CERT Collaboration with ISP to Enhance Cybersecurity

Jinhyun CHO, KrCERT/CC
Korea Internet & Security Agency
I. Alarming call for cooperation with ISPs

Slammer Worm

- Spread most of vulnerable SQL servers within 30 min. globally
- All Internet infrastructure in Korea disabled
- CERT Relations with ISPs: No coordination mechanism framework
II. Cybersecurity Collaboration with ISPs: Phase I

Initial setup stage (2003~2005)

- Formalization of cybersecurity private and public cooperation relations
- Needs for ISP coordination mechanism and procedure recognized
- Korea Internet Security Center (KrCERT/CC) opened in December, 2003
- Legal, policy and technical response to cyber attacks and threats

Amendment to relevant law
Threat Information Sharing
Collective Emergency Response
Security Exercise and Daily Checkup
II. Cybersecurity Collaboration with ISPs: Phase I

Amendment to Relevant Law

- Legal basis for the collective cybersecurity response actions
- Minimal standard for cybersecurity in telecommunication area
- Emergency response order
- Mandated incident reporting and threat information sharing

Threat Information Sharing

- Traffic and attack statistics from major ISPs
- Concerns, difficulties and issues discussed and resolved
- Information sharing agreement among ISPs before legislation
- Relevant costs covered by government
II. Cybersecurity Collaboration with ISPs: Phase I

Collective Emergency Response

- Emergency response action order to ISPs
- Order applied to domestic ISPs within a day
- The access blocked to foreign malicious website site or IPs
- Legal authority and responsibility

Security Exercise and Daily Checkup

- Major incident scenario based exercise with ISPs
- Systemic approach to response coordination procedure & process
- Train the relevant first-line cybersecurity staffs
- Daily security checkup with Radio system (alternative comm. channel)
III. Cybersecurity Collaboration with ISPs: Phase II

Stabilization Phase (2006~2009)

- Enhancing the collaboration relationship and make results with ISPs
- Major cyberthreat from botnet and response
- Emerging DDoS issue (availability)

Coordinated Botnet Response Action

Bi-annual workshop

DDoS Defense Investment
III. Cybersecurity Collaboration with ISPs: Phase II

Coordinated Botnet Response Action

- Implementation of national-wide botnet sinkhole system
- Access restriction to botnet c&c servers by changing IP address
- CSF: The close collaboration and voluntary participation from ISPs
- Trustworthy information source for cyber threats: KrCERT/CC

Bi-annual workshop

- Face-to-face trust building opportunity in a relaxed environment
- Closed technical presentation on security issue
- Proposal for collective security actions made in the workshop
DDoS Defense Investment

To promote the investment from ISPs on DDoS attacks from 2008
DDoS service commercialization and commodity service
DDoS defense device provided to selective ISPs by government budget
Calls for responsible ISP response to major cyber threats

III. Cybersecurity Collaboration with ISPs: Phase II

Internet Exchange (IX)
Aftermath Phase (2010~ Current)

- DDoS Attack in July 2009 and March 2011
- Renewal of national attention to cybersecurity with major incidents
- Collaboration and coordination among public and private sector
- Smart response for cybersecurity needed
IV. Cybersecurity Collaboration with ISPs: Phase III

**Investment on cyber security**
- Organizational restructure for strengthening incident prevention
- DDoS shelter service for SME (limited time-frame)

**Joint Voluntary Project**
- Joint initiative for cybersecurity outreach service
- Voluntary threat information sharing and project to tackle cyber threats

**High-level Attention & Support**
- Regular meeting for cybersecurity issues
- Awareness Raising for senior-level people for cybersecurity
1. Trust based Collaboration for Mutual Benefit

2. On-going Efforts for Emerging Cyber Threats

3. Collaboration and Cooperation in Action
THANK YOU!