Cross Border collaboration: Practices & experiences

Jiao Xulu
Admin. & Operation Dep. Of
CNCERT/CC
2005.9.5

Content

• Why we need cross border collaboration
• International Cooperation of CNCERT/CC
• Case Study
• Conclusions
Why we need cross-border cooperation for network security

- For attackers, there are no borders, but we have
  - A lot of incidents are across networks or economies
  - More organized attacking now
- Information sharing is essential for incident early warning
- Sharing related technology is also essential
- Global Problem, Global Solution

Phishing

- Economy A
- Economy B
- Economy C
- Internet
- target
- attacker
- Fraud site
DDoS by Botnet (Zombie Army)

What we get from International Cooperation

- Early warning information
- Tech. & experience sharing
- Training
What we contribute for international coordinators

- Early warning information
- Experience and technology sharing
- Training
- Incident handling

Case study

- **Case 1**: Worm : Deloder
  - Received report on Mar. 2003.
  - Jammed quite a few network area in China badly.
  - Inquired all carriers’ CERTs to obtain data of its spread scope
  - Informed all relevant organizations and studied the sample code.
  - Tried to find out the situation all over the world and what others did to handle it.
Case study

• Case 1: Worm : Deloder
  • Analyzed sample to find out approach of isolation.
  • Kept on monitoring and analyzing.
  • The whole network keep away from sever impact eventually
  
  experience:
  – IRS does great efforts

Case study

Case 2: Phishing incidents
  • Received report from Brazil that there was one phishing site located in China in July 2004.
  • Confirm the website lied on JiangSu province
  • CNCERT/CC inform the JiangSu branch
  • Colleagues in JiangSu found out the machine
  • With the help of the network manger, engineer search the film system at the site and found the film which the hacker replaced
Case study

Case 2: phishing incidents

- Recover and backup the system
- Give some advise
- Branch reported the process to HQ
- CNCERT/CC inform the Brazil

experience:
  - IRS does great efforts
  - The whole process took five days

Case study

Case 3: China-Japan-Korea collaboration during 8-15

- 8.15 is a sensitive period, Contact in advance to raise attention
- Enhance information sharing during particular period
- Watch trends of hackers' activities, through BBS, public chat rooms...etc
- Inform each other current situation. e.g JPCERT/CC announced to all members every half day. KrCERT notified JP and CN attack maybe happen
Case study

Case 3: China-Japan-Korean collaboration during 8-15

- Take a close look at the watch and warning system and inform our partner in the domestic cooperative system
- No sever incident happened.

experience:
- Benefit each team very much with pre-warning function, as well as incident handling.
  It is beyond political sensitivities and shows the value of APCERT community.

Conclusions

- Building up the trusted relationships between CERTs
- Information exchange and incident precaution
- Secure and convenient platform for information exchange
- Sign the formal file for sensitivity information for the long period collaboration

All participators are the beneficiaries
Thank you!

www.cert.org.cn
jxl@cert.org.cn