Asia Pacific Computer Emergency Response Team

APCERT 2004 Annual Report

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

Chair's Message

As Chair of APCERT, it is my pleasure again to provide a report to the members of APCERT about our progress during 2004. In little over 2 years, APCERT has grown to now represent 17 teams across 13 economies in the Asia Pacific region, with further teams and economies indicating their interest in joining APCERT. Beyond the Asia Pacific region, other CERT and CSIRT groups are looking to APCERT as working model for international CERT cooperation and collaboration.

At the recent annual general meeting of APCERT held in Kyoto in February 2005, the high level of good will and common focus that existed among APCERT members was readily apparent. These relationships are essential to forming strong community based around genuine information sharing, building trust and cooperative arrangements that mutually support the Internet security of our respective economies.

During 2004, we began developing APCERT policies and procedures for sharing information about serious and time critical computer network threats and vulnerabilities. This work is now near complete. We have worked collaboratively in putting our views and experiences about Internet security threats and vulnerabilities to APEC-TEL, and are working collaboratively on network monitoring capabilities across economies.

As we move into the latter half of 2005, I look forward to working together to ensure that APCERT delivers benefits to its teams through building strong cooperative arrangements to help protect against cyber threats and vulnerabilities in our region.

As Chair, I could not be more pleased at how far APCERT has come in such a short period of time and I believe this is encouraging for the future. However, none of this could be achieved without the good will, commitment and contribution of each and every APCERT team and the constituencies they represent.

In closing I would like to 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) and the Korea Computer Emergency Response Team Coordination Center (KrCERT/CC)provides a secretariat function.

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. 2004 APCERT Activity Report

The following is a list of the achievement by the APCERT members in 2004.

A. Representation to other Regional and International Bodies

1. 16th Annual FIRST Conference on Computer Security Incident Handling, 13-18 June 2004, Budapest, Hungary

KrCERT/CC and JPCERT/CC presented on Network Monitoring and web portal site Project in AP region, with the objective to draw the needs of coordination and information sharing not only for incident handling, but also to prevent incidents and to share the activities of AP region with FIRST members.
http://www.first.org/conference/2004/abstracts_conf.html#c04

2. APEC-TEL 30, 18 September 2004, Singapore

Updated security trends in the AP region.

B. APSIRC 2005 (APCERT AGM)

APSIRC 2005, 22-24 February 2005, Kyoto, Japan
http://www.apcert.org/apsirc2005/

APCERT organizes an Annual General Meeting called APSIRC *(Asia Pacific Security Incident Response Coordination Conference)* for CERTs/CSIRTs and other computer security professionals dealing with security incidents. APSIRC 2005 was hosted by JPCERT/CC and sponsored by Microsoft, held in conjunction with APRICOT (Asia Pacific Regional Internet Conference on Operational Technologies).

APRICOT (Asia Pacific Regional Internet Conference on Operational Technologies)
http://www.apricot.net/

C. Membership

The APCERT Accreditation Working Group has formed APCERT's membership accreditation rules, approved by the SC, which now enables APCERT to welcome new member teams. In 2004, APCERT welcomed BruCERT (Negara Brunei Darussalam) and GCISRT (Philippines).

D. Steering Committee (SC) Meetings

1. SC Conference Call

The SC had one telephone conference in 2004.
Date: Thursday, 2 December 2004
Time: 12:00 (GMT+09:00) -

Discussion Points

1. New applicants' application evaluation
2. APCERT POC
3. Schedule for APSIRC 2005 – 22-24 February 2005, Kyoto, Japan
4. Briefing on European Government CERTs (EGC) Meeting
5. APCERT involvement in APEC-Tel Meeting
6. APCERT SC and Chair election at APSIRC 2005
7. Future APSIRC venues

E. Administrative Matters

1. Mailing Lists

APCERT members communicate through several mailing lists developed by AusCERT:

Apcert-teams@apcert.org
accreditation-wg@apcert.org
comm-training-wg@apcert.org
apcert-sc@apcert.org

2. Website

APCERT website was designed by KrCERT/CC and maintained by JPCERT/CC.

http://www.apcer.org

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, we are the single point of contact for the provision of advice about computer network threats and vulnerabilities in Australia. Through our range of CERT contacts we also provide an incident response capability for Australian networks for attacks emanating from overseas and within Australia.

AusCERT services a range of subscribers throughout Australia, New Zealand and the Asia-Pacific region through the provision of computer security and incident handling advice. In particular, 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). We also operate a National IT Security Incident Reporting Scheme and National Alerts Service, with funding from the Australian government.

CSIRT training
During 2004, with funding from AusAID and ASEAN we provided CSIRT development training to representatives from Vietnam, Cambodia, Myanmar, Brunei, Laos, Indonesia, The Philippines and Thailand in cooperation with SingCERT, and MyCERT.

Online ID theft
During 2004 AusCERT substantially increased efforts in monitoring, analysing and response to incidents of online ID theft, primarily in response to increasing level of threat, both in terms of the volume and sophistication of incidents seen in Australia and elsewhere. Our work in this area has resulted in closer cooperation, including at an operational level, between other APCERT teams and organisations from the banking and finance sectors in Australia and elsewhere.

In this capacity we have worked closely with the Australian High Tech Crime Centre to provide a combined CERT and law enforcement strategy for responding to incidents of this nature affecting Australian institutions. Our efforts in this area has enabled stakeholders in industry and government in Australia and many other economies to gain a better understanding of the threat associated with online ID theft; the techniques being used to conduct online ID theft and the implications of this activity for e-commerce and other sectors that allow remote access to their information systems.

APCERT Capabilities
Since the formation of APCERT in February 2003, the relationship and level of cooperation between APCERT members has continued to grow in productive and tangible ways. During 2004, AusCERT continued to support APCERT in its capacity as Chair and a member of the steering committee.

We have helped to develop APCERT Point of Contact (POC) Arrangements and other procedures to

allow the APCERT community to progress mutual CERT interests in a cohesive and productive way.

Our work in training new and emerging CSIRTs in the Asia-Pacific regional has also contributed to our investment in the Asia-Pacific region CERT capacity-building.

The International Systems Security Professional Certification Scheme (ISSPCS)

AusCERT, in partnership with partner EWA Australia and Queensland University continued to progress the development of a computer security certification program and accompanying ISSPCS relevant training.

ISSPCS is a global and open certification scheme for information and systems security professionals that addresses 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: http://www.isspcs.org/

Public Key Infrastructure (PKI)

AusCERT is helping 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.

AusCERT Distributed Network Monitoring and Analysis System

A major priority for AusCERT in 2004 has been the development of a network monitoring and analysis system to provide detection and early warning of network attacks, based primarily on router netflow data. While functionality continues to be added to the prototype, the system has already shown useful potential for network anomaly analysis and detection. AusCERT will continue to invest in this capability throughout the coming year.

2004 Australian Computer Crime and Security Survey

In May 2004, AusCERT published the 2004 Australian Computer Crime and Security Survey in partnership with the Australian High Tech Crime Centre (AHTCC) and every police law enforcement agency in Australia. Its production was sponsored by the AFP, 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

AusCERT2004: Asia-Pacific IT Security Conference

AusCERT held its annual Asia-Pacific IT Security Conference at the Gold Coast in May 2004 at which around 700 delegates attended. The conference has shown itself to be the premier IT security conference in the Asia-Pacific region, conducted by IT security professionals for IT security professionals, IT managers and government decision makers in the field. The conference programs offers delegates presentations in business, technical streams and includes refereed papers from the academic community with support from QUT's Internet Security Research Centre (ISRC).

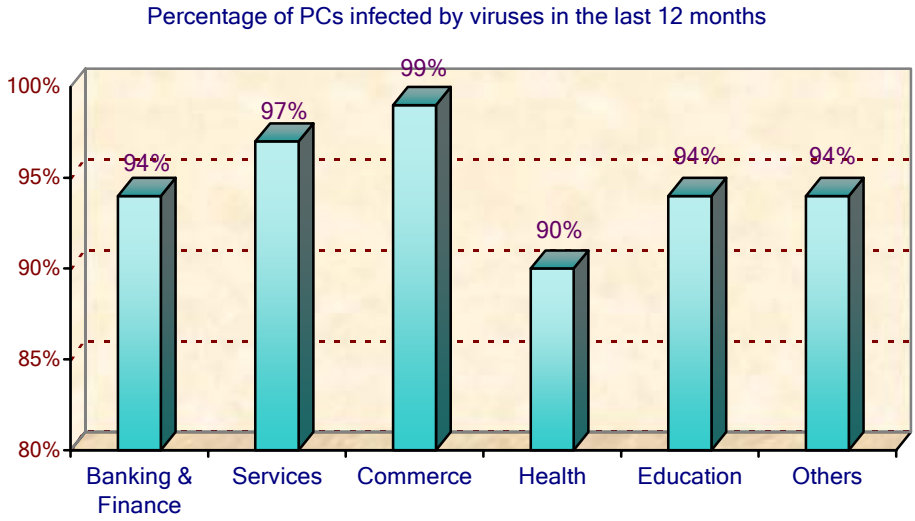
The conference increasingly has become a focal point for progressing discussions among like groups, such as CERTs, government and industry on a range of initiatives. See: http://conference.auscert.org.au/conf2004/

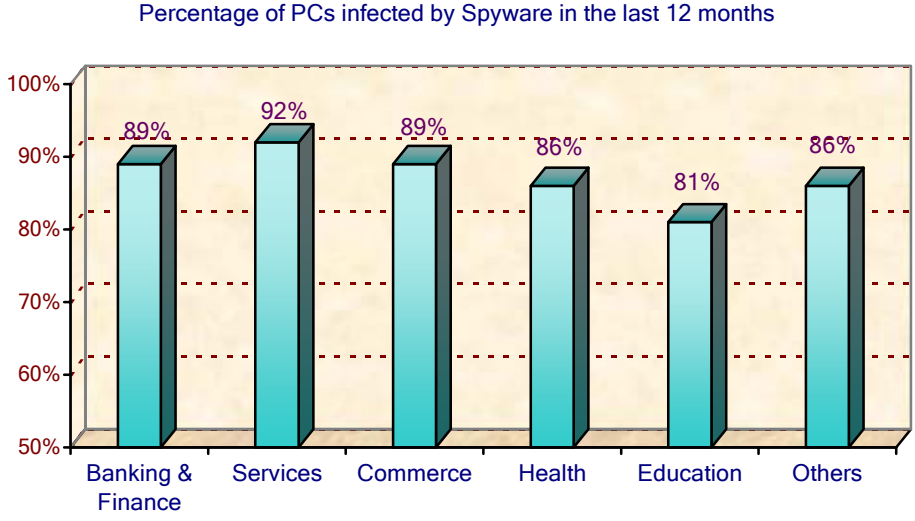
B. Report from BKIS

Bach Khoa Internetwork Security Center – Vietnam

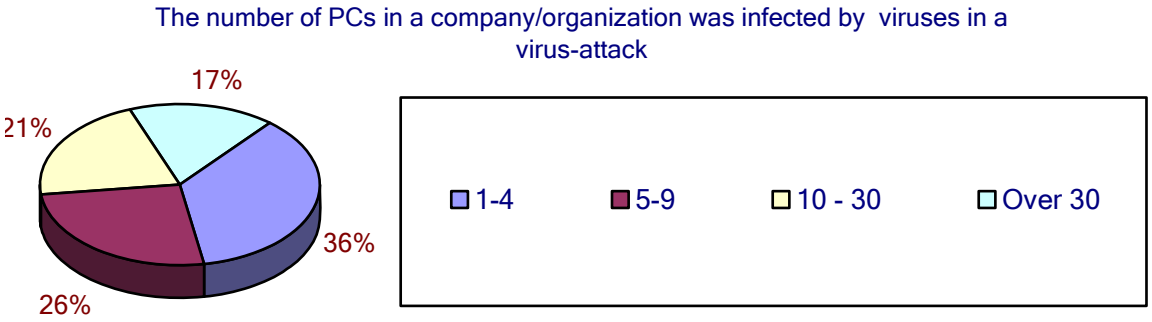
Activity report of 2004

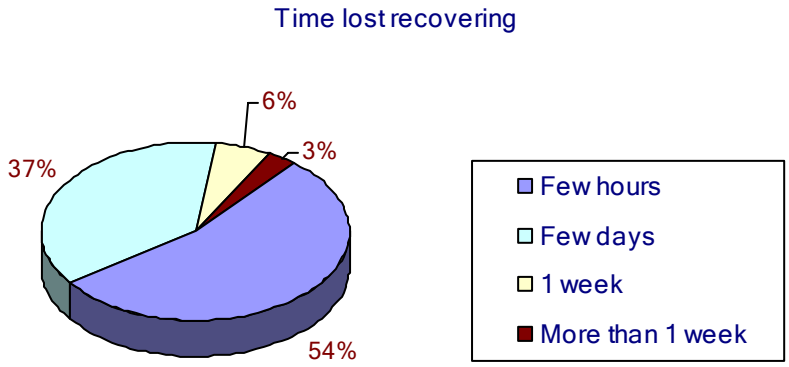
We performed the first national security survey in Vietnam at our website www.bkav.com.vn in December 2004. According to this survey, there was more than 95 percent of PCs infected by viruses or spyware in Vietnam and the damages go up to 390 thousand VND for each PC per year.

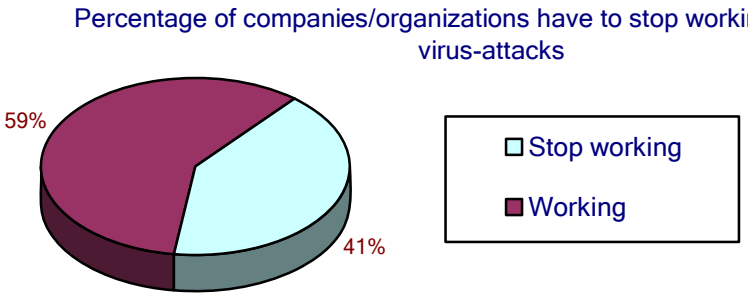




In our survey, we also asked our customers about damages of virus-attack. Following is the result:







In 2004, there were 84 new viruses appeared in Vietnam in comparison with 62 new viruses in 2003. Variants of Blaster & Sasser caused the most demages. As soon as new viruses appeared in Vietnam we updated our Antivirus software - BKAV to kill those viruses and sent the warning messages to all members in my mailing list and to public media.

In 2004, we updated our software once a week. We updated most of dangerous viruses in the world, such as: Erkez (alias Zafi), Beagle, SkyNet (alias Netsky), Spybot, Sober, MyDoom, etc.

We replied thousands of emails and telephone calls from victims of viruses and hackers. The number

of attacks and illegal access to websites in the last 12 months increased a little. There are approximate 1.5 million free downloads of our Antivirus software at website: http://www.bkav.com.vn

We took part in some conferences about Network Security, e-commerce, e-government... and in those conferences, the security problems we introduced got much attention from others.

We also took part in the computer networks design and setup phases for the Parliament Office in December, 2004. We also gave consultations and provide system maintenance services for governmental organizations such as Parliament Office, Ministry of Home Affair, etc.

We resolved incidents in some companies and organizations including governmental organizations.

We also supplied some training courses about Antivirus and Security for students, who were interested in this field. There were many students taking part in our courses and most of them still continue studying and working with us. In the future we will supply some courses for officers to introduce and provide them the basic knowledge about security.

Year 2004 is really busy but we were very happy with the result of our work in security field.

C. Report from CCERT

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

Incident Response

In 2004, CCERT has received 53,156 incidents reports, nearly twice of those of 2003. Taxonomy statistics of incidents reports are shown in figure 1. More than 71% of these incidents were related to spam, most of spam were send by virus and worm. Worm incidents are not counted separately but as virus or spam.

Figure 1. Taxonomy statistics

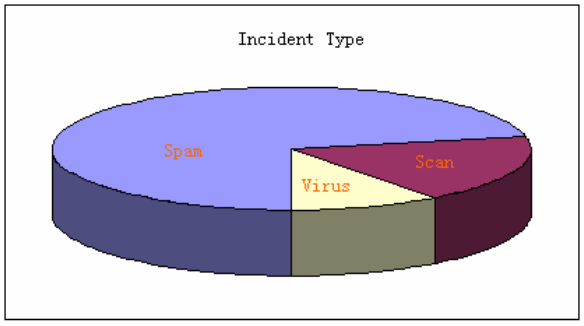


Table 1. Taxonomy statistics

Order	Taxonomy	Percent
1	Spam	71.79%
2	Scan	18.03%
3	Virus	10.07%
4	Ask for Help	0.05%
5	Intrusion	0.01%
6	Unknown	0.05%

More than 90% of these incident reports came from USA and Japan. Korea moved up from rank 10th counted in 2003 to rank 3rd in this year. The source of the reports is classified by the domain name or IP looking-up from APNIC WHOIS database.

Figure 2. Source of the report

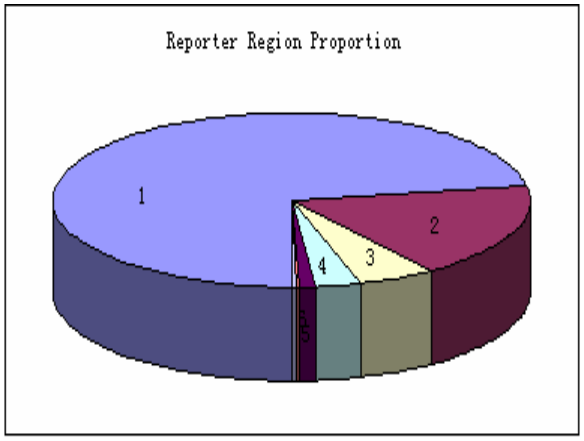


Table 2. Source of the report

Order	Country	Percent
1	USA	72.13%
2	Japan	17.98%
3	Korea	5.28%
4	Canada	2.85%
5	Brazil	1.10%
6	France	0.37%
7	China	0.12%
8	New Zealand	0.09%
9	Other	0.05%
10	Germany	0.01%

As responses to the most serious incidents, CCERT has published 8 advisories to the users of CERNET in 2004, much less than 20 advisories published in 2003. These advisories are listed as follows:

2004/12/23 Santy worm
2004/09/17 Winxp sp2 released
2004/05/01 W32.Sasser Worm
2004/04/16 Microsoft series vulnerabilities(MS04-011)
2004/02/20 Nachi Worm Variants
2004/02/19 Netsky Virus Email
2004/02/11 Microsoft series vulnerabilities(MS04-004)
2004/02/04 MyDoom.A/MyDoom.B

Projects

1. IODEF APIs and toolkit

For implementation the IODEF specification, we have developed 20 java APIs to manage IODEF objects and 13 Perl APIs to exchange IODEF objects. A toolkit is implemented too, including XML signature verification, register management based on rwhois system and IODEF schema configuration. Partial of the development is completed in conjunction with CNCERT/CC.

2. SpamAssassin Chinese Rules and Chinese Spam Database

We developed the first rule set to catch Chinese spam for SpamAssassin, named Chinese_rules.cf. It can be downloaded from the official website of SpamAssassin and it will be added into RedHat release suite. According to our statistics, about 500 email servers have been used the Chinese_rules.cf (of course with SpamAssassin) to mark Chinese spam, and 50% of them lies out of China. We have built a large Chinese spam database for the purpose of research. The spam are collected from CCERT Anti-spam Service, CCERT email server, and CCERT Honey-Pot.

3. Apollo for Google Hacking Risk Evaluation

Google hacking becomes very popular in 2004 and Santy worm, broke out in Dec. 21st 2004, destroyed more than ten thousands of PhpBB forum system with the help of search engines. We developed the software, named Apollo, to evaluate the risk of certain vulnerability which can be exploited by search engines.

Conference

1. As host organization of the CCAS2004 (Conference on Anti-Spam technology of China 2004), 2004/10/30, http://www.ccas.org.cn.
2. As joint organization, with Internet Society of China, of “Chinese Anti-Spam summit conference 2004”, 2004/4/23-24.

Training

A half-day training was hold during CERNET 2004(China Education and Research Network 2004 Annual Conference) in Beijing in Dec. 27th 2004 and three topics was concerned: Hacking Technologies in Campus Network, Incident Response and Analysis and Patch online update technologies. More than 200 administrators of campus networks of China attended the training.

Presentations

1. Internet Worm and Incident Response: Case study, Incident Response Workshop of Internet of China, 2004/2/10, Haikou city, Hainan Province.
2. Anti-Spam, Let’s Sharing Our Efforts, Chinese Anti-Spam Summit Conference 2004, 2004/4/23, Beijing.
3. Anti-spam Technologies and Analysis, User conference of Internet Society of China, 2004/9/14, Beijing
4. Active Technologies to Contain Internet Worm, XCON 2004 (XFocus Summit Conference), 2004/9/22, Beijing.
5. Research and Analysis of Spam Filtering Method, CCAS 2004, 2004/10/30, Beijing.
6. Malicious Mobile Code Analysis and Research, CERNET 2004, 2004/12/24, Beijing.
7. Anti-SPAM technologies and Chinese SPAM filter rules, CERNET 2004, 2004/12/24, Beijing.
8. Google Hacking and Intelligent Worm Defense, CNNOG1 (China Network Operators' Group), 2005/1/9, Beijing.

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.

Address: 310#, Main Building,
Tsinghua University, Beijing, China, 100084
URL: http://www.ccert.edu.cn
Email: report@ccert.edu.cn, spam@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

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 are:

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

CONTACT
URL：http://www.cert.org.cn/
E-mail：cncert@cert.org.cn
Hotline：+8610 82990999（Chinese）,82991000（English）
Fax：+8610 82990375
PGP Key：http://www.cert.org.cn/cncert.asc

Network Security Monitoring and Analysis

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

Vulnerability Alert and Research

CNCERT/CC has paid attention to vulnerability information collecting, compiling and publishing since 2003. For those critical vulnerabilities which are likely to cause mass network security incidents, we usually do primary verification and testing, then to release alert in time. Meanwhile, we also do research on potential vulnerability exploit and attack in advance, and put the critical one in monitoring.

Worm Monitoring

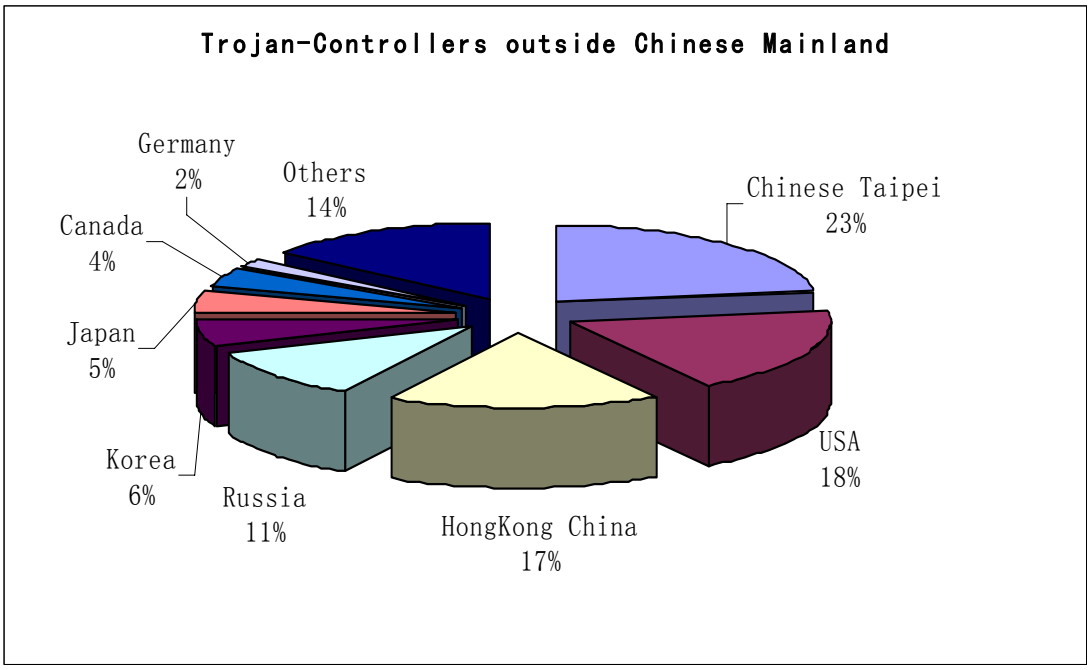
The most front-page incident about worm in 2004 is SASSER worm which exploited the vulnerability in MS Windows LSASS. A large number of computers were infected by SASSER. CNCERT/CC found out over 1,380,000 IP addresses infected in China mainland via sample monitoring.

Traffic Monitoring

By means of the abnormal traffic monitoring capability of the 863-917 Network Security Monitoring Platform, CNCERT/CC discovered the suspect network security incident for many times in China, and made the incident to be handled in time via coordinating related ISPs to verify and validate it.

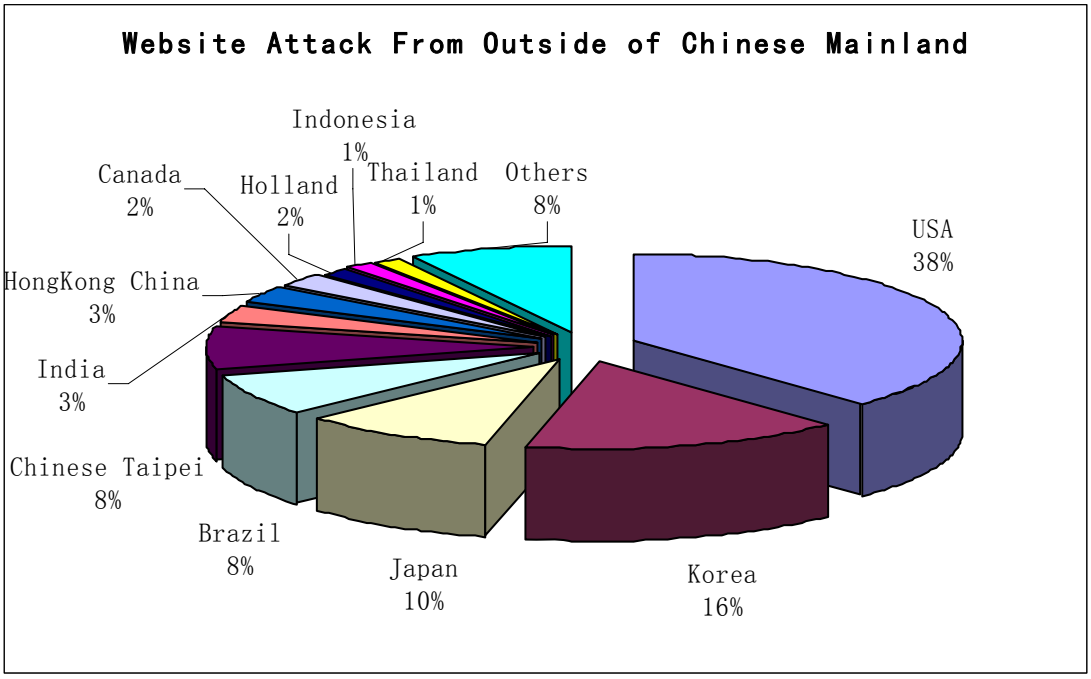
Trojan Monitoring

CNCERT/CC kept monitoring to over 20 popular Trojan programs and their activities, and discovered that more than 6,600 IP addresses of computers in China mainland had been injected with Trojan programs.



Website Attack Monitoring

CNCERT/CC kept monitoring to 38 popular kinds of website attack and discovered that 1024 foreign hosts had frequently launched attack to 3895 host machines in China mainland.



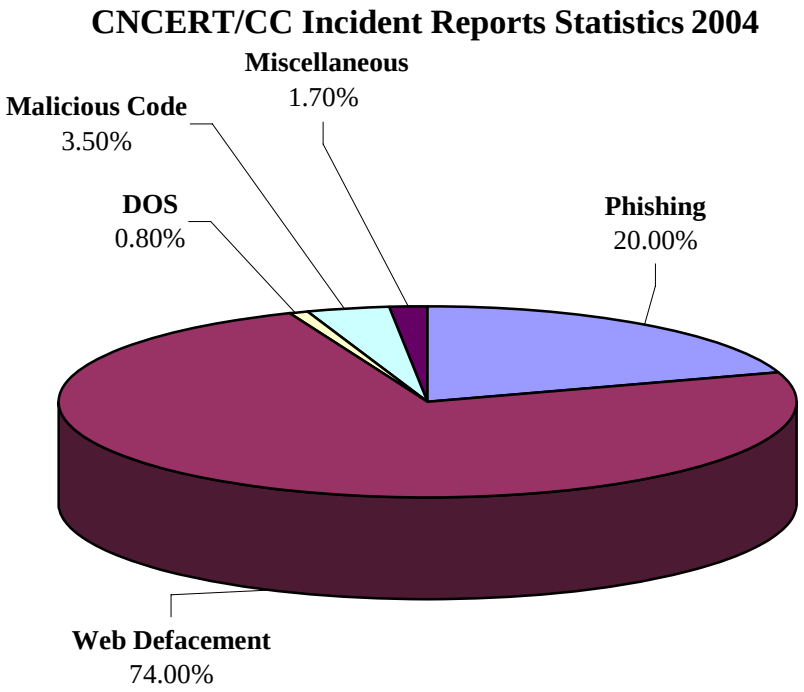
BotNet Monitoring

In a case of handling DOS incident, CNCERT/CC dug out a large active BotNet and got it to be handled successfully with the cooperation from the relevant department.

Incident Handling Overview

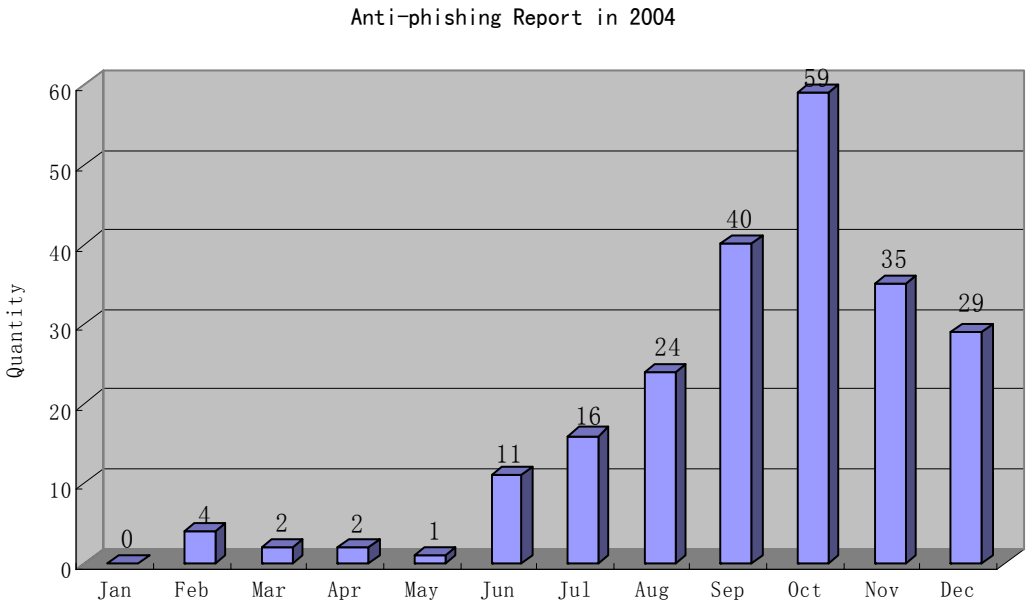
During the 2004 whole year round, CNCERT/CC had received over 64,000 security incident reports via our emergency response hotline, website, E-mail and so on, including domestic reports and those from other regions or countries, and nearly 93% reports are about scanning or probing. Thereinto, 245 incident reports are from 33 organizations of other regions except those automated forwarding scanning incident reports, including 223 Phishing reports, 4 Malicious website reports, 10 Trojan reports, 4 worm reports and 4 other miscellaneous reports.

In 2004, the main types of incident that CNCERT/CC had handled include Web Defacement, Phishing, Malicious Code, DOS and etc. The following figure shows the percentage of every type. Web Defacement（74%）and Phishing（20%） occupy the large proportion.



Phishing

CNCERT/CC had received 223 Phishing incident reports in 2004, mostly from foreign CERTs and security teams. The fraudulent finance and banking web pages also emerged in China mainland.

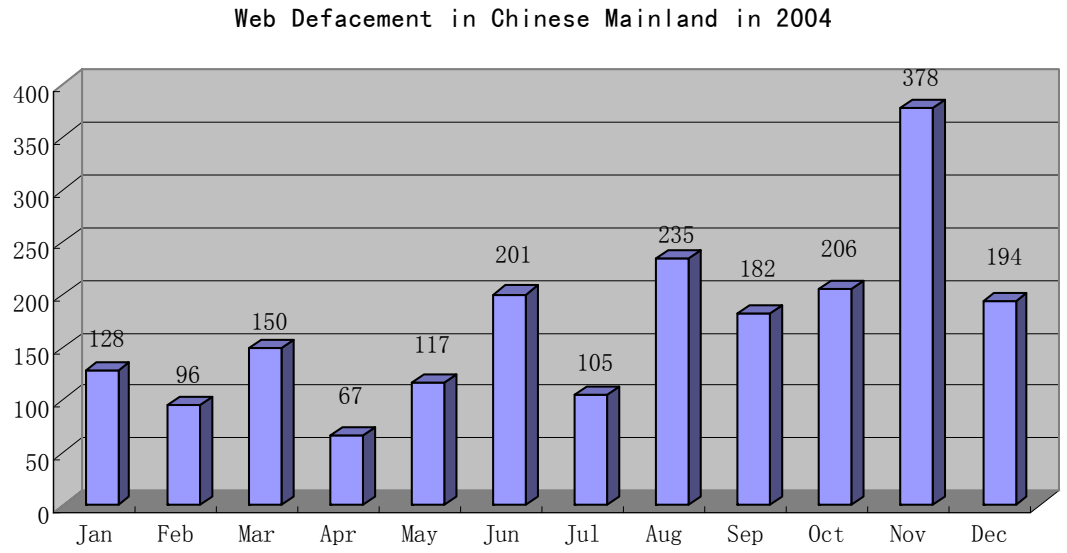


DOS

In 2004, CNCERT/CC had received quite a few severe DOS attack reports. CNCERT/CC was highly concerned about it and actively coordinated each related departments within Emergency Response System to handle them as critical incidents. In a case of DDOS, the user suffered from very long time of continual DDOS attack with the highest traffic of over 1Gbps on one occasion and over 11 types of attack. The user almost had no way to sustain their business activity, which resulted in huge economic lost. In this case, CNCERT/CC coordinated a few branches of CNCERT/CC and ISPs to deal with it, and cooperate with police agencies to do investigation and forensics. As a result, the evidence showed that, the malicious people who had launched DDOS attack via controlling a large BotNet actually aimed to crash down the victim website and beat the competitor.

Web Defacement

In 2004, CNCERT/CC kept daily monitoring to web defacement incidents in China mainland. For those discovered defaced websites, CNCERT/CC always coordinated the related provincial branches to inform websites owners to recover them as soon as possible. There were 2059 defaced websites discovered in China mainland during 2004.



Network Security Information Service

Website

CNCERT/CC's website has become the important window to provide network security information service to the public. In 2004, CNCERT/CC had published over 580 articles on the website, including security bulletins, vulnerability bulletins, virus forecasts, security reports, security news, security advisories, security tools, and statistic reports and so on.

E-mail

The current users of CNCERT/CC information service (mailing list subscribers) include provincial branches, ISP CERTs, entitled security service providers, and technical support organizations and so on.

Training and Domestic Conference

Internet Emergency Response Conference of China'2004- Hainan

CNCERT/CC undertook the Conference from 11th to 13th, February 2004.

NetSec Conference 2004 - Beijing

CNCERT/CC participated in the Conference from 24th to 25th, August 2004 as an associate.

Network Security Emergency Response Training - Harbin

CNCERT/CC hosted the Training from 8th to 11th, January 2004.

Network Security Emergency Response Speech & Presentation

CNCERT/CC staff had been invited to do presentation and speech at over 40 network security related domestic or international conference in 2004, including APEC-TEL Conference and China Internet Conference and etc.

Local Conference & Training

Many provincial branches of CNCERT/CC hosted local network security related conferences and trainings for local users in 2004.

International Cooperation and Exchange

APSIRC Conference 2004, Feb.23th -25th, 2004, Malaysia

CNCERT/CC delegation participated in the Conference. Meanwhile, CNCERT/CC delegation officially visited MyCERT.

1st China-Japan-Korea IT Network and Information Security WG, Mar.16th, 2004, Korea

CNCERT/CC participated in the Conference, and delivered a presentation.

29th APEC-TEL Conference, Mar. 21st - 23rd, 2004, Hong Kong, China

CNCERT/CC and MII delegation participated in the Conference, and delivered a presentation on "China Network Security Emergency Response Handling System and CNCERT/CC Work Introduction".

FIRST SC & APCERT SC Joint Conference, Apr. 2nd - 6th, 2004, Singapore

CNCERT/CC participated in the Conference.

AusCERT 2004 Conference, May 23rd -27th, 2004, Australia

CNCERT/CC delegation participated in the Conference.

16th FIRST Annual Conference, Jun. 13th -18th, 2004, Hungary

CNCERT/CC delegation participated in the Conference.

ITU WSIS Thematic Meeting on Countering Spam, Jul. 7th -9th, 2004, Switzerland

CNCERT/CC participated in the Conference.

2nd China-Japan-Korea ICT Business Forum, Jul. 26th, 2004, Japan

CNCERT/CC participated in the Conference, and delivered a presentation on "Challenge and Best Practice on National Public Network Protection".

3rd ASEAN-China ICT Cooperation Seminar, Aug.7th, 2004, Thailand

CNCERT/CC participated in the Conference, and delivered a presentation on "CERT: Most Active Sector in Internet Security".

APEC Computer Crime Legislation & Law enforcement Conference, Aug. 25th, 2004, Vietnam

CNCERT/CC participated in the Conference, and delivered a presentation.

CONCERT Annual Conference 2004, Nov. 23rd, 2004, Korea

CNCERT/CC participated in the Conference, and delivered a report on "Best Practice on National Network Security Protection".

Other CERTs Visits

In 2004, CNCERT/CC had welcomed other CERTs visits, such as JPCERT/CC, HKCERT and AusCERT.

Network Security Survey

In 2004, CNCERT/CC had made a nationwide network security situation survey, covering many industries and sectors, such as bank, transportation, electric energy, telecommunication, securities, insurance and etc. The survey staff had interview with nearly 3,000 network users and collected their questionnaire. The survey result will be announced at CNCERT/CC 2005 Annual Conference in March 2005.

E. Report from HKCERT/CC

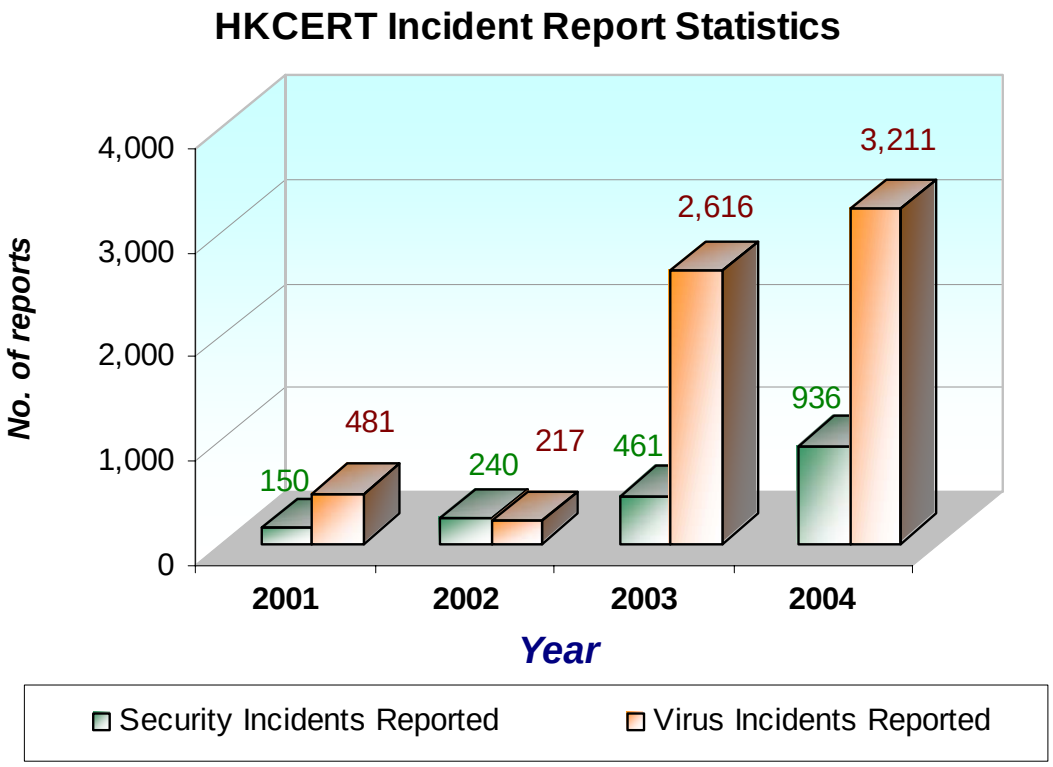
Hong Kong Computer Emergency Response Team/Coordination Center – Hong Kong, China

Regional CERT Ties Strengthened

The incident response capability of the Asia Pacific region has been greatly strengthened since 2003. HKCERT is glad to be one of the founding members of APCERT and was elected as one of the Steering Committee member in 2003. HKCERT is furthering a closer relationship with CERT teams in the region. With the sponsor of SingCERT, our centre has successfully joined FIRST in 2003. We also established formal relationship with individual CERT teams on information exchange and development, including the signing of memorandum of understanding.

Attacks Impacted Our Services

The Internet was subjected to more extensive attacks of various kinds. Since its establishment in 2001, HKCERT has received increasing number of incident reports each year, as depicted in the chart below.



The surge of incident reports during large scale attacks had drained our resources to the limits. Our support hotlines were filled up, the number of access to our web server was record high and the response was slow. In August 2003, the series of large-scale attacks caused by the Blaster, Welchia and Sobig.F worms had created tremendous impact to HKCERT incident response capacity. In that single month, HKCERT received over 1900 incident reports related to these worms. In May 2004, another worm, the Sasser worm, again brought over 1400 incident reports to HKCERT.

Improved Incident Response Capability

As a young CERT team, we definitely need to learn from other teams to improve and to provide our service timely. The attacks in 2003 & 2004 have resulted in improvements in our incident response strategy in the event of attacks of a similar scale in future.
We shall utilize the manpower resources from our mother organization, the Hong Kong Productivity Council, as a flexible backup workforce to handle the incoming phone calls;
We are upgrading the network and server capacities to handle the increase in web service requests during large scale attack period;
We has worked out with the government information web site and local content service providers to disseminate critical alert information during the period to diversify the network traffic. Some local ISPs have also agreed to post our information if needed;
We are considering the use of IVRS and fax-on-demand facilities to provide extra channels in distributing information and guidelines to the public with less direct involvement of our response team staff.

Tackling Recent Trends of Attack

Most of the recent attacks were caused by hacking worms exploiting vulnerabilities found in commonly used software. The requirement for patching the vulnerabilities as early as possible has

become more stringent because new hacking worms appear in a very shorter time frame after the disclosure of the vulnerability. The trusted communications among CERT teams and vendors on vulnerability disclosure have improved our capability in incident prevention, providing an additional dimension in incident handling. In several cases, for example, the Sendmail vulnerability, the coordination in the timing of the release of vulnerability information and the availability of the patch had prevented the public from unnecessary exposures and damages.

In Hong Kong, spamming and phishing came on the stage actively since 2003. More and more resources were driven to handle incidents and enquiries on these incidents. The Hong Kong government is considering on legislation against spamming. Our centre has also provided our views on the legislation to the government. In the past 2 years, there were increasing number of reports on fake web sites. These fraudulent web sites usually solicit the personal information from individual, including bank account numbers and e-banking passwords. HKCERT was instrumental in the referral of cases to the local law enforcement agency and CERT teams overseas. We also handled referrals from oversea CERT teams to deal with bogus web site located in Hong Kong. We had greatly benefited from the APCERT closed and trusted communications where confidential information can be exchanged with other teams directly and quickly.

Elevating the Response Capabilities of the Community

The Internet and electronic businesses are facing more and more threats these days. There is an increasing number of reported vulnerabilities. Other than handling incidents and tackling these vulnerability problems upfront, we have to make information available and disseminate to involved parties as soon as possible. We consider a better information dissemination, and public awareness and education very essential.

HKCERT had put a lot of effort in providing security awareness education and technical guidance to the public. We had organized public seminars every quarter since its establishment. In 2003 and 2004, we have organized seminars on the prevalent topics such as phishing and e-business security, and have invited representatives from regulatory bodies, banking industry, law enforcement and experts from the information security industry to share the experience and best practices with the general public. For the more sophisticated IT and information security professionals, HKCERT has organized seminars with topics such as information security Standards, and information security trends and technology, providing opportunities for them to upgrade the information security knowledge and capabilities. We have been actively participated in organizing the Information Security Summit in 2003 and 2004. These conferences were jointly organized by the major information security association and organizations in Hong Kong, including HKCERT. Reputable international speakers were invited to Hong Kong to give their views on the information security trends, development and best practices.

Enhancing Collaborative Framework

There are a number of organizations in Hong Kong with a strong interest in information security in Hong Kong. These organizations include the government related bodies, the critical infrastructure and businesses, and security service providers. HKCERT is very focused in building a long term relationship with these organizations to provide a secured information technology environment in Hong Kong.

In 2003, HKCERT, together with the Office of Government Chief Information Officer and the Hong Kong Police Force, formed a collaborative network called CONNECT (COordinatioN NEtwork on Cyber Threat). The mission of CONNECT is to coordinate the government initiatives on information security related activities to the internet community and general public of Hong Kong, including the promotional & educational activities, and the response actions in the events of high

impact incidents. Through this network, the organizations exchanged sensitive information on incidents, coordinated the analysis and actions to be taken on cyber threats and vulnerabilities, jointly organized the annual Hong Kong Information Security Survey, jointly promote the awareness of information security through seminars, exhibitions and short television drama series. The organizations also jointly published an information security guideline for small businesses. HKCERT also worked closely with Hong Kong Police Force in the report, information dissemination, technical analysis and the pulling down of phishing web sites. CONNECT is planning to expand this coordination network to include other critical infrastructure and businesses in Hong Kong.

HKCERT has established good relationship with the Financial sector in Hong Kong, through meetings and information updates with the financial organization regulatory bodies, trade associations of the banking sector on the emerging security threats especially on online banking threats. We also worked with the banking sector to promote the good online banking practices through seminars and awareness promotion.

HKCERT has also established close relationship with the internet service providers (ISPs), and internet content providers (ICPs) in Hong Kong. We had signed memorandum of understanding with the Internet Service Providers Association and a major internet content provider in Hong Kong, to exchange information on network and information security incidents. The organizations also helped disseminate alerts and security information to the members of the association and the general public.

HKCERT had coordinated with major software and security vendors closely. We held meetings regularly with these vendors. For example, we met with the security team of Microsoft to discuss security improvement and promotion activities, and to express our concerns on the disclosure of critical vulnerabilities and the schedule of corresponding patches. HKCERT also actively discussed with Microsoft on the release of Windows XP Service Pack 2, including suggesting on new features, user friendliness and the default settings. We also organized public seminar with Microsoft before the release of SP2 to inform the public on the new features and to raise the awareness. HKCERT is one of the organizations that were informed on the highlights of the latest security patches to be released by Microsoft before they were formally announced.

HKCERT has built closed connection with local anti-virus and security vendors and service providers. During critical worm attacks, HKCERT coordinates with these vendors to obtain the number of incident reports received from their Hong Kong customers to assess the overall impact of the attacks to Hong Kong. This was important especially when we have not installed a municipal network attack monitoring system covering the whole of Hong Kong. The alerts published by HKCERT also made references to the information from these security vendors. In 2003, we proactively contacted several anti-virus vendor research and development teams and suggested improvements to the anti-virus software on the notification to worm senders being manipulated by spoofing worms to generate unnecessary “spam” to innocent users whose email addresses were taken as sender.

Looking Forward

HKCERT will continue to enhance its incident response capabilities. Though we are a small team, we are willing to learn from other teams and share our experience with other teams. We shall utilize the limited resources available, and shall leverage on the resources of our partners to achieve our goals. We look forward to establishing a closer relationship with other regional CERT teams and setting up our network monitoring system in the near future.

We consider a strong collaboration of CERT teams in the region will be critical in tackling the future security threats. APCERT, as a collective force of CERT teams in the region, will be in a stronger

position in discussing and negotiating with the various parties, including multinational vendors and service providers, government bodies, and law enforcement agencies. The results of these discussions will ultimately benefit the individual teams. We expect APCERT will create a bigger influence to the community so that all parties will work closely together to provide a safer internet environment to work on.

F. Report from JPCERT/CC

Japan Computer Emergency Response Team/Coordination Center – Japan

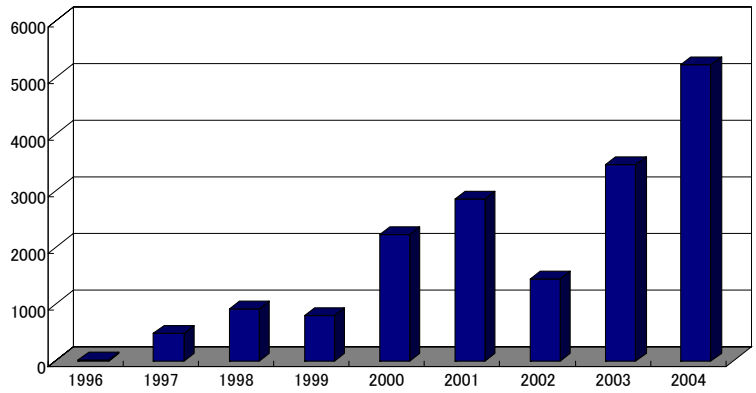
JPCERT/CC is a first CSIRT (Computer Emergency Response Team) established in Japan. It is an independent non-profit organization, acting as a national point of contact for the CSIRTs in Japan and worldwide. Since its inception in 1992, the center has been gathering computer incident and vulnerability 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 2004, JPCERT/CC issued 5,217 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 5,217 tickets, 4,974 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	644	920	1749	1904	**5217**

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	
.au	237	451	1192	628	2508
.net	124	189	264	883	1460
.jp	188	225	225	210	848

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 2004 are listed below:

- JPNIC-JPCERT/CC Security Seminar - a series of 5 security seminars jointly organized with JPNIC (3 Sep, 4, 5 Oct, 2004, and 3, 4 Feb 2005)
- InternetWeek 2004 in Yokohama – one day security track jointly organized with Japan Network Security Association (JNSA) and Telecom-ISAC Japan (1 Dec 2004)

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/

Activity Highlights

APCERT Secretariat

JPCERT/CC is supporting the security community in the Asia Pacific region by acting as a secretariat for APCERT. Our contribution also includes a 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 assisted two CSIRTs in Japan to become a member of FIRST.
- JPCERT/CC provide a program committee chair (co-chair) for the next 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
Three 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

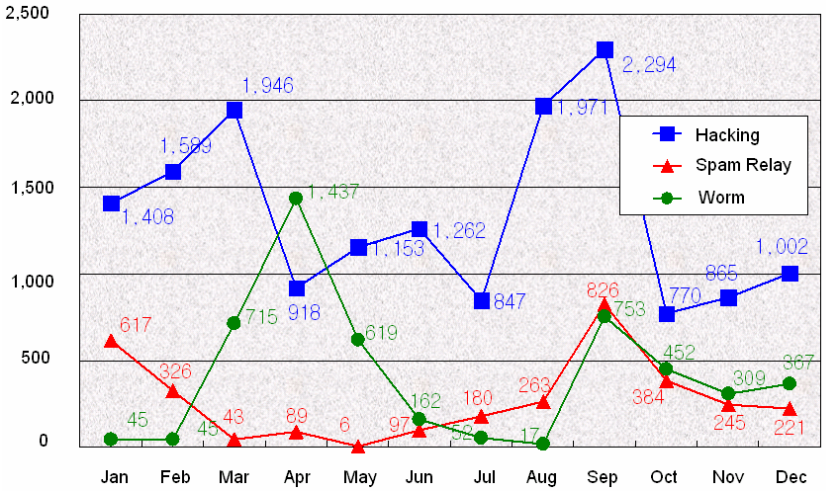
I. Introduction

KrCERT/CC(in other words, KISC, Korea Internet Security Center) is a critical point for detecting, analyzing and responding internet incidents such as worm, bot or hacking. To minimize the damage from the incidents and to ensure the convenient Internet use, KrCERT/CC has being working on 24/7 basis.

II. 2004 Activities

1. Internet Incidents statistics in 2004

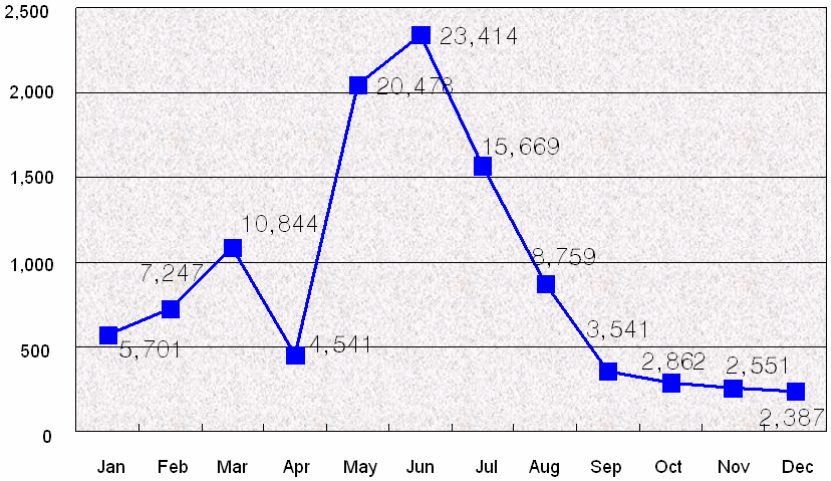
The total number of incident reports[1] in 2004 is 24,297. The incident reports consist of reports of hacking (16,027), spam relay (3,297) and worm (4,973) and the number of reports in 2004 was slightly decreased from that of 2003(26,179).



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

(Figure 1) Monthly Statistics on Incident Reports in 2004

10 new types of worm[2] emerged in 2004. This means the dramatic decrease in new variants compared to the variants emerged in 2003(108 types). Contrary to the decrease in new types of worm, the reports[3] on damage caused by worms(107,994) in 2004 increased from those in 2003(85,023).



(Figure 2) Monthly Statistics on domestic worm damage reports in 2004

220 domestic web servers[4] were exploited as the Phishing counterfeit sites in 2004.

KrCERT/CC announced 48 worm/virus alerts and published 22 advisories, 2 incident notes, and 20 technical reports.

2. New Project

1. Incident-related Information Collecting
To detect, analyze and respond Internet incidents early and effectively, sufficient information on the status of internet back-bone networks is essential. Based on the relevant law(abbreviated as network law) in Korea, amended and enacted in 2004, KrCERT/CC legally collects real-time statistics information from ISPs, IDCs, and MSSP5s. Incident-related information providers, including major ISPs, IDCs, critical communication infrastructure, MSSPs, private autonomous system operators and anti-virus companies, are obliged to provide statistics information composed of total traffic volume, BPS/PPS volume and attack type. In 2005, KrCERT/CC has a plan to expand the number of information providers to obtain statistics information so that the the accuracy and reliability of decision making on response can be improved.

2. International Joint Incident Handling Drill
CJK CERTs(CNCERT/CC, JPCERT/CC and KrCERT/CC) exercised the first international joint incident handling drill at 16th December. Not only CJK national CERTs but also each country's major ISPs participated in this drill and it lasted about two hours. The objectives of this drill were to verify the coordination system 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. The drill was practiced based on the two scenarios: Blocking intermediate BOT server and filtering the malicious traffic from the new worm

[2] **Statistics of new worm types excludes worm variant types**
[3] **Reported to and detected from major anti-virus companies in Korea and KrCERT/CC**
[4] **Reported from foreign CSIRTs or phished organizations to KrCERT**
[5] **Managed Security Service Provider**

III. 2005 Plan

First of all, KrCERT/CC is planning to open CERT-building training courses to Asia-Pacific undeveloped countries which don't have the capability of building CERT by themselves.

Second, KrCERT/CC will execute International Joint Incident Handling Drill periodically and invite other CSIRTs to participate in. This drill will give participating CSIRTs an opportunity to improve the response ability.

Third, KrCERT/CC will initialized the IODEF Project and improve the traffic monitoring website in which more CSIRTS' joining are pretty much welcome. More information will be in website soon.

Thank you.

POC:
Web site: http://www.krcert.or.kr
E-mail address: cert@certcc.or.kr
Telephone number: +82-2-405-5526

H. Report from MyCERT

Malaysian Computer Emergency Response Team – Malaysia

The year 2004 had been a hectic year for the Malaysian Computer Emergency Response Team (MyCERT), both in handling security incidents and involving in various activities in the field of ICT security which consequently saw MyCERT as a prominent CERT Team at national level as well as at international level.

MyCERT's activities for the year 2004 are listed as below:

A. Incident Handling

MyCERT had played a big role in fighting/eradicating some major incidents/outbreaks in the country and assisted organizations terribly affected by the W32.MyDoom outbreak in January 2004 and W32.Sasser worm outbreaks in May 2004. Other notable incidents that MyCERT had played big role in eradication are mass web defacements, harassments and forgeries. MyCERT had handled a total of 965 real incidents which included all categories of security incidents. MyCERT had also assisted the Malaysian Law Enforcement Agencies such as the Royal Malaysian Police, the Malaysian Communication and Multimedia Commission and the Attorney Chamber in handling some incidents including some high profile incidents in the country.

B. Produced Alerts, Advisories, Guidelines

In year 2004, MyCERT had produced 15 alerts on worm propagation, discovery of new exploit, phishing scams and mass web defacement. MyCERT had also produced 4 advisories on worm propagation and had produced 4 quarterly summaries. The above alerts, advisories and summaries are available at:

http://www.mycert.org.my/advisory/

MyCERT had also produced the monthly Incident Statistics throughout year 2004. In addition, MyCERT had also produced a document on CERT Establishment for the Afghanistan CERT. MyCERT had also released its first newsletter which was then succeeded as NISER e-Security Newsletter.

C. Organized Seminars/Workshops/Trainings

In early year 2004, MyCERT was entrusted to play an active role and responsibility in organizing the APCERT Conference from 23-26 February 2004 in conjunction with APRICOT 2004. This workshop was successfully held with overwhelming response from audience which comprised of APCERT members and the objective of the workshop was successfully accomplished.

D. Attended Seminars/Conferences/Meetings/Presented Papers

The role of MyCERT in the international arena was noted significantly where representatives from MyCERT had attended and presented papers at various seminars, conferences and meetings related to the field of ICT security.

- On 23-26 February 2004, seven representatives from MyCERT had attended the APCERT Workshop in Kuala Lumpur, Malaysia. A representative from MyCERT had presented a presentation titled "Incidents for Year 2003: MyCERT's Experience"

- In April 21 – 23 2004, two representatives from MyCERT had attended the Cansectwest in Vancouver, Canada. In this Conference, MyCERT's representative had presented a paper titled "Distributed NIDS Sensors".
- On 20th April 2004, a representative from MyCERT attended the ASIAN Senior Officials Meeting in Jakarta, Indonesia. A paper was presented by MyCERT's representatives titled "The establishment and experiences of the Malaysian Computer Emergency Response Team".
- Two representatives from MyCERT attended the Workdshop on Establishing CSIRT in Singapore, from 19 – 23 July 2004.
- In June 27 – July 2nd 2004, two representatives from MyCERT attended the USENIX'04 Annual Technical Conference, Boston, USA. A paper was presented by MyCERT representative titled "Building a NIDS with Open BSD".
- Four representatives from MyCERT attended the Hack In The Box conference in Kuala Lumpur, Malaysia from 14th – 17th October 2004. A paper was presented by MyCERT's representative titled "Honeypot and Internet Background Noise - Lesson Learned".

E. Trainings /Talks

a) In order to educate System Administrators/IT Personnel on proper incident handlings and response, MyCERT had conducted two sessions of Incident Handling and Response trainings on 15 April 2003 and on 28 – 29 July 2003. MyCERT received good response from individuals and companies to attend the trainings.

b) On December 13th – 17th, MyCERT organized a 5 day course by AUSCERT on CSIRT Training for Indonesia CERT. Participants for the course were from the Indonesian CERT as well as from MyCERT.

c) MYCERT was entrusted by the Malaysian Communication and Multimedia Commission to conduct series of talks and presentations on Incident Handling around the country with the purpose to educate Internet users on incident handling, around the country . As such MyCERT was involved in conducting 4 such Talks/presentations on Incident Handling at the following locations in Malaysia:

i) May 2004, Kuala Lumpur

ii) July 2004, Penang

iii) August 2004, Ipoh

iv) December 2004, Kuching

F.Initiatives to Establish Mutual Collaborations

MyCERT had also initiated close ties between MyCERT and Panda Software Anti-virus in promoting the Panda Software's 1st Worldwide Internet Security Campaign which aims in making the internet a safer place.

G.Other Noteworthy Activities

In year July 2004, MyCERT had initiated to form a Special Interest Group for the Incident Handling committee as well as for the ICT security committee in the country. In July 2004, MyCERT had successfully organized its first MyCERT Special Interest Group knowledge sharing session. The quarterly session received overwhelming response from Internet users and IT-driven organizations. As of now, MyCERT had successfully held its 3rd MyCERT SIG knowledge sharing session. We

received good response from participants of MyCERT's initiative to organize such a beneficial session.

I. Report from Ph-CERT

Philippine Computer Emergency Response Team – Philippine

The Philippine Computer Emergency Response Team (Ph-CERT) is a non-stock, non-profit organization which consists of information security practitioners and enthusiasts. It was formed on March 30, 2001 to provide the Philippine business community and the Philippine government bureaucracy with a reliable and trustworthy point of contact for computer-related, Internet-related and other information technology-related emergencies. Its officers serve on a voluntary basis.

Ph-CERT has been focused on promoting information security awareness through its advocacy programs. In 2004 Ph-CERT developed its five-point plan that covers the following:

- Building Partnerships with Government
- Strengthening Relations with Business and Industry
- Leveraging on Academic Relationships
- Nurturing Regional and International Relationships
- Policy and Rule Making

Accomplishments in each area are presented below:

Building Partnerships with Government – Ph-CERT is represented in the Task Force on the Security of Critical Infrastructure – Cyber Security Work Group (TFSCI-CSWG). The TFSCI-CSWG was created under the office of the President of the Republic of the Philippines with objective of drafting the Philippine Information Security Plan. The plan addresses the different information security needs of eleven (11) critical sectors. One of the significant outputs of the TFSCI-CWG is the creation of the Philippine Government Computer Security Incident Response Team (Philippine G-CSIRT), which is the IRT for Philippine Government Agencies. Ph-CERT provided expertise in setting up the Philippine G-CSIRT.

Ph-CERT is a member of the Advisory Board of the Philippine G-CSIRT.

Ph-CERT is consulted by the National Bureau of Investigation (NBI) and the Criminal Investigation and Detection Group (CIDG) of the Philippine National Police (PNP) on matters pertaining to security and cyber crime incidents. Ph-CERT provides, on a need basis, expertise on tracing the origins of intruders and provides advise on the collection and handling of evidence.

Strengthening Relationships with Business and Industry – Apart from providing information on internet security incidents to its members, Ph-CERT has been advocating for the creation of Business and Industry Level CERTS. Ph-CERT is now in the process of meeting with various business and industry associations to increase awareness on information security and the need to create CERTs or IRTs at their levels.

Leveraging on Academic Relationships – Ph-CERT has established a partnership with the Asia-Pacific College (APC), an educational institution that develops talents for the IT industry. Ph-CERT is providing assistance in the development of educational degree and non-degree programs on information security. An information security courseware has been prepared by the APC with the assistance of Ph-CERT which will be integrated in the curricular degree programs of the

educational institution. The courseware is scheduled to be offered to students during the third trimester (January to April) of the current school year. APC will also start offering short courses on information security to business and industry during the first quarter of 2005. Ph-CERT will provide speakers (to be source from among its members) who will conduct the short courses.

The Asia-Pacific College hosts the offices of Ph-CERT.

Nurturing Regional/International Relationships – As a member of the Asia Pacific Computer Emergency Response Team (APCERT), Ph-CERT collaborates with the APCERT by engaging in information exchange with member countries regarding Internet security incidents and current and emerging technologies for monitoring and handling of such incidents.

Ph-CERT, jointly with the Australia Computer Emergency Response Team (AusCERT) provided Ph-CERT members and non-members training on CERT Best Practices. This training was conducted in March 2004 at the Asia-Pacific College.

Ph-CERT participated at a conference organized by the Asia-Pacific Telecommunity held in Huahin, Thailand last September, 2004 and shared knowledge on CERT Best Practices and experience in building CERTs or IRTs. Ph-CERT is now in contact with representatives from countries like Afghanistan, Bhutan, Iran, Laos, Maldives, Mongolia, Myanmar, Nepal, Sri Lanka, Tonga, and Vietnam among others, providing them with suggestions on CERT Operations.

Policy and Rule Making – Ph-CERT has been participating in various government councils and task forces whose goal is to chart an ICT Roadmap for the Philippines and develop policies therefor.

Specifically, Ph-CERT officers are members of the Information Technology and Electronic Council (ITECC) and have helped in crafting proposed legislation on Cyber Crime, Information Security, and Information Privacy and Confidentiality, among others.

PH-CERT is consulted by the Commission on Information and Communications Technology (CICT) on matters pertaining to Internet Security.

Ph-CERT officers are also members of the Task Force on the Security of Critical Infrastructure which drafted, among others, the Philippine Information Security Plan.

Ph-CERT is also represented in the Philippine Supreme Court's E-Commerce Subcommittee which had drafted the rules on Electronic Evidence and is presently crafting rules on Electronic Notarization which is expected to be released by the Court in the early part of 2005.

Ph-CERT is advocating for the drafting a policy that will specifically address email spam and phishing. Expected outputs are the (1) creation of an information exchange program on email spam and phishing incidents and (2) creation of an awareness program geared towards the minimization of email spam and phishing incidents or the mitigation of the effects of such incidents.

J. Report from SingCERT

Singapore Computer Emergency Response Team – Singapore

Introduction

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 covering a wide range of security topics.

Incident Trend and Highlights for year 2004

SingCERT received over 500 incident reports for the year 2004. Probes and scans attempts continue to be a problem and contribute a significant percentage to the reported incidents. We see a surge in the number of probes and scans to ports 17300, 135 and 445 in the months of May, June and July, possibly due to the Kuang2 trojan, Gaobot and Sasser worms propagating through network shares.

SingCERT continues to work closely with our Internet Service Providers (ISP) to track down the persistent source of attacks and send them warnings. In severe cases, SingCERT will request that the ISPs suspend accounts and shut down systems.

In recent months, we see a rise in phishing attacks targeting local banks and other financial institutions. SingCERT assisted the local banks in tracing the bogus websites and worked with other CERTs to shutdown these fraudulent websites.

SingCERT Security Awareness Activities

SingCERT organised security seminars and workshops on a regular basis to raise the general level of security awareness in the industry and the general public. Sharing sessions were organised with our constituency on the latest developments and technologies in the field of security. The following is a list of topics conducted in year 2004 with industry collaboration:

- SingCERT Security Seminar - An Insight into Microsoft Security Initiatives
- SingCERT Security Seminar - IP Sec VPN or SSL-VPN
- SingCERT Security Seminar- Importance of Preemptive Security
- SingCERT Security Seminar- IT Practical Workshop: Web Exploit Engineering
- SingCERT Security Seminar - More than just firewall and Anti-virus
- SingCERT Security Workshop – Understanding Email Headers & Web Vulnerabilities

SingCERT Project Highlights

1. CSIRT Workshop for ASEAN CERTs

To accelerate the development of cybersecurity in ASEAN and in particular, to assist members that do not have a national CERT, SingCERT, in collaboration with AusCERT, organised a CSIRT Incident Handling Workshop for ASEAN from 19 – 23 July 2004 in Singapore. The workshop was attended by representatives from the 10 ASEAN member countries, namely, Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, Philippines, Thailand, Vietnam and Singapore.

The workshop was funded under the ASEAN-Australia Development Cooperation Program, Regional Partnerships Scheme and was meant to assist member countries, namely, Cambodia, Laos, Myanmar and Brunei to kickstart their plan to establish their national CERTs. To date, Myanmar and Brunei have established their national CERTs.

2. Preparation for 2005 FIRST Conference in Singapore

The 2005 FIRST Conference will be held in Singapore in June 2005. SingCERT's representative attended the 2004 FIRST Conference in Hungary to understand how SingCERT as the local CERT for the hosting country can assist in the preparation.

SingCERT provided assistance to the 2005 Program Committee in obtaining approval from IDA to officially support the event and to invite the Minister for Information, Communication and the Arts (MICA) of the Singapore government to deliver the keynote address. SingCERT provided contact information of local organisations which may be interested to become sponsors of the event to the FIRST conference organiser.

SingCERT will be the point of contact for APCERT where FIRST Conference 2005 is concerned and is working with APCERT members to help promote and market the event to boost the conference attendance.

3. SITEX 2004

SITEX, organised by the Singapore Infocomm Technology Federation, is one of the major IT and consumers electronics exhibitions held yearly in Singapore. Each year, hundreds of thousands of consumers visit SITEX to check out the latest IT gadgets, as well as to take advantage of discounts and promotions. This year SITEX 2004 was in held Singapore Expo on 15 -18 November 2004 in Singapore.

To inculcate infocomm security awareness amongst the general masses, IDA organised a series of security talks at the IDA's Pavilion and SingCERT presented one of the talks on "Cyber Security Tips for Home Users" to provide information and tips to users on how to cruise safely on the Internet and to defend themselves against spam, spywares and phishing attacks.

K. Report from ThaiCERT

Thai Computer Emergency Response Team – Thai

Review and Comparative Incident Statistics (2001-2004)

Since ThaiCERT formation in 2000, it has been receiving a number of security incidents and coordinated with the informers to help them fix the problems. The tables below show incident statistics since the year 2001-2004.

Year	2001	2002	2003	2004
Number of Incidents	150	355	386	400

Type of incident / Year	Spam Mail	Port Scan and Probe	Malware (Virus, Worm etc.)	Others (Hack, DDos etc.)
2001	66	38	34	12
2002	183	90	55	27
2003	31	170	171	17
2004	48	132	210	10

Summary and analysis type of incident

For year 2004 the highest percentage of incident type is malware case (52%), the second one is port scan and probe case (33%), the third one is spam mail (12%), and the last one is other types such as hacking or DDoS (3%).

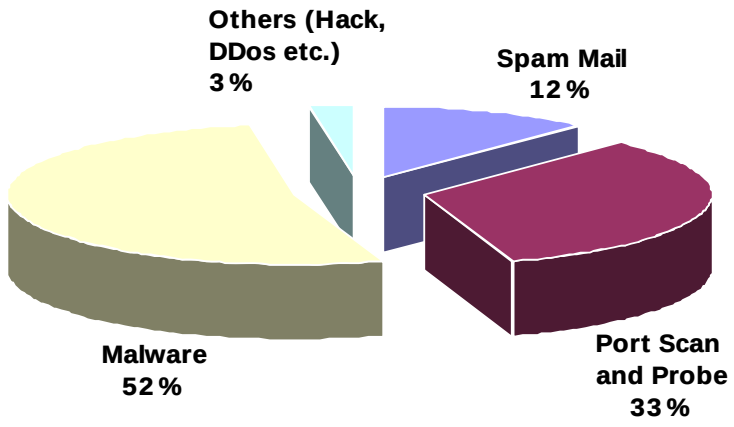


Figure 1 Display each type of incident in year 2004

Summary and analysis

For the total amounts, when compares with last 3 years, it still has been increased chronologically as you can see in the pie chart below.

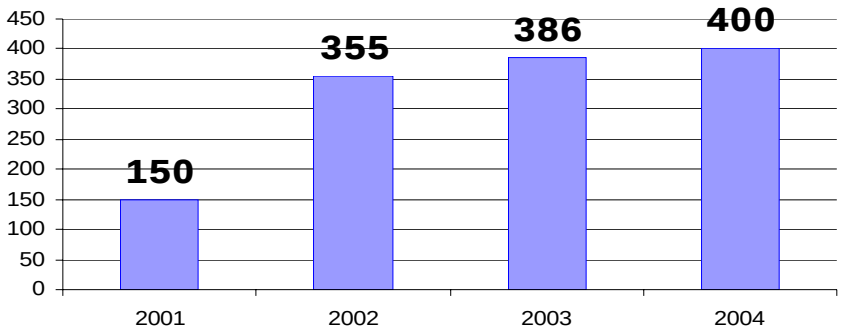


Figure 2 Display total amounts of incident cases in year 2004 (unit: cases)

Staff and Structure

Nowadays ThaiCERT has 15 full-time staff and 2 of part-time staff as a result of last year heavy recruitment. Moreover, our two staff has been received ISO17799 certification and one has got Certified Wireless Network Administrator Wireless (CWNA). However, security knowledge is all time update, so we plan to get more in other areas.

ThaiCERT's Services and Activities

1. Incident Response (as shown on the table and figure above)

2. CERT Advisory and Virus Alert in Thai language

We announced about security advisories in our website.

Viruses and Vulnerabilities Alert

- Perl.Santy.A
- W32.Zafi.D@mm or W32.Erkez.D@mm
- W32.Bagle.AZ@mm, and its variant or tail name
- W32.Mydoom.Q@mm, and its variant or tail name
- W32.Sasser.Worm and its variant or tail name
- W32.Netsky.S@mm and its variant or tail name

CERT Advisories 30 articles in Thai language

CA-2004-30 Exploitation of php BB highligh parameter vulnerability
CA-2004-29 Update for Microsoft Internet Explorer HTML Elements Vulnerability
CA-2004-28 Cisco IOS Input Queue Vulnerability
CA-2004-27 Buffer Overflow in Microsoft Internet Explorer
CA-2004-26 Multiple Vulnerabilities in Microsoft Internet Explorer
CA-2004-25 Multiple vulnerabilities in Mozilla products
CA-2004-24 Microsoft Windows JPEG component buffer overflow
CA-2004-23 Vulnerabilities in MIT Kerberos
CA-2004-22 Multiple Vulnerabilities in Oracle Products
CA-2004-21 Security Improvements in Windows XP Service Pack 2
CA-2004-20 Multiple Vulnerabilities in libpng
CA-2004-19 Critical Vulnerabilities in Microsoft Windows
CA-2004-18 Multiple Vulnerabilities in Microsoft Windows Components and Outlook Express
CA-2004-17 Internet Explorer Update to Disable ADODB.Stream ActiveX Control
CA-2004-16 Important Internet Explorer Update Available
CA-2004-15 Multiple Vulnerabilities in ISC DHCP version 3
CA-2004-14 Cross-Domain Redirect Vulnerability in Internet Explorer
CA-2004-13 SQL Injection Vulnerabilities in Oracle E-Business Suite
CA-2004-12 CVS Heap Overflow Vulnerability

CA-2004-11 Cisco IOS SNMP Message Handling Vulnerability
CA-2004-10 Vulnerabilities in TCP
CA-2004-09 Multiple Vulnerabilities in Microsoft Products
CA-2004-08 Vulnerability in Internet Explorer ITS Protocol Handler
CA-2004-07 Multiple Vulnerabilities in OpenSSL
CA-2004-06 Microsoft Outlook mailto URL Handling Vulnerability
CA-2004-05 Multiple Vulnerabilities in Microsoft ASN.1 Library
CA-2004-04 HTTP Parsing Vulnerabilities in Check Point Firewall-1
CA-2004-03 Multiple Vulnerabilities in Microsoft Internet Explorer
CA-2004-02 Email-borne Viruses
CA-2004-01 Multiple H.323 Message Vulnerabilities

Mailing List

Originally, ThaiCERT security advisories were issued through its website which was not enough to raise security awareness in the community. The mailing list service was thus added to provide another channel. The advisories issued are entirely in Thai and there are 3 types of mailing lists.

- ThaiCERT-news Mailing List: To announce monthly news, seminar and training courses offered by ThaiCERT and also to update ThaiCERT activities. Now there are about 7,750 members in our list (increasing about 1,000 members).
- ThaiCERT-advisory Mailing List: To announce CERT/CC Advisory (translated into Thai). Now there are about 8,122 members in our list (increasing about 1,200 members).
- ThaiCERT-virus-alert Mailing List: To announce virus alerts of which are high damage potency). Now this kind of member is about 10,000 (increasing about 1,000 members).

3. Vulnerability web scanner

It is a research and development project based on core competency of CERT. We would like to create much more security awareness for Thai network administrators, which this one is a convenient tool for him/her to detect their system's vulnerability may have. Furthermore, we are ongoing to bring about its value added with clearly, easily, and importantly recommendation for them to patching their system immediately.

4. ISO 17799 simplified course for planning and implementation

After Thai government announce the electronic transaction commission since last 3 years, ThaiCERT has been involved on its tasks—Secretariat of Security Sub-committee of this commission. As some survey show, Thailand IT systems still have many vulnerabilities and a few experts on this area, so it is tough if we do the standard as same as international's one. Therefore, this commission set its main target to enhance several government and private organization's IT systems to be more secured, which uses step by step improvement. Finally, ThaiCERT do produces the basic content in order to let them see the easy way to step up their systems referred to this standard.

One more important activity, ThaiCERT, as secretariat of Security Sub-committee had published and launched the Standard book in Thai language around 2,000 books. Its distribution focuses on government sector and also some important private organizations. We plan to held a seminar on this matter by inviting those CEOs, CIOs, IT managers, or experts to join soon.

5. FIRST member application

As a little bit long period of ThaiCERT establishment, we have joined CERT community conference and done some activities together such as sharing information, attending some training courses and so on. We believe that many CERTs trusted us, so it is a good opportunity for us to apply for FIRST member, and now we are on process of asking for the previous members nominating us to this forum. Accepted to be a FIRST member is our mandate for this year.

Training/Seminar/Education

We arrange a variety of Training/Seminar/Education in a year. A major event arranged annually is Thai IT Security day. There will be a number of security-related sessions to join and we invite many security experts in Thailand to provide speeches in several security topics.

Every year we open our ThaiCERT lab for others to visit. This year we showed virus and protection

steps and wireless security demonstrations.

We plan to produce e-learning materials to publish on the internet for our Thai community. The first series to produce is Safety Net – how to use internet in a secure manner.

We also arrange some training to the public, such as OS hardening, Server hardening, and ISO 17799 course a few time a year.

Other activities

We took some roles on the tsunami disaster such as coordination with the neighboring CERT, security monitoring, and checking for data validation on web site www.missingpersons.or.th .

Final remark

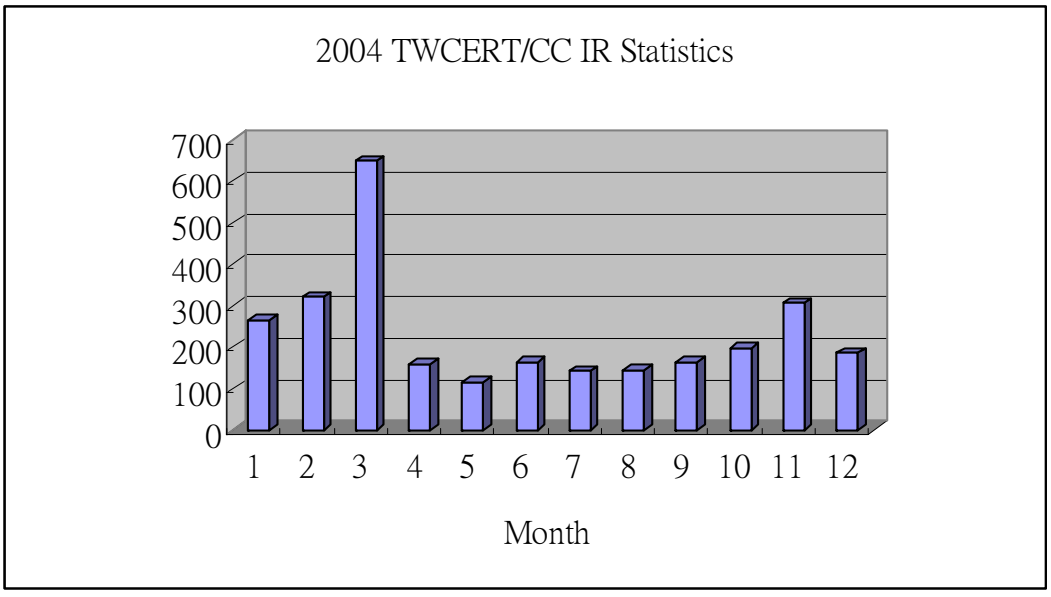
As some CERT knew that there was a worm spreading themselves using MSN—well known as Bropia worm, distributed on 19 January 2005. ThaiCERT had detected this situation and announced to our members via e-mail list prior to any launching of anti-virus signature agents and found that this can safe our internet users. Therefore, it was not much impacted to Thailand network traffic.

L. 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 2828 incidents during the year of 2004 as shown below.



- **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.
  - 5th Symposium of Internet：Information Law and Society
  - APSIRC 2004 (Febuary 23-25, Golden Horses, Kuala Lumpur, Malaysia)
  - AusCERT Asia Pacific Information Technology Security Conference 2004（May 23-27,Australia）
  - FIRST 2003 16th Annual Computer Security Incident Handling Conference (June 13-18, Hungary)
  - 30th APECTEL (September 19-24, Singapore)

- **SPAM Cooperation**

  TWCERT/CC Joined the Seoul-Melbourne Multilateral Memorandum of Understanding (MoU) on Cooperation in Countering Spam in December 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

M. Report from TWNCERT

Taiwan National Computer Emergency Response Team – Chinese Taipei

Introduction

TWCIRC has changed its name to TWNCERT (Taiwan National Computer Emergency Response Team) since the beginning of year 2004; it continues to provide information security services to Taiwan governmental agencies, 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 government response center that can help optimize the capability of immediate monitor, coordination, response and handling in the face of security incident. TWNECRT is therefore to enhance the government's ability to respond and deal with security incidents and internationalize our efforts.

2004 Highlights

1. Promotion of IT Security Awareness

TWNCERT offers IT security conferences, workshops, training courses, and exhibitions to government employees that include network managers, system administrators, technical staff etc. The organized events in 2004 are listed below:

- Conference
  - 2004 Network Security Engineering Conference (11-12 March)
  - Information Security Management System and Technical Resolution for Government Agency (29-30 April in Taipei, 5-6 May in Kaohsiung)
  - ISMS Forum- Practical Experience in Physical Security (March 25)
  - 2004 NATEA (North American Taiwanese Engineers' Association) e-Business and Software Security Conference (14 July)
  - Government Agency Operation System Security Conference (10 August in Taichung, 17 August in Taipei)
  - ISMS International Conference (22 October)
  - ISMS for Government Agency Conference (18 November in Kaohsiung, 29-30 November in Taipei)
- Workshop
  - Microsoft Security Patch Program and Deployment Workshop (20 April- 30 June, a series of 11 workshops)
  - ISMS Lead Auditor for Government Agency (3 May- 10 June, a series of 6 seminars)
  - Infrastructure of ISMS (23 June- 6 August, a series of 5 seminars)
- e-Learning
  - Network Security (Long Term Course: 8 July- 7 October, Short Term Course: 4-17 July/ 25 July- 7 August)
  - Online Course (10 April- 31 December)
- Exhibition

- International Information Technology Exhibition in Taipei (25-27 March)
- Applications for IT Industry & Government Agency in 21st Century (21-22 July)
- 2004 National Information Exhibition (4-31 December)

2. Information Security Publications

According to the current information security circumstances in Taiwan, TWNCERT has completed several security publications:

- An Analysis of International Information Security Regulations
- A Case study of Electronic Evidence in the Court
- 2004 Information Security Marketing Research in Taiwan

- Security Analysis for Classified Government Agency
- The Development and Research of Information Security

3. Monitor, Analysis, and Prevention
TWNCERT formed Information Security Technical Services Groups to visit governmental units, to comprehend the current situations of these units on virus protection, patch installation, log analysis, backup, weakness scan, and incident handling, etc.

4. Incident Handling
TWNCERT cooperates with IT security firms to handle incidence, provide solutions, and set up hacking database system in order to reduce the network incidence. It also contributes manpower to assist in investigation, sorts out the compromised governmental units, helps the recover and reduced damages from the incident, and effectively stops attempts of the attacks.

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 2004.

2005 Plan

1. Coordinating among relevant agencies and organizations to identify pertinent response and actions in case of security incident.
2. Providing an information exchange center for information at home and abroad.
3. Helping relevant government agencies to set up computer emergency response team (CERT).
4. Providing reference information to government agencies for formulation of security policies.
5. Executing NSOC (National Security Operation Center) project therefore to monitor, prevent, analysis, and report incidents for the mainly government units.

For the international cooperation, TWNCERT would like to share information with more global FIRST community in year 2005.

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