APCERT 2006 Annual Report

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

APCERT
Asia Pacific Computer Emergency Response Team

Chair’s Message 2006

As Chair of APCERT, it is again my pleasure to provide a report to the members of APCERT about our progress during 2006 and APCERT’s fourth year of operation. It is also the last year of AusCERT’s four year term as Chair.

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

During 2006, it was also particularly pleasing to welcome CERT-In to APCERT as the first CERT and the national CERT also, from India to join APCERT. We look forward to working closely with CERT-In and in turn encourage CERT-In’s active participation within APCERT. We are also pleased to see new two new CERTs from Singapore also join us, demonstrating that Singapore has a well-established CERT capability across its economy. APCERT now comprises 19 teams from 14 economies.

During 2006 APCERT has been particularly active within APEC Tel’s Security & Prosperity Steering Group (SPSG) and Jinhyun Cho (KrCERT/CC) is the new deputy convenor to the SPSG. APCERT has also begun to work more closely with the Organisation of Economic Cooperation and Development (OECD) and APEC Tel. APCERT is assisting in organising a joint OECD/APEC Tel workshop on malware in Manila in April 2007.

In December, KrCERT/CC organised another drill to test our level of responsiveness to intra-regional Internet based attacks. The drill was important for a number of reasons. I would urge you to read the media release published on the drill, if you have not already done so. See: http://www.auscert.org.au/7114.

For those of you who have not visited the APCERT web site, I would urge you to do so. It has been updated recently and there is information about APCERT policies and procedures, reports and events.

As Chair and on behalf of the rest of APCERT, I would like to extend our gratitude to this year’s hosts of the APCERT Annual General Meeting, MyCERT and the Malaysian Cyber Security Agency (MCSA), which is being held on the beautiful Langkawi Island, Malaysia. The generosity and warm hospitality they have shown in hosting this important event is vital to the continuing development of APCERT. As with previous hosts, JPCERT/CC and CNCERT/CC, this generosity is greatly appreciated by me personally and the whole of APCERT.

This year we are pleased to have as guests at our annual general meeting representatives from the newly formed IMPACT – International Multilateral Partnership Against Cyber-Terrorism, the Organisation of American States (OAS), Saudi Arabian CERT, Tunisian CERT, TF-CSIRT, Pakistan and FIRST. As part of a global community of CSIRTs, APCERT is mindful that we need to build relationships across and between other groups, such as these, that seek to improve Internet security within their region and the effectiveness of CSIRTs internationally. The representative from the European Network and Information Security Agency (ENISA) regrettably was unable to attend on this occasion but expressed a desire to do so in 2008. We are also delighted to have a number of other excellent speakers, experts in their particular fields, address our members and recognise the effort they have made to travel so far to share their experiences with us.

I have stated this previously and will do so again that while the foundations necessary to help achieve APCERT's goals and potential have largely been built, to continue to succeed and make APCERT relevant and useful to the economies of the Asia-Pacific region, we need to maintain and build on the good will, commitment and contribution of each and every APCERT team. There is no doubt that as cyber security threats seem to worsen that strong cooperative arrangements will continue to remain vital to help protect cyber security within our region.

As we move into 2007, AusCERT will continue to support APCERT, the new Chair and Steering Committee to build on our achievements thus far.

Graham Ingram
General Manager – AusCERT
Chair APCERT
February 2007

APCERT
Asia Pacific Computer Emergency Response Team

CONTENTS

Full Members

General Members

About APCERT

Objectives and Scope of Activities

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

APCERT aims to:

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

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

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

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

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

APCERT Members

APCERT was formed in 2003 by 15 teams from 12 economies across the Asia Pacific region, and has increased its membership since then. In 2006, APCERT welcomed three new teams as General Members: BP DSIRT (Singapore), CERT-In (India), and NUSCERT (Singapore). APCERT now consists of 19 teams from 14 economies across the AP region.

Full Members

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

General Members

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

Steering Committee (SC)

The following APCERT members currently serve as Steering Committee (SC) for APCERT.

- AusCERT, Chair
- CNCERT/CC, Deputy Chair
- HKCERT/CC
- JPCERT/CC, Secretariat
- 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

APCERT
Asia Pacific Computer Emergency Response Team

I. APCERT Steering Committee Report 2006

Steering Committee

During 2006 the steering committee comprised the following members:

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

The two-year terms for AusCERT, MyCERT and JPCERT/CC as members of the steering committee expire on 8 February 2007. These teams may nominate for election again. AusCERT's four year consecutive term as Chair expires on 8 February 2007.

APCERT SC Meetings

Since the last AGM in Beijing, the SC held 4 teleconferences.

Web site

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

New Team Applications

During the year three new general members were approved to join APCERT, CERT-In (India), NUSCERT and BP-DSIRT (Singapore).

APEC-Tel Security and Prosperity Steering Group

Jinhyun Cho from KrCERT/CC was appointed as Deputy Convener of the SPSG.

APCERT international relationships and engagements

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

- APCERT SC was represented as guest of APECTel and gave presentations to eSTG APECTel 33 in Calgary and SPSG APEC Tel 34 in Auckland in 2006.

- SC members (JPCERT/CC and KrCERT/CC) are representatives of the FIRST SC.

- AusCERT and JPCERT/CC attended the GovCERT.nl Symposium in the Netherlands in September 2006.

- AusCERT represented APCERT at a meeting of European Government CSIRTs in Netherlands in September 2006.

- AusCERT is assisting the OECD in drafting a paper on malware, along with other selected experts.

- AusCERT and JPCERT/CC attended the International Watch and Warning Network (IWWN), a multi-lateral government forum, in Washington, DC in April 2006.

- SingCERT co-ordinated the inaugural ASEAN CERT Incident Drill (ACID) in July 2006.

- KrCERT/CC hosted a training course(2006 APEC Security Training Course) for APCERT members and other APEC member economy's CSIRTs.

- CNCERT/CC organized the ASEAN-China Seminar on Networking Security Emergency Response, on 18~22 Dec, 2006, in Beijing, China.

APCERT Drill

In December 2006, KrCERT/CC organised another APCERT cross-border incident handling drill. A report of the drill will be provided separately by KrCERT/CC. CSIRTs from APEC economies were invited to participate. New Zealand also participated.

APCERT Policies and Procedures Progressed

No new policies or amendments progressed.

APCERT AGM 2007 (APCERT Annual General Meeting)

7-9 February 2007, Langkawi Island, Malaysia
http://www.niser.org.my/apcert/index.html

APCERT organizes an Annual General Meeting for CERTs/CSIRTs and other computer security professionals dealing with security incidents. APCERT AGM 2007 was successfully hosted by MyCERT.

Graham Ingram, AusCERT
Chair
APCERT

II. Activity Reports from APCERT Members

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

A. Report from AusCERT

Australian Computer Emergency Response Team – Australia

About AusCERT

AusCERT is the national CERT for Australia. As an independent, not-for-profit, non-government organisation, based at the University of Queensland, AusCERT is the single point of contact for the provision of advice about computer network threats and vulnerabilities in Australia. We also provide an incident response capability for cyber attacks emanating from within Australia or overseas against Australian networks.

AusCERT works closely with Australian government agencies, industry and technology vendors and provides computer security and incident handling advice to a range of subscribers throughout Australia, New Zealand and the Asia-Pacific region. All Australian universities and the majority of New Zealand universities are members of AusCERT and there is a strong relationship with the Council of Australian University Directors of Information Technology (CAUDIT).

CSIRT relationships

As Chair of APCERT from 2003 to 2006, AusCERT continued to build strong community trust relationships through information sharing and cooperative arrangements that help support the Internet security of the economies in the Asia-Pacific region. AusCERT's involvement in APCERT has been an important factor in AusCERT's ability to provide effective incident response support to many Australian organisations and their customers affected by online identity theft.

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

Government submissions

In keeping with its role as an independent advocate for Internet security and a source of information about computer network threats and vulnerabilities, AusCERT made a number of submissions to the Australian government to improve Internet security within Australia. Copies of these submissions are available here:

-Review of the structure and operation of the .au Internet domain 2006, http://www.auscert.org.au/7019
-Review of the e-Security National Agenda, http://www.auscert.org.au/7037
-Review of the Spam Act 2003, http://www.auscert.org.au/6200

CSIRT training
During 2006, with funding from APEC, AusCERT provided CSIRT development training in Mexico, Chile and Peru. AusCERT also assisted with the delivery of TRANSITS training in Seoul and Dubai. AusCERT also provided a range of training to Australian based organisations on various aspects of computer network security within Australia.

The International Systems Security Professional Certification Scheme (ISSPCS)
AusCERT, in partnership with partner EWA Australia and the University of Queensland continues to grow to support a community of IT practitioners with applicants from around the globe signing-up for certifications.

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

2006 Australian Computer Crime and Security Survey
In May 2006, AusCERT published the 2006 Australian Computer Crime and Security Survey in partnership with the Australian High Tech Crime Centre (AHTCC), the Australian Federal Police and every police law enforcement agency in Australia. Its production was sponsored by the Attorney-General's Department and 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

AusCERT2006: Asia-Pacific IT Security Conference
AusCERT held its annual Asia-Pacific IT Security Conference at the Gold Coast in May 2006 with over 1,000 delegates. The conference continues to show itself to be the premier information security conference in Australia, conducted by information security professionals for information security professionals, IT managers and government decision makers in the field.
See: http://conference.auscert.org.au/conf2006/

eSecurity Framework Project
The eSecurity Framework is an Australian government funded project which AusCERT and others are developing to create an environment in which universities can collaborate online with each other at low cost and low risk by establishing a Public Key Infrastructure (PKI) for the university and research sector. The outcome of the project will enable the secure sharing of resources and research infrastructure across the domestic sector and with international partners.

B. Report from BKIS

Bach Khoa Internetwork Security Center – Vietnam

Activity report of 2006:

The number of new viruses which appeared in Vietnam in 2006 is 880, with the average of 2.4 per day. This is four times bigger than 2005. Of these new viruses, 41 were written by Vietnamese and most Vietnamese viruses (37/41) spread through Yahoo Messenger.

Our nation-wide survey, which took place in December 2006, shows that 93% of computers in Vietnam were infected by virus in 2006. This percentage has decreased compared to 2005, but is still at a very high and undesirable level. This survey also suggests that 86.9% of computers in Vietnam were infected by spyware or adware, and 87.6% of computer users received spam everyday during the year.

This is the list of top ten widespread viruses in Vietnam in 2006 (Viruses were named by BKIS)

No	Virus name	Percentage
1	W32.RavMonE.Worm	7.24 %
2	W32.YMBest.Worm	6.46 %
3	W32.Flashy.Worm	5.54 %
4	W32.Rontokbro.Worm	4.64 %
5	W32.RontokbroE.Worm	3.62 %
6	W32.PerlovegaA.Worm	3.02 %
7	W32.RavMonEA.Worm	2.92 %
8	W32.PerlovegaB.Worm	2.69 %
9	W32.Dragon.Worm	1.77 %
10	W32.KillJeefo	1.72 %

In 2006, there were 350 attacks which targeted Vietnamese websites and 40 of the targets were Vietnamese government websites (websites with .gov.vn domain names). Of 340 websites which BKIS has checked for security holes, 90 contained high risk vulnerabilities which could allow hackers to take control of the whole system. BKIS has sent alerts and assisted the webmasters of these sites in patching these vulnerabilities.

BKIS also contributed to the great success of APEC 2006. With our technical experts and our latest security solutions, we were successful in ensuring network security for the meetings of APEC 2006.

In 2006, with the technical assistance of BKIS, many Vietnamese hackers, virus distributors, online phisers… were captured by the Vietnamese anti high-tech crime police. Here are some typical cases:

In April 2006, hacker Nguyen Thanh Cong (DantruongX) was captured. He created and used a botnet to carry out DDoS attacks on an e-commercial website Vietco.com.
In July 2006, another hacker was captured as he carried out DDOS attacks on a host service provider nhanhoa.com.

In October 2006, a virus distributor was captured. He was a first year student of a big University in Hanoi. His virus spread through Yahoo Messenger.
In November 2006, a hacker hacked into chodientu.com, defaced this website and stole its domain name. He was then discovered and captured. Another hacker who defaced the website of the Ministry of Education and Training, Bui Minh Tri, was also captured in this month.

We believe that these cases will help in raising public awareness of Internet security. They also bring more confidence in the safety of Internet to Vietnamese computer users.

Network security trend in Vietnam in 2007:

Virus, spyware and adware will continue to appear everyday while spam continue to be an annoying problem to Vietnamese email users.

We will witness more Vietnamese viruses and spywares in 2007. Cyber crimes will be more sophisticated and more damaging as they are committed for financial profits.

C. 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 82991000（English）
Fax：+8610 82990375
PGP Key：http://www.cert.org.cn/cncert.asc

Overview

In 2006, the incidents CNCERT/CC received in report or discovered increased in a large number compared with last year. The most severe incidents are those web defacements related to governmental organizations and critical information systems, phishing incidents related to business organizations, DDOS attacks targeted to Internet business companies. The threat coming from Botnet and Trojan is still very serious. Attackers seek for illegal benefits with more definite objective and more rampant behavior. The underground hacker industrial chain has been formed.

The vulnerabilities in IT systems are the main springhead of various security threats. In 2006, CNCERT/CC published 87 vulnerability alerts, 16% increasing. More and more 0-day attacks emerged in 2006. The typical one is Worm.Mocbot which exploits MS06-040 vulnerability and Trojan exploiting MS06-011 vulnerability.

In 2006, the number of malicious code captured by CNCERT/CC everyday via distributed honeynet reached 96 with average 3069 times capturing each day. Besides, Internet is filled with a huge number of malicious codes spreading by web pages, email, IM and P2P applications, which is extremely hard to defend effectively.

For Trojan, CNCERT/CC discovered 45,000 IP addresses including dynamic IP addresses of computers embedded with Trojan in Chinese mainland via sample monitoring, 100% increasing compared with last year. For botnet, CNCERT/CC discovered about 10,000,000 IP addresses of computers embedded with bot code. For web defacement, CNCERT/CC discovered 24,477 defaced web pages, nearly 100% increasing.

Incident Report & Handling

In 2006, CNCERT/CC received 26,476 incident reports (excluding scanning attacks), nearly 200% increasing.

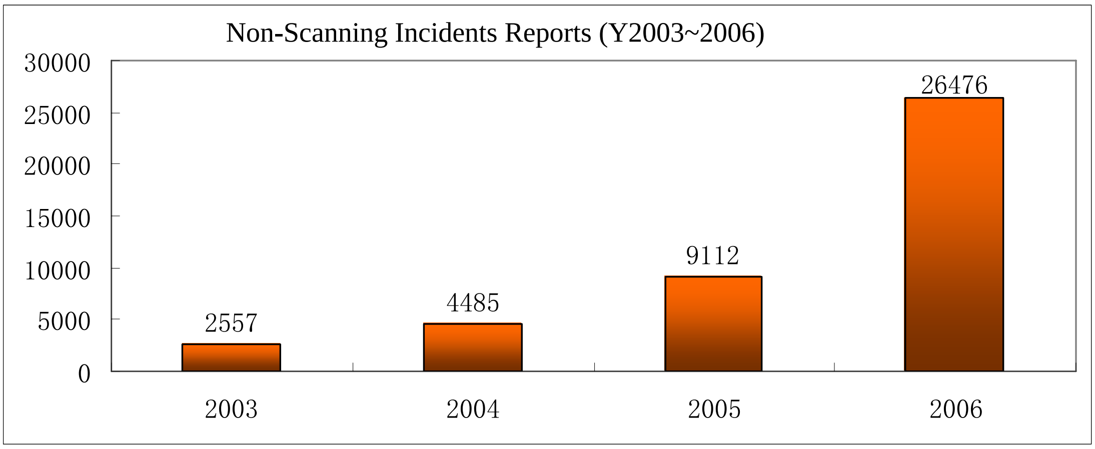


Figure 1 Incident Reports Increasing Y2003-2006

Most incident reports were web defacement, spam mail, phishing and web page embedded malicious code. In 2006, CNCERT/CC handled 613 incidents successfully which mainly include web defacement, phishing, web page embedded malicious code and DDOS. Those related to governmental organizations, critical information systems and international business organizations got the higher priority to be cared about.

The largest large-scale incident CNCERT/CC got to handle in 2006 is Worm.Mocbot related. CNCERT/CC captured 1,050,000 IP addresses of computers infected with Worm.Mocbot and send it to APCERT member teams and 13 national CERTs beyond APCERT boundary for handling.

In 2006, DDOS attack happened frequently with the characteristic of large scale, definite target and money driven. Thus, CNCERT/CC gave more efforts on DDOS handling, and handled 14 serious incidents.

Vulnerability Alert and Handling

In 2006, CNCERT/CC published 87 vulnerability alerts, 16% increasing compared with last year. Some vulnerability CNCERT/CC handled with higher priority is Windows IPSec vulnerability, MS Word buffer overflow vulnerability（MS06-027）, Juniper Router IPv6 vulnerability, Oracle product vulnerability published in June and MS Office remote code execution vulnerability（MS06-048） as well.

Traffic Monitoring and Analysis

According to CNCERT/CC's data of Internet traffic sample monitoring, the top 3 applications of TCP traffic are http, P2P and email.

TCP Port	TCP Traffic Rank	Percentage	Applications
80	1	23.3%	Http
4662	2	3.6%	eMule
25	3	1.2%	Email
3077	4	0.9%	Xunlei（downloader）
6881	5	0.6%	BitTorrent
443	6	0.5%	Https
554	7	0.5%	RTSP
10700	8	0.3%	eMule
8080	9	0.2%	Http
1755	10	0.2%	MMS

Table 1 TCP Traffic Top 10 Ports Y2006

The top 3 applications of UDP traffic are MS Messenger and DNS.

UDP Port	UDP Traffic Rank	Percentage	Applications
1026	1	4.6%	MS Messenger
1027	2	3.9%	MS Messenger
53	3	2.2%	DNS
3076	4	1.7%	Xunlei（downloader）
80	5	1.5%	Http
1434	6	1.5%	MSSQL
16800	7	1.1%	Tvants
3690	8	0.9%	svnserve
4672	9	0.9%	eMule
7000	10	0.7%	酷狗（downloader）

Table 2 UDP Traffic Top 10 Ports Y2006

Trojan & Botnet Monitoring

In 2006, CNCERT/CC monitored some popular Trojans and discovered 44,717 IP addressed of computers embedded with Trojans in Chinese mainland, 100% increasing compared with last year.

CNCERT/CC also kept on monitoring Botnet activities for a long time. In 2006, CNCERT/CC discovered over 10 million IP addresses of computers embedded with Bot clients in Chinese mainland. Meanwhile, more than 16 thousands of Bot servers outside of Chinese mainland were discovered to control Bot clients in Chinese mainland. Among these Bot servers, about 33% were in the United States, and 10% in South Korea.

In general, the size of Botnet is going to become small, localized and specialized. The botnet with less then 1 thousand Bot clients is much more favourite to attackers.

Among Botnet based on IRC application, only 24% Botnets use the Port 6667 which is the default port of IRC application. Therefore, port filtering is not effective enough to block attacker operating Bot clients within internal network of organizations.

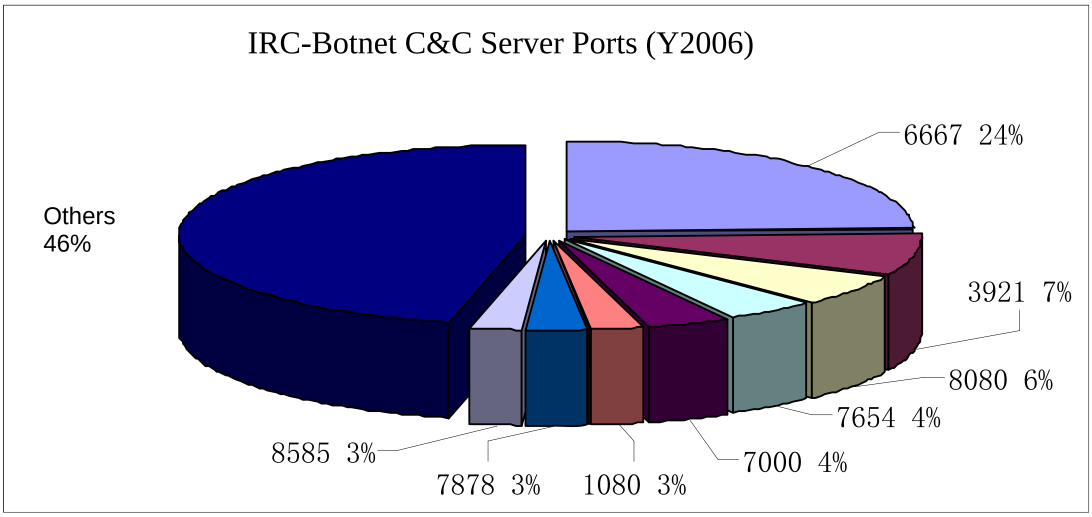


Figure 2 IRC-Botnet C&C Server Ports (Y2006)

Web Defacement Monitoring

In 2006, CNCERT/CC discovered totally 24,477 defaced websites in Chinese mainland, significantly increasing.

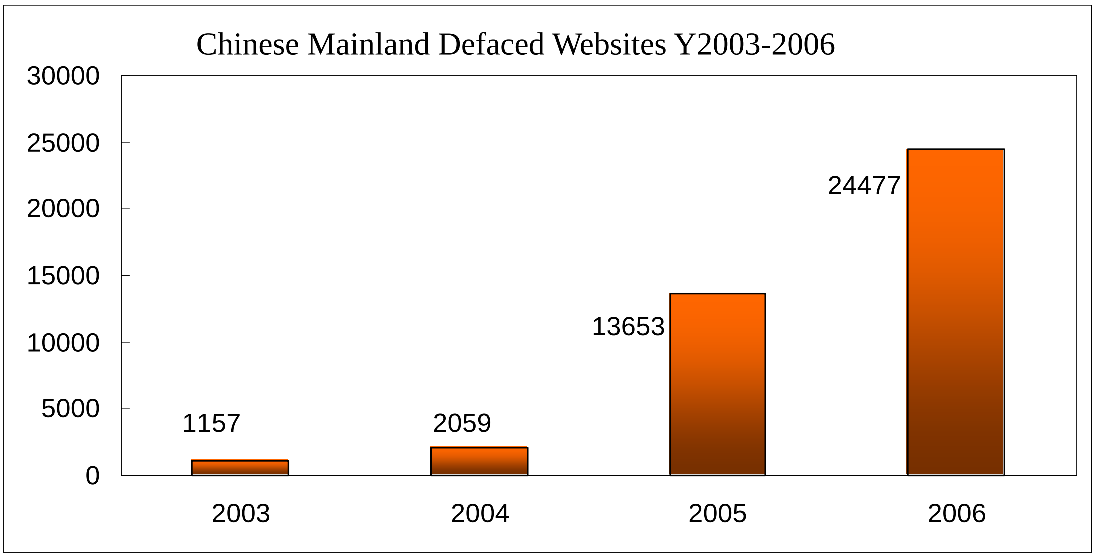


Figure 3 Chinese Mainland Defaced Websites Y2003-2006

According to monitoring data, the governmental websites seem to be much easier to be attacked due to their weak protection measures and maintenance.

Phishing Handling

According to APWG's data, Jan.-Nov. 2006, the number of phishing sites hosting on computers in Chinese mainland accounts for 14.36% of whole world, ranking No.2 in the world. In 2006, CNCERT/CC received 563 phishing reports and resolved 238 successfully. All of these phishing incidents were handled on the request of international CERTs or security organizations and the phishing sites are mostly famous international banking & finance systems.

Phishing Reporters	Number
eBay	207
Verisign	141
Brandimensions	46
HSBC	22
MM Ops Center	22

Table 3 Top 5 Phishing Reporters to CNCERT/CC

Malicious Code Capturing & Analysis

In order to enhance the capability of monitoring malicious code on Internet, CNCERT/CC started its honeynet covering 15 provinces on 19th, June, 2006. Since then, the average times of sample capturing everyday reached 3069.

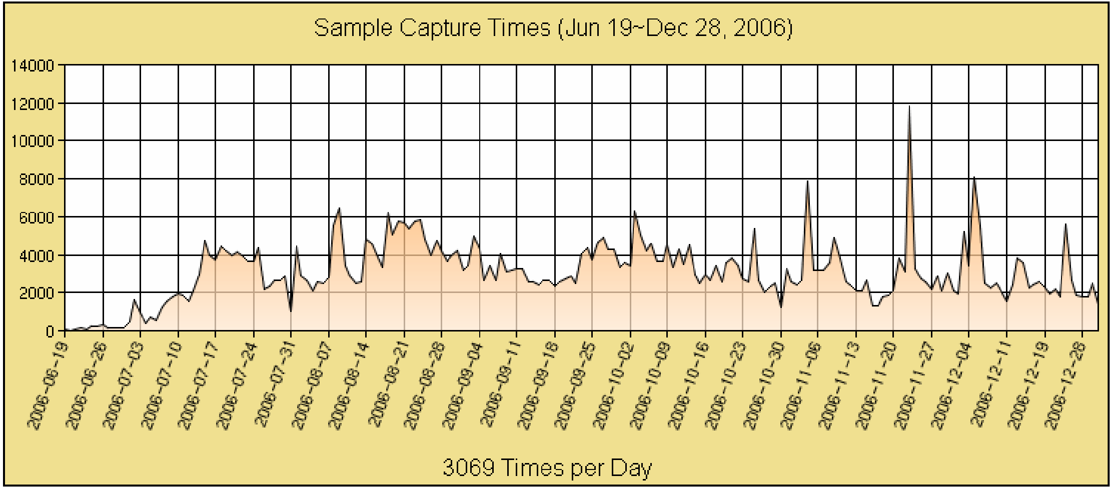


Figure 4 Samples Capturing Times Status

According to the data, the average number of new samples captured everyday is 96. That means new malicious codes were emerging in endlessly.

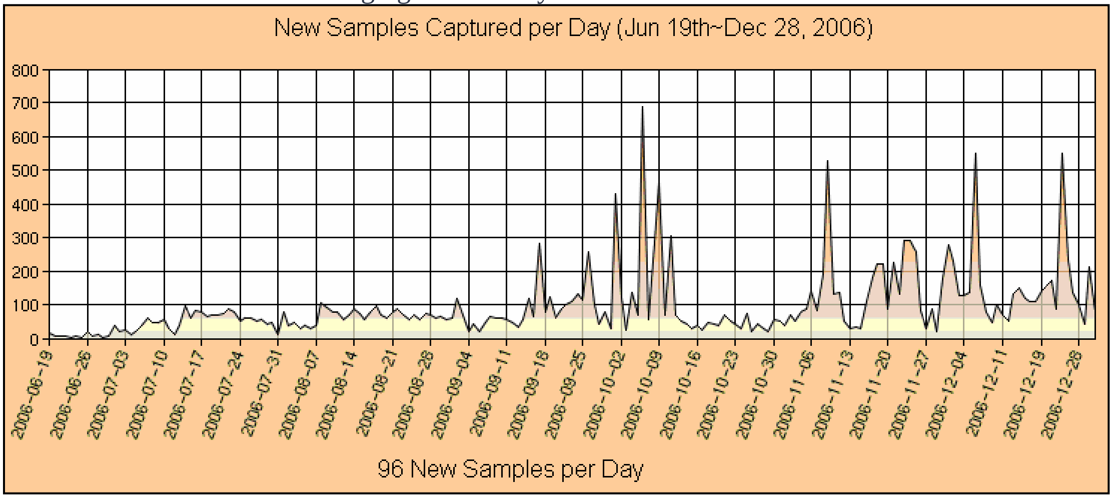


Figure 5 Number of Samples Captured Status

From 19th June to 31st December in 2006, 18,912 sample had been captured by CNCERT/CC's honeynet.

Rank	Name of Malicious Code	Times of Being Captured
1	Backdoor.Win32.Rbot.aem	38790
2	Virus.Win32.Virut.b	38617
3	Backdoor.Win32.PoeBot.c	36104
4	Backdoor.Win32.Rbot.bci	35657
5	Backdoor.Win32.SdBot.aad	31268
6	Backdoor.Win32.Rbot.gen	27246
7	Virus.Win32.Virut.a	17287
8	Backdoor.Win32.IRCBot.ul	14517
9	Backdoor.Win32.SdBot.xd	14242
10	Trojan-PSW.Win32.Nilage.zh	10018

Table 4 Top 10 Samples Captured

Events and Activities

During March 27th-29th, 2006, APCERT 2006 Annual Conference hosted by CNCERT/CC was held in conjunction with CNCERT 2006 Annual Conference in Beijing. The Conference lasted 2 and half days, including 3 closed sessions and 2 open sessions. About 50 delegates from 17 countries and regions participated in the Conference.

During March 28th-31st, 2006, CNCERT/CC 2006 Annual Conference was held in Beijing. About 350 delegates attended the Conference. The Conference provided 4 training courses and over 40 presentations.

During December 18th-22nd, 2006, China-ASEAN Network Security Emergency Response Seminar sponsored by MII was held in Beijing. As the organizer, CNCERT/CC designed the program and coordinated the proceedings.

On 19th December, 2006, CNCERT/CC participated in the 3rd APCERT Incident Handling Drill.

In 2006, CNCERT/CC made brochures about network security emergency response knowledge for public awareness and education. A guidebook of network security emergency response was also finished.

D. Report from HKCERT/CC

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

Summary

The constituency of HKCERT is the small and medium business and internet users in Hong Kong. In 2006, the security attack profile in Hong Kong followed a similar pattern as in 2005. There was a drop in the number of incident reports and yet the level of complexity of attacks increased. Hackers are making use of hurdles in cross border crime investigation and HKCERT has to spend more time coordinating with local and overseas parties. In the past year we have developed in closer collaboration with the local law enforcement agency, ISPs, domain name registration body and overseas CERT teams. We have contributed to the protection of critical internet infrastructure in Hong Kong. HKCERT will take a more proactive approach to tackle security problems and have proposed to the Government to establish an early warning system for cyber threats in Hong Kong.

Statistics

In 2006, HKCERT received 1,605 incident reports, including 468 virus incident reports and 1,127 security reports (See Figure 1). Since 2005, security incident reports have overtaken virus incident reports as major incidents.

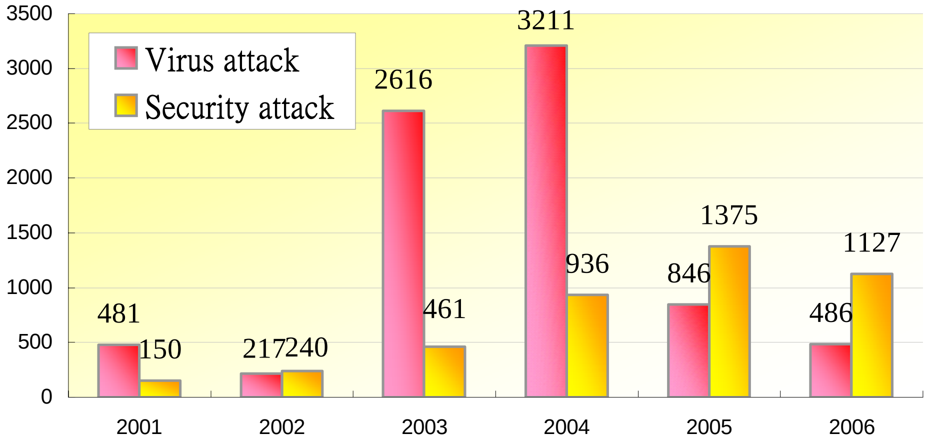


Figure 1. HKCERT incident report statistics 2006

Further analysis of the classification of security incidents indicates that the number of phishing and other incident reports (hacking and intrusion) accounted for over 70% of all security incident reports. The next higher count is the number of spyware incident reports. (See Table. 1) The major cause of the change is attributed to the financial motivation of hackers.

	2003	2004	2005	2006	
Hacking & Intrusion reports	461	783	206	416	(37%)
Phishing Incident reports		73	211	434	(39%)
Spamming incident reports		80	82	47	(4%)
Spyware incident reports			876	230	(20%)
All security incident reports	**461**	**936**	**1375**	**1127**	(100%)

Table 1. Distribution of security incident reports in 2005

During the period, HKCERT had published NIL virus alerts and 178 security alerts on our web site (compared to 8 virus alerts and 108 security alerts in 2005).

Highlights of Activities

- Continued to receive security incident reports and inform the constituency on the latest cyber threats;
- continued to work closely with the government and law enforcement agency, and held meetings to exchange information and to organize joint events regularly;
- established a closer working relationship with ISPs and planned drill in 2007;
- worked closely with Hong Kong Police in closing down phishing web sites;
- participated in the government committees on Information Infrastructure Liaison Group (IILG) and Special Task Force on Information Security (STFIS);
- published a security newsletter every month and sent out an alert summary two times each month;
- published an updated version of the "Information Security Guide for Small and Medium Enterprise (2nd Edition)", in both English & Chinese;
- organized public awareness programs on information security;
- organized the Information Security Summit 2006 with other organizations and associations in November 2006, inviting local and international speakers to provide insights and updates to local corporate users;
- invited to be speakers in information security events;
- responded frequently to media on information security issues;

Highlights of Major Achievements

Besides serving the constituency, one major achievement of HKCERT in 2006 was the contribution to the protection of critical infrastructure in Hong Kong, assisting the Government to assure a secured e-business environment in Hong Kong.

1. **Financial institutions**
   There was an increased concern from the financial sector on the continued growth and sophistication of malicious software. HKCERT worked with the Hong Kong Police Force, Hong Kong Monetary Authority and Hong Kong Association of Banks to promote the awareness of malwares and "Man-in-the-middle Attacks" to the IT security and risk management personnel of the banks in October 2006. HKCERT also relays information on attacks and malicious servers to these organizations.

2. Government cyber security assurance initiatives

HKCERT serves as an advisor to the government on information security issues by actively participating in the Information Infrastructure Liaison Group (IILG) and Special Taskforce on Information Security (STFIS) of the Government. HKCERT contributed to the cyber threat monitoring and advisory role during the ITU Telecom World held in December and the Policy Address of the Chief Executive in October. In late December, the submarine cables off Taiwan southern coast were severely damaged after the earthquake in Taiwan. Internet communication and some voice traffic were paralyzed. During the alert period from December 26, 2006 to January 12, 2007, HKCERT worked with other members of the IILG and coordinated with security vendors and Microsoft on patching and security signature update issues.

3. Hong Kong Domain Name Registry Body and ISPs

HKCERT had been working very closely with ISPs in pinning down phishing sites and botnets located in Hong Kong ISP network segments. In late 2006, we received a number of reports on the use of DNS entries under the ".hk" domain in botnets and phishing websites. HKCERT had worked closely with Hong Kong Domain Name Registration Company and Hong Kong Police Force to speed up the identification of malicious sites, and closely monitor such activities proactively. HKCERT also noted the recent announcement of Chinese domain name service in Hong Kong (or in a wider scope, Asian domain names), on the potential risk of giving criminal newer opportunity of brand theft which could facilitate phishing.

Looking Forward

HKCERT sees the need of active monitoring of the Internet on potential security threats from a local perspective and providing intelligence for pre-empting attack buildup and to assess local cyber risks. We are working to establish an early warning system of cyber threat in Hong Kong.

About HKCERT

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

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

E. Report from JPCERT/CC

Japan Computer Emergency Response Team/Coordination Center – Japan

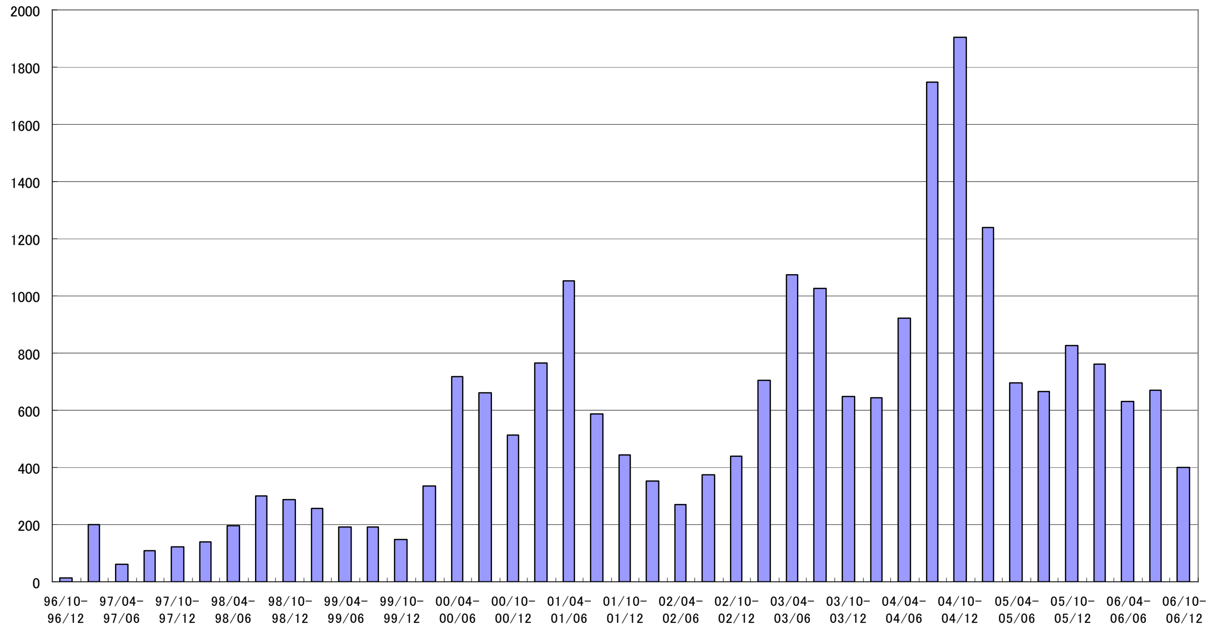
JPCERT/CC is a first CSIRT (Computer Emergency Response Team) established in Japan. It is an independent non-profit organization, acting as a national point of contact for the CSIRTs in Japan and worldwide. Since its inception in 1992, the center has been gathering computer incident and vulnerability 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 2006, JPCERT/CC issued 2,461 tickets responding to computer security incident reports received from Japan and overseas. A ticket number is assigned to each incident report to keep track of the development. Among the 2,461 tickets, 1,252 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	763	629	670	399	**2,461**

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.

<u>Source of Incident Reports</u>

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

ISO Code	1st Qtr	2nd Qtr	3rd Qtr	4th Qtr	Total
.jp	292	247	269	191	999
.com	237	239	330	134	940
.net	27	6	-	19	52

Education and Training

We offer seminars, workshops, and internships targeting system administrators, network managers, and technical staffs who are interested in learning computer security. Some of the events organized by JPCERT/CC in 2006 are listed below:

- Carnegie Mellon University Japan & JPCERT/CC Security Seminar (23 January 2006)
  A one day seminar jointly organized Carnegie Mellon University (CMU)

- Critical Information Infrastructure Protection Security Seminar (23 March 2006)
  A one day seminar jointly organized Information-Technology Promotion Agency(IPA)

- JPCERT/CC 10th Anniversary Symposium (25 October 2006)

- JPCERT/CC C/C++ Secure Coding Seminar (9-10 November 2006)

- InternetWeek 2006 Security Day (9 December 2006)
  A one day seminar jointly organized Japan Network Security Association (JNSA) and Telecom-ISAC Japan

- Bot Project kickoff meeting (12 December 2006)
  A one day meeting jointly organized by the Ministry of Internal Affairs and Communication (MIC) and the Ministry of Economy, Trade and Industry (METI)

Projects

1. Internet Scan Acquisition System (ISDAS) Project

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

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

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

http://jvn.jp/

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

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

Also, the following vulnerability information has been published on JVN in 2006.
-For vulnerability information reported within Japan, 83 cases were published.
-For information provided by CERT/CC, 39 Technical Alerts and 47 Vul Notes were translated and published.
-For information provided by NISCC, 3 cases were translated and published.

Activity Highlights

APCERT Secretariat

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

FIRST Related Activities

- The organization maintains a replica server for Forum of Incident Response and Security Teams (FIRST) in Japan.

http://www.first.org/

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

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

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

F. Report from KrCERT/CC

Korea Internet Security Center – Korea

I. Introduction

KrCERT/CC (AKA KISC, Korea Internet Security Center) serves as the nationwide coordination center in Korea responsible for detecting, analyzing and responding the Internet incident such as worm, bot, and hacking. To minimize the damage from those incidents and to ensure more secure Internet environment, KrCERT/CC is seamlessly operating on 24/7 basis.

II. 2006 Activities

1. Trend of Incident Reports to KrCERT/CC in 2006

Incident reports[1] received by the KrCERT/CC are categorized into malicious code, hacking incident, and bot. Hacking incident has sub categories; spam relay, phishing[2], intrusion attempt, webpage defacement, and other. The number of malicious code reported to KrCERT/CC in 2006 is 7,789, which has 52% decrease compared to that of the last year (16,093 in 2005). The number of hacking incident reported to KrCERT/CC in 2006 is 26,808, which has 20% decrease compared to that of the last year (33,633 in 2005).

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

a. Malicious Code Reports in 2006

The total number of incident reports on malicious code in 2006 is 7,789. The number of reports on worm takes the top (4,117), trojan (2,715) takes the second, virus the third (533), and others (964).

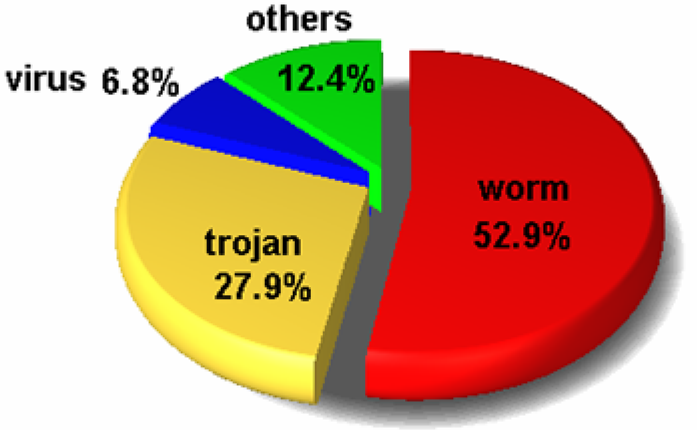


Figure 1. Ratio of reports on malicious code in 2006

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

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

Figure 1 shows that over the half of the reports was worm (52.9%). Unlike the year 2005 when trojan only took 5%, in the year 2006, it takes over one quarter. Although there exist variations on the monthly number of incident reports in 2006, general trend of reports on malicious code decreases compared to previous year.

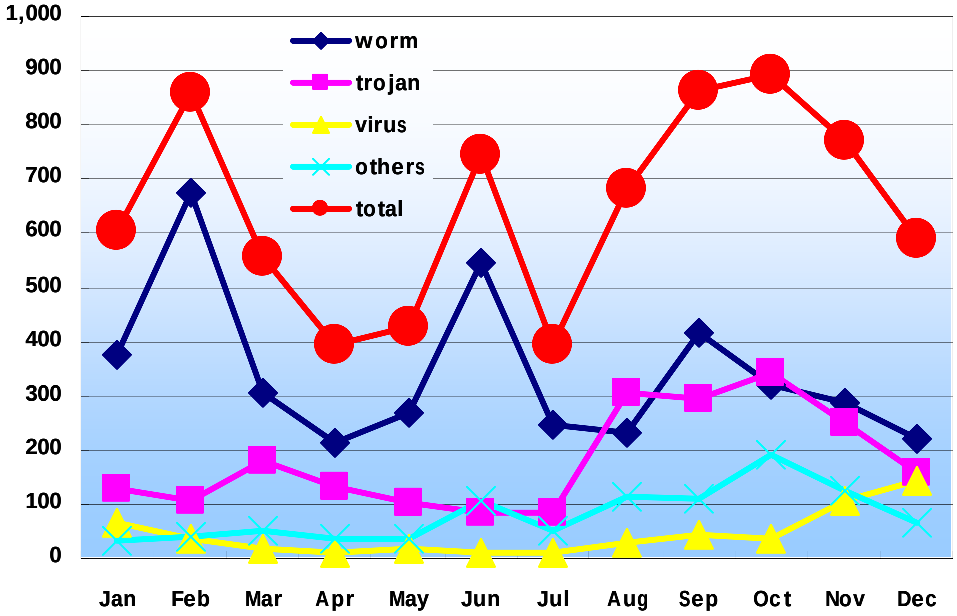


Figure 2. Monthly statistics of reports on malicious code in 2006

b. Incident Reports on Hacking Incidents in 2006

The total number of incident reports on hacking incident is 26,808. Among the reports on hacking incident, spam relay (14,055) takes over the half of the reports on hacking incident and increased more than double than that of 2005 (6,334).

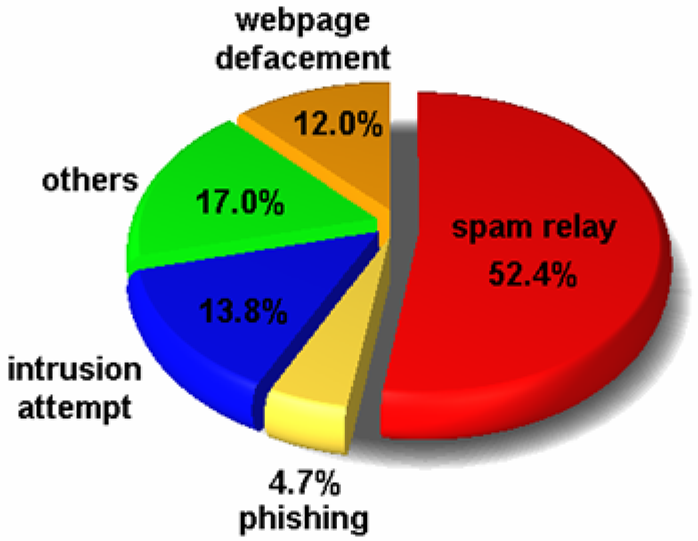


Figure 3. Ratio of reports on hacking incident in 2006

Webpage defacement (3,206) is dramatically decreased than year 2005 (16,692), so as intrusion attempt (3,711) and others (4,570). Phishing (1,266) is some increased compared to that of 2005 (1,087).

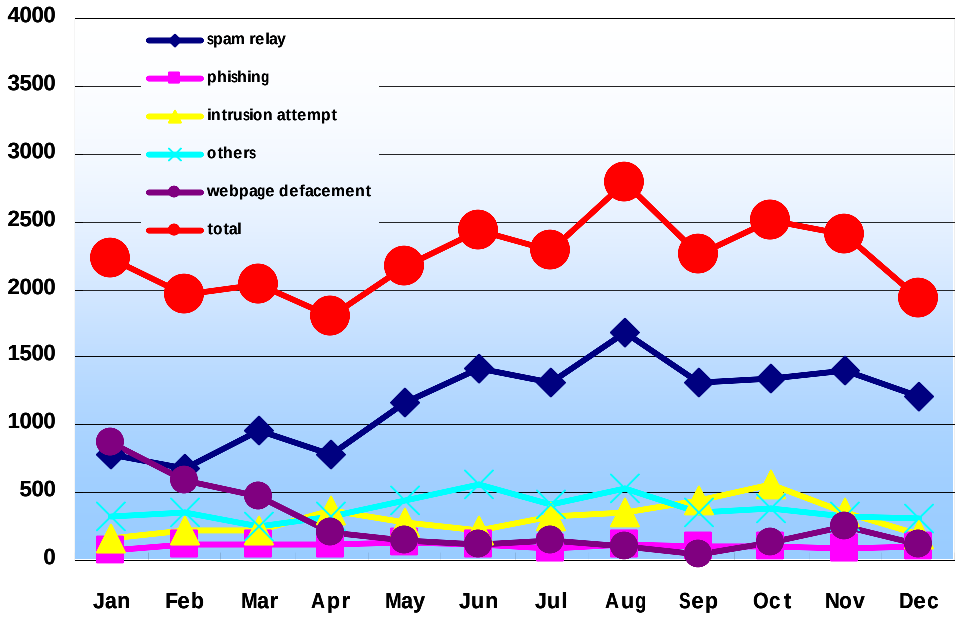


Figure 4. Monthly statistics of reports on hacking incident in 2006

Rather simple hacking incidents such as webpage defacement is steadily decreasing, instead, spam relay is increasing. This fact might imply the current trend that the hackers are seeking the financial gain through their hacked servers using them as spam relay servers for spam mail sending.

The number of reports on phishing is steadily increasing in past recent years. This trend shows seeking the financial gain will not be easily abandoned by the hackers. Recent years are discovered several user friendly phishing tool kits, which make more acceleration on the trend. Financial institutions are always the most targeting sector in phishing. One of the recent issues in Korea is that a different aspect of phishing is surfacing that establishing the fake site of the famous online game and extorting the user identities.

2. KrCERT/CC Activities in 2006

a. International Incident Handling Drill

Internet is in the nature of borderless and seamless network, so as Internet incident. It is characteristically not limited to one economy or region. This reality put more meaning on the importance of having an incident handling drill among many countries, cooperation between CSIRTs for various sectors. KrCERT/CC moderated the incident handling drill in 2006 which has ended with successful result.

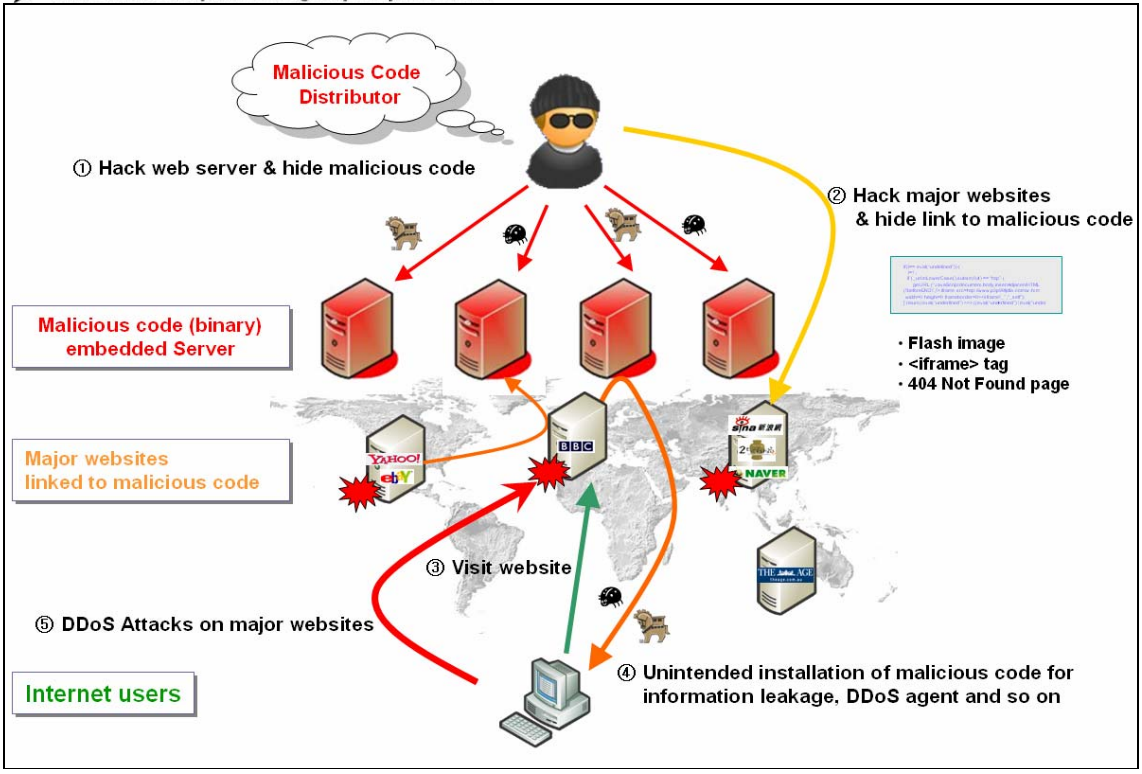

Malicious Code Distributor
① Hack web server & hide malicious code
② Hack major websites & hide link to malicious code
Malicious code (binary) embedded Server
· Flash image
· <iframe> tag
· 404 Not Found page
Major websites linked to malicious code
YAHOO!
ebY
BBC
sina
NAVER
THE AGE
③ Visit website
⑤ DDoS Attacks on major websites
Internet users
④ Unintended installation of malicious code for information leakage, DDoS agent and so on

Figure 5. Scenario of APCERT international incident handling drill 2006

The drill was to verify the coordination capabilities among CSIRTs on incident handling framework, deliver action plans to improve incident response system in each CSIRT, and give participants an experience of a coordination system in case of emergency. For the preparation, 24/7 POCs were shared for rapid communication channel. 15 APCERT member teams from 13 economies have joined the drill to shut down or block malicious code embedded website within or outside of their jurisdictions. Some economies had their drill with the local ISPs involved and made their own version of scenario and procedure. This means there were some time difference among teams to proceed to the next action to be taken, but sharing and preparation of overall framework and scenario were good enough for whole teams participated in, so as they have done their job successfully. Yet another good drill was performed in 2006 by the APCERT and APEC member economies jointly together.

b. 2006 APEC Security Training Course

KrCERT/CC held the 2006 APEC Security Training Course to support strengthening the response capabilities of the developing economies. The objective of this training course is on supporting developing countries to have Internet incident response capabilities while providing an education opportunity for establishing and managing CSIRT in their own country. This event was held on 18 - 22 September in Renaissance Seoul Hotel, with 34 trainees participated from 13 economies, within Asia Pacific region.

2006 APEC Security Training Course
18~22 September 2006 Renaissance Seoul Hotel Seoul, Republic of Korea

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

c. Efforts to reduce malware infection

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

Often a Trojan in the website inserted by a hacker spreads through Internet to users who connect to. It then penetrates to users' PCs without any cognitive indication, to be abused as a bot or for stealing the personal data. Financial gain is often or mostly an objective for these incidents these days and this trend is rising than any moment before. This trend can be seen since many of the infected systems are eventually used as or connected to a phishing or identity theft.

To mitigate this trend, KrCERT/CC is putting an enormous effort by monitoring and handling the malware infected systems while taking down those sites, using the fore-mentioned system we developed. KrCERT/CC also has a plan to distribute the engine of this system for major service providers, such as portals and media, to protect their own constituencies. KrCERT/CC is ready to share the experiences about malware incident handling to protect the users' rights that should not be intervened by the criminal attempts.

d. Efforts to reduce bot infection rate

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

Domestic bot infection rate has marked highest as 24.1% in January 2005, which gradually decreased month by month, and the monthly average rate of 2005 was 18.8%, which is decreased to 12.5% in 2006[3]. The graph of the domestic bot infection rate in 2006, figure 6, shows some ups and downs, but average rate is lower than that of the year 2005.

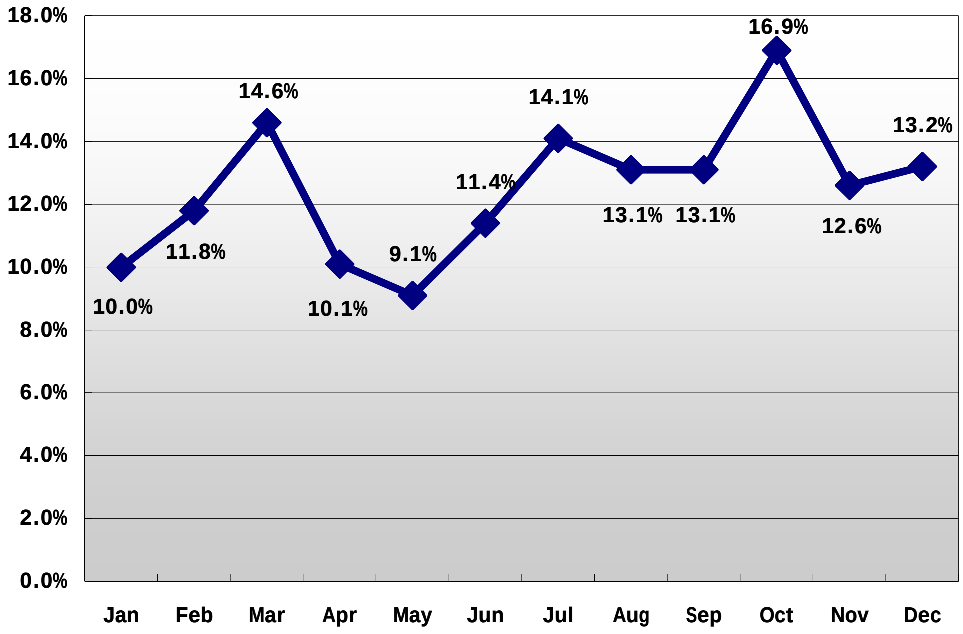


Figure 6. Domestic bot infection rate

III. KrCERT/CC's Plan in 2007

KrCERT/CC is planning to have another good opportunity to experiment and measure the global incident response capabilities in Asia Pacific region by moderating the international incident handling drill this year with most of the APCERT member teams and teams from APEC member economies, as we had successful drill with those teams in December 2006. It is going to be fourth drill since international drill first began on 2004 between China, Japan, and Korea. 15 teams from 13 economies have participated in the drill in 2006.

KrCERT/CC also plans to provide another good education opportunity to many IT and

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

security related professionals, by inviting them to give a security training course, as a part of an APEC project, through lectures and active discussions. This chance will give more skills and experiences in legal and technical way, not only to ones from developing countries who are or plans to building a CSIRT for their own constituencies, but also to leading teams by sharing the experiences and trends from all the economies from Asia Pacific region.

Thank you very much.

POC:

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

G. Report from MyCERT

Malaysian Computer Emergency Response Team – Malaysia

1.0 Introduction

2.0 Operations

2.1 Incident Handling
2.2 Abuse Statistics
2.3 New Services
2.4 Incident Handling Drills

3.0 Seminars, Workshops and Mutual Collaborations

4.0 Other Noteworthy Activities

1.0 Introduction

The year 2006 had been a hectic year for the Malaysian Computer Emergency Response Team (MyCERT), both in handling security incidents, involving in various activities in the field of ICT security at local and international level, as well as moving into our new office facility. In this report, key MyCERT's activities for the year 2006 will be highlighted.

2.0 Operations

2.1 Incident Handling

Year 2006 was a hectic year for MyCERT in handling security incidents reported to us. MyCERT received a total of 1372 incidents, which had increased 82% compared to year 2005. Besides recording the highest number of spam incidents, intrusion and fraud incidents continued to grow as was in previous years.

In year 2006, we received 895 reports on .MY websites defaced. Majority of the web defacements involved mass defacements of virtual websites hosted on single physical host. A particular case in May, we saw mass defacement of 178 websites hosted on a single IP address and in November more than 200 websites were defaced at one time. Based on our analysis of a web hosting server, we found the mass defacements of websites hosted on the server was due to exploiting PHP vulnerability through Cpanel web management system.

MyCERT produced an alert on the mass defacement of Malaysian websites, which is available at:
http://www.mycert.org.my/advisory/MA-103.022006.html

In year 2006, we also observed a surge on fraud cases with 287 reports, almost a one fold increase compared to year 2005. We also observed about 80% of the fraud cases are classified as phishing, mostly involving imitations of foreign banking websites. The phishing sites were mostly hosted on local machines running bots. About 41 (14%) of the incidents targeted local banks while the rest targeted foreign banks and other online payment gateways. MyCERT communicated with relevant parties resulting in the shutting down of the phishing sites and rectification of the infected systems.

In addition, MyCERT also received few reports related to Internet scams. Most of these scams propagated via spam emails which led to requests for financial deposits. Users are advised not to entertain or respond to any such requests. They are encouraged to conduct financial transactions only with trusted and verified parties.

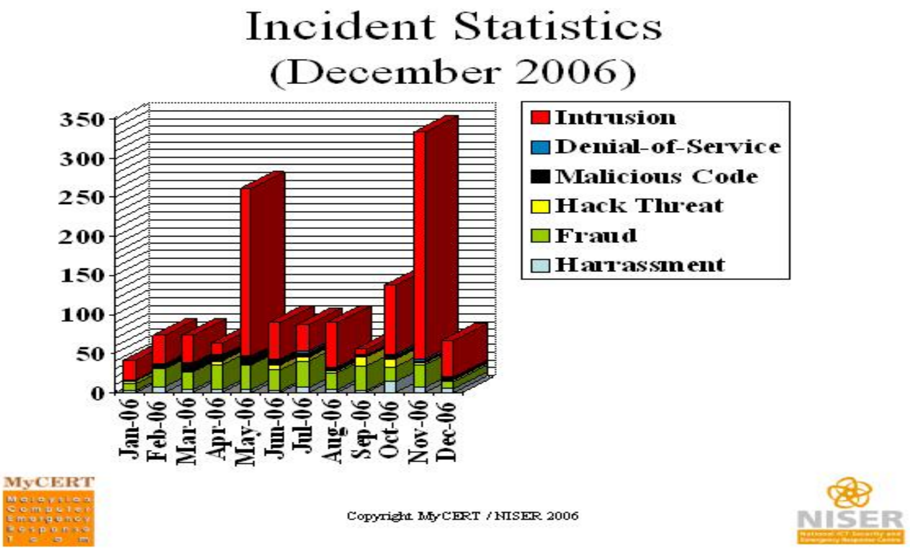
Other incidents that continue to increase are harassment. There were 63 harassment incidents, which is 46.51% increase compared to 2005. Most incidents involved email harassments from disgruntled employees against employers.

Spam continued to grow in 2006 compared to 2005 with more than 100% increase.

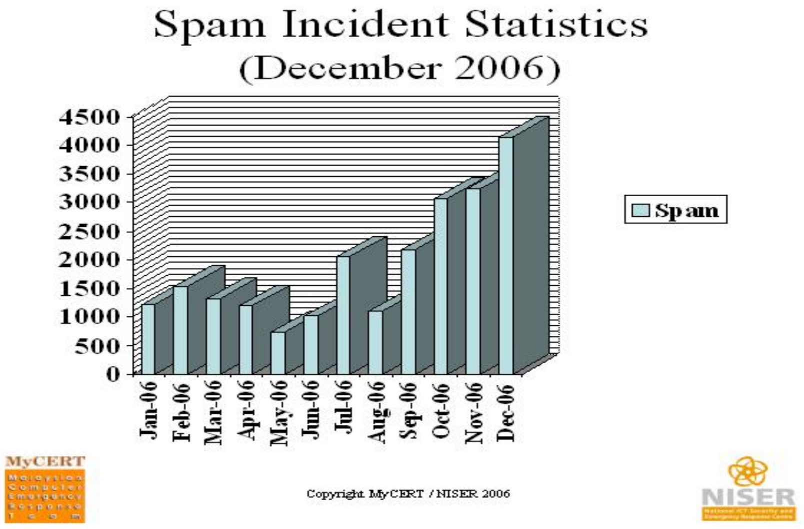
Reports on malicious code for Year 2006 had reduced by 17.1% compared to 2005. Other reports that had decreased in year 2006 are hack threat, by 41.4% and denial of service by 14.3%.

However, overall, there were no major security threats that had affected our ICT infrastructure other than the earth quake south of Taiwan in December resulting in disruption of Internet connectivity for a week.

2.2 Abuse Statistics



	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
Harassment	3	7	4	4	4	3	6	4	3	14	6	5
Fraud	9	23	22	32	31	26	34	21	31	19	30	9
Hack Threat	3	1	2	5	0	6	5	3	12	10	2	2
Malicious Code	1	6	10	7	12	8	6	5	2	4	3	4
Denial of Service	0	0	0	0	0	0	2	0	0	2	2	0
Intrusion	26	36	35	15	215	47	34	57	8	89	288	47
TOTAL	42	73	73	63	262	90	87	90	56	138	331	67



	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
Spam	1227	1538	1323	1200	743	1021	2059	1115	2182	3082	3245	4145

2.3 New Services

In September 2006, MyCERT had introduced another value added service which is the 24x7 Call Reporting Service, to enable Internet users/organizations to reach MyCERT during emergencies 24x7. This is another initiative made to encourage users/organizations within the constituency to report cyber security incidents to MyCERT.

2.4 Incident Handling Drills

In 2006, MyCERT was involved in two Incident Handling Drills. The ASEAN Incident Handling Drill held on 28th July involved nine CERTs from seven ASEAN economies, while the APCERT Incident Handling Drill held on the 9th December, involved 15 teams from 13 economies in the Asia Pacific region. The exercise illustrates the criticality in having immediate access to an effective contact point beyond physical borders and across time domains.

3. Seminars, Workshops and Mutual Collaborations

i) MyCERT Special Interest Group (SIG) Knowledge Sharing Sessions

In year 2006, MyCERT organized three SIG sessions targeting mainly technical personnel from various critical sectors, IT managers and researchers involving prominent presenters from industry who spoke and shared their knowledge and experience with the audience. These sessions proved to be an effective platform to promote networking across sector sharing common issues as well as counter measures.

ii) Promoting the Cooperation Between Local Banks in Incident Handling

In addition, MyCERT also actively participates in the Internet Banking Task Force which consists of representatives from almost all local banks in Malaysia.

iii) Incident Handling training

MyCERT had also conducted Incident Handling Trainings within the year to several public and private sectors.

4.0 Other Noteworthy Activities

i) Produced Alerts, Advisories and Quarterly Summaries

MyCERT had also produced security related documents, ie advisories, alerts, statistics, quarterly summaries and guides for the Internet communities in Malaysia. Some awareness articles are published in local newspapers, MyCERT's website and MyCERT's mailing lists. During the year 2006, twelve new Alerts, Advisories and Quarterly Summaries had been produced for public consumption. MyCERT's comments and views on current security issues were also published widely in local newspapers and magazines. MyCERT also disseminated alerts and advisories from other CERTs and vendors.

A list of alerts, advisories and quarterly summaries produced in 2006 is available from this link:
http://www.mycert.org.my/advisory/

H. Report from SingCERT

Singapore Computer Emergency Response Team – Singapore

About SingCERT

The Singapore Computer Emergency Response Team (SingCERT) is a one-stop centre for security incident response in Singapore. It was set up in 1997 to facilitate the detection, resolution and prevention of security related incidents on the Internet. SingCERT is a government funded national initiative and is managed and driven by the Infocomm Development Authority of Singapore.

Besides providing assistance to its constituency in incident resolution and co-ordination, SingCERT also broadcasts security alerts, advisories and security patches. To promote security awareness and to educate the general public, SingCERT organises frequent seminars, workshops and sharing sessions covering a wide range of security topics.

Incident Trends and Highlights for year 2006

There is a 57% increase in the total number of incidents reported to SingCERT for 2006. Intrusion into systems and the widespread of malcode were major concerns for year 2006. Phishing incidents targeting the banking and finance sector increased as well. SingCERT worked with other CERTs and Internet Service Providers (ISPs) to track down affected systems and users and informed them on how to secure their systems.

Major activities in year 2006

1. ASEAN CERTs Incident Drill (ACID) 2006

The 5th ASEAN TELMIN had endorsed the Hanoi Agenda on Promoting Online Services and Applications to Realise e-ASEAN in September 2005. One of the action items on Network Security calls for ASEAN "To strengthen cooperation in cybersecurity through activities such as conducting regional coordination drills to test out capabilities of National Computer Emergency Response Teams (CERTs) in ASEAN". SingCERT took the lead to plan and organise the inaugural ASEAN CERTs Incident Drill (ACID) which was conducted on 28 July 2006.

Seven (7) ASEAN CERTs participated in the drill. The points-of-contact were tested successfully. All incident reports were concise and comprehensive and the teams were prompt in responding to reports by other teams. This demonstrated that the teams had the necessary procedures and processes in place to handle incidents. The completion of the drill was reported at the 6th ASEAN TELMIN in September 2006.

2. APCERT Incident Drill

SingCERT participated in the 3rd Asia Pacific CERT (APCERT) incident drill in December 2006. APCERT was established by leading and national CERTs from the economies of the Asia Pacific region to improve the level of cooperation, response and information sharing among CERTs in the region. APCERT consists of 19 CERTs from 14 economies

3. Sponsorship

For 2006, SingCERT acted as sponsor for three CERTs for applications to join FIRST and APCERT. One of them is the Qatar Emergency Response Team (Q-CERT). Q-CERT is the national CERT of Qatar. SingCERT is one of the two sponsors assisting Q-CERT to apply for the FIRST Membership. The application is in process and is expected to be completed by February 2007.

SingCERT also sponsored the British Petroleum Digital Security Incident Response Team (BPSIRT) and the National University of Singapore Emergency Response Team (NUSCERT) for APCERT Membership in February and July 2006 respectively. Both teams have been accepted as General Member of APCERT.

4. Security Awareness

In our on-going efforts to educate our constituency and keep our security practitioners updated on security technology, SingCERT has organised a number of seminars and workshops for the year 2006. In addition, SingCERT is hosting a security awareness portal at www.singcert.org.sg/awareness to educate end-users on security and provide useful security resources to the general public.

I. Report from ThaiCERT

Thai Computer Emergency Response Team – Thai

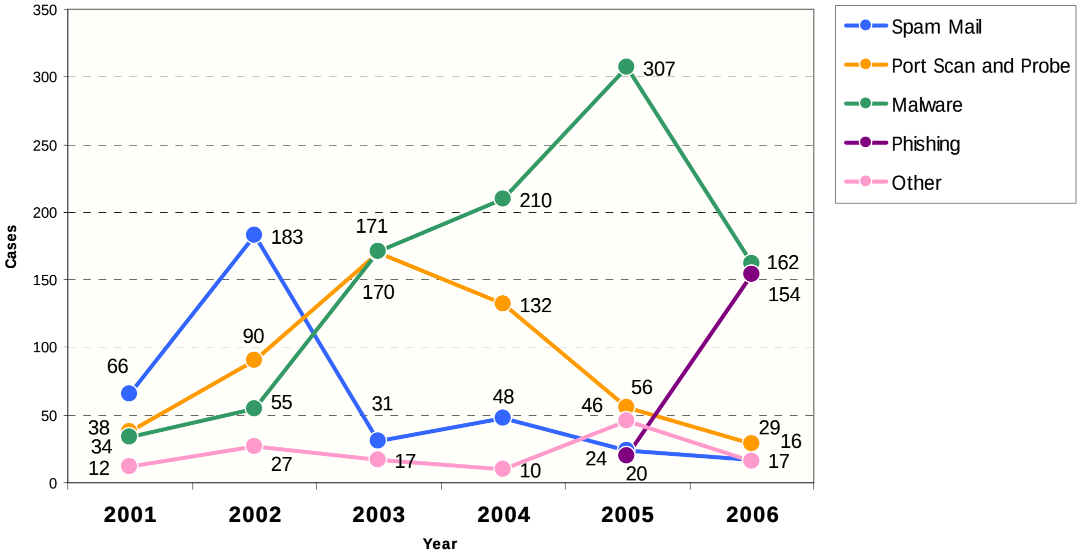
Year 2006 Review and Comparative Incident Statistics

ThaiCERT has been receiving a number of security incidents since the year 2001 -- year of ThaiCERT establishment -- and coordinated related organizations to fix them. Actually, ThaiCERT only provides response service for government units, but since occurrence of phishing cases we have to response to some private units -- concerning those cases -- for closing their compromised services. The table below shows incident statistics since 2001.

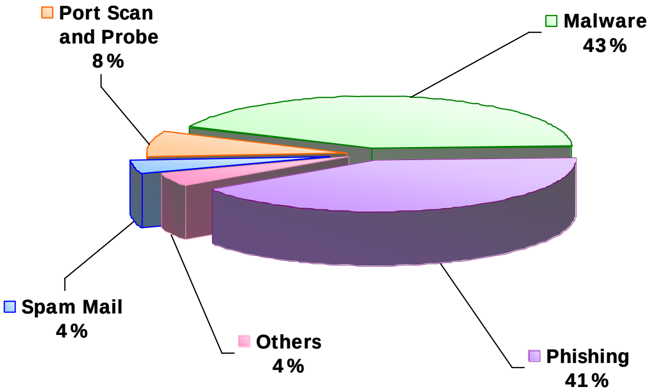
Year	2001	2002	2003	2004	2005	2006
Number of Incidents	150	355	389	400	453	378

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

According to "number of incident by type" table above, the phishing cases have been rapidly increased. They grew from 20 cases in 2005 to 154 cases in 2006 -- about 8 times rising. On the contrary, malware (computer virus, internet worm, etc.) cases have decreased about half of them in 2005. Many reasons can explain this situation. One of them -- in optimistic way -- is that many people have more awareness than before. Then they have sought ways to protect their computers and have found effective ones. The picture, plotted from last table, below makes clearer view.



Focusing on incidents of year 2006, the most type of incident is still malware case. Many malware cases reported to ThaiCERT relate to Trojan horses that were infected via USB storage devices. Some kinds of them are localized in Thailand then it is hard for anti-virus products to detect. The second most type is phishing case. The number of phishing case is around 40% of whole incidents in 2006 similar to phishing cases. On October, 12th 2006, the first phishing site of Thai bank was found while international banks and monetary businesses' phishing sites had been found 1-2 sites a day. The incident data of year 2006 can convert to pie chart like picture shown below.



Staff and Structure Update

Nowadays, ThaiCERT has 23 staff working in 3 security fields. Those 3 fields are infrastructure security, wireless security and security standard.

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

ThaiCERT Services

1. Incident Response

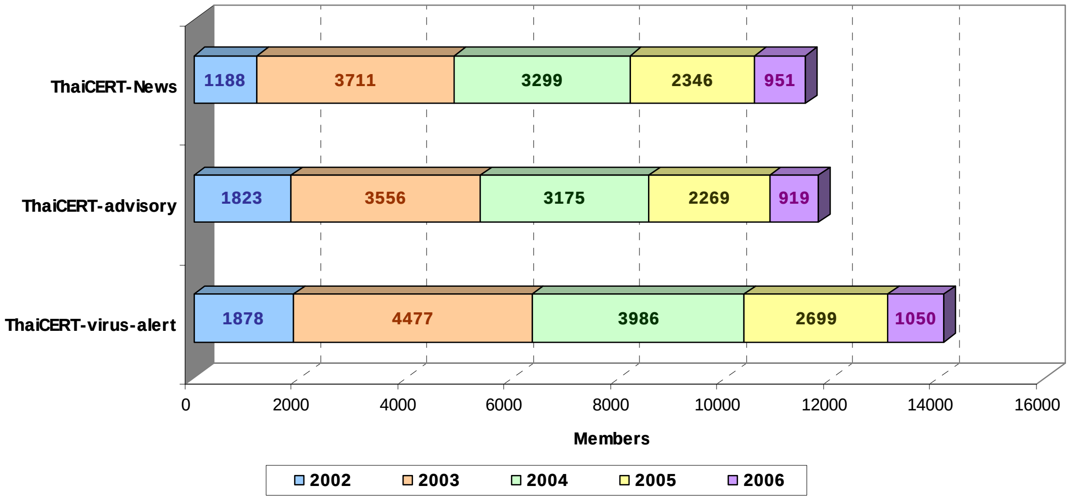
As told before, ThaiCERT has been receiving incident report to coordinate to related organizations. The more incident received, the more effort we have to spend. Therefore ThaiCERT has developed new incident response system based on an open source project, RTIR -- Best Solution Practice's Request Ticket for Incident Response. New IR system launched on September, 1st 2006, has made incident process being tracked easier.

2. ThaiCERT Mailing List Service

This service provides security stuffs to users who have been subscribed for free of charge. All those security stuffs were translated into Thai language and categorized to 3 kinds.

- ThaiCERT-news: 11,495 members
- ThaiCERT-advisory: 11,742 members
- ThaiCERT-virus-alert: 14,090 members

The picture below is shown numbers and types of mailing list service from 2002 to 2006.



3. Security Publications

Furthermore, there is a mailing list service; ThaiCERT has provided security publications in other ways such as web page and hard copy. There are 66 web pages and 1 hard copy in 2006. All were translated into Thai.

Web page:	General articles	10	pages
	CERT advisory	39	pages
	Virus and vulnerabilities alert	10	pages
	Monthly news	7	pages
Hard copy:	ISO/IEC 17799-2005 Standard		

4. Security Course Training

ThaiCERT arrange a variety of training courses in 2006. The objective is to raise information security awareness to Thai people. There are many training courses such as

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

5. **Security Auditing**

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

ThaiCERT Activities

1. **Seminar / Conference Participation**

   ThaiCERT has participated in some variant of regional and international conference in year 2006 such as

   - Asia Pacific Security Incident Response Team Annual General Meeting 2006, Beijing, China. (March 28th-29th)
   - 4th RAISS (Regional Asia Information Security Standards) Forum Meeting, South Korea. (April 19th-22nd)
   - 18th Annual FIRST Conference on Computer Security Incident Handling, Baltimore, Maryland, USA. (June 25th-30th)
   - Collaboration Meeting for CSIRTs with National Responsibility - June 2006, Pittsburgh, Pennsylvania, USA. (July 2nd-4th)
   - Etc.

2. **Incident Drill**

   In year 2006, There are 2 on-line incident drills that were set in our region.

   - ASEAN CERTs Incident Drill 2006 on July 28th, held by SingCERT.
   - APCERT Incident Handling Drill 2006 on December 19th, held by KrCERT/CC.

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

3. **Providing the secure wireless network for Regional Conference on Open Standards 2006, Bangkok, Thailand**

   As ad-hoc job and unplanned situation, we had to use all knowledge, skills and abilities of wireless team to provide solution for the attendant to use wireless network connected to internet without any interruptions. Eventually, we did that job smoothly.

4. **Enhancing encryption to 2D barcode application**

   We applied 2D barcode technology to use for registration in NSTDA (National Scientific and Technology Development Agent) Annual Conference 2006, Thailand. Moreover, we developed QR Code encoder/decoder with AES encryption and demonstrated this application in Thailand ICT Expo 2006.

J. Report from TWNCERT

Taiwan National Computer Emergency Response Team – Chinese Taipei

Introduction

TWNCERT is a non-profit organization intended for improving incident response and IT security awareness in Taiwan. It is mainly dedicated to create a response center that can help optimize the capability of real-time monitoring, coordination, response and handling in the face of security incidents.

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

2006 Highlights

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

   TWNCERT offers IT security conferences, workshops, training courses, and exhibitions for technical staffs and security managers. The organized events in 2006 are listed below:

   (1) Trainings

   - ISMS lead auditor training courses.
   - ISMS building training courses.
   - Training courses for internal auditors of ISMS
   - CEH (Certified Ethical Hacker) training course for 20 participants.
   - CISSP (Certified Information Systems Security Professionals) training course for 40 participants.
   - Trainings for information alerting system and vulnerability scanning.
   - Extra development of a total of 20 hours and 19 different e-Learning training courses.

   (2) Conferences and Workshops

   - 32 conferences and 2 workshops of information security technical issues are provided in 2006

2. **Incident Response and Prevention**

   TWNCERT publishes advisories and alerts for preventing and responding to computer incidents. We collect information from many sources (e.g. real-time monitoring, incident handling and forensic, malicious code analysis) and try to integrate for announcing security trends. In 2006, TWNCERT published total 808 advisories and alerts, including:

   (1) 199 alerts for intrusion incidents.
   (2) 45 advisories for system vulnerabilities or weakness.
   (3) 141 alerts for web site defacement incidents.
   (4) 422 advisories for warning the suspicious incidents and incident prevention.
   (5) 1 alerts for emergency incident.

3. **International Cooperation**

   TWNCERT is always glad to join in the international security organizations and share information with security communities. In 2006, TWNCERT continued to participate in the following security communities and attended many important conferences:

(1) APCERT
- Attend APCERT annual conference in Beijing, China.

(2) FIRST
- Attend FIRST annual conference in Baltimore, USA.

(3) APEC-TEL
- Attend APEC-TEL 33 meeting in Calgary, Canada.
- Attend APEC-TEL 34 meeting in Auckland, New Zealand.

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

(5) AVAR（Association of anti Virus Asia Researchers）
- Attend AVAR conference in Auckland, New Zealand.

TWNCERT receives the reporting of computer incidents about Taiwan and coordinate related law enforcement agencies to handle these incidents. We want to strengthen the ability of information security defense and reduce the damage cause by these incidents. In 2006, TWNCERT handle 97 incidents reporting from international security communities, including:

(1) All 97 incidents are about Taiwan phishing sites. TWNCERT coordinated law enforcement agencies to remove the phishing pages or shutdown the phishing hosts.

4. Presentations and Publications

TWNCERT is continuing to do research on security areas and publish the research results in the international security conferences in order to share our experiences with communities. The following is the presentation and paper published in 2006.

(1) TWNCERT 2005 annual report, APCERT 2006.

5. ISO 27001/BS7799 Information security management systems certification

In order to provide a highly security standard of services, TWNCERT had passed the new certification of ISO 27001/BS7799 by BSI in July, 2006.

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

URL: http://www.twncert.org.tw/en/main.php
Email: twncert@twncert.org.tw
Phone: +886-2739-1000 ext 661
Fax: +886-2733-1655

K. Report from CERT-In

Indian Computer Emergency Response Team– India

About CERT-In:

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

Activities of CERT-In

CERT-In provides:

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

The summary of activities carried out by CERT-In during the year 2006 is given in the following table:

Activities	Year 2006
Security Incidents handled	552
Security Alerts issued	48
Advisories Published	50
Vulnerability Notes Published	138
Security Guidelines Published	1
White Papers Published	2
Trainings Organized	7
Indian Website Defacements tracked	5211
Open Proxy Servers tracked	1837

Table 1. CERT-In Activities during year 2006

Summary of Computer Security Incidents handled by CERT-In during 2006

In the year 2006, CERT-In handled more than 550 incidents. The types of incidents handled were mostly of Phishing and Network Scanning & Probing. Among the malicious code incidents, significant numbers of incidents were reported in February, 2006 due to spreading of Nyxem (Kamasutra) worm, targeting Indian users. CERT-In published alert regarding spreading of this worm well in advance and suggested suitable countermeasures and disinfection tools thereby containing wide spread damage in the country.

The most widespread phishing attacks reported in 2006 is carried out against e-commerce sector. It is accounting for 76 % .The second most targeted sector is financial services which accounts for 24 % for the total number of incidents reported in the year 2006. Of the total phishing incidents handled in 2006, the cases in which Indian Financial Institutions were involved were only 2% and rest belonging to outside India.

The summary of various types of incidents handled during 2006 is given below:

Security Incidents	**2004**	**2005**	**2006**
Phishing	3	101	339
Network Scanning / Probing	11	40	177
Virus / Malicious Code	5	95	19
Email Spoofing	3	8	7
Others	1	10	10
Total	**23**	**254**	**552**

Table 2. Security Incidents handled yearly trend

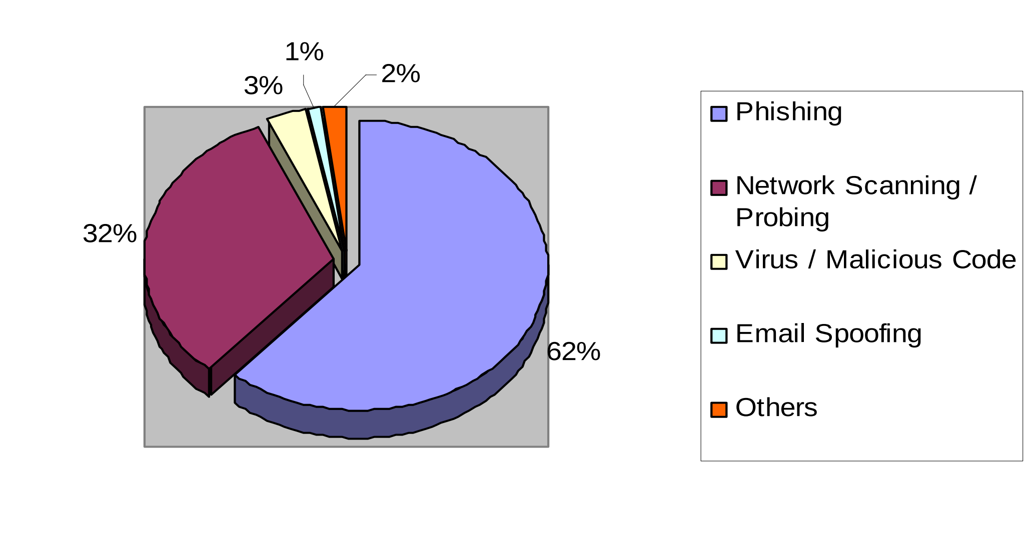


Figure 1. Summary of incidents handled by CERT-In during 2006

Tracking of Indian Website Defacements

CERT-In has been tracking the defacements of Indian websites and suggesting suitable measures to harden the web servers to concerned organizations. In all 5211 numbers of defacements have been tracked. Most of the defacements were done for the websites under ***.com*** domain. In total 1226 ***.in*** domain websites were defaced.

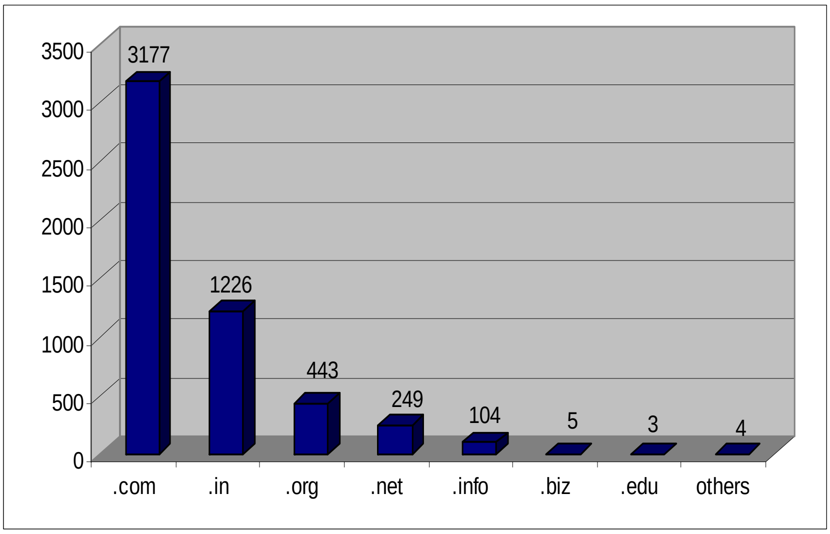


Figure 2. Indian websites defaced during 2006 (Top level domains)

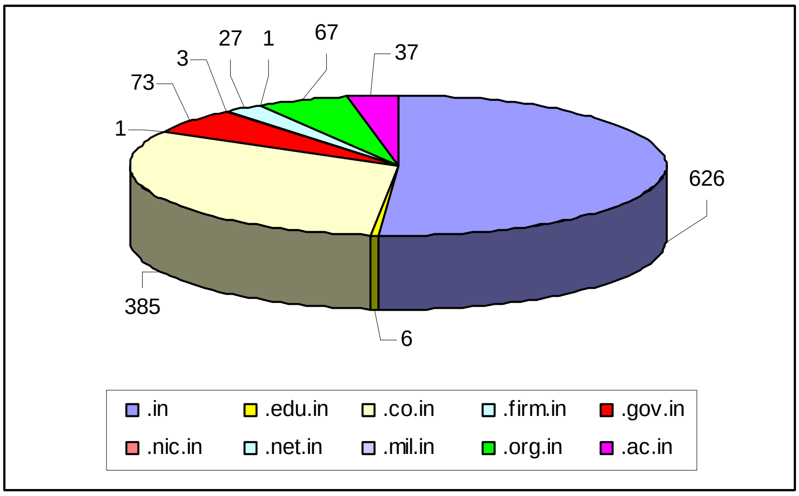


Figure 2.1 .in ccTLD defacements during 2006

The following figure shows the month wise comparison of the Indian website defacements in year 2005 and 2006. In the month of august unusual increase has been noticed in the year 2005 as well as in the year 2006. In the year 2006 total 1311 defacement were tracked on Indian websites during the month of August.

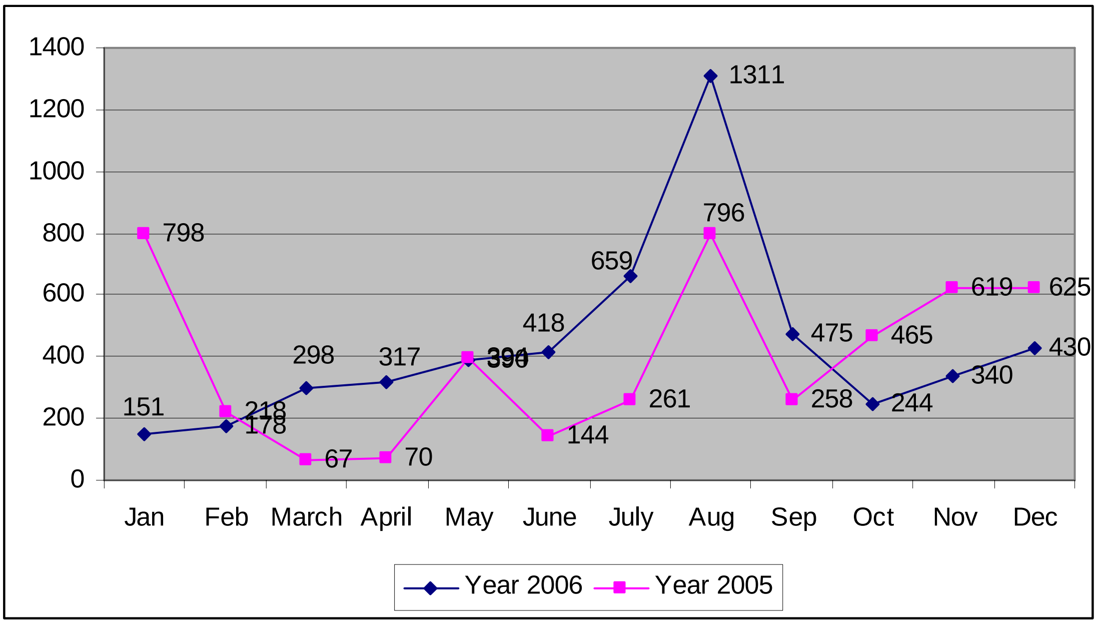


Figure 3. Monthly comparison of the Indian Website Defacements (2005 -2006)

Tracking of Open Proxy Servers

CERT-In is tracking the open proxy servers existing in India and proactively alerting concerned system administrators to properly configure the same in order to reduce spamming and other malicious activities originating from India. In all 1837 open proxy servers were tracked in the year 2006. As compared to previous year the number of open proxy have increased, 1156 open proxy were reported last year. A bar chart of open proxy servers tracked during this year is shown in the figure.

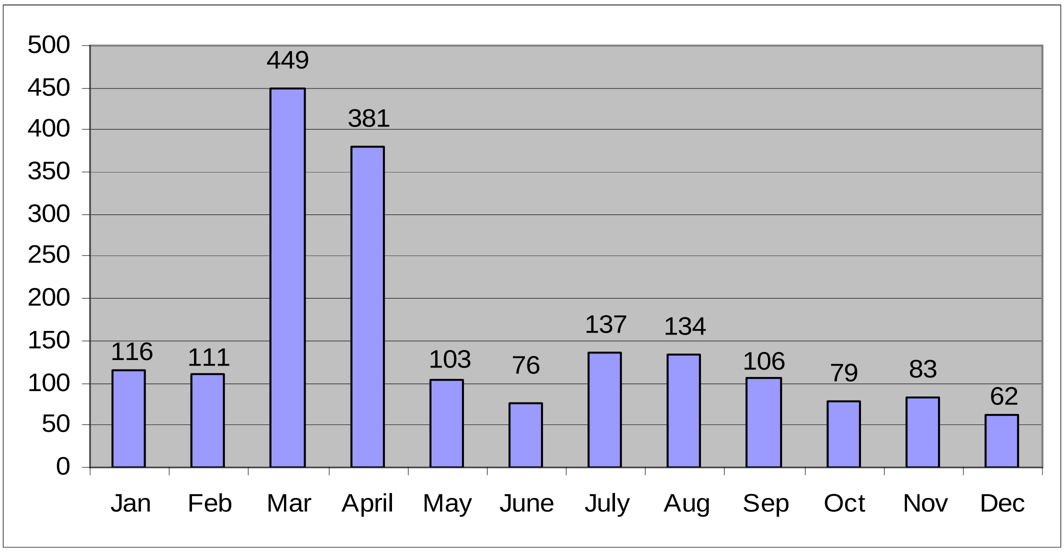


Figure 4. Monthly statistics of Open Proxy Servers in 2006

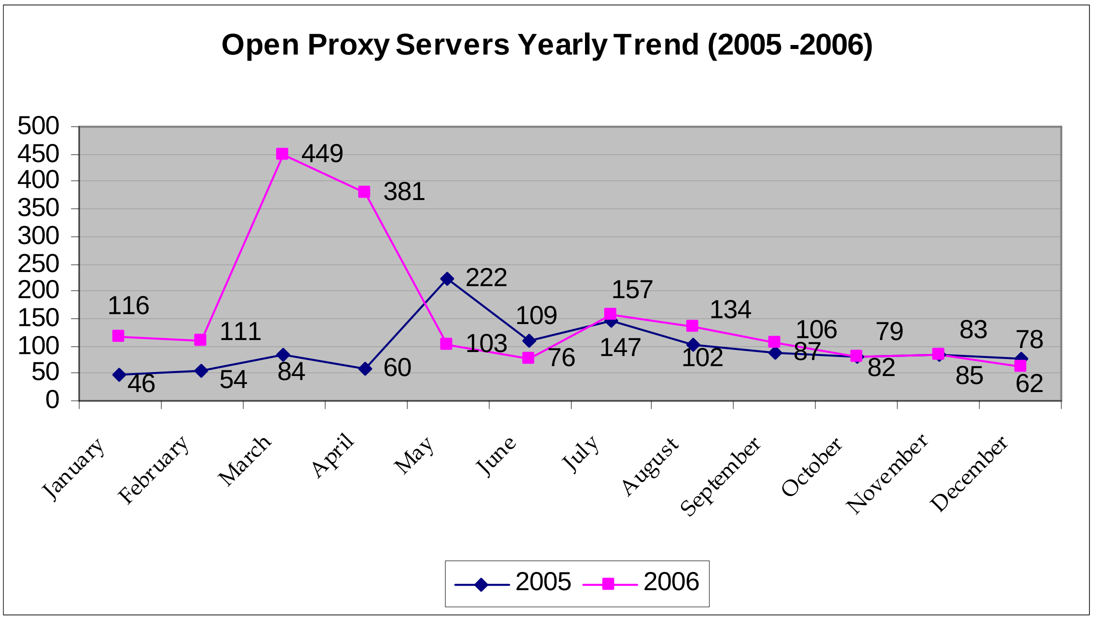


Figure 4.1 Monthly comparison of Open Proxy Servers (2005 -2006)

Education and Training

To create awareness and to enable users to implement best practices, CERT-In is organising workshops and training programmes on focused topics for targeted audience such as CIOs, financial and banking sector officers, System Admins, ISPs etc. Experts from industry are delivering lectures in these workshops apart from CERT-In. CERT-In has conducted the following training programmes for CIOs and System Administrators during 2006.

1. Workshop on "Protection against Phishing Scams" on 15th February, 2006

2. Workshop on "DNS DDoS Amplification Attacks and Mitigation" on 1st May, 2006

3. Workshop on "Information Security for CIOs" on 16th May 2006

4.Workshop on "Information Systems Security" for System Administrators of ASEAN Countries, 28-30 August 2006

5. ASEAN Regional Forum(ARF) Workshop on "Cyber Security", 6-8 September 2006

6. CERT-In & eBay joint workshop on "E-Commerce Security" on 26th September, 2006

7. Workshop for Points-of-Contact from critical sectors on "Cyber Security" on 31st October, 2006

Cyber Security Assurance Framework

CERT-In is establishing the National Cyber Security Assurance Framework for protection of Critical Information Infrastructure. As part of this, CERT-In has empanelled 57 'Security Auditors' for auditing, including vulnerability assessment & penetration testing of computer systems and networks of various organisations of the government, critical infrastructure organisations and those in other sectors of the Indian economy. CERT-In plays the role of mother CERT in the country and helping formulation of sectoral CERTs in critical sectors.

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

International collaboration

- CERT-In became general member of APCERT in March 2006. CERT-In wishes to convey its compliments to JPCERT/CC for being the Mentor in the registration process.

- CERT-In has organised a workshop on "Information Systems Security for System Administrators of ASEAN Countries" from 28th to 30th August 2006 at Manesar, Haryana , India in coordination with International Cooperation Division of Department of Information Technology and Ministry of External Affairs, Government of India. In all 21 participants including two members of ASEAN Secretariat have participated in the workshop.

- CERT-In has organised the ARF Workshop on "Cyber Security" under the guidance of Department of Information Technology and Ministry of External Affairs in New Delhi during 6th -8th September 2006 . In all 58 delegates from 20 ARF participating countries and representatives of ASEAN Secretariat and private sectors participated in the workshop. There were 13 country presentations and 4 industry presentations were made during the workshop. The topics of discussion included Threat of Cyber Terrorism – National Perspective, Government Initiatives on Cyber Security and Protection of Critical Information Infrastructure, Cyber Security - Trends and Protection Strategies and Strategy to Counter Cyber Terrorism and Areas of Cooperation.

- CERT-In participated in the APCERT International Incident Handling Drill 2006 coordinated by KrCERT. As part of the drill, the malicious websites were successfully brought down. Local ISPs and security vendors from India also participated in the Drill.

- CERT-In became member of FIRST in December 2006. CERT-In wishes to convey its compliments to JPCERT/CC and US-CERT for mentoring during the membership process.

Future Outlook

The thrust is to make CERT-In the most trusted referral agency in the area of information security in the country. CERT-In is focusing on building a network of CIOs of Critical Infrastructure Organisations and interacting with them to ensure security of the critical systems, collaboration with IT product and security vendors to mitigate the vulnerabilities in various systems, providing guidance for developing and augmenting sectoral CERTs, cooperation with international CERTs and security organizations on information sharing and incident response, promote R&D activities in the areas of Artifact analysis and Cyber Forensics and security training and awareness. CERT-In is developing a mechanism to issue advance warnings and alerts on cyber attacks and provide countermeasures by analyzing Internet traffic pattern.

CERT-In is also developing separate security web portal for Government & Critical information infrastructure organisations and home users. This web portal will publish information on latest threats & their countermeasures alongwith security best practices.