CNCERT/CC Annual Report 2007

（English Edition）

TABLE OF CONTENTS

1 About CNCERT/CC

1.1 Introduction

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.

1.1.1 Establishment

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.

1.1.2 Workforce power

CNCERT/CC, which is headquartered in Beijing, the capital of P.R.China, has 31 provincial branch offices in 31 provinces of China mainland.

1.1.3 Constituency & Etc

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

2 Activities & Operations

2.1 Incident Reports

In 2007, CNCERT/CC received 4,390 incidents reports (excluding scanning attacks) from domestic and international users and agencies.

Most incident reports were about phishing (1,326), spam mail (1,197) and webpage embedded malicious code (1,151). The reports of these 3 types of incident were increased by 136%, 104% and 260% compared with that of last year respectively.

2.2 Incident Handling

In 2007, CNCERT/CC handled 1,057 incidents, including webpage defacement, phishing, webpage embedded malicious code, DoS and malware.

2.3 Abuse Statistics

Traffic Monitoring and Analysis
According to CNCERT/CC's data of Internet traffic sample monitoring, the top 4 applications of TCP traffic are http, P2P, email and instant messenger.

TCP Port	Rank	Percentage	Applications
80	1	29.39%	Http
4662	2	1.11%	eMule
25	3	0.66%	SMTP
443	4	0.56%	Https
8080	5	0.39%	Http
3077	6	0.35%	Xunlei (downloader)

8000	7	0.27%	QQ
1863	8	0.13%	MSN Messenger
6881	9	0.13%	BitTorrent
19101	10	0.10%	clubbox

Table 1 TCP Traffic Top 10 in 2007

The top 3 applications of UDP traffic are Xunlei, MS Messenger and Http.

UDP Port	Rank	Percentage	Applications
15000	1	2.80%	Xunlei (downloader)
1026	2	2.76%	MS Messenger
1027	3	2.40%	MS Messenger
80	4	1.70%	Http
53	5	1.30%	DNS
53124	6	0.95%	Unknown
3076	7	0.79%	Xunlei (downloader)
8000	8	0.75%	QQ
4672	9	0.65%	eMule
1434	10	0.64%	MSSQL

Table 2 UDP Traffic Top 10 in Year 2007

Trojan & Botnet Monitoring

In 2007, CNCERT/CC monitored some popular Trojans and discovered 995,154 IP addresses of computers embedded with Trojans in Chinese mainland, which was increased by 2125% compared with that of year 2006.

CNCERT/CC also kept on monitoring Botnet activities for a long time. In 2007, CNCERT/CC discovered over 3,624,665 IP addresses of computers embedded with Botnet clients in Chinese mainland. Meanwhile, 10,399 Botnet servers outside of Chinese mainland were discovered controlling Botnet clients in Chinese mainland. Among these Botnet servers, about 32% were in the United States, 13% in Chinese Taiwan and 7% in South Korea.

Among ports used by Botnet based on IRC application, the top 3 ports are 6667 (40.1%), 1863 (5.2%) and 7000 (2.94%).

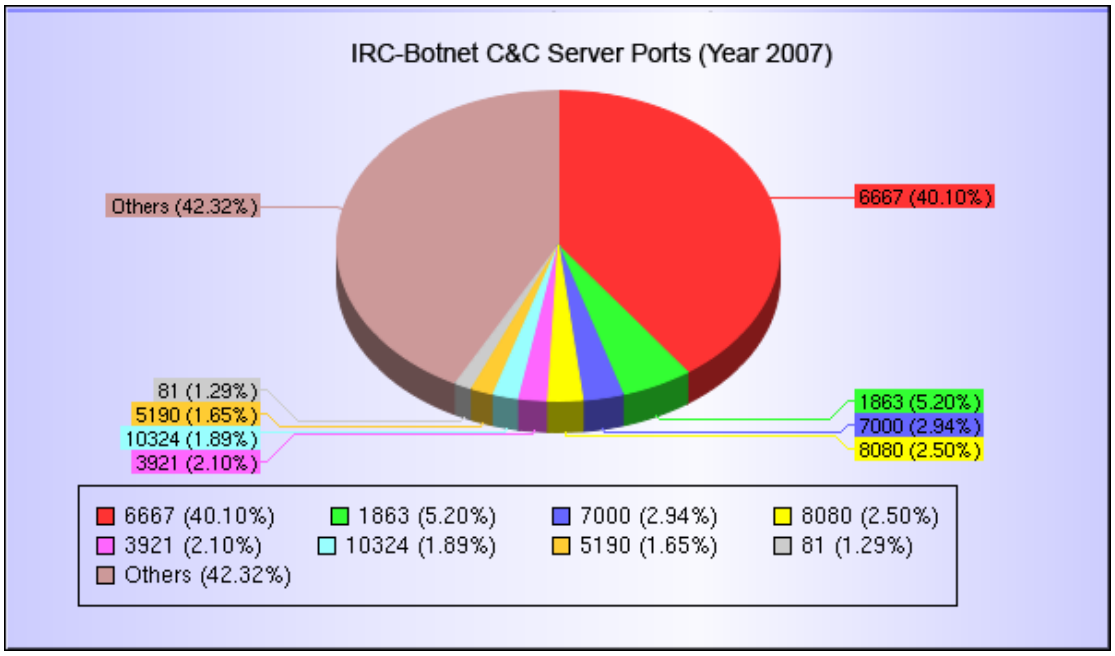

Figure 1 IRC-Botnet C&C Server Ports (Year 2007)

In general, the size of Botnets is going to become smaller, localized and specialized. The Botnet with less than 1 thousand Botnet clients is much more favorable to attackers.

Web Defacement Monitoring

In 2007, CNCERT/CC discovered totally 61,228 defaced websites in Chinese mainland, significantly increasing. According to monitoring data, the governmental websites seem to be much easier to be attacked due to their weak protection measures and maintenance.

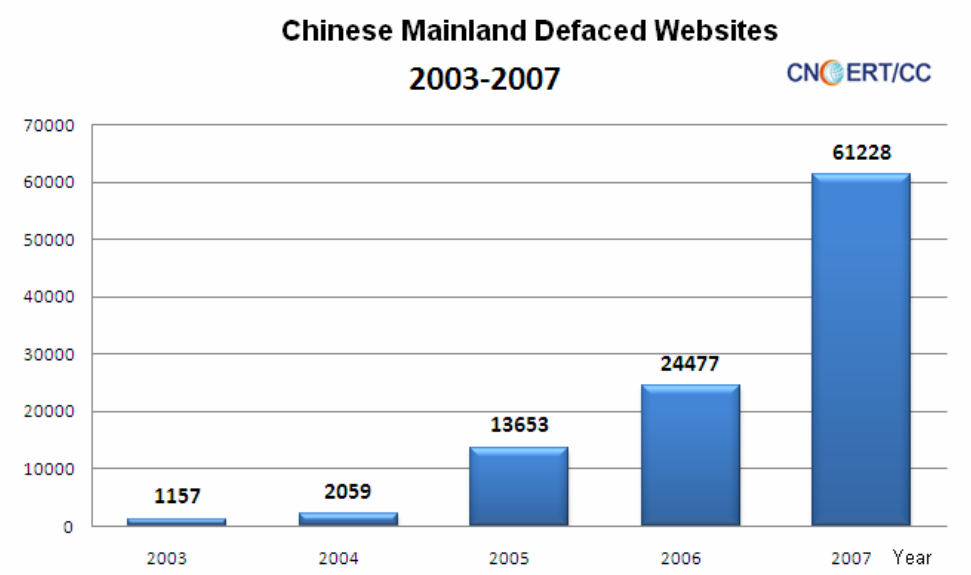

Figure 2 Chinese Mainland Defaced Websites Y2003-2007

According to CNCERT/CC's data, top 10 attackers who defaced Chinese websites in 2007 are listed below.

Rank	Attacker	Number of Web Defaced	Proportion
1	sinaritx	1731	2.8%
2	1923turk	1417	2.3%
3	the freedom	1156	1.9%
4	aLpTurkTegin	1052	1.7%
5	Mor0Ccan Islam Defenders Team	864	1.4%
6	iskorpitx	761	1.2%
7	寒水芊芊	754	1.2%
8	黑侠	681	1.1%
9	电脑迷	669	1.1%
10	lucifercihan	525	0.9%

Table 3 Top 10 Web Attackers in Year 2007

Phishing Handling

In 2007, CNCERT/CC received 1,326 phishing reports and resolved 394 successfully. All of these phishing incidents were handled on the request of international CERTs or security organizations. The phishing sites are mostly famous international banking & finance systems.

Phishing Reporters	Number
VeriSign	259
eBay	255
RSA Cyota	128
Castlecops	143
Mark Mornitor	74

Table 4 Top 5 Phishing Reporters to CNCERT/CC in Year 2007

Malicious Code Capturing & Analysis

In order to enhance the capability of monitoring malicious code on Internet, CNCERT/CC started up its distributed honeynet project in 2006. The average times of sample capturing everyday reached 3,408 in 2007.

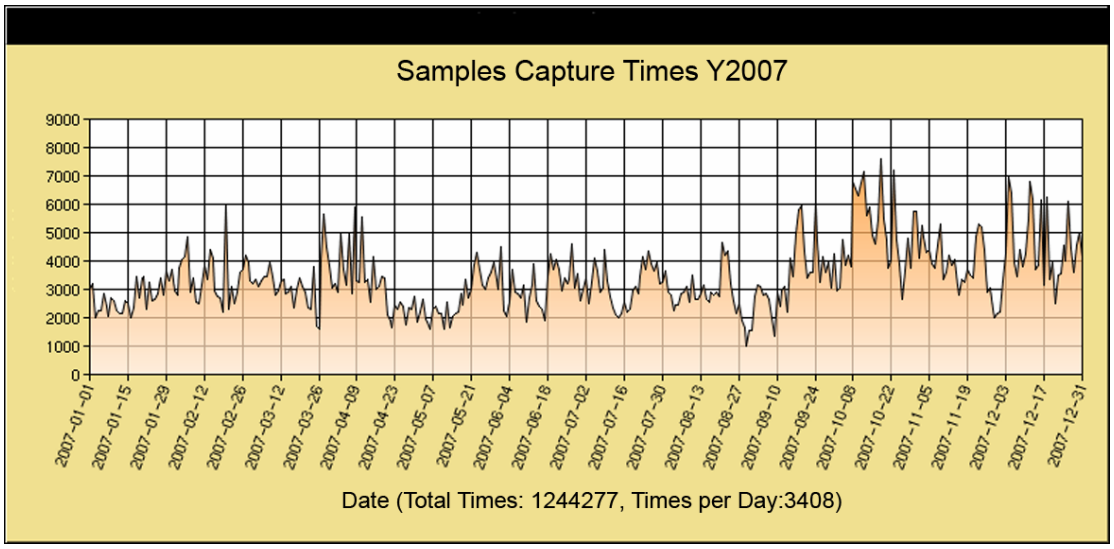

Figure 3 Samples Capturing Times Status

According to the data, the average number of new samples captured everyday is 496. That means new malicious codes were emerging endlessly.

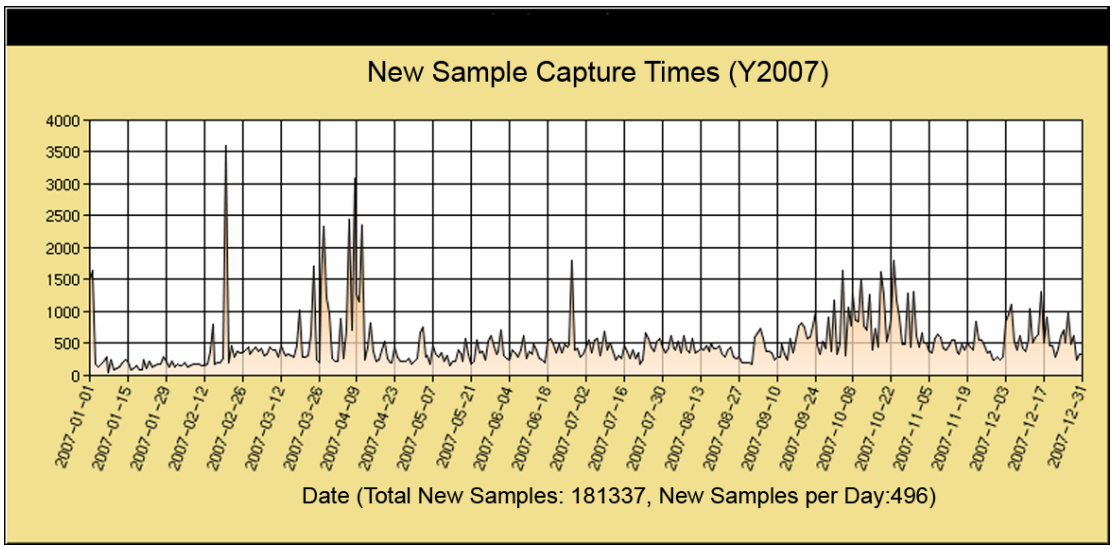

Figure 4 Number of Samples Captured Status

In 2007, 181,337 samples had been captured by CNCERT/CC's honeynet.

Rank	Malicious Code Name	Times of being Captured
1	Backdoor.Win32.VanBot.ax	82852
2	Net-Worm.Win32.Allaple.b	79196
3	Backdoor.Win32.PoeBot.c	69636
4	Net-Worm.Win32.Allaple.e	33712
5	Virus.Win32.Virut.b	33485
6	Backdoor.Win32.SdBot.aad	23998
7	Virus.Win32.Virut.a	21084
8	Backdoor.Win32.Rbot.bni	19348

9	Backdoor.Win32.Rbot.gen	18017
10	Backdoor.Win32.SdBot.xd	16891

Table 5 Top 10 Samples Captured by CNCERT/CC's honeynet

2.4 Security Information Services

CNCERT/CC's users of its security information services are ISPs, cooperative key infrastructures, and relevant government agencies as well. In 2007, 162 internal warnings and 5 critical vulnerability advisories had been delivered in time.

359 articles were published on CNCERT/CC's website, including security bulletins, vulnerability advisories, malware warnings, technical reports, security guide, and etc.

3 Events organized/co-organized

DDoS Seminar
The Seminar was held on 1st January, 2007 in Beijing. Delegates came from governments, security research organizations, enterprises and end users. The topics are the damage and prevention of DDoS attacks as well as how to mitigate its impact by technical and management means.

CNCERT/CC 2007 Annual Conference
The Conference was held in Wuxi from April 5 to 7, 2007. About 200 delegates attended the conference.

Computer Malicious Programs Handling Law Circumstance Seminar
The Seminar on law circumstance for handling computer malicious programs was held on 28 August, 2007, in Beijing.

Domain Name Abuse Handling Mechanism Seminar
The seminar on mechanism of handling network attack via domain name abuse was held on 12 September, 2007, in Beijing. It's sponsored by MII.

4 Achievement

4.1 Presentation and Publication

Introduction of Malware Issues, APEC-OECD Malware Workshop in APEC-TEL 35, 2007.4.22, Manila

National Network Security Capacity Building, ITU Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection, 2007.8, Hanoi

CERT/CSIRT's Role in Ensuring Olympic Cybersecurity, Information Security Summit

2007, 2007.12, Hong Kong

What Can National CERTs Contribute on Botnet Countermeasures, 2nd National CERT Meeting, 2007.6, Madrid

New Solution on New Threat: Learning from Botnet Incident Handling, MCMC 2nd Industry Talk, 2007.2, Malaysia

CNCERT/CC Annual Report 2006, APCERT 2007 Conference, 2007.2.7-9, Malaysia

Further Information Sharing on Botnet, APCERT 2007 Conference, 2007.2.7-9, Malaysia

Distributed Honeynet & Info Sharing on Malicious Server, CJK InfoSec WG 2007 meeting, 2007.5, Beijing.

12 monthly newsletters, 1 semiyearly special (in Chinese) were issued for high-end users in 2007.

4.2 Criteria

CNCERT/CC published “Incident Object Description and Exchange Format Criteria” (Chinese-edition).

5 International Cooperation

5.1 MoU

On June 14, 2007, CNCERT/CC signed Security Cooperation Protocol (SCP) with Microsoft China Corporation in Beijing.

5.2 Conference and Events

APCERT 2007 Annual Conference
CNCERT/CC delegation attended APCERT annual conference in Malaysia and was elected as the deputy chair of APCERT again.

4 CERTs Site Visit
During July 10-22, 2007, CNCERT/CC delegation visited VNCERT, LaoCERT, mmCERT and CamCERT successively.

ACID II 2007
CNCERT/CC participated in ACID II on 16th, July 2007.

APCERT Drill 2007

CNCERT/CC participated in the 4th APCERT incident handling drill on 21st, November 2007. CNCERT/CC appreciated that the Drill's scenario had been designed with Beijing 2008 Olympic Games as the background.

6 Future Plans

In 2008, Internet security during Beijing 2008 Olympic Games is the top priority to CNCERT/CC, who will play an important role then. Therefore, CNCERT/CC expects to keep a stronger collaboration with APCERT members.

7 Conclusion

In 2007, the overall security status of Internet in China mainland was relatively calm in general. There was no large-scale network security incident happened with mass damage. With the Beijing 2008 Olympic Games upcoming, potential security risks and threats is increasing greatly. The possibility of large-scale network security incidents occurring cannot be neglected at the moment. Thus, it is necessary for government, ISPs, internet users, and so on, to pay much more attention and cooperate with one another more effectively. CNCERT/CC is also in need of the collaboration with CERTs community from all over the world to prevent and mitigate the impact of any cyber threat compromising Beijing 2008 Olympic Games.