Practical Workflow for Automation and Orchestration of Addressing Cyber Threat: Case Study of Mirai Botnet in Malaysia

Megat Muazzam
Head of Malaysia CERT
CyberSecurity Malaysia
Agenda

• Introduction
• Issues Surrounding Protecting Malaysia Cyber Security
• Important of Threat Intelligent Sharing
• Traditional SOC “And” Threat Intelligent Information Sharing
• Case study Mirai
Cyber999™
Cyber Early Warning Services

- Incident Handling
- Cyber Early Warning
- Technical Coordination Centre
- Malware Research Center

Email us at: cyber999@cybersecurity.my

REFERENCE CENTRE FOR CYBER SECURITY ASSISTANCE

- for all internet users, including home users and organizations
What steps are taken by the Malaysian Government to keep cyber threats under control?

One of the most important step is creating:

- National Cyber Security Policy (NCSP)
- Establishing CyberSecurity Malaysia to implement NCSP
Issues Surrounding Cyber Security in Malaysia

- Vastly expanding attack surface area (Mobile, Cloud, Virtualization, IOT etc)
- Insufficient reliable data related to cyber threats
- No appropriate body or authority that provides reliable data
- Insufficient technical resources and expertise to expedite threat intelligence analysis and incident response.
CSIRT’s Role in Protecting Critical National Information Infrastructure

- Information sharing about latest threats and mitigation measures against the threats

- Early warning of latest outbreaks, provide Alert and Advisory on the latest outbreak which includes detection and mitigations

- Raise awareness about cybersecurity and critical infrastructure protection issues

- As a platform to promote mutual collaboration between all sectors in CNII, such as Government, Private, Financial sectors. A good example is a National-level Cyber Exercise.

- Engaging with various parties such as with Law Enforcement Agencies, ISPs, security experts on mitigations against cyber attacks against CNII.
Current Malaysia Practise for Mitigating Cyber Threats in Malaysia

- Coordinated Cyber Incident Escalation
- Annual Cyber Exercise “Code Name X-Maya”
- National Level Security Awareness
What is Threat Intel

“Threat Intelligence (TI) is evidence based knowledge, including context, mechanism, indicator, implications, and actionable advise about an existing or emerging menace or hazard to assets That can be used to inform decisions regarding the subject response to that menace or hazard”
- Gartner, 2013

• SANS Institute
- The set of data collected, assessed and applied regarding security threat, threat actors, exploits, malware, vulnerabilities and compromise indicators”
Importance of Threat Intelligence

To move threat intelligence sharing to the next level of efficiency and effectiveness, improvement is needed in three areas:

• We need to simplify event triage and provide a better environment for security practitioners to investigate high-priority threats.
• We need to do a better job establishing relationships between indicators of compromise so that we can understand their connections to attack campaigns.
• We need a better way to share threat intelligence among our stakeholders and relevant authorities.
Example of Threat Intelligence / Information Sharing Framework

Technological Platform / Framework
- MISP
- OpenIOC
- STIX / TAXII
- Collective Intelligence Framework (CIF)
- Avalanche/Soltra (FS-ISAC)

SIEM Communities
- Qradar Threat Exchange
- Splunk feeds

National CSIRTs/CERTs info sharing exchange
Traditional SOC Operation

Triage

Network Management Tools
Phone calls
Intrusion Detection Systems
SMSes
Faxes
Emails

Incident Report

• Information Requests
• Vulnerability Report

Analyze
Escalation
Technical Assistance

Resolution

Copyright © 2017 CyberSecurity Malaysia
Threat Intelligence Information Sharing Model

1. Threat Intel Sources
2. Honeynet
3. Feeds Provider
4. Foreign CERT

- Distribute Feeds & Raw Data
- Initial Analysis

Threat Intelligence Analysis Process

- Threat Intel Sources
- Honeynet
- Feeds Provider
- Foreign CERT

- Reporting System
- Advisory & Alerts
- Law Enforcement Agency (LEA): For crime related cases
- MyCERT: If require technical assistance, data preservation

Verified Data Escalation to related CNII Sectors

CNII Sectors may refer to CNII Portal advisories and alerts for proper handling of cases and for future reference

Blocking and Investigation process by related CNII Sectors

High Risk Information? Yes/No

CNII Sectors may refer to CNII Portal advisories and alerts for proper handling of cases and for future reference

Law Enforcement Agency (LEA): For crime related cases

MyCERT: If require technical assistance, data preservation
Tools Used for Information Sharing

- **MyLipas**
  - Semi-automated escalation tool
  - For mass IP notification

- **Honeynet**
  - Source of threat information

- **Automated Scripts**
  - Automating the analysis and processing of the threat information

- **Forensic tools**
  - Forensic analysis
Case Study - Mirai
Mirai Botnet Infection

https://intel.malwaretech.com/botnet/mirai/?t=24h&bid=all
20,585

### Top Countries

<table>
<thead>
<tr>
<th>Country</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malaysia</td>
<td>20,585</td>
</tr>
<tr>
<td>Kuala Lumpur</td>
<td>6,762</td>
</tr>
<tr>
<td>Petaling Jaya</td>
<td>2,020</td>
</tr>
<tr>
<td>Shah Alam</td>
<td>1,183</td>
</tr>
<tr>
<td>Klang</td>
<td>776</td>
</tr>
<tr>
<td>Kajang</td>
<td>362</td>
</tr>
</tbody>
</table>

### Top Cities

<table>
<thead>
<tr>
<th>City</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kuala Lumpur</td>
<td>6,762</td>
</tr>
<tr>
<td>Petaling Jaya</td>
<td>2,020</td>
</tr>
<tr>
<td>Shah Alam</td>
<td>1,183</td>
</tr>
<tr>
<td>Klang</td>
<td>776</td>
</tr>
<tr>
<td>Kajang</td>
<td>362</td>
</tr>
</tbody>
</table>

### Top Organizations

<table>
<thead>
<tr>
<th>Organization</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>TM Net</td>
<td>17,073</td>
</tr>
<tr>
<td>Maxis Broadband Sdn Bhd</td>
<td>1,447</td>
</tr>
<tr>
<td>Central</td>
<td>313</td>
</tr>
<tr>
<td>TM Business</td>
<td>208</td>
</tr>
<tr>
<td>Tt Dotcom Sdn Bhd</td>
<td>130</td>
</tr>
</tbody>
</table>

[https://www.shodan.io/](https://www.shodan.io/)
List of vectors found in source code.

<table>
<thead>
<tr>
<th>Attack</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UDP</td>
<td>UDP flood</td>
</tr>
<tr>
<td>VSE</td>
<td>Valve Source Engine query flood</td>
</tr>
<tr>
<td>DNS water</td>
<td>Recursive DNS query attack</td>
</tr>
<tr>
<td>torture</td>
<td></td>
</tr>
<tr>
<td>SYN</td>
<td>SYN packet flood</td>
</tr>
<tr>
<td>ACK</td>
<td>ACK packet flood</td>
</tr>
<tr>
<td>STOMP</td>
<td>ACK flood with STOMP</td>
</tr>
<tr>
<td>GRE IP</td>
<td>GRE flood</td>
</tr>
<tr>
<td>GRE Ethernet</td>
<td>Ethernet encapsulated inside GRE flood</td>
</tr>
<tr>
<td>Plain UDP</td>
<td>UDP flood optimized for speed</td>
</tr>
<tr>
<td>HTTP</td>
<td>HTTP layer 7 flood</td>
</tr>
</tbody>
</table>

The passwords come from the botnet's source code.
Security Feeds Information

Mirai infection CC-Port Scan Detected
Jan - April 2017

Infection Type by Variant

- Mirai: 228220, 69%
- Mirai-Botnet: 83781, 26%
- Mirai#14: 17452, 5%
- Mirai Wget Download: 408, 0%

Copyright © 2017 CyberSecurity Malaysia
Mirai detection using Honeypot

MTPot – open source honeypot developed by Cymmetria Research.

MTPot is written in Python

• the ip and port to which the honeypot shall bind
• a list of commands expected to be sent by the scanners and the responses that MTPot shall give
• the name of the attack (Mirai)
• a session timeout value
• some optional syslog settings to collect the fingerprinted IPs

- Escalation to ISP focus only for .my source of IP that have been infected.
Automated Escalation Process

Botnet Feeds

Centralized System

Cyber999

LebahNET Sensor
Automation of escalation
Mitigate the attacked

• Automated incident escalation to ISP
• Recommend ISPs identify compromised IoT devices by filtering traffic TCP23 / TCP 2323 / TCP 7547
  – ISP action: Isolate and notify legitimate owners of the problem and urge to take corrective action.
• Publish advisory to alert Malaysia Internet user
Recommendation to device owners

- Research the capabilities and security features of an IoT device before purchase
- Stop using default/generic passwords.
- Disable Telnet login and use SSH
- Disable or protect remote access to IoT devices when not needed
- Regularly check the manufacturer’s website for firmware updates
What is the challenges

Owner of Devices

– Not straightforward to patch/upgrade
– Not every user know how to resolve infected devices

IoT Manufacture

– Profit Vs Security
– Unnecessary services should be disabled by default
– Best practices: password

ISP

– Difficult to correlate information that have been share / escalate by CERT
– Need proper guidelines to informed affected customers.
Summary

- It worked for us in obtaining valid, reliable threat intelligent information from our trusted partners. This will eventually make identification and rectification work smoothly.

- It worked in identifying the threats, vulnerabilities to systems belonging to the CNII sector.

- It strengthens the working collaboration between CSIRTs and CNII sectors and position CSIRT as an entity that plays an important role in safeguarding the cyber space.

- CSIRTs partnership has become an integral part at international network to fight against cyber threats.

- To develop a baseline understanding of common threats and capabilities to enable coordinated actions among the CNII sectors in the event of large scale cyber attacks.
Questions?

- Find out more
  - [www.cybersecurity.my](http://www.cybersecurity.my)
  - [www.mycert.org.my](http://www.mycert.org.my)
  - [cyber999@cybersecurity.my](mailto:cyber999@cybersecurity.my)

- Personal
  - [megat@cybersecurity.my](mailto:megat@cybersecurity.my)
Thank you

Corporate Office
CyberSecurity Malaysia,
Level 5, Sapura@Mines
No. 7 Jalan Tasik
The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan, Malaysia.

T: +603 8992 6888
F: +603 8992 6841
H: +61 300 88 2999

www.cybersecurity.my
info@cybersecurity.my

Northern Regional Office
CyberSecurity Malaysia,
Level 19, Perak Techno-Trade Centre
Bandar Meru Raya, Off Jalan Jelapang
30020 Ipoh, Perak Darul Ridzuan, Malaysia

T: +605 528 2088
F: +605 528 1905

www.facebook.com/CyberSecurityMalaysia
twitter.com/cybersecuritymy
www.youtube.com/cybersecuritymy

Copyright © 2017 CyberSecurity Malaysia