeting in Santiago, Chile.

(4) BlackHat and DEFCON
- ✓ Attend BlackHat training course and DEFCON conference in Las Vegas, USA.

(5) AVAR（Association of anti Virus Asia Researchers）
✓ Attend AVAR conference in Seoul, Korea.

TWNCERT receives the reporting of computer incidents about Chinese Taipei and coordinate related law enforcement agencies to handle these incidents. We want to strengthen the ability of information security defense and reduce the damage cause by these incidents. In 2007, TWNCERT handle 97 incidents reporting from international security communities, including:

(1) All 97 incidents are about phishing sites located in Chinese Taipei. TWNCERT coordinated law enforcement agencies to remove the phishing pages or shutdown the phishing hosts as soon as possible.

4. Presentations and Publications

TWNCERT is continuing to do research on security areas and publish the research results in the international security conferences in order to share our experiences with communities. The following is the presentation and paper published in 2007.

(1) TWNCERT 2006 annual report for APCERT AGM 2007.

5. ISO 27001/BS7799 Information security management systems certification

In order to provide a highly security standard of services, TWNCERT had passed the external auditing of ISO 27001/BS7799 by BSI in 2007.

For the international cooperation, TWNCERT will continue to share information with global security communities in the future.

URL: http://www.twncert.org.tw/en/main.php
Email: twncert@twncert.org.tw

Deputy Director,
Jia-Chyi Wu
Email : jiachyi@icst.org.tw
Phone : +886-2739-1000 ext. 602
Fax : +886-2733-1655

Liaison Officer & Engineer,
Pei-Ching Liu / Peggy
Email: peggyliu@icst.org.tw
Phone: +886-2739-1000 ext.663
Fax: +886-2733-1655

L. BruCERT Activity Report 2007

Brunei National Computer Emergency Response Team – Negara Brunei Darussalam

1.0) About BruCERT

1.1) Introduction

Brunei National Computer Emergency Response Team (BruCERT) was established in May 2004. It was formed in collaboration with AITI, the Ministry of Communication, to become the nation's first trusted one-stop referral agency in dealing with computer-related and internet-related security incidents in Brunei Darussalam.

The *Brunei Computer Emergency Response Team Coordination Centre (BruCERT)* welcome reports on computer security related incident. Any computer related security incident can be reported to us by:

Telephone: (673) 2458001
Facsimile: (673) 2458002
Email: cert@brucert.org.bn

1.1.1) Services

- 24X7 Security Related Incidents and Emergency Response from BruCERT.
- 24X7 Security Related Incidents and Emergency Response onsite (Deployment response is within 2hrs after an incident is received). This service only applies to BruCERT Constituents.
- Broadcast alerts (Early Warning) of new vulnerabilities, advisories, viruses and Security Guidelines from BruCERT Website. BruCERT Constituents will receive alerts through email and telephone as well as defense strategies in tackling IT Security related issues.
- Promote Security Awareness program to educate and increase public awareness and understanding of information security and technical know-how through education, workshop, seminar and training.
- Coordinating with other CERT, Network Service Providers, Security Vendors, Government Agencies as well as other related organization to facilitate the detection, analysis and prevention of security incidents on the internet.

1.1.2 BruCERT Workforce

BruCERT currently with strength of 58 including 44 IT Staff (100% local) and the rest is administration. BruCERT has undergone training on various IT security module, such as A+, N+, Linux+, Server+, Security+, SCNP, SCNA, CIW, CEH, CCNA, CISSP and BS7799 Implementer, where most of BruCERT workforce has gain certification in certain fields.

1.1.3 BruCERT Constituents

BruCERT has close relationship with Government agencies, 2 major ISPs and various numbers of vendors.

Government Agencies

Provide a security incident response services to national and government agencies as ITPSS is appointed as a central hub for all IT security-related issues across the nation and to become the Government trusted E-Security Advisor.

AITI

Authority for Info-communications Technology Industry of Brunei Darussalam (AITI) is an independent statutory body to regulate, license and develop the local ICT industry and manage the national radio frequency spectrum.

AITI has appointed ITPSS (Information Technology Protective Security Services), an IT local security company to become the national CERT in dealing with incident response in Brunei.

Royal Brunei Police Force

BruCERT has been collaborating with RBPF to resolve computer-related incidents.

TelBru – BruNet

TELBru, the main service provider of internet gateway. and BruCERT have been working together to engage information sharing of internet-related statistics and the current situation of IT environment in Brunei.

DST –

The second largest internet service provider in Brunei.

2.0) BruCERT Activities and Operation in 2007

2.1) Incidents response (Phising Website)

In 2007, BruCERT receive its 1st Phising website incident. BruCERT receive the incident report from the local ISP saying that one of Brunei local company is hosting an ebay phising website. An investigation was conducted to verify the phising website claim and was found that the phising web site was uploaded through improperly configured FTP service. The incident was properly contained and eradicated by BruCERT before it can cause any further damage to the organization.

2.2) Internet Usage Statistics

Internet in Brunei Darussalam

Internet usage in Brunei Darussalam has been growing phenomenally since it was first launched in 1995. The 2 most popular internet connections in Brunei are the Broadband and Dial-Up technology. Based on the latest statistic (2005 and 2006) given by TelBru (BruNet) one of the ISPs in Brunei Darussalam, along with the estimated Brunei population of 380,000, there are an increased in number of users using Broadband.

The following figures provide information on the total number of subscribers using Dial-Up and Broadband Internet Connections.

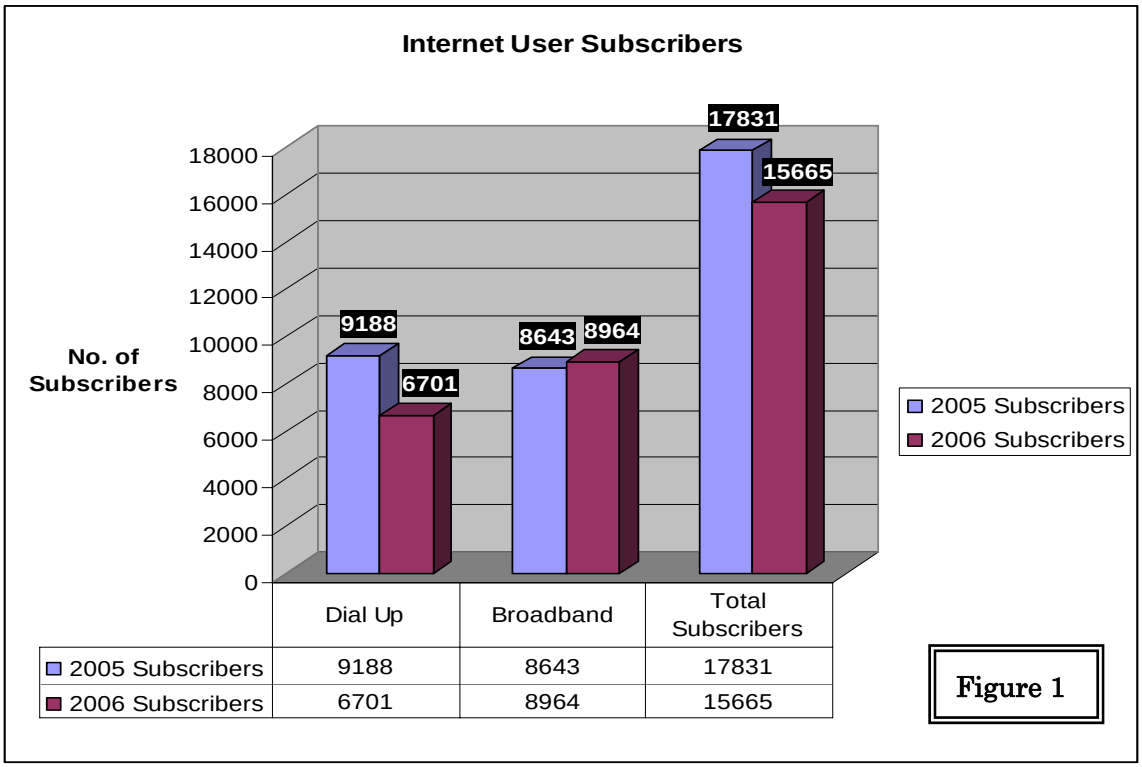
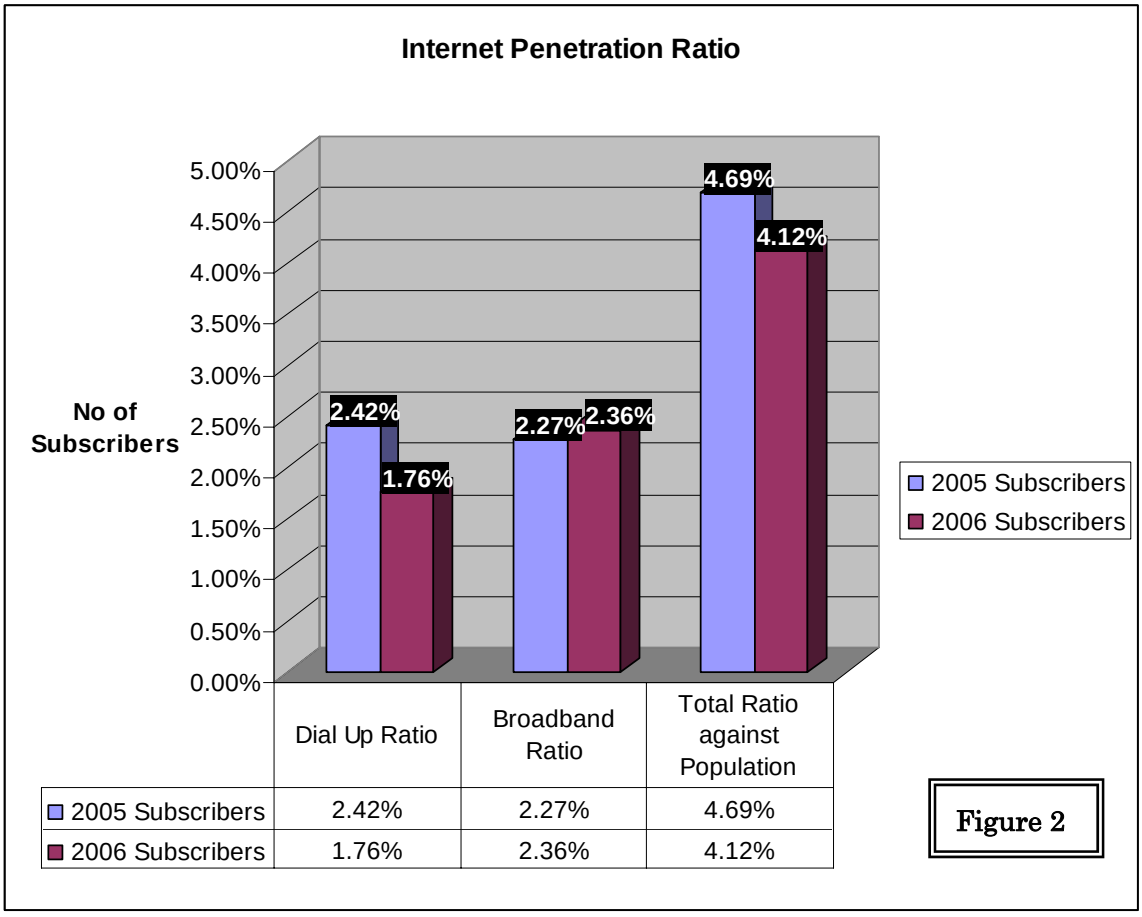


Figure 1



	Dial Up Ratio	Broadband Ratio	Total Ratio against Population
2005 Subscribers	2.42%	2.27%	4.69%
2006 Subscribers	1.76%	2.36%	4.12%

Figure 2

According to the statistics shown in both figures, it can be seen that Broadband subscribers is higher than Dial-Up subscribers from 2.27% (2005) to 2.36% (2006) and a fall in Dial-Up accounts from 2.42% (2005) to 1.76% (2006). This significant switch from dial-up to broadband usage could be influenced by the following factors:-

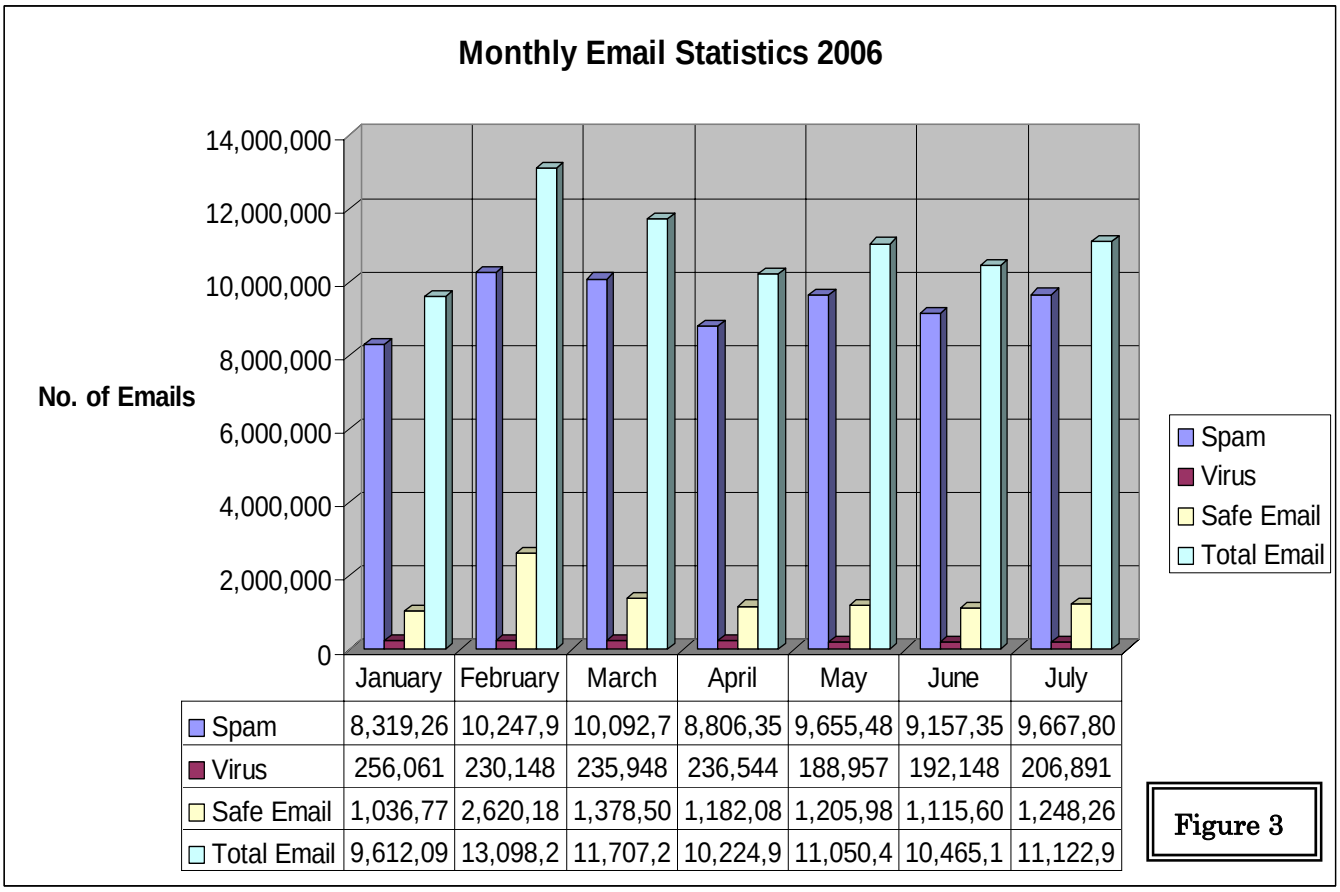
- higher bandwidth
- provide value-added services such as onsite technical support extended broadband service coverage nationwide
- latest IT gadgets in the markets such as wireless access point
- Information, Education, Business, etc purposes

In addition from Figure 2, the total internet penetration ratio is decreasing from 4.69% to 4.12% due to the following reasons:

- a significant declined in number of dial-up users
- popularity in the use of cell-phone internet
- cybercafés which offer free internet access point with high-speed broadband internet connection

Note: Please take into consideration that this statistics did not include subscribers using prepaid cards.

2.3) Statistics on malicious codes



	January	February	March	April	May	June	July
Spam	8,319,26	10,247,9	10,092,7	8,806,35	9,655,48	9,157,35	9,667,80
Virus	256,061	230,148	235,948	236,544	188,957	192,148	206,891
Safe Email	1,036,77	2,620,18	1,378,50	1,182,08	1,205,98	1,115,60	1,248,26
Total Email	9,612,09	13,098,2	11,707,2	10,224,9	11,050,4	10,465,1	11,122,9

Figure 3

As shown in Figure 3, spam is more popular than viruses. This might be because of the ISP had implemented an additional new hardware to assist in detecting spam mails as well as viruses and furthermore that the advantage of free advertisement through email seems to be at ease. While during February, the high percentage email utilization could possibly due to no new big impact viruses ever exist during that period.

As BruNet still lack of complete logging mechanism necessary for more effective and complete monitoring, thus they only managed to gather the statistics above. But they are in the process of upgrading their capabilities through their own initiatives or through some corroborative work with BruCERT.

3.0) BruCERT Activities in 2007

3.1 Attended Seminars/Conferences/Meetings/Visits

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

- In 8th February 2007 - Two BruCERT delegates attended the APCERT 2007 Annual General Meeting which takes place at Langkawi, Malaysia.

- On the 22nd till 27th May 2007, BruCERT participated in Civil Service Institute Customer Day held at Civil Service Institute in the capital.

- In July 16th 2007, BruCERT joined the ASEAN CERT Incident Response Drill, where the main objective is to simulate realistic cross-border incidents handling and promote collaboration among national CERTs in the region

- In Aug 2nd 2007, three of JPCERT delegates lead by its Director of Technical Operation paid a courtesy visit to BruCERT premise.

- In 10th till 14th September 2007, three BruCERT delegates joined the APISC Security Training Course hosted by KrCERT/CC

- In 22nd Nov 2007, BruCERT participated the APCERT Drill 2007 lead by AUSCERT.

3.2 Training and Seminars

From January 2007 onwards, BruCERT has conducted on-going *IT Security Awareness Training*, at the Civil Service Institute (IPA) of Brunei Darussalam for Government Officials in three levels, which are End Users, IT personnel and Executive Management.

Due to overwhelming response, the "Basic Information Security Workshop" was developed in May 2007 as an advanced course from the IT Security Awareness training. This particular training will be conducted on a regular basis at the Civil Service Institute, Brunei.

4.0) BruCERT Future Plans

- Applying for FIRST membership
  BruCERT plans to upgrade its member status to full member in APCERT and work on with other terms and conditions to qualify for the FIRST membership.

- Free Seminars to the local public
  A half-day or one-day talk will be given to the local public to enhance awareness on IT security-related topics.

- SMS Services
  BruCERT plans to offer SMS alert and notification service for the public. This subscription based service shall provide early notification to the public on IT security related events and alerts.

- BruCERT Road shows
  Organize Roadshows to further promote and publicize BruCERT services by conducting, educational programmes and games.

- Publications
  Produce educational booklets and posters. This is intended to provide basic IT security awareness to the general public and facilitate BruCERT road shows.

5.0) International Collaboration

In Aug 2nd 2007, three of JPCERT delegates lead by its Director of Technical Operation paid a courtesy visit to BruCERT premise. During the 2 days visit, BruCERT and JPCERT had sign the Memorandum of Understanding (MOU) to enhance the collaboration between the CERTS in handling IT Security Incident.

6.0) Conclusion

Due to the anonymity in cyberspace, Internet crimes are getting hard to detect. In order to address these computer threats, the collaboration between BruCERT and the enforcement of various legislations together with the involvement of law enforcement agencies can help to strengthen cyber security and protect the well being of the people and nation. Besides that, collaboration among CERTs is essential in an effort to work together mitigating the risk of further incidences in the region. Its hope that BruCERT can be make known and contribute more to the public through the implementation of the future plans mentioned above.

M. CERT-In Activity Report 2007

Indian Computer Emergency Response Team – India

1.0 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.

1.2 Establishment and Constituency

CERT-In was operational since January 2004. 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.

2.0 Activities and Operations of CERT-In

2.1 Services and Activities

CERT-In provides:

- Proactive services in the nature of Advisories, Security Alerts, Vulnerability Notes, and Security Guidelines to help organisations secure their systems and networks
- Reactive services when security incidents occur so as to minimize damage

The summary of activities carried out by CERT-In during the year 2007 is given in the following table:

Activities	Year, 2007
Security Incidents handled	1237
Security Alerts issued	44
Advisories Published	66
Vulnerability Notes Published	163
Security Guidelines Published	1
White papers Published	2
Trainings Organised	6
Indian Website Defacements tracked	5863

Open Proxy Servers tracked	**1805**
Bot Infected Systems tracked	**25915**

Table 1. CERT-In Activities during year 2007

2.2 Cyber Security Assurance Framework

CERT-In is establishing the National Cyber Security Assurance Framework for protection of Critical Information Infrastructure. As part of this CERT-In has empanelled 76 'Security Auditors' for auditing, including vulnerability assessment & penetration testing of computer systems and networks of various organisations of the government, critical infrastructure organisations and those in other sectors of the Indian economy. These audits enable CERT-In to assess the vulnerabilities in Critical Information Infrastructure systems and devise suitable corrective actions and response capabilities. Implementation of security measures as per ISO 27001 has been mandated for all government organisations. A comprehensive database of Chief Information Security Officers (CISO) of Critical Infrastructure organisations is being maintained and training programs have been conducted to form a network of CISOs and encourage them to implement best practices to secure their systems. CERT-In is providing early warning on emerging threats to CISOs so as to enable them to take suitable actions to mitigate the risk.

To facilitate its tasks, CERT-In has initiated steps to collaborate with IT product vendors and security vendors in the country. CERT-In is collaborating with international security organisations and CERTs to facilitate exchange of information related to latest cyber security threats and international best practices.

2.3 Incident Handling Reports

2.3.1 Summary of Computer Security Incidents handled by CERT-In during 2007

In the year 2007, CERT-In handled more than 1230 incidents. The types of incidents handled were mostly of Phishing, Malicious Code propagation and Network Scanning & Probing.

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

Security Incidents	**2004**	**2005**	**2006**	**2007**
Phishing	3	101	339	392
Network Scanning / Probing	11	40	177	223
Virus / Malicious Code	5	95	19	358
Others	4	18	17	264
Total	**23**	**254**	**552**	**1237**

Table 2. Year-wise summary of Security Incidents handled

2.3.2 Incident Statistics

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

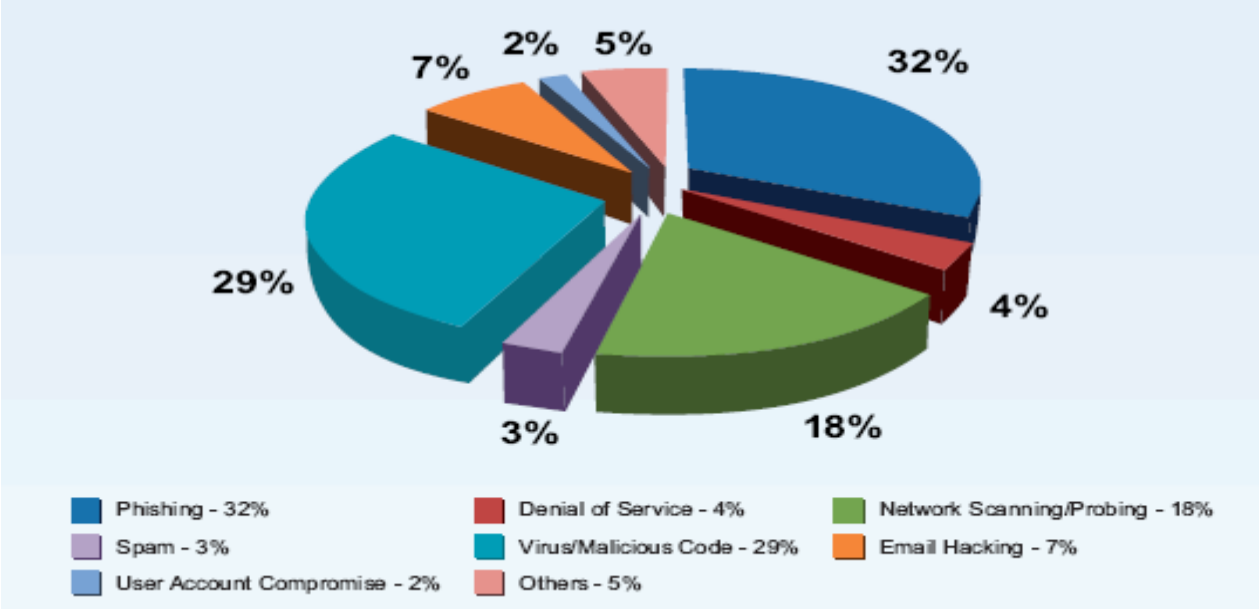


Figure 1. Summary of incidents handled by CERT-In during 2007

The phishing attacks reported in 2007 were primarily carried out against e-commerce sector and Financial services. While phishing attacks on E-commerce sector account for 51% of the total phishing attacks, the second most targeted sector is financial services which accounts for 47% of the total number. The phishing incidents affecting Indian Financial Institutions were around 12 % of total phishing incidents reported, while remaining incidents were affecting brands of other economies.

2.3.3 Incident Trends

In the year 2007 automated infection toolkits such as MPack and "Random JS Toolkit" used i-Frame injection and JavaScript injections to infect the websites and propagate malware.

Incidents of Phishing using toolkits such as Metaphisher were observed. Phishing websites were hosted on Fast-Flux DNS using Botnet such as Storm. Phishing Incidents using Rock-Phish and Fast-Flux techniques were on the rise.

CERT-In handled various cases of information stealing Trojans such as Clampi, Bzub and Nethell, affecting users of online transactions. These Trojans used key logging features to capture information that is fed to web forms and sent this captured information to the remote systems.

Storm worm, transpired in January 2007, used the spam to propagate using different social engineering techniques based on current events. Storm botnet spread to thousands of systems and used P2P network for Command & Control operations. This botnet was used for malicious purposes such as spam and phishing.

An increase in XSS attacks and website defacements exploiting vulnerabilities in PHP were observed in year 2007.

2.4 Proactive Services

2.4.1 Tracking of Indian Website Defacements

CERT-In has been tracking the defacements of Indian websites and suggesting suitable measures to harden the web servers to concerned organisations. In all 5863 numbers of defacements have been tracked. Most of the defacements were done for the websites under ***.com*** domain. In total 1693 ***.in*** domain websites were defaced.

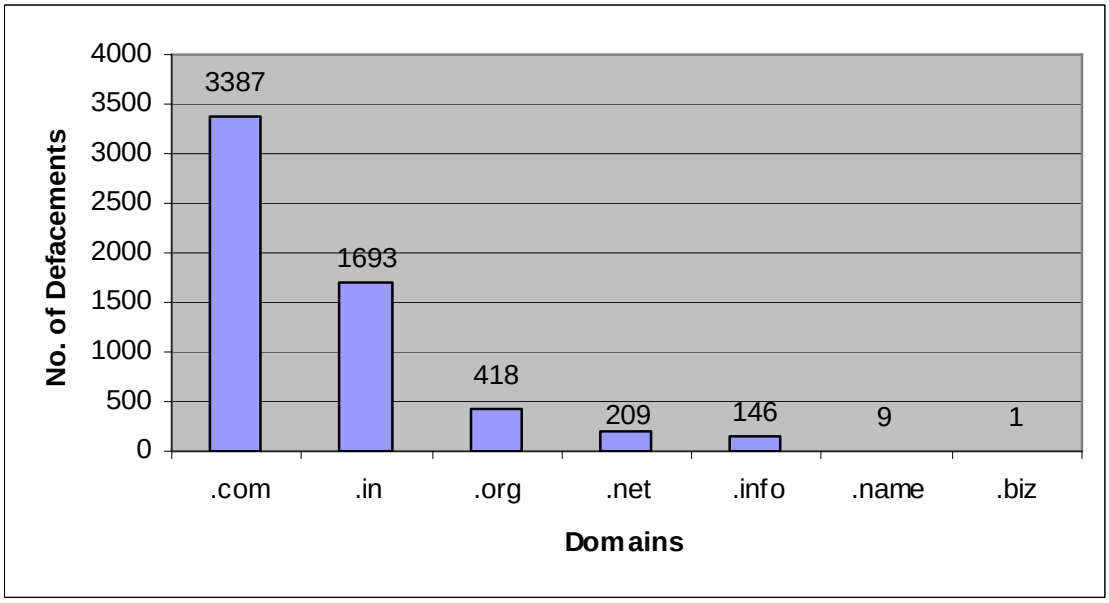


Figure 2. Indian websites defaced during 2007 (Top level domains)

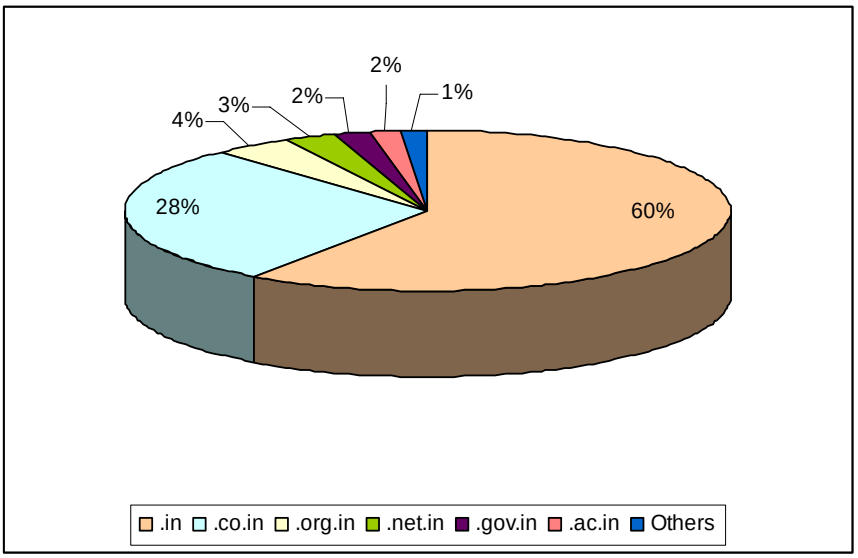


Figure 2.1 .in ccTLD defacements during 2007

2.4.2 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 1805 open proxy servers were tracked in the year

2007. As compared to previous year the number of open proxy servers has decreased, 1837 open proxy were reported last year. The month-wise distribution of open proxy servers tracked during this year is shown in the figure.

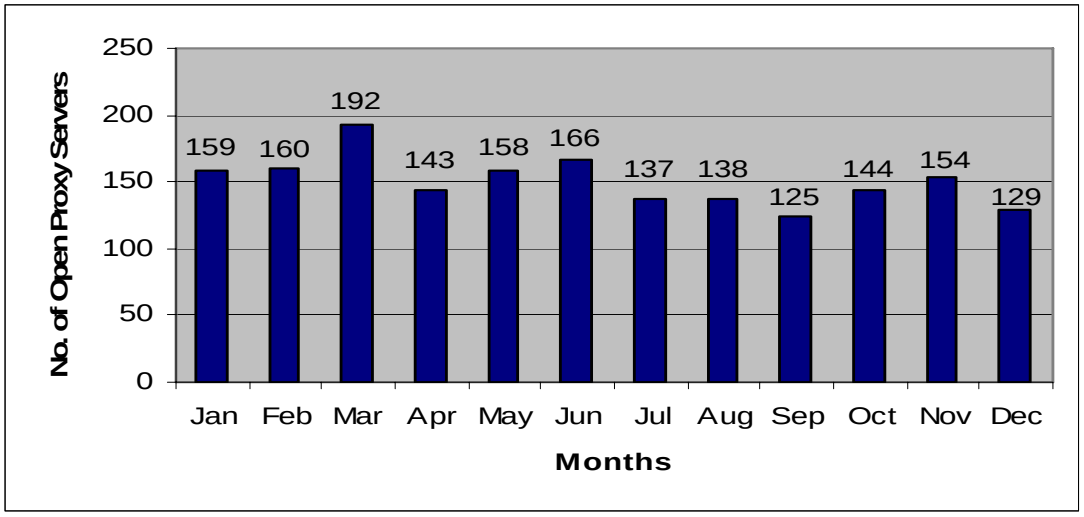


Figure 4. Monthly statistics of Open Proxy Servers in 2007

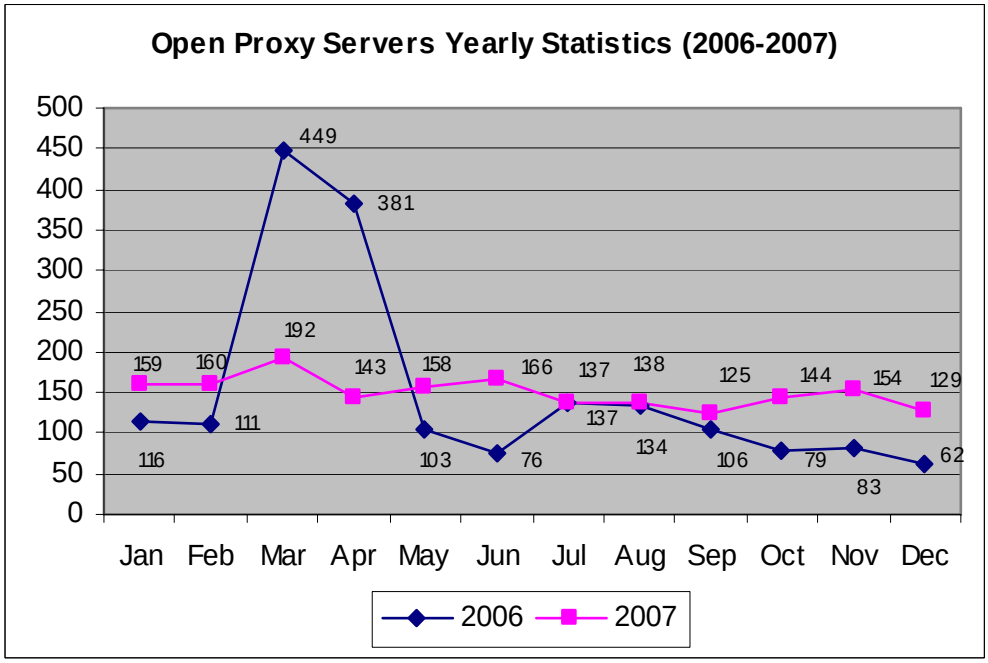


Figure 4.1 Comparison of Open Proxy Servers Month-wise (2006 -2007)

2.4.3 Botnet Tracking and Mitigation

CERT-In started the activity of tracking Bots and Botnets involving Indian systems. After tracking the IP addresses of C&C servers and Bots operating within India, actions are being taken to clean the respective systems and prevent malicious activities. Figure 5 shows the number of Bot infected systems and Command & Control servers tracked from June 2007.

Month	Number Of Bot Infected Systems	C&C Servers	
		C&C Servers- Outside India	C&C Servers in India
June	760	93	4
July	14835	138	4
August	4934	55	4
September	1976	57	4
October	1370	56	4
November	1020	48	2
December	1020	46	2
Top Ports used for the Botnet communication 6667, 1231, 4001, 5005, 65500, 3159, 9997, 7777, 13830, 34567			

Figure 5. Botnet statistics from June to December 2007

3.0 Events organised/ co-organised

3.1 Education and Training

To create awareness and to enable users to implement best practices, CERT-In is organising workshops and training programmes on focused topics for targeted audience such as CIOs, financial and banking sector officers, System Administrators, ISPs etc. Experts from industry are delivering lectures in these workshops apart from CERT-In staff. CERT-In has conducted the following training programmes for CIOs and System Administrators during 2007.

1. Workshop on "Implementing Secure Coding Practices" on 16th January, 2007
2. “Information Security Executives Readiness Training Programme for CISOs" on 12-14 February, 2007
3. Workshop on "Security aspects related to setting up SWAN" on 30 April 2007
4. Workshop on "Vulnerability Assessment Methodologies" on 16 October, 2007
5. Workshop on "Botnet Attacks and Defenses" on 26th October, 2007

3.2 Seminars/ Forums

CERT-In has formed forums in coordination with Confederation of Indian Industry (CII) for facilitating information exchange and joint programmes to combat Phishing attacks and Spam.

4.0 Achievements

4.1 Presentations

Various lectures were delivered by the staff of CERT-In in the national and international workshops/conferences/seminars.

CERT-In participated in the following international seminars/conferences:

- Botnet Task Force Conference held in Sydney in July 2007
- Blackhat Briefings, July 2007
- Internet Governance Forum meeting in Brazil in November 2007

4.2 Publications

The following white papers were published on website of CERT-In in the year 2007:

1. Analysis of defaced Indian websites year-2006

   The primary objective of this paper is to present the detailed statistical analysis of defaced Indian websites during year 2006. In the year 2006 a total no. of 5211 Indian websites were defaced.

2. Analysis of Phishing Incidents year-2006

   Phishing is a fast growing financial fraud prevailing across the globe. This document provides analysis of phishing incidents reported to CERT-In during the year 2006. The phishing incidents described in the document includes the cases in which either the phishing websites are hosted in India or domain registrant belongs to India. The document provides details on the incidents analyzed, targeted sectors, brands hijacked etc.

5.0 International collaboration

CERT-In is collaborating with international security organisations and CERTs to facilitate exchange of information related to latest cyber security threats and international best practices. CERT-In is general member of APCERT and member of FIRST.

5.1 MoUs:

CERT-In has signed MoUs with National Cyber Security Centre, Republic of Korea, JPCERT/CC and National Computer Board, Mauritius for mutual cooperation in the area of cyber security.

5.2 Drills

- CERT-In participated in the ASEAN CERTs Incident Handling Drill (ACID 2007) held on 16th July 2007.
- CERT-In participated in the APCERT International Incident Handling Drill 2007 held on 22nd November, 2007.

6.0 Future Plans/Projects

The thrust is to make CERT-In the most trusted referral agency in the area of information security in

the country. CERT-In is focusing on following activities:

- Building a network of CISOs of Critical Infrastructure Organisations and interacting with them to ensure security of the critical systems
- Collaboration with IT product and security vendors to mitigate the vulnerabilities in various systems
- Providing guidance for developing and augmenting sectoral CERTs
- Cooperation with international CERTs and security organizations on information sharing and incident response
- Promote Research and Development activities in the areas of Artifact analysis, Cyber Forensics and security training and awareness
- CERT-In is developing a mechanism to issue advance warnings and alerts on cyber attacks and provide countermeasures by analysing Internet traffic patterns

N. VNCERT Activity Report 2007

Vietnam Computer Emergency Response Team – Vietnam

1. About CERT

Introduction

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

Roles of VNCERT:

- Coordinating all actions, awareness, resources for combating Network and IS attacks of all kind;
- Promoting establishing a connective group of local CSIRTs;
- Supporting lawgiver and policymaker to understand about cyber security better;
- Cooperating comprehensively with international organizations and national CERTs of other country.

Staff and structure

VNCERT has four specialized divisions: division of operation, division of system technique, division of training & consultancy, division of research & developing. VNCERT also has two representative office, one in Hochiminh city and another in Danang city.
Current number of employees in VNCERT is thirty three.

2. Incident reports and handling

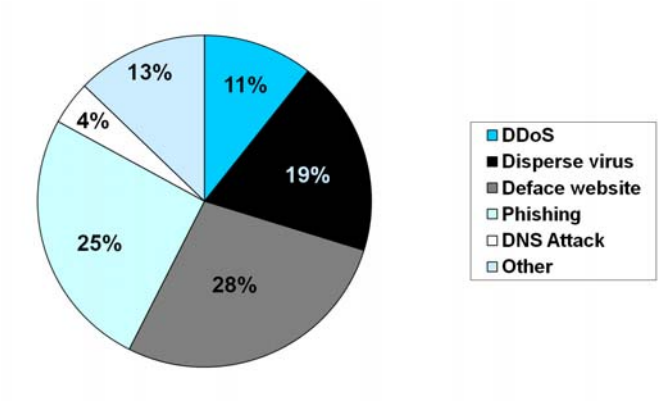
In 2007, the total number of serious incidents reported to VNCERT is 47, which has 19 incidents increase compared to 2006. Many reports are about website defacement and phishing: phishing incidents increased from 4 to 12, defacement incidents increased from 7 to 13.

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

Number of incidents related to virus also go up, and so many viruses used USB for spreading.

VNCERT works very actively in handling all incidents, especially incidents originated from Vietnam.

In 2007, some DNS attacks also occurred.



Types of incident

3. Training and consultancy

Training

In year 2007, VNCERT arranged some training courses for raising information security awareness to staff in some organizations, for example:

- Improving capability for information security for officials. This training course contains two classes, one in Hanoi city and another in Hochiminh city.
- Training course for information security staff of banks

Consultancy

- Support and participate in building of government degree No 64 on Information Technology application in state agencies' operation,
- Prepare and propose anti-spam regulation to government for issue in.
- Help government building state information security strategy
- Start to support some agencies and companies setup up CSIRTs
- Alert and assist many organizations to handle vulnerabilities and attacks.

4. International Collaboration

VNCERT attended many international activities last year:

- Join APCERT as a general member in April, 2007
- Participate annual Meeting of CSIRTs with national responsibility.
- Work with JPCERT/CC, CNCERT/CC about collaboration, MoU
- Discuss threats of hacker with National Intelligence Service of Korea
- Exchange information with MicrS, Mc Afee, Symantec

Drill

In September, 2007, VNCERT took part actively in the ASEAN CERTs Incident Drill (ACID) 2007 that have participation of 13 member in APCERT. The drill is successful and very helpful.

Workshops, seminars and conferences.

- Coordinate with other agencies to hold ITU regional workshop on “Network security structure and key infrastructure protection” in August, 2007.
- Attend and report in many workshops, seminars, conferences in Vietnam and other regions (APCERT, ASEAN, ARF, APECTEL, ITU, Meeting of national CSIRTs…)

- Appoint officials to take part many international training course on information security that organized by APT, APCERT,…

5.0 Future projects:

- Science and technology R&D project on building nation-wide distributed network security incident monitoring system: research system analysis and build demonstrative system (2008-2009).
- Expand CSIRT network to provinces, cities around the country (2008-2010).
- Support issuing anti-spam degree and start implementing total anti spam-mail solutions in the country when the Anti-spam decree have effect (May 2008).
- Build cyber incidents handling collaboration framework between organizations (2008).
- Build and promote the implementation of information risk management framework for government organizations as stated by the Decree No. 64/2007. (2008-2010)
- Organize the first Vietnam cyber drill - 2008 between ISPs, government organizations and other related companies.

6.0 Conclusion

We realize that to solve all the matter related to computer crime effectively, there must be a connective cooperation among CERTs around the world.

Ministry of Information and Communications of Vietnam, therefore, supports the APCERT initiative and promise to support VNCERT to take part in as well as actively contribute in the activities of the APCERT.

VNCERT will full participate in share data, research, response strategies, and early warning notifications with all others CERTs around the world.