CNCERT/CC Annual Report 2017

National Computer Network Emergency Response Technical Team / Coordination Center of China – People's Republic of China

1. About CNCERT

1.1 Introduction

The National Computer Network Emergency Response Technical Team/Coordination Center of China (known as CNCERT or CNCERT/CC) is a non-governmental non-profit cybersecurity technical center and the key coordination team for China's cybersecurity emergency response community.

1.2 Establishment

CNCERT was founded in 2002, and became a member of FIRST in Aug the same year. It also took an active part in the establishment of APCERT as a founding member.

1.3 Workforce power

CNCERT, which is based in Beijing, the capital of China, has spread branch offices in 31 provinces, autonomous regions and municipalities in mainland China.

1.4 Constituency

As a national CERT, CNCERT strives to improve the nation's cybersecurity posture and protect critical infrastructure cybersecurity. CNCERT leads efforts to prevent, detect, warn and coordinate cybersecurity threats and incidents, pursuant to the guideline of "proactive prevention, timely detection, prompt response and maximized recovery".

1.5 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

In 2017, CNCERT received a total of about 103.4 thousand incident complaints, a 17.7% decrease from the previous year. And among these incident complaints, 481 were reported by overseas organizations, making a 1.5% rise from the year of 2016. As shown in Figure 2-1, most of the victims were plagued by vulnerabilities (33.9%), phishing (24.3%) and malware (21.8%). Vulnerabilities overtook phishing to be the most complained about category.

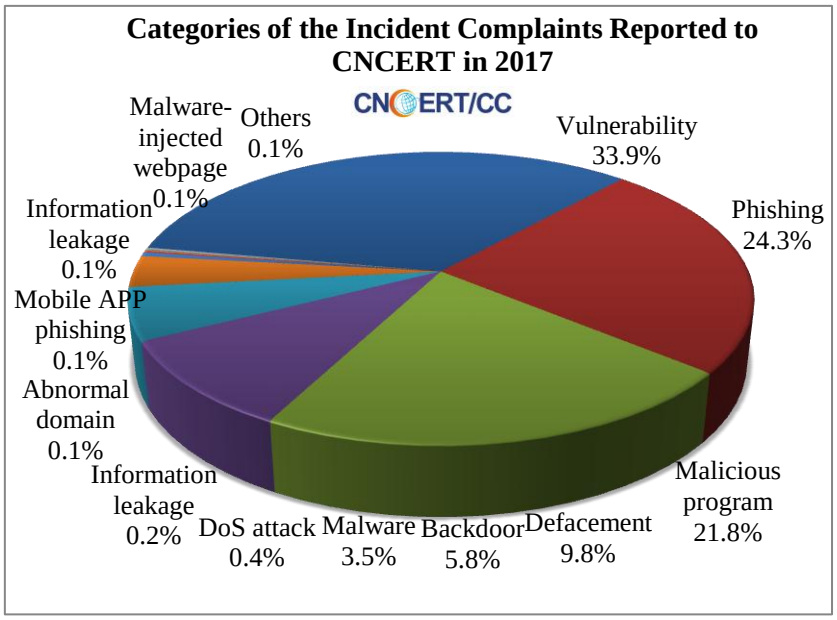

Figure 2-1Categories of the Incident Complaints Reported to CNCERT in 2017

In 2017, CNCERT handled almost 103.6 thousand incidents, a drop of 17.7% compared with that in 2016. As illustrated in Figure 2-2, vulnerabilities (33.9%) dominated the chart about categories of the incidents handled by CNCERT in 2017, followed by phishing (24.3%) and malware (21.7%).

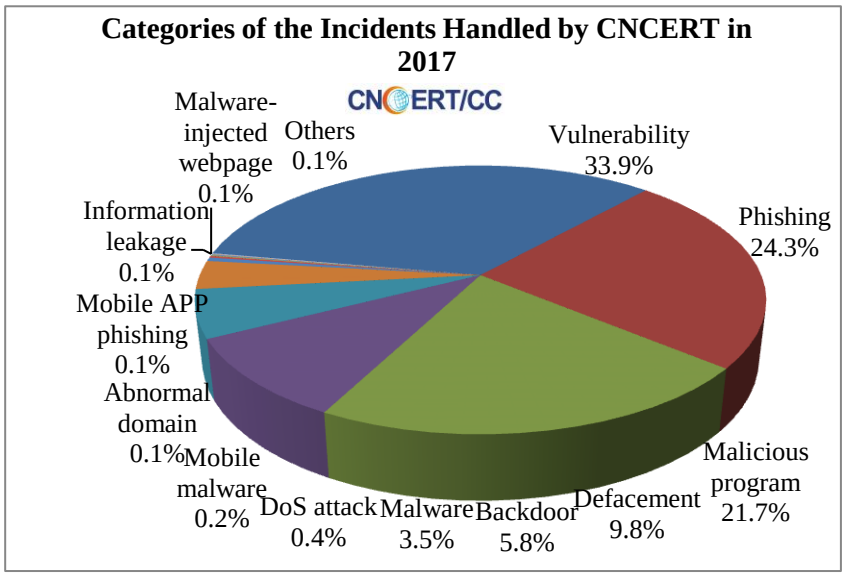

Figure 2-2 Categories of the Incidents Handled by CNCERT in 2017

2.2 Internet Threats

2.2.1 Malware Activities

In mainland China, IPs of the hosts infected with Trojan or Botnet reached about 12.6 million, which decreased by 26.1% compared with that in 2016. We saw more than 47.3 thousand overseas C&C servers which decreased by 1.2% from 2016. As shown in Figure 2-3, the U.S. hosted the largest number of overseas C&C servers' IPs of Trojan or Botnet, followed by Japan and Russia.

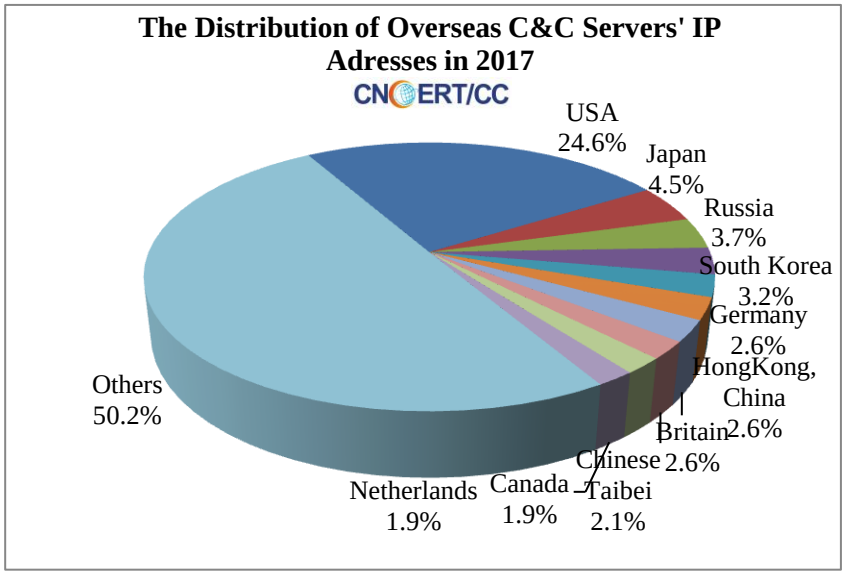

Figure 2-3 Distribution of overseas C&C servers' IP addresses in 2017

By CNCERT's Conficker Sinkhole, over 24.3 million hosts were suspected to be compromised all over the world, among which 3.8 million were located in mainland China. As shown in Figure 2-4, mainland China (15.5%) had the most

infection, followed by India (8.3%), and Brazil (5.2%).

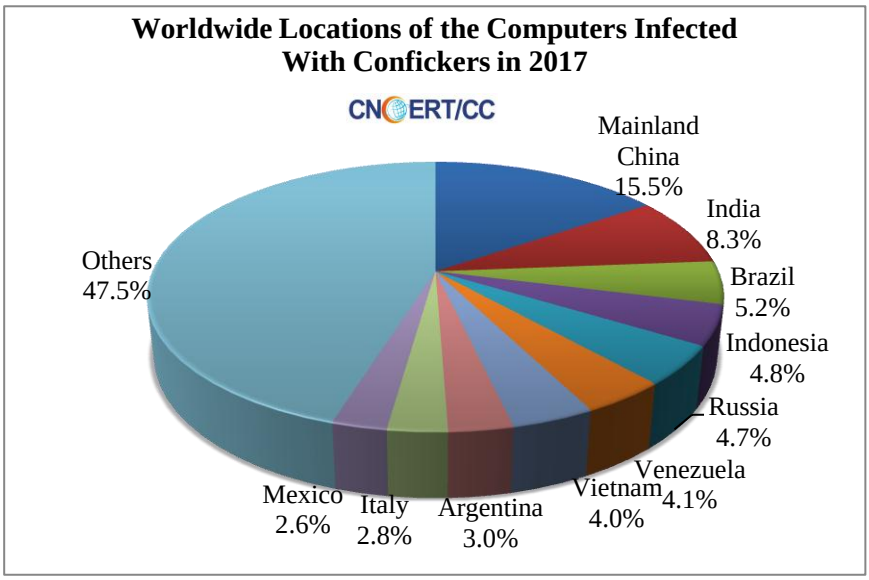

Figure 2-4 Worldwide Locations of the Computers Infected with Conficker in 2017

Malware-hosting websites are the jumping-off places for malware propagation. The malware-hosting websites monitored by CNCERT in 2017 involved about 10.0 thousand domains, 2.7 thousand IP addresses and 79.8 thousand malware download links. Among the 10.0 thousand malicious domains, 49.1% of their TLDs fell into the category of .com. Among the 2.7 thousand malicious IPs, 16.0% were located overseas.

2.2 Website Security

About 20.1 thousand websites in mainland China were defaced, an increase of 20.0% compared with that in 2016, including 618 government sites. Besides, about 29.2 thousand websites in mainland China were detected to be planted with backdoors and secretly controlled, out of which 1,339 were government sites.

In 2017, CNCERT found about 49.5 thousand phishing sites targeting the websites in mainland China. About 5.0 thousand IPs were used to host those fake pages, and 96.4% were out of mainland China. Most of the phishing servers (25.5%) were located in HongKong, China.

CNCERT found almost 21.5 thousand overseas IPs conducting remote control on over 25.5 thousand websites in mainland China. As shown in Figure 2-5, 2,322(10.8%) were located in the U.S., followed with 824 (3.8%) in HongKong,

China and 789 (3.7%) in Russia.

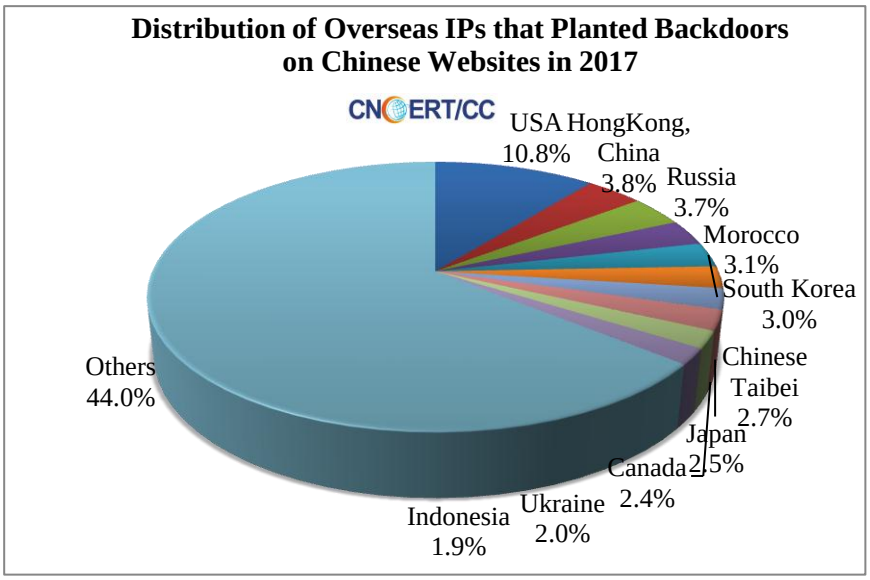

Figure 2-5 Distribution of Overseas IPs that Planted Backdoors on Chinese Websites in 2017

2.3 Mobile threats

In 2017, CNCERT collected about 2.53 million mobile malware samples in total. In terms of the intentions of these mobile malware, rogue behavior took the first place (35.9%), malicious fee deduction (34.3%) secured the second rank, and the next two were those intended for fee consumption and stealing privacy accounting for 10.4% and 7.9% respectively.

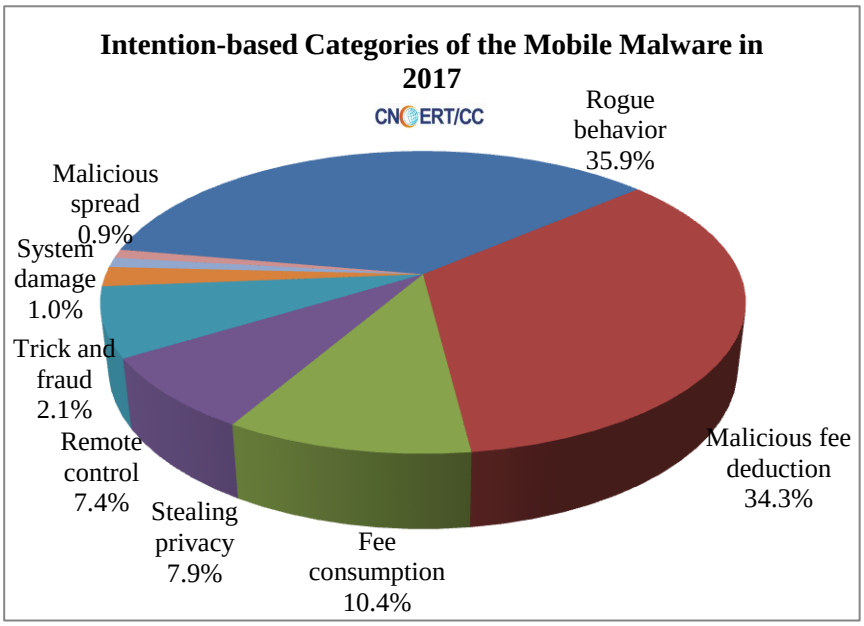

Figure 2-6 Intention-based Categories of the Mobile Malware in 2017

All of these mobile malware identified by CNCERT ran on Android system,

recording about 2.53 million (100.0%).

3. Events organized/co-organized

3.1 Conferences

Issuance of "The Review of the 2016 Network Security Situation in China"

CNCERT gave a press conference on the nation's 2016 Network Security Situation in Beijing on 19th April, 2017, introducing the overall picture and highlights of China's network security in 2016. Specialists and representatives from 50 organizations, including government agencies, operation departments of important information systems, telecom operators, domain name registrars, industry associations, Internet companies and security companies, attended this conference. This situation report, which was of distinctive industry characteristics and technical features, outlined the characteristics of China's network security threats in 2016, looked into the potential threats of great concern in 2017 and put forward a number of suggestions.

The 2017 CNCERT Annual Conference in Qingdao, Shandong Province

CNCERT held the 2017 Annual Chinese Conference on Computer and Network Security in Qingdao, Shandong province, from May 22nd to 24th, 2017. The theme of the Conference was "Industry Convergence to Promote Development, Mutual Collaboration to Build Security". Sub-Forums had been set up according to 5 subjects: Emergency Response, IoT Security, Cybersecurity Artisan, Incident Tracking and International Forum. More than 1,000 representatives from governments, important information systems departments, industries and enterprises, universities, research institutes and other organizations attended the meeting.

The 2nd CNCERT International Cooperation Forum & FIRST Technical Colloquium in Qingdao, Shandong Province

On May 22nd, 2017, the 2nd CNCERT International Cooperation Forum & FIRST Technical Colloquium was held in Qingdao, Shandong province with nearly 200 attendees. The representatives were from government departments for telecom affairs, cybersecurity emergency response organizations and

Internet companies in 15 countries and regions, such as Australia, Russia, Korea, Japan, India, Germany and Brazil. This Forum, by inviting both CNCERT international partners and FIRST members, has provided CNCERT, its international partners and cybersecurity enterprises with a profound exchange platform for cybersecurity emergency response affairs to further build trust, promote mutual learning and facilitate comprehensive cybersecurity cooperation.

This one-day event started with CNCERT introducing the implementation and future plan of the Forum, and followed by presentations from FIRST Board member, Ministry of Digital Economy and Society of Thailand, HKCERT, Korea Internet and Security Agency (KISA), (ISC)2, Siemens ProductCERT, CNCERT, Department of Information and Communications Technology (DICT) of the Philippines, Team Cymru, Hebei Unicom, Nanjing Sinovatio Technology and NSFocus on topics of cybersecurity capacity building, cybercrimes, APP security, cybersecurity threats, cybersecurity information sharing, national cybersecurity strategies, financial security, big data threats and cloud security, with best practices and experience being shared among each other.

The China-ASEAN Network Security Emergency Response Capacity Building Seminar in Qingdao, Shandong Province

CNCERT organized the China-ASEAN Network Security Emergency Response Capacity Building Seminar in Qingdao, Shandong province, from May 22nd to 24th, 2017. Delegates from the government departments for telecom affairs and CERTs of Cambodia, Indonesia, Laos, Myanmar, the Philippines, Thailand and Vietnam attended this event. The participants exchanged development, technological and management experience in the field of network security and discussed on how to conduct cooperation on network security emergency response between China and ASEAN.

4. Drill attended

APCERT Incident Drill 2017

CNCERT participated in the APCERT 2017 Drill as a participant on 22nd March,

2017 and completed it successfully. The theme of the APCERT Drill 2017 was "Emergence of a New DDoS Threat". In this year's drill scenario, the participating teams were tasked to mitigate DDoS incidents triggered by a type of malware which has been widely observed in the Asia Pacific region. This walkthrough is designed to test the participating teams' incident response handling arrangements. 23 CSIRT teams from 18 economies of APCERT took part in the exercise.

ASEAN CERT Incident Drill (ACID) 2017

CNCERT participated in the ASEAN CERT Incident Drill (ACID) 2017 on 11th September and completed it successfully. The theme for ACID 2016 was "The Dangers of Insufficient Authentication and Poor Access Control". According to the scenario, the participants played the "Hacker" and the "Incident Responder" roles. The "Hacker" role was involved in compromising actions and the "Incident Responder" was involved in detection, investigation of various attack and the response procedures.

5. Achievements

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

Table 5-1 Lists of CNCERT's publications throughout 2017

Title	No. of Issues	Description
CNCERT Weekly Reports (Chinese)	53	Emailed to over 400 organizations and individuals and published on CNCERT's Chinese website (http://www.cert.org.cn/)
CNCERT Weekly Reports (English)	53	Emailed to relevant organizations and individuals and published on CNCERT's English website (http://www.cert.org.cn/english_we

		b/documents.htm)
CNCERT Monthly Reports (Chinese)	12	Issued to over 400 organizations and individuals on a regular basis and published on CNCERT's website (http://www.cert.org.cn/)
CNCERT Annual Reports (Chinese)	5	Published on CNCERT's website (http://www.cert.org.cn/)
CNVD Vulnerability Weekly Reports (Chinese)	53	Published on CNCERT's website (http://www.cert.org.cn/)
Articles Analyzing Cybersecurity Threats	36	Published on journals and magazines