CNCERT/CC Annual Report 2008

（English Edition）

TABLE OF CONTENTS

1. About CNCERT/CC

1.1. Introduction

CNCERT/CC is a National level CERT organization, which is responsible for the coordination of activities among all Computer Emergency Response Teams within China concerning incidents in national public networks.

1.2. 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.

1.3. 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.

1.4. 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 2008, CNCERT/CC received 5,167 incidents reports (excluding scanning attacks) from domestic and international users and agencies.

Most incident reports were about spam mail (1,849), phishing (1,256) and webpage embedded malicious code (1,227). The reports of these 3 types of incident were increased by 54.5%, -5.3% and 6.6% compared with that of last year respectively.

2.2. Incident Handling

In 2008, CNCERT/CC handled 1,173 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 5 applications of TCP traffic are among HTTP, P2P and email.

TCP Port	Rank	Percentage	Applications
80	1	28.36%	HTTP
8080	2	1.00%	HTTP
4662	3	0.93%	eMule
443	4	0.80%	Https
25	5	0.60%	SMTP
554	6	0.25%	RTSP
3128	7	0.23%	HTTP
8000	8	0.18%	QQ IM

1863	9	0.18%	MSN Messenger
6881	10	0.10%	BitTorrent

Table 1 TCP Traffic Top 10 in 2008

The top 3 applications of UDP traffic are Xunlei, QQ and QQ IM (Instant Messenger).

UDP Port	Rank	Percentage	Applications
15000	1	3.70%	Xunlei (downloader)
29909	2	1.02%	QQ(downloader)
8000	3	0.94%	QQ IM
80	4	0.84%	Http
53	5	0.74%	DNS
1026	6	0.65%	MSN Messenger
7100	7	0.63%	Online Game
6881	8	0.63%	BitTorrent
1027	9	0.49%	MSN Messenger
4672	10	0.42%	eMule

Table 2 UDP Traffic Top 10 in Year 2008

Trojan & Botnet Monitoring

In 2008, CNCERT/CC monitored some popular Trojans and discovered 565,605 IP addresses of computers embedded with Trojans in Chinese mainland, which decreased by 43.2% compared with that of year 2007.

CNCERT/CC also kept on monitoring Botnet activities for a long time. In 2008, CNCERT/CC discovered over 1,237,043 IP addresses of computers embedded with Botnet clients in Chinese mainland. Meanwhile, 5,210 Botnet servers outside of Chinese mainland were discovered controlling Botnet clients in Chinese mainland. Among these Botnet servers, about 31% were in the United States, 10% in Hungary and 5% in South Korea.

Among ports used by Botnet based on IRC application, the top 3 ports are 6667 (41.39%), 8080 (3.64%) and 1863 (3.17%).

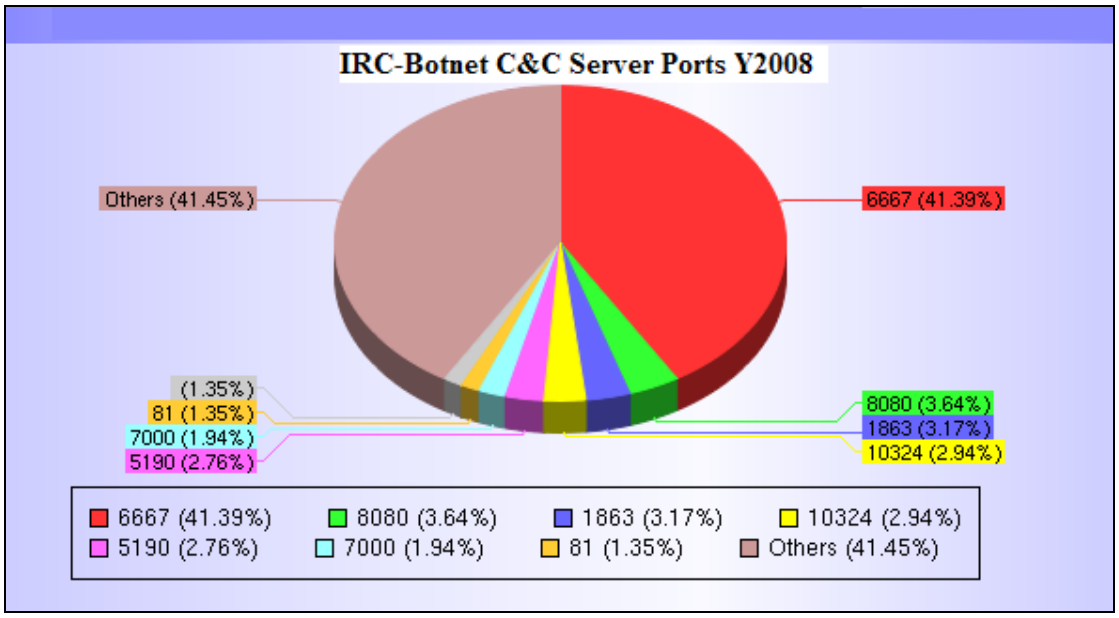

Figure 1 IRC-Botnet C&C Server Ports Year 2008

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 2008, CNCERT/CC discovered totally 53,917 defaced websites in Chinese mainland, which is decreasing slightly compared with that of year 2007. According to monitoring data, the governmental websites seem to be much easier to be attacked due to their weak protection measures and maintenance.

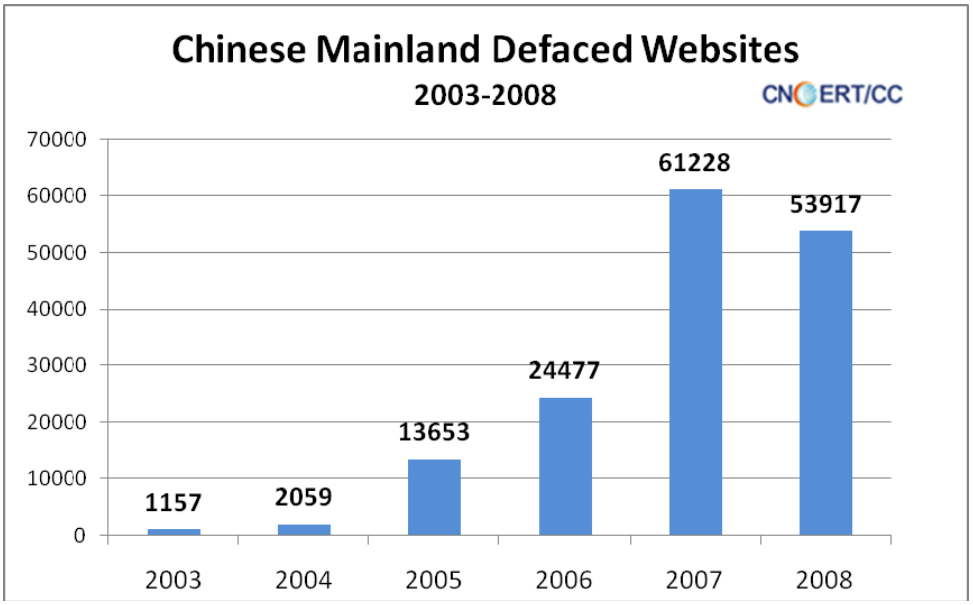

Figure 2 Chinese Mainland Defaced Websites Y2003-2008

Phishing Handling

In 2008, CNCERT/CC received 1,256 phishing reports and resolved 320 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
eBay	248
ACK CYFRONET AGH	125
HSBC	120
Mark Monitor	61
RSA Cyota	48

Table 3 Top 5 Phishing Reporters to CNCERT/CC in Year 2008

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 4,488 in 2008.

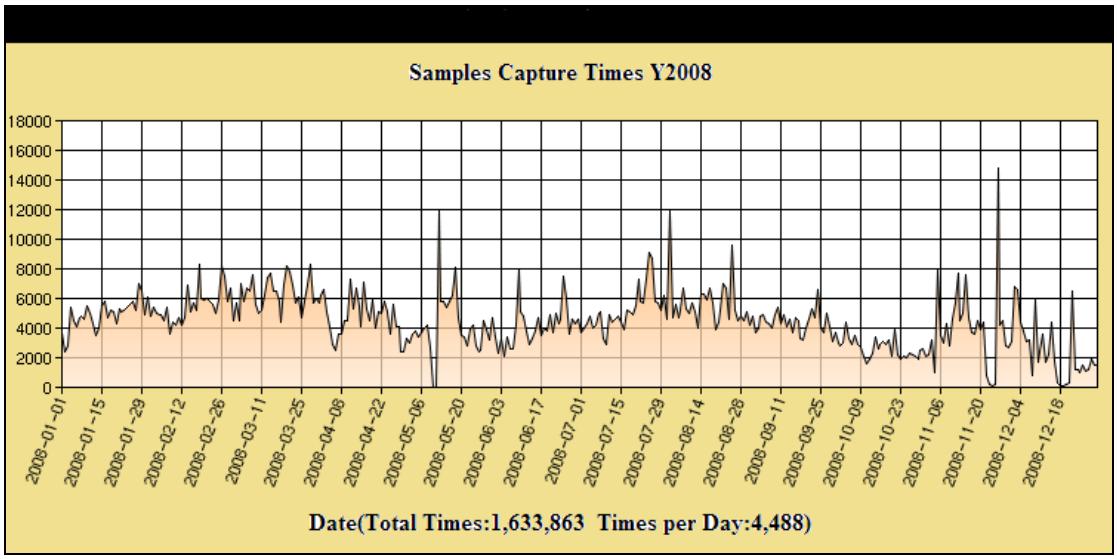

Figure 3 Samples Capturing Times Status

According to the data, the average number of new samples captured everyday is 427. That means new malicious codes were emerging endlessly.

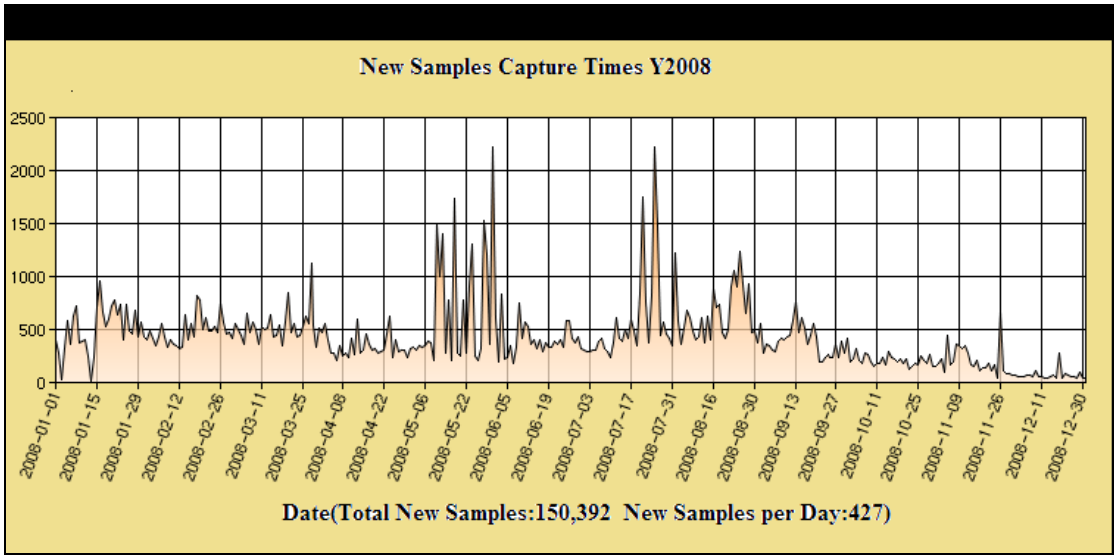

Figure 4 Number of Samples Captured Status

In 2008, 150,392 samples had been captured by CNCERT/CC's honeynet.

Rank	Malicious Code Name	Times of being Captured
1	Virus.Win32.Virut.n	111584
2	Backdoor.Win32.VanBot.ax	62219
3	Net-Worm.Win32.Allaple.b	48933
4	Trojan.Win32.Obfuscated.gen	43411
5	Backdoor.Win32.Nepoe.em	37284
6	Net-Worm.Win32.Allaple.e	27520
7	Backdoor.Win32.Rbot.bqj	24781
8	Porn-Dialer.Win32.InstantAccess.dan	24649
9	Trojan-Downloader.VBS.Small.gg	22216
10	Trojan.Win32.Qhost.aei	22153

Table 4 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 2008, 101 internal warnings and 4 critical vulnerability advisories had been delivered in time.

277 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

Anti-Botnet Seminar

The Seminar was held in Beijing on 23rd January 2008. Delegates came from governments, security research organizations, vendors and end users. The topic is to exchange information regarding to the threat and the trend of Botnet, share best practices and main difficulties, and discuss how to combat Botnet from the technical, regulatory, legal and other aspects.

APEC-TEL37 Anti-Botnet Workshop

The workshop was held on 23rd March 2008 at APEC-TEL37 in Tokyo. 12 experts gave the presentations to share their experiences and skills regarding to Botnet. The workshop provided an atmosphere that encourages the sharing of knowledge and experiences of effective solutions for preventing, detecting and controlling botnets.

CNCERT/CC 2008 Annual Conference

The Conference was held in Shenzhen from 7th to 9th April 2008. About 300 delegates from 12 countries and regions attended the conference.

CNCERT Cyber-security Training Camp

The training camp was held on 8th to 9th May 2008 in Beijing assisted by Microsoft. This activity invited about 30 trainees from critical information infrastructures and backbone ISPs to learn Windows OS enhanced security technologies, network attack technologies and tools, hacking habits, and network security attack and defense drills in simulated scenarios.

Accreditation for Domestic Qualification of Information Security Service Provider

CNCERT/CC completed the authorization for Domestic Qualification of Information Security Service Provider in June 2008, co-sponsored by China Information Security Certification Center (ISCCC).

Internet Security Work during Beijing 2008 Olympic Games

In cooperation with other relevant government departments and ISPs, the network of China mainland during the Beijing 2008 Olympic Games was running well smoothly with no major security incidents. CNCERT/CC completed the network security mission successfully.

4. Achievement

4.1. Presentation

Matrix, a Distributed Honeynet and its Applications, APCERT 2008 Annual Conference, 2008.3.10-12, Hong Kong China

Botnet Mitigation Practice in China, Anti-Botnet Workshop in APEC-TEL37, 2008.3.23, Japan

Matrix, a Distributed Honeynet and its Applications, Annual FIRST Conference 2008, 2008.6.22-27, Canada

Malicious Websites on the Chinese Web: Overview and Case Study, Annual FIRST Conference 2008, 2008.6.22-27, Canada.

Final Report of Anti-Botnet Report, APEC-TEL38, 2008.10.16, Peru

4.2. Publication

Best Practices & Guides on Network Security Emergency Response (in Chinese, ISBN: 978-7-121-06194-3), published and issued in March, 2008

Guide on Policy and Technical Approaches against Botnet, publicized on APEC Website in Dec. 2008

12 monthly newsletters, 1 semiyearly special (in Chinese) for high-end users in 2008

5. International Cooperation

5.1. Conference and Events

APCERT 2008 Annual Conference
CNCERT/CC delegation attended APCERT annual conference in Hong Kong and was elected as the deputy chair of APCERT again.

ACID III 2008
CNCERT/CC participated in ACID III on 30th July 2008.

APCERT Drill 2008
CNCERT/CC participated in APCERT incident handling drill on 4th December 2008.

6. Future Plans

CNCERT/CC completed the Internet security mission during the Beijing 2008 Olympic Games successfully. In the approaching 2009, CNCERT will continue to enhance its own capability of network monitoring, warning and handling as a national Computer Emergency Response Team. Therefore, we expect to keep a stronger collaboration with APCERT members.

7. Conclusion

In 2008, 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. Before the Beijing 2008 Olympic Games, CNCERT/CC took two special actions to restrain the increasing security risks and threats of Botnet and Trojan in cooperation with other government departments and ISPs. The actions play an important role in the healthy internet environment in China. Importantly, CNCERT/CC got much supports from the collaboration with CERTs community from all over the world to prevent and mitigate the impact of cyber threat in 2008.