APCERT

Asia Pacific Computer Emergency Response Team

2003 ANNUAL REPORT

Asia Pacific Computer Emergency Response Team (APCERT) Secretariat
Email: apcert-sec@apcert.org URL: http://www.apcert.org

Chairman's Message

In the late 1990s a vision was developed by the leading Computer Emergency Response Teams (CERTs) in the Asia Pacific to establish a mechanism for regional cross border cooperation. The Asia Pacific Security Incident Response Coordination WG (APSIRC-WG) or APSIRC as it was known, was chartered to create the Asia Pacific regional forum to providing a place to exchange ideas and expertise on Internet security incident handling.

In early 2001 an invitation was extended to the leading CERTs and Computer Security Incident Response Teams (CSIRTs) from the economies in the Asia Pacific region to attend an APSIRC meeting in Japan hosted by JPCERT/CC. The clear intention of this meeting was to discuss improved working relationships between neighbors across international borders. Interest in the meeting was strong.

One of the key outcomes from the APSIRC meeting in Japan was the decision to form APCERT as the vehicle for regional cross border cooperation and information sharing. A working group was formed which used a consultative process to forge an agreement for the 15 CERT teams from the 12 Asia Pacific economies that agreed to establish APCERT. The agreement developed by the working group was put to the meeting of APSIRC which was held in conjunction with APRICOT 2003 in February 2003 in Chinese Taipei. The APCERT agreement was accepted, the Steering Committee elected in conjunction with the Chair and Secretariat for APCERT.

In hindsight, many of the goals and objectives of APSIRC firmly established and became the legacy upon which APCERT is built. In the last few years, the Asia Pacific region has developed rapidly and so has the need for an Asia Pacific CERT/CSIRT community. As a number of economies have clearly identified, the information based societies that will be built in the region in the next five years must have a secure foundation to succeed.

We now come to the second annual meeting of APCERT in Malaysia. The twelve previous months have passed quickly, and the development and growth of APCERT is clearly visible and I suggest exceeded expectations in such a short period of time. APCERT has:

- Developed into a dynamic network of responsive CERT/CSIRT contacts which is now one of the best; and the first of its type in the world
- Gained the active support and confidence of the many governments in the region and the attention and interest of government and non government regional groups beyond the Asia Pacific region.
- Been invited to participate and contribute to intra-government forums such as APEC
- Become a model for the development of other regional groups in the world and a benchmark for such groups to measure against.
- Commenced active sharing of information about computer threats, vulnerabilities and incidents and demonstrated a capability to provide practical and effective incident response across national borders

As the Chair of APCERT, I am proud of the achievements of APCERT because they represent the enormous support and commitment of the teams that are APCERT and the individuals without whose efforts none of this would have been possible.

I look forward to improving further on these achievements in 2004 for the benefit of all APCERT members and the economies we serve.

Graham Ingram
General Manager - AusCERT

CONTENTS

What is APCERT?

Objectives and Scope of Activity

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

APCERT aims to:

- Enhance regional and international cooperation on information security in Asia Pacific,
- 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 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 CSIRTs at the organizational, national and regional levels is essential to the effective and efficient response to computer security incidents, widespread security vulnerabilities and incident coordination throughout the region. One important role of CSIRTs is education and training to raise awareness and encourage best practice. APCERT coordinates the activities with other regional and global organizations, such as 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 activity is 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 and http://www.apnic.net/info/brochure/apnicbroc.pdf.

At present, APCERT is chaired by a team from 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) (formerly CERTCC-KR).

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

APCERT Members

The existing members are the founding members, which consist of 15 CSIRTs from 12 economies across the Asia Pacific region:

(as of 1/31/04)

Team Name	Official Name	ISO Code
AusCERT	Australian Computer Emergency Response Team	AU
BKIS	Back Khoa Internetwork Security Center	VN
CCERT	CERNET Computer Emergency Response Team	CN
CNCERT/CC	National Computer Network Emergency Response Technical Team/ Coordination Center of China	CN
HKCERT/CC	Hong Kong Computer Emergency Response Team Coordination Center	HK
IDCERT	Indonesia Computer Emergency Response Team	ID
JPCERT/CC	Japan Computer Emergency Response Team/Coordination Center	JP
KrCERTCC	Korea Computer Emergency Response Team Coordination Center (formerly CERTCC-KR)	KR
MyCERT	Malaysian Computer Emergency Response Team	MY
PH-CERT	Philippine Computer Emergency Response Team	PH
SecurityMap.net CERT	Securitymap Network Computer Emergency Response Center	KR
SingCERT	Singapore Computer Emergency Response Team	SG
ThaiCERT	Thai Computer Emergency Response Team	TH
TWCERT/CC	Taiwan Computer Emergency Response Team/Coordination Center	TW
TW-CIRC	Taiwan Computer Incident Response Coordination Center	TW
	Total Members	15

Steering Committee (SC)

On 25 February 2003 at the Annual General Member Meeting held in Taipei, the following members had been elected to serve as a member of the Steering Committee (SC) for two years:

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

Working Groups (WG)

During the APSIRC 2003 conference held in Taipei, the following working groups were formed:

1. Accreditation Rule WG

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

2. Training & Communication WG

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

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), TWCERT/CC, AusCERT, HKCERT, CERTCC-KR, and TWCIRC

I. 2003 APCERT Activity Report

APCERT was initially formed with 15 members. Since its establishment, the founding members have been supporting the organization in various ways. The following is a list of the achievement by the members in 2003:

A. Representation to other Regional and International Bodies

1. 10th TF-CSIRT Meeting, 25-26 September 2003, Amsterdam, The Netherlands

JPCERT/CC and KrCERT/CC (formerly CERTCC-KR) introduced APCERT and its activity at the meeting. They managed to obtain a permission to use the TF-CSIRT accreditation scheme as a model for drafting membership accreditation rules for APCERT.
http://www.terena.nl/tech/task-forces/tf-csirt/meeting10/programme.html

2. APEC-TEL CERT Seminar, 25 March 2003, Kuala Lumpur, Malaysia

The seminar was organized by Attorney General of Australia and METI of Japan. The program and logistics were supported by AusCERT and JPCERT/CC, assisted by MyCERT as a local host.

3. APEC-TEL, 24-25 July 2003, Bangkok, Thailand

JPCERT/CC and CNCERT/CC attended this meeting. JPCERT/CC participated at a panel discussion titled, "law-enforcement and the industry collaboration from a CSIRT perspective. "

4. APNIC (regional Internet address registry), 5 November 2003, Brisbane, Australia

AusCERT and JPCERT/CC visited APNIC and introduced APCERT and its activity. They also discussed potential collaboration between APNIC and APCERT. The outcome was to hold a joint BoF on IRT object in APNIC whois database at APRICOT 2004 on 25 February 2004.

B. Conferences and Events

1. APSIRC 2003, 24-25 February 2003, Taipei
http://www.jpcert.or.jp/apsirc2003/

APCERT organizes an annual conference called APSIRC *(Asia Pacific Security Incident Response Coordination Conference)* for CSIRTs and other computer security professionals dealing with security incidents. APSIRC 2003 was held in conjunction with APRICOT conference, hosted by TWCERT/CC and TW-CIRT and sponsored by JPCERT/CC.

Again, APSIRC 2004 is going to be collocated with APRICOT 2004 and to be held from 23 to 25 February 2004. The program and other related information are available at http://www.apcert.org/ and http://www.apricot.net/ . MyCERT is a local host for this event, and JPCERT/CC is providing the funding for the venue.

2. APCERT Information Day, 7 October 2003, Tokyo, Japan

The event was organized in conjunction with the FIRST Technical Colloquium (TC) and hosted by JPCERT/CC. The objective of the Information Day was to introduce APCERT and its activity to the participants of the FIRST TC. AusCERT, CERTCC-KR, MyCERT, TWCERT/CC, and JPCERT/CC presented their updates.

C. Membership

APCERT is a membership-based organization. However, adding a new member is deferred until a draft of membership accreditation rules is approved by the founding members. The rules are in a process of development by the Accreditation Working Group. A proposal is going to be submitted to the Steering Committee as well as to the Members at APSIRC 2004 conference to be held on 24 February 2004 in Kuala Lumpur, Malaysia.

D. Steering Committee (SC) Meetings

1. SC Conference Call

The SC had one telephone conference in 2003.
Date: Tuesday 2 September 2003
Time: 14:00 (GMT+0900) – 17:30

Discussion Points

1. APEC-TEL Meeting – October 2003 in Taipei
2. European Government CERTs (EGC) Meeting – August 2003 in Amsterdam
3. TF-CSIRT Meeting – 25-26 September 2003 in Amsterdam
4. APSIRC 2004 – February 2004, Kuala Lumpur
5. APCERT Information Day – October 2003 in Tokyo
6. APCERT Working Groups
7. Mailing Lists
8. AusAID Training

E. Publications

APNIC kindly offered a space in their newsletter titled *Apster* for introducing APCERT:

a) *Apster*, p.11, Issue 8, January 2004.
http://www.apnic.net/docs/apster/issues/apster8-200401.pdf

b) *Apster*, Issue 9, February 2004. (to be distributed at APSIRC 2004 in Kuala Lumpur)

F. Administrative Matters

1. Mailing Lists

AusCERT developed encrypted mailing list and general mailing list below:

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

2. Website

APCERT website was designed by CERTCC-KR and maintained by JPCERT/CC.
http://www.apcer.org

II. Reports from Working Groups

A. Report from Accreditation Rule WG

Chair – JPCERT/CC
Members – AusCERT, KrCERT/CC (formerly CERTCC-KR), MyCERT, and HKCERT

Background and Objectives

APCERT member teams decided to have its own accreditation scheme to certify member teams in order to be able to handle sensitive information within the members with trust. Although there are existing accreditation criteria for the CSIRTs in Europe, the Asia Pacific region is unique for its wide economical gap and complicated security policy gap. Therefore, APCERT decided to set own criteria for the CSIRTs in the region.

The Accreditation Working Group (WG) was formed last February during APSIRC 2003 conference in Taipei, with a mission to draft an APCERT accreditation scheme and submit it to the Steering Committee for review by APSIRC 2004.

Milestone

25 September 2003: Visited TF-CSIRT Conference for Research about Trusted Introducer

Yurie Ito from JPCERT/CC and Jungu Kang from CERTCC-KR met with Dr. Klaus-Peter Kossakowski from PRESECURE and Dr. Don Stikvoort, the authors of the Trusted Introducer (TI), at TF-CSIRT conference in Amsterdam. At the meeting, both authors gave us a permission to use the TI criteria as a model for APCERT accreditation scheme. The WG recognized the mutual benefits especially as TI has been successfully operated for 2 years. For example, by using their working model, we would be able to expedite a process of drafting our accreditation scheme as well as to void some risks associated with implementing such a scheme. The authors would also benefit if their criteria become a global standard.

Note: Trusted Introducer (TI) is a process and a set of criteria to accredit new CSIRT in order to bring them into "the web of trust". TI is commissioned by TERENA.

3-6 November 2003: Drafted the APCERT Accreditation Rules

Yurie Ito from JPCERT/CC as well as Eric Haril and Mark McPerson from AusCERT got together at the AusCERT office, and wrote an initial draft for the scheme. The process were that 1) list out and define the requirements to become a trusted CSIRT, and 2) evaluate all the check points for each requirement.

November 2003: Invited comments about the Draft from the Members

The WG submitted the draft to APCERT members, requesting comments and suggestions.

Output

1. Draft APCERT Member Requirements
2. Draft APCERT Application Form
3. Draft SC and Sponsor's Check List

III. Activity Reports from APCERT Members

The followings are the reports form fourteen 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

2003 Review

* AusCERT Training

AusCERT training activities during the year included presentation of a variety of security courses including Intrusion Detection Systems, Information Security Management Essentials and Network Monitoring for System Administrators.

http://www.auscert.org.au/training/

* Security Certification

AusCERT has been assisting development of the International Systems Security Professional Certification Scheme (ISSPCS). The ISSPCS is a global and open certification scheme for IT and systems security professionals that addresses the shortfalls of traditional IT security certifications by founding the scheme on essential principles of security. For more information please see:

http://www.isspcs.org/

* Dutch CERT and AusCERT web site

AusCERT helped the Dutch government's national CERT (GOVCERT.NL) develop a web site which was modeled on AusCERT's new web site. AusCERT staff were invited as guests of the Dutch government to attend the web site launch in February.

* AusCERT2003 Conference

The AusCERT2003 Asia Pacific Information Technology Security Conference was held the 11th to the 17th May. Over 520 delegates from eight countries attended. The conference was well supported by sponsors and featured a very wide range of speakers, including the head of the Australian Hi Tech Crime Unit in Canberra, an agent from the FBI, the head of the US CERT in the Department of Homeland Security and many other international and local experts.

http://conference.auscert.org.au/conf2003/

* AusCERT National IT Security Incident Reporting Scheme and Alert Scheme

The Alerting Scheme is a Commonwealth government initiative designed to increase the accessibility of AusCERT security bulletins to the Australian public. The service provides a limited subset of AusCERT's security bulletins to subscribers by email.

The National Information Technology Incident Reporting Scheme was launched on Monday 23rd June, 2003 and provides national incident reporting information free to the public.

Funding for the development of both of these schemes was received from the Commonwealth Government.

http://national.auscert.org.au/

* 2003 Australian Computer Crime Survey

AusCERT, in conjunction with the Australian Federal Police, State police departments and the Commonwealth Attorney General's department conducted the 2003 Australian Computer Crime and Security Survey. Over 200 public and private sector organisations responded to the survey.

http://www.auscert.org.au/crimesurvey/

* AusAID CSIRT Training

The Australian government through its AusAID development program has provided funding for in-country CSIRT training. As part of this program AusCERT has been contracted to provide training for Thailand, Vietnam, the Phillipines, Indonesia and Papua New Guinea. The initial Thailand training was completed in December 2003 with the remaining countries expected to be completed in the first half of 2004.

* ISRC MOU at QUT

AusCERT signed a Memorandum of Understanding with the Information Security Research Centre (ISRC) at the Queensland University of Technology. We expect this MOU to help foster and develop the relationship we have between us and ISRC benefiting both of our groups.

* Conference participation

AusCERT presented or attended numerous security conferences during the year focusing on APCERT and other international initiatives. Conferences and events included the FIRST Annual Conference, FIRST Technical Colloquia (Tokyo), APSIRC, and APEC-TEL. AusCERT assisted with the CERT workshops at APECTEL-28 (Malaysia) and APECTEL-29 (Chinese Taipei). AusCERT also presented and also assisted with the workshops at the FIRST TC in Tokyo.

* FIRST Activities

AusCERT was very pleased to be the sponsor for MyCERT's successful application to FIRST.

Mark McPherson from AusCERT continues to maintain an active role in the FIRST Steering Committee and help represent Asia-Pacifics interests within the global FIRST community.

URL : http://www.auscert.org.au/
Email: auscert@auscert.org.au
Phone: +61 7 3365 4417 (hotline)
Fax: +61 7 3365 7031

B. Report from BKIS

Bach Khoa Internetwork Security Center - Vietnam

Activity report of 2003

In 2003, we always updated our software (BKAV- Bach Khoa antivirus is one of most popular Antivirus software in Vietnam) frequency is about once a week. We updated almost of dangerous viruses in the world, for example: W32.YahaK, W32.LivaA, W32.CodeRed.II, W32.Bugbear.B, W32.SobigE, W32.MsBlaster, W32.Mimail.C, etc, the newest is W32.LoveGate.G virus.

In our statistic, there was more than 90 percent of PC in Vietnam had infected by viruses and the damages go up to tens of billions of VND. In 2003, there are 62 new viruses appear in Vietnam in comparison with 30 new viruses in 2002.

Among of viruses there are 15 kinds which cause of wide spread attacking, almost attacking concentrated from June to December. Some typical cases are: W32.Swen, W32.Welchia, W32.Sobig.F, W32.MsBlaster, W32.Opaserv, W32.Bugbear, etc. As soon as those viruses appear we updated our Antivirus software to kill those viruses immediately and send the warning to all members in my mailing list and to public media (Radio, Televisions, and newspapers).

The activities of hacker are much diversified, in 2003. They attacked each other also attacked domestic websites. Some hacker's meetings had been organized, in that, hackers present to attack and modify some websites even some sensitive websites.

We replied mount to thousands of email and telephone call from victims of viruses and hackers. There are approximate 1 million times of downloading free our Antivirus software at website: http://www.bkav.com.vn

Ministry of Public Security is going to establish the Cyber Crime Unit to prevent and to handle cyber crime in Vietnam. On 24 October, 2003 a first conference about "The solution to prevent cyber crime" had organize. We participated and had ideas to help the police to plan in the future.

In the last of this year (in October and November), the network security problem really has interested by government, business and economic organization in Vietnam. The public media notify this problem continuously. We have been helped to raise the knowledge of people in Vietnam to know about security filed.

In this year, we also participated in the Cyber Crime Specialized Course at International Law Academy (ILEA) in Bangkok, Thailand. In this course we were had introduced some technical which use by hacker and criminal and we also knew about situation of security in some Asian country. Besides, we visited some government offices in Washington DC and New York to learn about network security in there.

We took part some conferences about Network Security, e-commerce, e-government... and in those conferences, the Security problems, which has brought out by us, got many attention from others.

We also arranged some training courses about Antivirus and Security for students, who were interesting in this field. There were many student take part our courses and most of them still continue studying and working with us. In the future we will take part some courses for official to introduce and provide to them the basic knowledge about security in office.

In this year, we were working actively prepare to establish the VietCERT organization. The concrete work is: to plan, to prepare material facilities, to setup framework of organization... We hope that in 2004 VietCERT will operate formally.

Year 2003 is a really busy year of us but we were very happy because of the security field has attended of people and government in Vietnam.

C. Report from CERTCC-KR (KrCERT/CC)

Computer Emergency Response Team Coordination Center - Korea

Introduction

CERTCC-KR is a department of KISA (Korea Information Security Agency) intended for an expert group leading the present and future of the information security. CERTCC-KR works for the promotion of information security through the following tasks as, mainly technology development, information security handling, thus contributing to secure and safe flow of information in the cyberspace.

2003 Activities

1. Incident Reports and Domestic Computer Virus Occurrence statistics in 2003

In 2003 total number of incidents reports we got was 26,179 by email and proportion of the reports related to home users were 73% and they were mainly related to slammer, open/proxy spam relay (especially proxy spam relay of personnel computer), worms using MS vulnerabilities, and etc.

Domestic computer virus occurrence statistics is 85,023 (This number came from major anti-virus companies in Korea and CERTCC-KR together). In the damage report from virus, we found 108 types of new virus in 2003 and each proportions of Internet worm, Trojan, and Virus were 63%, 28%, and 6%. Thus, we made worm and virus alert 48 times and publish 73 advisories, 6 technical documents, and 4 incidents notes.

Above two statistics (Incident Reports and Domestic Computer Virus Occurrence statistics) are not duplicate figures.

2. New Project

a) Establishing Korea Internet Security Center:
As we have seen the current attacks, Hacking, Virus, and Spam Techniques are integrated into one worm. Also, a worm that exploits multiple vulnerabilities is common. However, our previous incidents response system was very passive to reduce the damage from the attacks. To prevent incidents effectively, we needed to detect, analyze, and announce the related information of incidents actively. That's why we developed traffic monitoring system and real-time information sharing system. In the near future, we expect early detection, rapid prevention, and assurance of cooperation incidents response system.
Briefly explaining the system, every incident related Information collected is stored in the database as a name of Traffic Statistics at critical nodes (bps/pps), Attack Type Statistics by IDSs, Agent Event information, Correlation Analysis information, and Major DNS servers and Web servers connection status. All stored information will be the input to expert system to aid timely & accurate decision.

b) Providing web service to check the vulnerabilities of web:
From Oct. 24, in our web site (https://www.certcc.or.kr/vultest/), everyone can access and check if their operating web sites are vulnerable. In 2003 we got application for the checking web and provided vulnerable checking service to 800 sites and got 40 thanks mails.

2004 Plan

First of all, we will change the name of CERTCC-KR to KrCERT/CC from 2004.

We are planning to provide the information we collect from the monitoring system to the public in Korea by web sites for incident analysis and rapid response.

In order to share information in real-time, we will monitor Internet 24/7 and escalate the accuracy of system to reduce false positive. We will share information with other international CSIRTs as well as the CONCERT (Consortium of CERTs in Korea: 210 members).

For international cooperation, we will initialize the IODEF Project and the traffic monitoring information sharing.

URL: http://www.certcc.or.kr
E-mail: cert@certcc.or.kr
Phone: +82-2-405-5526

D. Report from CCERT

CERNET Computer Emergency Response Team (China)

Incidents response

In 2003, CCERT has received 28,424 incidents reports, more than twice of those of 2002. Taxonomy statistics of incidents reports are shown in figure 1. More than 62% of these incidents were related to worms, which gave rise to most serious Internet incidents.

Figure 1. Taxonomy statistics

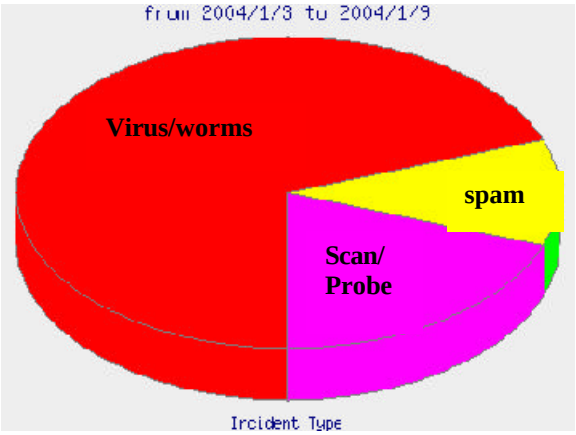


Table 1. Taxonomy statistics

Order	Taxonomy	Percent
1	Virus/Worm	62.87%
2	Spam	18.49%
3	Scan/Probe	17.36%
4	DoS	0.15%
5	Intrusion	0.12%
6	Unknown	0.46%

More than 70% of these incident reports came from Japan and USA. The reports from China domestic account for 8.1%. 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

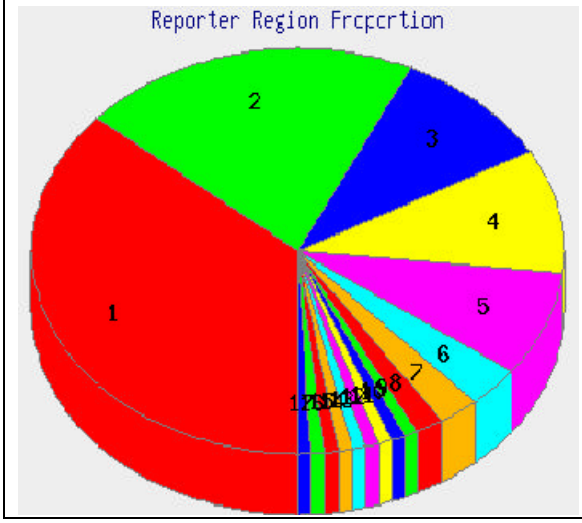


Table 2

Order	Country	Percent
1	Japan	52.0%
2	USA	19.8%
3	unknown	12.5%
4	Israel	9.2%
5	China	8.1%
6	Singapore	0.9%
7	Canada	0.7%
8	France	0.6%
9	Brazil	0.6%
10	South Korea	0.3%

As responses to the most serious incidents, CCERT has published 20 advisories to the users of CERNET in 2003. The top 10 of the most serious incidents in 2003 are listed as follows:

2003/01/25 Slammer.Worm
2003/03/08 DvlDr32/Deloder/W32.HLLW.Deloder
2003/03/19 CodeRed@F
2003/05/04 A large number of computers were installed with backdoors
2003/06/10 DDOS Attack against some BBS Servers
2003/06/30 Randex.C.worm
2003/08/12 Blaster.Worm
2003/08/19 Nachi/Welchina
2003/08/16 SoBig@F
2003/09/10 Worm_Swen.A

Projects

1. *Open signature database for IDSes*.

To update IDS systems in time when new worms or viruses break out, CCERT developed an open and shared signature database for IDSes. Now the signature database contains more than 1000 signatures for common attacks, virus, and worms. For each signature, there is a detailed description (in Chinese), protocol header, content payload, referenced URL, and a defensive solution.
Detection rules for IDS can be constructed according to these signatures. Now the syntax of the rule is snort-compatible. If the members of CCERT download and install a client side script, their IDS can be updated automatically with the signature database.

2. Distributed WHOIS database for incident response

The accuracy of WHOIS information is important for most CSIRTs, but most WHOIS information is maintained centrally, which leads to the inaccuracy and delay of information update. This project aims to develop a distributed WHOIS database which is updated and maintained by members of CCERT and shared by administrators of campus networks. The schema of the information will be extended to cover the needs of incident information. The database will be implemented with web service technology. The project will be finished in the end of 2004.

3. Incident Object description and Exchange Format.

To facilitate the information exchange and information sharing, this project aims to implement the IODEF specification. Localization, specially the coding of Chinese character set, is to be considered as well as digital signature. Now this project has just begun.

Training and seminars

1. *Network security overview,* a four-day course for administrators for northeast CERNET. More than 40 network administrators attended the course. 2003/01/9-01/12, Shenyang, Liaoning Prov.
2. *Security threats to campus networks and solutions,* a half-day seminar during the annual conference of CERNET North China. More than 50 administrators from universities and colleges attended the seminar. 2003/08/12, Beijing.
3. *Common security problems in campus networks recently and their solutions,* a half-day seminar via CERNET video conference. More than 30 people from top universities attended via network. 2003/05/16, Beijing.
4. *Worm incidents and response: case studies,* a half-day seminar during CERNET 11th Annual conference. 2003/10/17, Zhengzhou, Henan Prov..

Presentations

1. *Network worms and CCERT response,* Cisco Annual Conference 2003, 2003/10/31, Beijing.
2. *Spam and anti-spam technologies,* User conference of Internet Society of China, 2003/12/07, Beijing.
3. *A DNS-based solution for worm control,* XFocus Summit Conference, 2003/12/26, Beijing.

Publications

In 2003, members of CCERT translated and published several excellent books on incident response into Chinese:

1. E.Eugene Schultz, Russell Shumway, *Incident response: a strategic guide to handling system and network security breaches*, New Riders
2. Mike Schiffman, etc. *Hacker's Challenge 2: Test your network security & forensic skills,* McGraw Hill publishing.
3. Warren G. Kruse II, Jay G. Heiser. *Computer Forensics : incident response essentials* , Addison Wesley.
4. Eric Maiwald, William Siegleim. *Security Plan and Disaster recovery.* McGraw-Hill.

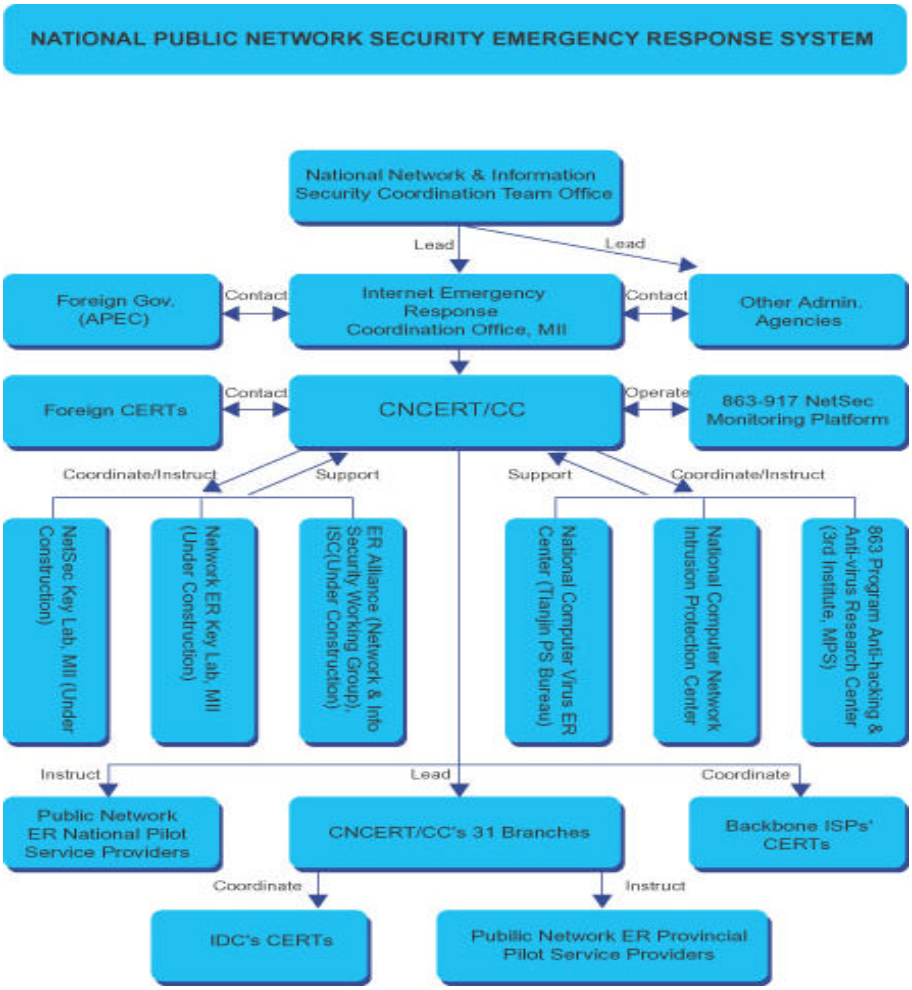
E. Report from CNCERT/CC

National Computer Network Emergency Response Technical Team / Coordination Center of China

CNCERT/CC ANNUAL REPORT 2003

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.

CNCERT/CC works as the coordination center of the "National Public Network Security Emergency Response System" of P.R.China shown as follows:



Incident Response

In 2003, there are lots of serious incidents such as SQL SLAMMER, Deloader, MSBlaster, which gave CNCERT/CC great pressure to handle.

1. Selected Cases

SQL Slammer: erupted in Jan. 2003 and made a highly severe impact on the global network resulting in the network broken down in large scale. The National Computer Network Emergency Response System with the core of CNCERT/CC worked together to accomplish timely detection, exact identification and fast recovery with the event. This incident was made to be under control effectively within a single day in China.

Deloder: erupted in Mar. 2003 and blocked quite a few network area in China badly. It's more difficult to defend against this worm as it exploits the vulnerability of weak password instead of technical flaw to launch attack. Through the National Computer Network Emergency Response System, CNCERT/CC discovered and analyzed the

worm in time, and contained it spreading effectively and efficiently together with its partners. The whole network was kept away from severe impact eventually.

Blaster/Blaster Remove: erupted in Aug. 2003 with an enormous infection. The network speed slowed down in some regions and a lot of PC users were infected. CNCERT/CC always kept in touch with foreign CERTs and domestic CERTs during the handling process, and corresponded each other, and opened a special news area at the website for the first time and provided users with technical support services.

DOS: CNCERT/CC tackled many DOS attack cases involving governmental portals, large ISPs and important websites in 2003. During the handling processes, CNCERT/CC got to track and locate attack sources with the close cooperation with ISPs nationwide.

Web Defacement: CNCERT/CC discovered many cases about web defacement in 2003, and contacted local related agencies to inform users and helped to solve the problem in time.

Web Fraud: CNCERT/CC received many reports on web fraud event, e. hackers intruded in victim's machines and made fraud to users of banks or commercial sites. CNCERT/CC quickly solved all these problems with the cooperation from related CERTs.

Others: CNCERT/CC received 13,295 reports on general security events in 2003 and handled them according to international rules. In 2003, CNCERT/CC detected around one million times of attack attempts targeted to Chinese networked computers on Internet via 863-917 network security monitoring platform.

2. Incident Reports Statistics

In 2003, CNCERT/CC received 13,295 incident reports on general security events and indicated an obvious leap compared with the number of 1761 in 2002. Most of reports were about intrusion activities from outside of Chinese territory. The following two figures show the data in detail.

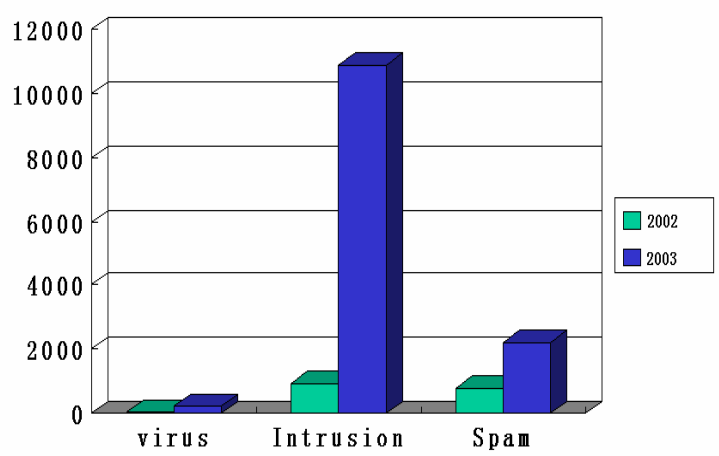


Figure1: Data Comparison Between 2002 and 2003

Incidents								Other
	Different type of incidents							Consultation
	Virus		Intrusion		Spam		total	
Month	Dom.	abroad	Dom.	Abroad	Dom.	Abroad		
Jan		2		342	2	129	475	13
Feb	10	2		482		172	666	5
Mar	15	2	1	724		135	862	7
Apr	4	1		383		156	540	2
May	3	11	5	980	2	168	1169	9
Jun	1	50	3	753		137	944	13
Jul	6	35	3	881	3	173	1101	21
Aug	16	11	4	1509	1	153	1694	3
Sep	20			1542		277	1839	2
Oct	10		1	1067	5	248	1331	15
Nov	9	3	2	1032	2	160	1208	23
Dec	3	6	1	1178	2	276	1466	3
total	97	123	20	10873	17	2184	13295	116

Figure2: Statistics of Incident Reports 2003

Projects

1. 863-917 NetSec Monitoring Platform

863-917 NetSec Monitoring Platform is a system used for network traffic monitoring and analyzing so that early response toward severe network incidents might be taken.

2. Resource Base on Vulnerabilities, Patches, Defending Tools

In order to provide Chinese network users with trusted information on vulnerabilities, patches and defending tools, we started to collect, translate and process these information in the beginning of 2003.

Media Exposure

1. Published 33 articles or reports at CNCERT/CC's website.
2. Issued a handbook on computer emergency response jointly with China Information World. (http://www.ciw.com.cn)
3. Translated materials on anti-cybercrime nearly one million of Chinese characters.

Establishment of CNCERT/CC's 31 Branches

The former national public network security emergency response system of China is a tree structure with CNCERT/CC as the root and CERTs of backbone ISPs as leaves. In order to speed up the progress of emergency response work, since 2003, we have established 31 branches of CNCERT/CC covering 31 provinces in mainland of China to form a network structure based ER system which had solved the old problem that ER work was lack of localized support, and not able to run high effectively.

Conferences

1. Cybercrime Legislation and Enforcement Capacity Building, July 21-25 2003, Bangkok, Thailand

CNCERT/CC and the Internet Emergency Response Coordination Office of MII participated in the "Cybercrime Legislation and Enforcement Capacity Building" conference hosted by APEC. We delivered a presentation on "Anti-Cybercrime Depend Upon The Community Working Together".

2. APT Seminar on Network Security Management and the Positive Use of Internet, August 18-20 2003, Kuala Lumpur, Malaysia

   One representative from CNCERT/CC attended the "APT Seminar on Network Security Management and the Positive Use of Internet" conference and delivered a presentation on "Introduction about Chinese Network Security & CNCERT/CC".

3. 2nd Asia Cybercrime Summit, November 5-6 2003, Hong Kong, China

   CNCERT/CC participated in the "2nd Asia Cybercrime Summit" and delivered a presentation on "Fighting with Large-Scale Internet Incidents".

2004 Plan

1. Consolidate the cooperation among each units of National Public Network Security Emergency Response System of China, including related projects on incidents classification, description and information exchanging
2. Stress on training and education
3. Enhance the cooperation with other international CERTs and IT security organizations
4. Continue the construction of 863-917 NetSec Monitoring Platform and resource base
5. Relevant research

URL: http://www.cert.org.cn/
Email: cncert@cert.org.cn
Phone: +8610 82990999, 82991000
Fax: +8610 82990375

F. Report from HKCERT

Hong Kong Computer Emergency Response Team Coordination Center

The 2003 is a tough but also a fruitful year for HKCERT.

The incident response of the region has been greatly strengthened in 2003. HKCERT is one of the CERT teams in the Asia Pacific to collaborate the APCERT forum and was elected as one of the Steering Committee member. HKCERT had also applied to the FIRST with SingCERT as our sponsor. The application was admitted in June. HKCERT is furthering more close relationship with CERT teams in the region and had just signed a memorandum of understanding with CNCERT to foster information exchange and development in the future.

The series of large-scale attacks accounted to the Blaster, Welchia and Sobig.F worms had created tremendous impact to HKCERT incident response. In August 2003, HKCERT received over 1900 incident reports related to these worms. The incidents had drained our resources to our limits. We have evaluated the strategy of the contingency plan to handle the capacity of a similar attack in the future. From 1-Dec-2003 to 15-Dec-2003, HKCERT had received over 3000 incident reports. Over 2500 are from virus/worms incidents and over 400 belongs to security incidents.

By the end of 2003, Hong Kong security concern was on the fraudulent online business websites. There were reports of deception in which criminals copied the corporate web pages of the Hong Kong Jockey Club and several financial

institutions in Hong Kong. The recent vulnerability of Microsoft Internet Explorer displaying incorrect address of crafted URL added to the severity of the problem. HKCERT is closely monitoring the status of the problem from the security awareness education and technical guideline perspective. We organized a public seminar in December and invited representatives from regulatory, banking industry and law enforcement to share the experience and best practice with the general public to combat the deception.

Locally HKCERT had put effort in developing more integrated network web for incident response. HKCERT had formed a closed network with government and police called the CONNCECT to exchange information and analysis of information security incidents. The communication structure is expanding to ISP and will further be extended to financial sectors and the critical infrastructures.

Besides incident response and information dissemination, HKCERT put effort in promoting the information security awareness and capabilities of the industry. In November 2003, Information Security Summit, a first local conference co-organized by HKCERT, HK Productivity Council and other local information security associations was held with success.

With a good foundation built up in 2003, HKCERT is looking forward to more collaboration with other regional CERT teams in 2004.

URL: www.hkcert.ort
Email: hkcert@hkcert.org
Phone: (852) 8105 6060
Fax: (852) 8105 9760

G. Report from JPCERT/CC

Japan Computer Emergency Response Team/Coordination Center

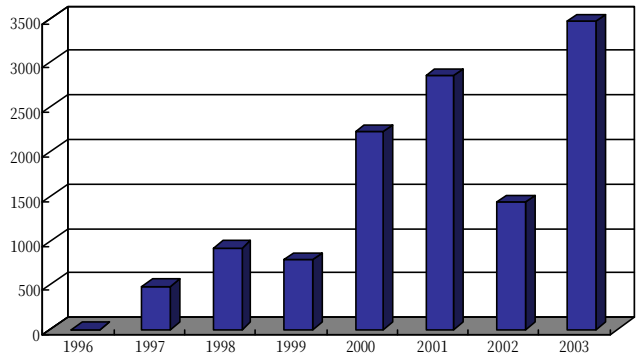
JPCERT/CC is a first CSIRT (Computer Emergency Response Team) established in Japan. It is an independent non-profit organization, acting as a national point of contact for the CSIRTs in Japan and worldwide. Since its inception in 1992, the center has been gathering computer incident and vulnerability 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 2003, JPCERT/CC issued 3,470 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 3,470 tickets, 3,224 tickets were related to probe, scan, and attempts that did not result in serious damages. The following figures include spam mail which amounted to 14,227 emails during the year.

	1st Qtr	2nd Qtr	3rd Qtr	4th Qtr	Total
Tickets Issued	708	1080	1030	652	**3,470**
Spam	2510	3224	3403	5090	**14,227**

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.

The list below contains probe/scan reports with the port numbers received during the last quarter in 2003:

According to the reports, Port number 135 seemed to be the major target during the last quarter:
(2003.10 – 12)

Port Number	Tickets	Port Number	Tickets
135 (epmap)	418 tickets	445 (microsoft-ds)	260 tickets
21 (ftp)	252	1080 (socks)	231
3389	215	139 (netbios-ssn)	209
80 (http)	210	17300	194
1434 (ms-sql-m)	188	137 (netbios-ns)	183
443 (https)	169	1433 (ms-sql-s)	167
901 (smpnameres)	126	8080	120
3128	119	25 (smtp)	115
icmp	111	24099	94
138 (netbios-dgm)	94	4899 (radmin-port)	92
554 (rtsp)	89	27374	87
111 (sunrpc)	84	1026	80

Source of Incident Reports

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

ISO Code	1st Qtr	2nd Qtr	3rd Qtr	4th Qtr	Total
.au	247	470	429	247	1393
.jp	251	357	403	207	1218
.net	97	106	113	116	432
.fr	53	41	44	33	171

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 2003 are listed below:

- JPNIC-JPCERT/CC Security Seminar - a series of 4 security seminars jointly organized with JPNIC (7-July, 12-Sept, 5-Nov, 2003, and 4 Feb 2004)
- FIRST Technical Colloquium in Tokyo – hosted jointly by JPCERT/CC and Internet Initiative Japan (6-Oct 2003)
- APCERT Information Day – held in conjunction with the FIRST TC in Tokyo (7-Oct 2003)
- InternetWeek 2003 in Yokohama – one day security track jointly organized with Japan Network Security Association (JNSA) (3-Dec 2003)

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 is 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.
http://jvn.doi.ics.keio.ac.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 meeting called, APSIRC since 2001. The next APSIRC will be held in February 2004 in Kuala Lumpur, Malaysia.

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.

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 during the 58th IETF held on 13 November 2003.

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.

In summary, 2003 was characterized as a year of "challenges and progress." JPCERT/CC was re-established as an independent legal entity in March. JPCERT/CC doubled the staff members and relocated the office to accommodate the increased staff and the activities. New projects were initiated and the relations with other domestic and international CSIRTs as well as other major players in the industry were strengthened.

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

H. Report from MyCERT

Malaysian Computer Emergency Response Team

The year 2003 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 2003 are listed as below:

1. Organized Seminars/Workshops

In early year 2003, MyCERT was entrusted to play an active role and responsibility in co-hosting the APCERT Workshop during the APECTEL 27th Meeting on 22 – 23 March 2003 at Kuala Lumpur, Malaysia. This workshop was successfully held with overwhelming response from audience which comprised of APCERT members and the objective of the workshop was successfully accomplished.

With regards to the above workshop, MyCERT had proposed a follow-up action to the Government of Malaysia through the Ministry of Energy, Communications and Multimedia (MECM) to continuously support CERT development programs in Malaysia and at International front.

2. Attended Seminars/Conferences/Meetings

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

- In Feb 24 – 25 2003, two representatives from MyCERT attended the APSIRC held in Taipei. In this Conference, MyCERT's representative had presented a paper titled "Incidents & Vulnerability trends in Asia Pacific".
- On 22-23 March 2003, seven representatives from MyCERT attended the APCERT Workshop in Kuala Lumpur, Malaysia. Two papers were presented by MyCERT's representatives titled "The Malaysian CERT Experience – The Online Environment" and "Managing National Cyber Threats".
- In June 22 – 27 2003, two representatives from MyCERT attended the FIRST Conference in Ottawa, Canada.
- Two representatives from MyCERT attended the FIRST Technical Colloquium on 6 – 7 October 2003 in Tokyo and then attended the APCERT Information Day on 7 October 2003 at the same venue. MyCERT's representative presented a SPAM Survey paper during the APCERT Information Day.

3. Elected as FIRST Membership

In May 2003, MyCERT was officially elected as a member of FIRST based on the successful evaluation of MyCERT's operations, achievements and the role it plays in as a National CERT. The thorough evaluation on MyCERT was conducted by AUSCERT, respectively.

4. Trainings

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.

5. Initiatives to Establish Mutual Collaborations

MyCERT had also initiated close ties between MyCERT and the Abuse Departments of local ISPs for effective and speed handlings of incidents in the country.

6. Other Noteworthy Activities

MyCERT had played a big role in fighting/eradicating some major incidents/outbreaks in the country and assisted organizations terribly affected by the Blaster outbreak in July 2003, Nachi and W32.Sobig.F outbreaks in August 2003. Other notable incidents include intrusions, hack attempts and spammings. A total of 3,536 incidents were reported to MyCERT till November 30 2003.

MyCERT had also produced security related documents, ie advisories, alerts, statistics, quarterly summaries and guides for the Internet society of Malaysia, available widely on local newspapers, MyCERT's websites and MyCERT's mailing lists. For year 2003, seven Advisories, two Alerts, four Quarterly Summary and two Guides were produced. MyCERT's comments and views on current security issues were also published widely in local newspapers/magazines.

In year 2003, the MyCERT Discussion Forum became active with overwhelming response from subscribers to actively participate in the forum, discussing current issues in the field of ICT security.

URL : http://www.niser.org.my/
Email: info@niser.org.my
Phone: +60 3 8996 1901
Fax: +60 3 8996 0827

I. Report from PH-CERT

Philippine Computer Emergency Response Team

1. Brief Introduction

Organizational Overview: The Philippine Computer Emergency Response Team (PH-CERT) is a non-profit organization that aims to provide reliable and trusted point of contact for computers, Internet and other information technology related emergencies.

Mission Statement: To build a knowledge base of computers, Internet and other information technology related security threats and emergencies through coordination with other Philippine-based Incident Response Teams.

2. Goals and Objectives

- Provide support to their constituents in an advocate or advisory capacity.
- Serve as the focal point for reporting computer security vulnerabilities and will provide coordinated support in response to such reports.
- Generate technical analysis reports pertaining to malicious code.
- Provide information on upcoming technology that may pose security threats.
- Interact with both internal and external parties to develop and maintain trust relationships.

Specific Objectives to support these goals include:

- Provide training to promote security awareness and improve expertise among its members and constituents.
- Provide announcements to aid in the dissemination of information on protective measures to take against existing or upcoming security threats.

- Provide guidelines on the effective use and combination of security tools for incident detection and prevention.
- Establish collaborative relationships with other entities such as law enforcement, service providers and the telephone company.

3. 2003 Highlights

2003 has been an 'advocacy' year for Ph-CERT less activity marked the fronts of incident response and more for advocacy. PH-CERT has been busy contributing to the creation of a comprehensive Anti-Cybercrime Bill and is actively participating in the Philippines highest I.T. Public/Private Sector policy making body the Information Technology and eCommerce Council (ITECC) chaired by the President of the Philippines and Managed by the Executive Director who is concurrently the Undersecretary for Information and Communications Technology for our Department of Transportation and Communication (The Philippines has no Department of ICT).

PH-CERT servers as public sector co-chair for two subcommittees in two different committees. These are the ICT Security Subcommittee under the Information Infrastructure Committee and the Information Security and Privacy Subcommittee under the Legal and Regulatory Committee. PH-CERT had also just concluded its first ever National Information Security Survey which will come out by January next Year. The survey was patterned after the US CSI/FBI Cybersecurity Survey. PH-CERT had also signed a Memorandum of Agreement with the Country's Law Enforcement Agencies to Provide FREE Basic Information Security training for its related Cybercrime departments.

PH-CERT is also assisting ITECC in coming out with a National Computer Emergency Response Team of the Government.

URL : http://www.ph-cert.org
Email: info@ph-cert.org

J. Report from SecurityMap.Net

SecurityMap.Net (South Korea)

Introduction

SecurityMap.Net CERT is a non-profit and non-government organization intended for improving incident response activities in Korea. It's comprised of many security professionals from security and IT industry area. All activities and projects are done by volunteer membership basis until now. We are mainly dedicated to provide security information to the public and to automate incident response processes.

2003 Activities

We announced best security practice almost once a month and operated three projects

1. IAM(Internet Attack Map) Project: It is for automating incident response process for CSIRT work. It collects incident report preprocessed from various sites through snort IDS and Firewall log and then automate the response process. It deals with more or less 1,000 incidents a month automatically. By the result of this project, we can gain more response rate from major ISP in Korea, and we can provide real-time incident response activities.

2. VMS(Vulnerability Management Service) Project: It is for announcing new vulnerability to the public. It's mainly based on CVE database.

3. Honeynet project: Let the public to know how to analyze an incident and how to deal with an incident. We announced some real incident analysis case and wrote a book on “incident analysis and response”.

2004 Plan

We are planning to extend IAM project by opening the IAM system to the public in Korea, and preparing some training courses for incident analysis and response.

URL: http://www.securitymap.net
Email: info@securitymap.net
Phone: +82-16-324-3589

K. Report from SingCERT

Singapore Computer Emergency Response Team

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 organizes frequent seminars covering a wide range of security topics.

Incident Trend and Highlights for year 2003

SingCERT received over 300 incidents for the year 2003. Not surprisingly probes and attempts category has the highest number of reports. SingCERT worked closely with our Internet Service Providers (ISP) to track down the persistent source of attacks, send them warnings and even block accounts of those repeated offenders.

Besides probes and unauthorized attempts, we see a surge in virus infection in February 03 due to the Slammer Worm. SingCERT provided relevant advisories on its website and pointers to users on how to detect and remove the virus. In August, we see another peak due to the Blaster and Welchia Worms. Users were advised to patch their Windows and instructions on how to carry out the Windows Update and how to enable the firewall in Windows XP were published on the SingCERT website for users’ reference.

SingCERT, however, only received a few reports on SoBig Worm and mostly from users who are not infected with the worm but their email addresses appeared on the FROM field. Advised users to PGP sign their outbound emails to ensure authenticity and practice caution when disclosing email address on the internet.

Website defacement activities peaked in October and November. Most of the websites were co-hosted by Service Providers. SingCERT contacted the affected Service Providers, informed them of the attacks, provided assistance on how to recover the system, recommended that sites take extra precaution to harden systems and patch the vulnerabilities as soon as possible. Most hacked systems were Linux and Windows machines.

SingCERT Security Awareness Activities

SingCERT organizes security seminars and workshops on a regular basis to raise the general level of security awareness in the industry and the general public and to share with our constituency the latest developments and technologies in the field of security. The following is a list of topics conducted in year 2003 with industry collaboration:

-Forum on " Information Warfare - The Home Front ", Jan 17, 2003
-Policies and Strategies to consider when planning for Enterprise Protection, Jan 20, 2003
-Internet Level Anti-virus Techniques, May 20, 2003
-The Mystery of Software Protection, July 10, 2003
-Instant Security in a Day by 'Privatising' your Web, July 10, 2003
-Issues and Risks that Arise from Internet Contents Arriving at Users' Desktop, Sep 26, 2003
-All about Real-time (All the Time) Network Awareness, Nov 10, 2003
-Security Incident Response: The common failures your company can avoid, Nov 12, 2003

SingCERT Project Highlights

1. ASEAN Telecommunications and Information Technology Ministers Meeting (TELMIN)

At the conclusion of the Third ASEAN Telecommunications and Information Technology Ministers Meeting held in Singapore 18-19 September 2003, the ASEAN ICT Ministers committed to initiatives and agreed to enhance regional cooperation in cybersecurity.

SingCERT has been called upon to provide inputs and recommendations on how to provide assistance to ASEAN countries with no computer incident response functions to develop and operationalise their national Computer Emergency Response Teams (CERT).

SingCERT has highlighted that the TEMIN cybersecurity initiatives coincide with APCERT's objectives. It has been agreed that capacity building activities should leverage on fora such as APCERT, APT and APEC. SingCERT is in the process of drafting the action plan.

2. Anti-Spam Programme

SingCERT is working on an anti-spam programme in collaboration with the internet service providers. The objectives of the programme are to raise the awareness among consumers and the industry on the Spam issues and to provide recommendations or solutions on how to combat the spamming issue. The objectives also include the creation of a forum for Internet users, administrators, marketers, anti-spam businesses and spam activists and allow them to collaborate and develop strategies that encourage responsible email marketing.

SingCERT will host the anti-spam website which will contain general information about Spam and its related issues. You will also find useful resources on how to combat spam and an interactive forum for Internet users, administrators, marketers, anti-spam businesses and spam activists to interact, collaborate and develop strategies that encourage responsible email marketing.
The website will be available by January 2004.

3. Incident Response Tracking System (IRTS)

SingCERT has developed an in-house web-based incident response system to ensure that all incidents are properly recorded and tracked. The system assigns ticket numbers randomly, performs whois check on request, records IP ranges and ownerships to a database and has a build-in search engine for incident tracking. The system is currently in the pilot phase. More features and enhancements will be included in the next phase.

4. FIRST Conference 2005

The FIRST SC has voted to host the FIRST Conference 2005 in Singapore. SingCERT has met up with the FIRST Conference organizer in September 2003 and has discussed with her the possible venues and themes for the conference. SingCERT will work with the organizer in providing recommendations and contacts in the coming months to ensure that the conference is a success.

URL: http://www.singcert.org.sg/

Email: cert@singcert.org.sg
Phone: +65-6211 0911 (hotline)
Fax: +65-6211 2105

L. Report from ThaiCERT

Thai Computer Emergency Response Team

Year 2003 Review and Comparative Incident Statistics

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

Year	2001	2002	2003
Number of Incidents*	150	355	386

* Incidents originated from government sector sites.

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

Summary and Analysis

It can be seen that the number of spam mail incidents had decreased by about a factorof 6 from the year 2002. This could be because ThaiCERT has continued to inform and assist mail server administrators in their spam problems. Also, it could also be that the community has now become familiar with spam mail and thus does not perceive it as a worthwhile problem to report to ThaiCERT. However, ThaiCERT expect an increasing trend of spam mail, both originating from viruses and spammers, in the future.

It can also be seen that there had been a two-fold increase of the port scan incidents. A likely reason for this is that there are more scanning and probing tools available and they are very easy to download and use. Moreover, there are many cases of port scan originating from machines infected with viruses or from those that are compromised.

From the data in the table, the number of cases in virus/worm/Trojan had increased by almost three times from the year 2002. There have been an increasing number of viruses every year. Their replication methods have been also more diversified and thus resulted in more damage to the Internet community.

Notable Virus Incident Response

MS SQL Worm (Slammer)

From the ThaiCERT monitoring process, it was found that SQL Slammer worm was most active from 12:30pm to 05:30am (GMT+7) on Jan 25th, 2003. This causes some ISPs in Thailand not to be able to provide internet access to their customers for a period of time around 5 hours in the day. This also results in ThaiCERT inability to provide advisory through the Internet to some part of the Thai community. However, assistance and advisory was given to the ISPs through telephone and fax and the worm was filtered by firewalls and routers.

The lesson learned from this major incident is that cooperation with APCERT and other means of communication such as telephone or fax should be established in advance so that a similar incident can be prevented and responded more effectively in the future.

Blaster/Nachi

This type of virus causes similar, albeit less, damage to Slammer. Receiving the report about its existence, ThaiCERT promptly issued an advisory through the mailing list and website. This helped reduce the damage potential and the actual damage was much less than that from the slammer case.

ThaiCERT's Notable Activities in 2003

1. 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 seminar and training courses offered by ThaiCERT and also to update ThaiCERT activities.
- ThaiCERT-advisory Mailing List: To announce CERT/CC Advisory (translated into Thai).
- ThaiCERT-virus-alert Mailing List: To announce virus alerts (those with great damage potential).

The mailing list service was commenced in March 2003. As of now (February 11th, 2004), the number of members in the list are as follows.

- ThaiCERT-news Mailing List: about 5500 members
- ThaiCERT-advisory Mailing List: about 6000 members
- ThaiCERT-virus-alert Mailing List: about 7000 members

2. Thai IT-Security Fair 2003

The purpose of the Thai IT-Security Fair is to provide and distribute IT security knowledge, understanding and awareness in Thailand. The first Thai IT-Security Fair was in the year 2001. ThaiCERT offered two courses in wireless security and virus awareness in the Fair. The Fair was held on October 8th, 2003.

3. ThaiCERT Training, sponsored by AusCERT

ThaiCERT was given assistance according to the AusAID CERT Training initiative where an AusCERT delegation visited Thailand to provide a training course in CSIRT operations during November 31st to December 4th, 2003. The AusCERT delegation consists of Eric Halil and Jamie Gillespie.

ThaiCERT receives many benefits from this training as it can use the knowledge gain to improve its structure, services, and operations to better suit the needs of the Internet community. An importance of cooperation among the Asia-Pacific region CSIRTs was also pointed out and very much understood and accepted.

4. APCERT activity/Seminar

In the year 2003, ThaiCERT participated in two of the APCERT conferences which are
- March 22-24 2003, APCERT SC meeting, KL Malaysia
- October 4-6 2003, APECTEL 28, Chinese Taipei

This also helps ThaiCERT to realize the importance and necessity of cooperation among CSIRTs in the region.

URL: http://thaicert.nectec.or.th/

M. Report from TWCERT/CC

Taiwan Computer Emergency Response Team /Coordination Center

2003 Review

* TWCERT/CC Training

TWCERT/CC training activities during the year as below:
- Network security education courses for Chiayi City academic network center
- TWCERT/CC network security certification courses (http://www.auscert.org.au/training/)
- Network security E-learning education courses

* 2003 Conference participation

TWCERT/CC presented or attended numerous security conferences during the year
- APSIRC 2003 (Feb. 24-25, Taipei)
- APECTEL 27th CERT Workshop (Mar.22-23, Malaysia)
- FIRST 2003 15th Annual Computer Security Incident Handling Conference (June 22-27, Ottawa)
- APECTEL 28th CERT Workshop (Oct. 4-10, Taipei)
- 2003 FIRST Technical Colloquium (Oct.6-7, Tokyo)
- APCERT Information Day (Oct. 7, Tokyo)

* TWCERT/CC 2003 symposium

- Training courses in government elementary organizations
- 4th symposium of Internet: Information Law and society
- DNS security symposium

* TWCERT/CC Regional IT Security Incident Reporting Scheme and Alert Scheme

- Deploy and operate the mechanism of Taiwan Security Cooperative Defense
- Investigate and deploy the protection mechanism for the 3rd layer DNS server security
- Plan and investigate denial of service attacks on the high speed Internet environment, NBEN
- Study on intrusion prevention

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

N. Report from TWCIRC

Taiwan Computer Incident Response Coordination Center

The main responsibilities of TWCIRC (Taiwan Computer Incident Response Coordination Center) are to assist Chinese Taipei governmental units in regard of information security related services and incident handlings. The main tasks of TWCIRC in the year 2003 were:

1. Information Security Technical Services Groups: TWCIRC 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.. TWCIRC has completed close to 200 governmental units visits this year.

2. Incident Handling – Hackers Intended to Compromise the Taiwan Computer Network: In August 2003, TWCIRC had found that a group of hackers planned to penetrate the Chinese Taipei governmental computer network. TWCIRC contributed manpower to assist in investigation, sorted out the compromised governmental units, helped them recover and reduced damages from this incident, and effectively stopped attempts of the attacks.

3. Information Security Related Technology Conferences and Trainings: For the purposes of improving network security, system security, and system forensics capabilities of the governmental information staff, TWCIRC hosted various information security related technology conferences and trainings, invited many industrial, academic, and research entities, and shared or instructed the newest information security related technologies. The main training goal for the year 2003 was invasion detection technologies, coupled with information security drills and wireless network security, TWCIRC have organized eight conferences and trainings, with total of 1200 information staff attended these events.

4. Information Security Publications: TWCIRC has completed publishing four publications.

5. Information and Communications Security Incidents Responding and Reporting Drills: To further improve on information and communications security incidents responding and reporting processes and procedures, and to test the incident handling and reporting efficiency and effectiveness of governmental units (include the Information and Communications Security Handling Teams, the Crisis Reporting Subgroups, and Information Security Technical Services Groups), TWCIRC organized an incident reporting drill in 2003. Most of governmental units were very cooperative, and the results were impressive.

6. Weakness Scan and Patch: Based on the most recent vulnerabilities and threats, TWCIRC performed weakness scan on all governmental network IPs. In addition, once the vulnerabilities had been found, TWCIRC would coordinate other information security units, together to patch and fix the vulnerabilities.

7. Promotion of ISMS: TWCIRC had completed five ISMS lead auditor training courses, three ISMS establishment training courses, and three ISMS promotion courses, for a total of eleven events.

In the year 2004, TWCIRC will change its name to TWNCERT and will continue to provide information security services to governmental units, and improve the interactions of international information security related organizations.

APCERT Contact Information:

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