EDINBURGH
JUNE 16-21
2019

Cyber Threats Incident Response Model for CNII Organizations

Dr. Aswami Ariffin

Megat Mutalib

Dr. Zahri Yunos

CyberSecurity MALAYSIA

Presentation Outline

1. Our Service: CyberDEF (Cyber Defence)
2. Our R&D Product: CMERP (Coordinated Malware Eradication & Remediation Project)

CyberI3

CMERP
Detection | Eradication | Remediation

Cyber999

CyberCSI
THE MALAYSIAN CHAPTER OF DIGITAL FORENSIC

R&D Papers

iOS anti-forensics: How can we securely conceal, delete and insert data?
C D'Orazio, A Ariffin, R Choo
47th Annual Hawaii International Conference on System Sciences (HICSS 2014)

iOS Forensics: How can we recover deleted image files with timestamp in a forensically sound manner?
A Ariffin, C D'Orazio, KKR Choo, J Slay
The 8th ARES Conference (ARES 2013), University of Regensburg, Germany.

Digital Camcorder Forensics
A Ariffin, KKR Choo, J Slay

Data Recovery From Proprietary-Formatted CCTV Hard Disks
A Ariffin, J Slay, KKR Choo
Advances in Digital Forensics IX

Forensic readiness: A case study on digital CCTV systems antiforensics
A Ariffin, KKR Choo, Z Yunos
Contemporary Digital Forensic Investigations of Cloud and Mobile …

Digital Forensics Institute in Malaysia: The way forward
A Ariffin, J Slay, H Jazri
Digital Evidence and Electronic Signature Law Review 9

Digital Forensics in Malaysia
A Ariffin, II Ishak
Digital Evidence & Elec. Signature L. Rev. 5, 161

Cyber threat intelligence: Issue and challenges
MS Abu, SR Selamat, A Ariffin, R Yusof
Indonesian Journal of Electrical Engineering and Computer Science 10 (1 …

Understanding Cyber Terrorism from Motivational Perspectives: A Qualitative Data Analysis
Z Yunos, A Ariffin
http://www.waset.org/downloads/16/papers/17za110003.pdf

The Rise of Ransomware
WZA Zakaria, MF Abdollah, O Mohd, AFM Ariffin
Proceedings of the 2017 International Conference on Software and e-Business …

CSIRT Management Workflow: Practical Guide for Critical Infrastructure Organizations
N Mohd, Z Yunos, A Ariffin, A Nor, CS Malaysia
Proceedings of the 10th European Conference on Information Systems …

Malware Forensic Analytics Framework Using Big Data Platform
S Chuprat, A Ariffin, S Sahibuddin, MN Mahrin, FM Senan, NA Ahmad, ...
Proceedings of the Future Technologies Conference, 261-274

1. Our Service: CyberDEF

D *"detection of cyber threat"*

E *"eradication of cyber threat"*

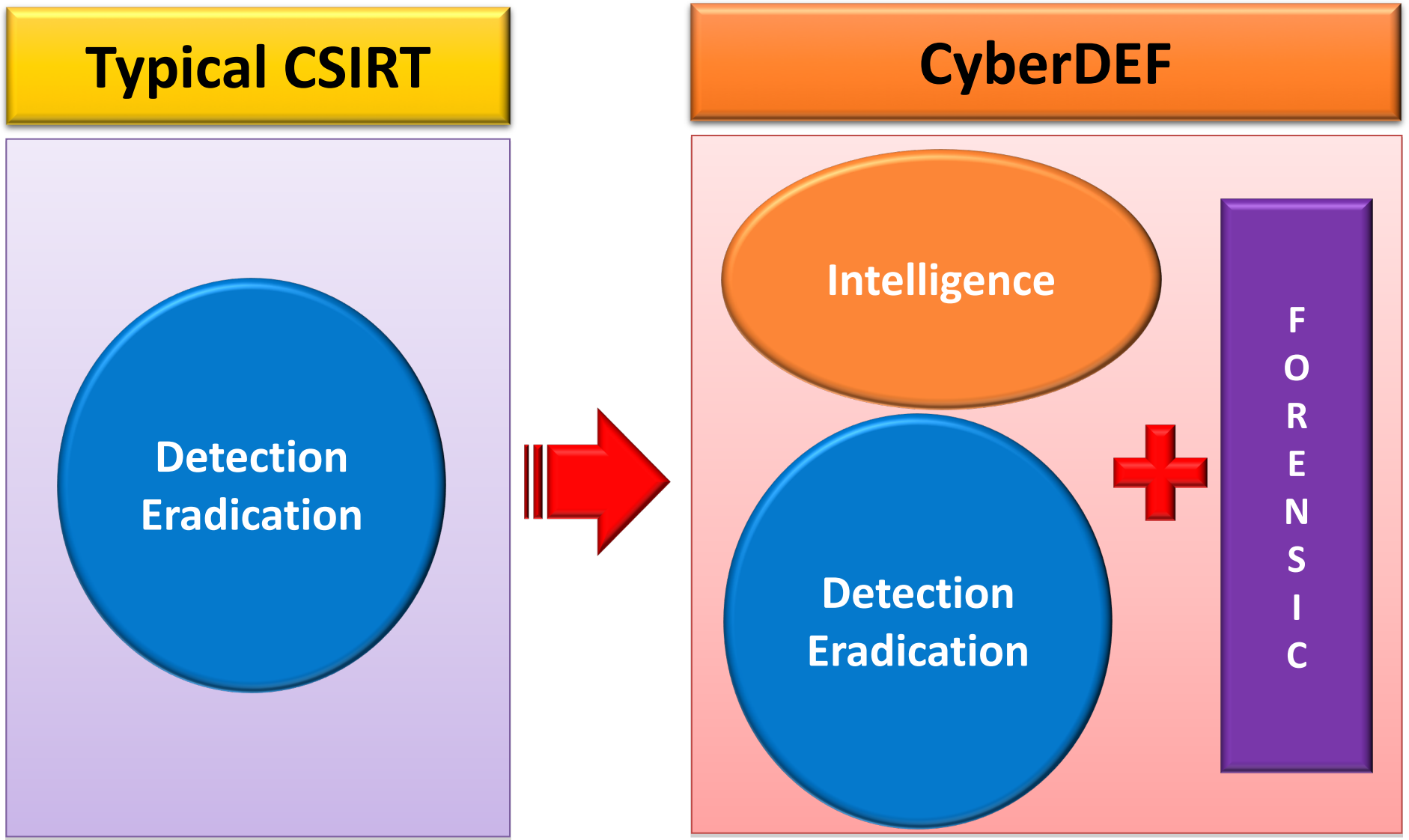
F *"forensic analysis of cyber threat"*

This stage is iterative, return to "D" or "E" to improve the technique further

CyberDEF

#cyberdefencemalaysia

CyberDEF (cont…)



CyberDEF (cont…)

Detection

Identify any loopholes, vulnerabilities and existing threats

1. Sensors
2. Sandbox
3. Analytics
4. Visualization
5. Situational Awareness

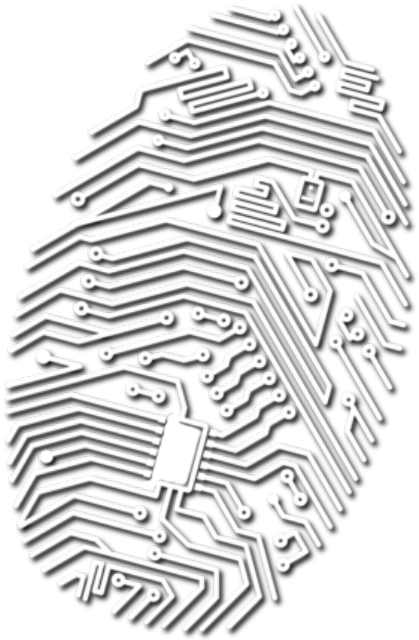
Eradication

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. Malaysia Computer Emergency Response Team (MyCERT)
3. Digital Forensic Department (DF)

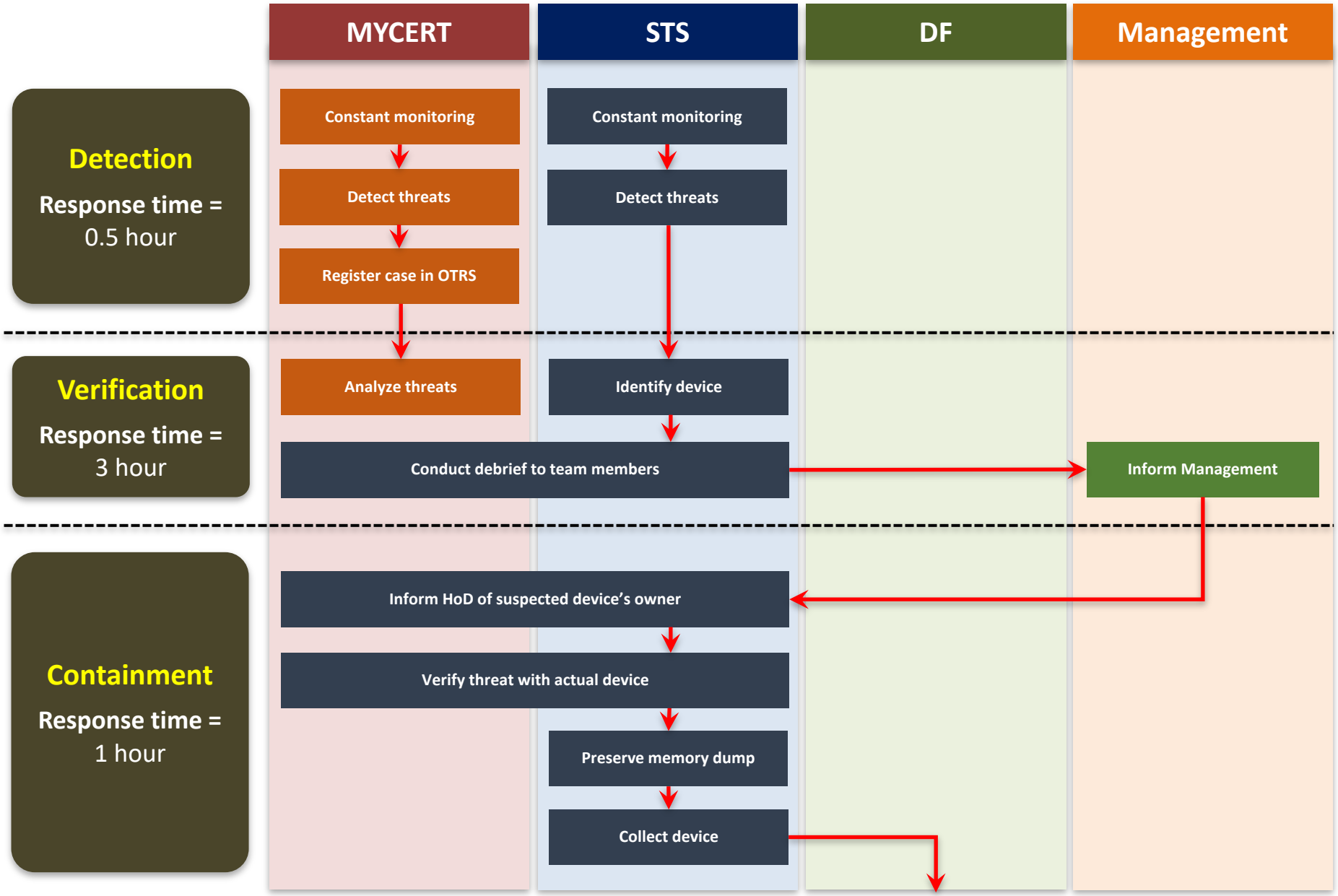
Centralized Governance

Effective **centralized governance** because all of the 3 departments are under the Cyber Security Responsive Services Division

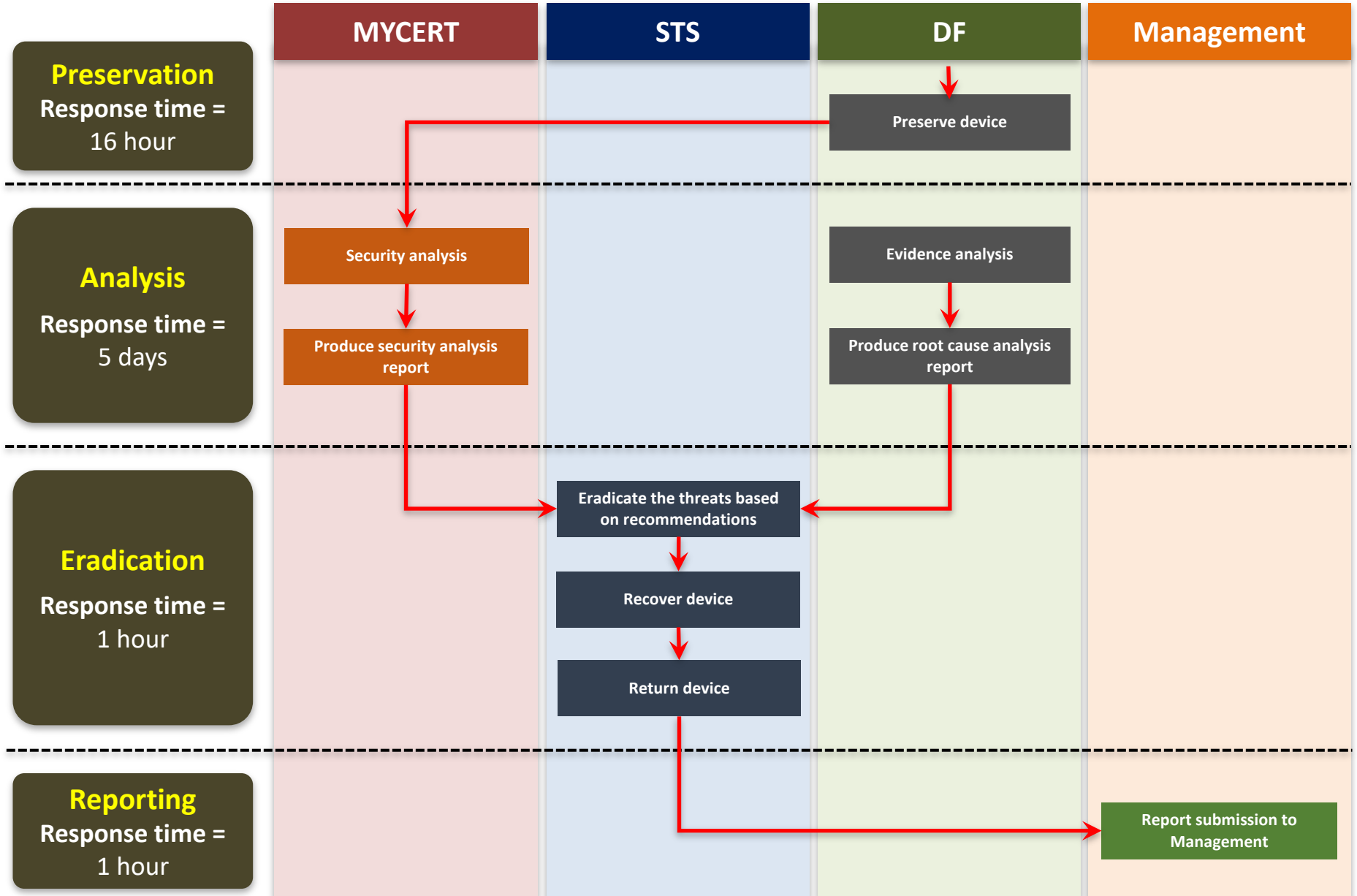
Forensic Element

Forensic element **incorporated** in the services offered and intelligence

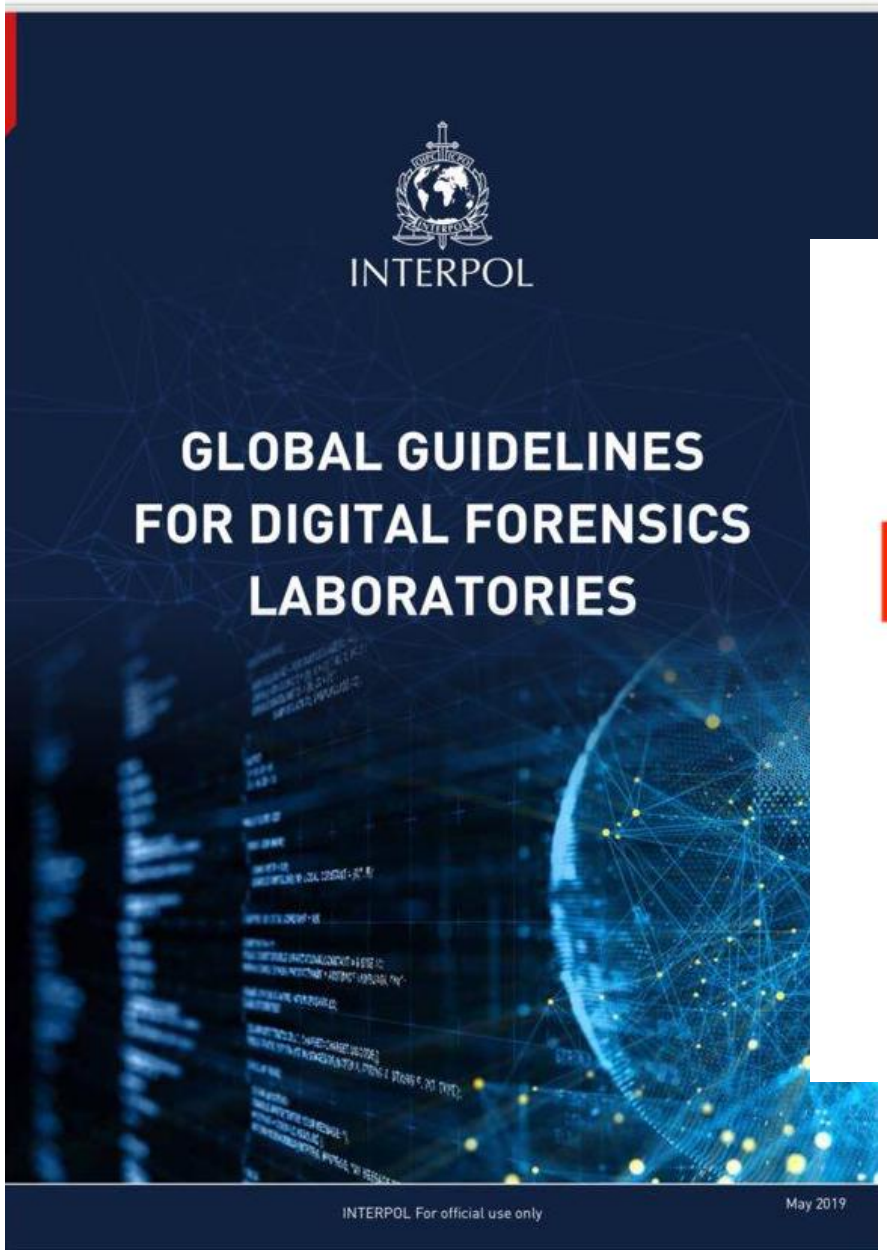
CyberDEF Management Workflow



CyberDEF Management Workflow



CyberDEF Management Workflow



ACKNOWLEDGMENT

Many parties have been involved in constructing the INTERPOL Guidelines for Digital Forensics.

First and foremost, INTERPOL would like to thank the Council of Europe for sharing the 'Basic Guide for the Management and Procedures of a Digital Forensics Laboratory' document. The Council of Europe's guide provided a strong foundation and has been used as a model for developing this document.

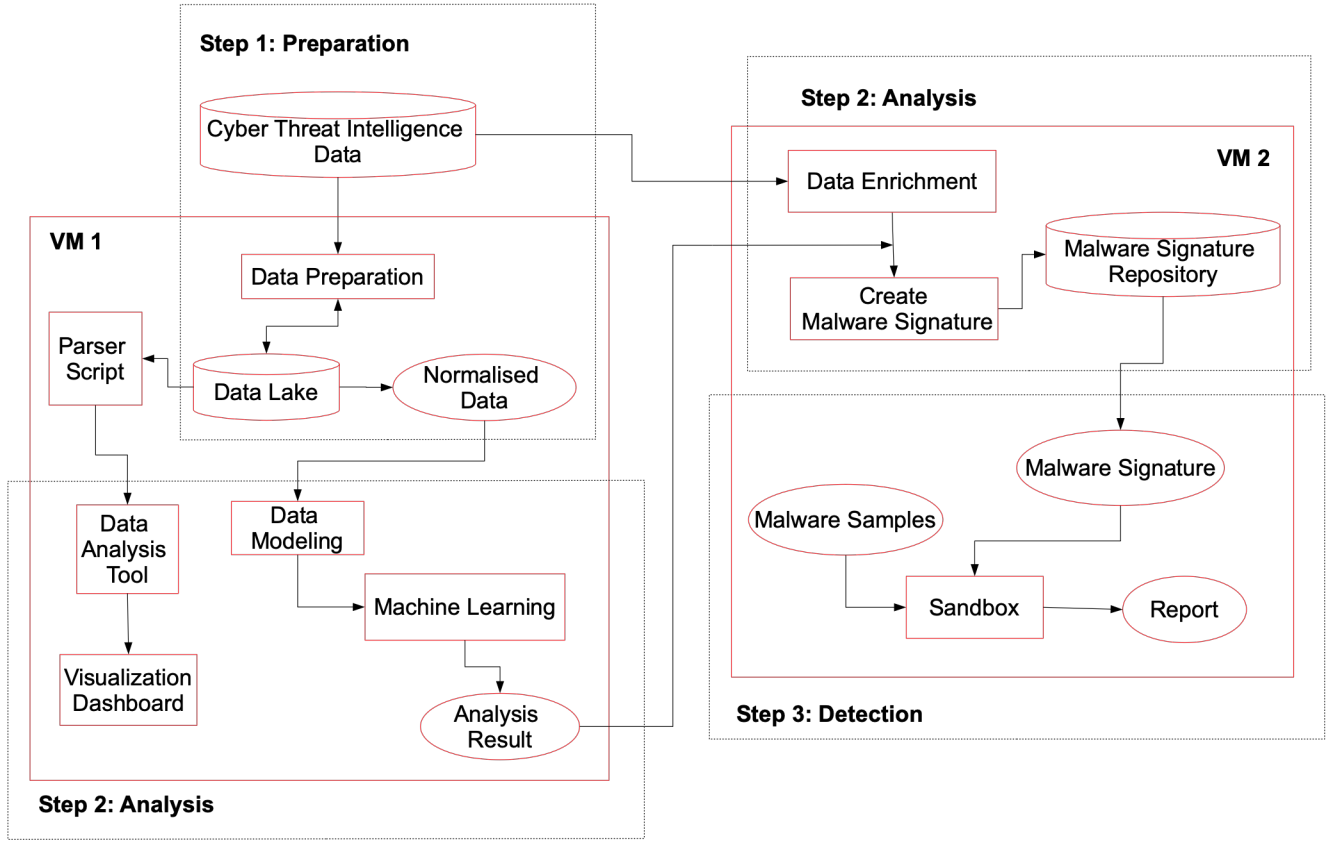
In addition, INTERPOL would like to express sincere gratitude to CyberSecurity Malaysia as the partner in making these guidelines a reality. CyberSecurity Malaysia's expertise and experience in an accredited digital forensics laboratory has been invaluable in completing this document.

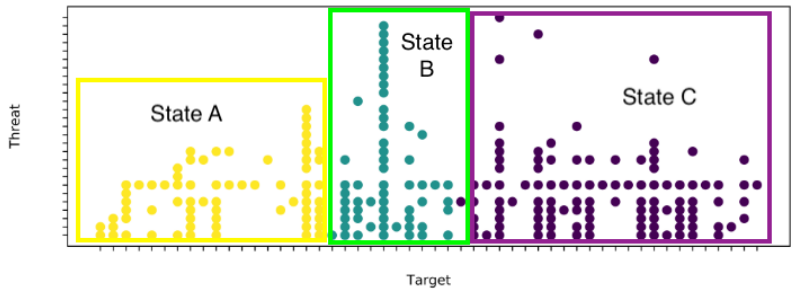
Finally we want to thank our colleagues from

- BAHRAIN: Cybercrime Department, Digital Forensics Unit;
- GERMANY: OE 12 – IT Forensik, Federal Criminal Police (BKA)
- KUWAIT: Digital Forensic Department/General Department of Criminal Evidence of Kuwait,
- SINGAPORE: Technology Crime Forensics Branch. Criminal Investigation Department. Singapore Police Force (SPF)
- SPAIN: Computer Forensic Section, General Commissary of Scientific Police (CGPC) of Spanish National Police (CNP);
- THE UNITED STATES OF AMERICA: Department of Homeland Security, Homeland Security Investigations;

whose valuable input has helped to improve the quality of this document and make it a common effort to serve as a global reference for Law Enforcement Agencies worldwide.

CyberDEF Detection Framework and System





Case Study: Detection

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

IP Location	United States Dallas David Zhou
ASN	AS36351 SOFTLAYER - SoftLayer Technologies Inc. (registered Dec 12, 2005)
Resolve Host	b.ab.c1ad.ip4.static.sl-reverse.com
Whois Server	whois.arin.net
IP Address	173.193.171.11

Alert 126915

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

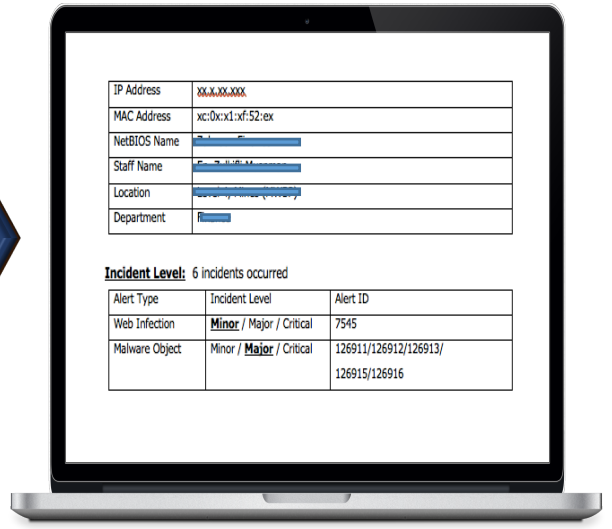
```
malware-detected:
    malware (name:Malware.Binary.exe):
      type: exe
      parent: 126911
      downloaded-at: 2016-02-23T07:36:45Z
      md5sum: dfd78e15d615109463c6322019e235e0
      original: wzUninstall.exe
      executed-at: 2016-02-23T07:43:08Z
      application: Windows Explorer
```

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: a67dce958b56e55aa92ec45299246022
      original: Migration.exe
      executed-at: 2016-02-23T07:38:58Z
      application: Windows Explorer
  cnc-services:
    cnc-service:
      protocol: tcp
      port: 80
      address: xa.xingcloud.com
```

Affected device identified



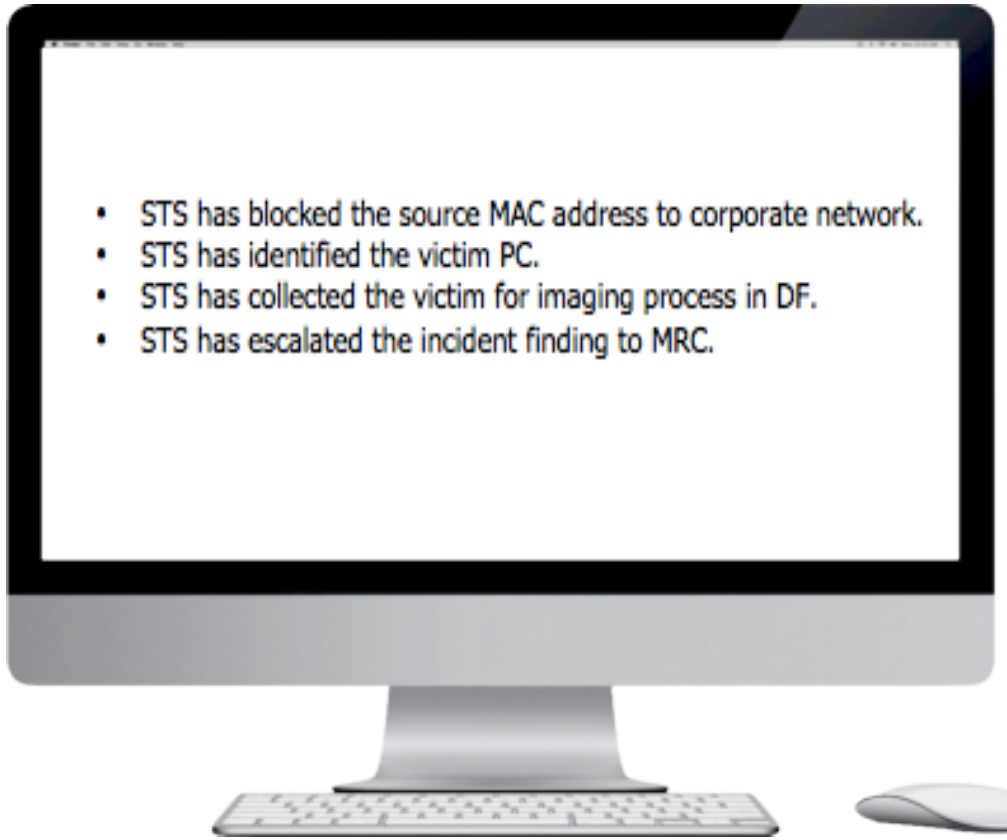
IP Address	xx.x.xx.xxx
MAC Address	xc:0x:x1:xf:52:ex
NetBIOS Name	
Staff Name	
Location	
Department	

Incident Level: 6 incidents occurred

Alert Type	Incident Level	Alert ID
Web Infection	**Minor** / Major / Critical	7545
Malware Object	Minor / **Major** / Critical	126911/126912/126913/ 126915/126916

Case Study: Eradication

Eradicate the malware



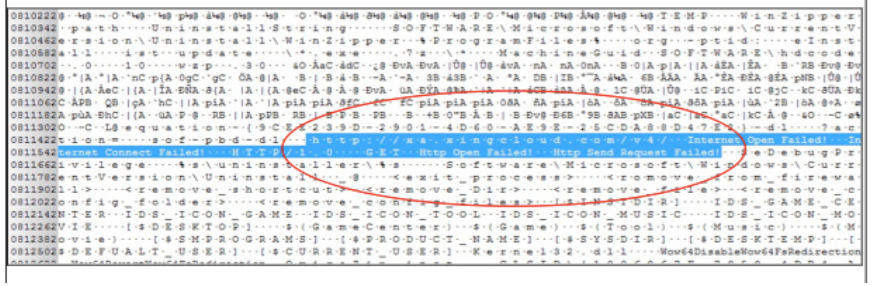
Case Study: Forensics Analysis

Extract metadata & registry info from malicious file and conduct forensics analysis

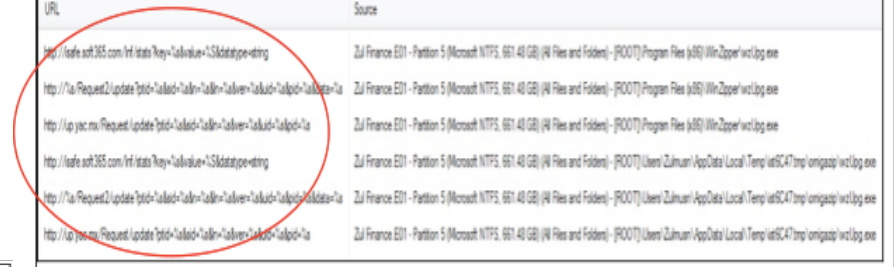
No	Exhibit	Methods
1.	INCIDENT_20160224(1)NB01_HD01	1. Connect exhibit to workstation. 2. Make forensic image of the exhibit using EnCase v6.18. 3. Calculate hash of the image file. *MD5*=**3fdf2da8aa5968bbef41de3921059e10** 4. Recover deleted data. 5. Run keywords related to the malicious software. 6. Bookmark and analyze files from exhibit. 7. Analyze registry data using IEF v6.6.3.0744 8. Bookmark and extract relevant information

Findings

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



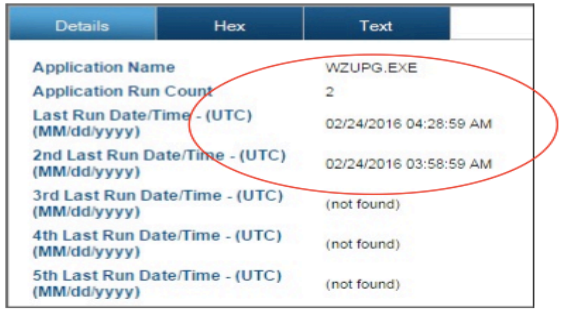
Found 6 **(six) browser activities** (URLs accessed) of a file named as **wzUpg.exe** in the exhibit as shown in the screenshot below:



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)



Screenshot 3: wzUpg.exe application run count

2. Our R&D Product: CMERP
Coordinated Malware Eradication & Remediation Project

CMERP
Detection | Eradication | Remediation

OBJECTIVE

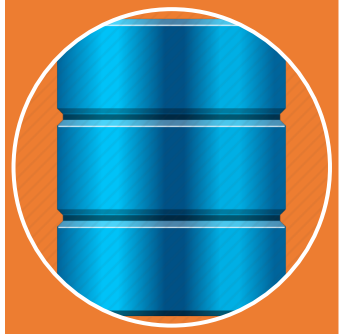
To **reduce** the number of **Malware infection** in Malaysia

DELIVERABLES

- **A framework and platform for effective malware detection and eradication**
- **A comprehensive system to mitigate malware infection**
- **Technical expertise in the areas of malware analysis, threat intelligence, and security data analytics**
- Malware threat landscape report and dashboard

CMERP
Detection | Eradication | Remediation

FRAMEWORK



Collection

- Detection
- Normalization
- Enrichment
- Correlation

Analysis

- Static
- Dynamic
- C2 Identification

Sinkhole

- Domain Sinkhole
- IP Sinkhole
- Infected host identification

Wall Garden

- Containment
- Malware Removal / Eradication

Report

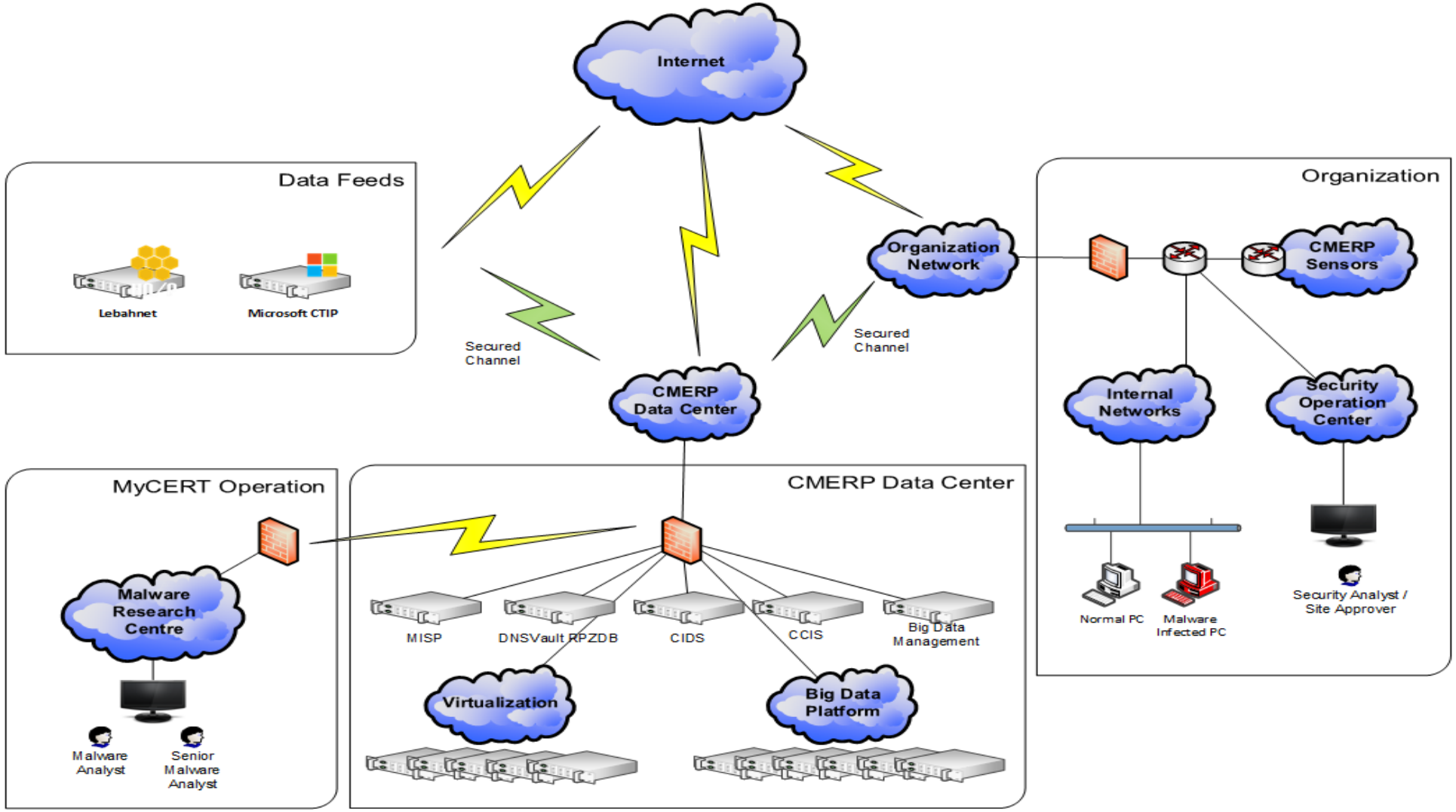
- Statistic
- Comparison
- Trend

CMERP Main Components

1. CMERP Intelligent Detection System (CIDS)	2. CMERP Coordinated Intelligence System (CCIS)	3. CMERP Sinkhole (CSH)	4. CMERP Walled Garden (CWG)	5. CMERP Removal Tool (CRT)
To **detect the activity of known & unknown (signatureless) malware** inside a network after a breach has occurred.	Big data platform that **coordinate malware detection, knowledge base and analysis in order to contain and mitigate malware infection** through CSH and CWG.	To **prevent and redirect** malicious network traffic inside the network infrastructure from communicating with Command & Control (C2) or Drop Site server. Through redirection, the system collects all infected host information.	To **quarantine infected PC** from accessing the network / Internet based on intelligence information from CCIS. Through quarantine process, the infected PC will be redirected to a captive portal with malware infection information and Malware Removal Tool.	Intelligent malware removal tool with based on Indicator of Compromised (IoC) as input. Purpose for **rapid malware removal tool** preparation.

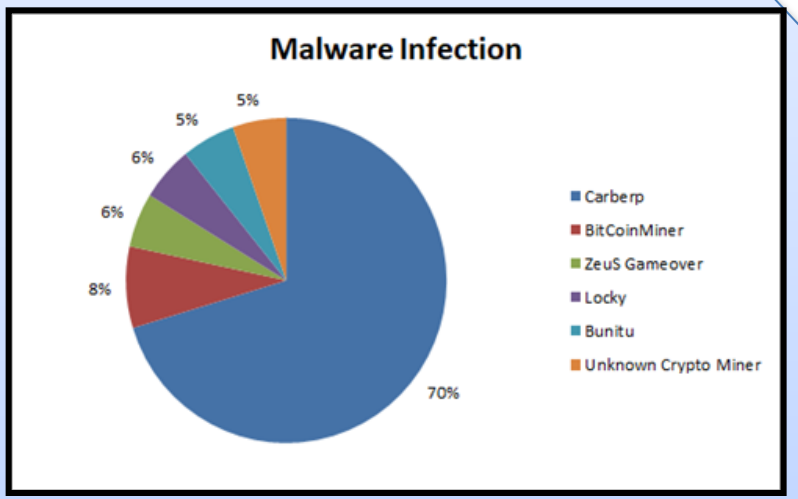
CMERP Ecosystem

CMERP Network Infrastructure



Pilot Implementation

Location : University Campus
Campaign Started : April 2018
Campaign Ended : May 2018
Malware Name : Carberp
Malware Severity : High

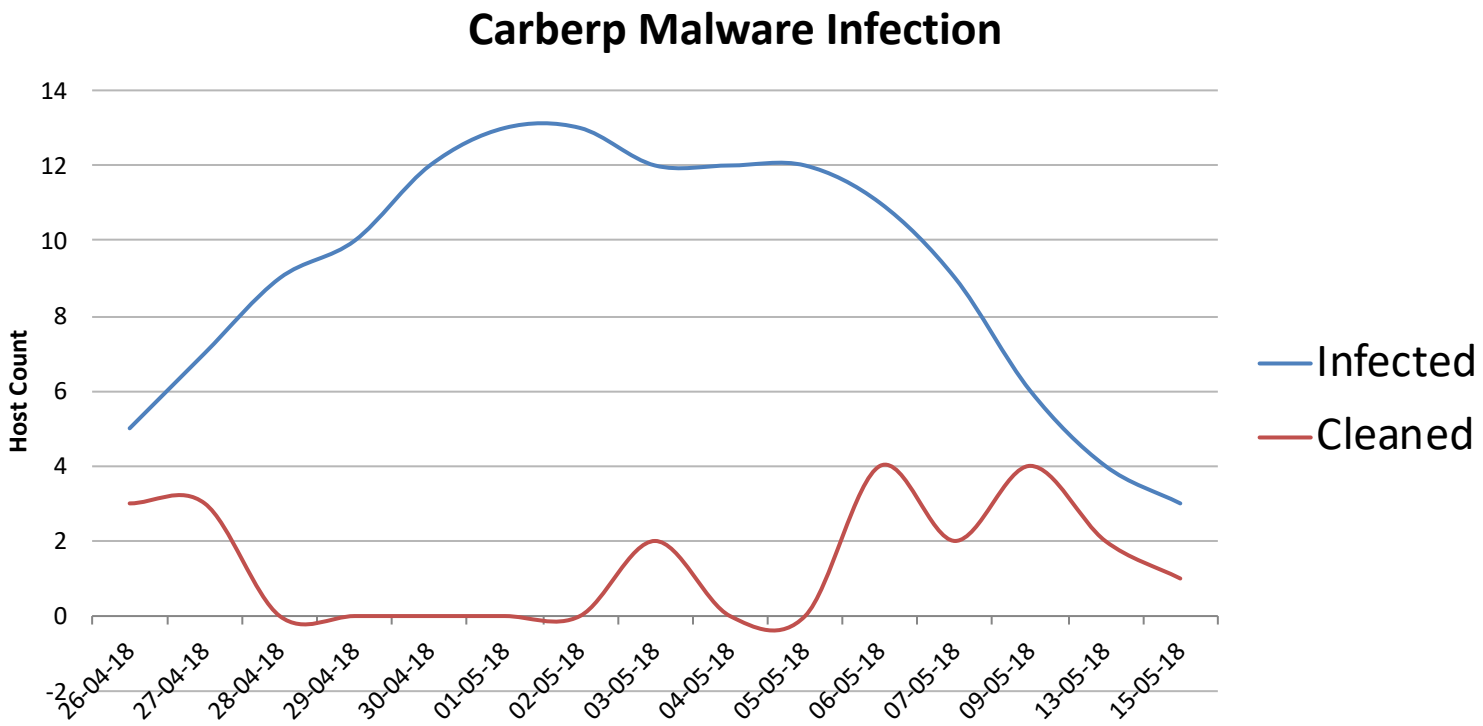


Malware Description:

This family of Trojans can **steal online banking credentials** as well as usernames and passwords from applications. The malware also has the capability to **download other malware** and **steal sensitive information** by taking screenshots or recording keyboard strokes.

Carberp Reference: https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Win32/Carberp

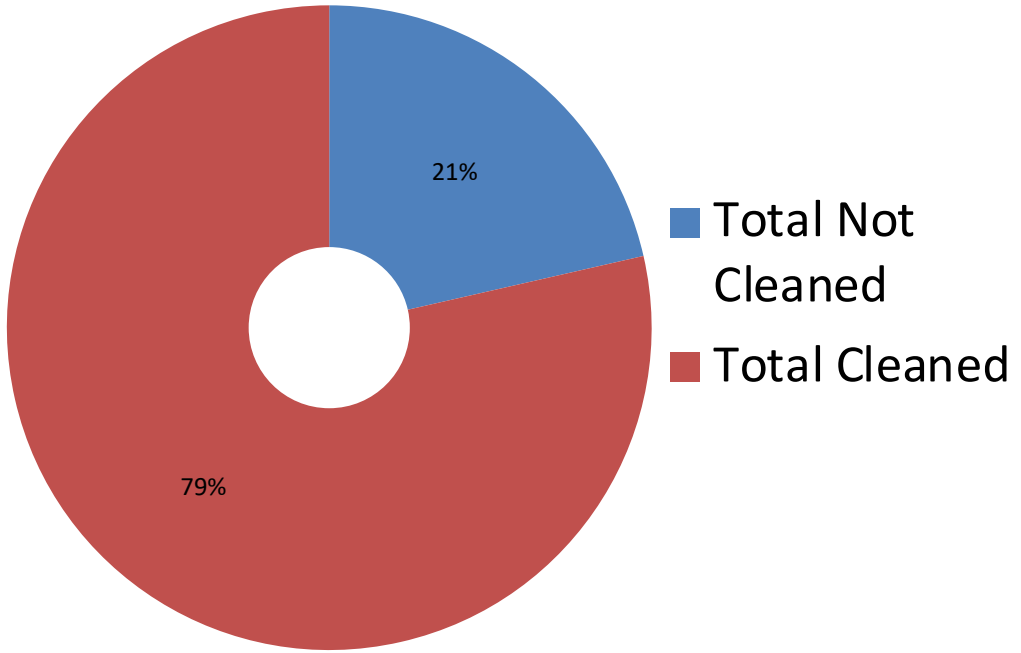
Pilot Outcome



Campaign Management

- Identified IOC information through malware analysis
- Redirected all C2 communications through Sinkhole process
- Infected hosts were quarantine during the Walled Garden process

Pilot Outcome



Analysis of Result:

- Some of Carberp malware variants are not only targeting for Microsoft Windows (PC) but for Android (Mobile Phone); which is outside the scope of this pilot project
- Lack of users awareness on the campaign, thus unable to clean the Carberp malware

Project Outcome

Strengthen the CNII sectors against cyber threats through CMERP implementation	**Comprehensive system** with threat intelligence capability	**Address sophisticated malware** including APT & unknown malware
Prevent data breach through Sinkhole	**Contain malware infection through Walled Garden** (notify & quarantine)	Using **100% local expertise** in collaboration with IHLs in developing CMERP system

FUTURE WORKS

CMERP Intelligence Detection System :
- Improve Sandbox detection.
- To support Sandbox Evasion malware.
- Agentless Sandbox – VM Introspection.
- High bandwidth support (> 40Gbps).
- Android & Mac Sandbox support.

CMERP Walled Garden :
- More product support other than Cisco.
- 802.1x implementation for organization level.

CMERP Sinkhole :
- More product support other than Cisco.
- OS fingerprinting.
- High performance sinkhole.
- Ability to sinkhole bad traffic only.

CMERP Coordinated Intelligence System :
- Machine Learning / Artificial Intelligence.
- More event types supported such as Netflow, Firewall, Honeypot, etc.

Overall :
- Endpoint Detection & Response.
- Improve System performance and stability

Conclusion

1. Our strategy to cope with emerging new threats is by adopting a holistic approach – people, process and technology

2. We need to be prepared all the times by enhancing:
   a. Information sharing amongst relevant stakeholders
   b. Cyber incidents response and coordination
   c. Collaborative & innovative research
   d. Capacity building and education
   e. Acculturation and outreach program