CNCERT/CC Annual Report 2010

（English Edition）

TABLE OF CONTENTS

1. ABOUT CNCERT 2

1.1. INTRODUCTION 2
1.2. ESTABLISHMENT 2
1.3. WORKFORCE POWER 2
1.4. CONSTITUENCY & ETC 2

2. ACTIVITIES & OPERATIONS 2

2.1. INCIDENT HANDLING REPORTS 2
2.2. ABUSE STATISTICS 3
2.3. NEW SERVICES 5

3. EVENTS ORGANIZED/CO-ORGANIZED 5

3.1. TRAINING 5
3.2. DRILLS 5
3.3. SEMINARS & ETC 5

4. ACHIEVEMENTS 6

4.1. PRESENTATION 6
4.2. PUBLICATION 7
4.3. CERTIFICATION & ETC 7

5. INTERNATIONAL COLLABORATION 7

5.1. MOU 7
5.2. CONFERENCES AND EVENTS 7

6. FUTURE PLANS 8

6.1. FUTURE PROJECTS 8
6.2. FRAMEWORK 8
6.3. ETC 8

7. CONCLUSION 8

1. About CNCERT

1.1. Introduction

CNCERT is a National level CERT organization, which is responsible for the coordination of activities among all CERTs within China concerning incidents in national public networks.

1.2. Establishment

CNCERT was founded in Oct., 2000, and became a member of FIRST in Aug 2002. CNCERT took an active part in the establishment of APCERT as a founding member.

1.3. Workforce power

CNCERT, 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 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.

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 handling reports

In 2010, CNCERT received 10,433 incidents reports[1] and 5070 of them were from international users and agencies. Most incident reports were about vulnerability (33.04%), malicious code (29.61%), webpage malicious code (21.35%) and phishing (15.01%).

In 2010, CNCERT handled 3,236 incidents. Malicious code (1,463), Webpage malicious code (649), phishing (631) and web defacement (410) were 4 main incidents handled.

[1] In 2010, CNCERT had not estimated spam incident reports in its data collection, instead, suggested users turn to Anti-spam center of ISC for incident report. Meanwhile, CNCERT sent all related reports to Anti-spam center for them to handle.

TOP 10 Phishing Reporters	
From	Number
s21sec.com	196
ebay.com	125
hsbc.com.cn	110
brandprotect.com	107
phishlabs.com	106
bradesco.com.br	86
cert.br	62
telefonica.es	61
irs.gov	58
rsa.com	57

TOP 10 Phishing Targets	
Target	Number
bbva.com	170
ebay.com	134
bradesco.com.br	127
Hsbc.com.cn	115
I irs.gov	73
wachovia.com	71
alliance-leicester.co.uk	57
Icbc.com.cn	51
cctv.com	51
ceca.es	37

2.2. Abuse Statistics

Trojan & Botnet Monitoring

According to CNCERT's sample monitoring, in 2010, there were 479,626 IPs of Trojan C&C server discovered with 21.3% reduction compared with 2009, and 10,317,169 IPs of Trojan clients discovered with a big increase of 274.9% than 2009.

Meanwhile, about 220,000 IPs of Trojan C&C servers were outside of Chinese mainland. Top 3 countries or regions are USA, India and Taiwan China.

As for Botnet, there were about 14,000 IPs of Botnet C&C server discovered with 39.6% reduction than 2009, and about 5,620,000 IPs of Bot discovered with 52.% reduction. Meanwhile, 6,531 IPs of Botnet C&C servers were outside of Chinese mainland. Top 3 countries or regions are USA, India and Turkey. In general, the size of IRC Botnets is going on to become smaller, localized and specialized. The Botnet with less than 1,000 bots is much more favorable to attackers.

Conficker Monitoring

By Dec 2010, there was over 60,000,000 IPs of computer infected with Conficker in the world. China mainland was still No.1‘severe disaster area’ with over 9,000,000 IPs of infected computer. Other severe disaster area includes USA(15%) and Brazil(7%).

Stuxnet Worm Monitoring

As the first worm infecting industrial controlling system, Stuxnet caused a world wide concerning in 2010. By the end of 2010, 578 IPs of computers have been infected in China mainland. The number is very few if comparing with other normal worms.

Mobile Virus Monitoring

In 2010, CNCERT discovered that there had been 2,003,515 cell phones infected with ‘DuMusicPlay’, 831,843 cell phones infected with ‘Skulls’, 216,147 infected with ‘FC.MapUp.A’ and 1431 infected with ‘Boothelper.A’.

Symbian was still the primary target for mobile virus and more than 69% mobile viruses compromised Symbian OS cell phone. J2ME(27%) was the second largest infected target. Android (3%) ranked No.3 and kept a fast growth.

Web Defacement Monitoring

In 2010, CNCERT discovered about 34,845 defaced websites in China mainland. 4,635 are governmental websites, a large proportion.

Malicious Domain Name Monitoring

In 2010, top 10 malicious domain names are as follows.

Rank	Domain Name
1	www.w22rt.com
2	annil.8866.org
3	a.ppmmoo.cn
4	lsrc.cn
5	vod123.8866.org
6	ferrari10.7766.org
7	jjeffyfc19.info

Rank	Domain Name
8	web.9bic.net
9	ghtoto.3322.org
10	ada.bij.pl

2.3. New services

In 2010, CNCERT had put more effort into the establishment of CNVD[2] and ANVA[3], which are 2 platforms for information sharing among all related members, aiming to provide constituency and users with richer information and data. Besides public information services, CNCERT also delivered more customized information reports to its contracted users.

Large event network security assistance is always the task of CNCERT. CNCERT provided monitoring and alert services for EXPO 2010 in Shanghai and 16th Asia Games in Guangzhou.

3. Events organized/co-organized

3.1. Training

N/A

3.2. Drills

APCERT 2010 Drill held on 28 Jan 2010, as the organizing committee member with HKCERT and MyCERT.

3.3. Seminars & Etc

Seminar on Network Security Terminology
The Seminar was held in Beijing, 23 Mar 2010, aiming to regulate the terminology of network security and make common sense among IT organizations.

Press Conference on 2009 China Netizen Network Security Investigation Report
The meeting was held in Beijing, 30 Mar 2010.

2010 CNVD[4] Spring Working Conference
The meeting was held in Beijing, 20 Apr 2010.

2010 ANVA[5] Working Conference
The meeting was held in Beijing, 6 Aug 2010.

[2] China National Vulnerability Database
[3] Anti-Network Virus Alliance
[4] China National Vulnerability Database
[5] Anti-Network Virus Alliance

September 2010 FIRST Technical Colloquium & CNCERT Annual Conference

The Conference was held in Beijing from 12 to 14 Sep 2010. Nearly 400 delegates from 10 countries and regions attended the conference. Mr. Yang Xueshan, the Minister of the Ministry of Industry and Information Technology of PRC addressed on the plenary meeting. This event was open to FIRST members and invited guests. It's a three day event comprising of 1 day hands-on workshop, 1day plenary meeting and 1 day breakout sessions.

For the hands-on workshop on 12th, there were 6 hands-on sessions and 6 instructors from FIRST members. Totally about 151 people attended the classes. For the plenary meeting on 13th and breakout sessions on 14th, 41 speakers delivered the speeches or presentations. 3 topics of high-level panel discussions were included in the plenary meeting. At the same time, 7 exhibition booths were provided for all delegates to visit on site.

China-USA Network Security Dialog Ongoing

Since Mar 2010, CNCERT had already organized 14 conferences on China-USA Network Security Dialog Mechanism Anti-spam Subject including both parties' face-face conferences, teleconferences and China side internal conferences. Members of China side are from Anti-spam Center of ISC, Beijing Post & Telecommunication University, China Telecom, China Unicom, Sina, Netease, 263.com, Tencent, HiChina, NSFocus and etc. Members of USA side are from Switch NAP、Google、 Northrop Grumman、Bell Labs、Comcast Cable Communications、VeriSign、Pennsylvania State University、George Washington University、CERT at CMU Software Engineering Institute、AT&T、Global Cyber Risk、San Jose State University、Cox Communications and etc. By the end of 2010, both parties had completed a draft on Anti-spam Proposal Joint Report based on sufficient view exchange.

4. Achievements

4.1. Presentation

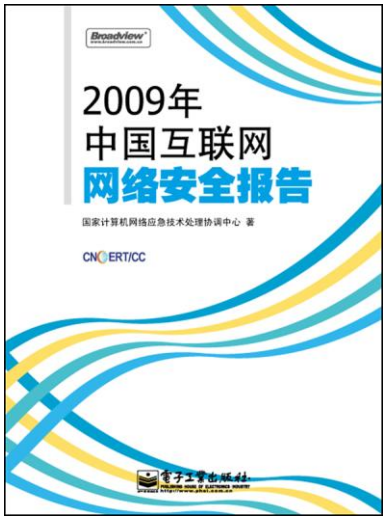
Network Threat VS Financial & Economic Security, 7th Worldwide Security Conference, Belgium, Feb 2010

CNCERT Activity Update & China-Japan Cooperation Proposal, China-Japan ICT & Industrial Policy Seminar, Beijing China, Apr 9 2010

China Update on Network Security Activity, 41st/42nd APEC-TEL Conferences, May/Aug 2010.

China Update on Internet Situation Awareness, 2nd Microsoft Anti Digital Crime Cooperation Conference, Montreal Canada, Oct 12-15 2010.

4.2. Publication



"2009 China Internet Security Report" (in Chinese, ISBN: 9787121115646).

4.3. Certification & Etc

By Dec 2010, as the Network Security Information Notification Center of Communication Industry, CNCERT had already built up a stable information notification working systems with 262 working units.

As the operation and administration organization, CNCERT developed 25 CNVD members and 22 ANVA members since its establishment in 2009.

5. International Collaboration

5.1. MoU

N/A

5.2. Conferences and Events

22nd Annual FIRST Conference
CNCERT delegation attended the FIRST Conference in Miami, USA, June 13-18 2010.

ACID 2010
CNCERT participated in ACID 2010 on 21 Sep 2010.

China-ASEAN Telecommunication Regulation Round Table Symposium
CNCERT participated in the Symposium in Vietnam, July 8 2010.

6. Future Plans

6.1. Future projects

N/A

6.2. Framework

6.2.1. Future operation

To better handle cross border incidents and exchanging necessary important information, CNCERT/CC is going to update or sign MOUs with more CERTs/CSIRTs teams around the world.

6.2.2. Tracking

Conficker worm, Mobile virus, and Stuxnet worm.

6.3. Etc

N/A

7. Conclusion

In 2010, the national Internet infrastructure generally ran good, and the level of network security got improved significantly. There was no severe security event like 5.19 event in 2009 (several provincial Internet failure) happened.

Baidu event tell us that the domain name systems security was relatively weak. 3Q event (conflict between 360.cn and QQ) indicates that there was urgent need to strengthen privacy protection for users, regulation on Internet value-added services competition and supervision/administration of Internet value-added service providers' network security. Government website security remains weak and vulnerable. Large E-commerce websites, large financial websites, third-party online payment websites and large social networking websites became the main target of online fraud. Industrial control systems faced new challenges because of Stuxnet worm.

Continuous efforts of combating Trojan horse and botnet resulted in public network environment improved. DoS attack shows 2 signs of transferring and large amount of flow. Some underground game service websites redirected its domain name to those large public websites to avoid attacks. More and more large-flow DDoS attacks increasingly became the serious threat to Internet infrastructure and important online applications, so it is recommended for the communication industry to further improve source address authentication mechanism.

Mobile virus grows fast, spreads wide, and harms big. Mobile Internet network environment should be in good governance urgently. More and more high-risk

vulnerabilities exposes out of network devices, operating systems, server systems, database software, application software and even security products. Base on CNVD 2010 vulnerabilities statistics, top 3 types of vulnerability are on application software (62%), operating system (16%) and Web application (9%).

Cross-border network security incidents have become increasingly prominent. Attackers are very fond of utilizing foreign resources to implement attacks, which calls for more international cooperation.