CASE STUDY: Cooperation within APCERT

KrCERT/CC
Jinhyun Cho
hyuni@kisa.or.kr

CASE 1: Attack on Private Site

- Major DDoS Attacks from Japan
  - Attack on BBS
  - First Attack (20th August): More than 10 times Traffic
  - Tons of Malicious Postings using Automated Script Tools
  - Unsolicited Pop-up when visiting the sites
- Damage on the Site: Slowdown of Access to pages
- Cooperation with JPCERT/CC (Attack Information)
  - 2nd Attack: Proxy Server, 3rd Attack; Mail Bomb
- Prevention action for the sequel attacks taken
  - Blocking IP addresses and Stopping the Mail Service
CASE 2 : Attack Cooperation

- HK Newspaper Article at the Beginning of July
  - Famous Chinese Hacker Group will hack into many Japanese sites on the specific day such as 15th August
  - KrCERT/CC : questioned the reliability of the article and the trends of the group
  - HKCERT : answered that that newspaper is not reliable and on alert for the matter
  - APCERT : All teams had interests on attacks from the Chinese Hacking group to break down the attack
  - Information Sharing on the Specific Attacks
  - No attacks happened and that group was dissolved

Lessons Learned

- Information Sharing among CERT/CSIRTs is important for mitigating the damage from Cyber Attacks

- Trust among CERT/CSIRT makes it possible to assist each other

- Face-to-face Meeting and Experience to work together makes CERT/CSIRT build the trust among CERT/CSIRT