CNCERT/CC Annual Report 2012

National Computer network Emergency Response technical Team / Coordination Center of China – People's Republic of China

1. About CNCERT

CNCERT or CNCERT/CC is the National CERT organization of China, which is serving as a national-level network security monitoring center, warning center and emergency handling center. It provides supports to the governmental departments for fulfilling their network security-related social management and public service functions, ensures the safe operation of national information infrastructures and undertakes the network security monitoring, early warning and emergency response of control systems. Branches of CNCERT spread in 31 provinces, autonomous regions and municipalities in mainland China.

Contact us

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

In 2012, CNCERT received a total of about 19 thousand incident complaints, a 24.5% increase from the previous year. And among these incident complaints, 1,200 were reported by overseas organizations, making a 42.9% drop from the year of 2011. As shown in Figure 2-1, most of the victims were plagued by phishing (49.5%), vulnerability (39.4%) and malware (5.4%). Different from the previous year, phishing overtook vulnerability to become the most frequent incident complained about. And malware still ranked the third place with a considerable decrease of 71.2% from 2011 because of CNCERT's Trojan and Botnet clean-up

campaigns in 2012.

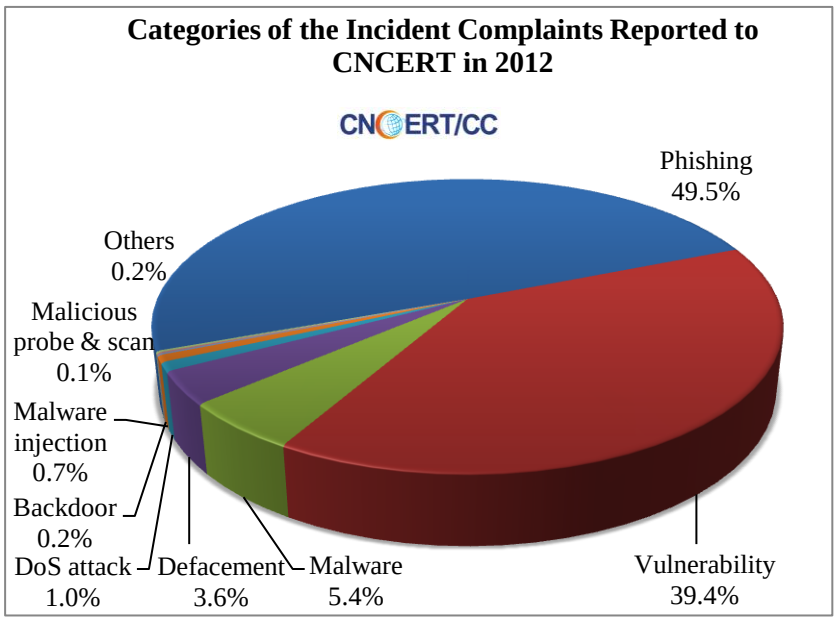

Figure 2-1 Categories of the Incident Reported to CNCERT in 2012

In 2012, CNCERT handled almost 19 thousand incidents, a significant rise of 72.1% compare with that in 2011. Besides, CNCERT has carried out 14 clean-up campaign against Trojans and Botnets as well as 6 clean-up campaigns against mobile malware in 2012. As illustrated in Figure 2-2, vulnerability (40.7%) dominated the categories of the incidents handled by CNCERT In 2012, followed by phishing (35%) and website defacement (11.7%).

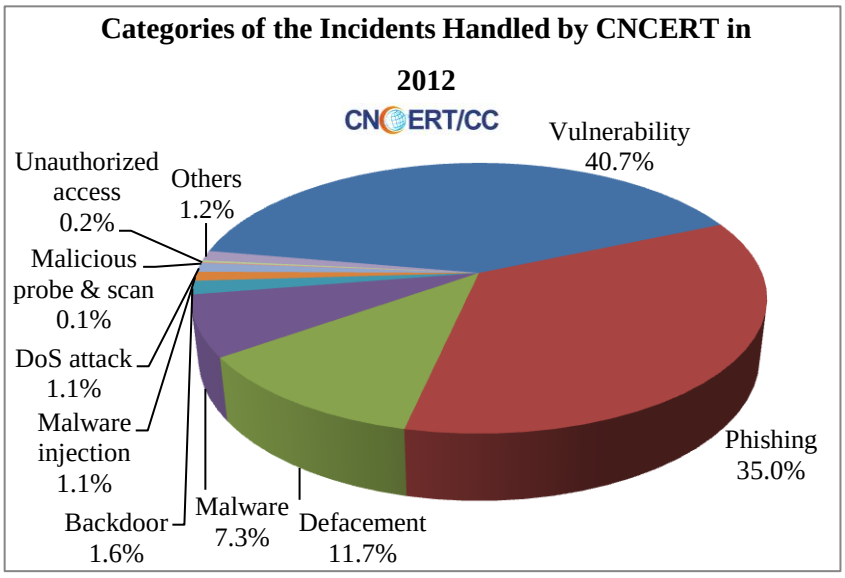

Figure 2-2 Categories of the Incidents Handled by CNCERT in 2012

2.2 Internet Monitoring

2.2.1 Compromised Hosts and Websites

In 2012, CNCERT monitored and discovered about 7.4 million incidents spreading known-type malware, which involved about 7 thousand domain names, about 8 thousand IP addresses and 38 thousand malware download links. Figure 2-3 depicts the monthly statistics of malware spreading incidents in 2012, with the most rampant malware activity in June.

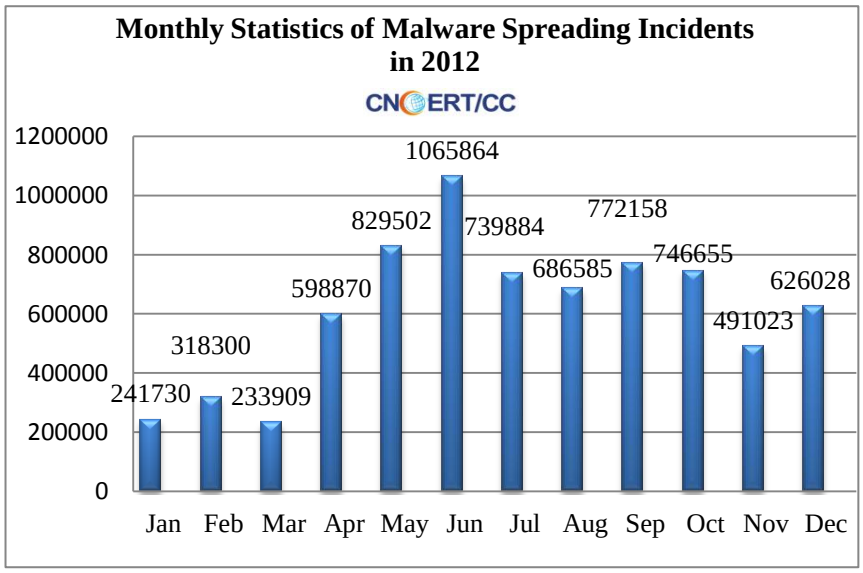

Figure 2-3 Monthly Statistics of Malware Spreading Incidents in 2012

In mainland China, IPs of the hosts infected with Trojan or Botnet reached about 14 million, which increased by 64.7% compared with that in 2011.

By CNCERT's Conficker Sinkhole system, over 28 million hosts per month on average were suspected to be infected all over the world. And 3.25 million compromised hosts per month were located in mainland China. As shown in Figure 2-4, mainland China (14.3%) had the most infection, followed by Brazil (10.9%), and Russia (6.5%).

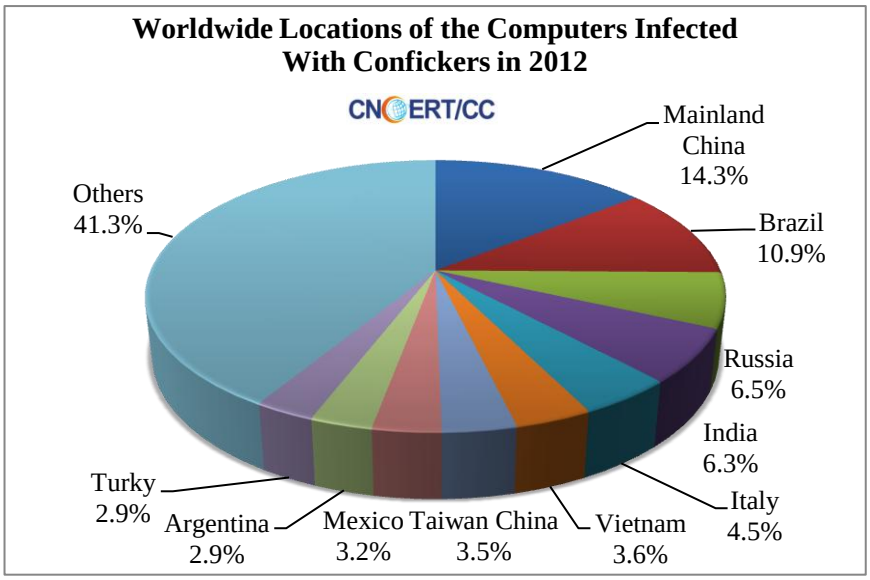

Figure 2-4 Worldwide Locations of the Computers Infected With Confickers in 2012

About 16 thousand websites in mainland China were defaced, a slight increase of 6.1% compare with that in 2011, including 1802 government sites. Besides, about 52 thousand websites were detected to be planted with backdoors and secretly controlled, including 3016 government sites.

2.2.2 Location of Malicious IPs

Because CNCERT's monitoring systems are all located in mainland China, most IPs of Trojan or Botnet C&C servers we detected were identified in local networks. But we still saw more than 73 thousand oversea C&C servers which increased 56.9% from 2011. The USA hosted the largest number of oversea Trojan or Botnet C&C servers' IPs, followed by Japan and Taiwan China.

In 2012, CNCERT detected about 22 thousand phishing sites targeting the banks in mainland China. About 2576 IPs were used to host those fake pages. 3.8% of those IPs were in mainland China and 96.2% were out of mainland China. The USA network hosted most of the phishing servers (80%).

CNCERT detected almost 58 thousand backdoor control IPs. Besides about 26 thousand were located in mainland China, 7370 (12.8%) were located in

the USA, followed with 4362 (7.6%) in Taiwan China and 2590 (4.5%) in HongKong China.

2.3 Mobile Internet Monitoring

In 2012, CNCERT captured and collected about 163 thousand mobile malware samples in total. In terms of intentions of these mobile malware, the malicious fee-deducting malware continued to take the first place (39.8%). Rogue malware (27.7%) rose to the second place. And followed it were those intended for fee consumption and remote control, accounting for 11% and 8.5% respectively.

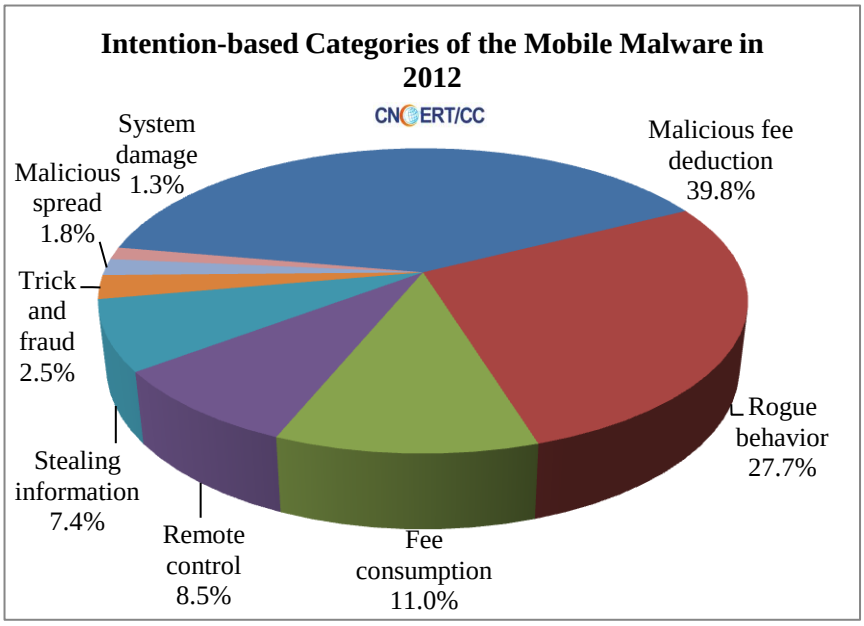

Figure 2-5 Intention-based Categories of the Mobile Malware in 2012

The majority of these mobile malware identified by CNCERT ran on Android and Symbian platform, recording about 134 thousand (82.5%) and about 28 thousand (17.5%) respectively.

3. Events organized/co-organized

3.1 Conferences

CNCERT 2012 Annual Conference

CNCERT organized CNCERT 2012 Annual Conference-"Build up Secure and Harmonious Network Environment" from 3rd to 5th July 2012 at Xi'an city, Shannxi province, China. Four tracks were designed for subject

presentations at the annual conference, including New Challenge and New technology, Vulnerabilities and Personal Information Protection, E-Government and Important Information System Security, and Analysis on Underground Industry and Corresponding Response.

Press Briefing of Report on 2011 China Network Security Landscape

CNCERT hosted the Press Briefing of Report on 2011 China Network Security Landscape on 19 March 2012 in Beijing which attracted 50 experts from over 40 relevant organizations. The report summarized new trends and features of network security in China in 2011 and predicated security trends in 2012 with some countermeasures offered.

4. Achievements

CNCERT's weekly, monthly and annual reports, as well the other released information, were reprinted and quoted by massive authoritative media and thesis home and abroad.

Figure 4-1 lists of CNCERT's publications throughout 2012

Name	Issues	Description
Weekly Report of CNCERT (Chinese)	52	Emailed to over 430 organizations and individuals and published on CNCERT's Chinese-version website (http://www.cert.org.cn/)
Weekly Report of CNCERT (English)	52	Emailed to relevant organizations and individuals and published on CNCERT's English-version website (http://www.cert.org.cn/english_web/documents.htm)
CNCERT Monthly Report on Internet Security Threats (Chinese)	12	Issued to over 400 organizations and individuals on regular basis and published on CNCERT's website (http://www.cert.org.cn/)
Annual Report on Network	1	Published on CNCERT's website

Security (Chinese)		(http://www.cert.org.cn/)
CNVD Vulnerability Weekly Report (Chinese)	52	Published on CNCERT's website (http://www.cert.org.cn/)
Articles Analyzing Network Security Data	24	Published on journals and magazines.

5. Conferences attended & speeches delivered

APCERT 2012 Drill-"Advance Persistent Threats and Global Coordination",

CNCERT participated in the APCERT 2012 Drill -"Advance Persistent Threats and Global Coordination" as a participant on 29 January 2012 and completed it successfully.

1ST China and Korea Internet Roundtable-"Development and Cooperation"

CNCERT took part in the First Internet Roundtable between China and Korea which was kicked off on 5 December 2012 in Beijing. This two-day conference covered the Internet economy, network infrastructure construction and cybercrime. At the conference, CNCERT presented a report on landscape of China internet security and countermeasures, as well as exchanged views on international cooperation on network security and other issues with the Korean delegates.

2012 APCERT Annual Conference-"Cleaning the Cyber Environment"

Four Delegates from CNCERT attended the APCERT Annual General Meeting and Conference 2012 which was held from March 25 to 28 in 2012 in Indonesia with the theme of "Cleaning the Cyber Environment". At the conference, CNCERT introduced its network security services in 2012, and gave a keynote speech of "New Challenges to Security of the Public Network Environment" as invited.

The 45th Meeting of APEC Telecommunications and Information Working Group

From 5th to 11th April 2012, CNCERT attended the 45th Meeting of APEC Telecommunications and Information Working Group (APEC TEL 45) held

in Da Nang city, Vietnam. At the meeting, the Chinese delegates introduced their efforts and achievements in improving the internet security, shared experience and methods in incident handling and information sharing.

ARF Workshop on Cyber Incident Response

CNCERT, together with 59 delegates from 17 countries, took part in the ARF (ASEAN Regional Forum) Workshop on Cyber Incident Response in Singapore from 6th to 8th September 2012. The CNCERT delegate presented a speech focusing on vulnerabilities of the industry controlling system and DDoS attacks.