Police Technical Approach to Cyber Threats

Jumpei Kawahara
Director of High-Tech Crime Technology Division,
National Police Agency, Japan
1 Overview
Current Situation

Number of consultations on cybercrimes, etc.

- Others
- Illegal and harmful information
- Internet auction fraud
- Unauthorized access and virus
- Defamation and abuse
- Spam e-mails
- Fraud and fraudulent business

<table>
<thead>
<tr>
<th>Year</th>
<th>Cases</th>
</tr>
</thead>
<tbody>
<tr>
<td>2011</td>
<td>80,273</td>
</tr>
<tr>
<td>2012</td>
<td>77,815</td>
</tr>
<tr>
<td>2013</td>
<td>84,863</td>
</tr>
<tr>
<td>2014</td>
<td>118,100</td>
</tr>
<tr>
<td>2015</td>
<td>128,097</td>
</tr>
</tbody>
</table>

Cases in 2015:
- Others: 15,822
- Illegal and harmful information: 4,854
- Internet auction fraud: 6,274
- Unauthorized access and virus: 7,089
- Defamation and abuse: 10,398
- Spam e-mails: 16,634
- Fraud and fraudulent business: 67,026
Advantages of Police

- Authority for investigation
- Nationwide working units
- Own technological capability
Police Organization for High-Tech Crime Technology

National Police Agency

High-Tech Crime Technology (HTCT) Div.

- Digital Forensic Center
- Cyber Force Center

Technical Support

Counter Cybercrime
- Cybercrime Div.

Counter Cyber Attack
- Security Planning Div.

Other crimes
- General Crimes
- Organized Crime
- Traffic
- Child Sexual Exploitation / Abuse
- etc.
Mission of HTCT Organization

To provide technical expertise to tackle cyber threats

Digital Forensics

- analysis of evidence stored in digital devices
- technical support for search, seizure, inspection, etc.

Cyber Forces

- 24/7 basis detection and analysis of suspicious traffic
- cooperation with private sectors
- malware analysis
- incident response activity
2 Digital Forensics
Digital Forensics

Extract

Digital devices seized at crime scenes

Visualize

Electronic evidence

E-mails
Accounts
Address List
etc.

Analyse

Identification of criminals
Proof of crimes
Disclosing crime syndicate
Electronic evidence can be valuable based on:

- **Correctness** of Procedure
- **Accuracy** of Analysis
- **Objective Verifiability**
Organization for Digital Forensics

- National Police Agency
  - Digital Forensics Center
- Regional Police Bureaus
- Prefectural Info-Communications Departments

Highly advanced digital forensic analysis
Handling Broken Mobile Phone – Transplant(1)

Broken smartphone

Removed circuit

Circuit

Memory IC
Handling Broken Mobile Phone – Transplant(2)

1. Transplant into alternative device (the same model as the broken one)
2. Analysis!
3  Cyber Forces
Cyber Forces Organization (CFs)

— Nationwide technical task forces for counter cyber attacks

CFs promote preventing cyber attacks and mitigating the damage in coordination with Critical Infrastructure providers, etc.
Real-time Detection Network System

Cyber Force Center

- Darknet Observation
- Web Defacement Detection
- DoS Attack Observation
- P2P Network Observation

Sensors

- Scanning
- Compromised

Illegal file
File-sharing network
Suspicious Incoming Packets

* Captured by NPA’s sensors

( packets per day per IP address )

<table>
<thead>
<tr>
<th>Year</th>
<th>FH</th>
<th>SH</th>
<th>FH</th>
<th>SH</th>
<th>FH</th>
</tr>
</thead>
<tbody>
<tr>
<td>2014</td>
<td>448.2</td>
<td>534.2</td>
<td>684.9</td>
<td>773.0</td>
<td>1119.1</td>
</tr>
<tr>
<td>2015</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2016</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* 2016 FH: 1119.1 packets per day per IP address.
Linux-based Devices

are drawing interest of attackers as hop points of attacks

Captured packets ～ destination port “23/TCP” (telnet)

0

2,000


Sharp increase

(packets / day / IP address)
Scanning Industrial Control Systems
connected to the Internet are continuously exposed to scans

Potential attackers
Industrial control system
Search engine on online devices

Scanning...
scan
scan

Suspicious Scanning Activities Discovered(2)
4 Our Efforts
Measures against Cyber Threats

Cyber Force Center

Suspicious traffic

Information sharing with local CFs, polices, private sectors, etc.

Analysis

Police-Industry Joint Drill

Calling public attention to threats on the portal website “@police”

(http://www.npa.go.jp/cyberpolice/)
Malware Information Sharing

Malware Analysis
- Dynamic Analysis
- Static Analysis

Counter Cyber Attack Section of NPA

Information sharing

Advanced Technology Industry

Critical Infrastructure

Anti Virus Vendors

Managed Security Service Providers
“Counter-Cybercrime Technology and Investigation Symposium (CTINS)” for Police officers and technical officers in Asian & Pacific region

— Discussions, Lectures & Hands-on Training

Experts Meetings

with digital forensics experts from foreign law enforcement agencies
Educational Training
at the National Police Academy
for experts in digital forensics, etc.
and for new employees

Nationwide Training Environment
as the basis of remote training for
nationwide CF members in terms of:
- incident response
- analysis of electronic evidences