CNCERT/CC ANNUAL REPORT 2004

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 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

URL：http://www.cert.org.cn/
E-mail：cncert@cert.org.cn
Hotline：+8610 82990999（Chinese）,82991000（English）
Fax：+8610 82990375
PGP Key：http://www.cert.org.cn/cncert.asc

Network Security Monitoring and Analysis

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

Vulnerability Alert and Research

CNCERT/CC has paid attention to vulnerability information collecting, compiling and publishing since 2003. For those critical vulnerabilities which are likely to cause mass network security incidents, we usually do primary verification and testing, then to release alert in time. Meanwhile, we also do research on potential vulnerability exploit and attack in advance, and put the critical one in monitoring.

Worm Monitoring

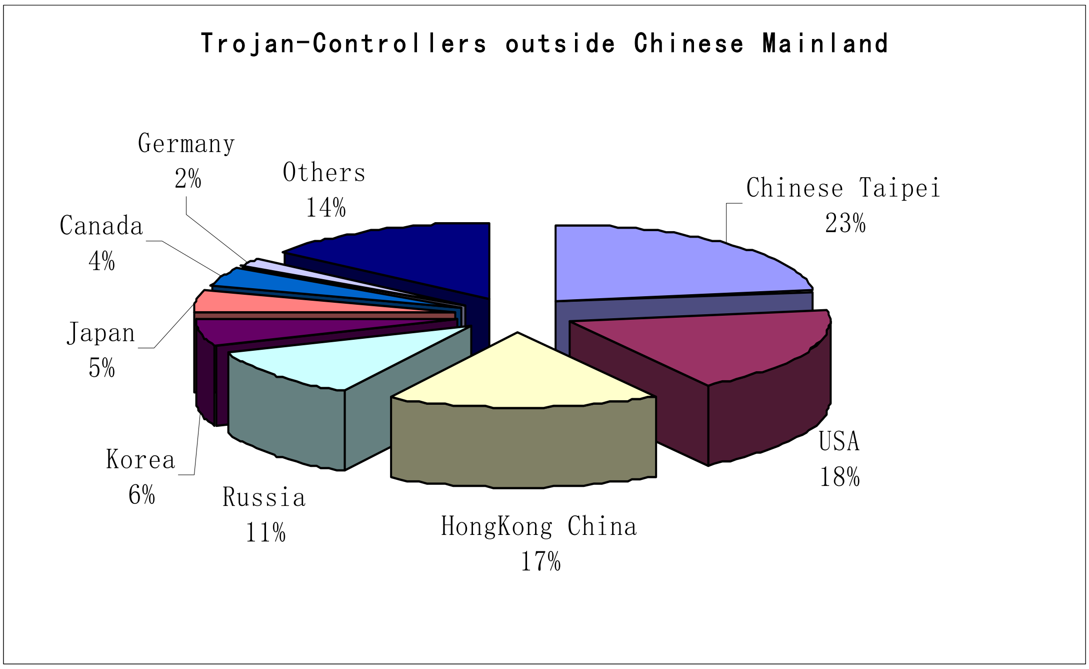
The most front-page incident about worm in 2004 is SASSER worm which exploited the vulnerability in MS Windows LSASS. A large number of computers were infected by SASSER. CNCERT/CC found out over 1,380,000 IP addresses infected in China mainland via sample monitoring.

Traffic Monitoring

By means of the abnormal traffic monitoring capability of the 863-917 Network Security Monitoring Platform, CNCERT/CC discovered the suspect network security incident for many times in China, and made the incident to be handled in time via coordinating related ISPs to verify and validate it.

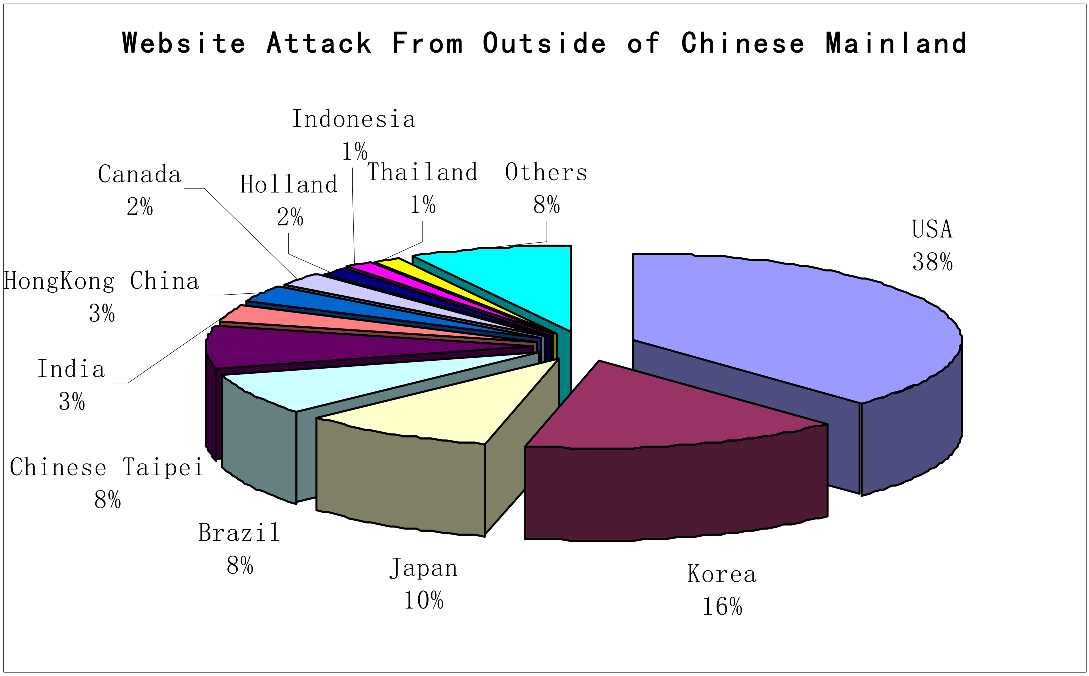
Trojan Monitoring

CNCERT/CC kept monitoring to over 20 popular Trojan programs and their activities, and discovered that more than 6,600 IP addresses of computers in China mainland had been injected with Trojan programs.



Website Attack Monitoring

CNCERT/CC kept monitoring to 38 popular kinds of website attack and discovered that 1024 foreign hosts had frequently launched attack to 3895 host machines in China mainland.



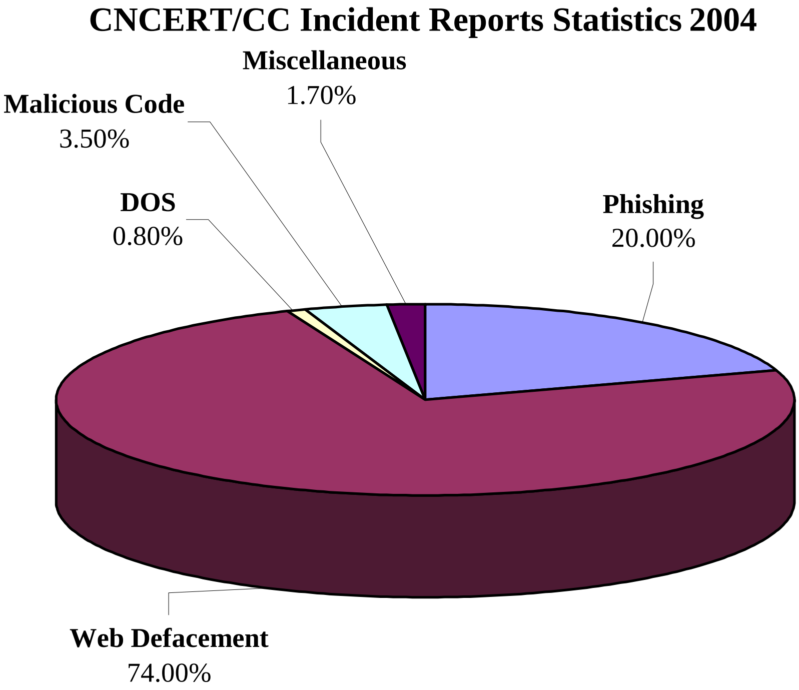
BotNet Monitoring

In a case of handling DOS incident, CNCERT/CC dug out a large active BotNet and got it to be handled successfully with the cooperation from the relevant department.

Incident Handling Overview

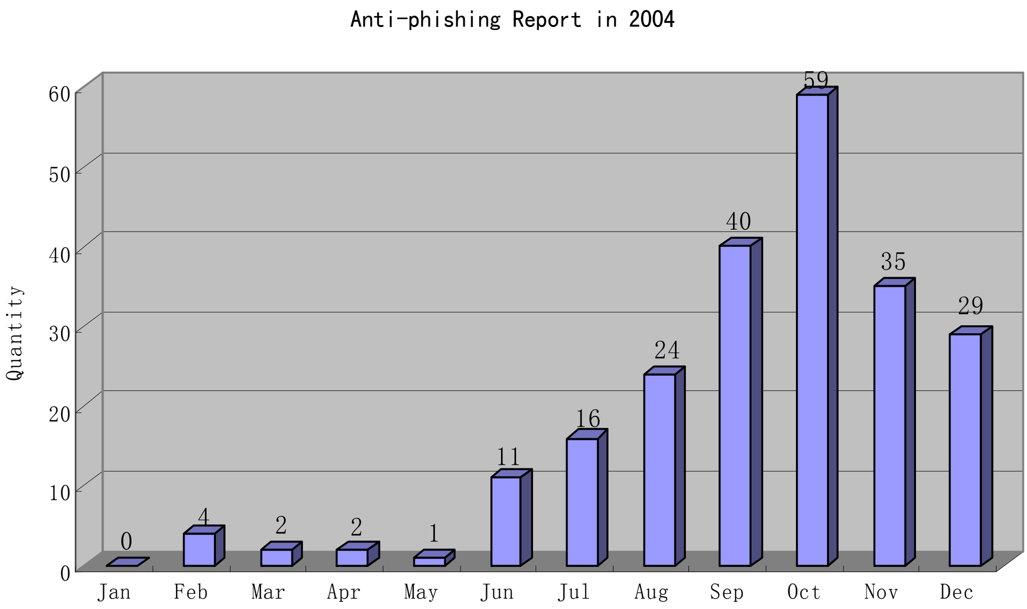
During the 2004 whole year round, CNCERT/CC had received over 64,000 security incident reports via our emergency response hotline, website, E-mail and so on, including domestic reports and those from other regions or countries, and nearly 93% reports are about scanning or probing. Thereinto, 245 incident reports are from 33 organizations of other regions except those automated forwarding scanning incident reports, including 223 Phishing reports, 4 Malicious website reports, 10 Trojan reports, 4 worm reports and 4 other miscellaneous reports.

In 2004, the main types of incident that CNCERT/CC had handled include Web Defacement, Phishing, Malicious Code, DOS and etc. The following figure shows the percentage of every type. Web Defacement（74%）and Phishing（20%） occupy the large proportion.



Phishing

CNCERT/CC had received 223 Phishing incident reports in 2004, mostly from foreign CERTs and security teams. The fraudulent finance and banking web pages also emerged in China mainland.



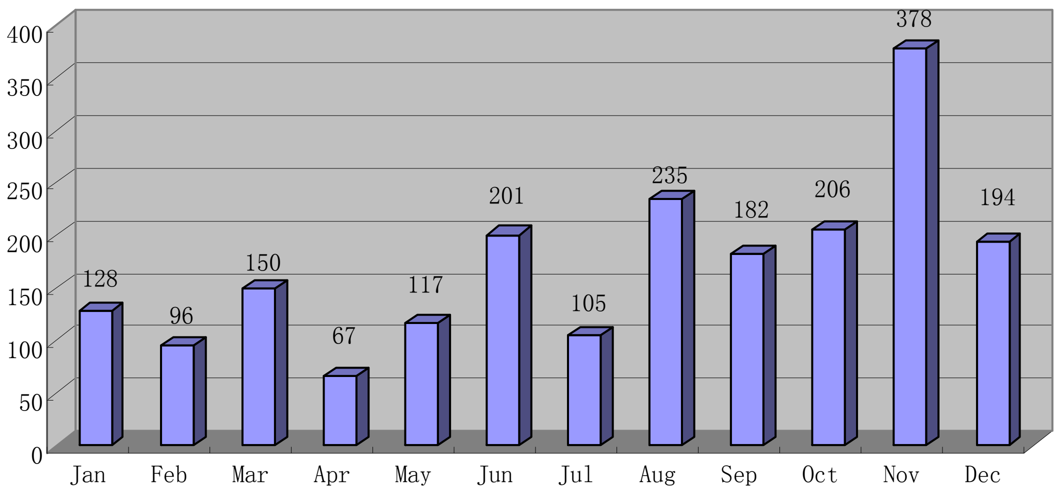
DOS

In 2004, CNCERT/CC had received quite a few severe DOS attack reports. CNCERT/CC was highly concerned about it and actively coordinated each related departments within Emergency Response System to handle them as critical incidents. In a case of DDOS, the user suffered from very long time of continual DDOS attack with the highest traffic of over 1Gbps on one occasion and over 11 types of attack. The user almost had no way to sustain their business activity, which resulted in huge economic lost. In this case, CNCERT/CC coordinated a few branches of CNCERT/CC and ISPs to deal with it, and cooperate with police agencies to do investigation and forensics. As a result, the evidence showed that, the malicious people who had launched DDOS attack via controlling a large BotNet actually aimed to crash down the victim website and beat the competitor.

Web Defacement

In 2004, CNCERT/CC kept daily monitoring to web defacement incidents in China mainland. For those discovered defaced websites, CNCERT/CC always coordinated the related provincial branches to inform websites owners to recover them as soon as possible. There were 2059 defaced websites discovered in China mainland during 2004.

Web Defacement in Chinese Mainland in 2004



Network Security Information Service

Website

CNCERT/CC's website has become the important window to provide network security information service to the public. In 2004, CNCERT/CC had published over 580 articles on the website, including security bulletins, vulnerability bulletins, virus forecasts, security reports, security news, security advisories, security tools, and statistic reports and so on.

E-mail

The current users of CNCERT/CC information service (mailing list subscribers) include provincial branches, ISP CERTs, entitled security service providers, and technical support organizations and so on.

Training and Domestic Conference

Internet Emergency Response Conference of China'2004- Hainan

CNCERT/CC undertook the Conference from 11th to 13th, February 2004.

NetSec Conference 2004 - Beijing

CNCERT/CC participated in the Conference from 24th to 25th, August 2004 as an associate.

Network Security Emergency Response Training - Harbin

CNCERT/CC hosted the Training from 8th to 11th, January 2004.

Network Security Emergency Response Speech & Presentation

CNCERT/CC staff had been invited to do presentation and speech at over 40 network security related domestic or international conference in 2004, including APEC-TEL Conference and China Internet Conference and etc.

Local Conference & Training

Many provincial branches of CNCERT/CC hosted local network security related conferences and trainings for local users in 2004.

International Cooperation and Exchange

APSIRC Conference 2004, Feb.23th -25th, 2004, Malaysia

CNCERT/CC delegation participated in the Conference. Meanwhile, CNCERT/CC delegation officially visited MyCERT.

1st China-Japan-Korea IT Network and Information Security WG, Mar.16th, 2004, Korea

CNCERT/CC participated in the Conference, and delivered a presentation.

29th APEC-TEL Conference, Mar. 21st - 23rd, 2004, Hong Kong, China

CNCERT/CC and MII delegation participated in the Conference, and delivered a presentation on “China Network Security Emergency Response Handling System and CNCERT/CC Work Introduction”.

FIRST SC & APCERT SC Joint Conference, Apr. 2nd - 6th, 2004, Singapore

CNCERT/CC participated in the Conference.

AusCERT 2004 Conference, May 23rd -27th, 2004, Australia

CNCERT/CC delegation participated in the Conference.

16th FIRST Annual Conference, Jun. 13th -18th, 2004, Hungary

CNCERT/CC delegation participated in the Conference.

ITU WSIS Thematic Meeting on Countering Spam, Jul. 7th -9th, 2004, Switzerland

CNCERT/CC participated in the Conference.

2nd China-Japan-Korea ICT Business Forum, Jul. 26th, 2004, Japan

CNCERT/CC participated in the Conference, and delivered a presentation on “Challenge and Best Practice on National Public Network Protection”.

3rd ASEAN-China ICT Cooperation Seminar, Aug.7th, 2004, Thailand

CNCERT/CC participated in the Conference, and delivered a presentation on “CERT: Most Active Sector in Internet Security”.

APEC Computer Crime Legislation & Law enforcement Conference, Aug. 25th, 2004, Vietnam

CNCERT/CC participated in the Conference, and delivered a presentation.

CONCERT Annual Conference 2004, Nov. 23rd, 2004, Korea

CNCERT/CC participated in the Conference, and delivered a report on “Best Practice on National Network Security Protection”.

Other CERTs Visits

In 2004, CNCERT/CC had welcomed other CERTs visits, such as JPCERT/CC, HKCERT and AusCERT.

Network Security Survey

In 2004, CNCERT/CC had made a nationwide network security situation survey, covering many industries and sectors, such as bank, transportation, electric energy, telecommunication, securities, insurance and etc. The survey staff had interview with nearly 3,000 network users and collected their questionnaire. The survey result will be announced at CNCERT/CC 2005 Annual Conference in March 2005.