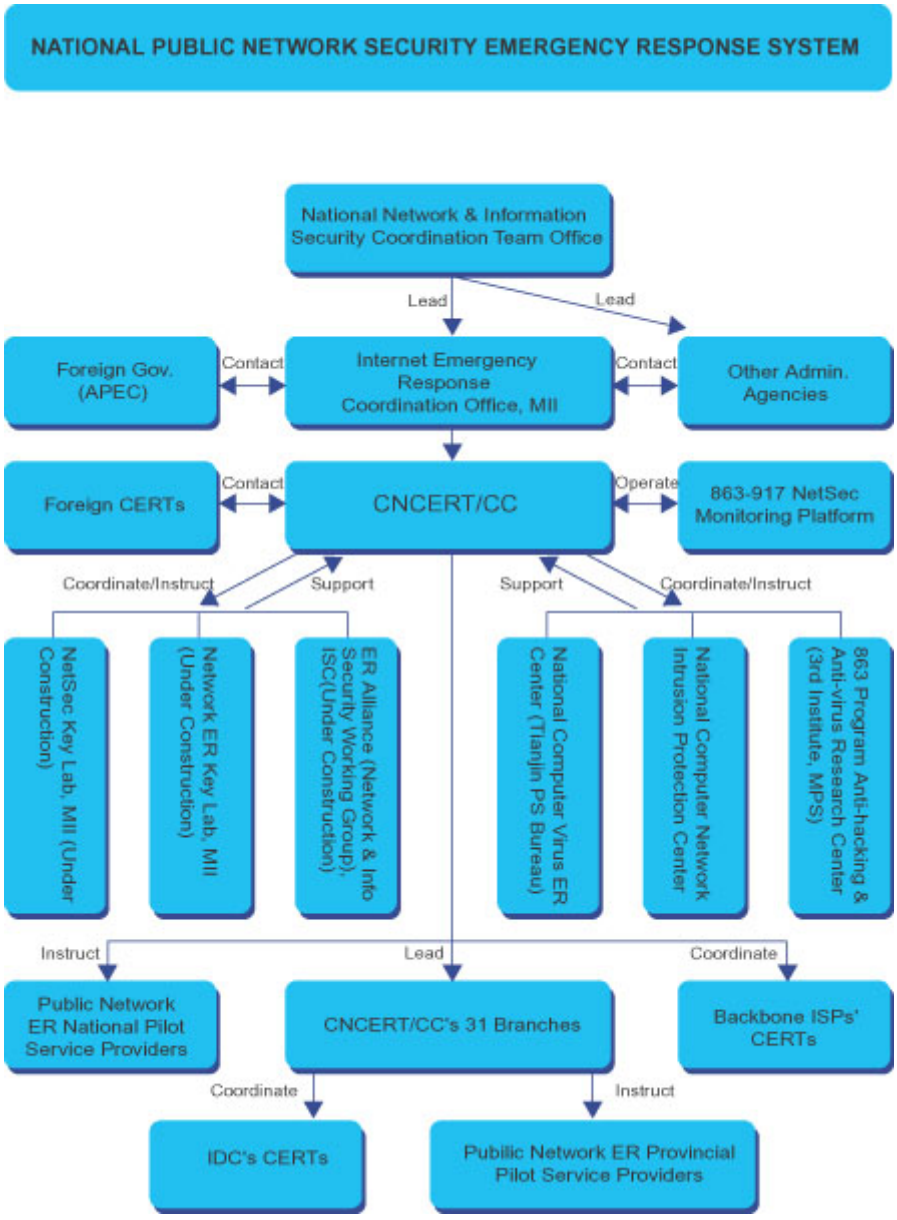
CNCERT/CC ANNUAL REPORT 2003

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.

CNCERT/CC works as the coordination center of the "National Public Network Security Emergency Response System" of P.R.China shown as follows:



Incident Response

In 2003, there are lots of serious incidents such as SQL SLAMMER, Deloader, MSBlaster, which gave CNCERT/CC great pressure to handle.

1. Selected Cases

SQL Slammer: erupted in Jan. 2003 and made a highly severe impact on the global network resulting in the network broken down in large scale. The National Computer Network Emergency Response System with the core of CNCERT/CC worked together to accomplish timely detection, exact identification and fast recovery with the event. This incident was made to be under control effectively within a single day in China.

Deloder: erupted in Mar. 2003 and blocked quite a few network area in China badly. It's more difficult to defend against this worm as it exploits the vulnerability of weak password instead of technical flaw to launch attack. Through the National Computer Network Emergency Response System, CNCERT/CC discovered and analyzed the worm in time, and contained it spreading effectively and efficiently together with its partners. The whole network was kept away from severe impact eventually.

Blaster/Blaster Remove: erupted in Aug. 2003 with an enormous infection. The network speed slowed down in some regions and a lot of PC users were infected. CNCERT/CC always kept in touch with foreign CERTs and domestic CERTs during the handling process, and corresponded each other, and opened a special news area at the website for the first time and provided users with technical support services.

DOS: CNCERT/CC tackled many DOS attack cases involving governmental portals, large ISPs and important websites in 2003. During the handling processes, CNCERT/CC got to track and locate attack sources with the close cooperation with ISPs nationwide.

Web Defacement: CNCERT/CC discovered many cases about web defacement in 2003, and contacted local related agencies to inform users and helped to solve the problem in time.

Web Fraud: CNCERT/CC received many reports on web fraud event, e. hackers intruded in victim's machines and made fraud to users of banks or commercial sites. CNCERT/CC quickly solved all these problems with the cooperation from related CERTs.

Others: CNCERT/CC received 13,295 reports on general security events in 2003 and handled them according to international rules. In 2003, CNCERT/CC detected around one million times of attack attempts targeted to Chinese networked computers on Internet via 863-917 network security monitoring platform.

2. Incident Reports Statistics

In 2003, CNCERT/CC received 13,295 incident reports on general security events and indicated an obvious leap compared with the number of 1761 in 2002. Most of reports were about intrusion activities from outside of Chinese territory. The following two figures show the data in detail.

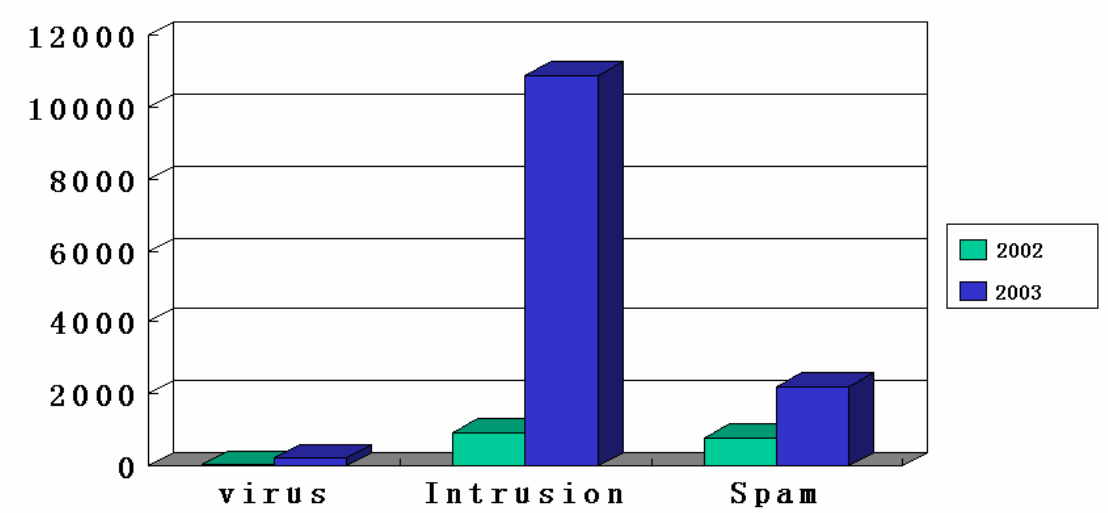


Figure1: Data Comparison Between 2002 and 2003

Incidents								**other**
	Different type of incidents							Consultation
	Virus		Intrusion		Spam		total	
Month	Dom.	abroad	Dom.	Abroad	Dom.	Abroad		
Jan		2		342	2	129	475	13
Feb	10	2		482		172	666	5
Mar	15	2	1	724		135	862	7
Apr	4	1		383		156	540	2
May	3	11	5	980	2	168	1169	9
Jun	1	50	3	753		137	944	13
Jul	6	35	3	881	3	173	1101	21
Aug	16	11	4	1509	1	153	1694	3
Sep	20			1542		277	1839	2
Oct	10		1	1067	5	248	1331	15
Nov	9	3	2	1032	2	160	1208	23
Dec	3	6	1	1178	2	276	1466	3
total	97	123	20	10873	17	2184	13295	116

Figure2: Statistics of Incident Reports 2003

Projects

1. 863-917 NetSec Monitoring Platform

863-917 NetSec Monitoring Platform is a system used for network traffic monitoring and

analyzing so that early response toward severe network incidents might be taken.

2. Resource Base on Vulnerabilities, Patches, Defending Tools

In order to provide Chinese network users with trusted information on vulnerabilities, patches and defending tools, we started to collect, translate and process these information in the beginning of 2003.

Media Exposure

1. Published 33 articles or reports at CNCERT/CC's website.
2. Issued a handbook on computer emergency response jointly with China Information World. (http://www.ciw.com.cn)
3. Translated materials on anti-cybercrime nearly one million of Chinese characters.

Establishment of CNCERT/CC's 31 Branches

The former national public network security emergency response system of China is a tree structure with CNCERT/CC as the root and CERTs of backbone ISPs as leaves. In order to speed up the progress of emergency response work, since 2003, we have established 31 branches of CNCERT/CC covering 31 provinces in mainland of China to form a network structure based ER system which had solved the old problem that ER work was lack of localized support, and not able to run high effectively.

Conferences

1. Cybercrime Legislation and Enforcement Capacity Building, July 21-25 2003, Bangkok, Thailand

   CNCERT/CC and the Internet Emergency Response Coordination Office of MII participated in the "Cybercrime Legislation and Enforcement Capacity Building" conference hosted by APEC. We delivered a presentation on "Anti-Cybercrime Depend Upon The Community Working Together".

2. APT Seminar on Network Security Management and the Positive Use of Internet, August 18-20 2003, Kuala Lumpur, Malaysia

   One representative from CNCERT/CC attended the "APT Seminar on Network Security Management and the Positive Use of Internet" conference and delivered a presentation on "Introduction about Chinese Network Security & CNCERT/CC".

3. 2nd Asia Cybercrime Summit, November 5-6 2003, Hong Kong, China

CNCERT/CC participated in the “2nd Asia Cybercrime Summit” and delivered a presentation on “Fighting with Large-Scale Internet Incidents”.

2004 Plan

1. Consolidate the cooperation among each units of National Public Network Security Emergency Response System of China, including related projects on incidents classification, description and information exchanging
2. Stress on training and education
3. Enhance the cooperation with other international CERTs and IT security organizations
4. Continue the construction of 863-917 NetSec Monitoring Platform and resource base
5. Relevant research

URL：http://www.cert.org.cn/
Email：cncert@cert.org.cn
Phone：+8610 82990999, 82991000
Fax：+8610 82990375