Korean Cybersecurity Framework

23 Sep 2009

Hyderabad, India
2009 ITU Regional Cybersecurity Forum for Asia-Pacific

Terrence Park
KrCERT/CC
Korea Internet & Security Agency
Conten

- Cybersecurity Constituency in Korea
- Code of Conduct in Korea
- Evolution of Cyber Incident
- National Cybersecurity Framework
- KrCERT/CC Activity
- 7.7 DDoS
Public Officer: 610K
Local Officer: 270K
Public Org: 250K Officers
Government: 1 million (inferred)
Server: 15K (inferred)

Population: 48 million, Internet User: 35 million
PC: 30 million, Server: 5.7 million
Broadband Subscriber (Jun 2009): 16 million
IPv4 (Jun 2009): 73 million
VoIP Subscriber (May 2009): 4 million
IPTV Subscriber (Jul 2009): 0.5 million

Private Corp.
User
IPTV, VoIP
Portal

Public Sector
(National Intelligence Service)

Military
(MND)

Military Officer, Server & PC

Private Sector
(Korea Communications Commission)

Nationa Cybersecurity Strategy Council

IPTV, VoIP
Portal

Government
Public Org
Mobile
Financial

Military Websites

IPTV, VoIP
Portal

Internet
Article 48-2 (Response, etc. to Infringement Accident)
(1) The Chairman of Korea Communications Commission shall perform the task falling under each of the following subparagraphs to properly cope with any infringement accident and may, if necessary, get the Security Agency to perform the task, in whole or in part:
   1. The collection and dissemination of information on infringement accident;
   2. The forecast and alert of infringement accident;
   3. Emergency measures against infringement accident; and
   4. Other measures prescribed by the Presidential Decree to cope with infringement accident.
(2) The person falling under each of the following subparagraphs shall furnish information pertaining to infringement accident, including the statistics of infringement accident by type, the statistics of traffic volume in the relevant information and communications networks and the statistics of uses by connection channel, to the Minister of Information and Communication or the Security Agency under the conditions as prescribed by the Ordinance of the Korea Communications Commission:
   1. The provider of major information and communications services;
   2. The business operator of agglomerated information and communications facilities; and
   3. Other person who is prescribed by the Presidential Decree as the operator of the information and communications networks.

Article 48-3 (Report on Infringement Accident, etc.)
(1) The person falling under each of the following subparagraphs shall, when any infringement accident occurs or he finds signs of any infringement accident, report without delay the occurrence of such infringement accident or his finding of such signs to The Chairman of Communications Commission or the Security Agency. In this case, if any notice is served in accordance with Article 13 (1) of the Act on the Protection of Information and Communications Infrastructure, such notice shall be deemed the report referred to in the former part:
   1. The provider of information and communications services;
   2. The business operator of agglomerated information and communications facilities; and
   3. Other person who is prescribed by the Presidential Decree as the operator of the information and communications networks.
Evolution of Cyber Incident

Security Threat Paradigm

1998
- Hacking, virus
- DoS
- Internet Worm
- Independent attack
- Point Security Solution (IDS, F/W)
- Increase of industrial spy/ internal breach
- Increase of cross-border hacking activity
- DDoS by BOT (increase of malicious traffic)

1999-2003
- DDoS
- Internet Worm
- Distributed attack
- Embedded, automatic
- Integrated security management
- Distributed detection /analysis
- Security trend analysis
- BOT, BotNet
- Spyware, Crimeware
- Phishing
- Organized Crime (financial)
- Focused/smarter
- Social engineering
- Intelligent security system
- Threat management framework
- Coop orgs/info sharing
- Policy/managerial security

2004-Present
- BOT, BotNet
- Spyware, Crimeware
- Phishing
- Organized Crime (financial)
- Focused/smarter
- Social engineering
- Intelligent security system
- Threat management framework
- Coop orgs/info sharing
- Policy/managerial security

Increase of personal credential leakage
Increase of online financial crime
Increase of industrial spyINTERNAL breach
Increase of cross-border hacking activity
DDoS by BOT (increase of malicious traffic)
President

National Cybersecurity Strategy Council
(Chair: Head of NIS)

National Cybersecurity Planning Council
(Chair: 2nd Head of NIS)

President

Joint Investigation

Public: NIS, MND, KCC
Private: experts from industry/academic/research

Recovery Support

Public: NIS, MND, KCC
Private: experts from industry/academic/research

Ministry of National Defense
Defense Security Command
Military Area/each unit

National Intelligence Service
KNCERT/CC
Critical Infrastructures in Government/public sector

Korea Communications Commission
KrCERT/CC
Critical Infrastructures in private sector

## National Cybersecurity Framework

### Internet Security Warning Level

<table>
<thead>
<tr>
<th>LEVEL</th>
<th>CONTENTS</th>
</tr>
</thead>
</table>
| Critical     | - Traffic error occurs over all the Internet service areas of the nation.  
- Damages to major information and communication infrastructure facilities cause inconvenience in the service function to the general public.  
- Internet services in a private sector are paralyzed.  
- Collaborative response in a national level is required.                              |
| Severe       | - Multiple ISP networks or major information and communication infrastructures impaired.  
- Hacking attacks and new security threats cause serious damages in private sector including major corporations, portal sites, laboratories, etc.  
- Private sectors suffers from widespread damages arising from worm, virus and hacking.  
- Collaborative response and action between a private sector and a government is required. |
| Substantial  | - Regional damage is incurred by worm, virus, hacking, etc.  
- Regional Internet communication errors or internet service-related errors occurs or might occur.  
- Urgent security measures should be taken by ISP/IDC, general individual users and corporations. |
| Moderate     | - The appearance of highly threatening worms, viruses, vulnerabilities, hacking methods and attacking codes might increase the possibility of damages.  
- Security incidents are spreading in other countries and the network of the nation is increasingly vulnerable to security threats.  
- The increased possibility of abnormal traffic in the domestic Internet.               |
| Normal       | - Internet communication traffic in a private sector is flowing smoothly  
- Unless they don't affect Internet communication or its usage - Malicious codes including worms and viruses were detected  
- New security flaws or hacking methods were announced  
- Possible existence of regionally abnormal traffic with low risk |
National Cybersecurity Framework

Local Cooperation Framework

Public Sector: Government, Public Orgs

- National Cyber Security Center
  - Incident Escalation & Info Sharing
- Education support
  - Internet Crime related Support
- Onsite Joint Investigation
  - Incident Escalation for Serious Crime
- Technical Documents
  - Hacking Analysis report

Private Sector: ISP, IDC, etc

ISP/IDC/SO

National Crisis Situation Center

KOREA COMMUNICATIONS COMMISSION

National Cybersecurity Framework
Zombies do not act on real-time basis, no herder needed
Crafted to act based on pre-designed scenario
Damages fixed drive on certain time

C&C blocking does not work
Clearing possible only when entire zombies are cured
Limited countermeasure in network aspect
7.7 DDoS

**Attack & Response Flow**

1. 1st DDoS attack (1900)
2. 2nd DDoS attack (1800)
3. 3rd DDoS attack (1800)
4. HDD attack (0000)
5. DDoS attack ended (1800)

**External**
- 7/7
- 7/8
- 7/9
- 7/10
- 7/11
- 7/12
- 7/15

**Internal**
- Issue Warning ‘Substantial’ (0240)
- Block Malware Host
- Block Malware Host
- Block HDD damage hosts
- Block HDD damage hosts
- Block HDD damage hosts
- Alert on HDD Destruction (2330)
- Warning level down to Moderate (1500)

- DDoS malware sample secured
- Forward sample to AV vendor
- HDD damage info secured
- Block HDD damage hosts
- Initiate Public Service for HDD damage
- Malware host info secured
7.7 DDoS

Attack & Response Timeline

DDoS attack occurred (7 Jul)

DDoS Attack Terminated

Attack detected by DDoS Response System

Attack Log & IP Secured (7 Jul)
(KrCERT/CC, Auction, Naver)

Request & Secure Zombies (7 Jul)

Analyze zombie (remote & onsite)

Handling Entire zombies (15 Jul)

Confirmed there’s no C&C

Malware Analysis

DDoS malware Collected (7 Jul)
Thank you
twpark@krcert.or.kr