2006 Annual Report by 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.

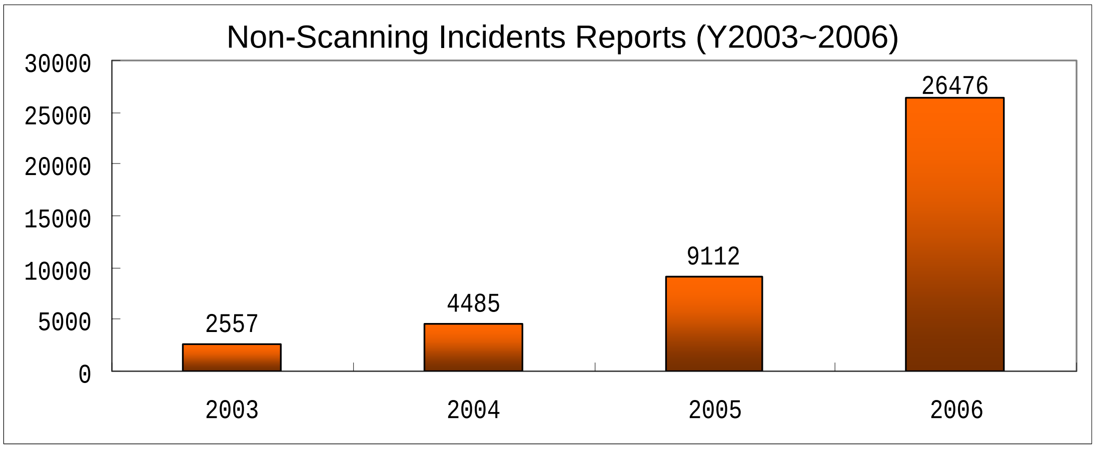

Figure 1 Incident Reports Increasing Y2003-2006

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%	Kugou（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.

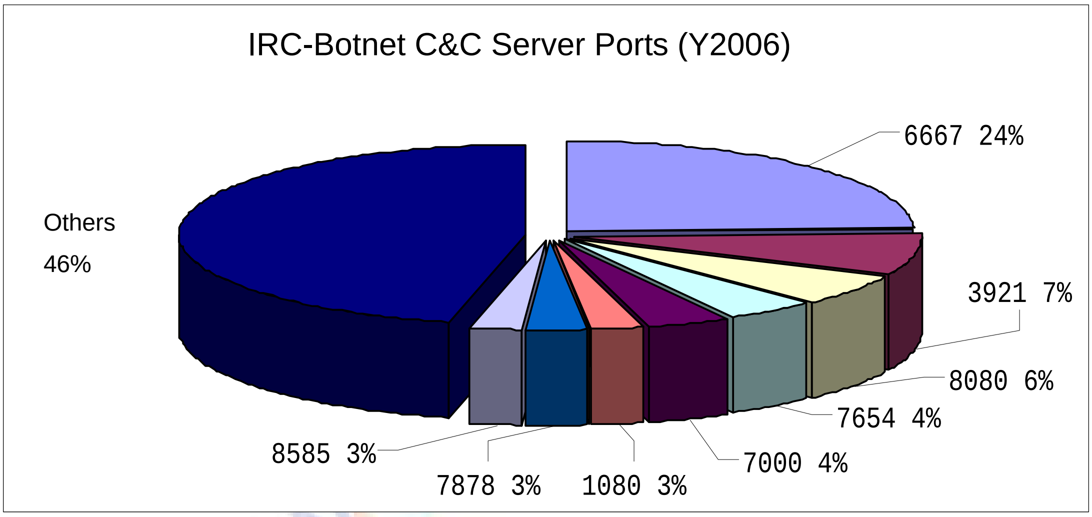

Figure 2 IRC-Botnet C&C Server Ports (Y2006)

Web Defacement Monitoring

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

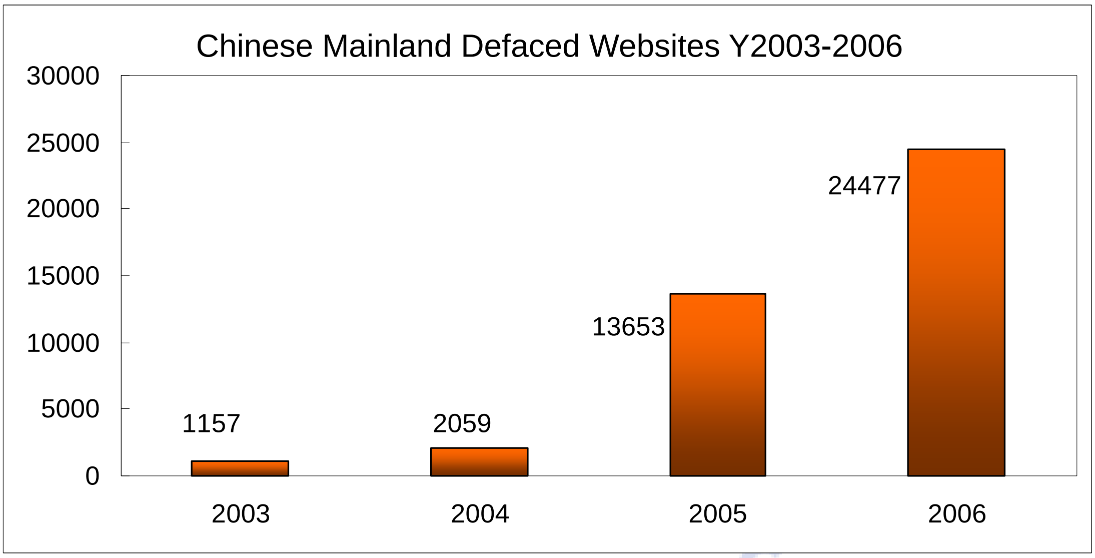

Figure 3 Chinese Mainland Defaced Websites Y2003-2006

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

Melicious 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.

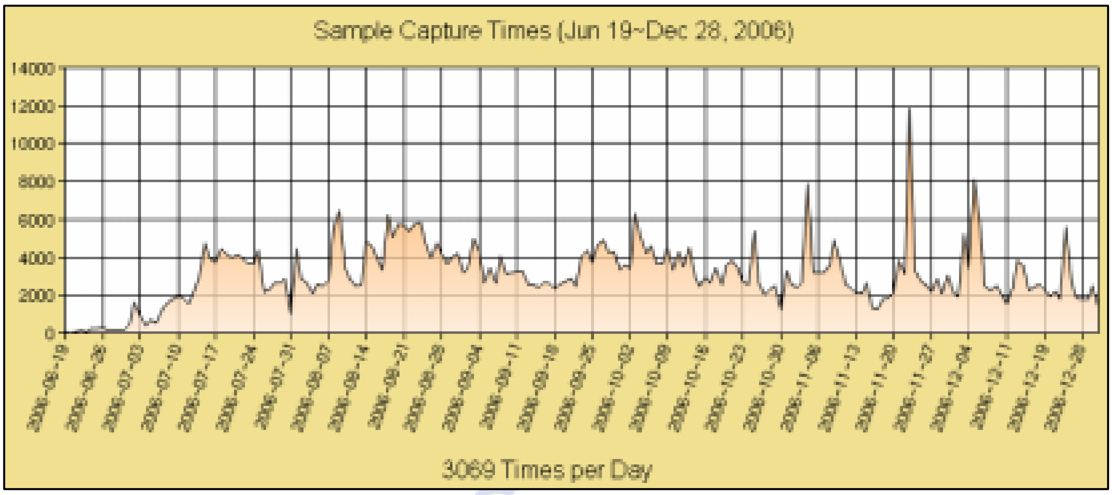

Figure 4 Samples Capturing Times Status

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

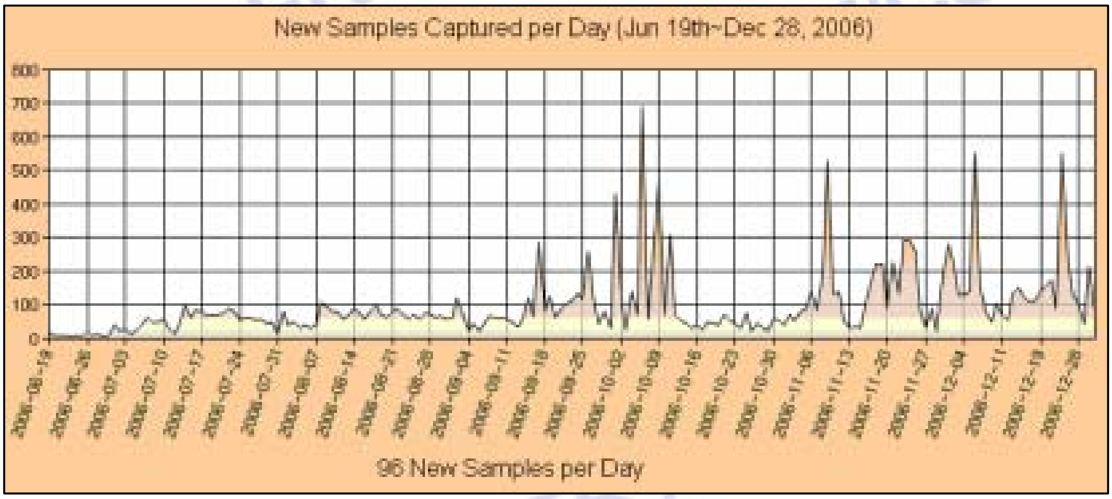

Figure 5 Number of Samples Captured Status

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.