Asia Pacific Computer Emergency Response Team

APCERT 2005 Annual Report

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

Chair’s Message

As Chair of APCERT, it is again my pleasure to provide a report to the members of APCERT about our progress during 2005, and our third year of operation.

The individual APCERT team reports highlight the depth and breadth of APCERT activities in the Asia-Pacific region, as each team works within its own economy and among its own constituents to improve Internet security. APCERT builds on these individual team initiatives by improving cross border cooperation and information sharing. It is the combined expertise and collaboration of APCERT teams that helps make each team more effective within its own economy and constituency and of value to the broader Asia-Pacific region.

While much work lies ahead, the basic foundations necessary to help achieve APCERT’s goals and potential have largely been built. None of this could have occurred without the good will, commitment and contribution of each and every APCERT team and the constituencies they represent. I have been particularly pleased at the contributions made by the members of the Steering Committee who, as individuals and representatives of their teams, have made substantial contribution to the work and direction of APCERT.

During 2005, we continued the task of developing APCERT policies and procedures for sharing information about serious and time critical computer network threats and vulnerabilities and have begun to put in place procedures for the day to day operation of APCERT and how APCERT will conduct itself. In December, the operational nature of APCERT was put into focus with a drill designed to test our level of responsiveness to intra-regional Internet based attacks. The drill was important for a number of reasons. I would urge you to read the media release published on the drill, if you have not already done so. See: http://www.auscert.org.au/5851

After representing APCERT interests and views at various APEC-Tel meetings about Internet security threats we have gained guest observer status at APEC-Tel itself. More work now needs to be done to ensure that APCERT continues to provide valuable input into APEC-Tel fora.

This year we are pleased to have as guests at our annual general meeting representatives from the Organisation of American States (OAS), the European Network and Information Security Agency (ENISA), TF-CSIRT, APEC-Tel and FIRST. As part of a global community of CSIRTs, APCERT is mindful that we need to build relationships across and between other groups that seek to improve Internet security within their region and the effectiveness of CSIRTs internationally.

As we move into 2006, I look forward to building on our achievements further to help APCERT deliver tangible benefits to all its teams through strong cooperative arrangements to help protect against cyber threats in our region.

I thank the members of APCERT for making all this possible.

Graham Ingram
General Manager – AusCERT
Chair APCERT

CONTENTS

About APCERT

Objectives and Scope of Activities

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

APCERT aims to:

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

The formation of CERTs/CSIRTs at the organizational, national and regional levels is essential to the effective and efficient response to computer security incidents, widespread security vulnerabilities and incident coordinations throughout the region. One important role of CERTs/CSIRTs is education and training to raise awareness and encourage best practice. APCERT coordinates the activities with other regional and global organizations, such as the Forum of incident Response and Security Teams (FIRST) www.first.org and TF-CSIRT, a team of CSIRTs in Europe www.terena.nl/tech/task-forces/tf-csirt/.

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

At present, APCERT is chaired by the Australian Computer Emergency Response Team (AusCERT). Japan Computer Emergency Response Team/Coordination Center (JPCERT/CC) provides a secretariat function. The secretariat operation is supported by Korea Computer Emergency Response Team Coordination Center (KrCERT/CC).

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

APCERT Members

In addition to APCERT Full Members (founding members of APCERT consisting of 15 CERTs/CSIRTs from 12 economies across the Asia Pacific region), APCERT welcomed two new teams, BruCERT and GCSIRT, as General Members at the APCERT Annual General Meeting in Kyoto, Japan, 22-24 February 2004. APCERT now consists of 17 teams from 13 economies across the AP region.

Full Members

Team	Official Team Name	Economy
AusCERT	Australian Computer Emergency Response Team	Australia
BKIS	Bach Khoa Internetwork Security Center	Vietnam
CCERT	CERNET Computer Emergency Response Team	People's Republic of China
CNCERT/CC	National Computer network Emergency Response technical Team / Coordination Center of China	People's Republic of China
HKCERT	Hong Kong Computer Emergency Response Team Coordination Centre	Hong Kong, China
ID-CERT	Indonesia Computer Emergency Response Team	Indonesia
JPCERT/CC	Japan Computer Emergency Response Team/Coordination Center	Japan
KrCERTCC	Korea Internet Security Center	Korea
MyCERT	Malaysian Computer Emergency Response Team	Malaysia
PH-CERT	Philippine Computer Emergency Response Team	Philippine
SecurityMap	Securitymap Networks Computer Emergency Response Center	Korea
SingCERT	Singapore Computer Emergency Response Team	Singapore
ThaiCERT	Thai Computer Emergency Response Team	Thailand
TWCERT/CC	Taiwan Computer Emergency Response Team/Coordination Center	Chinese Taipei
TWNCERT	Taiwan National Computer Emergency Response Team	Chinese Taipei

General Members

Team	Official Team Name	Economy
BruCERT	Brunei Computer Emergency Response Team	Negara Brunei Darussalam
GCSIRT	Government Computer Security and Incident Response Team	Philippine

Steering Committee (SC)

The following APCERT members serve as Steering Committee (SC) for the second consecutive year, since the election held on 25 February 2003 at the APCERT Annual General Meeting held in Chinese Taipei.

AusCERT
CNCERT/CC
HKCERT/CC
JPCERT/CC
KrCERT/CC
MyCERT
SingCERT

Working Groups (WG)

The following Working Groups are formed within APCERT.

1. Accreditation Rule WG

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

2. Training & Communication WG

Objective: To discuss a training mechanism within APCERT (i.e. information exchange, CERT/CSIRT training)
Members: TWCERT/CC (Chair), AusCERT, KrCERT/CC, MyCERT and SingCERT

3. Finance WG

Objective: To discuss membership fee in the short run and develop a concrete scheme in the long run
Members: JPCERT/CC (Chair), AusCERT, HKCERT, KrCERT/CC, TWCERT/CC and TWNCERT

I. 2005 APCERT Steering Committee Report

A. APCERT SC Meetings

Since the last AGM in Kyoto, Japan, the SC held six teleconferences and two SC meetings in person.

B. APCERT Policies and Procedures Progressed

1. Finalised the APCERT Point of Contact Arrangements in June 2005 (which are now subject to AGM approval)
2. Established the Operational Framework (which are now subject to AGM approval)

C. Secretariat

During the last 12 month period, the Secretariat (JPCERT/CC) supported the SC through recording minutes and making meeting arrangements and has contributed fellowship funding for smaller APCERT teams.

D. New Team Applications

JPCERT/CC conducted a site visit of CERT-In as part of their sponsorship of CERT-In's application for APCERT membership. SingCERT has provided an application from BP DSCIRT to join APCERT and will follow up with a site visit and sponsor report to complete the process.

E. Web Site

JPCERT/CC has released a new APCERT.org web site. The APCERT web site will be updated further to enable APCERT member only access to POC contact details and other non-public APCERT documentation.

F. APCERT International Relationships and Engagements

SC members have been active in terms of promoting and representing APCERT in various international government and non-government forums. For example:

1. Achieved gaining recognition for APCERT as guest status on APEC Tel e-Security workgroup.

2. APCERT was represented, and gave presentations to APEC Tel e-Security workgroups in 2005.

3. Four APCERT SC team members briefed the ASEAN CIOs in Vietnam in March 2006.

4. SC members (JPCERT/CC and KRCERT/CC) are representatives of the FIRST SC.

5. In September 2005, CNCERT/CC hosted a symposium on "National Computer Emergency Response Capability Building and Regional Cooperation" for ASEAN countries.

6. SingCERT put up a proposal to ASEAN to conduct an incident drill for member countries. The proposal was accepted and the drill is planned for mid 2006.

7. JPCERT/CC represented APCERT at the TF-CSIRT meeting in Lisbon in September 2005.

8. AusCERT represented APCERT at the Organisation of American States in Brazil in September 2005.

9. AusCERT and JPCERT/CC attended the GovCERT.nl Symposium in the Netherlands in September 2005.

10. AusCERT represented APCERT at a meeting of European Government CSIRTs in Netherlands in September 2005.

11. As a result of some of these relationship-building activities, European Network Information Security Agency (ENISA), TF-CSIRT and Organisation of Amercian States (OAS) representatives will attend the APCERT AGM.

12. JPCERT/CC attended the International Watch and Warning Network (IWWN), a multi-lateral government forum, in Germany in October 2005 and gave a presentation about APCERT.

G. APCERT Incident Handling Drill

In December, APCERT teams conducted a cross-border incident handling drill. A full report of the drill will be provided by separately by KrCERT/CC.

H. APCERT 2006 (APCERT AGM)

APCERT 2006, 28-29 March 2006, Beijing, China
http://www.apcert.org/events/conferences/APCERT2006.html
http://2006.cert.org.cn/en/

APCERT organizes an Annual General Meeting for CERTs/CSIRTs and other computer security professionals dealing with security incidents. APCERT 2006 was hosted by CNCERT/CC, held in conjunction with the CNCERT 2006 Conference.

II. Activity Reports from APCERT Members

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

A. Report from AusCERT

Australian Computer Emergency Response Team – Australia

About AusCERT

AusCERT is the national CERT for Australia. As an independent, not-for-profit, non-government organisation, based at the University of Queensland, AusCERT is the single point of contact for the provision of advice about computer network threats and vulnerabilities in Australia. Through our range of international CERT contacts we also provide an incident response capability for Australian networks for attacks emanating from overseas and within Australia. With funding from the Australian government, AusCERT operates a National IT Security Incident Reporting Scheme and National Alerts Service.

AusCERT works closely with Australian government agencies, industry and IT vendors and services a range of subscribers throughout Australia, New Zealand and the Asia-Pacific region through the provision of computer security and incident handling advice. 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).

CSIRT relationships

As Chair of APCERT, AusCERT continues to build strong community trust relationships through information sharing, and cooperative arrangements that help support the Internet security of the economies in the Asia-Pacific region. AusCERT's involvement in APCERT has been an important factor in AusCERT's ability to provide effective incident response support to many Australian organisations and their customers affected by online ID theft.

APCERT, and its member teams, has in its relatively short time of operation, proven to be a vital strategic partner for AusCERT and one that AusCERT hopes to build upon in future for the benefit of all Asia-Pacific economies.

CSIRT training

During 2005, with continued funding from AusAID we provided CSIRT development training in the Asia-Pacific region. AusCERT is also continuing negotiations with the Attorney-General's Department on behalf of APEC to conduct CERT training in South American countries. AusCERT also assisted with the delivery of TRANSITS training within the region.

AusCERT also provides a range of training to Australian based organisations on various aspects of computer network security.

The International Systems Security Professional Certification Scheme (ISSPCS)

AusCERT, in partnership with partner EWA Australia and University of Queensland continues to grow to support a community of IT practitioners with applicants from around the globe signing-up for certification under what is becoming a well respected IT security certification.

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/

2005 Australian Computer Crime and Security Survey

In May 2005, AusCERT published the 2005 Australian Computer Crime and Security Survey in partnership with the Australian High Tech Crime Centre (AHTCC), the Australian Federal Police and every police law enforcement agency in Australia. Its production was sponsored by the Attorney-General's Department and Department of Communications, IT and the Arts and has remained a popular source of data about computer security attack trends and issues for Australia throughout the year. See: www.auscert.org.au/crimesurvey

AusCERT2005: Asia-Pacific IT Security Conference

AusCERT held its annual Asia-Pacific IT Security Conference at the Gold Coast in May 2005 at which around 900 delegates attended. The conference continues to show itself to be the premier IT security conference in Australia, conducted by IT security professionals for IT security professionals, IT managers and government decision makers in the field. See: http://conference.auscert.org.au/conf2005/

Public Key Infrastructure (PKI)

AusCERT continues to develop policies and standards to enable the collaborative use of Public Key Infrastructure (PKI) amongst and between Australian universities and to implement a prototype PKI system. This work should provide a basis for establishing a National Certificate Authority for international interoperation which is likely to be run by AusCERT under direction from CAUDIT and a managing committee. The purpose of the project is to implement secure access, authentication and authorisation of researchers, who access services and infrastructure across global networks.

B. Report from BKIS

Bach Khoa Internetwork Security Center – Vietnam

Activity report of 2005

We performed a national survey on Information Security (IS), using our website at www.bkav.com.vn, on December 2005. This is the second nation-wide survey on Information Security we have performed, which has over 3000 participants. According to this survey, 94% of PCs in Vietnam had been infected by viruses or Spyware in the year of 2005 (that is 1% drop compare to last year's report) and the damage goes up to 410.000VND (about 25USD) for each PC per year.

Spam is also a new, but very fast-growing problem. 79% of the person who were asked said that they receive spams daily. In Vietnam, the amount of spam is now probably bigger than the amount of ham. Since the late of 2005, we have developed an anti-spam solution. The experimental results are very promising. We hope to deploy the solution in the next few months, and help solving the spam problem.

During the year 2005, the Vietnam police have investigated several cases of making fake credit cards to get illegal money from public ATM. Some criminals have been arrested. This is a good sign in fighting against high-tech criminals in Vietnam. BKIS has played very active role in helping the police to investigate computer crimes.

Most of the attacks, which took place in Vietnam in 2005, are DDOS attacks. This fact shows that DDOS is the most popular attacking method among Vietnamese hackers, because the method is easy to implement and could deal a great damage. In April, a Turkish hacker group defaced some Vietnamese websites (including some websites of the government). Although the damage is not very high, this brings up a big issue about Vietnamese websites' security.

In 2005, there were 232 new viruses appeared in Vietnam. This is more than 176% increase, in comparison to 84 new viruses in 2004. Some of them are made by Vietnamese hackers. Some Vietnamese websites tried to exploit IE's and Windows' vulnerabilities, to install malwares on the victim's computers.

This is the list of top ten widespread viruses in Vietnam in 2005:

1. W32.LovGate.RB
2. W32.SoberX.Worm
3. W32.LovGate.R
4. W32.Mytob.Worm
5. W32.SkyNetP.Worm
6. W32.MytobV.Worm
7. W32.LovGate.RA
8. W32.SkyNetPN.Worm

9. W32.MytobM.Worm
10. W32.MytobS.Worm

Our anti-virus solution, Bkav, is updated regularly and has the average of 10.000 downloads per day. Besides supporting thousands of customers via emails and telephone; we also took part in designing computer networks for the Vietnam Office of the Government; giving consultations on Information security to governmental organizations and ministries such as Ministry of Home Affair, Ministry of Planning and Investment, etc; deploying anti-virus solution in some major banks and companies in Vietnam.

In the year of 2005, BKIS participated some conference on the subject of Internet security, e-government, e-commercial in Vietnam. Our solution, E-Office - which we brought to the e-government conference in Danang, VietNam on December 2005, received many good comments.

2005 is also a really busy year but we are happy with what we have achieved.

C. Report from CCERT

CERNET Computer Emergency Response Team – People's Republic of China

Incident Response

In 2005, CCERT has received 45,642 incidents reports, decreased nearly 14% compared with 2004. Taxonomy statistics of incidents reports are shown in figure 1. More than 81% of these incidents were related to spam, increased more than 10% compared with 2004. More than 200 times of phishing incidents were reported to CCERT in 2005, so we gained much experience in phishing incidents handling last year.

Figure 1. Taxonomy statistics

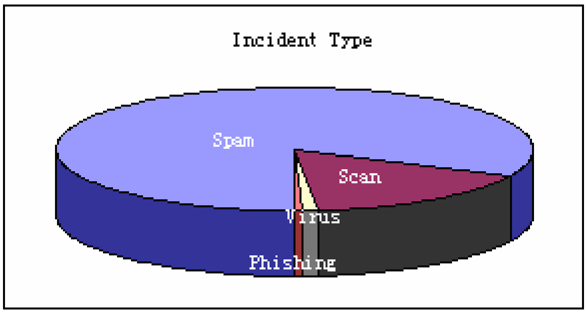


Table 1. Taxonomy statistics

Order	Taxonomy	Percent
1	Spam	81.99%
2	Scan	16.23%
3	Virus	1.10%
4	Phishing	0.51%
5	Intrusion	0.08%
6	Ask for Help	0.05%
7	Unknown	0.03%

More than 80% of these incident reports came from USA. Korea moved up from rank 3rd counted in 2004 to rank 2nd in this year and same time Japan moved down to rank 6th from rank 2nd.

The source of the reports is classified by the domain name or IP looking-up from APNIC WHOIS database. The rank of reporter sometimes implies security threats changing trend in his region.

Figure 2. Source of the report

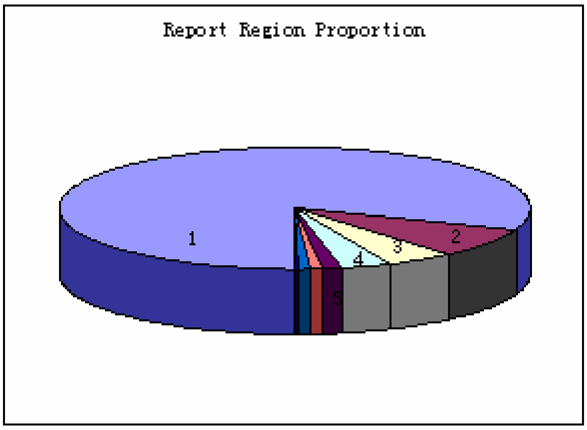


Table 2. Source of the report

Order	Country	Percent
1	USA	80.61%
2	Korea	8.04%
3	Canada	4.73%
4	Brazil	3.40%
5	China	1.32%
6	Japan	0.80%
7	France	0.75%
8	Other	0.21%
9	Australia	0.12%
10	Israel	0.02%

As responses to the most serious incidents, CCERT has published 2 advisories to the users of CERNET in 2005, much less than 8 advisories published in 2004. It seems there were no special incidents happened in 2005. These advisories are listed as follows:

2005-006 Advisory on How to defense the worm attacking MS05-051 vulnerability.

2005-004 Advisory on How to defense the Zotob worm and its variations.

Projects

1. Botnet Auto-discovery System

CCERT are developing a Botnet auto-discovery system, which can analyze all the suspect IP addresses got from border routers, and pick out which one is Botnet server and show the size of Botnet. Based on the result given by this Botnet auto-discovery system, we can control and mitigate Botnet inner CERNET conveniently.

2. Malicious Code Test-Bed

Test-bed has been developed nearly 2 years for monitoring malicious code behaviors in a controlled environment. This test-bed is composed of hosts with VM (virtual machines) and provides a GUI for malicious code management and analysis reports presentation. We have analyzed all the malicious code sent to the virus collecting mail-list (virus-submit@auscert.org.au) with the test-bed.

3. Data sets of Chinese emails

CCERT released a part of our database as data sets of Chinese emails for the purpose of research. They are of interest to all researchers working on the general problem of anti-spam. Now we are collaborating with TREC (http://trec.nist.gov) in putting a Chinese TREC Corpus. See http://www.ccert.edu.cn/spam/sa/datasets.htm for more details.

Events

1. Take part in APWG as individual member, and report more than 17 phishing sites to APWG.
2. In APCERT Drill 2005, CCERT contributed the video conference control center. During test, the teams including CCERT, CNCERT, JPCERT, KrCERT, SingCERT, AusCERT(with netmeeting) and a test point, total 7 points succeed to communicate simultaneously.
3. On the 9th Dec. 2005, CCERT captured a new worm, which was named Dasher worm lastly, and sent the alert to all of APCERT members in time.

Training

1. Email administrator Security techology and Application training,organized by ISC and CCERT Anti-spam Team. Apr. 2005
2. SpamAssassin, a typical anti-spam framework. Email administrator training, organized by ISC, Beijing, China, Apr. 2005,

Presentations

1. Hui ZHENG. *Deep Analysis into the Access Point Links of Phishing Sites.* NetSec 2005, Beijing, China.
2. Hui ZHENG. *Forensics Points in Phinshing Incidents Response.* CFAT 2005, Beijing, China.
3. Hui ZHENG. *Internet worm technologies.* CNCERT/CC 2005, Guilin, China.
4. Quang-Anh Tran. *Anti-Spam techniques and Chinese spam filter rules.* May. 2005, Shandong University, Shandong, China.
5. Quang-Anh Tran. *CCERT report on spam.* Nov. 2005, Chinese American Networking Symposium, Shenzhen, China.

About us

Founded in 1999, CCERT (China Education and Research Network Computer Emergency Response Team) is the first CSIRT(Computer Security Incident Response Team) in China and is a nonprofit organization who provides computer security related incident response service for people and organizations all over China, although our original intention is educational users. CCERT is one of the initial members of APCERT.

Address: 310#, Main Building,
Tsinghua University, Beijing, China, 100084
URL: http://www.ccert.edu.cn
Email: incidentreport@ccert.edu.cn
Tel: +86-10-62784301
Fax: +86-10-62785933

D. Report from CNCERT/CC

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

1. About CNCERT/CC

CNCERT/CC is a functional organization under Internet Emergency Response Coordination Office of Ministry of Information Industry of China, who is responsible for the coordination of activities among all Computer Emergency Response Teams within China concerning incidents in national public networks. It 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 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. Thus CNCERT/CC stands for a new platform for better International cooperation and a prestigious interface of network security incident response of China.

CNCERT/CC's activities include information collecting, event monitoring, incident handling, data analyzing, resource building, security research, security training, technical consulting, and international exchanging. (See http://www.cert.org.cn/en for more information)

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. Network Security Monitoring and Analysis

The 863-917 Network Security Monitoring Platform established and operated by CNCERT/CC is the core platform of network security incident monitoring in China up to date, which has been 7x24 non-stop running and monitoring on network security incidents.

2.1 Traffic Monitoring

The statistic result of sampling traffic data shows that, the most bandwidth consuming application is Web Access (37.82) and P2P File Sharing (15.43). The email traffic through port TCP 25 is about 6%, which consist of not only normal email but also great deal of spams caused by worms and spamers. TCP 135/445 were usually used by attacks. Most of Bots we detected take use of those ports to spread.

Since April 2005, there is a huge number of spam messages sent through port UDP 1026/1027. The

corresponding traffic has been much higher than email, only lower than the Web Access and P2P. Under relevant parties' measures, it has finally been constrained successfully.
In the second half of 2005, CNCERT/CC handled 78 incidents detected by traffic monitoring. 50% of the incidents were caused by SQL Slammer.

2.2 Trojans Monitoring

In 2005, CNCERT/CC made sample monitoring of 28 popular kinds of Trojans and found more than 22,500 IP hosts had been planted with Trojans. The hosts are distributed in most provinces of mainland. The top 7 provinces Trojans hosts lied in are Guangdong (21%), Shanghai （15％）, Jiangsu (10%), Zhejiang (9%), Beijing (7%), Fujian (6%) and Hubei (4%). The hosts in other province totaled up to 28%.

Meanwhile, CNCERT/CC found more than 22,800 IP hosts outside China's mainland had some communication with those Trojan hosts. The distribution of percentage is: USA (25%), Chinese Taipei (18%), Hong Kong China (18%), Japan(12%), Canada (4%), Korea (4%), Australia (3%), Unite Kingdom (2%), and others (14%).

2.3 Spyware Monitoring

In 2005, CNCERT/CC made a sample monitoring on 30 kinds of usual Spyware and found more than 700,000 IP hosts had been planted with Spyware. Those Spyware secretly delivered users' private information to corresponding control servers, fetched keywords for data stealing and downloaded update version from the control servers. Those control servers mainly lay outside Chinese mainland. The top 2 countries with the control servers were USA (42) and Korea (26).

2.4 Website Attack Monitoring

CNCERT/CC's 2005 sample monitoring on 50 popular kinds of website attack found that 220,000 foreign hosts had frequently launched attacks to websites in China's mainland. The counties and regions which launched the most frequent attacks to mainland's websites are USA (40%), Japan (11%), Chinese Taipei (10%) and Korea (8%).

2.5 Botnet

Everyday, CNCERT/CC kept detecting newly emerging BotNets and monitoring the BotNets which once appearred . The scales of Botnets which we found differed from hundreds to more than 10 thousands. From January to December, the number of active BotNets in scale of more than 5000 Bots was 143. The biggest Diablo BotNet had about 157 thousand hosts at the most . Those BotNet continuously expanded, upgraded, downloaded spyware and Trojans, and launched all kinds of DoS attacks. CNCERT/CC also detected some botware which hid themselves by rootkit techniques. Due to concealment of Bot, there may appear ,more such kind of botware by use of rootkit in future.

The BotNet scale is getting smaller and smaller. The BotNets in scale from 1 to 10 thousand were the most favorites of attackers.

3. Incident Handing

3.1 Incident Reports

In 2005, CNCERT/CC received more than 120 thousand incident reports from domestic and international users and agencies, 93% of which are scan incidents. The number of non-scan incident reports is 9112. The total number of both scan and non-scan reports doubled in comparison with that in 2004.

Regarding the non-scan reports, most of them were about webpage defacement (8130), phishing (475) and spam email (161).

The number of non-scan reports from international agencies is 464. Most of them were about phishing (456) and some of them were about Trojans. The top 10 phishing incidents reporters were eBay(207), MarkMornitor(43), Brandimension(22), BFKCERT(17), VeriSign(17), AUSCERT(15), Inter identitiy(14), MasterCard(13), HSBC(10), Royal Bank of Scotland(10), KrCERT/CC(7), Citigroup(6).

3.2 Incident Handling

In 2005, CNCERT/CC handled more than 400 incidents, most of which were handled by CNCERT/CC Branches around each province. The incidents included webpage defacement, phishing, host intrusion, DoS and malware. Of all kinds of incidents, the webpage defacement and phishing occupied a majority with 53% and 31%.

3.3 Significant Incident Handling

3.3.1 Abnormal Traffic on UDP1026 and1027

From June to July 2005, through 863-917 platform CNCERT/CC detected a rush increase traffic on UDP 1026/1027 which soared to 11.49% of total traffic. Analysis result shows that the abnormal traffic results from large mount of junk messages sent by hackers through Windows Message Service. CNCERT/CC located and stopped the source hosts and suggested ISPs take responsive filtering measures. The traffic was reduced by nearly 3Gbps after an ISP followed the advice.

3.3.2 Vigilant on domestic and international hackers’ activities around 8.15

The report by a Hong Kong newspaper that some “China Honker” planned to launch attackes against Japanese rightist websites on 8.15 possibly through some Korean hosts was widely transcribed in China, Japan and Korea. CNCERT/CC kept vigilant on the hackers’ moves and contacted with JPCERT/CC and KrCERT/CC to have continuous knowledge of the hackers’ activities in Japan and Korea. But we did not find any sign of organized actions of hackers. It turned out that no such events happened as the media reported.

3.3.3 Toxbot

October 17th 2005, CNCERT/CC received a report from SURFnet CERT that more than 290 thousands Chinese computers were infected with W32/Toxbot and ran as members of a huge BotNet which consisted about 1.2 million computers. CNCERT/CC responded quickly on this report with several measures including studying the method of detecting and cleaning, warning ISPs and partners to make self-examination and raise public awareness of security consolidation.

3.3.4 Dasher.B

December 15th 2005, CNCERT/CC detected a new worm (Dasher.B) which exploits a newly announced highly risky vulnerability (MS05-051). After intruding, the worm will connect to a control server in Changsha, Hunan Province, to fetch hacker's instruction, and then connect to a ftp server assigned in hacker's instruction as a dynamic domain name to download key logger and worm body. Under CNCERT/CC's coordination, local branch quickly located and stopped the control server and ftp server so that a potential wide spread was successfully stopped from the beginning. CNCERT/CC also published relevant advisories to suggest users check and enhance their systems.

3.3.5 Phishing of West Pacific and MasterCard

October 25th 2005, CNCERT/CC received IBM-CERT's report that a Chinese computer was running a phshing site of Bank West Pacific. During the handling process, CNCERT/CC found some clues of another phishing action. and a file of eleven credit card users' information, including name, address, card number, ATM password, birthday, transaction security number. CNCERT/CC carefully queried partners about the relevant banks. According to an APWG member's hint, CNCERT/CC ascertain that these information belonged to users of MasterCard. Then CNCERT/CC contact with MasterCard and return the file in time.

3.3.6 DoS

Attacks of DoS still often occurred in 2005 and cause huge damage. In January, CNCERT/CC stopped a severe DDoS launched from a huge BotNet. The BotNet caused about 1G bps traffic to the target with more than 11 kinds of DoS techniques. The victim's business completely collapsed with direct loss of more than one million RMB. With the cooperation of CNCERT/CC, the police successfully arrested the attacker who intended to break down competitor's business by such means.Besides, CNCERT/CC also successfully handled some other severe DoS incidents, such as the attack on a website of human resources service in Shenzhen in April, the attack on a domain name registrar and virtual host provider in August.

3.3.7 Web Page defacement

In 2005, CNCERT/CC detected about 13.7 thousand web page defacement incidents in China. Hereinto the defacements on governmental web site of China's mainland totaled up to 2027, occupying 22% of all. This ratio is significantly bigger than the ratio of 2.2% that governmental websites occupied of all website, which showed that the Chinese governmental websites were the most likely to be attacked. So it is a pressing task to improve the safety of governmental websites.

4. Security Information Service

In 2005, CNCERT/CC enhanced the security informing service to ISPs and cooperative key infrastructures, as well as to relevant government agencies. More than 2 hundred of interior warnings and 75 critical vulnerability advisories were delivered in time.

More than 440 articles were published on CNCERT/CC's website, including security announcements, vulnerability advisories, malware warnings, technical reports, safety guidence, etc. After CNCERT/CC'2005 annual conference, CNCERT/CC particularly published all the conference materials on the website for public references. The materials has been widely referenced and quoted by both domestic and international network security agencies.

Besides website, CNCERT/CC also delivered information services directly to users by email, so that the users can be informed in time. By far, CNCERT/CC email subscriber groups includes CNCERT/CC branches, ISP CERTs, Pilot Internet Security Service Providers of MII, Technical Supporting Organizations, NSC-ISC members, TRANSIT-Guilin trainees, and China-ASEAN 2005 NetSec Trainees, etc.

5. Netsec conference and training

In 2005, CNCERT/CC organized many public activities on internet security and emergency response to raise the security awareness of government, industry and netizens.

- CNCERT/CC'2005 Annual Conference, March 24th~25th , Guilin City
- TRANSIT Training of FIRST, March 22nd~23th, Guilin City
- China-ASEAN Computer Emergency Response Capability Building and Cooperation WG, September 9th~12th, Beijing
- 'Healthy Wang Zhong Xing' TV Contest of NetSec Knowledge, September 17th, Beijing
- 2005 China Internet Security Emergency Response Drill, December 12th , Beijing.

6. International Cooperation and Communication

In 2005, CNCERT/CC took active part in international events.

- APCERT2005 on February 22nd~24th, voted as Deputy Chair.
- 31st APEC Tel on April 3rd~8th
- 2nd China-Japan-Korea Network and Information Security Workshop on June 9th
- ASEM Network Security Workshop on June 23rd~24th
- 17th FIRST Annual Conference on June 24th~July 2nd
- ITU WSIS Thematic Meeting for Cybersecurity on June 28th~July 1st
- 32nd APEC Tel on September 5th~9th
- APCERT 2005 Incident Handling Drill on December 12th

7. Conclusion

In general, there was no large scale of network security incident with grave consequences. The worms spreading by exploiting vulnerability doesn't play as leading actors any more. Instead, malwares with representatives of bot, spyware, identiy thieft code became the top threat. Meanwhile, DoS, phishing and spam email were still rampant. Besides, there were many network attacks incidents related to political events and memorial days in 2005. With a remarkably increase of total number, the security incidents in 2005 were characterized by the complexity of techniques, profit tendency and political motivations.

Since the hackers' motivation has changed, there will be less possibility of large scale severe incident in 2006. The incidents of malware, phishing, pharming, etc will continuously increase, as well as the attack on new computer applications. All these problems will result in the constant increase of total incident number.

Altogether, with the rapid continuous development of Internet in China, the security situation will be sophisticated and critical more and more. As the basic technical supporting agency on network security, under the lead of MII, CNCERT/CC will further work around the main task of capability building and service widening, to enhance the function of network monitoring and incident analyzing and management, expanding and exerting the function of emergency response system, and fully boost the public network security protection.

E. Report from HKCERT/CC

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

Summary

Growth of home broadband in Hong Kong is prevalent. HKCERT had expanded its services to include home users and school networks. In the past year, we experienced a drop in the number of incident reports and yet the level of sophistication of attacks increased. We are dealing more and more with unknown attacks and non-recoverable compromises. Crime related attacks increased in the past year resulted in closer collaboration with the local law enforcement agency. We anticipate that the trend of increasing malwares, botnets will continue. Home users, school networks and Small-to-medium Enterprises (SMEs) will continue to be breeding bed of botnets. HKCERT will take a more proactive approach and closer collaboration with other CERT teams to meet the new challenges.

Incident Report Statistics

In 2005, HKCERT received 2,223 incident reports, including 846 virus incident reports and 1,375 security reports (See Figure 1). It is clear that the number of security incident reports is overtaking virus incident reports.

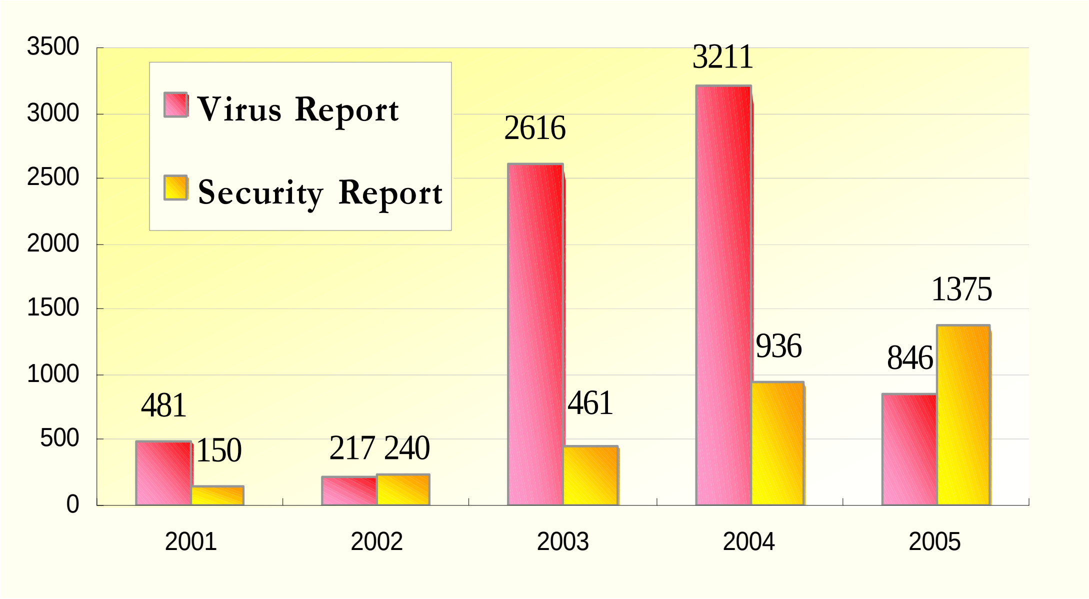


Figure 1. HKCERT incident report statistics 2005

Analysis of Composition of security alerts

Further analysis of the partitioning of security incident indicates that the number of spyware incident reports accounted for over 60% of all security incident reports. The next higher count is the number of phishing incident reports. (See Table. 1)

	2003	2004	2005
Other security incident reports	461	783	206 (15%)
Phishing Incident reports		73	211 (15%)
Spamming incident reports		80	82 (6%)
Spyware incident reports			**876 (64%)**
All security incident reports	**461**	**936**	**1375 (100%)**

Table 1. Distribution of security incident reports in 2005

The major cause of the change is attributed to the financial motivation of hackers. In order to sustain the compromised computers for longer period for money-making activities, security attacks are more targeted, stealthy and silent. The total number of incident reports is lowered and yet the attacks are now more sophisticated. The malwares are harder to be detected and removed.

General Activities highlighted

During the period, HKCERT had:

- published 8 virus alerts and 108 security alerts on our web site;
- published 12 issues of newsletter and sent out the alert summary two times each month;
- published the results of the annual Information Security Survey in early 2005;
- published an Information Security Guide for Small and Medium Enterprise, in both English & Chinese;

- continued to work closely with the government and law enforcement agency, and held meetings to exchange information and to organize joint events regularly;
- participated in the government committees on Information Infrastructure Liaison Group and Information Security Task Force;
- worked closely with police in pinning down phishing web sites;
- organized the Information Security Summit 2005 with other organizations and associations in November 2005, inviting local and international speakers to provide insights and updates to local corporate users

Major Events Highlighted

1. Fighting against Malware and Botnet

The growth of spyware was a concern to HKCERT. In February 2005, Hong Kong Monetary Authority, Hong Kong Association of Banks and some local banks contacted HKCERT for assistance. Some of the banks discovered their users were infected by a certain spyware. HKCERT delivered two internal briefings for banks and one public seminar dedicated to spyware. HKCERT also provided support to local banks in their campaign of notifying the affected users. We have provided technical advice to more than 300 users in dealing with the suspected undesirable software.

In November 2005, HKCERT worked with the HKSAR Government in organizing a security awareness programme called the “Clean PC Day” campaign, which included public seminars, promotional pamphlets and stickers, and the distribution of security software. The activities also helped the end users in cleaning up their PC from malware infections and prevented them from becoming part of the botnet.

2. Providing support for WTO MC6 cyber security assurance

The 6th Ministerial Conference (MC6) of the World Trade Organization (WTO) was hosted by Hong Kong in December 2005. To provide the cyber security assurance, HKCERT worked closely with the government and law enforcement agency, local ISPs, and other infrastructure providers to monitor the Internet health on 24x7 basis and provided intelligence and analysis in the alert period. HKCERT also obtained supports from some APCERT teams to provide the health status information in the region. Fortunately, there was no major issue identified in the cyber world.

3. Promoting Security Awareness in the Education Sector

In the first half of the year, we noticed that a number of schools were hacked and became hosts to phishing web pages. There was a grave concern from the law enforcement agency. HKCERT presented a number of public briefings to the education sector to alert them of the growing trend of malware and botnet. Some attending schools invited HKCERT to school visits and to delivering seminars for teachers and parents. The Education and Manpower Bureau of the HKSAR government also sought advice from HKCERT on how to assure security of schools.

Looking Forward

The change of cyber attack profile has resulted in different approaches in tackling these new threats. We have to proactively monitor the stealthy security compromises. HKCERT had proactively monitored the defaced web sites within .hk domain and contacted the web site owners should the defacement persist. Other than defacement, we see the need of active monitoring of Internet security status from a local perspective to provide intelligence for preempting attack buildup and to assess local cyber risks. Such kind of local weather report of Internet requires a dedicated Distributed Network Monitoring System to be installed and continuously managed. We shall acquire the necessary knowledge from the CERT community to identify the feasibility of setting up one in Hong Kong.

About HKCERT

HKCERT was founded in 2001 by HKSAR Government and is under the operation of Hong Kong Productivity Council. The constituencies include small and medium business and home users. HKCERT acts as a centralized contact on computer and network security incident reporting and response for in case of security incidents. She coordinates response and recovery actions for reported incidents, help monitoring and disseminating information on security related issues, and provide advice on preventive measures against security threats.

URL:	http://www.hkcert.org
Email:	hkcert@hkcert.org
Tel:	(852) 8105 6060
Fax:	(852) 8105 9760

F. Report from JPCERT/CC

Japan Computer Emergency Response Team/Coordination Center – Japan

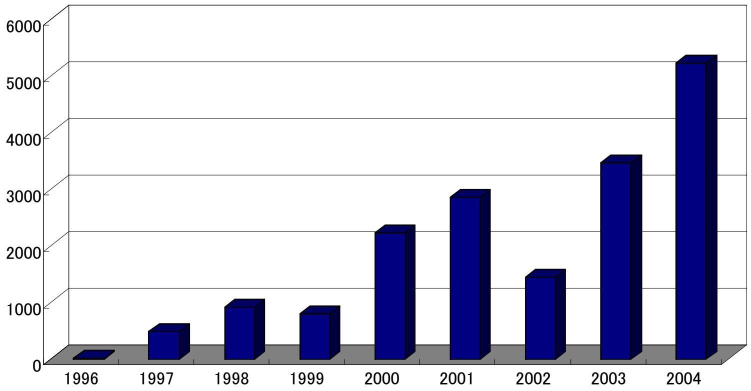
JPCERT/CC is a first CSIRT (Computer Emergency Response Team) established in Japan. It is an independent non-profit organization, acting as a national point of contact for the CSIRTs in Japan and worldwide. Since its inception in 1992, the center has been gathering computer incident and vulnerability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

Incident Statistics and Trends

In 2005, JPCERT/CC issued 3,429 tickets responding to computer security incident reports received from Japan and overseas. A ticket number is assigned to each incident report to keep track of the development. Among the 3,429 tickets, 3,020 tickets were related to probe, scan, and attempts that did not result in serious damages.

	1st Qtr	2nd Qtr	3rd Qtr	4th Qtr	Total
Tickets Issued	1240	695	667	827	**3429**

The incident reports that JPCERT/CC received since 1996:



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

Source of Incident Reports

As the table below shows, JPCERT/CC received incident reports primarily from .au, .net, and .jp. Notably, a number of reports from Australia and .net were more than that of Japan.

ISO Code	1st Qtr	2nd Qtr	3rd Qtr	4th Qtr	Total
.au	1	4	3	5	13
.net	843	215	386	109	1553
.jp	226	260	272	397	1155

Education and Training

We offer seminars, workshop, and internship targeting system administrators, network managers, technical staff who are interested in learning computer security. Some of the events organized by JPCERT/CC in 2005 are listed below:

- JPNIC-JPCERT/CC Security Seminar 2005- a series of 3 security seminars jointly organized with JPNIC (6-7 & 20 Oct and 8 Nov 2005)
- InternetWeek 2005 in Yokohama – one day security track jointly organized with Japan Network Security Association (JNSA) and Telecom-ISAC Japan (8 Dec 2005)

Projects

1. Internet Scan Acquisition System (ISDAS) Project

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

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

The project was initiated in 2001 with the objective to gather the vulnerability information about the domestic products and to provide the information in Japanese on the Internet. The JVN website therefore lists a type of vulnerability, affected hardware or software, possible damage, technical tips, vendor information, and reference documents. This began as a joint project with JPCERT/CC and Keio University. The project team works closely with domestic vendors, including software/hardware/OS/router vendors, as well as network service providers. And now, JPCERT/CC and Information-technology Promotion Agency, Japan The Information-technology SEcurity Center (IPA/ISEC) operate this project.

http://jvn.jp/

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

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

Also, the following vulnerability information has been published on JVN in 2005.
-For vulnerability information reported within Japan, 50 cases were published.
-For information provided by CERT/CC, 29 Technical Alerts and 42 Vul Notes were translated and published.
-For information provided by NISCC, 8 cases were translated and published.

Activity Highlights

APCERT Secretariat

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

FIRST Related Activities

- The organization maintains a replica server for Forum of Incident Response and Security Teams

(FIRST) in Japan.

http://www.first.org/

- JPCERT/CC provided a program committee chair (co-chair) for the FIRST Annual Conference in Singapore (Jun. 2005).

Incident Object Description and Exchange Format (IODEF)

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

Security Industry Forum

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

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

G. Report from KrCERT/CC

Korea Internet Security Center – Korea

I. Introduction

KrCERT/CC(in other words, KISC, Korea Internet Security Center) serves as the nationalwide coordination center in Korea doing the task of detecting, analyzing and responding internet incidents such as worm, bot or hacking. To minimize the damage from those incidents and to ensure more secure internet environment, KrCERT/CC is seamlessly operating on 24/7 basis.

II. 2005 Activities

1. The trend of Incidents Reports to KrCERT/CC in 2005

Incident Reports[1] to KrCERT/CC consist of malicious codes, hacking incidents and so on. Malicious codes can be categorized down into Worm, Trojan, Virus and etc. Hacking incidents can be categorized down into spam relay, phishing site[2], general hacking case and homepage defacement. The number of reports on malicious codes in 2005 is 16,093 and that on hacking incidents is 33,633.

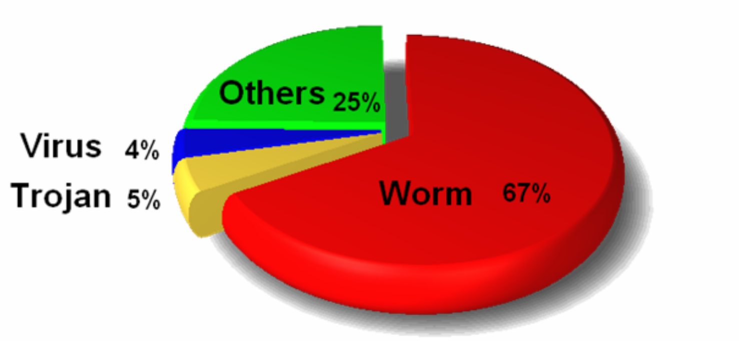
[1] **Reported to KrCERT/CC by e-mail or phone**

[2] **Although any phishing case targeting for Korean companies, such as bank or financial service company, has not occurred yet, many phishing sites targeting for foreign companies have been found in Korea. Foreign hackers exploit Korean websites for the tool for obtaining the personal finance information.**

This fact shows that the damage from hacking incident is severer than that from malicious code. In addition, it means that the major trend of cyber attacks has moved from the malicious codes to hacking incidents.

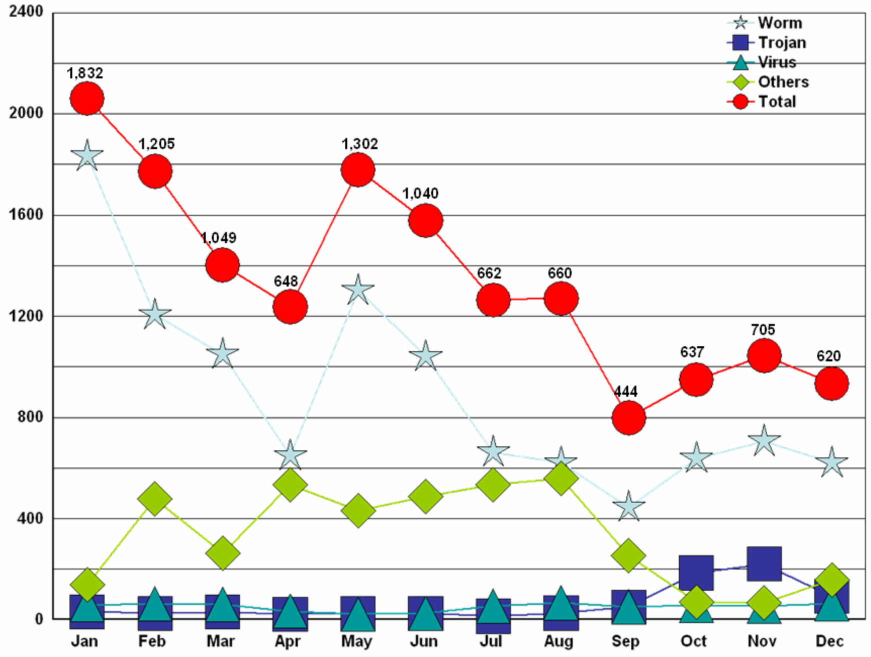
a. Incident Reports on Malicious Codes in 2005

The total number of incident reports on malicious codes in 2005 is 16,093. Among malicious codes, the number of reports on worm takes the highest one(10,764 cases). Trojan (746 cases) takes the second and virus (611 cases) the third.



(Figure 1) The percentage of reports on malicious codes in 2005

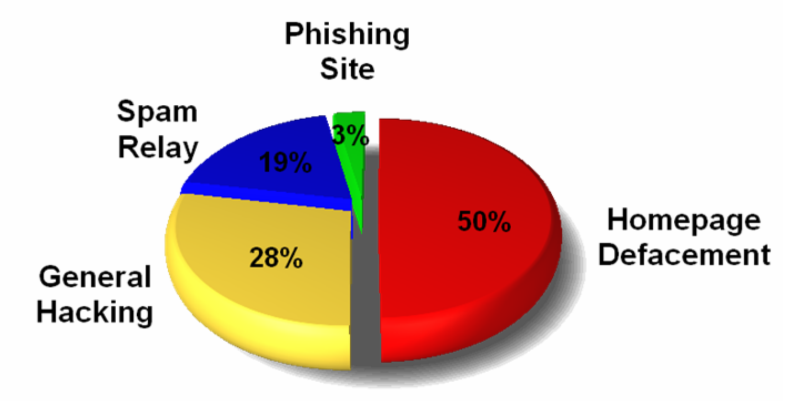
Fig. 1 shows that most of incident reports are related with worm. It takes over the half of the reports (67%). Although there exist variations on the monthly number of incident reports in 2005, the general trend of reports on malicious codes decreases.



(Figure 2) Monthly statistics of incident reports on malicious codes in 2005

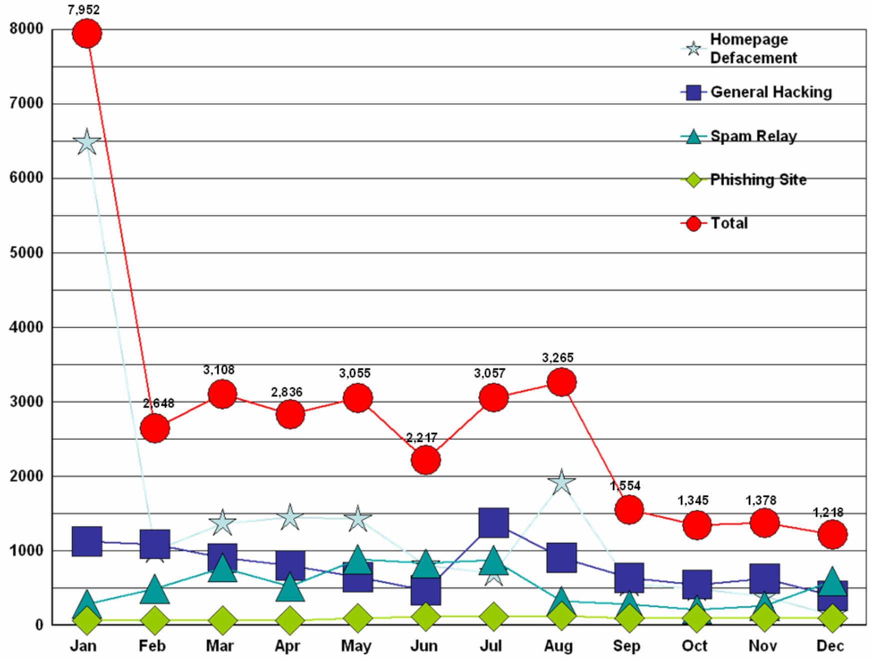
b. Incident Reports on Hacking Incidents in 2005

The total number of incident reports on hacking incidents is 33,633. Among the reports on hacking incidents, homepage defacement(16,692) takes almost half of the reports on hacking incidents and increased more than 3 times than that in 2004(4,812 cases)



(Figure 3) The percentage of reports on hacking incidents in 2005

Except the general hacking cases, reports on spam relay(6,334) and phishing site(1,087) increased more than 2 times than those in 2004(spam relay: 3,297, phishing site: 220)



(Figure 4) Monthly statistics of incident reports on hacking incidents in 2005

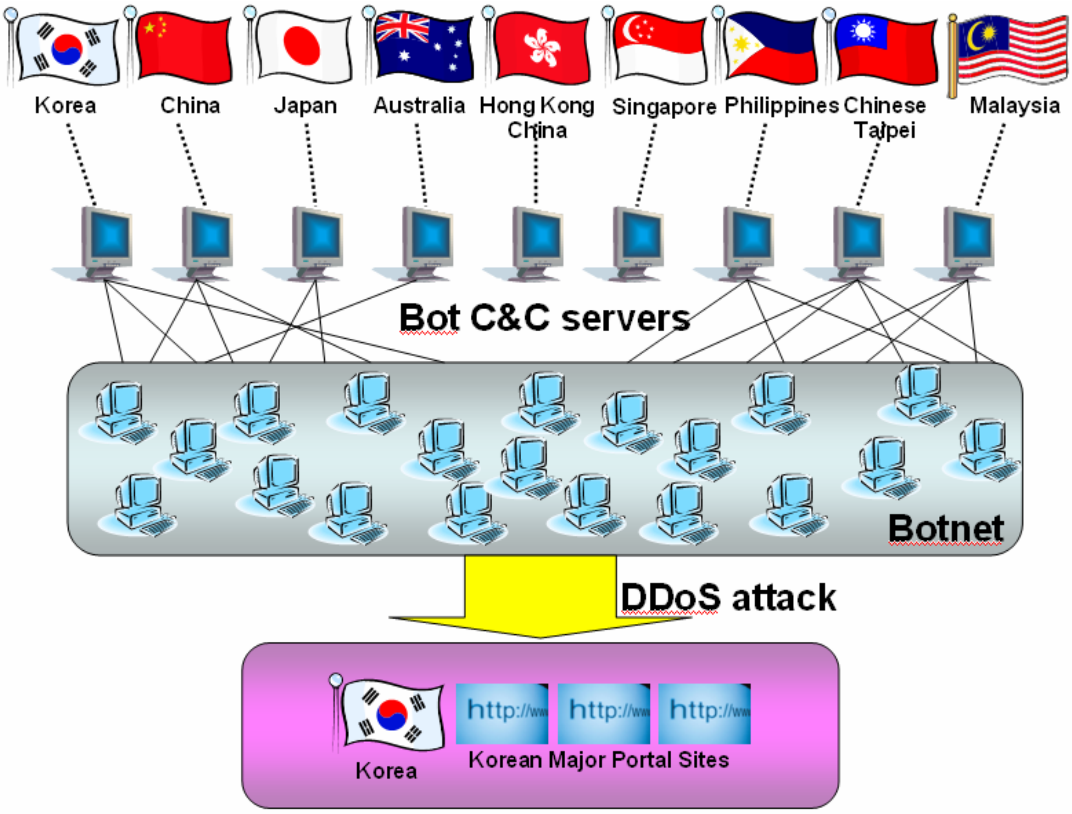
Especially in January, massive homepage defacements were done by some foreign hacker group. Almost half of the homepage defacements in 2005 occurred in January. The group exploited vulnerabilities of PHP and BBS programs, hacked multiple web servers managed by hosting company with the same IP addresses with the automatic hacking tools, inserted the same defaced page for the main page.

The reports on phishing sites increased more than 5 times than those in 2004. This increasing trend will last fro several years to come. The most targeted industry sector is financial service. The main stream of cyber attacks is changing to pursuing the financial gain. This stream will not change easily.

2. KrCERT/CC Activities in 2005

a. International Joint Incident Handling Drill

Most of cyber threats are not limited to one economy. Since Internet is the borderless and seamless network connecting the world, the cyber threats and attacks can spread regardless of the border of economy. This calls for the international cooperation in incident handling



(Figure 5) APCERT International Joint Incident Handling Drill

The drill was to verify the coordination capabilities among CSIRTs on incident handling framework, deliver action plans to improve incident response system in each CSIRT, and give participants an experience of a coordination system in case of emergency. For the preparation, 24/7 POCs were shared and the video conferencing were tested as the alternative communication channels. During the drill, 10 APCERT teams from 9 economies joined to shut down the botnet C&C servers within their economies. Although there were some gaps in handling the shut-down, the drill was successful and most of teams wanted to exercise periodically.

b. 2005 APISC Security Training Course

To support strengthening the response capabilities of the developing economies, KrCERT/CC held the training course on establishing and managing CSIRT(2005 APISC Security Training Course) from 29th August to 2nd September in Seoul. 27 trainees from 10 economies, within Asian region, participated in the course. Trainers from AusCERT and CNCERT/CC led some classes.

The course consists of 5 day classes, one day for the introduction of information security and KISA, three and half days for TRANSIT(lecture and case discussion), one half day for the tour. Most of the attendees were satisfied with the course. Much time is allocated to the discussion and active interaction and participation from the trainers as well as the trainees made it possible for the course to be successful and fruitful.

c. 2005 ASEM Cyber Security Workshop

KrCERT/CC hosted the Asia and Europe intergovernmental event ‘2005 ASEM Cyber Security Workshop(23rd ~ 24th June). The workshop was the first ASEM official meeting to discuss dedicated to discuss cybersecurity issues. The delegates from ASEM economies and International Organization, such as OECD, multi-national companies participated and shared their experiences and knowledge.

d. Websites infected with malicious links and programs

Many Korean major websites, which the internet users frequently visit, are hacked and inserted with some malicious codes. The malicious code is inserted to a website to make users to download the malicious code without any recognition. Users cannot see any difference or anomaly in the homepage. Most of the administrators, as well, are not aware that the malicious code is inserted and information leaks. Unlike the defacement of homepages, the website is operating fine as usual. Consequently, the link inserted in the page leads to a malicious code which can be downloaded to compromise the local system.

Many malicious codes, such as Trojan, linked from malicious links of websites are for obtaining the user ID and password of Korean on-line games. Like the phishing cases, the information collected from those sites can be used for the on-line crimes, obtaining the illegal financial gains, such as selling the on-line game items with other people identities.

KrCERT/CC developed the system to detect whether malicious links are inserted in the websites. KrCERT/CC monitors major domestic websites and notifies to administrators that the malicious links are inserted.

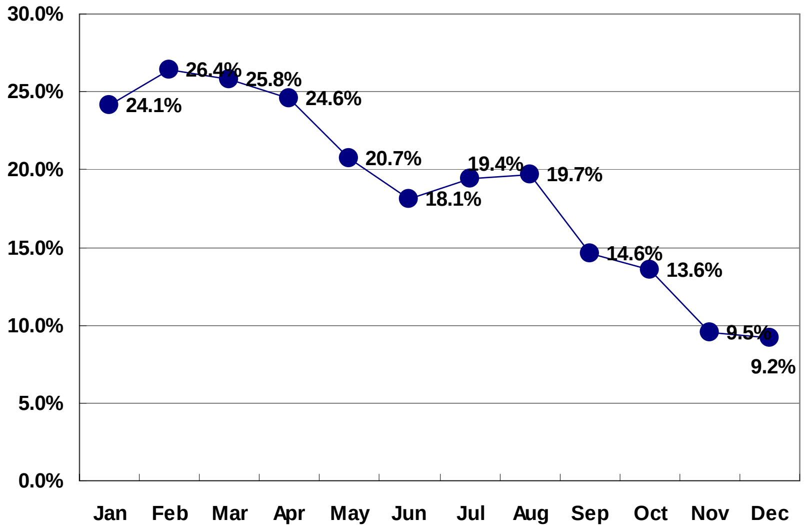
e. Efforts to reduce the bot infection rate

One of the worst cyber threats in the recent years is “BOT”. Bot can spread itself by e-mail or by the vulnerabilities of Microsoft Windows. Hackers can even set up the network consisting of thousands or millions of bot infected PCs(botnet) for other cyber attacks. Bot infected computers (Zombie) can be used for cyber attacks, such as zombies for DDoS and spam mail server and etc.

In the beginning of 2005, the bot-infected PCs in Korea took 24.1% of the bot-infected PCs of all over the world[3]. This information analyzed from KrCERT/CC’s Bot Detection System shows that Korea took almost one quarter of all bot-infected PCs ranked the 1st or 2nd most bot-infected country. The potential damage from bot or botnet is very severe

KrCERT/CC began to work on reducing the domestic bot infection ratio. Based on the information collected, the domestic and foreign bonet C&C server, which Bot herders use for commanding and controlling the Zombie PCs(bot infected PCs), were identified and removed from the network. The cooperation with major ISPs, where domestic servers reside, to shut down botnet C&C servers automatically contributes to the success of the mitigation in bot infection rate. The infection rate in the end of 2005 fell down to under 10%, almost one third than that of the beginning of 2005.

[3] **This statistics is analyzed from KrCERT/CC’s honeynet and honeypot system in Seoul, Korea. KrCERT/CC is operating Bot Detection System on real-time basis. The system collects IP addresses infected by bot in the world.**



(Figure 6) Domestic bot infection rate

III. 2006 Plan

First of all, KrCERT/CC is happy to have an experience to work with APCERT members, especially like the joint international drill. The drill in 2006 will be the opportunity to improve the response capabilities again.

Second, KrCERT/CC is planning to open CERT-building training courses to Asia-Pacific undeveloped countries which don't have enough resources or capabilities to build CERT by themselves. The training course will be a part of APEC project organized by KrCERT/CC.

Thank you.

POC:

Web site: http://www.krcert.or.kr
E-mail address: cert@krcert.or.kr
Telephone number: +82-118

H. Report from MyCERT

Malaysian Computer Emergency Response Team – Malaysia

Background

Malaysian Computer Emergency Response Team (MyCERT) was formed in 1997 and provides a point of reference for the local Internet community to deal with computer security incidents and methods of prevention. MyCERT is a unit under the National ICT Security & Emergency Response Center or NISER. NISER, a not for profit organization, was formed to address ICT security issues in Malaysia. NISER is under the supervision of the Ministry of Science, Technology and Innovation (MOSTI), Malaysia.

MyCERT acts as an independent focal point for Malaysian hosts, which allows both local and international experts, incident response teams, vendors, clients and law enforcement agencies, to cooperate and conduct vital technical and remedial action at sites affected by computer security incidents.

MyCERT's rapid response in analyzing problems and providing solutions can help the nation, organizations or companies to minimize damage from attacks and prevent further unauthorized activity.

Incident & Abuse Statistics:

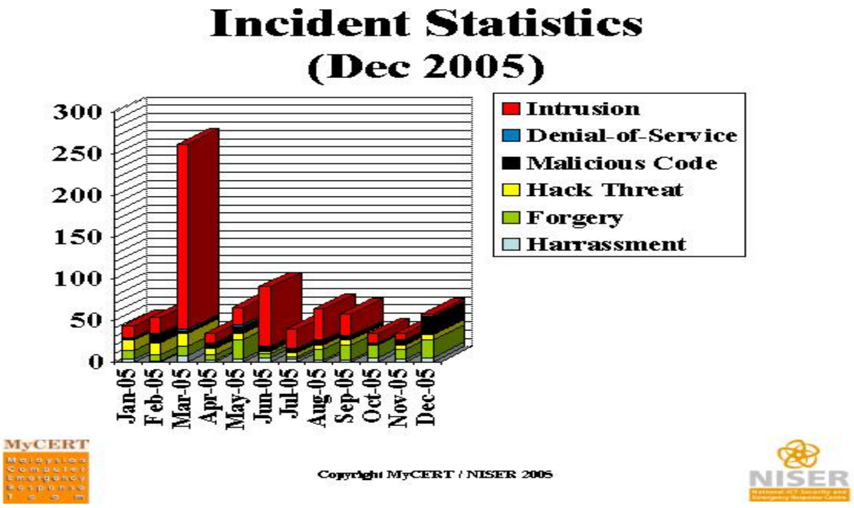
In 2005, MyCERT received a total of 10,147 incident reports with spam being the highest. MyCERT estimated about 75% of reports received in 2005 were from local constituency and the rest were from overseas. Though the number of incidents had dropped slightly by 33.6% as compared to year 2004, the complexity of incidents reported to us had increased. Nevertheless, incidents reported to MyCERT were managed successfully.

A total of 9,282 spam incidents were reported in 2005, which was a significant drop from 14,371 reports in 2004. The main reason for this significant decrease could be due to local ISPs and organizations applied anti-spam filters at their gateways to filter out spam emails. This was a positive measure in minimizing spam activities in the country.

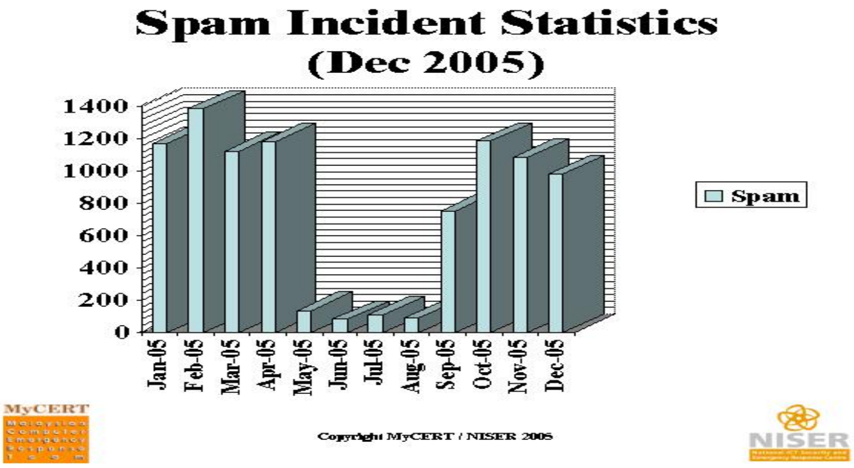
Meanwhile, harassment incidents had slightly dropped this year with a total of 43 reports compared to 47 reports in year 2004. Majority of harassment incidents were referred to the Law Enforcement Agencies for further investigation.

2005 also saw a decrease in malicious code incidents with a total of 82 reports received as compared to 242 reports in 2004. This was a positive progress and for 2005, we did not observe any worm outbreaks that had affected our ICT infrastructure.

Below is the statistics for Security Incidents reported to MyCERT in 2005:



	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
Harassment	3	1	8	2	3	5	3	2	2	6	3	5
Forgery	11	8	11	7	24	5	4	13	18	15	12	21
Hack Threat	12	14	15	7	7	3	4	6	6	0	6	7
Malicious Code	3	11	3	6	9	4	5	5	6	2	6	22
Denial of Service	0	1	2	1	2	1	0	0	0	0	0	0
Intrusion	15	18	223	11	20	72	23	37	26	11	8	3
TOTAL	44	53	262	34	65	90	39	63	58	34	65	58



	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
Spam	1172	1385	1126	1183	135	82	107	91	754	1184	1083	980

Security Trend Analysis

Based on our analysis of the incidents reported to MyCERT from our constituency, the following security trends in year 2005 were observed:

Forgery

Incidents on Forgery saw a tremendous increase of 40.6% this year as compared to previous years, with main contributor being phishing activities, which in fact had been a worldwide trend throughout 2005. Phishing had become a serious issue in Malaysia in 2005 due to the increasing number of reports received from local as well as foreign sources.

It is observed that more major Internet bankings in Malaysia were becoming targets to phishing activities with the phishing sites hosted on foreign servers. In addressing this, MyCERT managed to communicate with relevant parties to shutdown the phishing sites within a short period of time. In addition, a large number of local machines were compromised and were used to run phishing sites of well known overseas financial institutions.

Intrusion

In the Malaysian economic scenario, intrusion had made a security trend in 2005 with mainly web defacements of local websites from various sectors. In the first quarter of 2005 alone, we observed a significant surge in web defacements of local websites, with about 216 websites were defaced that resulted in an Alert was declared during this period. The MyCERT Operation Centre was opened for 24 hours to contain and handle the incident in order to prevent more Malaysian sites to be defaced.

For 2005, we received 467 reports on intrusion with about 80% representing web defacements of Malaysian websites. Majority of the defacements were due to websites running on poorly secured machines and without proper patches/upgrades.

Organized Seminars/Workshops

MyCERT has worked successfully on a series of seminars and workshops to raise awareness and educate interested groups on the importance of cyberspace security. Among its activities for 2005 were as follows:

1. International Conference on Cryptology (MyCrypt 2005 Conference)

Mycrypt 2005 Conference was Malaysia's first ever international conference on cryptology. The conference was held from 28-30 Sept 2005 at PWTC. There were 60 delegates from 17 countries attended this conference. Majority of the participants were from overseas such as from Switzerland, USA, Australia, Belgium, Norway, Japan, Taiwan, Germany, Singapore, France, South Korea, Indonesia, Sweden, Canada, Hong Kong and China. The conference was jointly organised by NISER, Swinburne University of Technology (Sarawak Campus) and University Putra Malaysia (UPM).

2. E-Secure Malaysia 2005 Conference

The four-day mega event was held from 28th September to 1st October 2005 at Putra World Trade Centre, Kuala Lumpur, and targeted at security experts, IT professionals, corporate players, policy makers, researchers and end users. E-Secure Malaysia 2005 was jointly organised by the Ministry of Science, Technology and Innovation (MOSTI), Malaysian Communications and Multimedia Commission (MCMC) and NISER. It is supported by Ministry of Energy, Water and Communications (MEWC) and Malaysian National Computer Confederation (MNCC). The conference was officially launched by Yang Berhormat Dato' Sri Dr Jamaludin bin Dato' Mohd Jarjis, Minister of Science, Technology and Innovation. About 180 delegates attended this conference. There were six (6) tracks with a total of 46 speakers with 19 foreign and 27 local speakers. A total of 15,000 attendees attended the e-Secure Malaysia Exhibition.

3. MyCERT Special Interest Group Knowledge Sharing Sessions

In 2005, MyCERT organized four (4) sessions of MyCERT quarterly knowledge sharing sessions, which received an overwhelming response from the constituency. More and more IT practitioners from various fields were attending the sessions in order to gain knowledge in information security.

Other Noteworthy Activities

1. Produced Alerts, Advisories and Other Publications

MyCERT had also produced security related documents, i.e. advisories, alerts, statistics, quarterly summaries and guides for the Internet communities in Malaysia. Those were available widely on local newspapers, MyCERT's websites and MyCERT's mailing lists. For year 2005, eight (8) alerts and four (4) quarterly summaries were produced. MyCERT's comments and views on current security issues were also published widely in local newspapers/magazines.

2. MyCERT Mailing Lists

In 2005, the MyCERT Discussion Forum became active with an overwhelming response from its members to actively participate in the forum, discussing current issues in the field of ICT security.

3. The Asia Pacific Computer Emergency Response Team (APCERT) Drill

MyCERT team had also participated in the APCERT Drill in December 2005.

I. Report from SingCERT

Singapore Computer Emergency Response Team – Singapore

About SingCERT

The Singapore Computer Emergency Response Team (SingCERT) is a one-stop centre for security incident response in Singapore. It 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.

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.

Incident Trends and Highlights for year 2005

For 2005, SingCERT received more than 100% increase in email-related attacks. This is mainly due to the increase in the number of Phishing attacks both targeting at local and overseas banks. SingCERT cooperated with other Asia Pacific CERTs namely CNCERT, KRCERT and PH-CERT to help bring down these bogus sites.

Besides Phishing attacks, probes and scans attempts continue to be a problem and contribute a significant percentage to the reported incidents. SingCERT continue to work closely with our Internet Service Providers (ISP) to track down the source of these probes and take appropriate action against the subscribers.

Major activities in year 2005

1. FIRST Conference 2005 in Singapore

The FIRST Conference 2005 was held in Singapore from 26th June to 1st July 2005. As the local host, SingCERT provided assistance to the 2005 Program Committee in obtaining approval from IDA to officially support the event and invited our Minister for Information, Communication and the Arts (MICA) of the Singapore Government to deliver the keynote address. SingCERT also assisted with the organisation of the Corporate Executive Program (CEP), a newly organised event along side with FIRST Conference, in recommending keynote speakers and providing contacts.

SingCERT acted as the point of contact for APCERT where the FIRST Conference 2005 is concerned and worked with APCERT members to help promote and market the event. Attendance for the conference was very positive (350+ attendees) and exceeded expectations.

2. ASEAN

In September 2005, the 5th ASEAN Telecommunications Meeting for Ministers (TELMIN) endorsed the Hanoi Agenda on Promoting Online Services and Applications to realise e-ASEAN. One of the action items on Network security calls for ASEAN "To strengthen cooperation in cybersecurity through activities such as conducting regional coordination drills to test out capabilities of National Computer Emergency Response Teams (CERTs) in ASEAN". As a result, SingCERT has been asked to organise an ASEAN CERTs Incident Drill (ACID). SingCERT has been liaising with various ASEAN CERTs and to date, a working group has been formed and details of the drill are being worked out.

3. APCERT Incident Drill

SingCERT participated in an incident drill organised by KRCERT for APCERT members. The drill was attended by various APCERT member teams and was successfully completed in Dec 05.

4. Sponsorship

For 2005, SingCERT acted as sponsor for two CERTs, Brunei Computer Emergency Response Team (BruCERT) and eCop Pte Ltd.

BruCERT is Brunei’s first trusted one-stop referral agency in dealing with computer-related and internet-related security incidents. With SingCERT’s assistance, BruCERT has successfully joined APCERT as a General Member.

SingCERT sponsored eCop Pte Ltd in their application for membership to the Forum of Incident Response and Security Teams (FIRST). eCop is a Singapore based private company providing Info-security surveillance, managed security and professional consultation services. They have been accepted as a member of FIRST effective April 2006.

J. Report from ThaiCERT

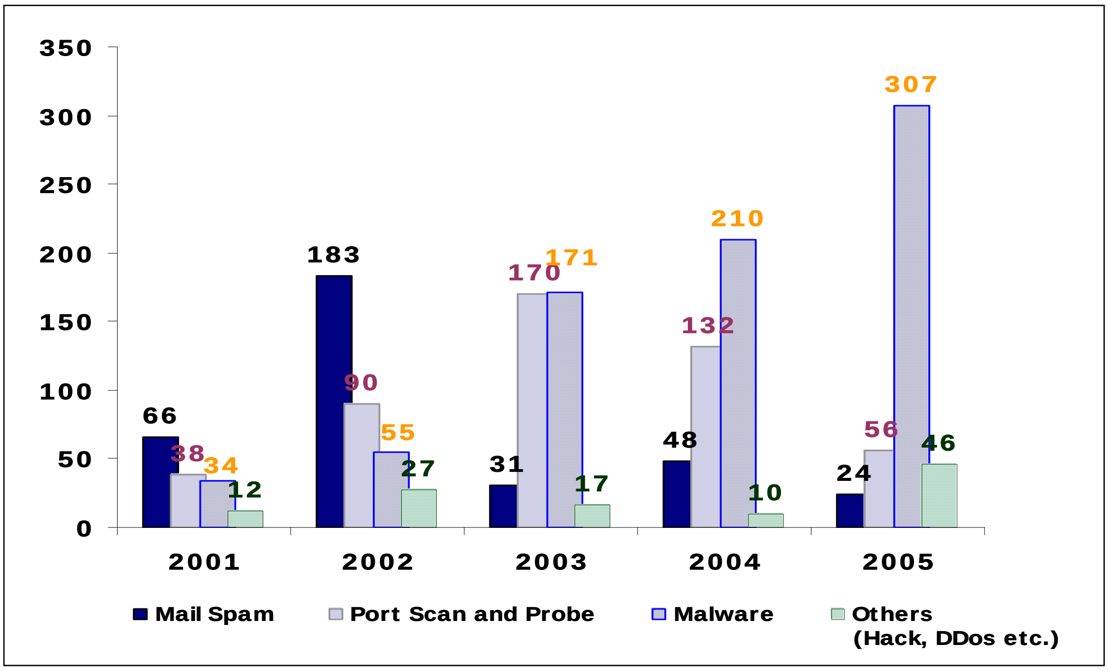
Thai Computer Emergency Response Team – Thai

Year 2005 Review and Comparative Incident Statistics

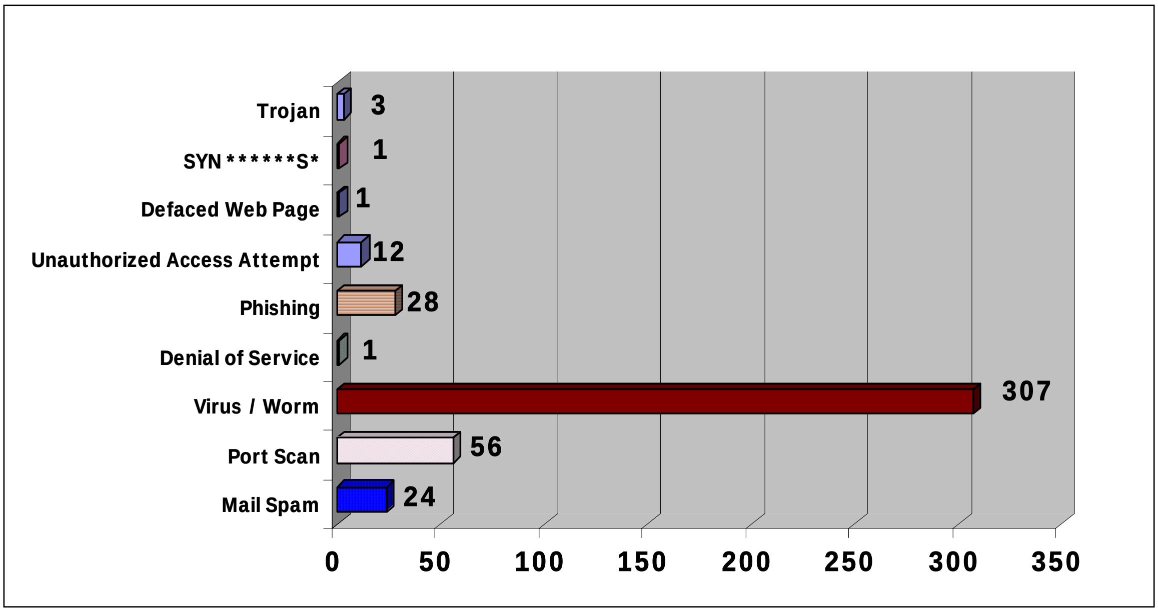
ThaiCERT has been receiving a number of security incidents since its formation and coordinates with the reporters to help them fix their problems. The table below shows incident statistics since the year 2001—year of ThaiCERT establishment. These incidents originated from government sectors and some of them came from private sectors who reported via our community of CERT teams. Actually, ThaiCERT only provides response service for governmental units, but since the occurrence of Phishing case in last two years we have to response to some private units for closing the caused sites to stop their compromised services. Respectively, the numbers of incidents become slightly going up.

Year	*2001*	*2002*	*2003*	*2004*	*2005*
Number of Incidents*	150	355	389	400	433

Remark * Incidents originated from government sector sites and some coordinating CERT teams.



This picture shows the numbers of incidents, which also were reported to ThaiCERT since year 2001 to 2005. From the picture, it can be concluded that malware spreading is still rising slightly when compares with its amount in the recent years. In contrast, the number of mail spam is decreasing when considers in the same intervals. For the surprising number is “others” case. It increases around 4.5 times from last year. This may cause by a new type of incident has been added, which is Phishing incident. Then see the next picture, it indicates "others" in detail.



This picture also appears that worm and virus spreading is a number one of incident reported because they damage IT resources, cost, business benefit, and so on. When looking into the top-four, we can list as follow: 1) Port Scan; 2) Phishing; 3) Mail Spam; 4) Unauthorized access attempt.

Notable Virus and Worm Incident Response

The first-three is likely to be Sober, Mydoom, and Bagle, which are slightly hard to eliminate and they distribute themselves via large numbers of e-mail. Moreover, they have many types of variant; therefore, many users don't know how to clean each one correctly and timely.

Besides, worm "Bropia" is a new one that spreads via MSN network. After, we had heard the news of its spreading, then we propagated how to protect it in soon and the users could be aware by patching this vulnerability in time.

For other incident about virus, it appears that there is a news about mobile virus, which named "SymbOS.Doomboot". For this type we also provided content how to protect it on our web site including more information for the user knowledge.

ThaiCERT activities

1. Overview for IT security enhancement and APCERT seminar

Last year, we have been working for Security Steering Committee, which is under Electronic Transactions Commission, to raise security awareness issue to all of Thai users. Especially, security standards, such as ISO 17799-2005, 27001, which we had arranged into Thai version and had provided a way to step up some organizations by means of Security Maturity Model as we had presented at Kyoto, 2005 APSIRC conference.

2. Joining with Regional Asia Pacific Information Security Standards Forum (RAISS)

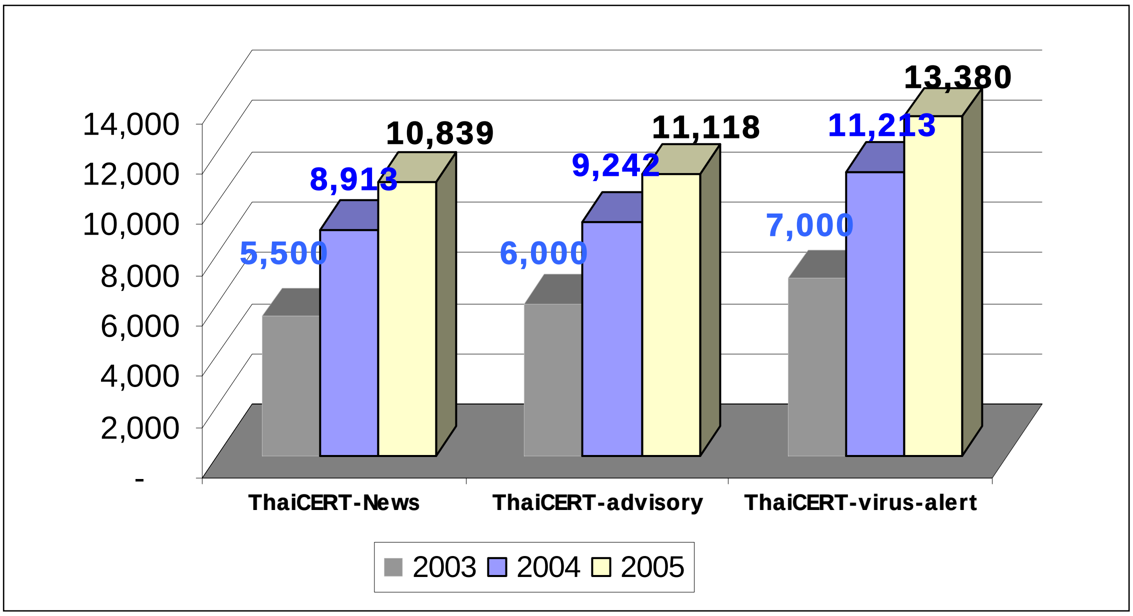
Since year 2004, ThaiCERT has organized a unit for studying and developing security standards in Thailand, and then we have to join the conference regarding the well known security standard as a group of user-- ISMS standards. This forum can help us to exchange and improve the knowledge about them greatly. Furthermore, this forum is for security standards contribution such as proposing some papers, hence, proposed a paper in title “Modified Risk Assessment by using a New Logical Way of Thinking”.

3. Taking part of panel discussion in “Thai ICT Expo Alliances 2005”

For this panel, ThaiCERT as partner of government sector so we joined to provide content about IT security standards and opened a panel discussion for receiving any comments to the security standard that we had arranged. When those comments or any suggestions are concluded, we will take them to the consideration of the Security Steering Committee to approve for new solution or any further recommendations.

4. ThaiCERT mailing list service

This kind of service is provided for free of charge. When some virus/worm spreading at high risk level, we have to pre-alert for making awareness for them and even some vulnerabilities found and they are vital to large amount of users, then we have to announce these content via the mailing list. The picture below is shown numbers and types of services we provided as named ThaiCERT-news, ThaiCERT-advisory, ThaiCERT-virus-alert, respectively. Most of them are increasing slightly compared with each other in each year.



5. Providing the secure wireless network for APECTEL 31 meeting held in Thailand

At that time, this project looks like ad-hoc job or unplanned situation, but with the strength of wireless teamwork, we can provide many solutions for the attendant to use wireless network connected to Internet without any inconsistent events like worm/virus spreading or any interruptions.

6. ThaiCERT is a member of FIRST

In last year, ThaiCERT applied for Forum of Incident Response and Security Teams or FIRST, which is a well known security incident forum in global. We had been fully supported by JPCERT/CC and KrCERT/CC to promote us to be a member of FIRST, and finally it was done. ThaiCERT staff is appreciated and thank to JPCERT/CC and KrCERT/CC for pretty much afford to contribute to ThaiCERT.

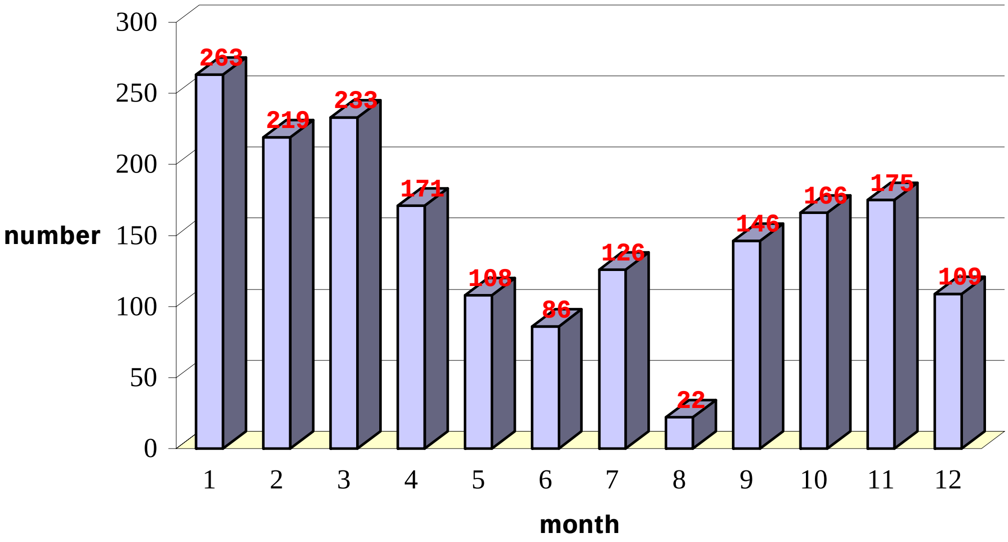
K. Report from TWCERT/CC

Taiwan Computer Emergency Response Team/Coordination Center – Chinese Taipei

- **Incidents response handling**

One of TWCERT/CC major responsibities is to assist in handling computer security incidents and to coordinate with other CSIRTs. We have processed 1824 incidents during the year of 2005 as shown below.

2005 IR monthly occurances



- **Security education training**

TWCERT/CC conducted a variety of security courses for government agencies, industries, and interested individuals. The list of courses is as follows.

✶ Security training for DNS administrators
✶ Short-term and long-term on-line customized information security education
✶ TWCERT/CC information and network security certification courses
✶ Customized government agency security education

- **Security Conference participation**

Participating security conferences could exchange security information and incident handling experiences with other CSIRTs and provides the accessibility to the international security technology. TWCERT/CC took a part on the following conferences.

✶ APSIRC 2005 (Feb 22-24, Kyoto International Conference Hall, Kyoto, Japan)
✶ AusCERT Asia Pacific Information Technology Security Conference 2005（May 22-26, Royal Pines Resort, Gold Coast, Australia）
✶ FIRST 2005 17th Annual Computer Security Incident Handling Conference (June 26-July 1, Shangri-La Hotel, Singapore)

- **SPAM Cooperation**

  TWCERT/CC Joined the Seoul-Melbourne Multilateral Memorandum of Understanding (MoU) on Cooperation in Countering Spam in December 2004 to collaborate with other countries on Spam problems.

- **Localized Vulnerability Database**

  TWCERT/CC maintains a localized vulnerability database and provides localized security advisories and newsletters to raise the awareness of information security in our country. TWCERT/CC also provides a localized and customized security auditing system to help our constituency improve the network security infrastructure.

URL: http://www.cert.org.tw/eng/index.htm
Email: twcert@cert.org.tw
Phone: +886 7 5250211; +886 2 2356 3303
Fax: +886 7 5250212; +886 2 2392 4082

L. Report from TWNCERT

Taiwan National Computer Emergency Response Team – Chinese Taipei

Introduction

TWNCERT continues to provide information security services, promote IT security awareness, engage research and development, gather computer incident and vulnerability information, provide incident responses and IT security seminars and forums, and the interactions of international information security related organizations.

TWNECRT is a non-profit organization intended for improving incident response activities 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 incident. TWNECRT is therefore to enhance the ability to respond and deal with security incidents and internationalize our efforts.

2005 Highlights

1. **Promote Security Awareness and Provide Training Course**

   TWNCERT offers IT security conferences, workshops, training courses, and exhibitions to network administrators, system administrators and technical staff, .etc. The organized events in 2005 are listed below:

   (1) Trainings
   - ✓ ISMS Lead Auditor Training Course for 250 participants.
   - ✓ CEH (Certified Ethical Hacker) Training Course for 20 participants.
   - ✓ CISSP (certified information systems security professionals) Training Course for 20 participants.

- ✓ ITE (Information Technology Expert) for Information Security Training Course for 179 participants. (*ITE is a local certification for specialized test in Taiwan)
- ✓ Provide a total of 30 hours and 22 different e-Learning training courses.

(2) Exhibitions

- ✓ 2005 iSecuTech Expo: Taipei International Information Technology Exhibition in Taipei.
- ✓ 2005 Taipei Computer Spring Exhibition.

2. International Cooperation

TWNCERT is always glad to join in the international security organizations and share information with security communities. In 2005, TWNCERT joined in the following security communities and attended many important conferences:

(1) APCERT

- ✓ Attend APCERT 2005 annual conference in Kyoto, Japan.

(2) FIRST

- ✓ Attend FIRST 2005 annual conference in Singapore.

(3) APEC-TEL

- ✓ Attend APEC-TEL 31 meeting in Bangkok, Thailand.
- ✓ Attend APEC-TEL 32 meeting in Seoul, Korea.

(4) DEFCON

- ✓ Attend DEFCON conference in Las Vegas, USA.

(5) AVAR（Association of anti Virus Asia Researchers）

- ✓ Attend AVAR2005 Conference in Tianjin, China.

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 2005, TWNCERT handle 28 incidents reporting from international security communities, including:

(1) 22 phishing web site incidents. TWNCERT coordinated law enforcement agencies to remove the phishing pages or shutdown the phishing hosts.

(2) 6 suspicious attacking incidents. TWNCERT informed the victims directly or indirectly and helped them recovery and harden their systems.

3. Presentations and Publications

TWNCERT is continuing to do research on security areas and publish the research results in the international security conferences in order to share our experiences with communities. The followings are the presentations and papers published in 2005.

(1) TWNCERT 2004 report, APCERT 2005.

(2) SIDEx: Security Incident Data Exchange, APEC-TEL 31.

(3) A Distributed Intrusion Alert System, FIRST 2005 annual conference.

(4) How Will Cracking Evolve? The Discovery of MS05-036 Vulnerability, APEC-TEL 32.

4. Incident Response and Prevention

TWNCERT publishes advisories and alerts to prevent and response to the incidents. In 2005, TWNCERT published total 191 advisories and alerts, including:

(1) 58 alerts for intrusion incidents.
(2) 43 advisories for system vulnerabilities or weakness.
(3) 90 alerts for web site defacement incidents.

5. **BS 7799-2:2002 Information security management systems routine assessment visit**
In order to provide a highly standard of service, TWNCERT has been verified with BS 7799-2:2002 by BSI as routine assessment visit in July and December 2005.

For the international cooperation, TWNCERT will continue to share information with global security communities in 2006.

URL: http://www.twncert.org.tw/en/main.php
Email: twncert@twncert.org.tw
Phone: +886 2738 3300
Fax: +886 2 2378 1309

M. Report from BruCERT

Brunei Computer Emergency Response Team– Negara Brunei Darussalam

Introduction

The Brunei Computer Emergency Response Team (BruCERT) is the national coordinating centre for IT security incident reporting in Negara Brunei Darussalam. It was setup in collaboration with Authority for Info-communications Technology Industry (AiTi) to facilitate the coordination of all security related incident and response in the country. BruCERT was initially established in May 2004 and officially in January 2005 as an initiative by AiTi to support the creation of a national coordinating body for reporting and repository of all security related events for the benefit of the country. This move also complies to the formation of CERT coordinating body as a requirement for all countries in the region in response to ASEAN Telsom WG meeting in Jakarta, Indonesia in April 2004.

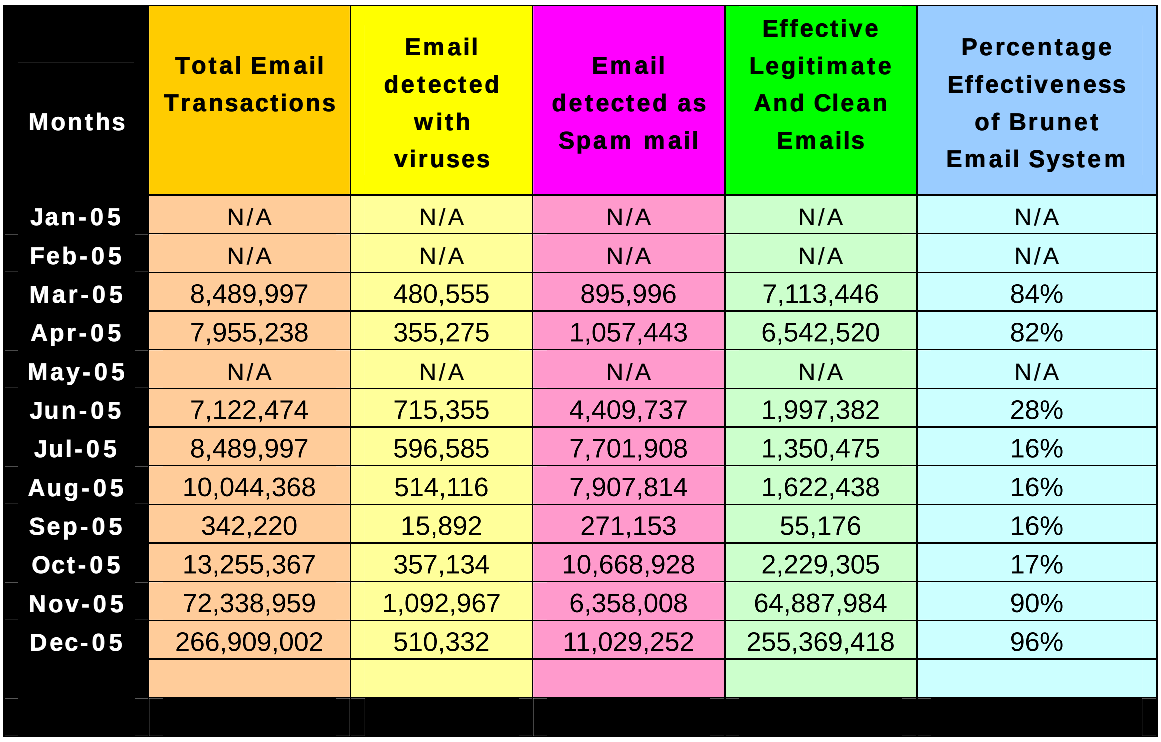
BruCERT Activities 2005

Incidents and Trends

BruCERT is currently communicating with relevant authorities in gathering statistical information to measure the level of security awareness in the public and security related incidences in the country. One such move is to approach the two main internet service providers in the country, Brunet and SimpurNet. Discussions are carried out to collaborate and facilitate each other in providing and sharing expertise, technology and methodology for providing statistical information from the two ISPs.

Recent statistical information obtained from Brunet saw the trends in the distribution of spam and viruses through the ISP hosted email system. Being the first ISP in the country, the email system hold various email accounts spanning from the public and the private sector. However the email transaction requires further security improvement to be effective.

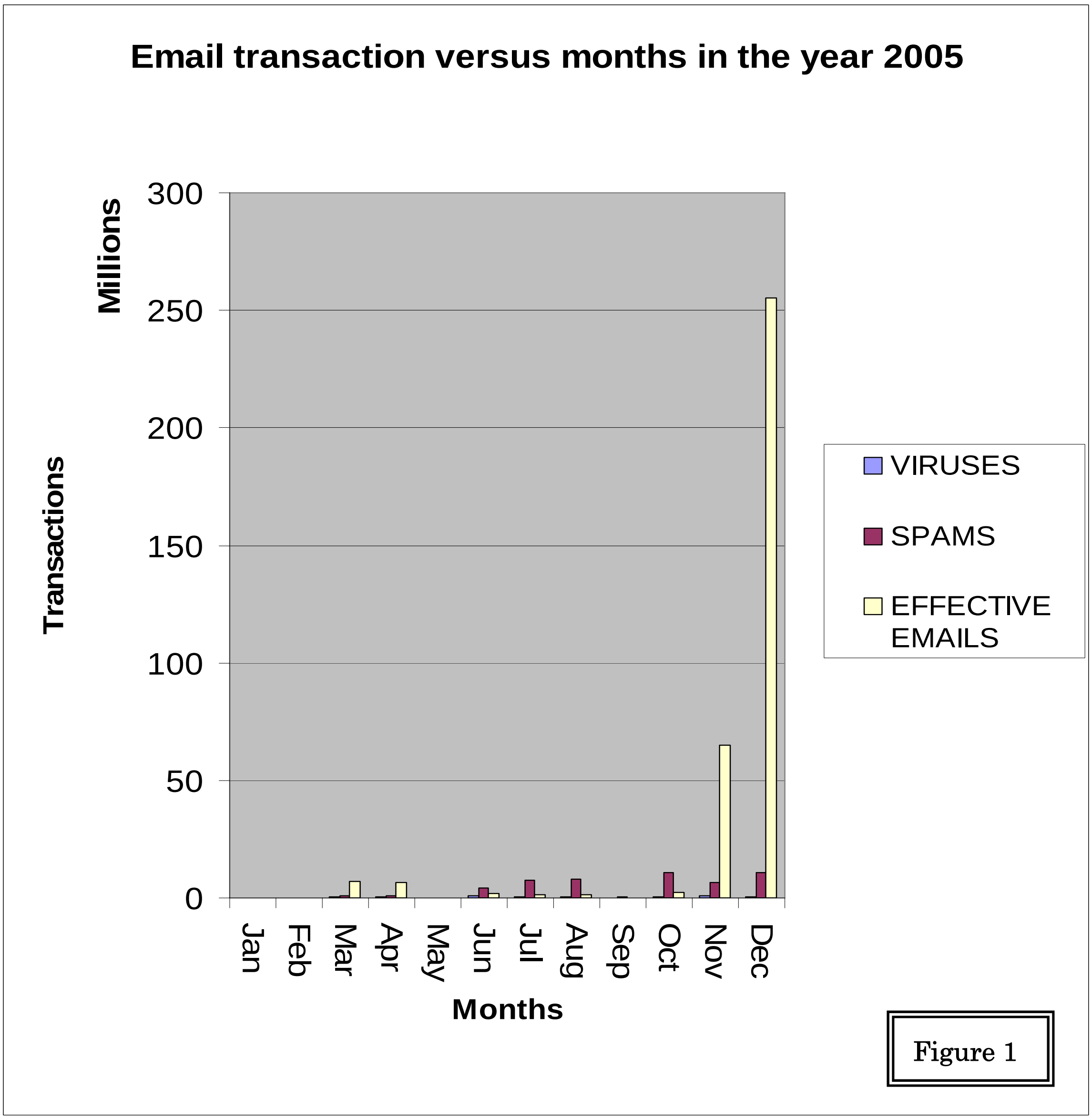
Two main threats had been identified in the email system - viruses and spam. The table below was extracted from the statistics acquired from Brunet. Statistical information in January, February and May 2005 were not available due to the internal logging problems.



Months	Total Email Transactions	Email detected with viruses	Email detected as Spam mail	Effective Legitimate And Clean Emails	Percentage Effectiveness of Brunet Email System
Jan-05	N/A	N/A	N/A	N/A	N/A
Feb-05	N/A	N/A	N/A	N/A	N/A
Mar-05	8,489,997	480,555	895,996	7,113,446	84%
Apr-05	7,955,238	355,275	1,057,443	6,542,520	82%
May-05	N/A	N/A	N/A	N/A	N/A
Jun-05	7,122,474	715,355	4,409,737	1,997,382	28%
Jul-05	8,489,997	596,585	7,701,908	1,350,475	16%
Aug-05	10,044,368	514,116	7,907,814	1,622,438	16%
Sep-05	342,220	15,892	271,153	55,176	16%
Oct-05	13,255,367	357,134	10,668,928	2,229,305	17%
Nov-05	72,338,959	1,092,967	6,358,008	64,887,984	90%
Dec-05	266,909,002	510,332	11,029,252	255,369,418	96%

Courtesy of Brunet Internet Service Provider, Telecom Department, Ministry of Communications.

As shown in Figure 1, spam is more popular than viruses. This might be because of Brunet had implemented an additional new hardware to assist in detecting viruses and furthermore that the advantage of free advertisement through email seems to be at ease. The significant increasing in emails usage in November and December might be due to festive seasons and school holiday. This reason also applies to the high percentage of email utilization for the both of the same months shown in Figure 2. While during March and April, the high percentage email utilization could possibly due to no new big impact viruses ever exist during that period.


Email transaction versus months in the year 2005
Transactions
Millions
300
250
200
150
100
50
0
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
Months
VIRUSES
SPAMS
EFFECTIVE EMAILS
Figure 1

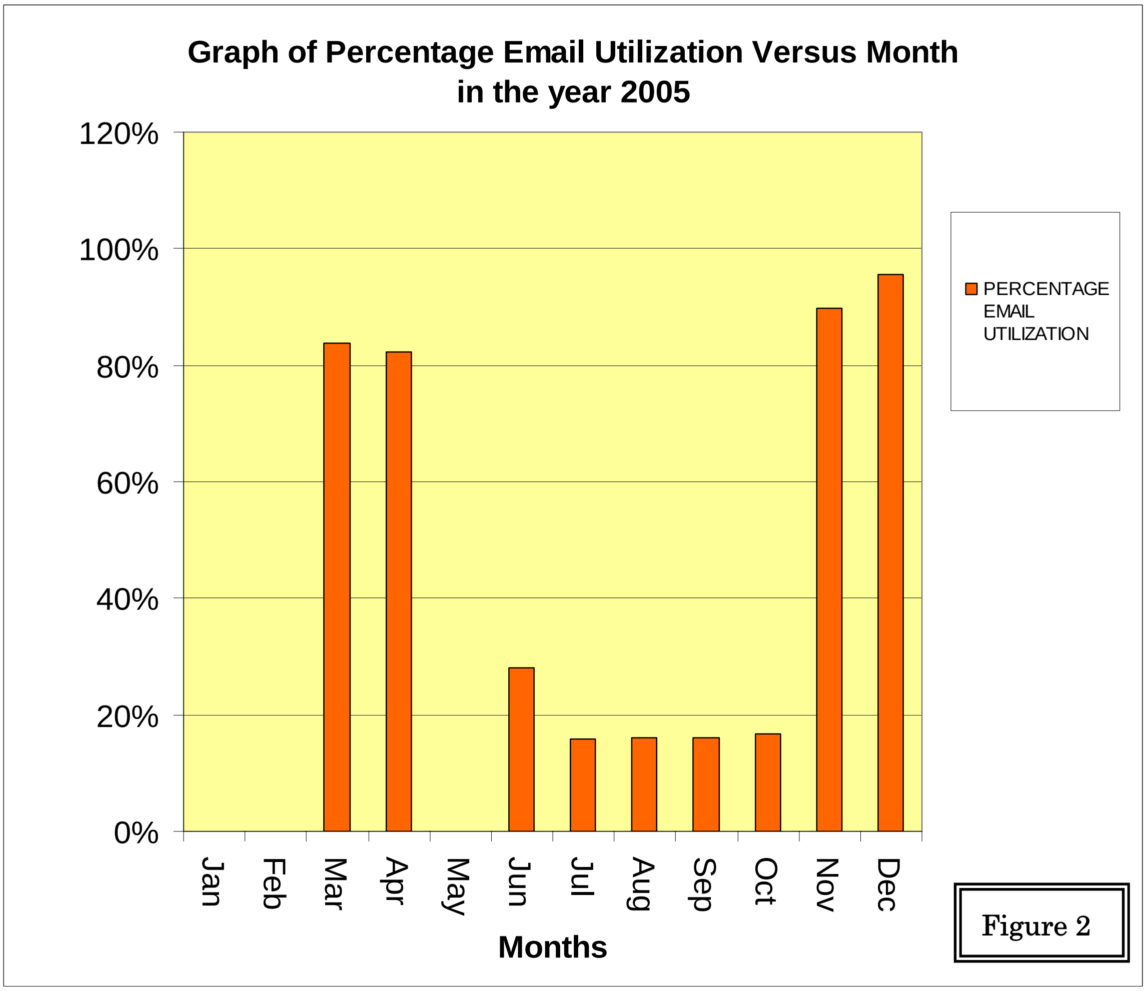


Figure 2

Incidents Handling

In 2005, BruCERT has received 2 incident reports which related to worms.

In March 2005, IT officials from one of the leading bank in Brunei observed anomalies to some of the computers in their headquarters. Some administrative operation failed to response on these computers and aroused suspicions that these computers could have been compromised. The incident was reported to BruCERT and the Incident Response Team (IRT) was deployed prior an emergency request by the bank's management to investigate the cause of the anomalies. The outcome of the investigation discover a new virus called WORM_SDBOT.AYI which was believed to be propogated from an internet PC running IRC program by replication agent called "VolumeControl.exe". Through our research and development team (RND), further investigation and liaison with one of the leading antivirus vendor, Trend Micro revealed that the variant was a new discovery and further containment and eradication procedures were carried out. The existence of the worm variant had caused major service disruption to the bank.

In mid October 2005, BruCERT received its 2nd incident report involving the Slammer worm. Further investigation also revealed that the infected computers virus definitions were not updated. Lack of security policy and awareness were the main reasons for the incident.

BruCERT Website

In our website, security related issues and white papers are published and updated to build a more alert and knowledgeable public. Website contents include periodic advisories, vulnerabilities, security news and guidelines.

Elected as APCERT General Member

In February 2005, BruCERT was officially elected as a general member of APCERT. Prior to the election, representative from SingCERT were invited to ITPSS premises as part of the membership registration procedure to APCERT. BruCERT would like to convey its compliments and appreciation to SingCERT for being the Mentor in the registration and evaluation process.

Attended Seminars/Conferences/Meetings

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

- In 22-26 March 2005, 2 representatives from BruCERT attended the CNCERT/CC Conference 2005 Guilin, China. The workshop was conducted by Mark McPherson (AusCERT), Don Stikvoort (FIRST), David Crochemore (FIRST) and Arnold (KrCERT).

- In June 26 – July 1st 2005, three representatives from BruCERT attended the 17th Annual FIRST Conference held in Singapore. In this Conference, BruCERT’s representative presented a brief overview of BruCERT and the current activities and events related to its roles as the national computer emergency response team.

- On October 2005, BruCERT provides IT Security related presentation during the Brunei Info-Communication Technology Awards (BICTA) and conferences The conference saw the participation of various government and private organizations and is an annual event hosted by the Ministry of Communication.

Attended National Conference

BruCERT participated in the “National Summit on Information Society (NASIS)” conference held at the national convention center in the capital. The international summit had invited international and local speakers to discuss on various aspects of information technology, e-application, human resource development, digital divide, ethics of information society, environment and enabling policies and security.

Training and Seminars

IT Security Awareness, a one-day and a two-days seminar for End Users, IT personnel and Executive Management were held at the public service institute, a centralized institution for conducting training program for the government civil servants. More than 140 government officers attended the seminars which were held in June, August and November 2005.

Exhibitions Participation

BruCERT participated in two local exhibitions:

- The e-application expo in conjunction with the NASIS summit at the national convention center.

- and the government “Public Service Day”

In both exhibitions, BruCERT presented various services offerings which includes authentication and authorization technologies, incident response and awareness seminars.

Educational visits to BruCERT

IT faculty students from two local technical institutions and one local business college visit to our premise. The visits provide BruCERT an opportunity to educate and provide IT security awareness to the students including brief history of the establishment and the structure of the incident response team.

Future Plans

Ongoing security awareness training to government

Maintain and extend the security awareness seminars for the government civil servants through the public service institute. Future plan shall include the introduction of new coursewares related to IT security and customized trainings.

Security Event Statistics

Conduct more activities in collecting statistical information related to security events and awareness to the public in general and the internet subscribers in the country. BruCERT initiated the discussion with the local internet service provider for gathering security related statistical events. BruCERT introduces the Managed Security Services (MSS) to the service provider to facilitate and assist them to realize the objectives.

SMS Services

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

BruCERT Road shows

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

Free Seminars to the local public

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

Conferences

Organize several conferences for APCERT members among the ASEAN countries. Members can share information, ideas, best practices guidelines and policies on various IT security related postures.

Applying for FIRST membership

BruCERT intend to apply for FIRST membership to share information and experiences among FIRST members. BruCERT plans to upgrade its member status to full member in APCERT and work on with other terms and conditions to qualify for the FIRST membership.

Publications

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

N. Report from GCSIRT

Government Computer Security and Incident Response Team– Philippine

Outline of Annual Accomplishment Report

1. Formulation of National Cyber Security Plan (NCSP)

The plan was approved by President Gloria Macapagal Arroyo last February 21, 2005. The NCSP will serve as a guide to protect the nation's digital infrastructure and the Philippine cyberspace as a whole. It is a working plan that seeks to generate a coordinative, cooperative and collaborative effort between the public and private sectors to protect our cyber or digital infrastructure. It is also envisions harmonizing and systemizing national cyber security policies and programs.

2. Participated in Asia Pacific Economic Cooperation (APEC) Telecommunications and Information Working Group 3RD CYBERCRIME LEGISLATION AND ENFORCEMENT CAPACITY BUILDING CONFERENCE OF EXPERTS AND TRAINING SEMINAR held at Seoul, Korea on 22-24 June 2005.

3. Participated in 2005 Asia Pacific Information Security Center (APISC) Security Training Course

held at COEX Conference Room, Seoul, South Korea on August 29- September 2, 2005.

4. Participated in 2005 Asian Regional Forum on Cyber Terrorism held at Waterfront Hotel, Cebu City, Philippines on October 3-5, 2005.

5. Conducted training on Incident Response Course in Cebu City (Visayas area) on October 17-21, 2005.

6. Conducted training on Incident Response Course in Davao City (Mindanao Area) on October 24-28, 2005.

7. Participated in various congressional hearings as resource person on topics of cybercrimes, e-commerce, consumer protection, internet frauds and others.