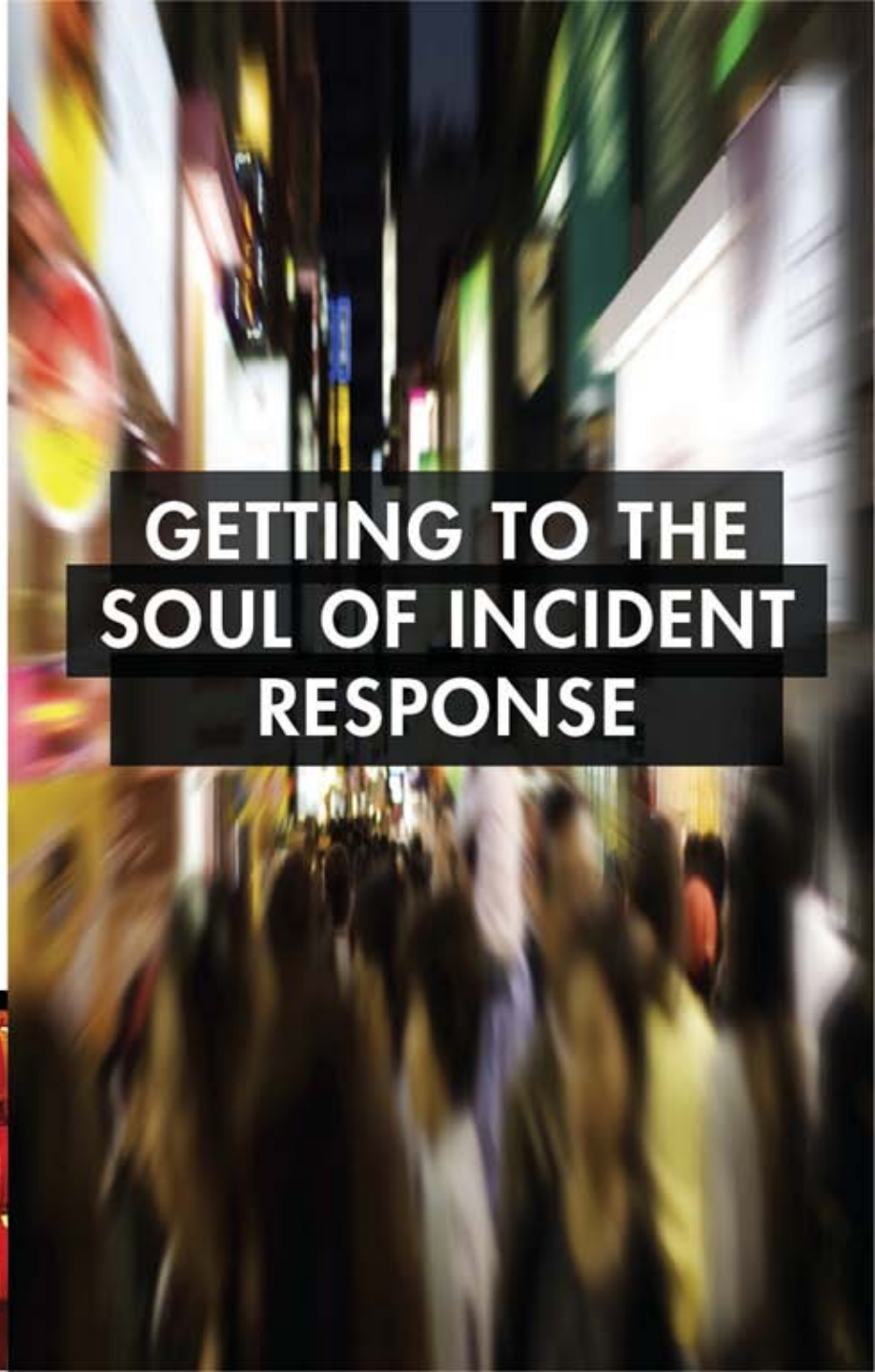
28th ANNUAL FIRST CONFERENCE

SEOUL

JUNE 12 - 17, 2016



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

28th ANNUAL FIRST CONFERENCE SEOUL JUNE 12 - 17, 2016
CyberSecurity MALAYSIA

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[1] injection

Target: **Database servers**
purpose:
- Obtain account and user credentials
- Steal sensitive data

CYBER INCIDENTS BY SECTORS

Rank	Sector	Number of Incidents	Percentage of Incidents (100%)
1	Healthcare	116	37%
2	Retail	34	11%
3	Education	31	10%
4	Gov. & Public Sector	26	8%
5	Financial	19	6%
6	Computer Software	13	4%
7	Hospitality	12	4%
8	Insurance	11	4%
9	Transportation	9	3%
10	Arts and Media	6	2%

Top 10 Sectors Breached by Number of Incidents

Source: Symantec

CYBER INCIDENTS - MALAYSIA

April 2015

MYNIC Berhad

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.

June 2015

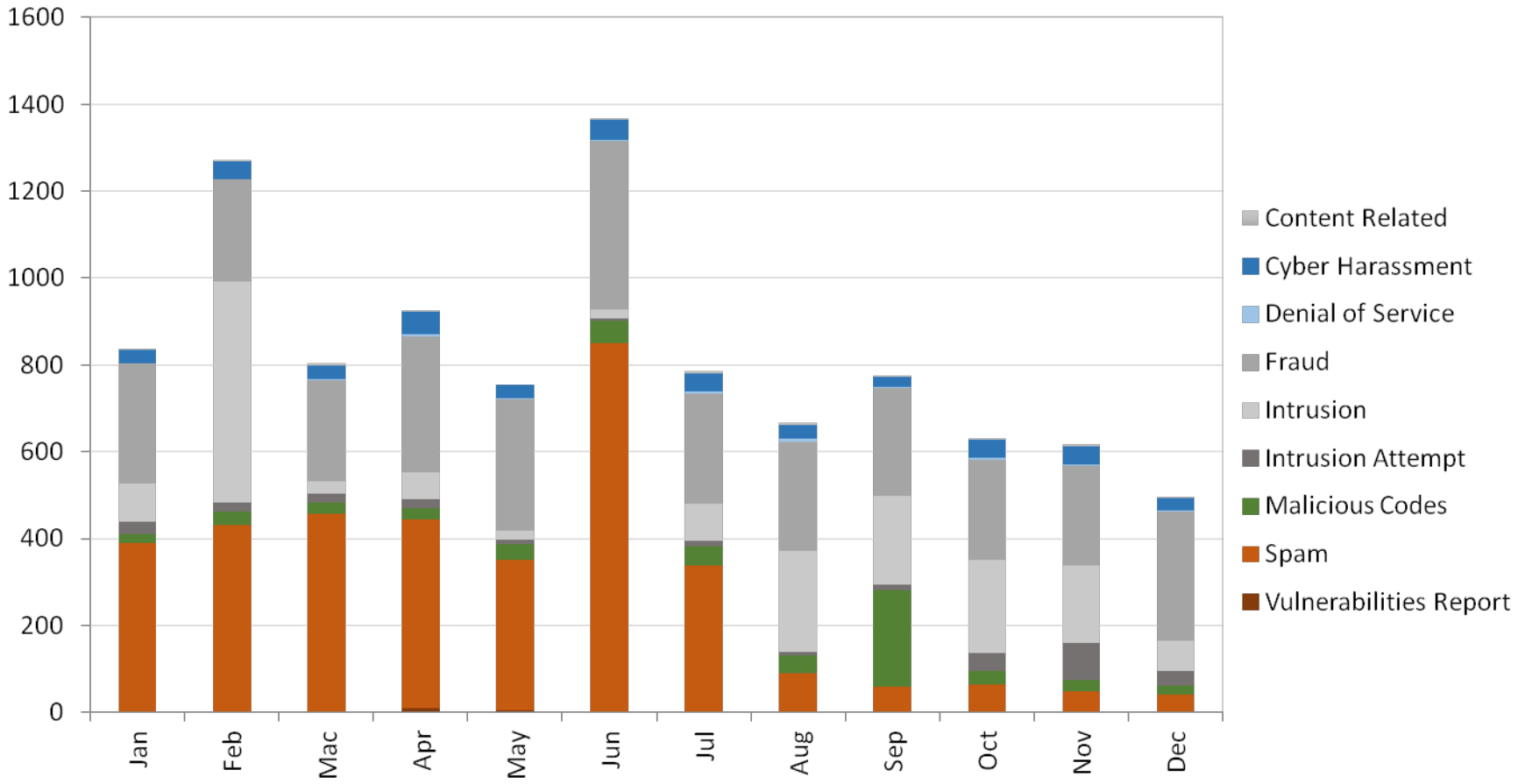
Malaysia Airlines

The home page of ***Malaysia Airllines 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



REQUIREMENTS FOR CSIRT IN ORGANIZATION IN MALAYSIA

In 2013, the National Security Council of Malaysia (NSC) released the guideline *"NSC Directive 24: National Cyber Crisis Management Mechanism."*

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*

SERVICES OFFERED BY CSIRT (Example)

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

Prepare for any possible imminent problems

Respond to problems & incident handling

Quality management service

CyberDEF

D *"detection of cyber treat"*

E *"eradication of cyber treat"*

F *"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

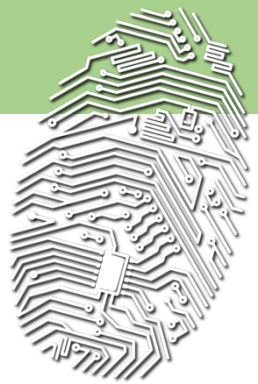
Eradication

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.

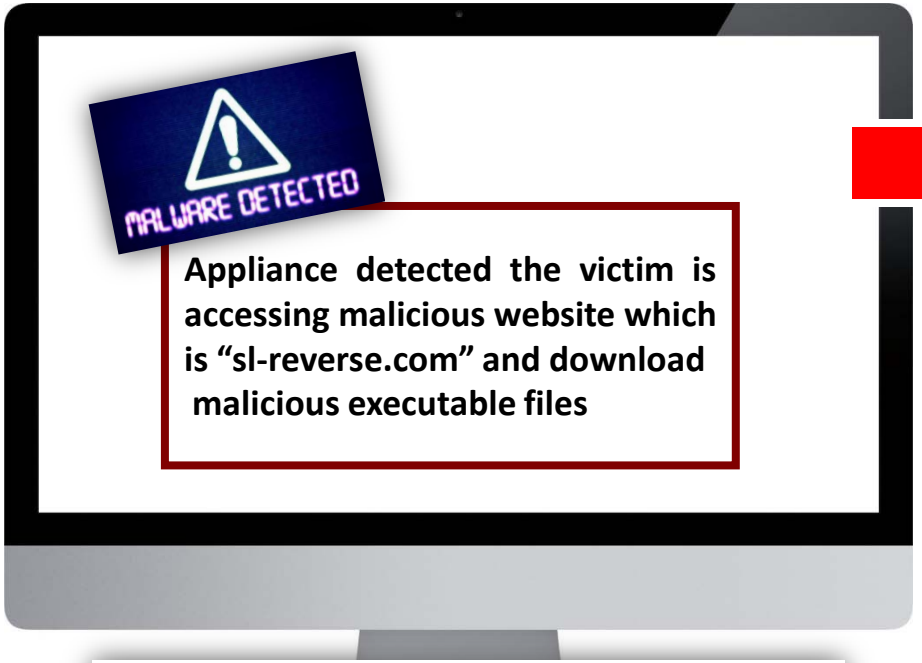
Forensic Element

Forensic element **incorporated** in the services offered

CSIRT MANAGEMENT WORKFLOW

Process	MyCERT	STS	DF	C-Level
Detection **Response time =** 0.5 hour	Constant monitoring Detect threats Register case in OTRS	Constant monitoring Detect threats		
Verification **Response time =** 3 hour	Analyze threats Conduct debrief to team members	Identify device		Inform Top Management
Containment **Response time =** 1 hour	Inform HoD of suspected device's owner Verify threat with actual device	Preserve memory dump Collect device		
Preservation **Response time =** 16 hour			Preserve device	
Analysis **Response time =** 5 days	Security analysis Produce security analysis report		Evidence analysis Produce root cause analysis report	
Eradication **Response time =** 1 hour		Eradicate the threats based on recommendations Recover device Return device		
Reporting **Response time =** 1 hour				Report submission to Top Management

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 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
```

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
```

CASE STUDY: DETECTION (Cont…)

Affected device identified

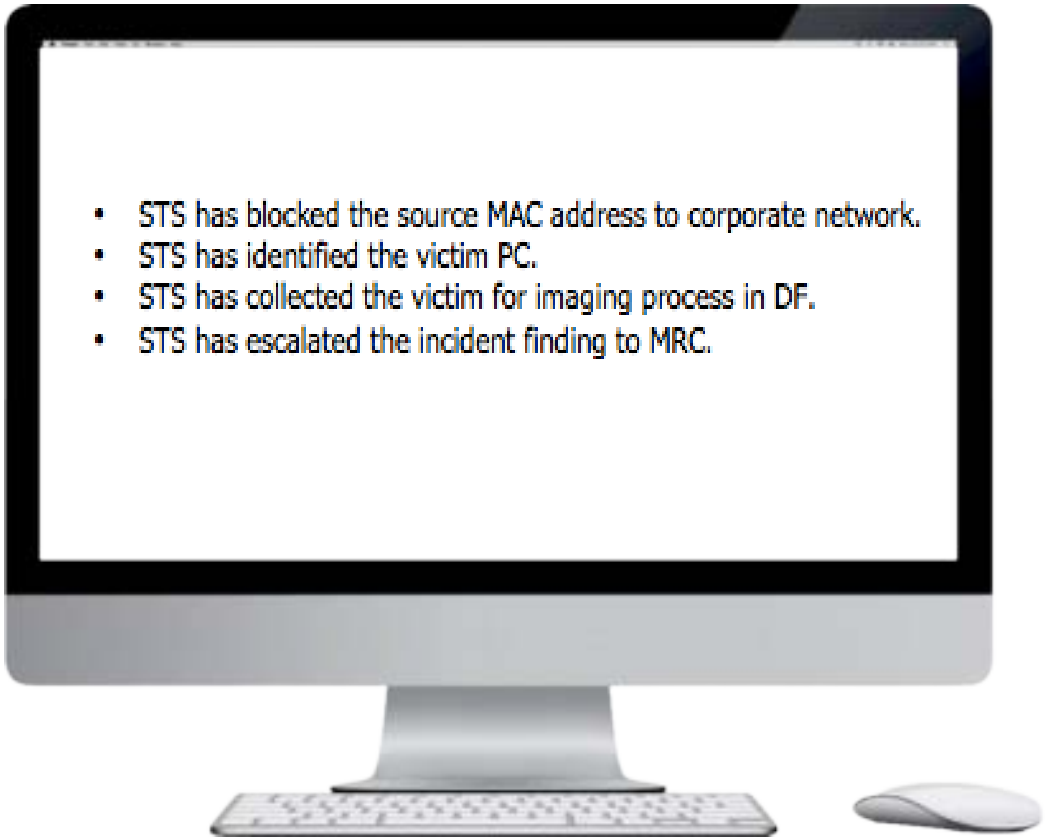
IP Address	xx.x.xx.xxx
MAC Address	xc:0x:x1:xf:52:ex
NetBIOS Name	[redacted]
Staff Name	[redacted]
Location	[redacted]
Department	[redacted]

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

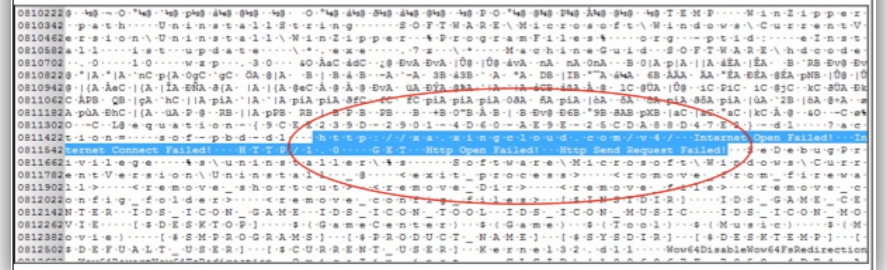
Analysis

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

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:



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:

URL	Source
http://safe.soft365.com/lrd/stats?key=1&dvalue=1&dstatype=string	Zul Finance E01 - Partition 5 (Microsoft NTFS, 661.48 GB) (All Files and Folders) - [ROOT]/Program Files (x86)/WinZipper/wz1bg.exe
http://ua/Request2/update?ptid=1&dacd=1&dln=1&dlr=1&dver=1&dudt=1&dpcd=1&data=1a	Zul Finance E01 - Partition 5 (Microsoft NTFS, 661.48 GB) (All Files and Folders) - [ROOT]/Program Files (x86)/WinZipper/wz1bg.exe
http://up.yac.mx/Request/update?ptid=1&dacd=1&dln=1&dver=1&dudt=1&dpcd=1a	Zul Finance E01 - Partition 5 (Microsoft NTFS, 661.48 GB) (All Files and Folders) - [ROOT]/Program Files (x86)/WinZipper/wz1bg.exe
http://safe.soft365.com/lrd/stats?key=1&dvalue=1&dstatype=string	Zul Finance E01 - Partition 5 (Microsoft NTFS, 661.48 GB) (All Files and Folders) - [ROOT]/Users/Zulmuni/AppData/Local/Temp/at6C47tmp/omigasp/wz1bg.exe
http://ua/Request2/update?ptid=1&dacd=1&dln=1&dlr=1&dver=1&dudt=1&dpcd=1&data=1a	Zul Finance E01 - Partition 5 (Microsoft NTFS, 661.48 GB) (All Files and Folders) - [ROOT]/Users/Zulmuni/AppData/Local/Temp/at6C47tmp/omigasp/wz1bg.exe
http://up.yac.mx/Request/update?ptid=1&dacd=1&dln=1&dver=1&dudt=1&dpcd=1a	Zul Finance E01 - Partition 5 (Microsoft NTFS, 661.48 GB) (All Files and Folders) - [ROOT]/Users/Zulmuni/AppData/Local/Temp/at6C47tmp/omigasp/wz1bg.exe

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)

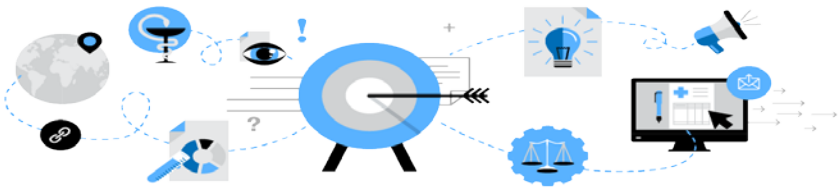
Details | Hex | Text

Application Name	WZUPG.EXE
Application Run Count	2
Last Run Date/Time - (UTC) (MM/dd/yyyy)	02/24/2016 04:28:59 AM
2nd Last Run Date/Time - (UTC) (MM/dd/yyyy)	02/24/2016 03:58:59 AM
3rd Last Run Date/Time - (UTC) (MM/dd/yyyy)	(not found)
4th Last Run Date/Time - (UTC) (MM/dd/yyyy)	(not found)
5th Last Run Date/Time - (UTC) (MM/dd/yyyy)	(not found)

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

CyberSecurity MALAYSIA

MOSTI
KEMENTERIAN SAINS, TEKNOLOGI DAN INOVASI
MINISTRY OF SCIENCE, TECHNOLOGY AND INNOVATION

Best Brand Internet Security 2008 & 2009

ISMS SIRIM — CERTIFIED TO ISO/IEC 27001:2005 CERT NO. : AR4658

STANDARDS MALAYSIA — MS ISO/IEC 17025 TESTING SAMM NO. 456 (MyBEP LABORATORY)

MSC MALAYSIA Status Company

Best Child Online Protection Website

28th ANNUAL FIRST CONFERENCE SEOUL JUNE 12 - 17, 2016