IOC-DREAM

-- IOC Distribution in Restricted Environment and Automating response based on MISP

Yifan Wang, Fukusuke Takahashi, Kunio Miyamoto

June 5th, 2023

NTTDATA-CERT | Information Security Office | Cyber security engineering department | NTT DATA Corporation
Agenda

• Self Introduction
• Why we choose MISP
• What we implement via MISP
• Integration with others
• Real threat response
• Future work
Introduction
Self Introduction

• **NTTDATA-CERT**
  • CSIRT team of NTT DATA Corporation HQ, established on Jul 1st, 2010 in Tokyo
  • Handle internal incident response over 15 years, have over 20 skilled members

• **Authors**

  **Yifan Wang**  
  <Yifan.Wang@nttdata.com>  
  Joined NTTDATA-CERT from 2017, worked on IR, OSINT, SOAR for 6 years

  **Fukusuke Takahashi**  
  <Fukusuke.Takahashi@nttdata.com>  
  Joined NTTDATA-CERT from 2018, worked on IR, OSINT, SOAR for 5 years

  **Kunio Miyamoto**  
  <Kunio.Miyamoto@nttdata.com>  
  Work at NTTDATA-CERT for 13 years (one of NTTDATA-CERT founders)  
  One of Speaker of 31st Annual FIRST Conference@Edinburgh
Why we choose MISP
Old workflow (Security Operation)

Have to collect threat intelligence due to multiple sources

Suspicious mail

SIEM Detection

External organizations/sites

Have to wait more minutes due to over 10000 IoCs in shared book

(2) Management Book

The process:

Give me the automated process!!!

Have to deploy on the device due to manual IoC extraction

Firewall

SIEM

Group companies

(1) Input

IOC management sheet

(3) Output
Old workflow (Threat Sharing)

- In most cases, it would spend over 1 day from distribution to final deployment
- When some operation miss occurred, there would be a **vicious circle** for extra N days

Please let me share the IoCs in real-time…
About MISP

• **MISP** : **Malware Information Sharing Platform**
  - An opensource threat intelligence sharing platform
  - with sharing, storing and correlating functions

• **MISP Format**
  » **MISP Event** :
    - Used to manage each threat
    - Commonly created for each Incident/Malware/Detection

  - **MISP Attribute** :
    - Used to manage each IoC
    - Commonly created for each IoC, which is related and included within a MISPevent

* [https://indico.cern.ch/event/595396/contributions/2566371/attachments/1448720/2233260/2017-04-25__MISP_Training_slides.pdf](https://indico.cern.ch/event/595396/contributions/2566371/attachments/1448720/2233260/2017-04-25__MISP_Training_slides.pdf)
Benefit of MISP integration within NTTDATA Group

1. Optimize SOC workflow and implement SOC automation
   -> Details would be introduced as next slides.

2. Expand available, trusted IoC sources without self-validation
   -> Not only worldwide attacks, some specified/targeted attack information also can be shared as soon as possible.

3. Solve time-lag problem in incident response or other emergency cases.
   -> real-time IoC Sharing is the beginning of real-time auto-response.
What we implement
New Automated workflow based on MISP

Automate the workflow by API integration 😊
=> over 35000$/year cost reduction
Jenkins jobs used for daily security operation of NTTDATA-CERT

<table>
<thead>
<tr>
<th>S</th>
<th>名前</th>
<th>最新の成功ビルト</th>
<th>最新の失敗ビルト</th>
<th>ビルド所要時間</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><img src="image" alt="MISP_Event_Extract_from_SOC_confirmed(PyMISP)" /></td>
<td>11 時間 #105</td>
<td>29 日 #76</td>
<td>19 秒</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="MISP_Event_Output(PyMISP)" /></td>
<td>22 時間 #452</td>
<td>8 日 0 時間 #446</td>
<td>24 秒</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="MISP_Event_Republish_to_Outside(PyMISP)" /></td>
<td>1 日 13 時間 #988</td>
<td>一</td>
<td>6 分 23 秒</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="MISP_Event_Upload(PyMISP)" /></td>
<td>1 日 13 時間 #631</td>
<td>23 日 #620</td>
<td>17 秒</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="MISP_Exa_Enrichment_01(Common)" /></td>
<td>21 時間 #86</td>
<td>一</td>
<td>18 秒</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="MISP_HealthCheck" /></td>
<td>29 分 #16386</td>
<td>一</td>
<td>1.6 秒</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="MISP_Job_Input_02(CCI_mail)" /></td>
<td>1 ヶ月 2 日 #58</td>
<td>一</td>
<td>3.8 秒</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="MISP_Job_Input_03(CCI_req)" /></td>
<td>13 時間 #842</td>
<td>一</td>
<td>25 秒</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="MISP_Job_Input_05(Other)" /></td>
<td>9 日 4 時間 #240</td>
<td>一</td>
<td>3.7 秒</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="MISP_Job_Input_06(Suspicious_mail)" /></td>
<td>21 時間 #505</td>
<td>29 日 #494</td>
<td>43 秒</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="MISP_Meta_Enrichment_01(Common)" /></td>
<td>13 時間 #1508</td>
<td>一</td>
<td>16 秒</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="MISP_Type_Classification_00(PyMISP)" /></td>
<td>13 時間 #1496</td>
<td>一</td>
<td>12 秒</td>
</tr>
</tbody>
</table>

1. Extract IoC from different sources
2. Process IoC with formatting for MISP
3. Enrichment with external services like SIEM
4. Upload to MISP
5. Integration with others
Integration with others
MISP Integration Architecture within NTT Group

- NTT Group MISP Hub
- NTT HQ
- NTT-CERT
- NTT EAST
- NTT WEST
- NTT DATA
- NTT DATA INTELLILINK
- NTT Communications
- NTT DATA Americas, Inc.
- NTTDATA-CERT
- NTT DATA Italy - zenSOC
- NTTDATA-ES-CERT
- Incident Response
- Suspicious Mail Analysis
- Malware Traffic Analysis
- SANS
- Abuse.ch
- External OSINT
- MISP Feeds
- External Organizations
- SIEM
- DQB
- Proxy
- FIRST

Manual → Auto
Data flow on MISP (for TLP:RED)

To-Be:
IoCs of TLP:RED would not be shared to outside of each OpCo

Solutions:
- add push rules for connected instances
- set distribution as “Your organization ONLY”
- NOT publish
Data flow on MISP (for TLP:AMBER)

OpCo’s CSIRT

To-Be:
IoCs of TLP:AMBER would not be shared to outside of NTTDATA Group

Solutions:
- add push rules for connected instances
- set distribution as “Connected communities”
Data flow on MISP (for TLP:GREEN)

**To-Be:**
IoCs of TLP:GREEN would not be shared to outside of NTT Group

**Solutions:** (apply on NTTDATA HQ, Other NTT companies)
- add push rules for connected instances
- set distribution as “Connected communities”

Change distribution to forward IoCs to other NTT companies

Change distribution to forward IoCs to their group companies
Data flow on MISP (for TLP:WHITE)

To-Be:
IoCs of TLP:WHITE would be shared to all connected instances.

Solutions:
- set distribution as “All”
- NO need to share official MISP feeds
- Add push rules on connected instances
Real threat response
-- Emotet
## Background

<table>
<thead>
<tr>
<th>News</th>
<th>Event</th>
<th>Sample</th>
<th>Opened</th>
<th>Note</th>
</tr>
</thead>
</table>
| Nov  | Emotet restarted[1]  
Dec   | Compromised case appeared @Japan [2] | | | |
| 2021 | | | | |
| Feb  | 1st Suspicious mail received @NTTDATA-CERT | ○ | | |
| Feb 4 | 1st Suspicious mail opened by Group company A | ○ | | |
| Feb 8 | Suspicious mail received @Group company A | ○ | | |
| Feb 10 | 2nd Suspicious mail received @NTTDATA-CERT | ○ | | |
| Feb 22 | Monitor & Block started | | | |
| Feb 28 | 3rd Suspicious mail received @NTTDATA-CERT | ○ | | |
| Mar 3 | 2nd Awareness of JPCERT/CC [3] | | | |
| Mar 22 | Suspicious mail opened by Group company B | ○ | | |
| Apr 26 | 3rd Awareness of JPCERT/CC [3] | | | |
| Mar 28 | 2nd Suspicious mail opened by Group company A | x | | Detected & blocked |
| May 10 | Monitor & Block finished | | | No events in April and May |

Review of HQ’s Emotet IoC collection

• Import IoCs of Emotet from abuse.ch by script
  • FeodoTracker
  • URL Haus (tag:emotet)
• Difference from abuse.ch feed on MISP
  • Abuse.ch feed on MISP
    - Import each URL as an MISPEvent
  • Import tool (script)
    - Import URL/domain/IP into MISP
    - Segment all IoCs (Each MISPEvent has 1000 MISPAttributes)
• Flexible for customization
  - Extract domain/IP/fqdn from URL for block-list
  - Add sighting to mark the status online/offline
    - Also can be used for visualization and evaluation
## Review

### Sources

<table>
<thead>
<tr>
<th>Date of mail received</th>
<th>Event</th>
<th>Count of Malicious traffic</th>
<th>ABUSE.CH</th>
<th>External Organization A</th>
<th>Malware Traffic Analysis</th>
<th>SANS Internet Storm Center</th>
<th>External Organization B</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feb 2</td>
<td>1st Suspicious mail received @NTTDATA-CERT</td>
<td>5</td>
<td>5(〇)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Feb 4</td>
<td>1st Suspicious mail opened by Group company A</td>
<td>12</td>
<td>12(〇)</td>
<td>12(×)</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Feb 8</td>
<td>Suspicious mail received @Group company A</td>
<td>20</td>
<td>20(〇)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Feb 10</td>
<td>2nd Suspicious mail received @NTTDATA-CERT</td>
<td>14</td>
<td>14(〇)</td>
<td>14(×)</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Feb 28</td>
<td>Monitor &amp; Block started</td>
<td>7</td>
<td>7(〇)</td>
<td>2(×)</td>
<td>2(×)</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Mar 22</td>
<td>3rd Suspicious mail received @NTTDATA-CERT</td>
<td>8</td>
<td>8(〇)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

(〇) ... Collect IoCs before receive suspicious mail  
(×) ... Collect IoCs after receive suspicious mail

---

All malicious traffic can be blocked by collecting IoCs from abuse.ch

Not enough to block all malicious traffic
Future work
Standard intelligence management process

1. Planning
2. Collection
3. Processing
4. Analysis
5. Dissemination

Effectively manage intelligence with continuous feedback cycles

Joint Chiefs of Staff Document (JP2-0: Joint Intelligence)
https://irp.fas.org/doddir/dod/jp2_0.pdf
To be

NTTDATA-CERT focuses on IoC management and target to implement the process on daily security operation.

- **IoC Management**
  - Process
  - Evaluate performance of each IoC
  - Take inventory to prevent false positives
  - Automatically distribute and deploy on devices
  - Distribute the right IoC for the right device
  - Based on the analysis of threat trends, establish a plan for IoC collection and management
  - Implement automation of IoC collection
  - IoC stored as standard format (STIX/CSV/JSON...)
  - IoC enriched and stored

*Figure 1-3. The Intelligence Process*
Address the gaps between To-be and As-is
NTTDATA-CERT plan to incorporate IoC Metabolism activation model

-> Improve quality of IoCs and respond to threat trends better!

Introduce evaluation process
Implement IoC inventory (IoC metabolism activation model)
Analyze on internal and external threat trends
IoC source evaluation
(IoC metabolism activation model)

Increase integrated devices
Implement automation of IoC distribution.
(IoC metabolic activation model)

Establishment of IoC evaluation method
and Feedback

Figure 1-3. The Intelligence Process