GETTING TO THE SOUL OF INCIDENT RESPONSE
CSIRT MANAGEMENT WORKFLOW:
PRACTICAL GUIDE FOR CRITICAL INFRASTRUCTURE ORGANIZATIONS

PREPARED BY:
NURUL HUSNA MOHD NOR HAZALIN
ZAHRI YUNOS
ASWAMI FADILLAH ARIFFIN
MOHD AZLAN MOHD NOR
INTRODUCTION

Critical National Information Infrastructure (CNII) In Malaysia

VISION
‘Malaysia’s Critical National Information Infrastructure shall be secure, resilient and self-reliant. Infused with a culture of security, it will promote stability, social well being and wealth creation’

DEFENCE & SECURITY

TRANSPORTATION

BANKING & FINANCE

HEALTH SERVICES

EMERGENCY SERVICES

CRITICAL NATIONAL INFORMATION INFRASTRUCTURE
Assets (real & virtual), systems and functions that are vital to the nation that their incapacity or destruction would have a devastating impact on
- National defense & security
- National economic strength
- National image
- Government capability to function
- Public health & safety

ENERGY

INFORMATION & COMMUNICATIONS

GOVERNMENT

FOOD & AGRICULTURE

WATER
TYPE OF CYBER THREATS

**Social and phishing**
- **Target:** Individual users
- **Purpose:**
  - Pre-attack Intelligence recon
  - Build trust using fake social profiles
  - Initial infection

**Malware, zero-day and botnets**
- **Target:** Endpoint systems and servers
- **Purpose:**
  - Obtain access to systems
  - Create backdoors
  - Establish command-and-control over large network of devices

**Passwords and configs**
- **Target:** Endpoint systems and servers
- **Purpose:**
  - Initial penetration
  - Expansion of reach
  - Escalation of privileges

**Distributed denial-of-service**
- **Target:** Network and application infrastructure
- **Purpose:**
  - Cause operational disruption
  - Create diversion for other attacks

**Smart and mobile hacking**
- **Target:** Mobile and embedded services
- **Purpose:**
  - New attack surface and entry point to enterprise network
  - Gain access to user data through vulnerable mobile OS and apps

**SQL injection**
- **Target:** Database servers
- **Purpose:**
  - Obtain account and user credentials
  - Steal sensitive data
## CYBER INCIDENTS BY SECTORS

<table>
<thead>
<tr>
<th>Rank</th>
<th>Sector</th>
<th>Number of Incidents</th>
<th>Percentage of Incidents</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Healthcare</td>
<td>116</td>
<td>37%</td>
</tr>
<tr>
<td>2</td>
<td>Retail</td>
<td>34</td>
<td>11%</td>
</tr>
<tr>
<td>3</td>
<td>Education</td>
<td>31</td>
<td>10%</td>
</tr>
<tr>
<td>4</td>
<td>Gov. &amp; Public Sector</td>
<td>26</td>
<td>8%</td>
</tr>
<tr>
<td>5</td>
<td>Financial</td>
<td>19</td>
<td>6%</td>
</tr>
<tr>
<td>6</td>
<td>Computer Software</td>
<td>13</td>
<td>4%</td>
</tr>
<tr>
<td>7</td>
<td>Hospitality</td>
<td>12</td>
<td>4%</td>
</tr>
<tr>
<td>8</td>
<td>Insurance</td>
<td>11</td>
<td>4%</td>
</tr>
<tr>
<td>9</td>
<td>Transportation</td>
<td>9</td>
<td>3%</td>
</tr>
<tr>
<td>10</td>
<td>Arts and Media</td>
<td>6</td>
<td>2%</td>
</tr>
</tbody>
</table>

**Top 10 Sectors Breached by Number of Incidents**

*Source: Symantec*
Unauthorized modification were made to the .MY (domain registry DNS (domain name server)) to redirect traffic to a rogue site when users visited websites such as Google Malaysia & Yahoo Malaysia.

Some internet users see the affected page for 24 hours due to DNS hijacking.

The home page of Malaysia Airlines website was replaced by a photo of a MAS Airbus A380, with the word “404-Plane not found”.

A group calling itself “Cyber Caliphate” has claimed responsible for the incident.
REPORTED CYBERSECURITY INCIDENTS - MALAYSIA

Reported incidents based on general incident classification statistics 2015
This directive specifies the requirement for all government agencies to establish their own CSIRT as one of the initiatives to manage cyber incidents.

In 2013, the latest version of the ISMS standard (27001:2013(E)) contains three additional sub clauses under paragraph A16.1, which emphasize on response and assessment of information security incidents:

1. A 16.1.5 Response to information security incidents
2. A 16.1.6 Learning from information security incidents
3. A 16.1.7 Collection of evidence

In 2013, the National Security Council of Malaysia (NSC) released the guideline “NSC Directive 24: National Cyber Crisis Management Mechanism.”
## SERVICES OFFERED BY CSIRT (Example)

<table>
<thead>
<tr>
<th>Proactive Services</th>
<th>Reactive Services</th>
<th>Post-Incident Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Cyber security alerts, warnings and announcements</td>
<td>1. Triage function</td>
<td>1. Risk analysis</td>
</tr>
<tr>
<td>2. Technology watch</td>
<td>• Incident handling - incident analysis, response on site,</td>
<td>2. Business Continuity and Disaster Recovery Planning</td>
</tr>
<tr>
<td>3. Security audit or assessment</td>
<td>• response support, response coordination</td>
<td>3. Awareness building</td>
</tr>
<tr>
<td>4. Cyber security information dissemination</td>
<td>• Handling vulnerabilities - vulnerability analysis,</td>
<td>4. Education/training</td>
</tr>
<tr>
<td>5. Cyber security monitoring (e.g. intrusion detection, network monitoring)</td>
<td>• response, response coordination</td>
<td>5. Information sharing with other teams in the organization</td>
</tr>
<tr>
<td>6. Configuration and maintenance of security tools, applications and infrastructure</td>
<td>• Artefact handling - artefact analysis, response, response coordination</td>
<td></td>
</tr>
<tr>
<td>7. Awareness and training programs related to handling cyber security incidents</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Prepare for any possible imminent problems**

**Respond to problems & incident handling**

**Quality management service**
CyberDEF

"detection of cyber treat"

"eradication of cyber treat"

"forensic analysis of cyber treat"

This stage is iterative, return to “D” or “E” to improve the technique further.
CyberDEF (cont…)

Typical CSIRT

Detection Eradication

CyberDEF

Detection Eradication + FORENSIC
CyberDEF (cont...)

**Detection**
- Identify any loopholes, vulnerabilities and existing threats
  1. Sensors
  2. Sandbox
  3. Analytics
  4. Visualization

**Eradication**
- Close loopholes, patch vulnerabilities and neutralize existing threats
  - Perform cyber threats exercise or drill to test the feasibility and resiliency of the new defense / prevention system

**Forensics**
- 1. E-Discovery
- 2. Root cause analysis
- 3. Investigation
- 4. Forensics readiness
- 5. Forensic compliance
CyberDEF (cont…)

Why CyberDEF is unique?

3 Technical Departments

- Consists of 3 technical departments:
  1. Secure Technology Services department (STS)
  2. Digital Forensic department (DF)
  3. Malaysia Computer Emergency Response Team (MyCERT)

Centralized Governance

- Effective centralized governance because all of the 3 involved departments report directly to Vice President of Cyber Security Responsive Services.

Forensic Element

- Forensic element incorporated in the services offered
# CSIRT MANAGEMENT WORKFLOW

<table>
<thead>
<tr>
<th>Process</th>
<th>MyCERT</th>
<th>STS</th>
<th>DF</th>
<th>C-Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detection</td>
<td>Constant monitoring</td>
<td>Constant monitoring</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Detect threats</td>
<td>Detect threats</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Register case in OTRS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Verification</td>
<td>Analyze threats</td>
<td>Identify device</td>
<td>Conduct debrief to team members</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Containment</td>
<td>Inform HoD of suspected device’s owner</td>
<td>Verify threat with actual device</td>
<td>Preserve memory dump</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Collect device</td>
<td></td>
</tr>
<tr>
<td>Preservation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Analysis</td>
<td>Security analysis</td>
<td>Evidence analysis</td>
<td>Produce root cause analysis report</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Produce security analysis report</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Eradication</td>
<td>Eradicate the threats based on recommendations</td>
<td>Recover device</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Return device</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reporting</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Response times:**
- Detection: 0.5 hour
- Verification: 3 hour
- Containment: 1 hour
- Preservation: 16 hours
- Analysis: 5 days
- Eradication: 1 hour
- Reporting: 1 hour

---

**Response time examples:**
- Detection: 0.5 hour
- Verification: 3 hour
- Containment: 1 hour
- Preservation: 16 hours
- Analysis: 5 days
- Eradication: 1 hour
- Reporting: 1 hour
CASE STUDY: DETECTION

Appliance detected the victim is accessing malicious website which is “sl-reverse.com” and download malicious executable files.

Alert 126915
Victim downloads malicious executable file which is "wzUninstall.exe":

```
malware-detected:
  malware (name:Malware.Binary.exe):
    type: exe
    parent: 126911
    downloaded-at: 2016-02-23T07:36:45Z
    md5sum: dfd78e15d615109463c36322919e235e0
    original: wzUninstall.exe
    executed-at: 2016-02-23T07:43:08Z
    application: Windows Explorer
```

Alert 126912
Victim downloads malicious executable file which is "Migration.exe" from “xa.xingcloud.com”:

```
malware-detected:
  malware (name:Malware.Binary.exe):
    type: exe
    parent: 126911
    downloaded-at: 2016-02-23T07:36:44Z
    md5sum: a57dce958b56e55a92ec45299246022
    original: Migration.exe
    executed-at: 2016-02-23T07:38:58Z
    application: Windows Explorer
```

IP Location: United States Dallas David Zhou
ASN: AS36351 SOFTLAYER - SoftLayer Technologies Inc. (registered Dec 12, 2005)
Resolve Host: b.ab.c1.ad.ip4.static.sl-reverse.com
Whois Server: whois.arin.net
IP Address: 173.193.171.11
**CASE STUDY: DETECTION (Cont...)**

**Affected device identified**

<table>
<thead>
<tr>
<th>IP Address</th>
<th>XXX.XXX.XXX</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
<td>00:00:00:00</td>
</tr>
<tr>
<td>NetBIOS Name</td>
<td>Server1</td>
</tr>
<tr>
<td>Staff Name</td>
<td>IT Support</td>
</tr>
<tr>
<td>Location</td>
<td>Finance</td>
</tr>
<tr>
<td>Department</td>
<td>Finance</td>
</tr>
</tbody>
</table>

**Incident Level:** 6 incidents occurred

<table>
<thead>
<tr>
<th>Alert Type</th>
<th>Incident Level</th>
<th>Alert ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Infection</td>
<td>Minor / Major / Critical</td>
<td>7545</td>
</tr>
<tr>
<td>Malware Object</td>
<td>Minor / Major / Critical</td>
<td>126911/126912/126913/126915/126916</td>
</tr>
</tbody>
</table>
CASE STUDY: ERADICATION

- STS has blocked the source MAC address to corporate network.
- STS has identified the victim PC.
- STS has collected the victim for imaging process in DF.
- STS has escalated the incident finding to MRC.

Eradicate the malware
CASE STUDY: FORENSICS

Analysis

Extract metadata & registry info from malicious file and analyze it using available tools

Findings

Found 1 (one) attempt of file named as Migration.exe to connect to http://xa.xingcloud.com as shown in the screenshot below:
CASE STUDY: FORENSICS (Cont…)

Findings

Found 6 (six) browser activities (URLs accessed) of a file named as wzUpg.exe in the exhibit as shown in the screenshot below:

Screenshot 2: wzUpg.exe access to several URLs

Found that an application named as WZUPG.exe had ran for 2 (two) times as the details in the screenshot below:

(Please refer Appendix C for the screenshots below)

<table>
<thead>
<tr>
<th>Details</th>
<th>Hex</th>
<th>Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Name</td>
<td>WZUPG.EXE</td>
<td></td>
</tr>
<tr>
<td>Application Run Count</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Last Run Date/Time</td>
<td>02/24/2016 04:28:59 AM</td>
<td></td>
</tr>
<tr>
<td>2nd Last Run Date/Time</td>
<td>02/24/2016 03:58:59 AM</td>
<td></td>
</tr>
<tr>
<td>3rd Last Run Date/Time</td>
<td>(not found)</td>
<td></td>
</tr>
<tr>
<td>4th Last Run Date/Time</td>
<td>(not found)</td>
<td></td>
</tr>
<tr>
<td>5th Last Run Date/Time</td>
<td>(not found)</td>
<td></td>
</tr>
</tbody>
</table>

Screenshot 3: wzUpg.exe application run count
CONCLUSION

• CSIRT Workflow Management should include elements of Detection, Eradication & Forensic

• It work for us!
  • effective CSIRT implementation
  • effective governance for managing incidents

• Communication, collaboration and information sharing are critical in CSIRT management
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