Digital Forensics and CSIRT Activities

NTT Computer Security Incident Readiness and Response Coordination Team

NTT Research and Development Headquarters
Tomohiko Yamakawa
NTT-CERT, organized in 2004 as the representative CSIRT of the NTT group, is responsible for prevention and damage minimization against cyber-attacks.

Provide “security services” to group colleagues for more secure

<table>
<thead>
<tr>
<th>Proactive</th>
<th>Reactive</th>
<th>Security Quality Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public Monitoring</td>
<td>Vulnerability handling</td>
<td>Evaluation of products and technologies</td>
</tr>
<tr>
<td>Security Alerts</td>
<td>Incident handling</td>
<td>Security consultation</td>
</tr>
<tr>
<td>Security Reporting</td>
<td>Digital Forensic</td>
<td>Training</td>
</tr>
<tr>
<td>Incident Detection</td>
<td>Malware Analysis</td>
<td>Enlightenment</td>
</tr>
</tbody>
</table>
Reactive Services/ Incident and Vulnerability Handling

**Incident handling**

Cooperation

Trusted third parties

Companies

Information

Requests for support

Detection

Support and coordination

Companies

Provide experience
Deep investigation with detection tools
Forensic support
Provide laboratory expertise

Support and coordination to minimize damage from incidents that have occurred

**Handling unpublished vulnerability information**

Obtain and organize information

Share data and investigations with relevant departments
Adjustments at time of publishing

Coordination with relevant departments of the NTT Group on investigation, countermeasures and preparations for the day of publication regarding unpublished vulnerabilities
Digital Forensics and Malware Analysis

- In case of unauthorized attack and information leakage, NTT–CERT supports group companies by providing technical support, such as digital forensics, malware analysis, and so on.
- In order to know what happened, to identify the scale of incident, to prevent further damages (not as legal responses but as technical or management ones)
- Log analysis, malware analysis, and so on

1st
Collecting information to preserve

Damaged PC (system)

2nd
Analysis

Analyze
Detecting malware
Analyzing malware
Logs of NW apparatus
Logs of NW apparatus
Information analyze

3rd
Documentation

- cause
- process
- response
Role of CSIRT and other division

- Information or data remain at the hand of system owner/operator
- CSIRT can not do forensics and other analysis (log analysis, malware analysis, and so on) without support or cooperation of system owner/operator

Information security management

CISO (CIO) → System owner → CSIRT

Management of IT operation
- Monitoring
- Information analysis
- Assessment

Incident handling
- Detect
- Triage
- Mitigate
- Response

Report → Feed back

Intrusion
Unauthorized access

LEA = Law enforcement agency
- Require information (mandatory or not)
- Experience and Advanced technologies (?)
Cloud security in Japan

• In 2012 “F case”
  • F, subsidiary of big IT service company, providing cloud servers to many customers (including many SMEs) as a service
  • More than 5700 customers’ data (not “5700 customer data”) disappeared by mistake in operation
  • Difficulty in recover

• 15 March 2014, METI released “Revised Cloud Security Guideline”
  • Mainly for prevention but partly recommending for “collecting evidence” as follows
    • Management
      • If security incident happens, (service provider and system owner) should collect, preserve, and submit data complying with law and regulations.
    • For cloud users
      • For appropriate data collection and preservation, users should confirm service provider whether necessary data is surely reserved and managed.
    • For service provider
      • Service provider should reserve data and inform its customer the fact with terms of data reservation.
    • FYI
      • Supportive service such as e-discovery would be fine...