APCERT 2008 Annual Report

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

APCERT
Asia Pacific Computer Emergency Response Team

CONTENTS

Chair's Message 2008

First of all, I would like to welcome everyone to the APCERT Conference 2009, hosted for the first time in this beautiful city, Kaohsiung.

The security and threat landscape in 2008 did not improve much compared to the previous years. Distributed denial of service attack, peer-to-peer based malware, fast-flux hosting, and phishing are all part of the underground economy and not showing any signs of slowing down.

On a positive note however, there has been more collaboration among security teams, researchers, operators, and enforcement agencies to mitigate threats. The various topics addressed and discussed by experts at this conference is a good example of this collaboration.

The APCERT initiative has demonstrated that cross-border coordination is not only relevant in managing cyber security incidents, but also important in ensuring that the emergency response teams in various countries in the region are always prepared in dealing with evolving threats.

An example of such effort is the annual APCERT Cyber Exercise that was conducted on 4th of December 2008. It involved 14 teams representing 13 economies and 5 different time zones within the Asia Pacific Region. I have personally heard good comments from other organizations outside the region for this particular initiative.

The APCERT has also been active in recruiting new members. On this note, I would like to welcome Bangladesh CERT (BDCERT) to the APCERT family.

It is my sincere hope and belief that the APCERT will continue to grow and contribute at the global stage.

Finally, I would like to take this opportunity to extend our utmost thank and gratitude the host of this year's APCERT Annual General Meeting and Conference, Taiwan CERT/CC for their dedication in ensuring the success of this event.

Husin Jazri
Chair of APCERT
Chief Executive Officer (CEO), Cybersecurity Malaysia - MyCERT
March 2009

I. About APCERT

1. Objectives and Scope of Activities

APCERT *(Asia Pacific Computer Emergency Response Team)* is a coalition of the forum of CERTs *(Computer Emergency Response Teams)* and CSIRTs *(Computer Security Incident Response Teams)*. The organization was established 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 <www.terena.nl/tech/task-forces/tf-csirt/> - a team of CSIRTs in Europe.

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 MyCERT (Malaysian Computer Emergency Response Team. Deputy Chair is HKCERT (Hong Kong Computer Emergency Response Team/Coordination Center). JPCERT/CC (Japan Computer Emergency Response Team/Coordination Center) serves as Secretariat.

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

2. APCERT Members

APCERT was formed in 2003 by 15 teams from 12 economies across the Asia Pacific region, and has increased its membership since then. This year, BDCERT (Bangladesh Computer Emergency Response Team) and SLCERT (Sri Lanka Computer Emergency Response Team) have been approved as General Member of APCERT.
APCERT now consists of 22 teams from 16 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
CERT-In	Indian Computer Emergency Response Team	India
CNCERT/CC	National Computer network Emergency Response technical Team / Coordination Center of China	People's Republic of China
HKCERT	Hong Kong Computer Emergency Response Team Coordination Centre	Hong Kong, China
ID-CERT	Indonesia Computer Emergency Response Team	Indonesia
JPCERT/CC	Japan Computer Emergency Response Team/Coordination Center	Japan
KrCERTCC	Korea Internet Security Center	Korea
MyCERT	Malaysian Computer Emergency Response Team	Malaysia
PHCERT	Philippine Computer Emergency Response Team	Philippine
SingCERT	Singapore Computer Emergency Response Team	Singapore
ThaiCERT	Thai Computer Emergency Response Team	Thailand
TWCERT/CC	Taiwan Computer Emergency Response Team/Coordination Center	Chinese Taipei
TWNCERT	Taiwan National Computer Emergency Response Team	Chinese Taipei
VNCERT	Vietnam Computer Emergency Response Team	Vietnam

General Members

Team	Official Team Name	Economy
BDCERT	Bangladesh Computer Emergency Response Team	Bangladesh
BP DSIRT	BP Digital Security Incident Response Team	Singapore
BruCERT	Brunei Computer Emergency Response Team	Negara Brunei Darussalam
GCSIRT	Government Computer Security and Incident Response Team	Philippine
NUSCERT	National University of Singapore Computer Emergency Response Team	Singapore
SLCERT	Sri Lanka Computer Emergency Response Team	Sri Lanka

3. Steering Committee (SC)

Since the last APCERT AGM held in March 2008, Hong Kong, China, the following members served as APCERT Steering Committee (SC).

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

4. 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 2008

1. APCERT Activities & International Relationships/Engagements

APCERT has been active in terms of promoting and representing APCERT in various international forums. Followings are activities of APCERT members in 2008 contributing to APCERT international activities:

APCERT AGM & Conference 2008 – Hosted by HKCERT
10-12 March 2008 in Hong Kong, China
http://apcert2008.hkcert.org/

The event was held in conjunction with the 7th APCERT AGM & Conference which was attended by the APCERT members and invited guests. APCERT 2008 was a venue for regional information security professionals to meet and discuss strategic development issues, to share experience in dealing with most updated security attack at the frontier and the new initiatives to combat the hacker and cyber-criminals. It was a valuable opportunity to learn, share information and network with the global and regional experts.

APEC TEL 37
23-28 March 2008 in Tokyo, Japan

China is forwarding a project on developing policies and technical documents against Botnet, in APEC TEL SPSG (Security and Prosperity Steering Group).
Mr. Jinhyun Cho, KrCERT/CC, was elected as Convenor of APEC TEL SPSG.

Joint Workshop on Security 2008, Tokyo
25-26 March 2008 in Tokyo, Japan
http://www.first.org/events/colloquia/mar2008/program/

JPCERT/CC presented on APCERT and its activities in the Asia Pacific region in this two day joint security workshop of CSIRT initiatives.

CNCERT/CC 2008 Conference
7-10 April 2008 in Shenzhen, China
http://2008.cert.org.cn/About%20the%20Conference.html

The event offered access to a seminar community that helps to meet industry security goals. Developing a wide range of professional relationships.
1. Provide opportunity and platform for international users in research, education, digital communication, finance
2. Share latest technologies and experiences, promote research and application development
3. Strengthen cooperation and prosperity
CNCERT/CC hosted the event, and HKCERT presented on APCERT activity updates.

20th Annual FIRST Conference
22-27 June 2008 in Vancouver, Canada
http://www.first.org/conference/2008/

Participant teams of APCERT had a meeting with members of FIRST, TF-CSIRT, CERT-TCC (Tunisia) and others to share information and discussions on relevant issues.

TF-CSIRT Meeting
13-14th May 2008 in Oslo, Norway
http://www.terena.org/activities/tf-csirt/meeting24/

TF-CSIRT is a task force that promotes collaboration between CSIRTs at the European level, and liaises with similar groups in other regions.
MyCERT presented on APCERT activity updates and APCERT Drill 2007.

ASEAN CERT Incident Drill (ACID) 2008
30 July 2008

The ASEAN CERT Incident Drill (ACID) 2008 was held on 30 July 2008. The drill focused on the topic of handling cross-border incidents pertaining to malware.
SingCERT coordinated and developed several non-malicious applications simulationg malware.

APCERT approved as General Guest in APEC TEL
6 August 2008

APCERT renewed its status as APEC TEL General Guest, to continue contribution and participation in APEC TEL (APEC Telecommunications and Information Working Group).

AP* Retreat Meeting
24 August 2008 in Christchurch, New Zealand
http://www.apstar.org/apstar_agenda.php?p_content_category_id=2&p_meeting_id=27

AP* Retreat Meeting gathers Internet-related organizations from the Asia Pacific region in order to share the respective activities, to discuss issues that need to be considered as AP community, as well as to establish a trust relationship. The meeting is held every once or twice a year.
AusCERT presented on APCERT activity updates.

APEC TEL 38
12-17 October 2008 in Lima, Peru
http://www.mtc.gob.pe/portal/apectel38/index.html

MyCERT presented on APCERT activity updates and challenges:
http://www.mtc.gob.pe/portal/apectel38/security.html
JPCERT/CC shared a joint presentation on APCERT member contributions in awareness raising activities:
http://www.mtc.gob.pe/portal/apectel38/cyber.html

DotAsia Advisory Council
October 2008
http://www.dotasia.org/index.html

APCERT joined the council to assist DotAsia in policy development and relevant community projects.
Mr. Roy Ko, HKCERT, is appointed as member of the Advisory Council.

APCERT Drill 2008
4 December 2008
http://www.apcert.org/documents/pdf/APCERT-drill-2008.pdf

APCERT Drill 2008 was held on 4 December 2008 with 14 teams participating in the drill. The drill was coordinated by MyCERT and AusCERT and used the APCERT IRC server, established by MyCERT, for real time coordination. The simulated attacks were themed to be deployed by the professional cybercriminal groups who trade stolen data or malicious online service in the underground economy.

AVAR 2008
10-12 December 2008 in New Delhi, India
http://www.aavar.org/avar2008/index.htm

APCERT contributed as Supporting Partner of AVAR 2008 - 11th Association of anti-Virus Asia Researchers Internation Conference.

OIC-CERT Seminar 2009 for OIC Countries
13-15 January 2009 in Kuala Lumpur, Malaysia
http://www.ansi.tn/oic-cert/index.html

The OIC-CERT or Organisation of The Islamic Conference-Computer Emergency Response Team is an organization that encourages and supports the collaboration and cooperation between CERTs among the OIC member countries. The OIC-CERT Seminar 2009 was an annual information security event targeting ICT security professionals, policy makers, industry players and researchers from the OIC member countries.
CyberSecurity Malaysia organized the seminar.

AP* Retreat meeting
24 February 2009 in Manila, Philippines
http://www.apstar.org/apstar_agenda.php?p_content_category_id=2&p_meeting_id=28

AP* Retreat Meeting gathers Internet-related organizations from the Asia Pacific region in order to share the respective activities, to discuss issues that need to be considered

as AP community, as well as to establish a trust relationship. The meeting is held every once or twice a year.
PHCERT presented on APCERT activity updates.

Other International Relationships & Engagements

*** APEC TEL SPSG (Security and Prosperity Steering Group)**
Convenor - Mr. Jinhyun Cho, KrCERT/CC

*** FIRST (Forum of Incident Response and Security Teams)**
Director & SC Member - Ms. Yurie Ito, JPCERT/CC

2. APCERT SC Meetings

Since the last APCERT AGM held in March 2008, Hong Kong, China, SC members held 6 teleconferences to discuss on APCERT operations and activities.

3. Approval of New General / Full Members

The following teams newly joined APCERT General / Full Memberships.

- SLCERT (Sri Lanka) was approved as General Member as of 10 Mar 2008.
- CERT-In (India) was approved as Full Member as of 5 Sep 2008.
- VNCERT (Vietnam) was approved as Full Member as of 25 Dec 2008.
- BDCERT (Bangladesh) was approved as General Member as of 25 Dec 2008.

4. APCERT Website

JPCERT/CC manages and updates the APCERT website <www.apcert.org>.

On a temporary basis, AusCERT hosts the POC contact details for each of the APCERT POCs. Access is by password only for APCERT teams.

III. Activity Reports from APCERT Members

Full Members

1. AusCERT Activity Report 2008

Australian Computer Emergency Response Team – Australia

1. About AusCERT

1.1. Introduction

As the national CERT, AusCERT serves Australia's national interest by improving Internet security for Australian Internet users.

AusCERT does this by:

- collecting, analyzing 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 and networks.

Increasingly, AusCERT has used its unique operational vantage monitoring, analyzing and mitigating cyber attacks to advocate best practice in Internet security, particularly in areas involving cooperation between entities around the world and attack impact mitigation.

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 AusCERT's focus changed from being university centric to include the interests of all sectors.

AusCERT is an independent, non-government, self-funded not-for-profit team of information and technical security professionals based at the University of

Queensland. The University of Queensland is one of Australia's premier learning and research institutions.

AusCERT is recognized as the national computer emergency response team (CERT) by the Australian government.

1.3. Staffing

AusCERT employs 17 staff. Eight Coordination-Centre staff provide incident handling and security bulletins services to AusCERT members, the public and contacts overseas. 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

AusCERT's constituents are Australian Internet users in the public and private sector, home and business. Given that AusCERTrelies on revenue from its subscribers, member organisations remain the 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 & 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;
- 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 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 Statistics

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.

[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

Each incident represents a single unique URL or domain name that is hosted by one or more compromised computers for the purpose of stealing sensitive information and access credentials from other computers. Multiple incidents can be associated with each attack, which is the set of compromised computers needed to launch the attack and collect the stolen data. The number of IP addresses associated in a single incident and a single attack is variable but can range from 1 to around 5,000.

This graph does not include specific compromised hosts involved in any single attack or incident - only URLs and domain names. Nor does this depict the number of computer infections (compromised hosts) that occur due to each malware attack of which there is generally many hundreds or thousands.

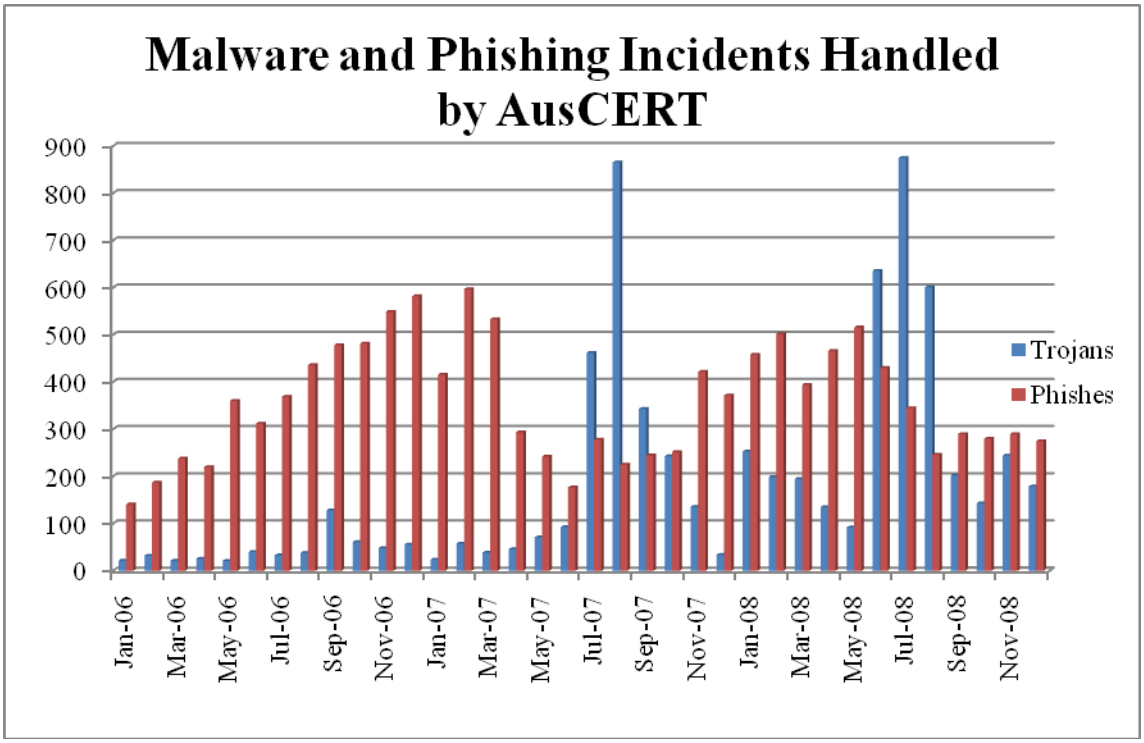


Figure 1

The figures above are representative of specific types of incidents handled by AusCERT. Total incidents handled are much greater.

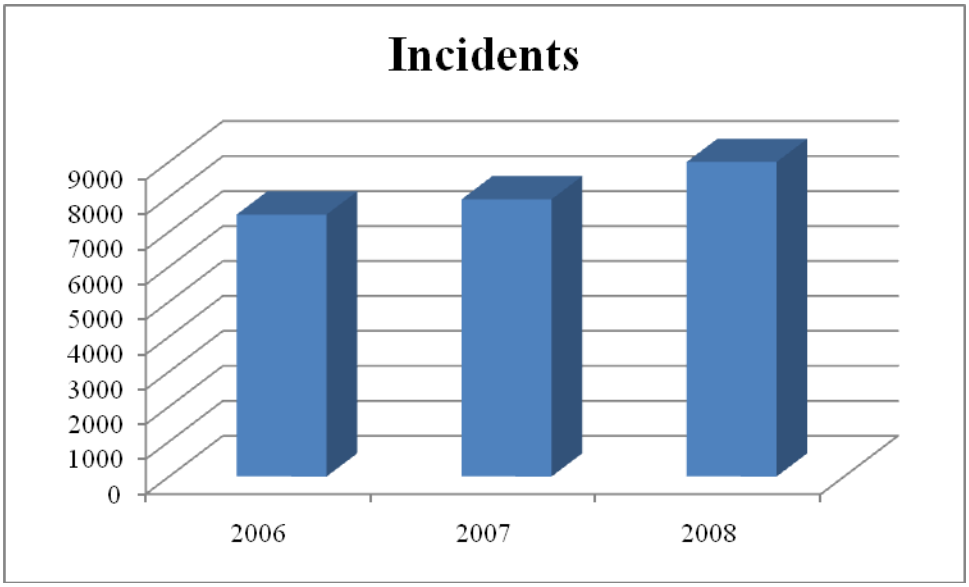


Figure 2

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 2008, AusCERT published 1,163 external security bulletins (ESB), 270 advisories, 131 alerts, and 30 updates and 76 blog items.

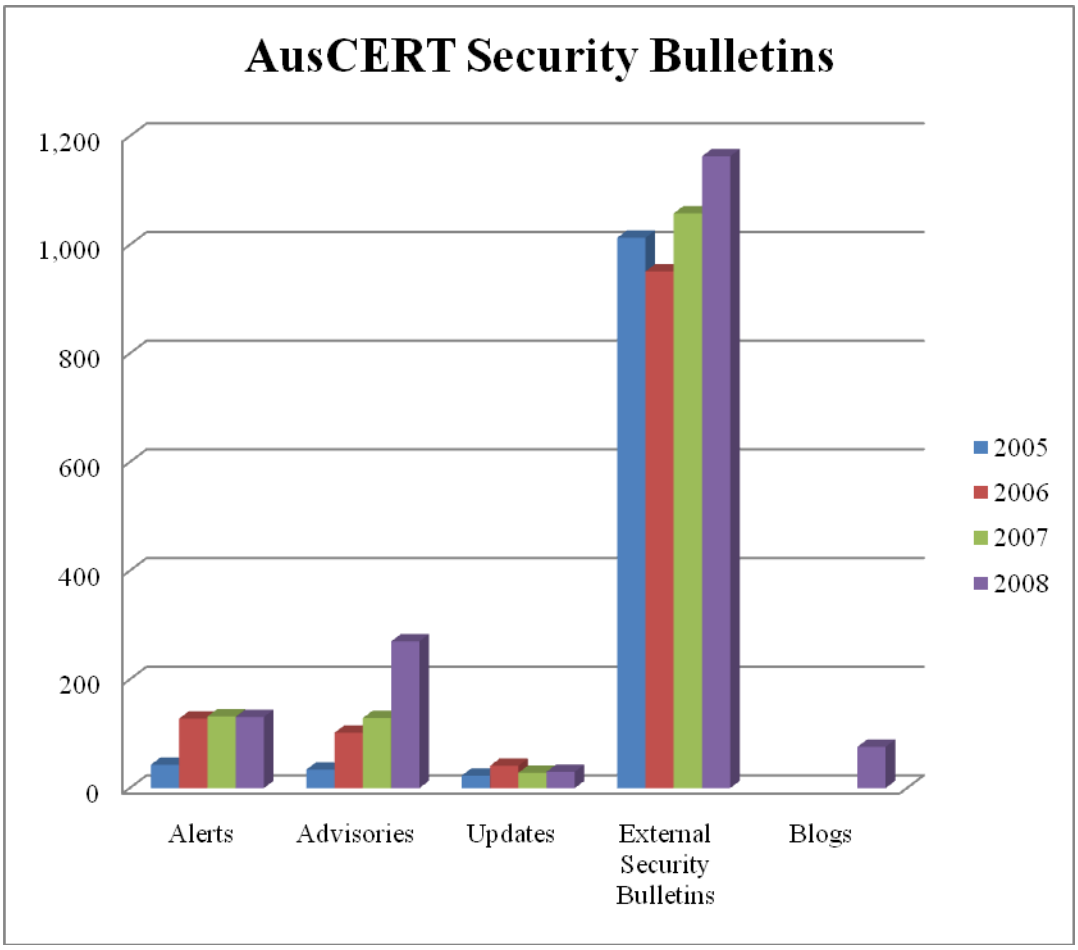


Figure 3

2.3. Network monitoring

AusCERT is collaborating with a number of partners operating monitoring projects, by hosting sensors.

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. 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 developing the first two components of this project.

AusCERT's ability to include its root certificate into major vendors' browsers coupled with the deployment of a public key infrastructure for the AAF is looking at reducing the barriers to increased use of PKI in the higher education and research sector 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, eg, for access to sensitive/expensive resources and secure email
- Quality validation services eg, OCSP support

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

2.6. New Services

AusCERT Remote Monitoring (ARM)

In 2008 AusCERT launched the AusCERT Remote Monitoring (ARM) service. The ARM service is available to AusCERT members only and provides a mechanism for them to remotely monitor their publicly accessible systems and services for unexpected events such as system failure or compromise. Members may configure the service to perform standard ICMP and TCP tests for host and service connectivity, as well as security-specific tests for web defacement and DNS compromise. Reporting is by SMS and email.

Stay Smart Online Alert Service

In June 2008 AusCERT commenced a new service under contract from the Australian government, which is part of the government's broader Stay Smart Online initiative[3]. The Stay Smart Online Alert Service is a free service aimed at home users and SMEs with little or no technical knowledge. The service provides access to email, web and RSS feeds and includes a monthly newsletter and fact sheets[4].

3. Events organized / co-organized

3.1. Training

AusCERT provided a series of public "hands on" workshops for Australian and New Zealand security professionals (including AusCERT members) throughout 2008, including Information Security Management workshops held in Brisbane, Perth, Adelaide, Auckland, Melbourne, Canberra and Sydney.

AusCERT also focussed recently on engaging with local industry groups in Australia including the Australian Computer Society and on educating Australian secondary schools.

AusCERT prepared consumer security advice and participated in the Australian government's Stay Smart Online Awareness week, coordinated by the Department of Broadband, Communications and the Digital Economy.

3.2. Drills

In December 2008, APCERT ran its annual security exercise based on a fictional scenario involving 14 teams across 13 Asia Pacific economies. AusCERT helped organise the running of the drill and participated in the drill exercise as responders.

3.3. Conferences

AusCERT held its annual Asia-Pacific Information Security Conference at the Gold Coast Australia in May 2008 with over 1,000 delegates[5]. The conference continues to show itself to be the premier information security conference in Australia and the southern hemisphere conducted by information security

[3] www.staysmartonline.gov.au

[4] www.ssoalertservice.net.au

[5] conference.auscert.org.au/conf2008/

professionals for information security professionals, IT managers and government decision makers in the field.

Coinciding with the annual AusCERT conference, AusCERT also hosts other networking and information sharing events. For example, AusCERT 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 experts with particular insight into the problems to share their knowledge and experience with those who have the ability to help address the problems.

Computer Security Day is an international event to raise awareness of computer security issues. To mark Computer Security Day in 2008, AusCERT organised a non-profit event in Brisbane.

During 2008, AusCERT participated in a number of international conferences and events, including:

- Digital Phishnet, Singapore
- APCERT2008, Hong Kong
- CyberStorm International Cyber Security Exercise
- FIRST annual conference and technical colloquium
- GovCERT.nl annual conference
- AP*
- CERT-FI seminar
- APEC-Tel Stability and Security Committee meetings

4. Achievements

4.1. Presentations

AusCERT has given presentations at several conferences throughout 2008. These include presentations at PICISOC's PacINET conference in the Cook Islands, APEC-Tel, the Botnet Taskforce and NATO training and several workshops within Australia 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

Last year, AusCERT reported on its role in providing content and technical expertise for the OECD's paper on malware, Malicious Software (Malware) - A Threat to the Internet Economy. At the time, the paper was not yet released but is now available[6]. 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.

During 2008, conducted and published the AusCERT Home Users Computer Security Survey 2008[7] and made a submission to the Australian government's e-security review[8].

5. International Collaboration

AusCERT continues to be actively involved with APCERT, serving on the Steering Committee again during 2008. AusCERT also manages the APCERT mailing lists and restricted web access to the APCERT Point of Contacts.
AusCERT also works closely with 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] http://www.oecd.org/dataoecd/53/34/40724457.pdf

[7] http://www.auscert.org.au/usersurvey

[8] https://www.auscert.org.au/9771

2. BKIS Activity Report 2008

Bach Khoa Internetwork Security Center

1. About Bkis – Vietnam

Bkis - Bach Khoa Internetwok Security Center is a Vietnam's leading Center in reseaching, 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 member of APCERT in 2003.

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

2. Activities & Operations

Security Statistic

Computer Virus 2008 (in Vietnam)	Quatity
Number of computers infected viruses	59,450,000
Number of new viruses appear in 2008	33,137
Number of new viruses per day	90.78 new viruses / day
The most infected virus: **W32.SecretW.Worm**	Infect 420.000 computers
Security 2008 (in Vietnam)	**Quatity**
Obsered by Bkis:	
Number of websites hacked by Vietnamese hackers	210
Number of websites hacked by International hackers	251
Summary	**461**
Vulnerability Report:	
Number of important websites Bkis reports vulnerability	**104**

Top 15 viruses in 2008 in Vietnam

No	Virus
1	W32.SecretW.Worm
2	X97M.XFSic
3	W32.VetorL.PE
4	W32.SeekmoOE.Adware
5	W32.VomoC.PE
6	W32.ZhaouCam.Trojan
7	W32.SCkeylogA.Trojan
8	W32.ZangoSOE.Worm
9	W32.ShopperHT.Adware
10	W32.DashferHtml.PE
11	W32.StarwareG.Adware
12	W32.CSSExploit.Trojan
13	W32.AcLuC.PE
14	W32.EncryptVBS.Worm
15	W32.HackerOnlineN.Worm

Publishing

Objects	Quatity
Security News	12 for 12 months in 2008
Security Articles	70 for magazines
Security Advisory	60

Noticeable Activities

Noticeable Activities
Participate in APCERT Drill 2007, taking on the scenario of an attack during the Beijing 2008 Olympic Games
Give paper presentation at Bellua Cyber Security Asia 2008 in Indonesia.
Detect and disclose vulnerabilities in: Windows Media Encoder, Google Chromes and Face Recognition Technology used by Asus, Lenovo, Toshiba …
Training Security Essential for more than 90 leading engineers and managers of many large Companies and Corporations.

3. CERT-In Activity Report 2008

The Indian Computer Emergency Response Team

1. About CERT-In

1.1. Introduction

CERT-In is a functional organisation of Department of Information Technology, Ministry of Communications and Information Technology, Government of India, with the objective of securing Indian cyber space. CERT-In provides Incident Prevention and Response services as well as Security Quality Management Services.

1.2. Establishment

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. Activities & 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 2008 is given in the following table:

Activities	Year 2008
Security Incidents handled	2565
Security Alerts issued	49
Advisories Published	76
Vulnerability Notes Published	197
Security Guidelines Published	1
White papers Published	1
Trainings Organized	18
Indian Website Defacements tracked	5475
Open Proxy Servers tracked	2332
Bot Infected Systems tracked	146891

Table 1. CERT-In Activities during year 2008

2.2. Cyber Security Assurance Framework

CERT-In has taken steps to implement National Information Security Assurance Programme (NISAP) to create awareness in government and critical sector organisations and to develop and implement information security policy and information security best practices based on ISO/IEC 27001 for protection of their infrastructure. For communicating with these organisations, CERT-In maintains a comprehensive database of more than 800 Point-of Contacts (PoC) and Chief Information Security Officers (CISO). As a proactive measure, CERT-In has also empanelled 76 information security auditing organisations to carry out information security audit, including the vulnerability assessment and penetration test of the networked infrastructure of government and critical sector organisations. The technical competency of the empanelled orgnanisations is regularly reviewed by CERT-In with the help of a test network.

CERT-In plays the role of mother CERT and is regularly interacting with the cyber security officers of sectorial CERTs in Defense, Finance and other sectors to advise them in the matters related to cyber security.

To facilitate its tasks, CERT-In has collaboration arrangements with IT product vendors, security vendors and Industry in the country and abroad. Security Cooperation agreements and MoUs have been signed with Microsoft, RedHat, Cisco, EMC2, eBay, Trend Micro, Symantec, Quickheal, Radware, McAfee and Afilias. This collaboration facilitates exchange of information on vulnerabilities in relevant products, developing suitable countermeasures to protect these systems and providing training on latest products and technologies.

2.3. Incident Handling Reports

2.3.1. Summary of Computer Security Incidents handled by CERT-In during 2008

In the year 2008, CERT-In handled more than 2500 incidents. The types of incidents handled were mostly of Phishing, Malicious Code, Website compromise & propagation of malware and Network Scanning & Probing.
The year-wise summary of various types of incidents handled is given below:

Security Incidents	2004	2005	2006	2007	2008
Phishing	3	101	339	392	604
Network Scanning / Probing	11	40	177	223	265
Virus / Malicious Code	5	95	19	358	408
Spam	-	-	-	-	305
Website Compromise & Malware Propagation	-	-	-	-	835
Denial of Service	-	-	-	-	54
Others	4	18	17	264	94
Total	**23**	**254**	**552**	**1237**	**2565**

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.

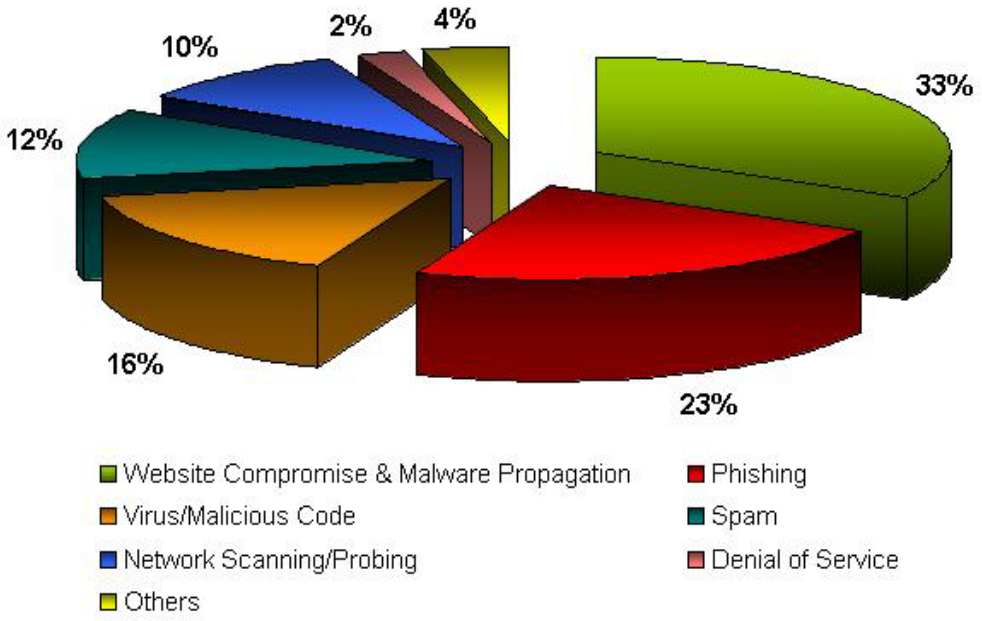


Figure 1. Summary of incidents handled by CERT-In during 2008

2.3.3. Incident Trends

CERT-In has observed many new innovative attack trends during 2008. The prominent types of attacks were malware propagation through compromised websites. Attackers exploited Web application vulnerabilities, especially SQL injection, to compromise websites and inject iFrame and Javascript links to

malicious websites to propagate malware through drive by downloads. Toolkits such as mPack, Neosploit, Random JS CuteQQ, AdM, FirePack, were actively used in these attacks.

Many incidents of mass scale SQL injection on websites running ASP were reported since March 2008. Subsequently the ASPROX botnet actively compromised many websites through SQL injection and redirected users of these websites to malicious domains hosted on Fastflux DNS. Similarly rise in exploitation of Cross site scripting and Remote File Inclusion (RFI) attacks to exploit vulnerabilities in PHP were also observed.

There has been a massive increase in the number of Trojans such as 'Trojan.FakeAV.Winfixer' pretending to be Antivirus products known as "scareware".

Malware was also propagated using various social engineering techniques through malicious .doc, pdf , codec files , autorun methods, and spamming of popular news items.

CERT-In handled various cases of information theft through Trojans such as WOW, Hupigun, Nethell, Zbot, affecting users of online transactions.

Many incidents of propagation of Conficker worm exploiting Microsoft Windows Server Service vulnerability (MS08-067) were reported.

CERT-In has observed different types of spam such as Image-based, Animated GIF, PDF spam, Spam messages containing complicated HTML frameworks that intersperse random characters between the actual spam text.

The phishing attacks reported in 2008 were primarily carried out against Financial services and e-commerce sector. While phishing attacks on Financial services sector accounted for 59% of the total phishing attacks, the second most targeted sector is E-Commerce sector which accounts for 37% of the total number. The phishing incidents affecting Indian Financial Institutions were around 36% of total phishing incidents reported, while remaining incidents were

affecting brands of other countries. Further, domain phishing incidents through Registrar impersonation were also reported.

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 organizations. In all 5475 numbers of defacements have been tracked. Most of the defacements were done for the websites under .in domain. In total 3042 .in domain websites were defaced.

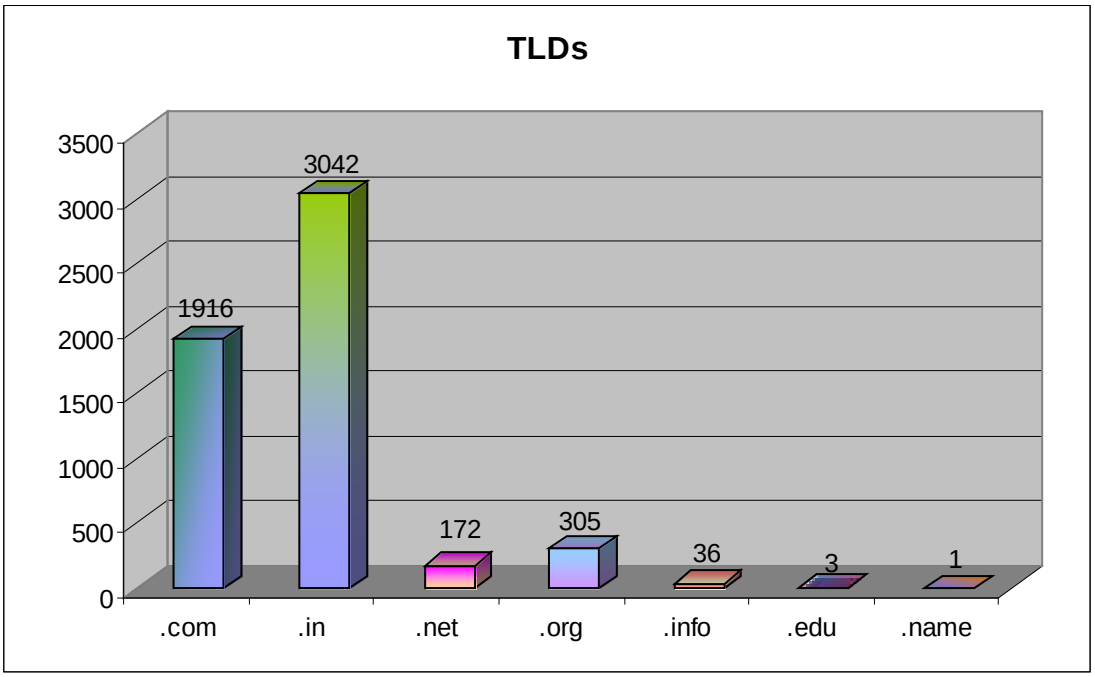


Figure 2. Indian websites defaced during 2008 (Top level domains)

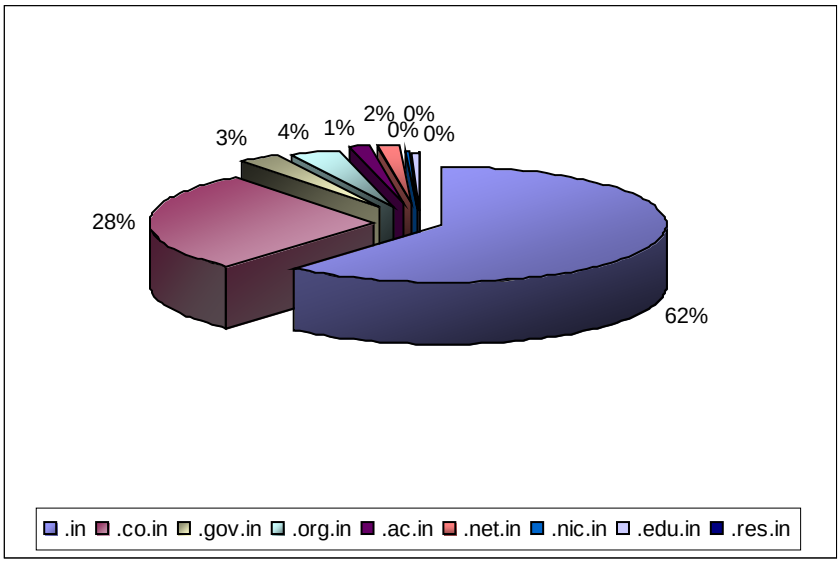


Figure 2.1 .in ccTLD defacements during 2008

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 2332 open proxy servers were tracked in the year 2008. The month-wise distribution of open proxy servers tracked during this year is shown in the figure 3.

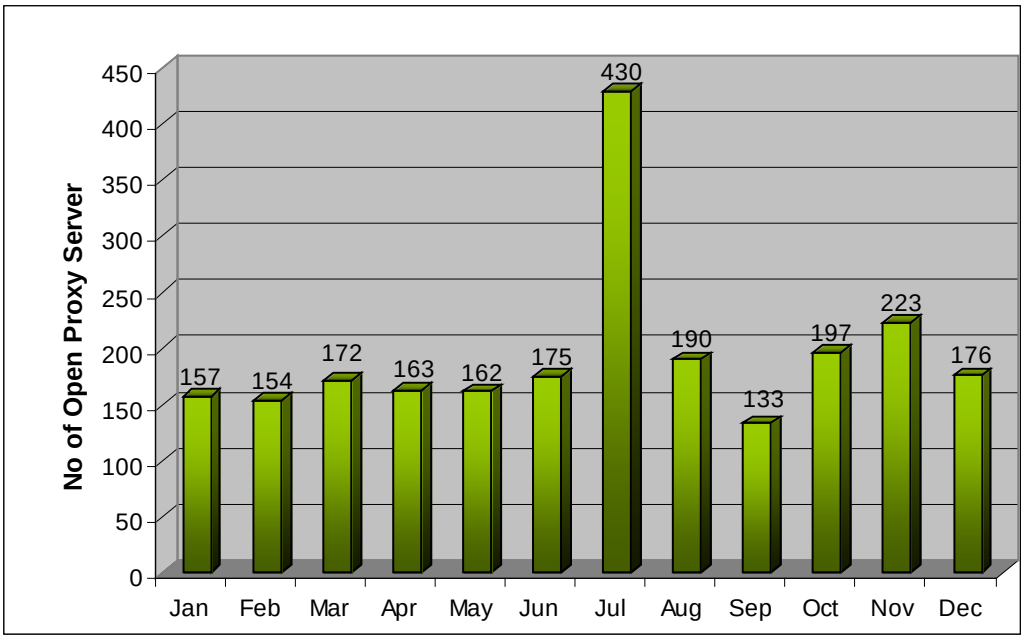


Figure 3. Monthly statistics of Open Proxy Servers in 2008

2.4.3. Botnet Tracking and Mitigation

CERT-In is tracking Bots and Botnets involving Indian systems. After tracking the IP addresses of Command and Control servers and Bots operating within India, actions are being taken to clean the respective systems and prevent malicious activities. Figure 4 shows the number of Bot infected systems and Command & Control servers tracked in 2008.

Month	Number of Bot Infected Systems	C&C Servers
January	2102	2
February	1279	10
March	15160	19
April	8514	14
May	6182	12
June	5537	13
July	74753	2
August	7055	3
September	5903	4
October	5219	3
November	6435	2
December	8866	4

Figure 4. Botnet statistics in 2008

3. Events organized / co-organized

3.1. Education and Training

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

workshops apart from CERT-In staff. CERT-In has conducted the following training programmes during 2008.

- Workshop on "Mail Server Security" on 29th January, 2008
- Workshop on "Implementation of Information Security Management in Government & Critical Sector Organizations" on 12th February, 2008
- Workshop on "Database Security and Auditing" on 28th March, 2008
- "Consumer Information Security Awareness Week" during 1-7 May 2008 jointly organised with Confederation of Indian Industry
- Workshop on "Computer Forensics for System Administrators" on May 07, 2008
- Workshop on "Network Security" on 25th June, 2008
- Workshop on "Windows Web Server Security" on 26th June, 2008
- Workshop on "Linux Security" on 31st July, 2008
- Workshop on "DNSSEC in India" on 18th August, 2008
- Workshop on "Web Application Security" on 21st August, 2008
- Workshop on "Cryptographic Primitives" on 29th August, 2008
- Workshop on "Cyber Security: Latest Attack Methods" on 04th September, 2008
- Workshop on "Intrusion Prevention System Technology" on 05th September, 2008
- Workshop on "Wireless Security" on 29th September, 2008
- Workshop on "Information Security Best Practices and Compliance" on 30th September, 2008
- Workshop on "Information Security-Risk Management and Business Continuity Management" on 27th November, 2008

- Workshop on "Identity Theft and Access Management" on 14th November, 2008
- Workshop on "Crimeware and Financial Frauds" on 5th November, 2008

- "Cyber Security Awareness Program" jointly organised with Data Security Council of India during 10-12 November 2008
- Workshop on "Managing Organization's Network Security" on 16th December, 2008

3.2. Forums

CERT-In, Department of Information Technology and Confederation of Indian Industry (CII) have established the Information Security Advisory Forum to foster cooperation between government, industry, consumer and law enforcement agencies on information security issues. As part of its many activities the Forum organizes Conferences, Training and Awareness Programs for the internet consumers (that include children, parents and teachers) who are often susceptible to cyber attacks, and aims to provide tools and resources to counter such threats.

CERT-In is collaborating with National Association of Software & Service Companies (NASSCOM) and Data Security Council of India to spread the cyber security awareness and facilitate interaction with various user groups.

4. 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 Lyon, France in February 2008
- Digital Phishnet Conference held in San Diego, USA in September 2008
- Internet Governance Forum meeting held in Hyderabad, India in December 2008
- Association of Antivirus Asia Researchers (AVAR) Conference held in New Delhi, India in December 2008

4.2. Publications

The following papers were published by CERT-In in the year 2008:

1. Whitepaper "Analysis of Phishing Incidents year-2007" CIWP-2008-01
2. This document provides analysis of phishing incidents reported to CERT-In during the year 2007. 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.
3. Guidelines for Auditing and Logging (CISG-2008-01)
4. This guideline attempts to provide some insights into the issues related to Auditing and Log Management and suggest best practices for enabling

and maintaining Auditing and logging on Windows hosts, Linux hosts, Microsoft IIS Web server, Apache Web server, Oracle 10g Database Server and Microsoft SQL Server 2005. Implementation of these best practices will enable administrators to acquire vital information to identify and respond to the computer security incidents.

5. Case study "Website compromise and launch of further attacks by exploiting PHP Remote File Inclusion vulnerability" (CICS-2008-01)
6. The case study provides analysis of the attack and identified vulnerabilities which were exploited to compromise the website. It also provides appropriate countermeasures to secure webserver and web applications from such type of attacks.
7. Case study "Website compromise and launch of further attacks by exploiting SQL injection vulnerability" (CICS-2008-02)
8. This case study provides analysis of mass scale SQL Injection attacks used to compromise websites and inject Javascript links to malicious websites.
9. Paper titled "Propagation of malware through compromised websites: Attack trends and countermeasures" (11th International AVAR Conference, New Delhi, India)
10. This paper attempts to examine the current trends in malware propagation and functionalities of large scale botnets such as operating Fast Flux DNS, hosting of malicious websites and injecting malicous links on legitimate websites. Various types of attacks on Indian websites, observed by CERT-In are examined. Typical attack scenarios are discussed in detail. The mitigation of these threats demands greater cooperation among various agencies such as CERTs, Security vendors, ISPs, Domain Registrars. Ways and means of such cooperation are explored.

4.3. Awards

A staff member of CERT-In Mr. Madhur Verma was awarded as "Most Valuable Professional" in the area of Consumer Security by Microsoft in December 2008.

5. 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 member of FIRST since December 2006. CERT-In has become full member of Asia Pacific CERT (APCERT) since August,

2008. CERT-In has become Research Partner of Anti-Phishing Working Group (APWG) in May 2008.

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. Members of CERT-In visited Mauritius for setting up of CERT-MU in Mauritius and provided training on CERT operations to technical staff of CERT-Mauritius. CERT-MU has been operationalised and launched in May 2008.

5.2. Drills

- CERT-In participated in the ASEAN CERTs Incident Handling Drill (ACID 2008) held on 30th July 2008.
- CERT-In participated in the APCERT International Incident Handling Drill 2008 held on 4th December, 2008.

6. Future Plans/Projects

CERT-In has been evolved as the most trusted referral agency in the area of information security in the country. CERT-In is regularly interacting with CISOs of Critical Infrastructure Organisations and sectorial CERTs to ensure security of the critical systems, collaboration with IT product and security vendors to mitigate the vulnerabilities in various systems, cooperation with international CERTs and security organizations on information sharing and incident response, promote R&D activities in the areas of Artifact analysis and Cyber Forensics and security training and awareness. CERT-In is implementing a project for Attack Detection and Threat Assessment at ISP and organisation level. This project will enable detection of cyber threats and attacks and issuance of early warning to take appropriate countermeasures to mitigate the attacks and contain the damage.

4. CNCERT/CC Activity Report 2008

National Computer Network Emergency Response Technical Team / Coordination Center

- China

1. About CNCERT/CC

1.1. Introduction

CNCERT/CC is a National level CERT organization, which is responsible for the coordination of activities among all Computer Emergency Response Teams within China concerning incidents in national public networks.

1.2. 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.

1.3. 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.

1.4. 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. Activities & Operations

2.1. Incident Reports

In 2008, CNCERT/CC received 5,167 incidents reports (excluding scanning attacks) from domestic and international users and agencies.

Most incident reports were about spam mail (1,849), phishing (1,256) and webpage embedded malicious code (1,227). The reports of these 3 types of incident were increased by 54.5%, -5.3% and 6.6% compared with that of last year respectively.

2.2. Incident Handling

In 2008, CNCERT/CC handled 1,173 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 5 applications of TCP traffic are among HTTP, P2P and email.

TCP Port	Rank	Percentage	Applications
80	1	28.36%	HTTP
8080	2	1.00%	HTTP
4662	3	0.93%	eMule
443	4	0.80%	Https
25	5	0.60%	SMTP
554	6	0.25%	RTSP
3128	7	0.23%	HTTP
8000	8	0.18%	QQ IM
1863	9	0.18%	MSN Messenger
6881	10	0.10%	BitTorrent

Table 1 TCP Traffic Top 10 in 2008

The top 3 applications of UDP traffic are Xunlei, QQ and QQ IM (Instant Messenger).

UDP Port	Rank	Percentage	Applications
15000	1	3.70%	Xunlei (downloader)
29909	2	1.02%	QQ(downloader)
8000	3	0.94%	QQ IM
80	4	0.84%	Http
53	5	0.74%	DNS
1026	6	0.65%	MSN Messenger
7100	7	0.63%	Online Game
6881	8	0.63%	BitTorrent
1027	9	0.49%	MSN Messenger
4672	10	0.42%	eMule

Table 2 UDP Traffic Top 10 in Year 2008

Trojan & Botnet Monitoring

In 2008, CNCERT/CC monitored some popular Trojans and discovered 565,605 IP addresses of computers embedded with Trojans in Chinese mainland, which decreased by 43.2% compared with that of year 2007.

CNCERT/CC also kept on monitoring Botnet activities for a long time. In 2008, CNCERT/CC discovered over 1,237,043 IP addresses of computers embedded with Botnet clients in Chinese mainland. Meanwhile, 5,210 Botnet servers outside of Chinese mainland were discovered controlling Botnet clients in Chinese mainland. Among these Botnet servers, about 31% were in the United States, 10% in Hungary and 5% in South Korea.

Among ports used by Botnet based on IRC application, the top 3 ports are 6667 (41.39%), 8080 (3.64%) and 1863 (3.17%).

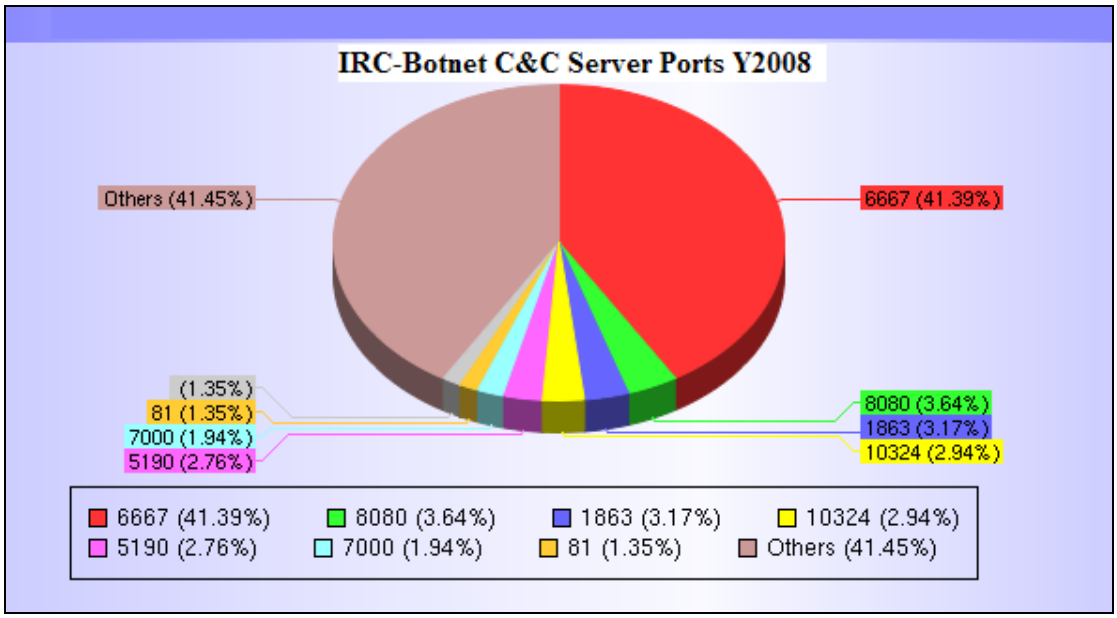


Figure 1 IRC-Botnet C&C Server Ports Year 2008

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 2008, CNCERT/CC discovered totally 53,917 defaced websites in Chinese mainland, which is decreasing slightly compared with that of year 2007. According to monitoring data, the governmental websites seem to be much easier to be attacked due to their weak protection measures and maintenance.

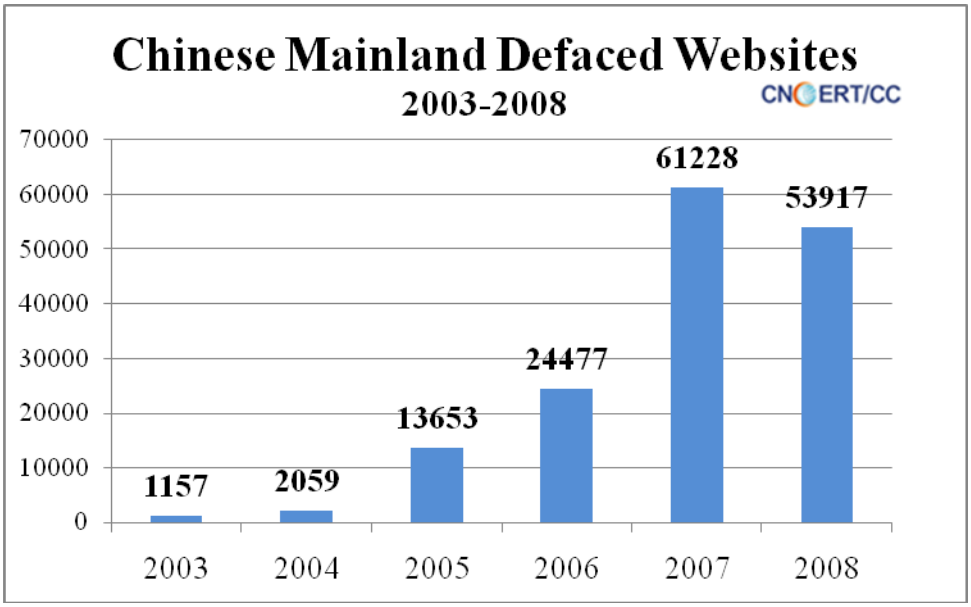


Figure 2 Chinese Mainland Defaced Websites Y2003-2008

Phishing Handling

In 2008, CNCERT/CC received 1,256 phishing reports and resolved 320 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
eBay	248
ACK CYFRONET AGH	125
HSBC	120
Mark Monitor	61
RSA Cyota	48

Table 3 Top 5 Phishing Reporters to CNCERT/CC in Year 2008

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 4,488 in 2008.

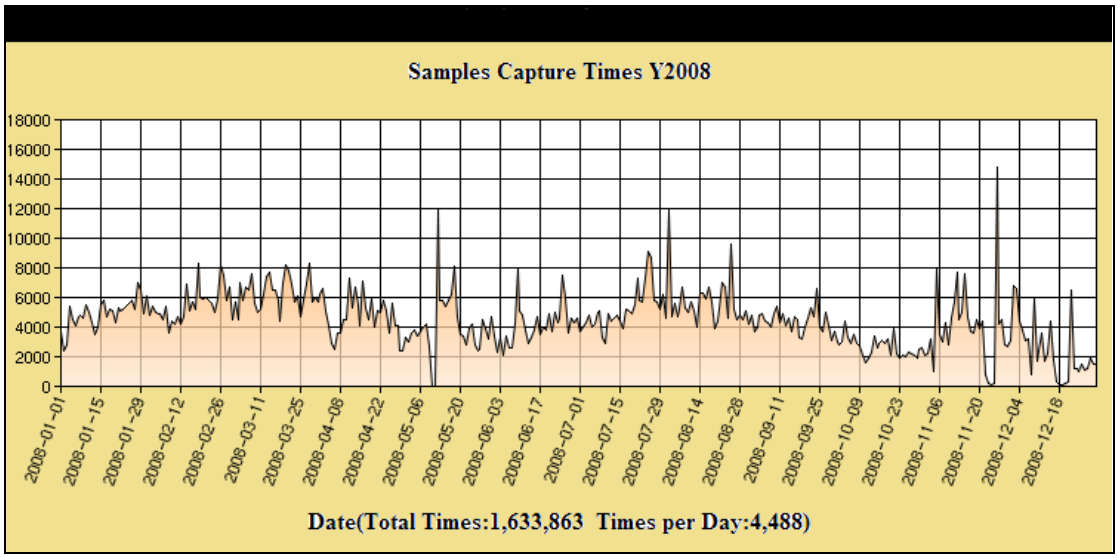


Figure 3 Samples Capturing Times Status

According to the data, the average number of new samples captured everyday is 427. That means new malicious codes were emerging endlessly.

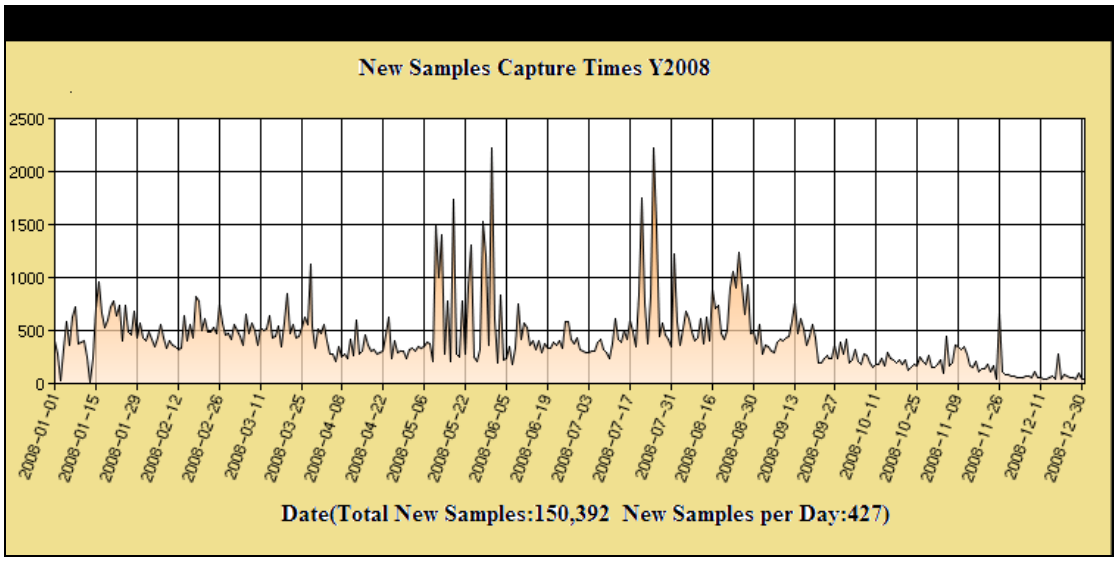


Figure 4 Number of Samples Captured Status

In 2008, 150,392 samples had been captured by CNCERT/CC's honeynet.

Rank	Malicious Code Name	Times of being Captured
1	Virus.Win32.Virut.n	111584
2	Backdoor.Win32.VanBot.ax	62219
3	Net-Worm.Win32.Allaple.b	48933
4	Trojan.Win32.Obfuscated.gen	43411
5	Backdoor.Win32.Nepoe.em	37284
6	Net-Worm.Win32.Allaple.e	27520
7	Backdoor.Win32.Rbot.bqj	24781
8	Porn-Dialer.Win32.InstantAccess.dan	24649
9	Trojan-Downloader.VBS.Small.gg	22216
10	Trojan.Win32.Qhost.aei	22153

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 2008, 101 internal warnings and 4 critical vulnerability advisories had been delivered in time.

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

3. Events organized / co-organized

Anti-Botnet Seminar

The Seminar was held in Beijing on 23rd January 2008. Delegates came from governments, security research organizations, vendors and end users. The topic is to exchange information regarding to the threat and the trend of Botnet, share best practices and main difficulties, and discuss how to combat Botnet from the technical, regulatory, legal and other aspects.

APEC-TEL37 Anti-Botnet Workshop

The workshop was held on 23rd March 2008 at APEC-TEL37 in Tokyo. 12 experts gave the presentations to share their experiences and skills regarding to Botnet. The workshop provided an atmosphere that encourages the sharing of knowledge and experiences of effective solutions for preventing, detecting and controlling botnets.

CNCERT/CC 2008 Annual Conference

The Conference was held in Shenzhen from 7th to 9th April 2008. About 300 delegates from 12 countries and regions attended the conference.

CNCERT Cyber-security Training Camp

The training camp was held on 8th to 9th May 2008 in Beijing assisted by Microsoft. This activity invited about 30 trainees from critical information infrastructures and backbone ISPs to learn Windows OS enhanced security technologies, network attack technologies and tools, hacking habits, and network security attack and defense drills in simulated scenarios.

Accreditation for Domestic Qualification of Information Security Service Provider

CNCERT/CC completed the authorization for Domestic Qualification of Information Security Service Provider in June 2008, co-sponsored by China Information Security Certification Center (ISCCC).

Internet Security Work during Beijing 2008 Olympic Games

In cooperation with other relevant government departments and ISPs, the network of China mainland during the Beijing 2008 Olympic Games was running well smoothly with no major security incidents. CNCERT/CC completed the network security mission successfully.

4. Achievements

4.1. Presentations

Matrix, a Distributed Honeynet and its Applications, APCERT 2008 Annual Conference, 2008.3.10-12, Hong Kong China

Botnet Mitigation Practice in China, Anti-Botnet Workshop in APEC-TEL37, 2008.3.23, Japan

Matrix, a Distributed Honeynet and its Applications, Annual FIRST Conference 2008, 2008.6.22-27, Canada

Malicious Websites on the Chinese Web: Overview and Case Study, Annual FIRST Conference 2008, 2008.6.22-27, Canada.

Final Report of Anti-Botnet Report, APEC-TEL38, 2008.10.16, Peru

4.2. Publications

Best Practices & Guides on Network Security Emergency Response (in Chinese, ISBN: 978-7-121-06194-3), published and issued in March, 2008

Guide on Policy and Technical Approaches against Botnet, publicized on APEC Website in Dec. 2008

12 monthly newsletters, 1 semiyearly special (in Chinese) for high-end users in 2008

5. International Collaboration

5.1. Conference and Events

APCERT 2008 Annual Conference

CNCERT/CC delegation attended APCERT annual conference in Hong Kong and was elected as the deputy chair of APCERT again.

ACID III 2008

CNCERT/CC participated in ACID III on 30th July 2008.

APCERT Drill 2008

CNCERT/CC participated in APCERT incident handling drill on 4th December 2008.

6. Future Plans

CNCERT/CC completed the Internet security mission during the Beijing 2008 Olympic Games successfully. In the approaching 2009, CNCERT will continue to enhance its own capability of network monitoring, warning and handling as a national Computer Emergency Response Team. Therefore, we expect to keep a stronger collaboration with APCERT members

7. Conclusion

In 2008, 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. Before the Beijing 2008 Olympic Games, CNCERT/CC took two special actions to restrain the increasing security risks and threats of Botnet and Trojan in cooperation with other government departments and ISPs. The actions play an important role in the healthy internet environment in China. Importantly, CNCERT/CC got much supports from the collaboration with CERTs community from all over the world to prevent and mitigate the impact of cyber threat in 2008.

5. HKCERT Activity Report 2008

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

1. About HKCERT

1.1. Introduction

1.1.1. Establishment

Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) was established in 2001 with funding from the Hong Kong SAR Government. The Hong Kong Productivity Council (HKPC), which is a government subvented organization in Hong Kong, has operated the centre since then.

1.1.2. Mission and Constituency

HKCERT is the centre of coordination of computer security incident response for local enterprises and Internet users in Hong Kong. Her missions are to facilitate information dissemination, to provide advices on preventive measures against security threats, to provide information security awareness, and to maintain network with other computer emergency response team (CERT) organisation to facilitate cooperation and coordination.

1.1.3. Workforce power

The centre is managed by the Centre Manager. Two consultants and a security operation team take care of the daily operations.

2. Activities & Operations

2.1. Incident Handling Statistics

During the period from January to December of 2008, HKCERT had handled 1255 incidents, including 322 virus incidents, 922 security incidents and 11 other incidents. Security incident reports continue to overtake virus incident reports (See Figure 1).

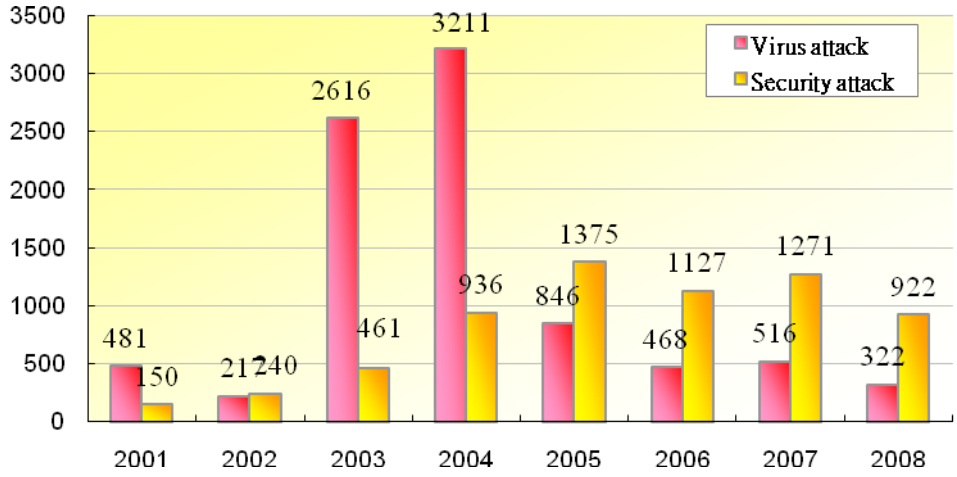


Figure 1. HKCERT Incident Reports in 2008

Analysis of Composition of security alerts

Further analysis of the partitioning of security incident indicates that the number of phishing cases that peaked in 2007 has dropped significantly. On the other hand other security incidents (active hacking, code injection, defacement, etc.) rose sharply (See Table.1.) . Among the 611 reported security incidents, code injection (31%) and web defacement (19%) accounted for half of them.

	2003	2004	2005	2006	2007	2008	
Other security incident repor	461	783	206	416	416	**611**	***(66%)***
Phishing Incident reports		73	211	434	745	232	*(25%)*
Spamming incident reports		80	82	47	32	29	*(3%)*
Spyware incident reports			876	230	78	50	*(5%)*
All security incident reports	**461**	**936**	**1375**	**1127**	**1271**	**922**	(100%)

Table 1. Distribution of HKCERT security incident reports in 2008

2.2. Alert statistics

During the period from January to December of 2008, HKCERT published 232 security alerts and no virus alert was published. The low figure in virus alert attributed to the disappearance of massive worm attack due to a change of strategies of attackers to stay stealthy.

2.3. Special Advisories and Press Briefings

HKCERT issued two special security advisories, one on code injection and another on DNS vulnerability.

- In July, Dan Kaminsky announced a critical DNS vulnerability that affects the Internet infrastructure as a whole. HKCERT released a detailed advisory and

issued targeted alert to local ISPs and Internet data centers. HKCERT monitored the patch progress of major ISPs to ensure they fix the security hole as soon as possible.

- After receiving 79 incidents of malware hosting in local website from April to July 2008, HKCERT issued a security advisory and called a press briefing in August, alerting the public that hackers are targeting web server using the SQL Injection exploit. We advised web server owners to evaluate the security of their web servers and the web applications running on them.
- HKCERT alerted the threat of Botnet in a joint press briefing in November 2008 with the Government and Police.

2.4. Miscellaneous

- KCERT continued to work closely with the government and law enforcement agency, and held meetings to exchange information and to organize joint events regularly;
- We participated in the government's Information Infrastructure Liaison Group and Information Security Task Force
- We worked closely with police in pinning down phishing web sites and command and control servers;

3. Events organized / co-organized

3.1. Seminars, Conference and Meetings

- KCERT hosted the APCERT Annual General Meeting and Conference in Hong Kong. The event was a success.
- There were 40 representatives from 16 member CERTs attending the AGM.
- There were 29 overseas partner organizations and guests joining, some were from long distance away, like Africa and UAE. There were 13 local strategic partners including Government, Police, domain name registries and ISP representatives attending the closed conference.
- For the public conference, there were 127 participants, including 46 from the overseas. The two workshops, one on SurfIDS and another on network security monitoring workshop had a full house.
- We jointly organized the Hong Kong Clean PC Day 2008 seminar with the Government and Police.
- We organized the Information Security Summit 2008 with other organizations and associations in November 2008, inviting local and international speakers to provide insights and updates to local corporate users.

3.2. Training

- We have assisted the organization of the technical training workshops of the Information Security Summit and coordinated two overseas experts to deliver hands-on workshops on Botnet Analysis and Security Visualization.

3.3. Drills

- We participated in the APCERT Drill on 3 December 2008 and prepared one of the scenarios for the drill. The drill was a great success.

4. Achievements

4.1. Speeches and Presentations

HKCERT was invited to deliver speeches and presentations on various occasions. We were also interviewed by the media from time to time to give objective and professional views on information security topics and incidents.

4.2. Publications

- We had published 12 issues of e-Newsletter and sent out alert summaries twice per month.
- We published several technical guidelines including SQL Injection Defense Guideline, Data Protection Guideline, Guideline for Safety Using Wireless LAN (updated) and "Autorun virus" Removal Procedure.

5. Collaboration

5.1. International Collaboration

HKCERT had participated in the following international collaborations:

- Joining the Microsoft Security Cooperation Program to share information.
- Representing APCERT in the Advisory Council of DotAsia
- Joining the Tsubame distributed honeypot project of JPCERT/CC
- Conducting Risk Assessment of APCERT IRC server
- Participating in the APCERT AGM and Conference in March
- Participating in the FIRST AGM and Conference in June and the Collaboration Meeting for CSIRT with National Responsibility organized by CERT/CC in July

5.2. Local Collaboration

HKCERT had participated in the following local collaborations:

- Collaborating with Government in the cyber security assurance of and Beijing Olympic Games Equestrian event (August) and Paralympics Games (September) in Hong Kong

- Collaboration with police on closing down bulletproof hosting in Hong Kong
- Collaboration with ISPs on closing down the DNS vulnerabilities

6. Future Plans

HKCERT has secured Government funding to provide the basic CERT services starting 2009. In 2009, we plan to organize a drill with the local ISPs and Domain Name Registries, and will start to enhance our capability in proactive security threat monitoring and malware analysis. We shall work with the government closely to plan for the future services of HKCERT.

7. Conclusion

HKCERT sees the year 2008 a fruitful year with many achievements. At the same time, we also see the security threats becoming more complex and more prominent. We shall continue to review and enhance our services and to develop stronger collaboration with local and global partners, including CERT teams around the world, and jointly combat cyber crimes in order to safeguard Internet as a viable platform for business and enjoyment.

6. JPCERT/CC Activity Report 2008

Japan Computer Emergency Response Team/Coordination Center – Japan

1. About JPCERT/CC

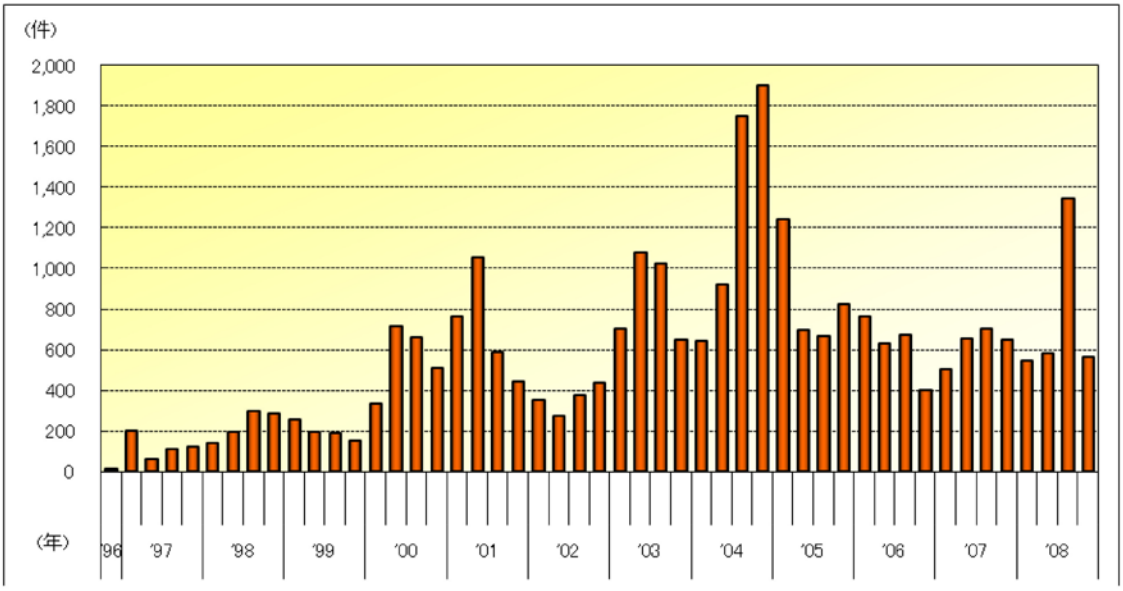
JPCERT/CC is the first CSIRT (Computer Emergency Response Team) established in Japan. It is an independent non-profit organization, acting as a national point of contact for the CSIRTs in Japan and worldwide. Since its inception in 1992, JPCERT/CC has been conducting incident handling operations, vulnerability handling operations, issuing security alerts and advisories to national critical infrastructures and to the wide public, engaging in threat analysis, organizing forums and seminars to raise awareness of security issues, and supporting the establishment/development of CSIRTs in Japan and overseas.

2. Activities & Operations

2.1. Incident Handling Statistics

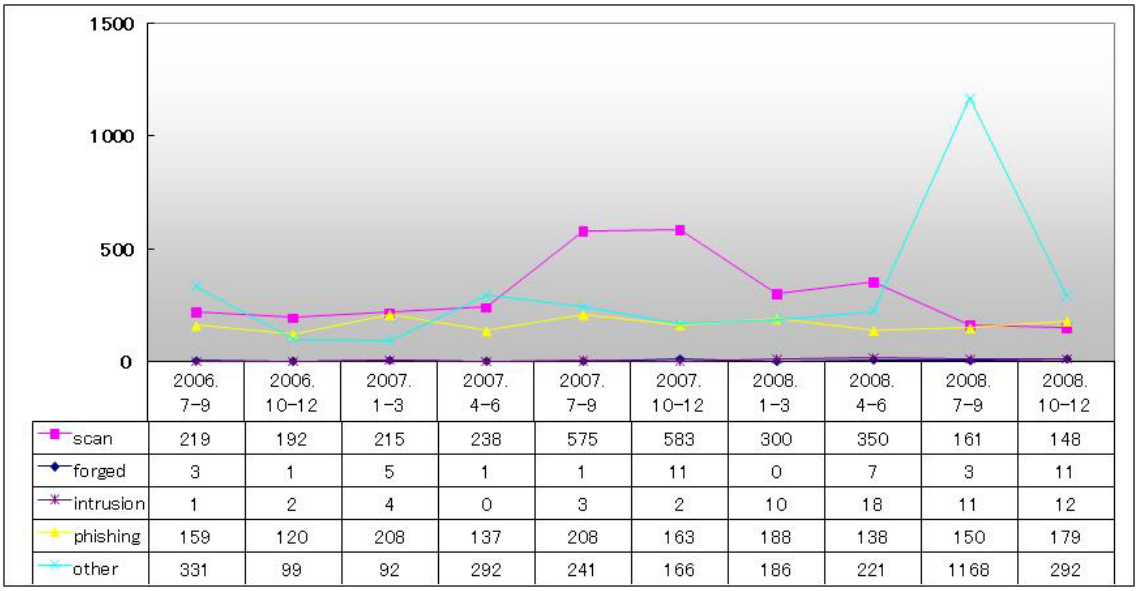
In 2008, JPCERT/CC received 4,016 reports on computer security incidents from Japan and overseas. A ticket number is assigned to each incident report to keep track of the development.

	1st Qtr	2nd Qtr	3rd Qtr	4th Qtr	Total
Incident Reports	545	768	1786	917	**4,016**



2.2. Abuse Statistics

1. scan (Probe, Scan, Other Suspicious Access) - 959 reports
2. forged (Forged Send Header E-mails) -21 reports
3. intrusion (System Intrusion) - 51 reports
4. phishing - 655 reports
5. other (DoS, computer virus, malware, etc.) - 1,867 reports



	2006. 7-9	2006. 10-12	2007. 1-3	2007. 4-6	2007. 7-9	2007. 10-12	2008. 1-3	2008. 4-6	2008. 7-9	2008. 10-12
scan	219	192	215	238	575	583	300	350	161	148
forged	3	1	5	1	1	11	0	7	3	11
intrusion	1	2	4	0	3	2	10	18	11	12
phishing	159	120	208	137	208	163	188	138	150	179
other	331	99	92	292	241	166	186	221	1168	292

2.3. Internet Scan Acquisition System (ISDAS)

http://www.jpcert.or.jp/isdas/index-en.html

The Internet Scan Data Acquisition System (ISDAS) is similar to weather stations for monitoring barometric pressure, temperature, and humidity. Instead of monitoring weather, the system monitors Internet traffics in Japan. The project began in November 2003 with the objective of improving Internet security by providing up-to-date graphs and reports gathered by ISDAS.

2.4. Japan Vulnerability Notes (JVN)

http://jvn.jp/en/

Japan Vulnerability Notes (JVN) is a vulnerability information portal site designed to help ensure Internet security by providing vulnerability information and their solutions for software products used in Japan, jointly operated by JPCERT/CC and the Information-technology Promotion Agency (IPA).

What information is available on JVN website?
JVN provides the description, solutions, and product developers' statements (including information on affected products, workarounds and solutions, such as updates and patches) on each vulnerability.
Vulnerabilities are security problems that may lead to loss of or decrease in functions or performance of software due to attacks such as computer viruses and unauthorized access to computers.

JPCERT/CC conducts vulnerability handling operations cooperatively with CERT/CC (http://www.cert.org/) and CPNI (http://www.cpni.gov.uk/).

In 2008, JPCERT/CC coordinated 168 vulnerabilities and published on JVN. Among them 79 cases were received from reporters in Japan. Furthermore, 87 cases were published in cooperation with CERT/CC, and 2 cases were published in cooperation with CPNI.

2.5. Anti-Bot Project

JPCERT/CC contributes to Anti-Bot operations in Japan by participating in the Cyber Clean Center (CCC) project - a joint project by the Ministry of Internal Affairs and Communications (MIC) and Ministry of Economy, Trade and Industry (METI).

JPCERT/CC serves as the Bot Program Analysis Group and analyzes malware, as well as develops disinfestation tools for infected users.

Cyber Clean Center (CCC)
https://www.ccc.go.jp/en_index.html

2.6. Security Industry Forum – SECOND

JPCERT/CC has established a forum called SECOND, with the objective to build a trust network among major players in the Japanese industry, and to cooperate in time of emergency. It provides an opportunity for security experts of major ISPs and vendors to meet regularly and exchange information on Internet security.

3. Events organized / co-organized

3.1. Training

JPCERT/CC offers trainings, seminars and workshops, for technical staffs, system administrators, network managers, etc., in the field of computer security. Some of the events organized or co-organized by JPCERT/CC in 2008 are as follows:

Critical Information Infrastructure Protection Security Seminar 2008 (20th February 2008)

A one day seminar co-organized by JPCERT/CC and Information-Technology Promotion Agency (IPA) for critical infrastructures

CSIRT Training (19th-26th March 2008)

Incident handling workshop for Bangladesh, Cambodia, Indonesia, Mongol, Philippines, Sri Lanka

C/C++ Secure Coding Twilight Seminar

A free seminar providing technical know-how on coding secure programs in C/C++ language

Security Day 2008 (16th December 2008)

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), to share the challenges of information security issues in Japan.

JPNIC, JPCERT/CC Security Seminar 2007 (16th December 2008)

A one day seminar co-organized by JPCERT/CC and Japan Network Information Center (JPNIC)

3.2. Drills

JPCERT/CC participated in the following drills:

1. ASEAN CERT Incident Drill (ACID) 2008, on 16th July 2008 (coordinated by SingCERT)

2. APCERT Drill 2008, on 4th December 2008 (coordinated by MyCERT and AusCERT)

4. Future Plans

TSUBAME (Internet Threat Monitoring Data Sharing Project)

TSUBAME project is to collect, share and analyze Internet traffic data, in order to understand the Internet threat situation in the Asia Pacific region. It places sensors widely in the region and collects/shares the data with all participating teams. TSUBAME project is aimed to establish a common platform to promote collaboration among CSIRTs in the Asia Pacific region.

5. International Collaboration

5.1. APCERT SC & Secetariat

JPCERT/CC supports the Internet security community in the Asia Pacific region by serving as a Steering Committee members and the Secretariat for APCERT.

5.2. FIRST (Forum of Incident Response and Security Teams)

http://www.first.org

JPCERT/CC supports the Internet security community in the world by serving as a Director and Steering Committee member of the FIRST organization, since 2005.

5.3. Standardization (ISO/IEC JTC1/SC27)

JPCERT/CC contributes to the standardization in two work items: Responsible Vulnerability Disclosure (RVD) and Information Security Incident Management (ISIM), which are developed in ISO/IEC JTC1/SC27.

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

7. KrCERT/CC Activity Report 2008

Korea Internet Security Center – Korea

1. About KrCERT/CC

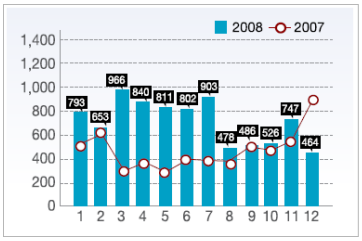
KrCERT/CC, also known as KISC, Korea Internet Security Center, serves as the nationwide Internet incident handling and coordination center in Korea, and is responsible for detecting, analyzing and responding all nationwide Internet incidents such as hacking, worm/virus, bot, phishing, and all other various Internet threats. 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. Internet Incident Statistics and Analysis

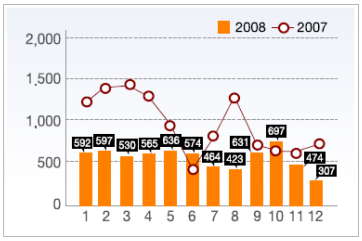
2.1. Overview

Internet incident reports received by the KrCERT/CC are categorized into worm/virus, hacking incident, and bot. Hacking incident has subcategories; spam relay, phishing[9] , intrusion attempt, webpage defacement, and other. The number of malicious code reported to KrCERT/CC in 2008 is 8,469, which is 41% increase compared with that of the last year (5,996 in 2007). The number of hacking incident reported to KrCERT/CC in 2008 is 15,940, which has 27% decrease compared with that of the last year (21,732 in 2007).

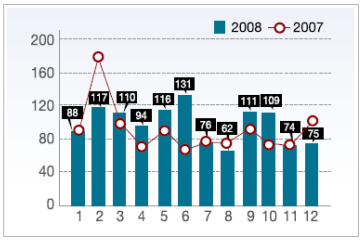
Worm/Virus



Spam Relay



Phishing Host

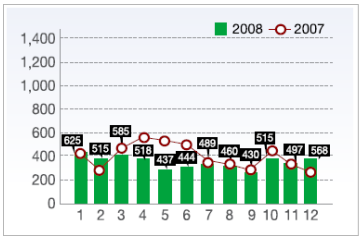


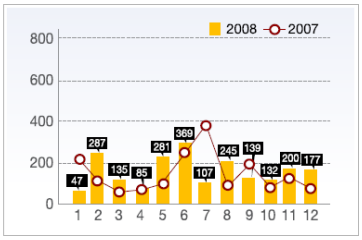
Intrusion + Other

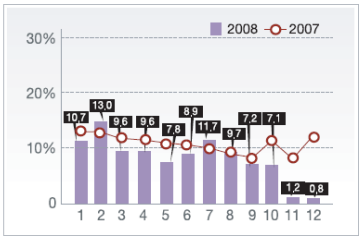
Web Defacement

Bot Infection

[9] Phishing targeting Korean brands is very rare; however, many Korean websites are abused as phishing host targeting foreign brands.







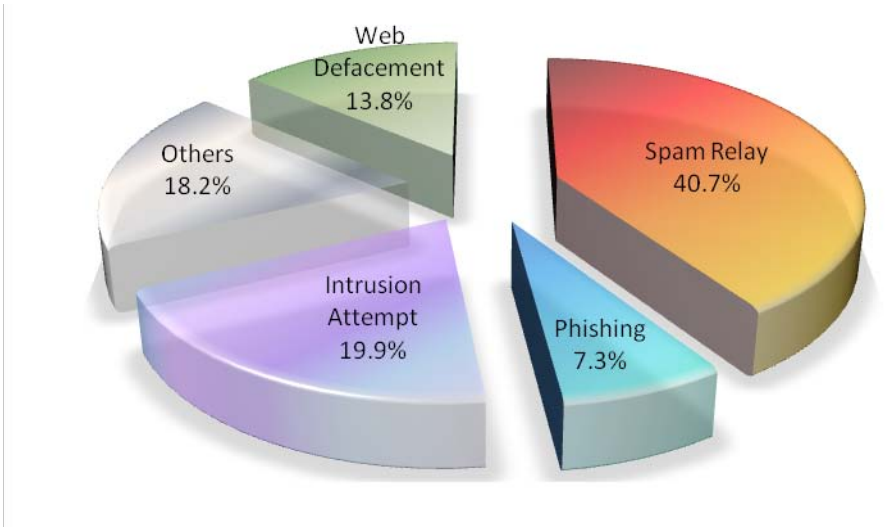
However, these figures do not necessarily imply that the damage caused by the malicious code and hacking incident is also increased or decreased. Current trend shows that the attacks are targeting more narrowed scope and specific victim rather than the anonymous majority, and the victims can be vary from individuals to corporations. Therefore, figuring out the overall damage caused by those incidents is getting more difficult, as the attacks are evolving in its aspect and methodology.

2.2. Worm/Virus

Throughout the year 2008, the number of worm/virus reported to KrCERT/CC is 8,469, which is 41.2% increase compared with that of the last year (5,996 in 2007). This is mainly due to the fact that we have seen the increase of the malware such as ONLINEGAMEHACK, KORGAMEHACK, which has been distributed for stealing credential information for using in certain online games. These malwares have been continuously increased that the number of cases was 1,060 in year 2007 and 1,895 in 2008.

2.3. Hacking Incident

The total number of reports on hacking incident in year 2008 is 15,940. Among the reports on hacking incident, spam relay (6,490) takes 40.7% and it has been decreased 44% than that of the year 2007 (11,668).



Internet incidents reported to KrCERT/CC in 2008

The number of Phishing hosts (1,163) is increased compared with that of the last year (1,095). The number of webpage defacement is 2,204 and others 2,908. The number of intrusion attempt (3,175) is decreased compared with that of the last year (4,316).

Simple and traditional hacking incidents such as webpage defacement, spam relay are decreasing, but takes quite a portion in the entire number of incidents, taking over a half together. On the other hand, phishing and others are increased, as the trend goes to seeking the financial gain, and it may reflect the fact that the attacks directly seeking the financial gain are increasing, and the attacks are getting diverse, making the traditional method of categorizing less meaningful.

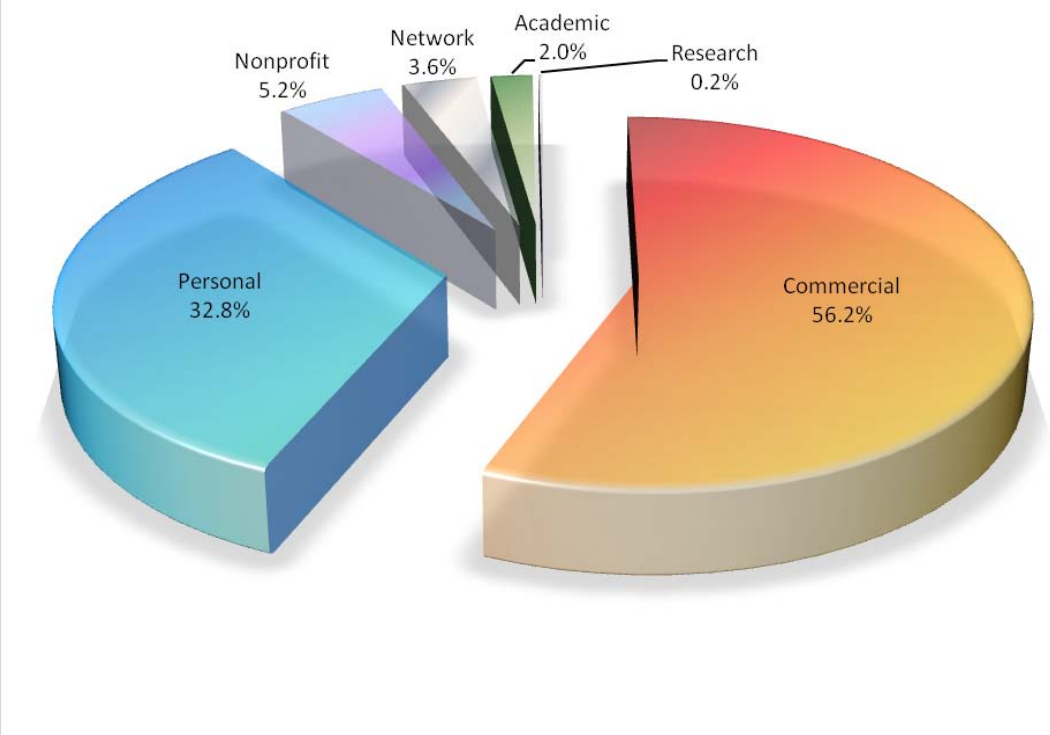
The number of reports on phishing is somewhat increased, showing steady growth in recent years. This trend shows seeking the financial gain will not be easily abandoned by the hackers or fraudsters. Recent years are told that several user-friendly phishing tool kits in the wild, which makes more acceleration on the trend. Financial institutions are always the most targeting sector in phishing. The problem is that, in Korea, only a combination of two credentials of person's real name and resident ID number can be used for stealing the individual proprietary.

2.4. Efforts to reduce malware embedded websites

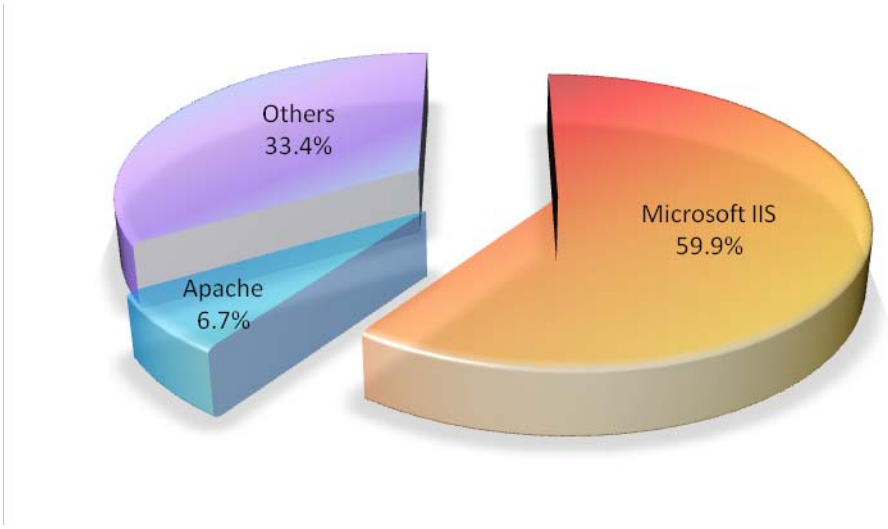
KrCERT/CC operates a malware embedded website detection and response system, so-called MCFinder (malicious code finder), which enables to detect and manage malware embedded websites. This detection system crawls and hunts for more than 125,000 websites in Korea that potentially embedded with a malware, and links to a malware in web pages. The system has a pattern database for detection to determine whether the website is embedded with a malware and/or its link, and the database is 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 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 abused systems are eventually used as or leaded to a phishing or identity theft.

To mitigate this trend, KrCERT/CC is putting an enormous effort by monitoring and handling the malware embedded websites while taking down those sites, using the MCFinder system. The number of detected malware embedded websites in year 2008 is 8,978, which is 62% increase compared with that (5,551) of the year 2007. We categorized them by business sectors as shown below.



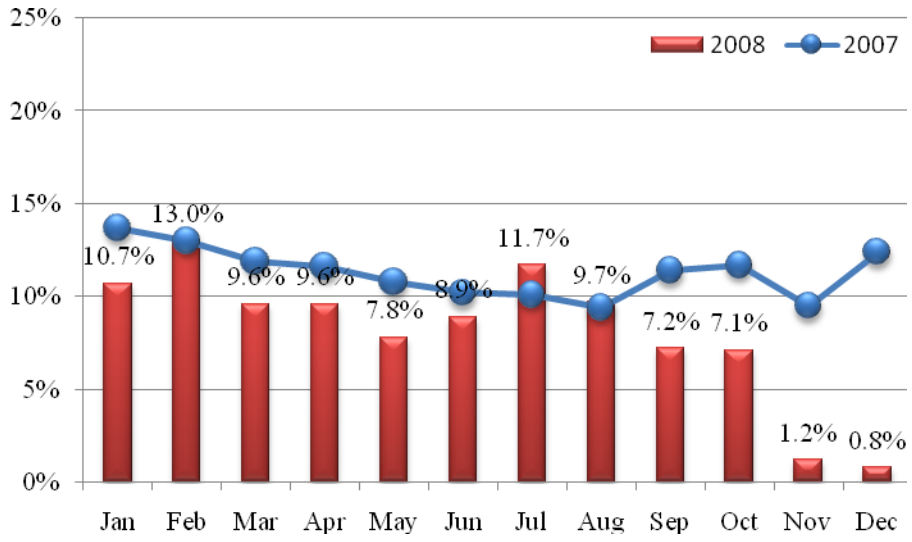
Most of the web server detected in the system is Microsoft IIS web server, which takes 59.9%, Apache takes 6.7%, and others 33.4%, as shown below.



2.5. Efforts to reduce bot infection

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 well-sorted infrastructure in Korea, since Bot C&C servers characteristically prefer faster network. KrCERT/CC is pouring a great effort to reduce the domestic bot infection rate, by monitoring and applying sinkhole method to the bot C&C servers, 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 2007 was 11.3%, which is decreased to 8.1% in 2008[10] . The graph of the domestic bot infection rate in 2008, shown below, has some ups and downs, but average rate is lower than that of the year 2007.



Monthly domestic bot infection rate in 2008

3. Events organized / co-organized

3.1. 2008 APISC Security Training Course

KrCERT/CC hosted the 2008 APISC Security Training Course to support strengthening the response capabilities of the developing economies. The

[10] 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.

objective of this training course is to assist developing economies to establish Internet incident response capabilities while providing a training opportunity for establishing and managing CSIRT in their own economy. This event was held on 1 - 5 September in Ibis Myeong-dong Hotel, Seoul, Korea, with 24 trainees participated from 14 economies, 4 trainers from 3 economies, throughout the Asia and Pacific region.

The content of 5 days course includes general overview of the information security and Korea Information Security Agency, and TRANSITS (Training of Network Security Incident Teams Staff) course. Active participation from the trainees benefited all participants 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.

3.2. APCERT 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 2008 which has ended with successful result.

The drill was again to verify the coordination capabilities among CSIRTs on incident handling framework, deliver actions to improve incident response system in each CSIRT, and give participants an experience of a coordination system. 24/7 POCs were shared for preparation and an IRC channel was used for real-time communication. 14 APCERT member teams from 13 economies have joined the drill, as the scenario was not distributed before the actual drill commenced. Some economies had their own drill with local ISPs involved and played with their own coordination system with the given version of scenario. MyCERT has successfully completed to coordinate the drill, as whole other participated teams have successfully done their tasks. Yet another good drill was performed in 2008 by the APCERT members.

4. International Activities

KrCERT/CC has participated in National CSIRT meeting held in June 2008 in Vancouver, Canada, hosted by CERT Coordination Center. We shared our experience presenting on tools we developed; MC-Finder, WHISTL, and CASTLE,

which are respectively on malware website detection, web shell detection, and a tool for secure website.

In APEC TEL 37 meeting held in Tokyo, Japan, an APEC funded project that KrCERT/CC had proposed and completed was finally approved in the SPSG (Security and Prosperity Steering Group) and Plenary meeting, which the outcomes of the projects are; Cooperative Response Guidelines in Cross-border Environment, Best Practice for cooperative response based on public and private partnership, and 2006 APEC Security Training Course, which were officially published as APEC documents. At the end of the SPSG meeting, Mr. Jinhyun CHO from KrCERT/CC was appointed as the new SPSG convenor, who had served as a deputy convenor for 2 years, and will serve for 2 more years. Also, Mr. Jinhyun CHO moderated a session in the "Workshop on Policy and Technical Approaches against Botnet". In APEC TEL 38 meeting held in Lima, Peru, Mr. Jinhyun CHO has led the SPSG meeting and spoke in other meetings and workshops regarding strengthening the global cyber security capability.

5. Future Plans

KrCERT/CC is planning to provide another training opportunity in the year 2009, in the earlier season than before, by hosting the APISC Security Training Course, to many potential security experts as possible, by inviting them to attend our training course with lectures and active discussions. This chance will give more skills and experience to the attendees in both legal and technical perspective, not only to ones from developing economies who plans to build a CSIRT, but also to existing teams by sharing the experience and trend from all the economies from Asia Pacific region.

8. MyCERT Activity Report 2008

Malaysian Computer Emergency Response Team – Malaysia

1. About MyCERT

1.1. Introduction

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 essence of MyCERT's existence, providing a point of reference in resolving computer security incidents.

1.2. Establishment

MyCERT was established in 1997, and now operates under CyberSecurity Malaysia, a non-profit organization under the purview of the Ministry of Science, Technology and Innovation (MOSTI), Malaysia.

CyberSecurity Malaysia main roles can be summarized as follows:

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

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

1.3. Workforce

As of December 2008, CyberSecurity Malaysia has 140 staff strength with MyCERT consisted of 15 staff.

1.4. Constituency

MyCERT's constituency is the Malaysian Internet Users. Therefore, MyCERT handles security incidents reported by Malaysian as well as foreign institutions where the sources or target of incidents are within Malaysia. Malaysian Internet users are about 14.9 million users.

2. Activities & Operations

In year 2008, MyCERT had received reports involving growing numbers of targeted attacks such as defacements, online fraud and identity theft. In dealing with these incidents, collaboration and coordination with various parties such as law enforcement agencies, corporate IT departments and legal departments were so sought to resolve the attacks.

2.1. Incident Handling Statistics

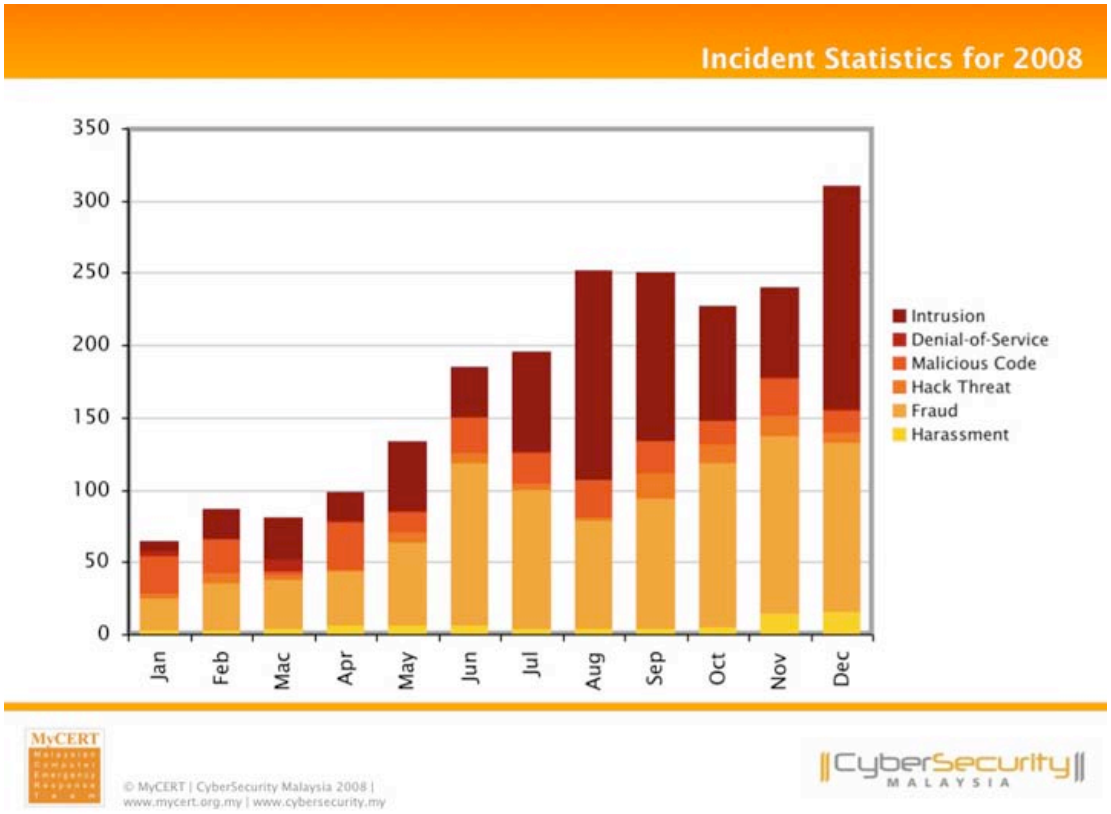
There were 2123 incidents referred to MyCERT in year 2008. Generally, the security incidents are categorized as intrusion, malicious code, fraud, harassment and spam. Fraud and intrusion related incidents make up about 78% of total incidents handled. The majority of the cases for fraud are of phishing in nature. Incidents involving malware in particular botnet command and control, drop sites, and bot infection were also significant in year 2008. 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. Trends in 2008

Abuse statistics and trends are available on MyCERT website. In addition, quarterly reports for year 1999 to 2008 can also be viewed at http://www.mycert.org.my/en/services/statistic/mycert/2008/main/detail/566/index.html

2.3. Abuse Statistics

The year 2008 abuse statistics and incidents chart are as shown below:



3. 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, malware analysis, and security trends for different kinds of audience. Internationally, MyCERT was also invited to seminars and conferences to share insights and case studies on a variety of security related topic.

3.1. Training

There were several workshops or hands-on training conducted by MyCERT in year 2008 which include:

- Network Security Monitoring Training at the APCERT Conference in HongKong and FIRST-TC in Tokyo.
- Distributed Honeypot Training for Higher Learning Institution and ISPs.
- Incident Handling Workshops for local organizations.

3.2. Cyber Exercises

In year 2008, MyCERT had participated in three cyber-exercises:

- A National Cyber Exercise

MyCERT co-ordinated the cyber exercises with participation from local agencies.

- ASEAN CERT Incident Drill 2008 (ACID)
  MyCERT participated as a player in the drill organized by SingCERT.
- APCERT Cyber Exercise 2008
  MyCERT assisted in the co-ordination of the drill with AusCERT.

3.3. Seminars and Conferences

In order to establish closer working relationship with other security practitioners globally, MyCERT staff attended various CSIRT related events in year 2008. They include:

- Digital Phishnet Conference, Singapore
- APCERT Conference 2008, Hong Kong
- APWG Counter E-Crime Conference, Japan
- FIRST Annual Conference, Canada
- CSIRT with National Responsibility Meeting, Canada
- AusCERT Conference 2008
- APECTEL 38, Peru

4. Achievements

4.1. Presentations

MyCERT was invited to speak at seminars and conferences in year 2008. The following are the international conferences where MyCERT had participated as speakers:

- APCERT Conference, Hong Kong
- APTLD Meeting, Kuala Lumpur
- CNCERT Conference, China
- TF-CSIRT Meeting 2008, Norway
- APECTEL 38, Peru
- OIC-CERT Meeting, Tunisia

In Malaysia, MyCERT conducted more than 21 presentations at local seminars. Some of the topics covered are malware analysis, deploying distributed honeynet, and network security trends.

4.2. Publications

4.2.1. Alerts and Advisories

Alerts, advisories and publications such as MyCERT's quarterly report are available at MyCERT's website, http//www.mycert.org.my/

4.2.2. APCERT Annual Cyber Exercise 2007 Video

A video dramatizing the sequence of events simulated in the APCERT Cyber Exercise 2007 was produced in May 2008. The video was used to educate and explain to public on the importance of emergency readiness and regional collaboration in mitigating security incidents. With the permission of the steering committee members of APCERT, the video was first released at World Cyber Security Summit in Kuala Lumpur.

5. International Collaboration

5.1. MoU

As part of MyCERT initiatives to establish greater collaboration with other international teams, MyCERT, via its parent organization, CyberSecurity Malaysia, signed two MoUs in year 2008 with the Tunisian CERT (CERT-TCC) and the Indonesia Security and Incident Response Team on Internet Infrastructure (ID-SIIRTI).

In addition to the MoUs, MyCERT had also become a member of the Anti-Phishing Working Group and the Honeynet Project.

5.2. Team Sponsorship

MyCERT was one of the sponsors for Sri Lanka CERT (SLCERT) to become a member of FIRST. In addition, MyCERT also sponsored a CSIRT for a multinational organization based in Malaysia for FIRST membership.

5.3. APCERT IRC Server

MyCERT was given the privilege to host the IRC server for APCERT. This new communication platform was introduced to encourage more discussion and collaboration between teams.

6. Conclusion

Year 2008 has been a memorable year or MyCERT in various aspects. The team had learned a lot and enjoyed good working relationship with various teams, particularly the APCERT teams.

In year 2009, MyCERT plans to improve further its capabilities and help more organizations to establish incident handling capabilities service for their constituencies. MyCERT also intends to participate actively in regional and global collaborative efforts in mitigating security incidents.

9. SingCERT Activity Report 2008

Singapore Computer Emergency Response Team – Singapore

1. About SingCERT

1.1. Introduction

The Singapore Computer Emergency Response Team (SingCERT) is a one-stop centre for security incident response in Singapore. Besides providing assistance to its constituency in incident resolution and co-ordination, SingCERT also broadcasts security alerts, advisories and security patches. To promote security awareness and to educate the general public, SingCERT organises frequent seminars, workshops and sharing sessions covering a wide range of security topics.

1.2. 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.

1.3. Constituency

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

2. Activities & Operations

2.1. Incident Trend

There is an increase in the total number of incidents reported to SingCERT in the year 2008 as compared to the year 2007. Phishing and the widespread of malwares were the major concerns in 2008. Besides that, there were increased attempts and probes targeting at hosting environment and the ISPs in the later part of the year. SingCERT continues to work with other CERTs and our Internet Service Providers (ISPs) to track down affected users and keep them informed on how to secure their systems. On the regional and international fronts, collaboration and cooperation among CERTs have proved effective in the resolution of many of our cross-border incidents.

3. Events organized / co-organized

3.1. Seminars and Workshops

In our continued efforts to keep our constituency updated on security trends and developments, SingCERT organised 5 seminars and workshops for the year 2008. These events were co-organised with industry partners to bring the latest technology and knowledge to our security practitioners.

3.2. ASEAN CERTs Incident Drill 2008

With the objectives to share experience and widen the scope of collaboration, Singapore invited MCMC (the Malaysian Communications and Multimedia Commission), Malaysia to jointly organise the ASEAN CERTs Incident Drill (ACID) 2008. 13 CERTs from ASEAN, Europe and Asia participated in ACID 2008. The drill was conducted successfully on 30 July 2008 and received good feedback from all the participants.

4. International Collaboration

4.1. Incident Drill

SingCERT organised the ASEAN CERT Incident Drill in July 2008 and participated in the APCERT Annual incident drill in late 2008.

4.2. Dialogue and Information Sharing

A delegation from the Information Technology Industry Development Agency (ITIDA), and the National Telecom Regulatory Authority (NTRA) of Egypt visited Singapore to have a government-to-government discussion and exchange on infocomm security initiatives/masterplan and incident management.

A delegation from the Information Technology Authority (ITA) of Oman visited the Infocomm Development Authority of Singapore and SingCERT shared with them our experience in managing and operating a national CERT.

A delegation from Vietnam CERT (VNCERT) visited SingCERT to understand how we operate a security operations centre.

5. Future Plans and Project

SingCERT, will be organising the 4th ASEAN CERTs Incident Drill for the year 2009. Discussions are in progress to work out the scope and coverage.

10. ThaiCERT Activity Report 2008

Thai Computer Emergency Response Team – Thai

Year 2008 ThaiCERT's handled Incident Response Summary

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.

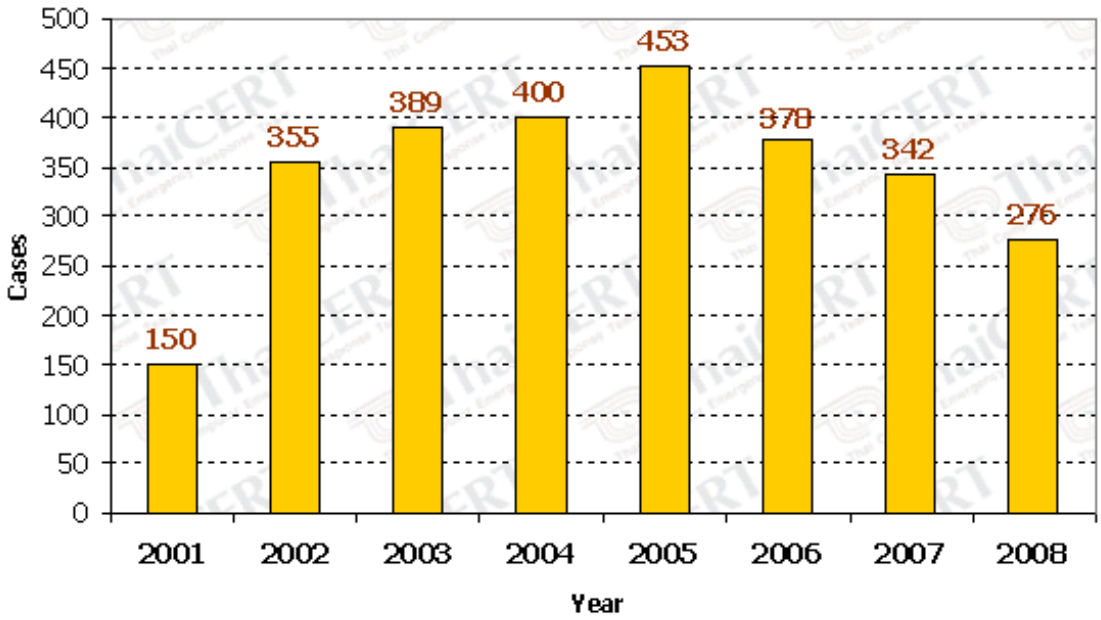


Chart 1: Number of ThaiCERT's handled incident in each year from 2001 to 2007.

According to the number of handled incidents in each year since 2001 in Chart 1 shown above, in year 2008 the total incident cases have been decreased from previous years little bit. From the number of incidents categorized by types in Table 1 shown below, the phishing cases have been decreased about 28 percent. The reason of decreasing trend is due to more collaboration with many ISPs and IT related organizations in helping handling this type of incidents. But they still grew about 22 percent from year 2006. On the contrary, malware (computer virus, internet worm, etc.) cases decreased to only 43 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.

Type of Incident / Year	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
2008	**3**	**20**	**43**	**188**	**22**

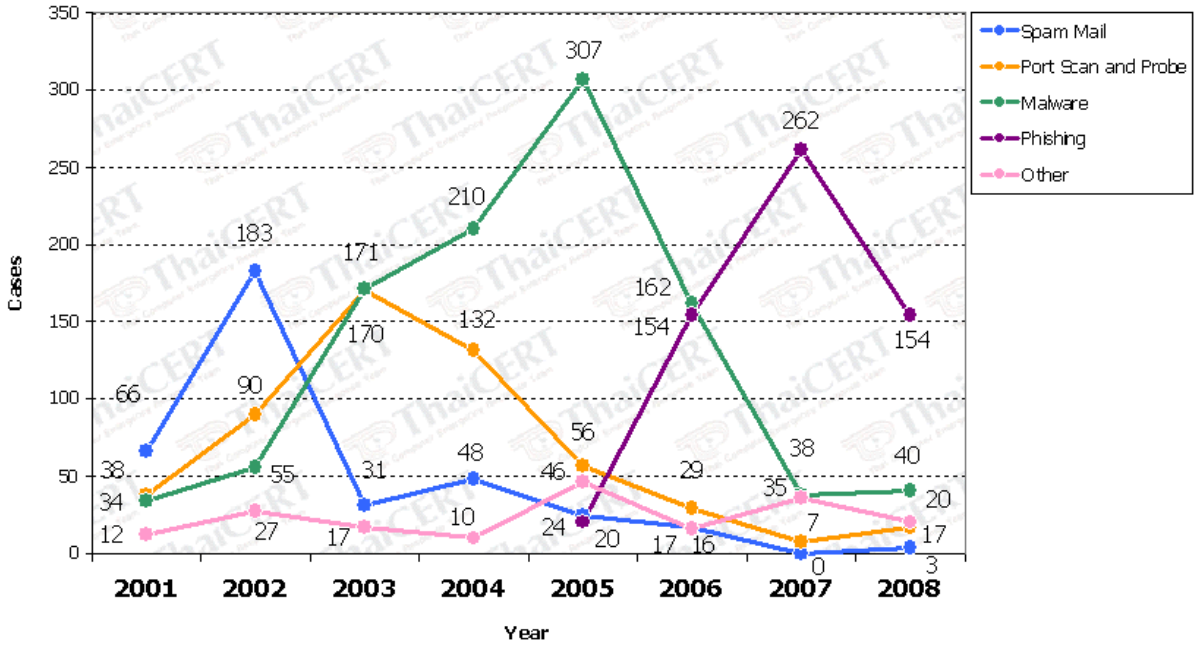


Chart 2: Number of ThaiCERT's handled incident from the year 2001 categorized by incident types.

Focusing on incidents in the year 2008, the most frequent type of incidents has still been 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 remained targeting 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 2008's phishing cases, most of the cases use compromised servers in Thailand to publish phishing web sites.

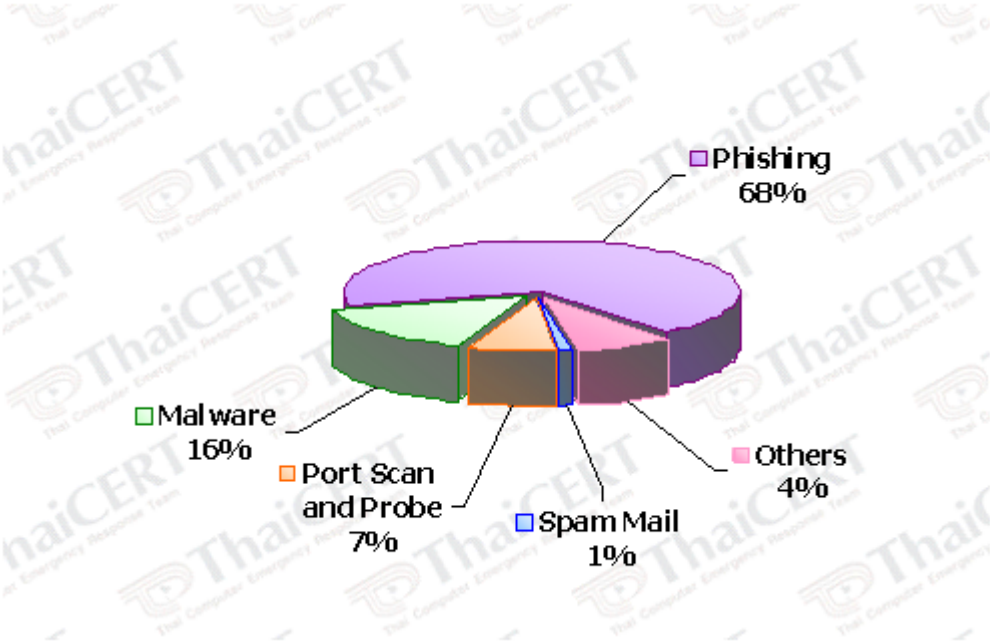


Chart 3: Ratio of each type of ThaiCERT's reported incidents in the year 2008.

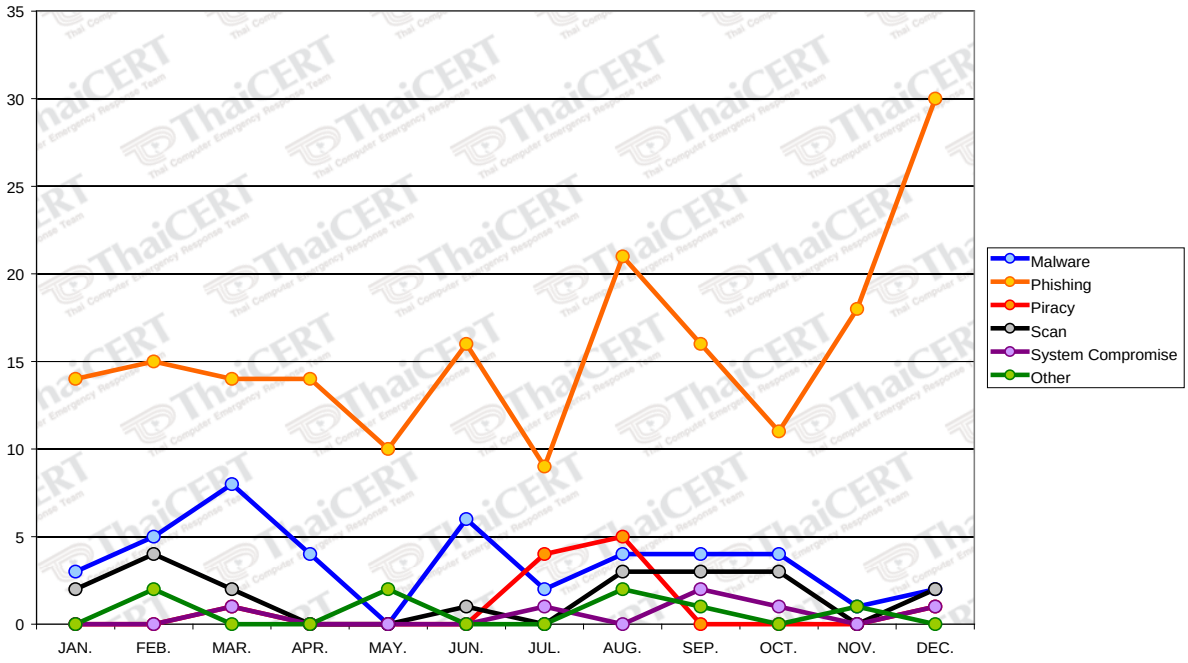


Chart 4: Number of incidents in each month during the year 2008, categorized by incident type.

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 December 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 late of the year from August to December while during the early and the middle of the year 2008 there were fewer cases.

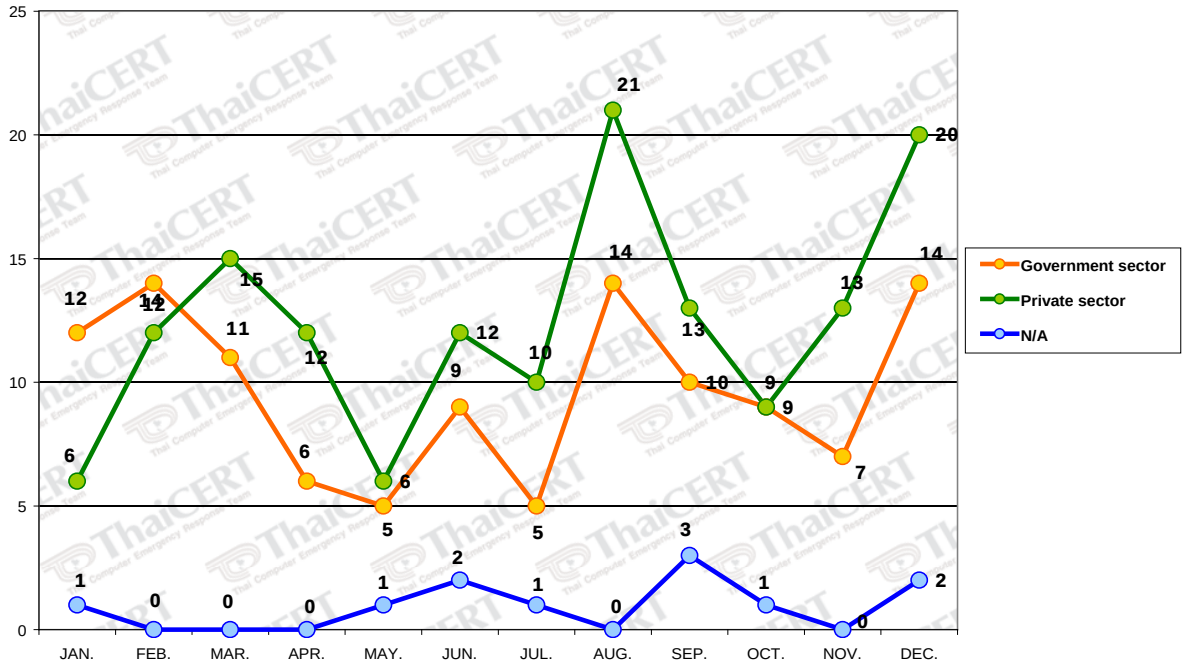


Chart 5: Number of incidents in each month of year 2008, categorized by incident source organization type.

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 116 cases while the private's ones had 149 cases. Other 11 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 2008 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.

Reference

[1] "Phishing", http://www.thaicert.org/paper/basic/phishing.php.

[2] Origins of the Word "Phishing", http://www.antiphishing.org/word_phish.html, 15.02.2008.

11. TWCERT/CC Activity Report 2008

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 Taiwan, to analyze the system vulnerabilities, to provide computer and network security tools and related documents for the system administrators and the programming guidelines for the developers, and conduct a series of training programs to raise the awareness of network security. TWCERT/CC is constantly reinforcing the organization functions and refining the network security services. With the dedicated devotion and seamless collaboration of the whole team, TWCERT/CC has accomplished several significant gradational goals and missions as follows:

1. To assist the handling of the intrusion incidents around the region;
2. To announce the system vulnerability information;
3. To provide security training and education on protection and defending technologies and skills;
4. To research and develop the Security Auditing System (SAS) which audits the subscribed client systems;
5. To assess periodically the regional security level in the Internet;
6. To be the official international coordination in Taiwan 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 the national wide network security, and reconcile the combination and interchange on security information.
- Encourage and coordinate the exchanges and cooperation between each international emergency response institution to maintain the global network security.

2. Activities & Operations

2.1. 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 Taiwan'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	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008
Total	9	85	962	1260	5318	2874	1824	788	660	1087

Table 1. TWCERT/CC incident response statistics

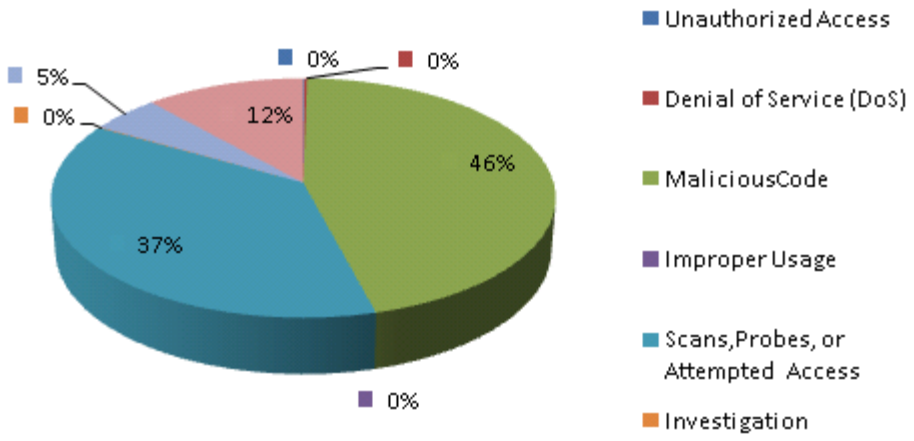


Fig 1. TWCERT/CC incident response classification

2.2. 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	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008
Advisory	186	178	172	258	142	197	140	138	119	49

Table2. TWCERT/CC Advisory statistics

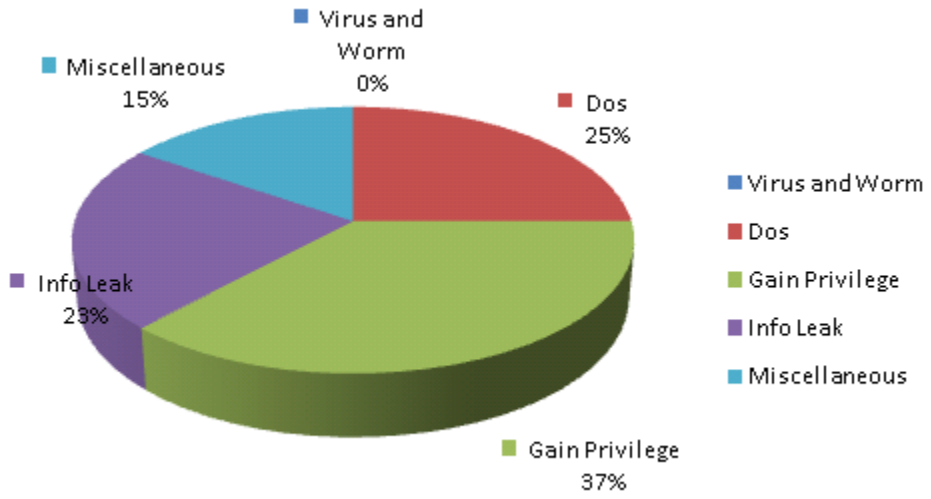


Fig 2. TWCERT/CC Advisory classification

2.3. 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 Taiwan publicity to achieve the synchronicity of worldwide circulating information as soon as possible. In addition, the monthly TWCERT/CC Newsletters include special columns on the latest network security information, technologies, or skills to raise the awareness of network security in Taiwan.

2.4. 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.

2.5. 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

2.6. 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.

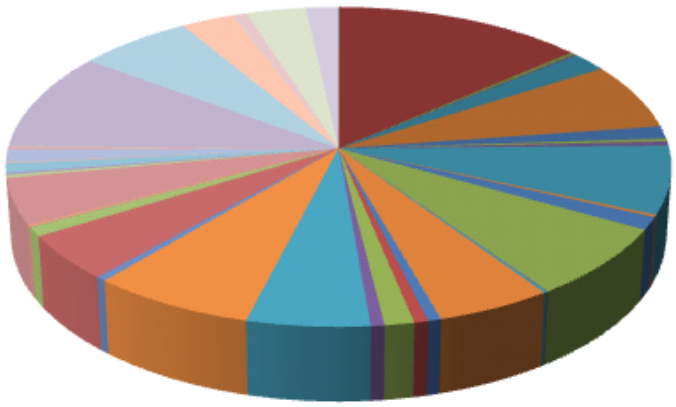


Fig 3. Categories of TWCERT/CC Vulnerability Database

2.7. 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.

2.8. 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
2008/03/20	Strongly Diagnosable Networks
2008/03/27	Medical Image Compression Using Cubic Spine Interpolation for Low Bit Rate Telemedicine Application
2008/05/15	Strongly Diagnosable Networks
2008/06/12	Anonymous Fair Transaction Protocols
2008/06/18	How can networked virtual environments (NVEs)take advantage of peer-to-peer (P2P) schemes?

3.2. Seminars

Date	Seminar	Host	Location
2008/11/24 | 2008/11/25	Taiwan-Germany Information Technology Workshop 2008	TWISC	Kaohsiung, Taiwan
2008/07/07 | 2008/07/77	Security Camp 2008	TWISC	Tai-Nan, Taiwan
2008/03/10 | 2008/03/12	2008 APCERT Annual Meeting	HKCERT	Hong Kong, China
2008/04/16 | 2008/04/18	Info Security 2008	Isecutech	Taipei, Taiwan

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.

- **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 Taiwan to reinforce the information exchange and collaborations among all the other CERTs around the world. On account of the cooperation among the network security organizations, we expect to provide a secure and convenient network environment for the Internet users.

4.2. Publication

Publication	Publish
An Optimal New-Node Placement to Enhance the Coverage of Wireless Sensor Networks	Wireless Networks (SCI)
Improved Intelligent Genetic Algorithm Applied to Long-endurance Airfoil Optimization Design	Engineering Optimization (SCI)
Anti-Spam Filter Based on Data Mining and Statistical Test	Journal of e-Business(TSSCI)
A Collaborative Anti-Spam System	Expert Systems with Applications
Efficient Network Monitoring for Large Networks	Journal of Computer
Detecting Denial of Service Attacks in Sensor Networks	Journal of Computers
Ant-Based IP Traceback	Expert Systems with Applications

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.

5.1. Forum of Incident Response and Security Teams (FIRST)

FIRST is the Forum of Incident Response and Security Teams. It was clear from then on that information exchange and cooperation on issues of mutual interest like new vulnerabilities or wide ranging attacks - especially on core system like the DNS servers or the Internet as a critical infrastructure itself - were the key issues for security and incident response teams. FIRST brings together a wide variety of security and incident response teams including especially product security teams from the government, commercial, and academic sectors.

TWCERT/CC becomes the first official international coordination in Taiwan by joining the FIRST in October 2001 to share the latest security information and technologies in FIRST forum with members, attends annual FIRT conference to establish a transnational security joint defense system and enhances incident-handling capability for integrated early-warning mechanism.

5.2. Asia Pacific Computer Emergency Response Team (APCERT)

Besides globalization organizations, Asia Pacific Computer Emergency Response Team is a regional coordination organization established by countries of the Asia Pacific region in 2002 to enhance regional and international cooperation on cyber security. APCERT cooperates with CERTs and CSIRTs to maintain a trusted contact network of security experts in the Asia Pacific region to improve the region's awareness and competency in relation to cyber security incidents.

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

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

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

Seoul-Melbourne Multilateral Memorandum of Understanding on Cooperation in Counting SPAM is an agreement signed by Australian Communications and

Media Authority (ACMA) and Korea Information Security Agency (KISA) in 2003. Participates in Seoul-Melbourne MoU are part of a network of computer security incident response and security teams that work together voluntarily to deal with spam problem and prevention.

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

The key points of our missions are:

1. To cope Taiwan'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 Taiwan's international image and position.

6. Future Plans

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 Taiwan 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.

12. TWNCERT Activity Report 2008

Taiwan National Computer Emergency Response Team – Chinese Taipei

1. Introduction

TWNECRT is a non-profit organization intended for improving incident response and IT security awareness in Taiwan. 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 Taiwan and to share security information with each other.

2. 2008 Highlights

2.1 Promote Security Awareness and Provide Training Course

- TWNCERT offers IT security conferences, workshops, training courses, and exhibitions for technical staffs and security managers.

2.2 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 2008, TWNCERT published total 1790 advisories and alerts, including:

(1) 1790 advisories for intrusion incidents.

(2) 14 advisories for information security message.

(3) 159 advisories for web site defacement incidents.

(4) 1409 advisories for warning the suspicious incidents and incident prevention.

(5) 2 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 2008, TWNCERT continued to participate in the following security communities and attended many important conferences:

(1) APCERT 2008
(2) FIRST 2008
(3) APEC-TEL 2008
(4) AVAR 2008
(5) Virus Bulletin 2008
(6) AFACT 2008
(7) DeepSec IDSC 2008
(8) ISACA International Conference and Annual Meeting of the Membership 2008
(9) USENIX 2008
(10) Cyber Defense Info-Security Asia 2008

In addition, TWNCERT receives the reporting of computer incidents about Taiwan 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 2008, TWNCERT handle about 280 incidents reporting from about 15 international security communities.

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.

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
Phone: +886-2739-1000 ext 661
Fax: +886-2733-1655

13. VNCERT Activity Report 2008

Vietnam Computer Emergency Response Team – Vietnam

1. About VNCERT

VNCERT is an agency under Ministry of Information and Communications of Vietnam, established by decision of Vietnam's Prime minister in December, 2005. With functions of coordinating national computer incident response activities, watching and warning computer network security problems, building and co-ordinating to build computer network security technical standard, promoting to build CERTs in the organizations, enterprises, agencies in Vietnam, VNCERT is responsible for state management of information security (IS) area and is the point of contact of Vietnam with the oversea CERTs in this area.

VNCERT has four specialized divisions: division of operation, division of system technique, division of training & consultancy and division of research and development. VNCERT also has two branches, one in Hochiminh city and another in Danang city.

Current number of employees in VNCERT is about forty.

2. Activities & Operations

In 2008, the total number of serious incidents reported to VNCERT is 95, which has 48 incidents increase compared to 2007. VNCERT worked very actively and directly in handling 73 incidents and took part in 22 incident handling consultancy situations.

In 2008 there are 02 serious incidents in Viet Nam: 01 attack to DNS and 01 attack to PAvietnam. No incident occurred on government agency systems. VNCERT handled those.

The reports of 2008 are about website defacement and phishing. Almost phishing incidents related to finance, commonly forging banks to steal bank's account, and they are reported from outside Vietnam.

In 2008 the internal and external coordinating information Chanels have been set up for 2 ministries, 03 government websites, and 7 Internet service providers.

VNCERT:

- informed hundreds of websites and electronic newspapers of VNCERT's point of contact to receive emergency response;
- helped to secure all online important government events;

- coordinated with the Vietnam Information Security Association (VNISA) carried out a survey of IS situation in enterprises and state agencies in all over Vietnam;
- early detected and warned the IS threats on the large scale, supported to handle the IS vulnerabilities and preventing incident on the national scale.

3. Events organized / co-organized

3.1. Training & Drills

In 2008 VNCERT:

- arranged some information security training programs for the staff of some organizations in Hai Phong, Da Nang, Ho Chi Minh city.
- took part in building the plan and preparing the materials of IS courses to train managerial staff of some governmental institutions to raise the awareness of IS and improve capability of IS for officers.
- VNCERT participated in 02 international drills in 2008: ASEAN CERTs Incident Drill (ACID 2008), and APCERT Drill 2008.
- VNCERT coordinated to organize IS contest between the students of 8 universities in Vietnam.

3.2. Seminars&Etc

VNCERT:

- organized 02 great annual events "SecurityWorld" and "Vietnam Information Security Day"
- participated in 03 conferences of ministry level, 03 international bilateral workshops taking place in Vietnam and participated in some seminars at the universities, institutes of Vietnam.

3.3. Consultancy

VNCERT supports the state and private organizations in the IS area and helps the Government to develop the national strategy to secure cyber-space.

4. Achievements

VNCERT:

- took part in the national and international conferences related IS, VNCERT always made detailed reports on network security, actively expressed the idea and enthusiasm to the conference programs.
- have a good communication with the press and other means of communication to inform the VNCERT's activities to the public, aiming to

raise prestige and state management role of Ministry of Information and Communication.

- deployed RD project on building system model suitable for monitoring internet space in all over Vietnam.
- proposed state macro-management model of the email-spam and SMS spam to the Government.

5. International Collaboration

Active international cooperation relations help VNCERT to learn experiences, knowledge, and to reach promptly the regional and international standard related IS.

VNCERT has officially been approved as a Full Member of APCERT on 18th December 2008.

VNCERT coordinated to settle the problems according to the request of other CERTs and oversea organizations.

5.1. Multilateral Collaboration:

VNCERT participated and reported in many workshops, seminars, conferences in Vietnam and other regions such as APCERT, ASEAN, ARF, APECTEL, ITU, Meeting of national CSIRTs…

VNCERT attended 05 international training courses on IS.

5.2. Bilateral Collaboration:

VNCERT have successfully arranged some bilateral international seminars and workshops, developed bilateral strategic cooperation between VNCERT and JPCERT/CC to improve common exertion for IS, supported JPCERT/CC's training course about developing CSIRTs in Vietnam (11/2008), worked and discussed with some other international organizations from Laos, Israel, Poland, Japan, Singapore, Malaysia…

6. Future Plans

VNCERT is:

developing the state master plan to secure cyber-space.

developing the technical standard on information security management and the Project of National Network Security Technical Center

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

organizing the national workshops/ events on cyber security.

deploying official websites of VNCERT for cyber security and for anti-spam management

implementing the RD project on building the technical system for watch, warning and incident response and taking part in some international collaboration research projects.

participating actively in the collaboration activities among APCERT and ASEAN CERTs

7. Conclusion

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

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

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

General Members

14. BDCERT Activity Report 2008

Bangladesh Computer Emergency Response Team - Bangladesh

1. About BDCERT

1.1. Introduction

BDCERT is the Computer Emergency Response Team for Bangladesh and is the primary Point of Contact for handling incidents from Bangladesh networks. We work for improving Internet security for Bangladeshi Internet users.

We provide information about threats and vulnerabilities that could affect the users. We work closely with various organizations and associations such as ISPAB, BASIS, BCS, SANOG, BTRC, Law Enforcement Agencies to stop attacks that are either sourced from Bangladesh or outside.

We help to mitigate Internet attacks directed at Bangladesh Internet users and networks.
We provide training and awareness programs on Information Security and issues affecting Internet security in Bangladesh and globally.

1.2. Establishment

BDCERT was formed on July 2007 and started Incident Response on 15th November 2007. BDCERT is initiated by some IT professionals who have long experience in data and Internet communication and technologies industry. It is funded voluntarily with limited resource but highly motivated professionals.

1.3. Workforce power

We currently have a working group of 12 professionals from ISP, DDCSP, Telco, Vendors, University, Media, Bangladesh Internet Exchange (BDIX) & National International Internet Gateway (IIG) who are working voluntarily with great enthusiasm and motivation. Some of the activities that we are involved with are Incident Handling, National POC for national and international incident handling, Security Awareness program, Training & Workshops, New Letters, Traffic Analysis, etc.

1.4. Constituency

As a national CERT the constituencies of BDCERT are all the Internet users of Bangladesh. We work closely with all the ICT stake holders particularly with ISP

Association of Bangladesh (ISPAB), Bangladesh Association of Software & Information Service (BASIS), Bangladesh Computer Samity (BCS), Bangladesh Computer Council (BCC), Bangladesh Telecommunication Regulatory Commission (BTRC) and various Government Organization, Non Government Organization, Universities and Government Law Enforcement Agencies to mitigate Internet threats.

2. Activities & Operations

2.1. Incident Handling Statistics

In year 2008, BDCERT has received 121 incidents reports. Taxonomy statistics of incidents report are shown in figure 1. Majority of incidents are related with spam and spam like email.

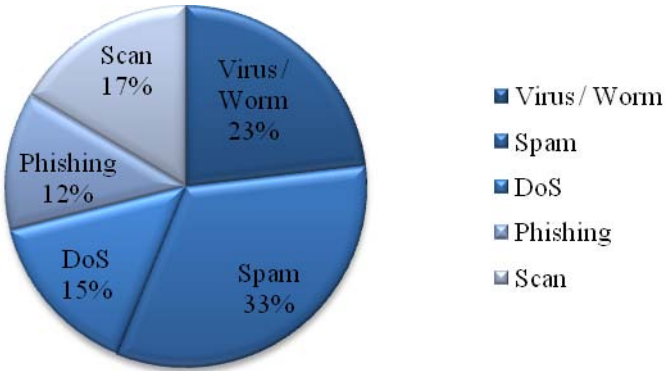
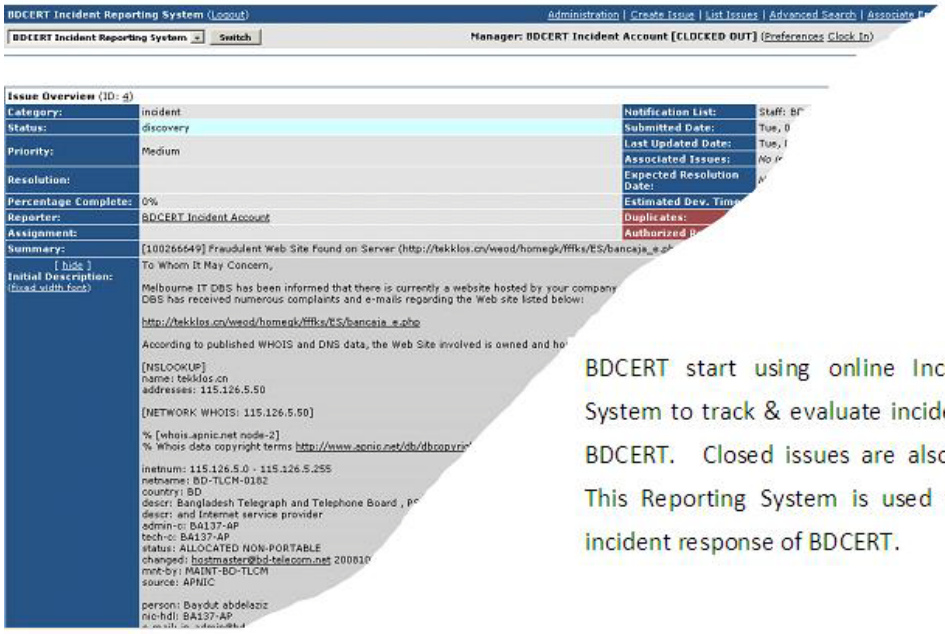


Figure 1 : Taxonomy statics of Incident

Taxonomy	Incident No
Virus / Worm	28
Spam	40
DoS	18
Phishing	15
Scan	20

2.2. New services

Online Incident Reporting System:



BDCERT start using online Incident Reporting System to track & evaluate incidents reported to BDCERT. Closed issues are also tracked down. This Reporting System is used to evaluate the incident response of BDCERT.

SMS Based Incident Reporting:

BDCERT has unique SMS based Incident Reporting System. Any one can report incident through SMS. Details are in http://www.bdcert.org/incident.php

3. Events organized / co-organized

3.1. Trainings& Seminars Organized

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

- 10-18 January 2008: APNIC / Team Cymru ISP/NSP Security Workshop

It was a great event with large numbers of enthusiastic participants from all sector of IT. Ryan Connolly of Team Cymru, Mr. Cecil Goldstein and Mr. Champika Wijayatunga of APNIC were the trainers. The workshop covered Network Security Fundamentals, Network Analysis & Forensics, Botnets, Penetration Testing, and Network Protocol Analysis.

- 4-6 November 2008: BDCERT Information Security Conference & Workshop 2008.

  It was arranged with support from ISP Association of Bangladesh (ISPAB), ICT Business Promotion Council (BPC), JPCERT/CC and some other members of BDCERT.

  Ms. Yurie Ito, Director of Technical Operation, JPCERT/CC was the special spokes person, while Mr. Keisuke Kamata, Manager, Watch and Warning Group, JPCERT/CC was the technical trainer.

  It was a very successful event with over 60 participants from all law enforcement agencies, BTRC, Banks, Academics, Telcos and ISPs.

  Some of the Major topics covered are: Creating a CSIRT, CSIRT Operation, Overview of Incident Handling, Incident Analysis, PGP, CSIRT Tools, Network Monitoring, Information Gathering, etc.

3.2. Trainings & Seminars Participated

- 19-26 March 2008- The Training Program on Information Security for Asian Countries (ASIS) Hosted by JPCERT/CC.
- 1 - 5 September 2008 - 2008 Asia Pacific Information Security Center (APISC) Security Training workshop held at Korea, supported by KrCERT/CC.
- 13-15 January 2009 - OIC-CERT Seminar "Strategic Partnership Against Cyber Threats", held at Kuala Lumpur Malaysia, hosted by Cyber Security Malaysia.

4. Achievements

- Successfully conducted ISP/NSP Security Workshop with support from APNIC, Team Cymru, ISPAB, ICT BPC and other sponsors. Large no of IT professionals from various organizations participated with great enthusiasm.
- Successfully conducted" BDCERT Information Security Conference & Workshop 2008". A large number of audiences from all government and private

sectors attended the Conference. Ms. Yurie Ito, Director of Technical Operation, JPCERT/CC was the special speaker of the seminar. In the technical workshop we had participants from National Security Intelligence (NSI), Criminal Investigation Department (CID), Special Branch (SB), Detective Branch (DB), Dhaka Metropolitan Police (DMP), Bangladesh Telecommunication Regulatory Commission, etc.

- BDCERT has been approved as APCERT General Member as of 18th December 2008.
- BDCERT has been approved as OIC-CERT General Member on 15th January 2009.

4.1. Presentations

BDCERT has given presentations at several conferences throughout 2008 which includes APISC Security Training workshop, hosted by KRCERT/CC; BDCERT Information Security Conference & Workshop 2008, hosted by BDCERT; and OIC-CERT Seminar, hosted by Cyber Security Malaysia.

4.2. Publications

The first edition of BDCERT News Bulletin was issued on March 2008. BDCERT also has awareness programs regularly published in the IT Magazines.

5. International Collaboration

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

6. Future Plans& Projects

A. Government Endorsement for BDCERT
B. Full Membership of APCERT
C. Full Membership of OIC-CERT
D. Membership of FIRST
E. Fund Raising
F. Information Security Hands -on training with fresh University Graduates, Government Organizations and Banks and Financial Institutes.
G. Awareness Programs: Security Week to raise general awareness on basic information security.

7. Conclusion

Bangladesh has seen a rapid growth in Information Communication Technology over the past 7-10 years Bangladesh has seen a great boom in the Telecommunication sector. Bangladesh got connected to the global submarine system SEA-ME-WE-4 in May 2006 and the Internet users are growing exponentially. Though we have huge growth in Telecommunication and Internet but cyber security is not very familiar to general people except getting virus infection. Thus BDCERT has enormous task of educating Government policy makers and the people. BDCERT has the industry experience, knowledge and skills to provide Incident response for both local and international cyber threats.

15. SLCERT Activity Report 2008

Sri Lanka Computer Emergency Response Team - Sri Lanka

1. About SLCERT

1.1. Introduction

The Sri Lanka Computer Emergency Response Team (SLCERT) is the Center for cyber security in Sri Lanka, mandated to protect the nation's information infrastructure and to coordinate protective measures against, and responses to cyber security threats and vulnerabilities.

1.2. Establishment

Sri Lanka CERT currently has a total of six security team members and one staff for administration and the CEO. The staff is highly skilled and has training on various IT security certifications, such as GCIH, MCSE, CEH, CCNA, CCSP and CISSP.

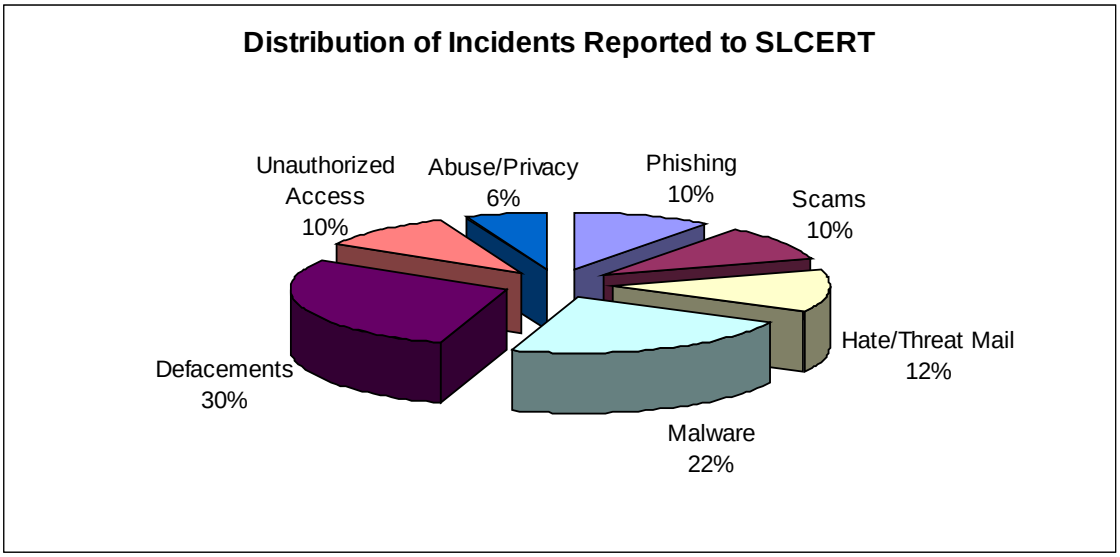
1.3. Workforce power

Sri Lanka CERT 's Constituency consists of the cyber community of Sri Lanka (Private & Public sector organizations, and general public). Sri Lanka CERT maintains a good rapport with government and private establishments, and extends assistance to the general public.

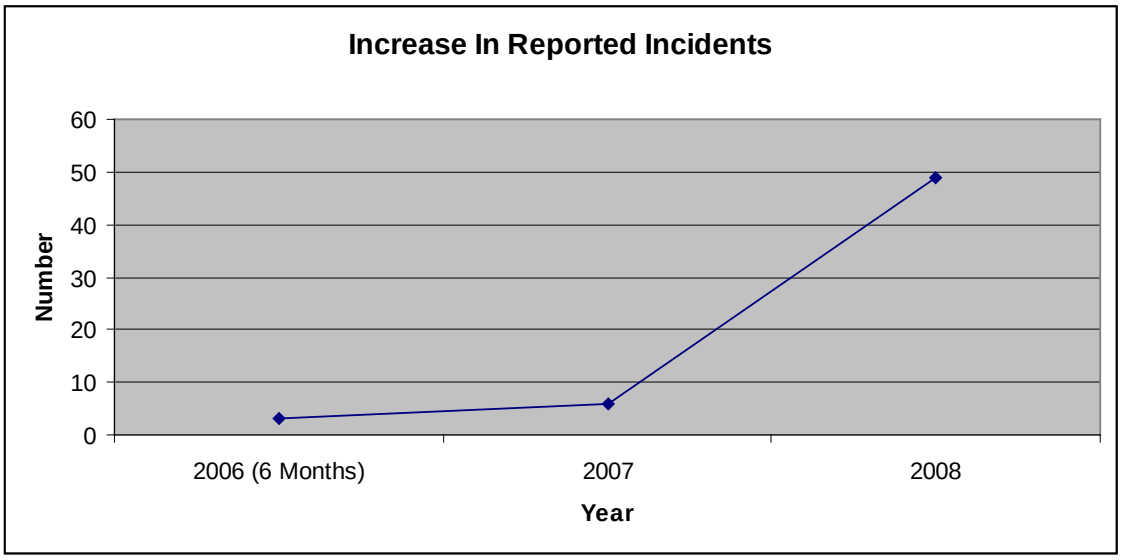
2. Activities & Operations

2.1. Incident Handling Statistics

Incidents reported to SLCERT increased up to 49 in the year 2008. This is a major hike in the number of incidents reported compared to the 6 incidences reported in 2007. The following chart depicts the distribution of various types of incidents reported to SLCERT. All the incidents reported to SLCERT have been resolved satisfactorily.

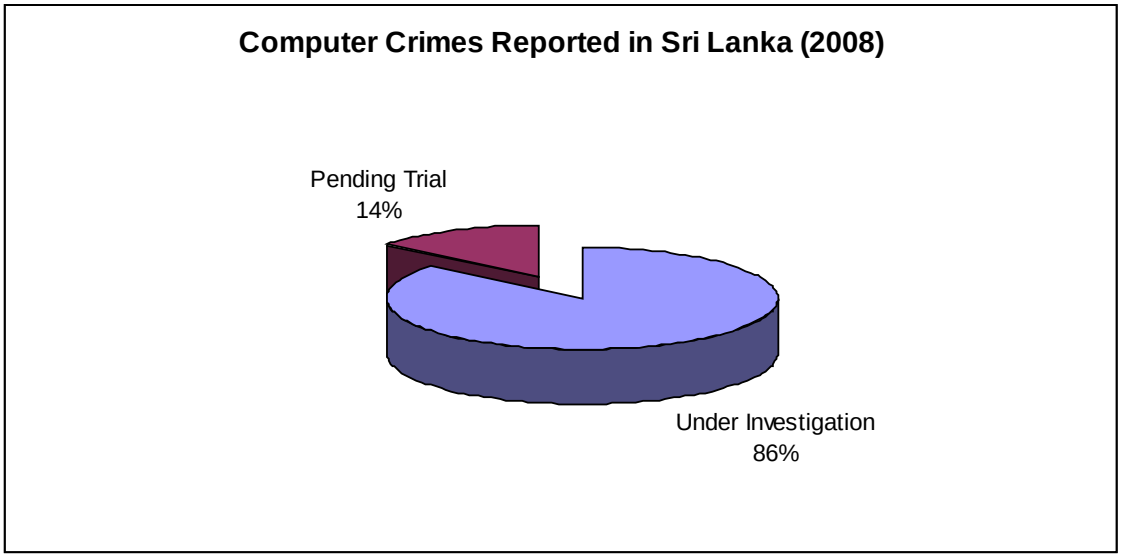


The following graph depicts the increase in the number of incidents since the inception of SLCERT in mid-2006.



2.2. Computer Crime Statistics

Sri Lankan Government introduced a new act titled Computer Crimes Act in 2007 to curb electronic crimes in Sri Lanka. The act enables the law enforcement officers to obtain the technical expertise of recognized information security professionals and organizations to extract and present digital evidence in courts. Accordingly, SLCERT has assisted Sri Lankan law enforcement agencies in carrying out forensic investigations. The following graph depicts the number of computer crime related offences reported to Sri Lankan law enforcement in year 2008.



2.3. New services

2.3.1. Behavioral Analysis of Malware

SLCERT started behavioral analysis of malware in the first quarter of year 2008 in order to provide better recovery procedures for affected constituents. At the moment analysis of malware is carried out once an infection in a critical information system is reported to SLCERT.

2.3.2. Digital Forensics

The Computer Crimes Act of 2007 enabled the law enforcement officers to obtain the assistance of recognized information security professionals and organizations in carrying out digital forensic investigations. Due to the requests from law enforcement agencies SLCERT started offering digital forensics as a service for law enforcement agencies since the third quarter of 2008. SLCERT also carries out forensic investigations for other government establishments in Sri Lanka.

2.3.3. Penetration Testing

There were some major attacks on critical information systems in Sri Lanka during 2008. As a proactive measure SLCERT has been assigned the task of carrying out vulnerability assessments and penetration tests for some major information systems. SLCERT started this service during the fourth quarter of 2008.

3. Events organized / co-organized

3.1. Training / Education

Sri Lanka CERT is organizing training programs and education sessions targeting various audiences including CIOs, Engineers, System Administrators, Banking and telecom sector staffs, Students, general public, etc.

During the year 2008 SLCERT conducted the following training, education programs successfully:

1. Lecture on "Information Security for eGovernance" for MBA students
2. Media message campaign on "Information Security"
3. Participated in a Leading IT exhibition educating the General public

3.2. Consultancy

SLCERT provides consultancy services for requests, especially for government departments.

During the year 2008, the following consultancy services were provided:

1. Network reviews for 4 government departments
2. Forensics investigation support for Law enforcement
3. Setting up a CA server for a government department
4. Initiated setting up a computer forensics laboratory for Police Department

3.3. Seminars & Workshops

Cyber Security Week 2008

Cyber Security Week 2008 was an inaugural endeavor, held in the month of October, which featured a series of events:

- Poster and essay competitions for secondary and tertiary level students, respectively
- Workshops for Technical and non-technical professionals, namely:
  - Incident Response
  - Managerial aspects of Information Security
  - Penetration Testing
- A two-day Conference

4. Achievements

4.1. Presentations

1. Conducted 3 lectures related to IS for Chief Information Officers (CIO) of government organizations following MBA in e-Governance course.

2. Conducted Presentations on following topics during the Cyber Security Week 2008 (CSW_2008) Conference in October 2008:
   - SSH (In) Security and Phishing Hosted in Sri Lanka.
   - Website Compromise.
3. Economy update on Sri Lanka during APISC Training course, Seoul, Korea

4.2. Publications & Other media

1. Web site

   Through SLCERT website published security related awareness details for public via News, Alerts and Knowledge Base. Glossaries, case studies, FAQs are among some of the published items.

2. E-mails

   Disseminating security related information via e-mail alerts.

3. Newspapers

   Published security related articles during the period of cyber security month (October 2008) to create awareness among the general public:
   - How to Use Credit Cards Online Securely.
   - Safe Use of Social Networking Sites.
   - How to control Children's Internet access.
   - How to protect yourself from malicious software.
   - How to identify genuinely secure web site.
   - Privacy in Cyber Cafes.

4.3. Certification & Membership

4.3.1. Security Certifications obtained by staff members within the period:

1. CISSP
2. CCSP

4.3.2. Memberships obtained in professional security organizations in the period 2008:

1. APCERT General Membership
2. FIRST Full Membership

5. International Collaboration

5.1. Event participation

1. January 14th - 16th

   Digital PhishNet Conference

   Singapore

Participant trained on Phishing investigation and countermeasures. Became a member of the NCFTA Digital PhishNet Community. Made new contacts with CERTs, researchers, etc.

2. February 5th - 7th

   7th International BTF Conference

   Lyon, France

   Participant made new contacts in law enforcement, especially resource people for malware analysis aid

3. March 10th - 14th

   APCERT Annual General Meeting and 2008 Conference

   Hong Kong

   Participated in the APCERT Annual General Meeting, where the Steering Committee formally approved SLCERT's application for APCERT Membership. Also attended the Annual Conference attended by a host of CERT's from other parts of the world.

4. May 19th - 23rd

   AusCERT Annual Conference 2008

   Gold Coast, Australia

   Participated in this annual conference which is billed as the premier regional conference. It is attended by top IT security officials from Asian Region as well as from Europe, USA and Canada. Renewed friendships and made good use of the networking opportunities available.

5. June 22nd - 27th

   FIRST Annual Conference and AGM 2008

   Vancouver, Canada

   Attended this AGM and conference for the first time in support of SLCERT's application for membership of FIRST, which is the world body for IT Security with a membership of over 400. SLCERT's Application which was sponsored by Malaysia and Japan, was approved at the AGM.

6. September 29th to October 1st

   Digital Phishnet Conference

   San Diego, USA

   Discussion on latest phishing trends. Training on Phishing investigation

7. December 4th

   APCERT Regional Drill 2008

   Simulated attack and response scenario. Participated as a Player.

8. September 18th and 19th 2008
   ISACA Annual Conference
   Gained practical knowledge on Audit methodologies, made new local contacts

5.2. International incident coordination

Details on incidents suppressed to prevent unauthorized disclosure.

1. MyCERT
2. Internet Identity
3. BrCERT
4. CERT/CC
5. Virginia Tech
6. CERT Hungary

6. Future Plans

6.1. Future projects

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

1. Certificate Authority server for Nationwide Government Network
2. Establishment of a Security Operations Centre (SOC)
3. Initial Sensor deployment for "Tsubame" project, followed by additional deployments at external sites to cover 32 IP Address ranges belonging to Sri Lanka

6.2. Framework

6.2.1. Future Operations

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

1. Increase of SLCERT team strength with the addition of two new Information Security Engineers
2. Acquisition of additional floor space to accommodate planned SOC, along with recruitment of two dedicated full time professionals to man SOC
3. Implementation of workflow (incident management system) to streamline incident handling process

6.2.2. Operations Support projects

These have been initiated to develop internally or procure necessary applications, hardware and personnel to support SLCERT's core business functions:

1. Development and adoption of an Incident Tracking System
2. Revamp of the SLCERT website
3. Update of SLCERT Information Asset Inventory Database and development of a web-based management interface
4. Server infrastructure upgrade (to increase forensics image storage facilities, evidence storage and resources for team operations)

7. Conclusion

Being nearly three years old, SLCERT has faced an uphill task of raising awareness of Information Security in Sri Lanka. The increase in the number of incidents reported and handled by SLCERT in consecutive years is testament to the success of its awareness campaigns.

SLCERT shall now focus on extending its service offering, while streamlining existing services so as to achieve maximum effectiveness with its staff strength. Focus shall be redirected on training staff in the necessary competencies to ensure continued operation.

SLCERT shall continue to participate in regional events such as the Annual APCERT drill and also welcomes opportunities to collaborate with its sister CERTs in incident coordination.

We remain committed to serving our constituency, and this, 2009, being the year of ICT in Sri Lanka, hope to continue hosting the Cyber Security Week conference and workshops while finding new ways to reach an even wider audience. We are increasingly entrusted with key security roles within the government and its information systems due to recognition of our capabilities.

We look forward to being a bigger part of APCERT in 2009 and contributing as much to it as we gain from it.