Approach and outcome of “AOKI” - DNS sinkhole by JPCERT/CC.

Sho AOKI
Japan Computer Emergency Response Team Coordination Center (JPCERT/CC)
Agenda

■ Background
  - About JPCERT Coordination Center
  - Sinkhole mechanism & purpose

■ The flow of research & coordination
  - Collect and Investigate
  - Architecture of Sinkhole System "AOKI"
  - Investigate access log and Coordination

■ Tracing Targeted Attack Cases
  - Case Study

■ Future of this project
Self introduction

Sho Aoki

Information Analyst at
Watch & Warning Group,
JPCERT/CC since 2015.

**Collect:**
Collect Information
(Public and Private Disclosure, Incident Reports)

**Analyze:**
Analyze the collected information from various viewpoints

**Transmit:**
Provide or transmit information to appropriate parties
- Public Notification (Website or Mailing List)
- Critical Infrastructure
- Domestic CSIRTs
Background
About JPCERT Coordination Center

- **Foundation** - October, 1996
- **Organization Status & Constituency**
  - An independent, non-profit organization
  - Internet users in Japan, for enterprises
  - Mainly providing service through technical staffs with high degree of professionalism in enterprise
  - International and Regional Activities

**International and Regional Activities**

- Coordinate with developers on unknown vulnerability information
- Secure coding
- Mitigating the damage through efficient incident handling
- Information sharing to prevent similar incidents

**Prevent**
- Vulnerability Information Handling
  - Coordinate with developers on unknown vulnerability information
  - Secure coding

**Watch**
- Information gathering / analysis / sharing
- Internet Traffic Monitoring
  - Alert / Advisories

**Respond**
- Incident handling
  - Mitigating the damage through efficient incident handling
  - Information sharing to prevent similar incidents
Breakdown of coordinated incidents

● Abuse Statistics of FY2015

<table>
<thead>
<tr>
<th>Category</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan</td>
<td>49.9%</td>
</tr>
<tr>
<td>Website defacement</td>
<td>21.9%</td>
</tr>
<tr>
<td>Phishing</td>
<td>14%</td>
</tr>
<tr>
<td>Malware</td>
<td>3.3%</td>
</tr>
<tr>
<td>DDoS</td>
<td>1.2%</td>
</tr>
<tr>
<td>Targeted Attack</td>
<td>0.9%</td>
</tr>
<tr>
<td>ICS</td>
<td>0.2%</td>
</tr>
<tr>
<td>Other</td>
<td>8.6%</td>
</tr>
</tbody>
</table>

● “Targeted attack” has became a prominent topic through news media in Japan

Communication with C2 servers sometimes continued even after completing a series of attacks
Sinkhole mechanism and purpose

● Why we started the sinkhole project

- To identify victim organizations through gathering information from the traces left by the attackers.

● Sinkhole mechanism

- Attackers infect the devices with malware and remotely control it using domains and IP addresses

- Attack infrastructure is usually complex and diverse:
  - Delay in detection
  - Alternative ways to continue access to infected devices
Sinkhole mechanism and purpose

- **Why we started the sinkhole project**
  - To identify victim organizations through gathering information from the traces left by the attackers.

- **Sinkhole mechanism**
  - Some domains are on sale while the communication is still alive:
    - Fund issue
    - Temporary suspension of an attack campaign
Sinkhole mechanism and purpose

● Why we started the sinkhole project
  - To identify victim organizations through gathering information from the traces left by the attackers.

● Sinkhole mechanism
  - Communication from infected devices can be seen by obtaining the associated domains
Sinkhole mechanism and purpose

- Purpose of Sinkhole
  
  [ Mission as a National CSIRT ]
  - To grasp the range of cyber attack damage
  - To notify the victim of the attack and promote countermeasures

  [ Our expectations ]
  - To research attacker behavior in the victim’s PC
  - To research the reliabilities of the attacker’s infrastructure information.
The flow of investigation and coordination
Collect and Investigate

Research the domain to obtain

① Collect information on attack activities
   - Data gained through actual incident coordination
   - Reports published by vendors/researchers
   - Malware database updates

② Investigate relations and similarities with other attack activities
   - Domain information
   - IP addresses change history
   - Similarity in malware and its function
   - Targeted attack method and information on attackers

③ Obtain the domain
   (if expired and available)
Architecture of Sinkhole System "AOKI"

◆ **Web Server**
  - Located in the cloud
  - 80(HTTP) / 443(HTTPS) is open
  - Output access log
  - When the domains are accessed, a webpage is displayed to notify that it is a sinkhole

◆ **Application**
  - Forwards the access log
  - Collects the logs and researches access by day/week/month
  - Manage logs by IPs and domains
  - Manage the obtained domains
Investigate access log and Coordination

- Identify victim organization from public information
  - We basically refer to public information.
    - WHOIS information (organization name, domain name)
    - NS information (domain name)

- Our original application and its featured functions
  - Associate organization names and IP addresses
  - Manage coordination status
    Done / In process / To be assigned / Blacklist
Investigate access log and Coordination

Coordination from JPCERT

<table>
<thead>
<tr>
<th>From JPCERT</th>
<th>Coordination</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Japanese</td>
<td>Coordinate individually in case there is a report on suspicious communication with external servers</td>
</tr>
<tr>
<td>organizations</td>
<td></td>
</tr>
<tr>
<td>To Foreign</td>
<td>Share information gained through sinkhole with the National CSIRT of the economy</td>
</tr>
<tr>
<td>organizations</td>
<td></td>
</tr>
</tbody>
</table>

- Cases coordinated (Sep. 2015 – Mar. 2016)

9 Economies

24 Organizations

33 IP addresses

⇒ Issues have been addressed in 25 IP addresses. about 70% of the total.
Investigate access log and Coordination

**Coordination using a questionnaire**

- **Questions for victims (voluntary)**

  - What is the purpose of the infected device(s)?
    For operation / For personal use / Others

  - Who is the user of the infected device(s)?
    Position / Assigned duties

  - Did you manage to identify the malware and the source of infection?
    Yes / No
    (If yes) Is it possible to share the data with us?
    Yes / No

  - Is there any information stolen?
    (Comments)
Tracing Targeted Attack Cases
Case Study

- Tracing attack activities based on published reports
  - We investigated malware “Elise/Esile”, reported in 2015
  - The attackers seem to be targeting Eastern Asian economies. (VN / PH / TW / HK / ID)

- Motivation
  - We were able to obtain some of the domains used for the attacks
  - We wanted to see the link with the attacks targeting Japan

original tool : Hiryu
https://github.com/S03D4-164/Hiryu
Investigation results after sinkholing

- Information on domains related to the attacks on reports
  (about 50 domains)

<table>
<thead>
<tr>
<th>Category</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domains that work as a sinkhole and that JPCERT/CC observes logs</td>
<td>44%</td>
</tr>
<tr>
<td>Domains that attackers own</td>
<td>16%</td>
</tr>
<tr>
<td>Unknown owners / others</td>
<td>40%</td>
</tr>
</tbody>
</table>

- Criteria for the categorization

  • Judged that attackers own the domain if the WHOIS detail available and the ownership has not changed, or the IP remains as the time of attack campaign
  • Judged “unknown owner” when the registrant information is hidden using WHOIS privacy service etc.
Case Study

- Communication to sinkhole domains (Apr, 2016)
  Analyzed the communication purpose for each unique IP address

35% Scan, searching?
51% Crawler / Spider
14% HTTP request from Elise infected devices

Examples of HTTP request sent from Elise malware
{random numbers}/ketwer90o/{random numbers}.html
{random numbers}/archive/{random numbers}.html
{random characters}/page_{random numbers}.html

source: AOKI incoming traffic
Case Study

- Transition of the number of IP addresses which Elise malware sent a HTTP request to

(number of unique IPs)

A lot of access to “asean-star.com / usa-moon.net / ismartmusic.net / aseaneco.org / phil-healthy.org”

A lot of access to “tgecc.org”


PH  MY  US  SG  VN  NL  Others
Case Study

- Comparison of IP addresses that communicate with expired domains

(PH) 0 20 40 60 80 100 120 140 160

Dec, 2015

Apr, 2016

(MY)

Dec, 2015

Apr, 2016

New IP (New Infected)
Conclusion and plan for future

The expectations were fulfilled
- Similar attack situation have been observed as mentioned in the report
- Obtained certain degree of expertise on the investigation

Taking over IP addresses
- Malware communicates not only with domains but also with IPs
- Seeking for assistance from Japanese partners

Working towards global information sharing
- Like SinkDB and join other information sharing community.

Thank you for listening!! ☺️