Back to the ‘root’ of Incident Response

Boston Park Plaza Hotel | June 22-27, 2014
First Step Guide for Building Cyber Threat Intelligence Team

Hitoshi ENDOH (NTT-CERT)
Natsuko INUI (CDI-CIRT)
Agenda

• About Us
  • CDI-CIRT
  • NTT-CERT

• Part 1 – Cyber Threat Intelligence Team Building Basics

• Part 2 – NTT-CERT’s experience (case study)

• Part 3 – Comparison of 2 Different Teams

• Summary
Agenda

• About Us
  • CDI-CIRT
  • NTT-CERT

• Part 1 – Cyber Threat Intelligence Team Building Basics

• Part 2 – NTT-CERT’s experience (case study)

• Part 3 – Comparison of 2 Different Teams

• Summary
About CDI-CIRT

• Cyber Defense Institute Cyber Incident Response Team
• Provides incident response services to clients and non-clients (private & public sector)
• Most activities are within Japan
• Cooperation with international organizations

Contact us at cirt@cyberdefense.jp

For more details, please visit us below, thanks!
http://www.cirt.jp/
Who am I? What do I do?

• Natsuko Inui
• Chief Analyst @ Cyber Defense Institute
• Incident Response (Coordination)
• Cyber Exercises
• OSINT, Research
• Most work is with the Public Sector (Including Defense)

• Cleaning up after my boss
Cleaning up after my boss

After your first year, they give you a rake.

KEEP CALM
BOSS MAKING A MESS

© Just Jobs.com

IS YOUR BOSS A SLAVE-DRIVING PSYCHO?
Hobbies, loves

• Ducati Monster 696
  • Aella Slip-on Silencer

• Flute
  • Started lessons again this year!

• Music (highly addicted)
  • Classical to R&B to Heavy Metal
About NTT-CERT

- NTT is the biggest telecommunication company in Japan. (946 subsidiaries, 240k employees)
- NTT Group provides a lot of public services.
- Our constituency is NTT Group.
- POC of security matters related NTT Group.

https://www.ntt-cert.org/index-en.html
Who am I? What do I do?

- Hitoshi Endoh
- Research Engineer @ NTT Secure Platform Labs.
- Cyber threat analysis
- OSINT, Research
- Community Activities (JNSA, NCA, etc.)

JNSA: NPO Japan Network Security Association
NCA: Nippon CSIRT Association
Agenda

• About Us
  • CDI-CIRT
  • NTT-CERT

• Part 1 – Cyber Threat Intelligence Team Building Basics

• Part 2 – NTT-CERT’s experience (case study)

• Part 3 – Comparison of 2 Different Teams

• Summary
The 3 Steps – Back to the Basics

• Recognition

• Assessment

• Taking Action
Step 1. Recognition

• Situational Awareness
  • Know your enemy
  • Know thyself

• Lesson Learned
  • No “off-the-shelf” solution
    • Think!! Don’t be lazy!!
  • Attackers “try” too
  • (Japan) Third party “marunage”
Step 2. Assessment

• Don’t forget what you learned in the “recognition” phase

• Measure the risk(s)
  • Where should sensors be implemented?
  • Leveraging knowledge through discussions
Step 3. Taking Action

• Building the entire mechanism
  • Framework
  • System
  • Human resources
  • Operation

• Lessons Learned
  • Aligning indicators, reading patterns
  • Gathering information (FIRST members, blacklists, reports)
  • Defining the roles of human resources
Agenda

• About Us
  • CDI-CIRT
  • NTT-CERT

• Part 1 – Cyber Threat Intelligence Team Building Basics

• Part 2 – NTT-CERT’s experience (case study)

• Part 3 – Comparison of 2 Different Teams

• Summary
NTT-CERT’s experience (case study)

• Introduce NTT-CERT’s Activities based on CDI’s 3 steps
  • Step 1. Recognition
  • Step 2. Assessment
  • Step 3. Taking Action

• Sharing OSINT information
• Lessons Learned
Step 1. Recognition
Step 2. Assessment

• Proactive measures are very important. NTT Group provides national critical infrastructure of network communications.

• NTT-CERT needs Cyber Threat Intelligence Team.

• OSINT is suitable for us to collect information. Due to limitation of Japanese law, we can’t use subsidiaries’ log data.

• OSINT is very useful to share (no confidential information).
## Step 3. Taking Action in 2013

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Team building**
- **Setting up, start daily work**
- **Training**
- **Quarterly report (Apr.-Jun.)**
- **Start sharing information**
- **Quarterly report (Jul.-Sep.)**
- **Conference Speaker**

*Image: BOSTON 26th annual FIRST conference*
Training by Senior Analyst, outside the company

Benefit:

• Great skill up in the short term
• Valuable tools for collecting information and How to collect information safely
• Other useful tools and How to use them
• Methodology of making threat analysis, analyst report
• Improvement of expression ability
• Lessons Learned, Beneficial Know How
## Daily Work

<table>
<thead>
<tr>
<th>Time</th>
<th>Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>9:30</td>
<td>Collect articles</td>
</tr>
<tr>
<td>10:00</td>
<td>Read articles, Summarize</td>
</tr>
<tr>
<td>11:00</td>
<td>Sharing, discussion</td>
</tr>
<tr>
<td>12:00</td>
<td>- Detail analysis</td>
</tr>
<tr>
<td>13:00</td>
<td>- Tools evaluation</td>
</tr>
<tr>
<td>14:00</td>
<td>- Create reports</td>
</tr>
<tr>
<td>15:00</td>
<td>- etc.</td>
</tr>
<tr>
<td>16:00</td>
<td></td>
</tr>
<tr>
<td>17:00</td>
<td></td>
</tr>
</tbody>
</table>
Sharing OSINT information

NTT-CERT

I don’t know why.

Oh, I got it!!

Share

Feedbacks

Other CSIRTs

It’s a difference of perspective
L/L (1/4) OSINT Requirements

- Isolated Network from intranet
- Virtual PC and Resets every use
- Secure Browser with plug-ins
  (A lot of Japanese don’t use plug-ins)
- Research tools
  (ex. Keeping source IP secret.)
L/L (2/4) Local Languages are very important

- Most detail information from local language
- Slang (Not in Dictionary, Rapid change)

<table>
<thead>
<tr>
<th>Language</th>
<th>Cyber Attack</th>
</tr>
</thead>
<tbody>
<tr>
<td>English</td>
<td>Cyber Attack</td>
</tr>
<tr>
<td>Japanese</td>
<td>サイバー攻撃</td>
</tr>
<tr>
<td>Chinese</td>
<td>网络攻击</td>
</tr>
<tr>
<td>Korean</td>
<td>사이버 공격</td>
</tr>
<tr>
<td>Russian</td>
<td>кибератака</td>
</tr>
<tr>
<td>Arabic</td>
<td>هجوم عبر الانترنت</td>
</tr>
</tbody>
</table>
L/L (3/4) Local languages are very important

- Machine Translation is not perfect.

“軍艦巻き” is a kind of Sushi!
L/L(4/4) Facility

• World news programs with large screen televisions
  → Notice a big news quickly
  → Get latest topics and key words
Future work

• Sharing and Collaborating widely, Extending our knowledge
• Social Media
• Useful Tools
• Multilingual
• Imaginations (ex. Media literacy) (There is no Media literacy curriculum in Japanese school.)
Agenda

• About Us
  • CDI-CIRT
  • NTT-CERT
• Part 1 – Cyber Threat Intelligence Team Building Basics
• Part 2 – NTT-CERT’s experience (case study)
• Part 3 – Comparison of 2 Different Teams
• Summary
## Comparison of 2 Different Teams

<table>
<thead>
<tr>
<th>Category of Business</th>
<th>CDI-CIRT</th>
<th>NTT-CERT</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Vendor</td>
<td>Telecommunication</td>
</tr>
<tr>
<td>Important thing</td>
<td>Specialty</td>
<td>Teamwork</td>
</tr>
<tr>
<td>Position of the intelligence</td>
<td>Cutting edge</td>
<td>For proactive defense for NTT Group</td>
</tr>
<tr>
<td>Constituency</td>
<td>Client / Non Client (some exceptions)</td>
<td>All Group Companies</td>
</tr>
</tbody>
</table>
Comparison of 2 Different Teams

<table>
<thead>
<tr>
<th></th>
<th>CDI-CIRT</th>
<th>NTT-CERT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Relationships with other specialists</td>
<td>By personal efforts</td>
<td>By Team’s activity</td>
</tr>
<tr>
<td>Situation Awareness</td>
<td>IR itself</td>
<td>Cyber Threat is global</td>
</tr>
<tr>
<td>Shortage</td>
<td>SOC</td>
<td>Fixed members</td>
</tr>
</tbody>
</table>

- There are big differences between 2 companies same in Japan
Agenda

• About Us
  • CDI-CIRT
  • NTT-CERT
• Part 1 – Cyber Threat Intelligence Team Building Basics
• Part 2 – NTT-CERT’s experience (case study)
• Part 3 – Comparison of 2 Different Teams
• Summary
Summary

• No “off-the-shelf” solution for Cyber Threat Intelligence Team
  Think!! Don’t be lazy!!

• CDI’s 3 step methodology is useful for building the team
Thank you!