CNCERT/CC
Annual Report 2005

March 7, 2006

Content

CNCERT/CC ANNUAL REPORT 2005

1. About CNCERT/CC

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. It 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 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. Thus CNCERT/CC stands for a new platform for better International cooperation and a prestigious interface of network security incident response of China.

CNCERT/CC's activities include information collecting, event monitoring, incident handling, data analyzing, resource building, security research, security training, technical consulting, and international exchanging. (See http://www.cert.org.cn/en for more information)

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. Network Security Monitoring and Analysis

The 863-917 Network Security Monitoring Platform established and operated by CNCERT/CC is the core platform of network security incident monitoring in China up to date, which has been 7x24 non-stop running and monitoring on network security incidents.

2.1 Traffic Monitoring

The statistic result of sampling traffic data shows that, the most bandwidth consuming application is Web Access (37.82) and P2P File Sharing (15.43). The email traffic through port TCP 25 is about 6%, which consist of not only normal email but also great deal of spams caused by worms and spamers. TCP 135/445 were usually used by attacks. Most of Bots we detected take use of those ports to spread.

Since April 2005, there is a huge number of spam messages sent through port UDP 1026/1027. The corresponding traffic has been much higher than email, only lower than the Web Access and P2P. Under relevant parties' measures, it has finally been constrained successfully.
In the second half of 2005, CNCERT/CC handled 78 incidents detected by traffic monitoring. 50% of the incidents were caused by SQL Slammer.

2.2 Trojans Monitoring

In 2005, CNCERT/CC made sample monitoring of 28 popular kinds of Trojans and found more than 22,500 IP hosts had been planted with Trojans. The hosts are distributed in most provinces of mainland. The top 7 provinces Trojans hosts lied in are Guangdong (21%), Shanghai （15%）, Jiangsu (10%), Zhejiang (9%), Beijing (7%), Fujian (6%) and Hubei (4%). The hosts in other province totaled up to 28%.

Meanwhile, CNCERT/CC found more than 22,800 IP hosts outside China's mainland had some communication with those Trojan hosts. The distribution of percentage is: USA (25%), Chinese Taipei (18%), Hong Kong China (18%), Japan(12%), Canada (4%), Korea (4%), Australia (3%), Unite Kingdom (2%), and others (14%).

2.3 Spyware Monitoring

In 2005, CNCERT/CC made a sample monitoring on 30 kinds of usual Spyware and found more than 700,000 IP hosts had been planted with Spyware. Those Spyware secretly delivered users' private information to corresponding control servers, fetched keywords for data stealing and downloaded update version from the control servers. Those control servers mainly lay outside Chinese mainland. The top 2 countries with the control servers were USA (42) and Korea (26).

2.4 Website Attack Monitoring

CNCERT/CC's 2005 sample monitoring on 50 popular kinds of website attack found that 220,000 foreign hosts had frequently launched attacks to websites in China's mainland. The counties and regions which launched the most frequent attacks to mainland's websites are USA (40%), Japan (11%), Chinese Taipei (10%) and Korea (8%).

2.5 Botnet

Everyday, CNCERT/CC kept detecting newly emerging BotNets and monitoring the BotNets which once appearred . The scales of Botnets which we found differed from hundreds to more than 10 thousands. From January to December, the number of active BotNets in scale of more than 5000 Bots was 143. The biggest Diablo BotNet had about 157 thousand hosts at the most . Those BotNet continuously expanded, upgraded, downloaded spyware and Trojans, and launched all kinds of DoS attacks. CNCERT/CC also detected some botware which hid themselves by rootkit techniques. Due to concealment of Bot, there may appear ,more such kind of botware by use of rootkit in future.

The BotNet scale is getting smaller and smaller. The BotNets in scale from 1 to 10 thousand were the most favorites of attackers.

3. Incident Handing

3.1Incident Reports

In 2005, CNCERT/CC received more than 120 thousand incident reports from domestic and international users and agencies, 93% of which are scan incidents. The number of non-scan incident reports is 9112. The total number of both scan and non-scan reports doubled in comparison with that in 2004.

Regarding the non-scan reports, most of them were about webpage defacement (8130), phishing (475) and spam email (161).

The number of non-scan reports from international agencies is 464. Most of them were about phishing (456) and some of them were about Trojans. The top 10 phishing incidents reporters were eBay(207), MarkMornitor(43), Brandimension(22), BFKCERT(17), VeriSign(17), AUSCERT(15), Inter identitiy(14), MasterCard(13), HSBC(10), Royal Bank of Scotland(10), KrCERT/CC(7), Citigroup(6).

3.2 Incident Handling

In 2005, CNCERT/CC handled more than 400 incidents, most of which were handled by CNCERT/CC Branches around each province. The incidents included webpage defacement, phishing, host intrusion, DoS and malware. Of all kinds of incidents, the webpage defacement and phishing occupied a majority with 53% and 31%.

3.3 Significant Incident Handling

3.3.1 Abnormal Traffic on UDP1026 and1027

From June to July 2005, through 863-917 platform CNCERT/CC detected a rush increase traffic on UDP 1026/1027 which soared to 11.49% of total traffic. Analysis result shows that the abnormal traffic results from large mount of junk messages sent by hackers through Windows Message Service. CNCERT/CC located and stopped the source hosts and suggested ISPs take responsive filtering measures. The traffic was reduced by nearly 3Gbps after an ISP followed the advice.

3.3.2 Vigilant on domestic and international hackers' activities around 8.15

The report by a Hong Kong newspaper that some "China Honker" planned to launch attackes against Japanese rightist websites on 8.15 possibly through some Korean hosts was widely transcribed in China, Japan and Korea. CNCERT/CC kept vigilant on the hackers' moves and contacted with JPCERT/CC and KrCERT/CC to have continuous knowledge of the hackers'

activities in Japan and Korea. But we did not find any sign of organized actions of hackers. It turned out that no such events happened as the media reported.

3.3.3 Toxbot

October 17th 2005, CNCERT/CC received a report from SURFnet CERT that more than 290 thousands Chinese computers were infected with W32/Toxbot and ran as members of a huge BotNet which consisted about 1.2 million computers. CNCERT/CC responded quickly on this report with several measures including studying the method of detecting and cleaning, warning ISPs and partners to make self-examination and raise public awareness of security consolidation.

3.3.4 Dasher.B

December 15th 2005, CNCERT/CC detected a new worm (Dasher.B) which exploits a newly announced highly risky vulnerability (MS05-051). After intruding, the worm will connect to a control server in Changsha, Hunan Province, to fetch hacker's instruction, and then connect to a ftp server assigned in hacker's instruction as a dynamic domain name to download key logger and worm body. Under CNCERT/CC's coordination, local branch quickly located and stopped the control server and ftp server so that a potential wide spread was successfully stopped from the beginning. CNCERT/CC also published relevant advisories to suggest users check and enhance their systems.

3.3.5 Phishing of West Pacific and MasterCard

October 25th 2005, CNCERT/CC received IBM-CERT's report that a Chinese computer was running a phshing site of Bank West Pacific. During the handling process, CNCERT/CC found some clues of another phishing action. and a file of eleven credit card users' information, including name, address, card number, ATM password, birthday, transaction security number. CNCERT/CC carefully queried partners about the relevant banks. According to an APWG member's hint, CNCERT/CC ascertain that these information belonged to users of MasterCard. Then CNCERT/CC contact with MasterCard and return the file in time.

3.3.6 DoS

Attacks of DoS still often occurred in 2005 and cause huge damage. In January, CNCERT/CC stopped a severe DDoS launched from a huge BotNet. The BotNet caused about 1G bps traffic to the target with more than 11 kinds of DoS techniques. The victim's business completely collapsed with direct loss of more than one million RMB. With the cooperation of CNCERT/CC, the police successfully arrested the attacker who intended to break down competitor‘s business by such means.Besides, CNCERT/CC also successfully handled some other severe DoS incidents, such as the attack on a website of human resources service in Shenzhen in April, the attack on a domain name registrar and virtual host provider in August.

3.3.7 Web Page defacement

In 2005, CNCERT/CC detected about 13.7 thousand web page defacement incidents in China.

Hereinto the defacements on governmental web site of China's mainland totaled up to 2027, occupying 22% of all. This ratio is significantly bigger than the ratio of 2.2% that governmental websites occupied of all website, which showed that the Chinese governmental websites were the most likely to be attacked. So it is a pressing task to improve the safety of governmental websites.

4. Security Information Service

In 2005, CNCERT/CC enhanced the security informing service to ISPs and cooperative key infrastructures, as well as to relevant government agencies. More than 2 hundred of interior warnings and 75 critical vulnerability advisories were delivered in time.

More than 440 articles were published on CNCERT/CC's website, including security announcements, vulnerability advisories, malware warnings, technical reports, safety guidence, etc. After CNCERT/CC'2005 annual conference, CNCERT/CC particularly published all the conference materials on the website for public references. The materials has been widely referenced and quoted by both domestic and international network security agencies.

Besides website, CNCERT/CC also delivered information services directly to users by email, so that the users can be informed in time. By far, CNCERT/CC email subscriber groups includes CNCERT/CC branches, ISP CERTs, Pilot Internet Security Service Providers of MII, Technical Supporting Organizations, NSC-ISC members, TRANSIT-Guilin trainees, and China-ASEAN 2005 NetSec Trainees, etc.

5. Netsec conference and training

In 2005, CNCERT/CC organized many public activities on internet security and emergency response to raise the security awareness of government, industry and netizens.

- CNCERT/CC'2005 Annual Conference, March 24th~25th , Guilin City
- TRANSIT Training of FIRST, March 22nd~23th, Guilin City
- China-ASEAN Computer Emergency Response Capability Building and Cooperation WG, September 9th~12th, Beijing
- 'Healthy Wang Zhong Xing' TV Contest of NetSec Knowledge, September 17th, Beijing
- 2005 China Internet Security Emergency Response Drill, December 12th , Beijing.

6. International Cooperation and Communication

In 2005, CNCERT/CC took active part in international events.

- APCERT2005 on February 22nd~24th, voted as Deputy Chair.
- 31st APEC Tel on April 3rd~8th
- 2nd China-Japan-Korea Network and Information Security Workshop on June 9th
- ASEM Network Security Workshop on June 23rd~24th
- 17th FIRST Annual Conference on June 24th~July 2nd
- ITU WSIS Thematic Meeting for Cybersecurity on June 28th~July 1st

- 32nd APEC Tel on September 5th~9th
- APCERT 2005 Incident Handling Drill on December 12th

7. Conclusion

In general, there was no large scale of network security incident with grave consequences. The worms spreading by exploiting vulnerability doesn't play as leading actors any more. Instead, malwares with representatives of bot, spyware, identiy thieft code became the top threat. Meanwhile, DoS, phishing and spam email were still rampant. Besides, there were many network attacks incidents related to political events and memorial days in 2005. With a remarkably increase of total number, the security incidents in 2005 were characterized by the complexity of techniques, profit tendency and political motivations.

Since the hackers' motivation has changed, there will be less possibility of large scale severe incident in 2006. The incidents of malware, phishing, pharming, etc will continuously increase, as well as the attack on new computer applications. All these problems will result in the constant increase of total incident number.

Altogether, with the rapid continuous development of Internet in China, the security situation will be sophisticated and critical more and more. As the basic technical supporting agency on network security, under the lead of MII, CNCERT/CC will further work around the main task of capability building and service widening, to enhance the function of network monitoring and incident analyzing and management, expanding and exerting the function of emergency response system, and fully boost the public network security protection.