The incident response and the police in Japan

Yoshio Yamada
Assistant Director,
High-Tech Crime Technology Division,
National Police Agency, Japan
Structure of Japanese police
Roles of High-Tech Crime Technology Division
Cyber Force Center
Cooperation among the organizations including the police
Effort of early warning by the police
Actual incident responses
Organization of Japanese government

Diet
- House of Representatives
- House of Councilors

Cabinet
- Cabinet Office
  - National Public Safety Commissions
    - National Police Agency
  - Other Agencies
  - Other Ministries

Courts
- Supreme Court
- High Courts
- District Courts
- Summary Courts
- Family Courts
Roles of the High-Tech Crime Technology Division (HTCTD)

- **Technical support**
  - Technical support for local police force’s investigations
  - Technical analysis on the Internet activities
  - Provide training for staff (officers and engineers)

- **International cooperation on technical matters**
  - 24 hour point of contact in technical area (G8, ICPO, etc…)
  - Technical capacity building

- **Research and Development**
  - Research of emerging technologies
  - Development of technical tools and standards for investigation support
Roles of HTCTD

HTCTD plays an important role in the following areas:

**Digital Forensics**
Sophisticated analysis provided by forensic examiners
(computer virus, malicious code, cyber crime and cyber-terrorism attempt.)

**Computer Incident Prevention and Response at Critical Infrastructures**
Support to limit the damage of attacks aiming at computer network systems of critical infrastructures on the Internet.
Duties:

- Technical matters to prevent crimes against information systems which could affect life, social and economic activities, and of incident response to control damage caused by the crimes (Cabinet Office Ordinance)
Counter cyber terrorism initiative by the police

- objectives
  - prevention
  - damage control
  - arrests
Measures and policies

- Acquire predictive information and recognize cases at the 24h operating “cyber force”
- Provide information through the Internet
- Strengthen cooperation with critical infrastructures
- Strengthen cooperation with foreign LE agencies
- R&D for counter cyber terrorism
- Human resource development
- Strengthen information-gathering and investigative capability
Cyber Force Activities

- Operation of Internet threat monitoring systems
  - IP packets monitoring
  - Botnet monitoring
  - Malware capture

- Cooperation with critical infrastructures
  - Periodical meetings
  - Contact points

- Cooperation with outside organizations
  - Information Security Center, Cabinet Secretariat

- Information dissemination
  - @police
  - Mailing list amongst critical infrastructures

- Information-gathering and analysis
  - Security Planning Division
  - Cyber Crime Division, etc.

- National Police Agency

- Incident response at critical infrastructure
  - Technical support for local police forces
- IP packets monitoring
- Botnet monitoring
- Malware capture
Changes of the number of access against firewall

![Chart showing changes in access against the firewall from 2003 to 2008. The chart indicates a decrease in access over the years.]
Changes of the number of access
to destination TCP port 445

Per day/IP adress

Oct. 1st  Oct. 31st  Nov. 30th  Dec. 31st

- Japan
- PRC
- US
- Taiwan
- India
- Others/Unknown
Changes of the detected number of SYN flood attacks

- 2005: 263,827
- 2006: 214,977
- 2007: 91,417
- 2008: 377,825
- IP packets monitoring
- Botnet monitoring
- Malware capture
The number of bot-infected PCs in Japan:

<table>
<thead>
<tr>
<th>Year</th>
<th>Number of bot-infected PC in Japan</th>
<th>Number of bot-infected PC in the world</th>
<th>Ratio of bot-infected PCs in Japan</th>
</tr>
</thead>
<tbody>
<tr>
<td>2005</td>
<td>149,609</td>
<td>1,337,167</td>
<td>11.2%</td>
</tr>
<tr>
<td>2006</td>
<td>108,626</td>
<td>1,025,253</td>
<td>10.6%</td>
</tr>
<tr>
<td>2007</td>
<td>46,953</td>
<td>874,980</td>
<td>5.4%</td>
</tr>
<tr>
<td>2008</td>
<td>16,529</td>
<td>551,226</td>
<td>3.0%</td>
</tr>
</tbody>
</table>
The number of DoS attack
commands in botnet

<table>
<thead>
<tr>
<th>Year</th>
<th>SYN flood attack</th>
<th>UDP flood attack</th>
<th>PING flood attack</th>
</tr>
</thead>
<tbody>
<tr>
<td>2005</td>
<td>2,000</td>
<td>2,000</td>
<td>2,000</td>
</tr>
<tr>
<td>2006</td>
<td>4,000</td>
<td>8,000</td>
<td>4,000</td>
</tr>
<tr>
<td>2007</td>
<td>8,000</td>
<td>4,000</td>
<td>8,000</td>
</tr>
<tr>
<td>2008</td>
<td>16,000</td>
<td>12,000</td>
<td>16,000</td>
</tr>
</tbody>
</table>
Victim: a local government
Damage: webpage defacement

Our Action

We preserved its HDD as an evidence and advised the victim to limit the access permitted IP address; verify the web server’s vulnerabilities.

further investigation…
Victim: a financial institution
Damage: DoS (web)

We gave mitigating countermeasure to the victim, then collect attacker's information from the server's access log for further investigation.

further investigation…
End