I

Introduction on Chinese Network Emergency Response System & CNCERT/CC's Activities

Doc no:

telwg29/ IRF/07

Agenda item :

Incident Response and Forensics Workshop

Submitted by:

China

Introduction on Chinese Network Emergency Response System & CNCERT/CC's Activities

Contact: Zhou Yonglin
Email : zyl@cert.org.cn

APEC Telecommunications and Information Working Group
29th Meeting | 21-26 March 2004 | Hong Kong, China

Introduction on Chinese Network Emergency Response System & CNCERT/CC's Activities

Zhou. Yonglin

Deputy Director

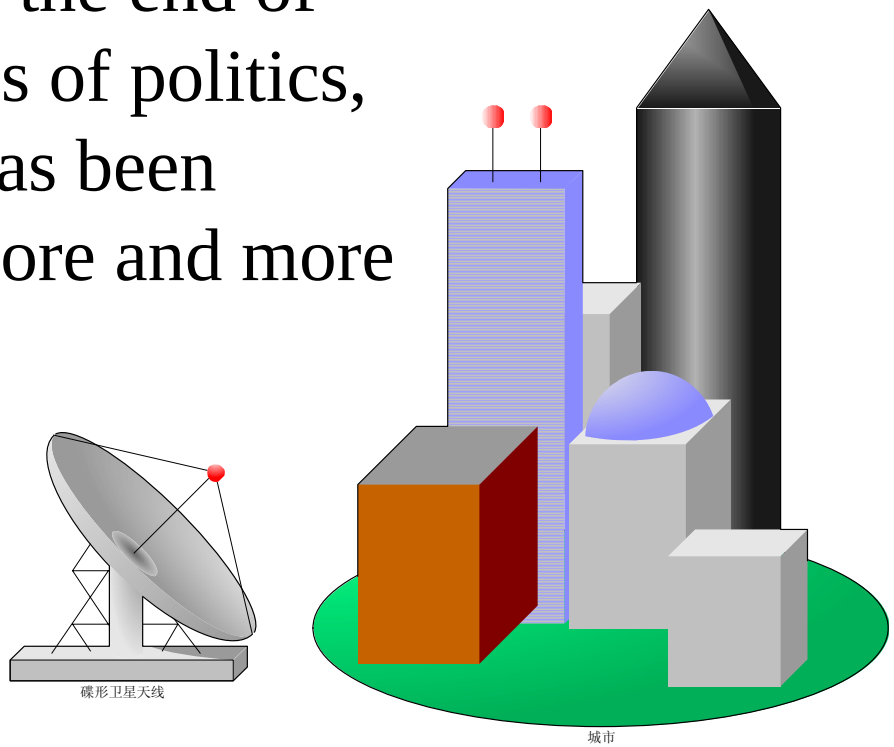
Administration & Operation Dep.

Outline

- Establishment & Growth of CNERS (Chinese Network Emergency Response System)
- Responsibilities & Services of CNCERT/CC
- How Does CNCERT/CC Act?
- Case Study
- What To Do Next?

Policies of National IT Promotion

- Since China released the policies of national IT promotion at the end of last century, the activities of politics, economics and culture has been depending on Internet more and more in recent years.



Development of Chinese Internet

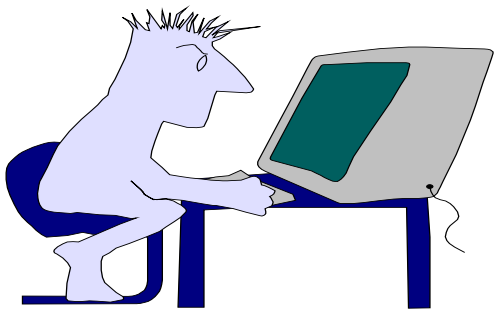
Year	Hosts (M)	Users (M)	Web sites (K)	Total Bandwidth (Gbps)
2001	8.92	22.5	265.4	2.799
2004	30.89	79.5	595.6	27.216
Multiples	3.5	3.5	2.2	9.7

- The construction of Internet Infrastructure has achieved a great deal of progress.
- The users has been increasing significantly, so does technical professionals.
- WWW and Email services always kept growing so fast. Meanwhile, commercial services, such as value-added services of Telco, e-Banking, e-Trading, charged online games and multimedia services, emerged constantly.
- The e-Government has been highly promoted forward.

(From CNNIC)

Confronting Threat

- Internet is playing a more and more important role in our political and economic activities.
- Large-scale network security incidents take place much frequently.
  - Worms
  - DDOS



CNERS Initiation

- Code Red (Aug.,2001) challenged the Internet security of China.
  - Lack of CSIRTs: only 4 CSIRTs (CNCERT/CC, CCERT, NCVERC and NCNIPC)
  - Lack of experiences in handling large-scale incidents
  - Less use of preventing Internet and important application networks from jam-up.
- An ER Alliance was formed, which marked the beginning of CNERS.
  - All Internet carriers, big IDCs, anti-virus companies and network security companies joined the alliance.
  - A primary principle was to set up the foundation for large-scale incidents response and handling in the future.
  - MII (Ministry of Information Industry) backed up this program.
  - Each Internet carrier started to set up its own CERT.

CNERS Growth

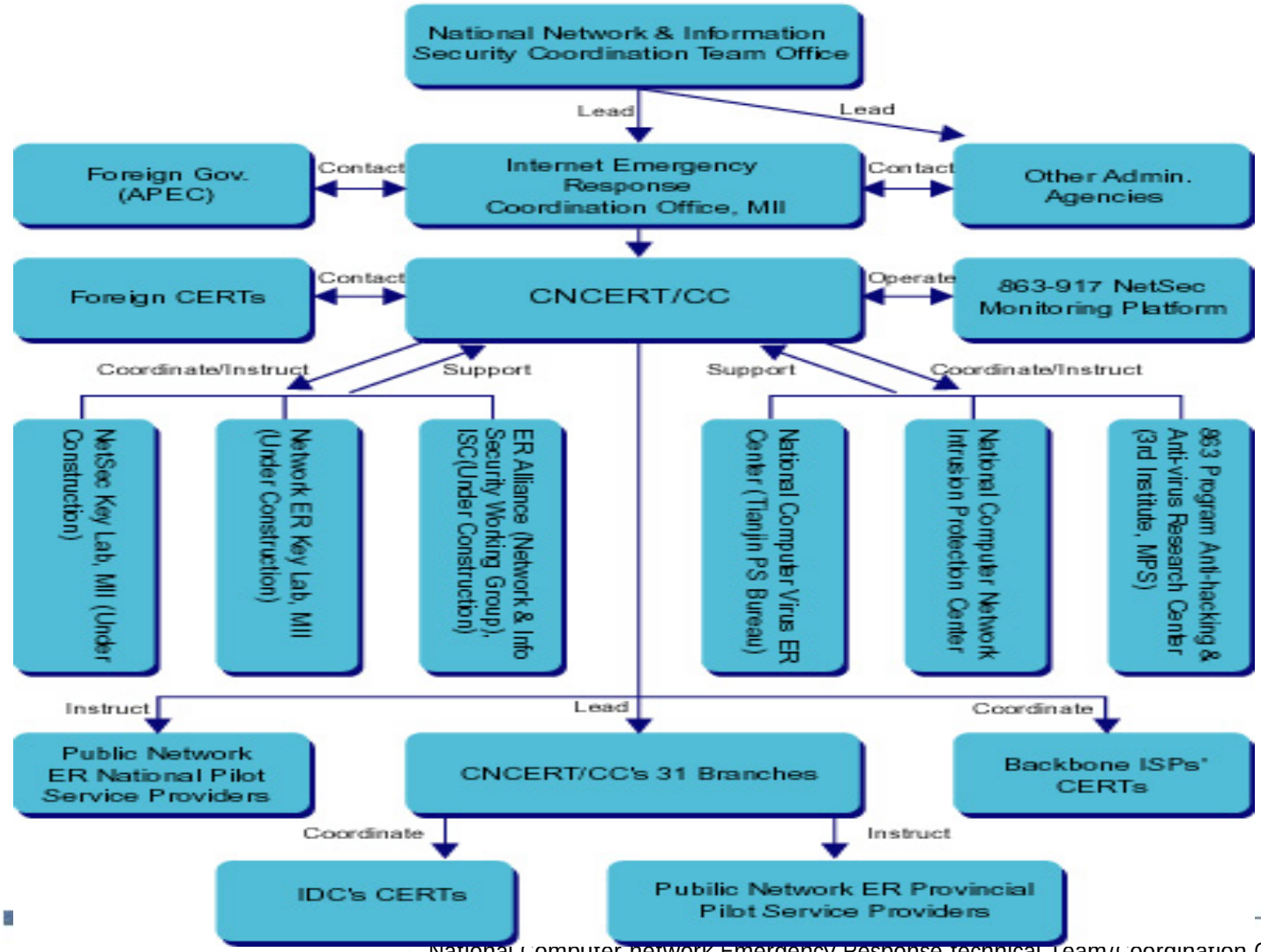
- International Cooperation：
  - CNCERT/CC became a full member of FIRST in 2002, and
  - At APSIRC2002, initiated APCERT (Asia Pacific Computer Emergency Response Team) with AusCERT, JPCERT/CC and etc.
  - At APSIRC2003, was nominated and elected as the Steering Committee member of APCERT.
  - IERCO (Internet Emergency Response Coordination Office) was set up by MII and took part in the APEC-TEL activities.

CNERS Growth

- Domestic Development：
  - CNCERT/CC did its best to promote technical capabilities and tools.
  - CNCERT/CC built up 31 branches across the country.
  - The cooperation mechanism within CNERS was developed.
  - IERCO designated some public network ER pilot organizations into CNERS.

CNCERT/CC

NATIONAL PUBLIC NETWORK SECURITY EMERGENCY RESPONSE SYSTEM



CNCERT/CC's Responsibilities

- Coordinates activities among all CERTs in China regarding incidents on national public networks.
- Provides computer network security services and technical support in handling of security incidents for national public networks, national critical application systems and important organizations, including detection, prediction, response and prevention.
- Collects, verifies, accumulates and publishes authoritative information on the Internet security issues.
- Exchanges information, coordinates activities with International Security Organizations.

CNCERT/CC's Activities

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.

CNCERT/CC's Activities

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.

How Does CNCERT/CC Act?

- As an exchange center of information
  - From national network security monitoring platform
  - From public incident warning and reports
  - To set up reliable and expedite communication channels to all domestic and international CERTs.
- To direct all the regional branches to work together.
- To cooperate with Internet carriers closely.
- As a security technology research center.
- To provide the most trusted data to government and the public.

Case Study

- The main events CNCERT/CC handled in 2003 are:
  - Worms
  - DDOS
  - Web Defacement
  - Web Fraud
  - Vulnerabilities
- Three cases as followed.

Case I： Worm SQL Slammer

- Received report at noon on Jan 25th, 2003.
- Inquired all carriers' CERTs to obtain data of its spread scope and speed.
- Informed all relevant organizations and studied the sample ASAP.
- Monitored the network to capture incident increase.
- Found out the situation all over the world and what nations else did to handle it.

Case I： Worm SQL Slammer

- Analyzed sample to find out approach of isolation.
- Informed carriers of isolation rules and to carry out immediately.
- Provided infected host IP addresses to carriers to help recover network at the same day.
- Kept on monitoring and analyzing.
- Reported to both MII and the public. ◦

Case II: A DDOS Incident

- Received report that from May 10th, 2003, a government network seemed to be blocked and local e-Government services and other 86 websites were affected seriously.
- Asked CNCERT/CC branch to handle it. The branch team analyzed and concluded it as a DDOS attack.
- The branch and local carrier worked together to track the attackers and finally found they were from Guizhou province.

Case II: A DDOS Incident

- CNCERT/CC coordinate Guizhou Branch to handle it jointly. Later in the evening, Guizhou branch located the attacking source in a hosting IDC through the cooperation with local carrier. The DDOS was stopped soon after the host in Guizhou province was removed.
- After security evaluation, CNCERT/CC gave some suggestions to the manager of attacked networks.

Case III：A Web-Fraud Incident

- On Dec. 8th, 2003, AusCERT reported two hosts in China had been cheating as financial sites.
- CNCERT/CC checked and located the hosts in 2 different provinces, Jiangsu and Yunnan, which were of big vulnerabilities and maybe abused by attackers.
- CNCERT/CC informed its branches to handle it. Before 10th, both 2 hosts were found and closed by local carriers with end users' grant.
- CNCERT/CC replied AusCERT about the result. And since Web-Fraud incidents became more and more popular, CNCERT/CC gave a particular report to MII in time.

Experiences

Only by multi-parties' cooperation according to a well-planed scheme can Internet security incidents be handled quickly and effectively.

What to do next

- Establish related criteria and scheme
- Promote the cooperation among CNERS
- Enhance the communication and cooperation with CNCERT/CC's branches.
- Organize more training and education
- Continue research on network security
- Improve the technical platform and tools

What to do next

- Promote cooperation with international CERTs and security organizations.
  - Set up reliable and expedite communication channels.
  - Establish a definition standard of security incident which will benefit important incident reporting and handling in time；
  - Promote the pre-warning and report.
  - Enhance the communication and cooperation on research of technology.

CN ERT/CC

Thank you !

www.cert.org.cn

zyl@cert.org.cn