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

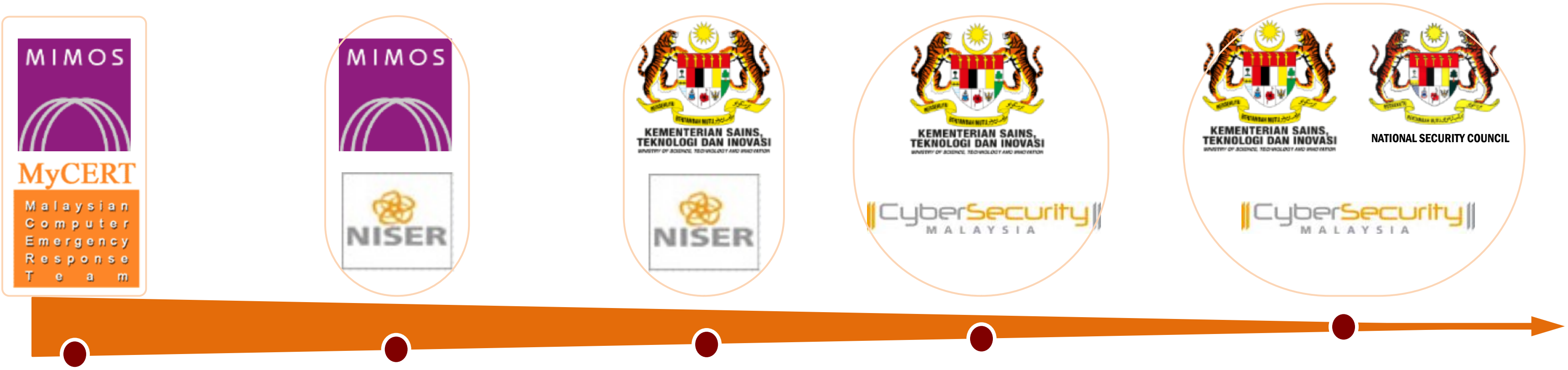
CyberSecurity MALAYSIA

DETECTION, ERADICATION & FORENSIC: CYBER THREATS INTELLIGENCE MODEL FOR CNII ORGANIZATIONS

PREPARED BY :

- NURUL HUSNA MOHD NOR HAZALIN
- ZAHRI YUNOS

ABOUT CYBERSECURITY MALAYSIA


MIMOS
MyCERT
Malaysian Computer Emergency Response Team
MIMOS
NISER
KEMENTERIAN SAINS, TEKNOLOGI DAN INOVASI
NISER
KEMENTERIAN SAINS, TEKNOLOGI DAN INOVASI
CyberSecurity MALAYSIA
KEMENTERIAN SAINS, TEKNOLOGI DAN INOVASI
NATIONAL SECURITY COUNCIL
CyberSecurity MALAYSIA

1997

2001

2006

2007

2017

- **A technical cyber security agency under the Ministry of Science, Technology & Innovation (MOSTI)**
- **Started operation as the Malaysia Computer Emergency Response Team (MyCERT) in year 1997 and later "rebranded" as CYBERSECURITY MALAYSIA in 2007**

30 Mar 2007
NISER was officially registered as CyberSecurity Malaysia (CSM)

20 Aug 2007
CSM was launched by YAB Prime Minister

11 Jan 2017
Cabinet meeting agreed that CSM national cybersecurity functions report directly to NACSA while CSM functions on industry development and R&D remain under the purview of MOSTI

21 Dec 2017
MOSTI & National Security Council signed *Memorandum of Understanding*

CyberSecurity Malaysia - Services

CYBER SECURITY RESPONSIVE SERVICES

Cyber999 Help Centre

Cyber999

MyCERT
Malaysia Computer Emergency Response Team

Digital Forensics

CYBER SECURITY PROACTIVE SERVICES

Security Management & Best Practices

Security Assurance

Cyber Security Certification

OUTREACH & CAPACITY BUILDING

Global Accredited Cybersecurity Education Scheme

Outreach

STRATEGIC STUDY & ENGAGEMENT

Strategic Engagement

Strategic Study

INDUSTRY & RESEARCH DEVELOPMENT

Industry Development

Research & Development

Cyber999™
Cyber Early Warning Services

Incident Handling

Cyber Early Warning

Technical Coordination Centre

Malware Research Center

REFERENCE CENTRE FOR CYBER SECURITY TECHNICAL ASSISTANCE

for all internet users, including home users and organizations

Email us at:
cyber999@cybersecurity.my

PROTECTION OF CRITICAL NATIONAL INFORMATION INFRASTRUCTURE (CNII)

- Key To Malaysia's E-Sovereignty

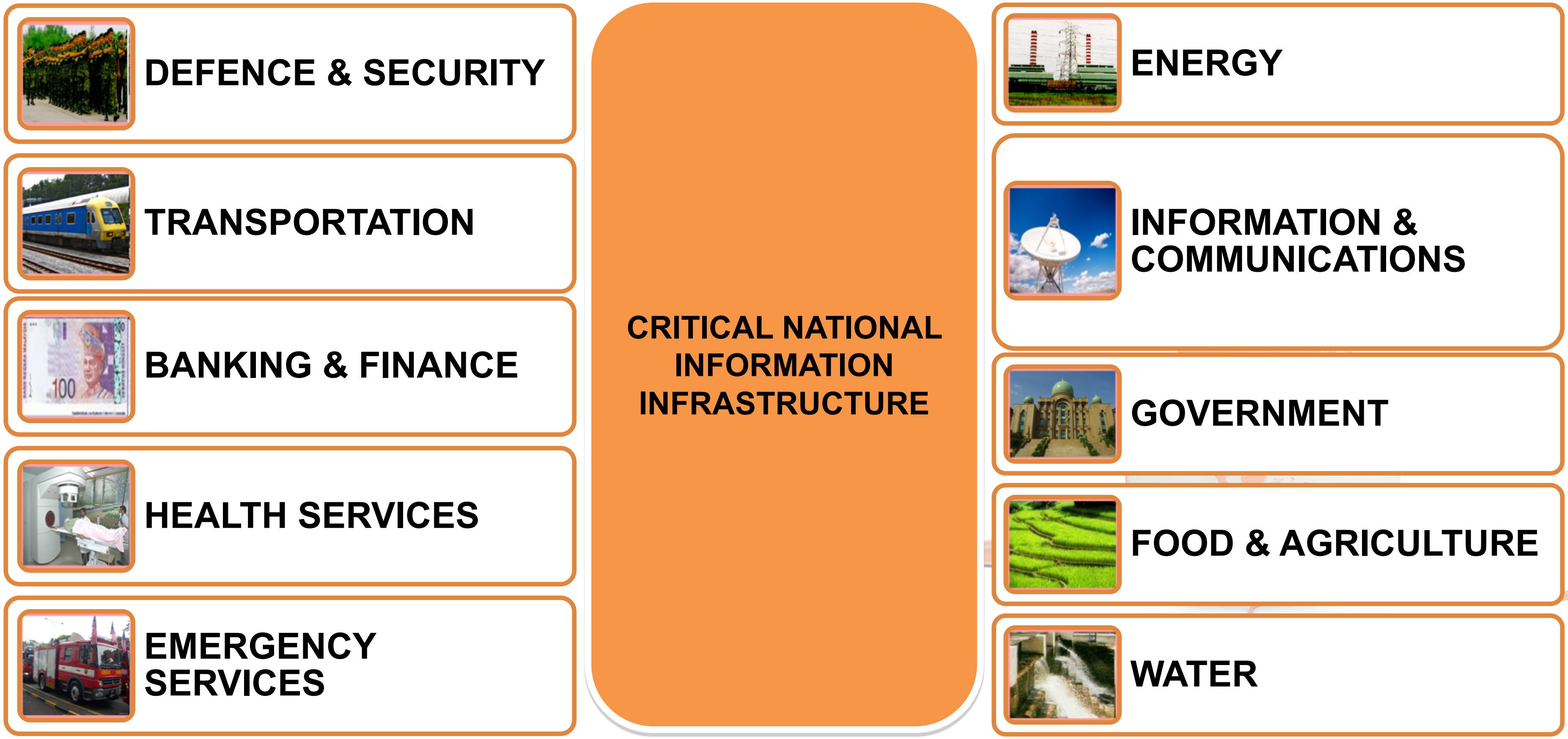
CNIIs:
Assets, systems and functions that are vital to the nation that their incapacity or destruction would have a devastating impact on:

- National Defence and Security
- National Economic Strength
- National Image
- Government Capabilities to Function
- Public Health and Safety

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'



CRITICAL NATIONAL INFORMATION INFRASTRUCTURE

DEFENCE & SECURITY

TRANSPORTATION

BANKING & FINANCE

HEALTH SERVICES

EMERGENCY SERVICES

ENERGY

INFORMATION & COMMUNICATIONS

GOVERNMENT

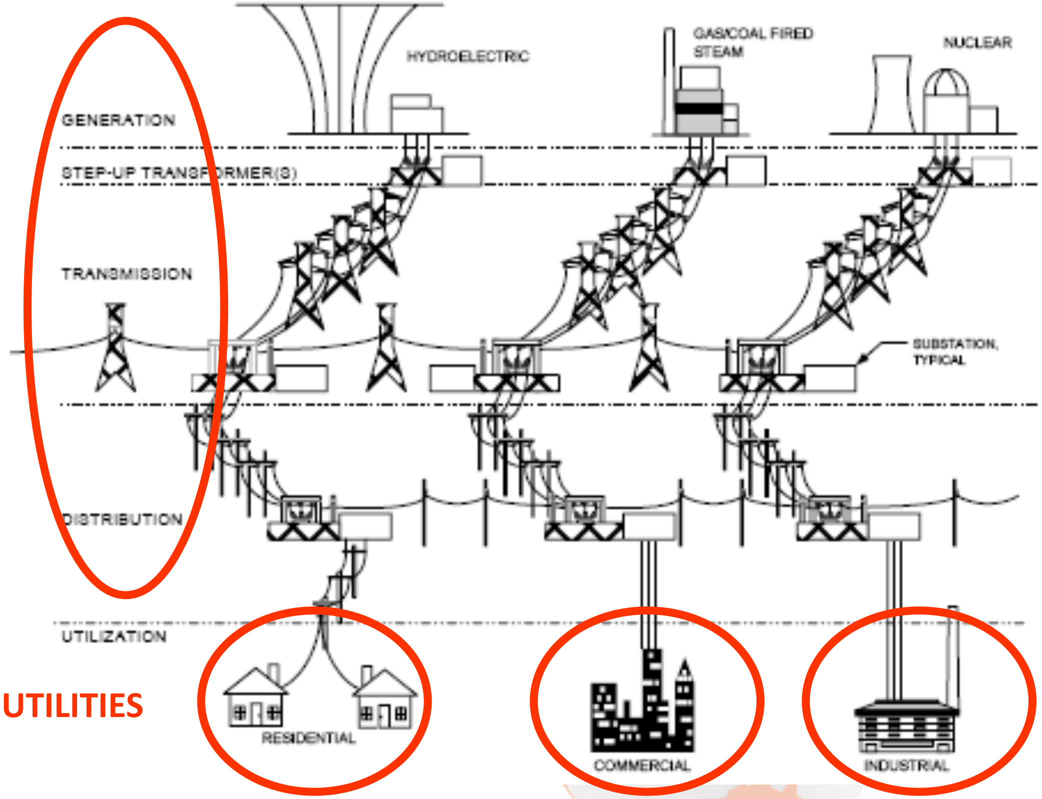
FOOD & AGRICULTURE

WATER

THREATS TO CNII : INTERDEPENDENCY

The high degree of interdependency between critical infrastructure sectors means failures in one sector can propagate into others.

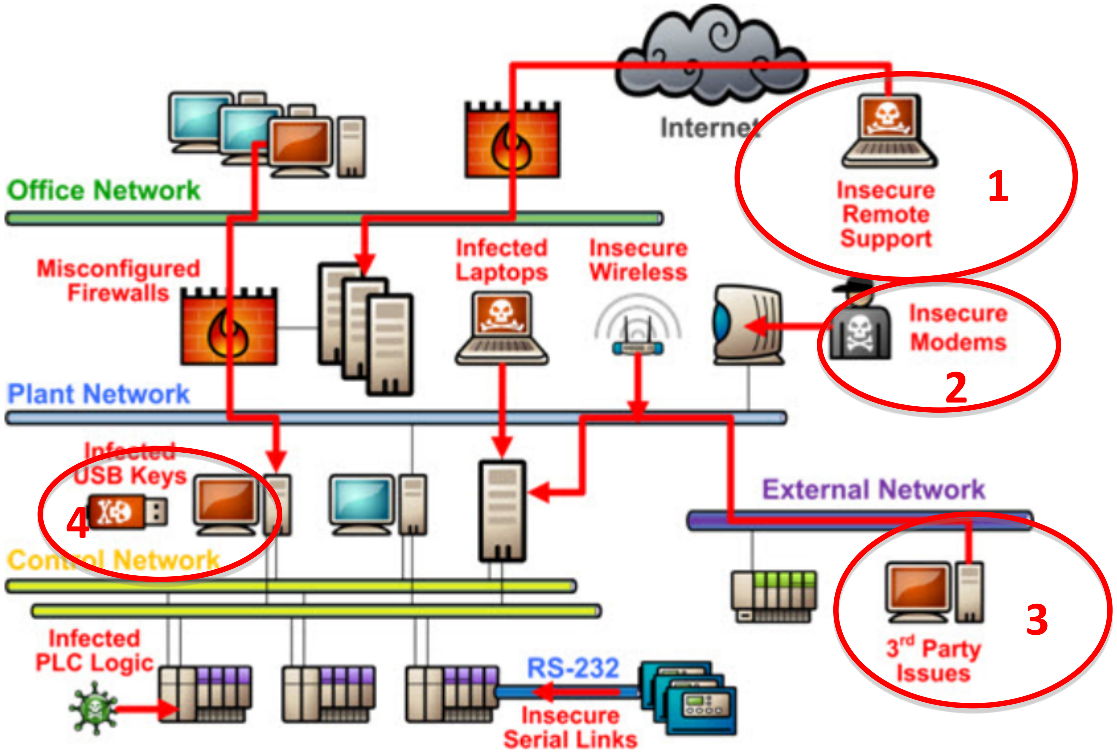
ELECTRICITY



UTILITIES

SECTORS / SERVICES

THREATS TO CNII : SCADA SYSTEMS



SCADA = Supervisory Control & Data Acquisition

1st Generation SCADA - Monolithic
Single server controlling a small number of sensors and/or actuators.

No wider connectivitiy.

↓

2nd Generation SCADA - Distributed
Connection of individual SCADA systems into centralised network.

No wider connectivitiy.

↓

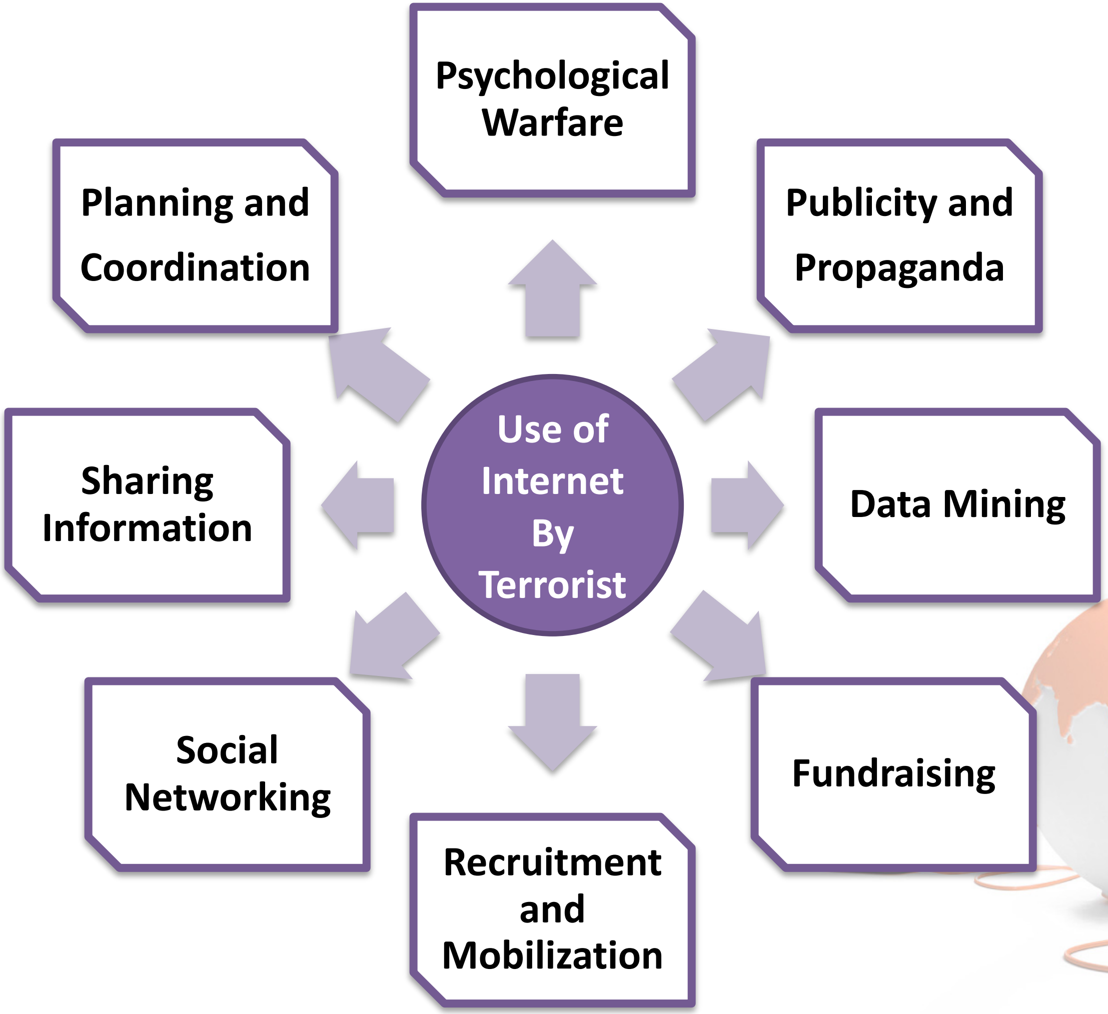
3rd Generation SCADA - Networked
SCADA network connected to corporate network.

Connectivity to internet and third parties via corporate network.

↓

4th Generation SCADA - Internet of Things
SCADA equipment connected directly to internet.

THREATS TO CNII : THE USE OF ICT AND CYBERSPACE BY TERRORIST



Use of Internet By Terrorist

Psychological Warfare

Publicity and Propaganda

Data Mining

Fundraising

Recruitment and Mobilization

Social Networking

Sharing Information

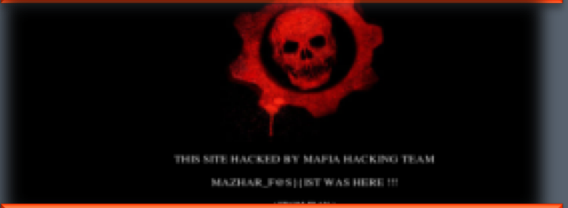
Planning and Coordination

CYBER THREATS COME IN VARIOUS FORMS

Technology Related Threats

Hack Threat

Intrusion


THIS SITE HACKED BY MAFIA HACKING TEAM
MAZHAR_F@S||IST WAS HERE !!!

Fraud

Maybank2u.com

Welcome

Spam

Malicious Code

Denial of Service Attack

Stacheldraht DDoS Attack
Internet
Targeted Server(s)

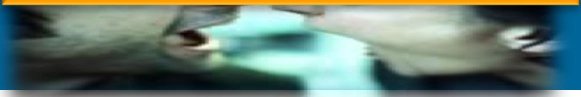
Cyber Content Related Threats

Threats to National Security

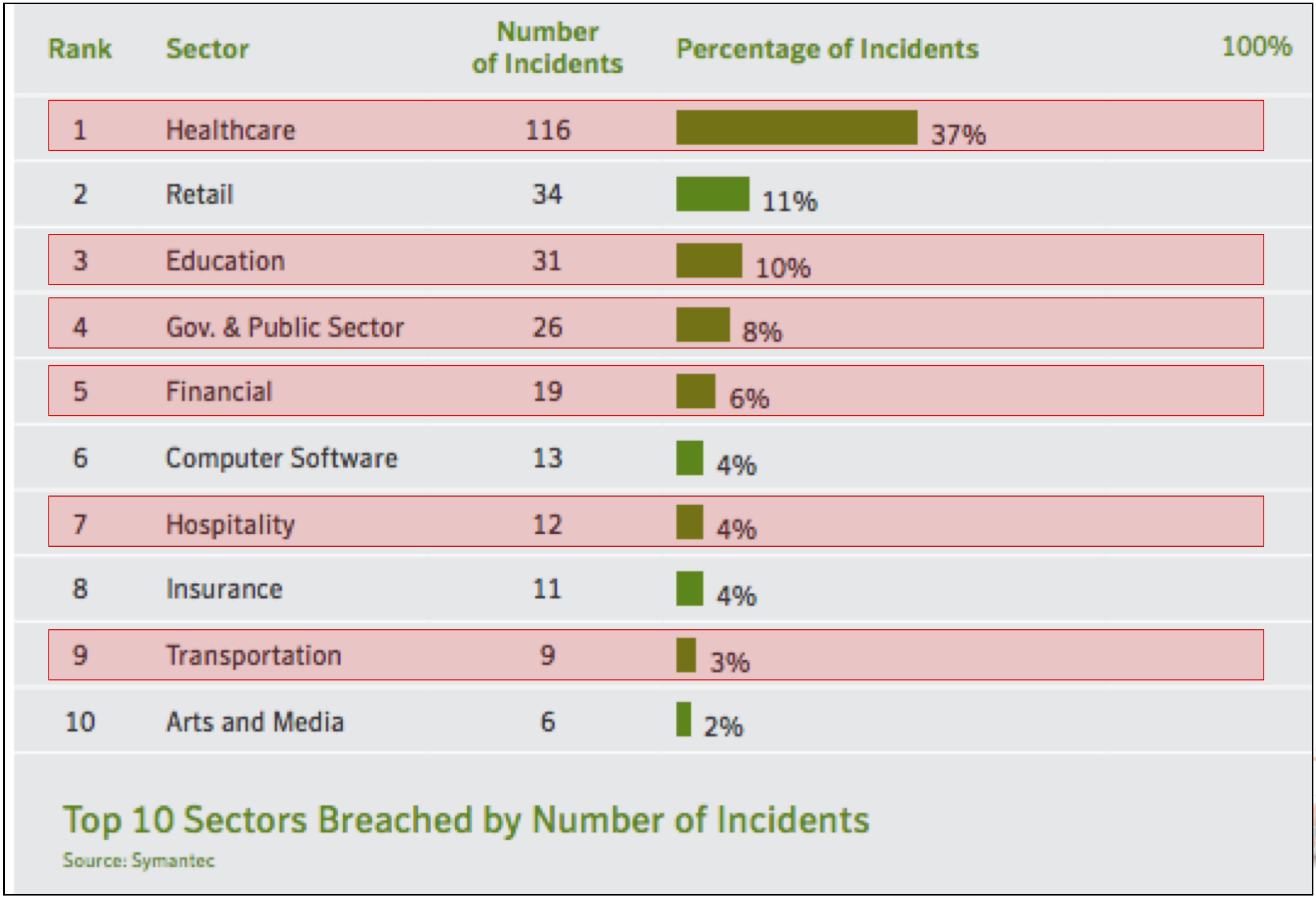
Cyber Harassment

Child Porn

Fake News / Defamation



CYBER INCIDENTS BY SECTORS

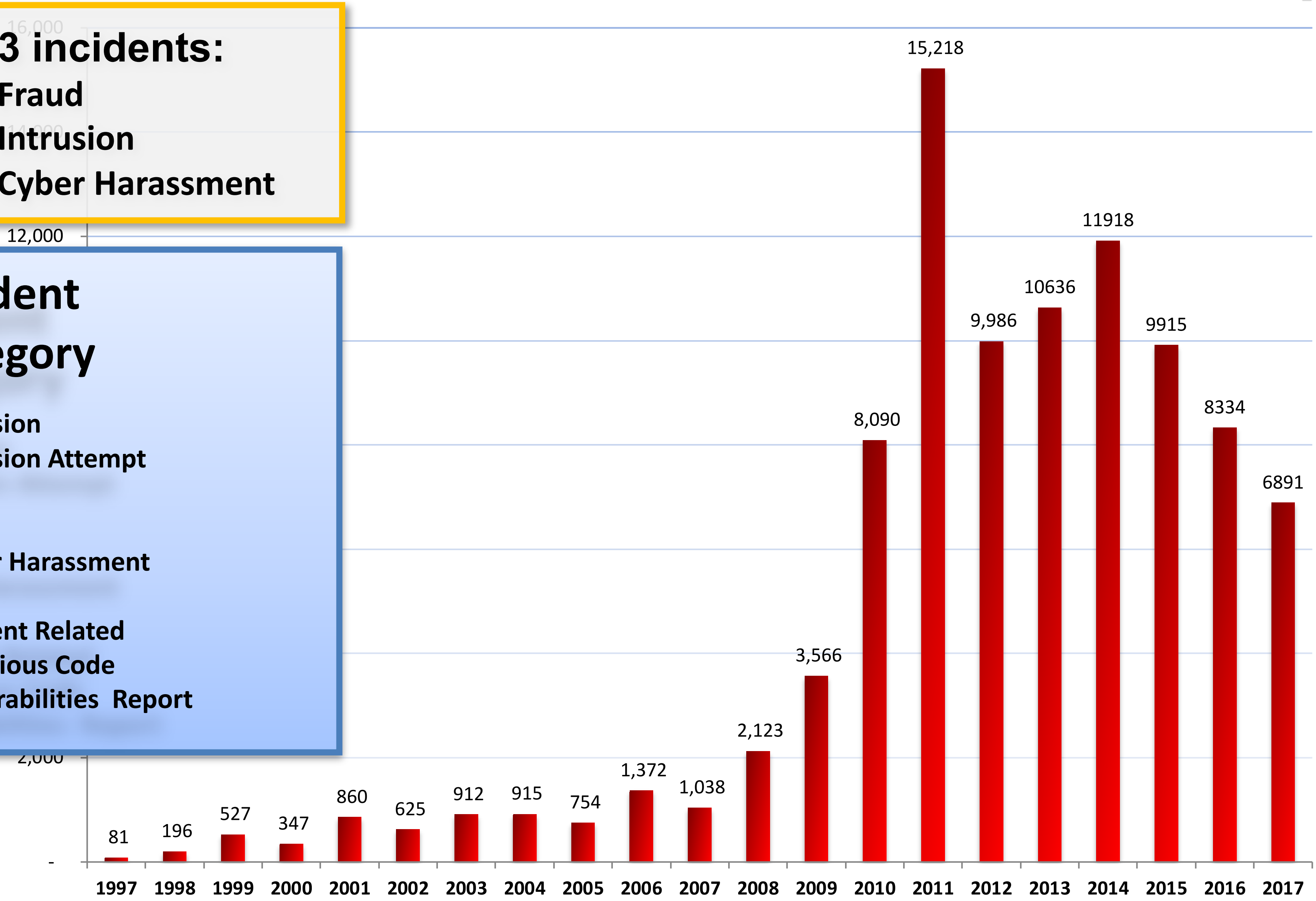


Rank	Sector	Number of Incidents	Percentage of Incidents	100%
1	Healthcare	116	37%	
2	Retail	34	11%	
3	Education	31	10%	
4	Gov. & Public Sector	26	8%	
5	Financial	19	6%	
6	Computer Software	13	4%	
7	Hospitality	12	4%	
8	Insurance	11	4%	
9	Transportation	9	3%	
10	Arts and Media	6	2%	

Top 10 Sectors Breached by Number of Incidents

Source: Symantec

CYBER SECURITY INCIDENTS REPORTED TO CYBERSECURITY MALAYSIA



Top 3 incidents:

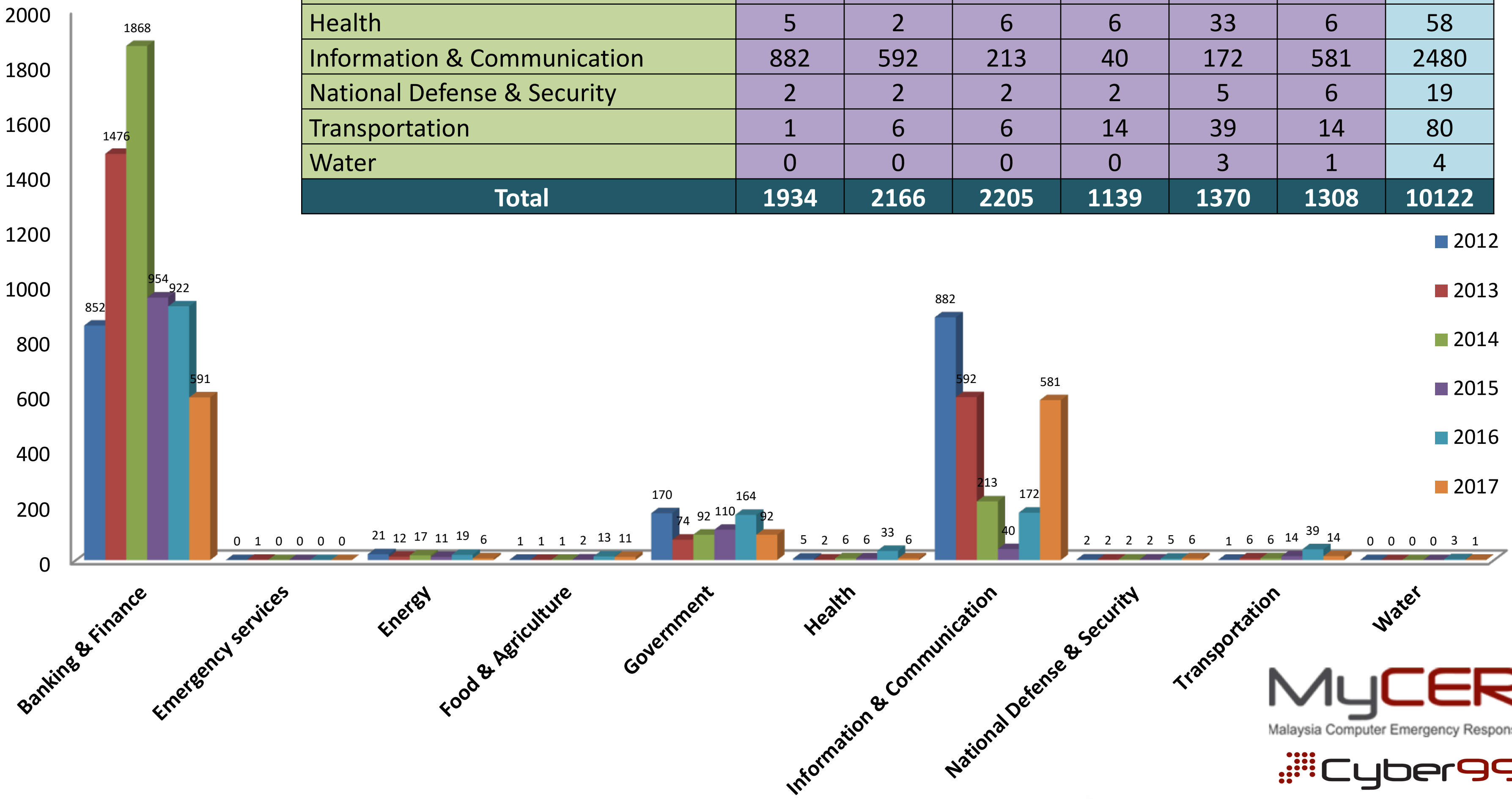
1. Fraud
2. Intrusion
3. Cyber Harassment

Incident Category

- Intrusion
- Intrusion Attempt
- Spam
- DOS
- Cyber Harassment
- Fraud
- Content Related
- Malicious Code
- Vulnerabilities Report

CYBER INCIDENTS BY SECTOR (2012-2017)

	2012	2013	2014	2015	2016	2017	TOTAL
Banking & Finance	852	1476	1868	954	922	591	6663
Emergency services	0	1	0	0	0	0	1
Energy	21	12	17	11	19	6	86
Food & Agriculture	1	1	1	2	13	11	29
Government	170	74	92	110	164	92	702
Health	5	2	6	6	33	6	58
Information & Communication	882	592	213	40	172	581	2480
National Defense & Security	2	2	2	2	5	6	19
Transportation	1	6	6	14	39	14	80
Water	0	0	0	0	3	1	4
Total	**1934**	**2166**	**2205**	**1139**	**1370**	**1308**	**10122**

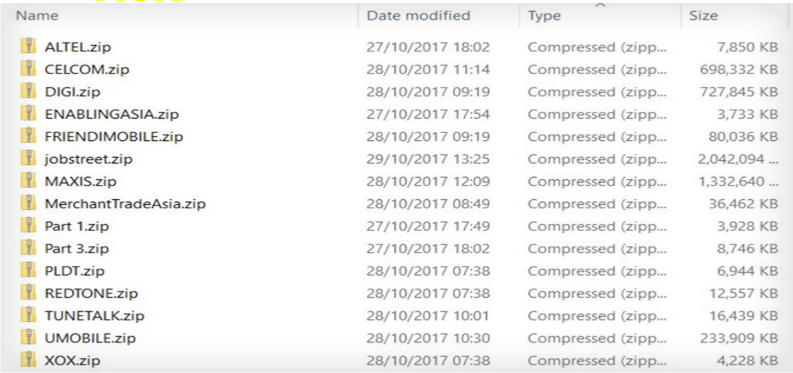


Source : www.mycert.org.my

CYBER INCIDENTS - MALAYSIA

Oct 2017

46.2M mobile subscribers at risk



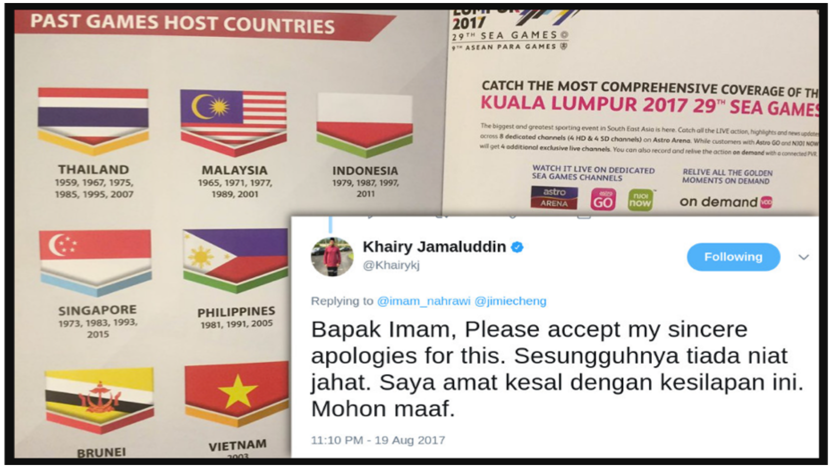
Name	Date modified	Type	Size
ALTEL.zip	27/10/2017 18:02	Compressed (zipp...	7,850 KB
CELCOM.zip	28/10/2017 11:14	Compressed (zipp...	698,332 KB
DIGI.zip	28/10/2017 09:19	Compressed (zipp...	727,845 KB
ENABLINGASIA.zip	27/10/2017 17:54	Compressed (zipp...	3,733 KB
FRIENDIMOBILE.zip	28/10/2017 09:19	Compressed (zipp...	80,036 KB
jobstreet.zip	29/10/2017 13:25	Compressed (zipp...	2,042,094 ...
MAXIS.zip	28/10/2017 12:09	Compressed (zipp...	1,332,640 ...
MerchantTradeAsia.zip	28/10/2017 08:49	Compressed (zipp...	36,462 KB
Part 1.zip	27/10/2017 17:49	Compressed (zipp...	3,928 KB
Part 3.zip	27/10/2017 18:02	Compressed (zipp...	8,746 KB
PLDT.zip	28/10/2017 07:38	Compressed (zipp...	6,944 KB
REDTONE.zip	28/10/2017 07:38	Compressed (zipp...	12,557 KB
TUNETALK.zip	28/10/2017 10:01	Compressed (zipp...	16,439 KB
UMOBILE.zip	28/10/2017 10:30	Compressed (zipp...	233,909 KB
XOX.zip	28/10/2017 07:38	Compressed (zipp...	4,228 KB

On 19th Oct, *lowyat.net,* reported that personal data of 46.2M mobile subscribers are being compromised and being sell online. These included IC numbers, addresses, IMSI, IMEI and SIM numbers as well

CYBER INCIDENTS - MALAYSIA

Aug 2017

OPS Bendera



Khairy Jamaluddin
@Khairykj

Replying to @imam_nahrawi @jimiecheng

Bapak Imam, Please accept my sincere apologies for this. Sesungguhnya tiada niat jahat. Saya amat kesal dengan kesilapan ini. Mohon maaf.

11:10 PM - 19 Aug 2017

Flag blunder in *Kuala Lumpur SEA Games* souvenir booklet has triggered anger among the Indonesian. The situation escalated further to the cyber world and Malaysia came under fire from a group of Indonesian hackers who infiltrated a large number of Malaysian websites.

CYBER INCIDENTS - MALAYSIA

Type of cyber attack:

Web defacement
total of 411 websites were observed to have been defaced (281 were .my websites, 75 .com sites, 47 .gov.my websites)

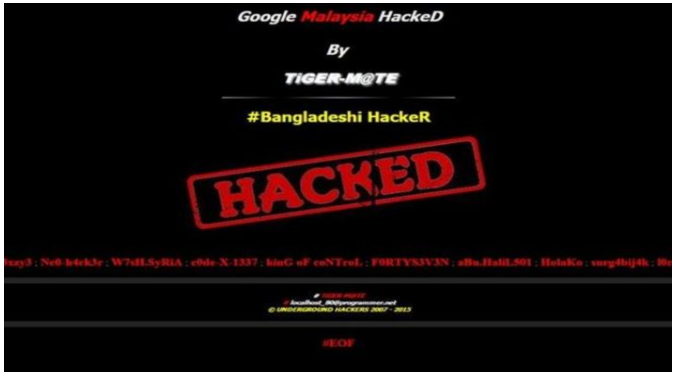
Confidential info leak
leaked and exposed on the publicly available Pastebin website. The types of information leaked were system vulnerabilities, usernames and passwords, and banking information.

Distributed Denial of Service (DDOS) attacked

CYBER INCIDENTS - MALAYSIA

April 2015

MYNIC Berhad



Google Malaysia HackeD

By

TiGER-M@TE

#Bangladeshi HackeR

HACKED

xzy3 : Ne0-h4ck3r : W7sIL.SyRiA : c0de-X-1337 : kinG oF coNTroL : F0RTYS3V3N : aBu.HaliL.501 : HolaKo : surg4bij4k : l0e

TIGER-M@TE
localhost_80@programmer.net
© UNDERGROUND HACKERS 2007 - 2015

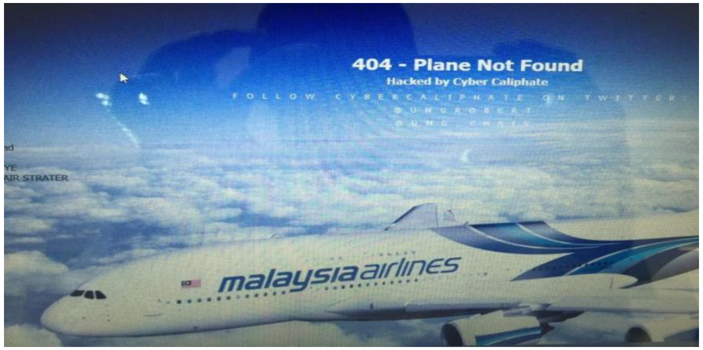
#EOF

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



404 - Plane Not Found
Hacked by Cyber Caliphate
FOLLOW CYBERCALIPHATE ON TWITTER:
@UMGROBERT
@UMG_CHRIS

ad

YE
AIR STRATER

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.

CYBER LAWS IN MALAYSIA

- 1.COMPUTER CRIME ACT 1997
- 2.COMMUNICATIONS AND MULTIMEDIA ACT 1998 (CMA)
- 3.MALAYSIAN COMMUNICATIONS AND MULTIMEDIA COMMISSION ACT 1998
- 4.DIGITAL SIGNATURE ACT 1997 5.COPYRIGHT ACT (AMENDMENT) 1997
- 6.TELEMEDICINE ACT 1997 7.OPTICAL DISC ACT 2000 8.ELECTRONIC TRANSACTIONS ACT 2006

ISSUES AND CHALLENGES

1) Legal challenges

- Digital evidence quality
- Identity / ownership
- Cross border jurisdiction
- Laws & Regulations

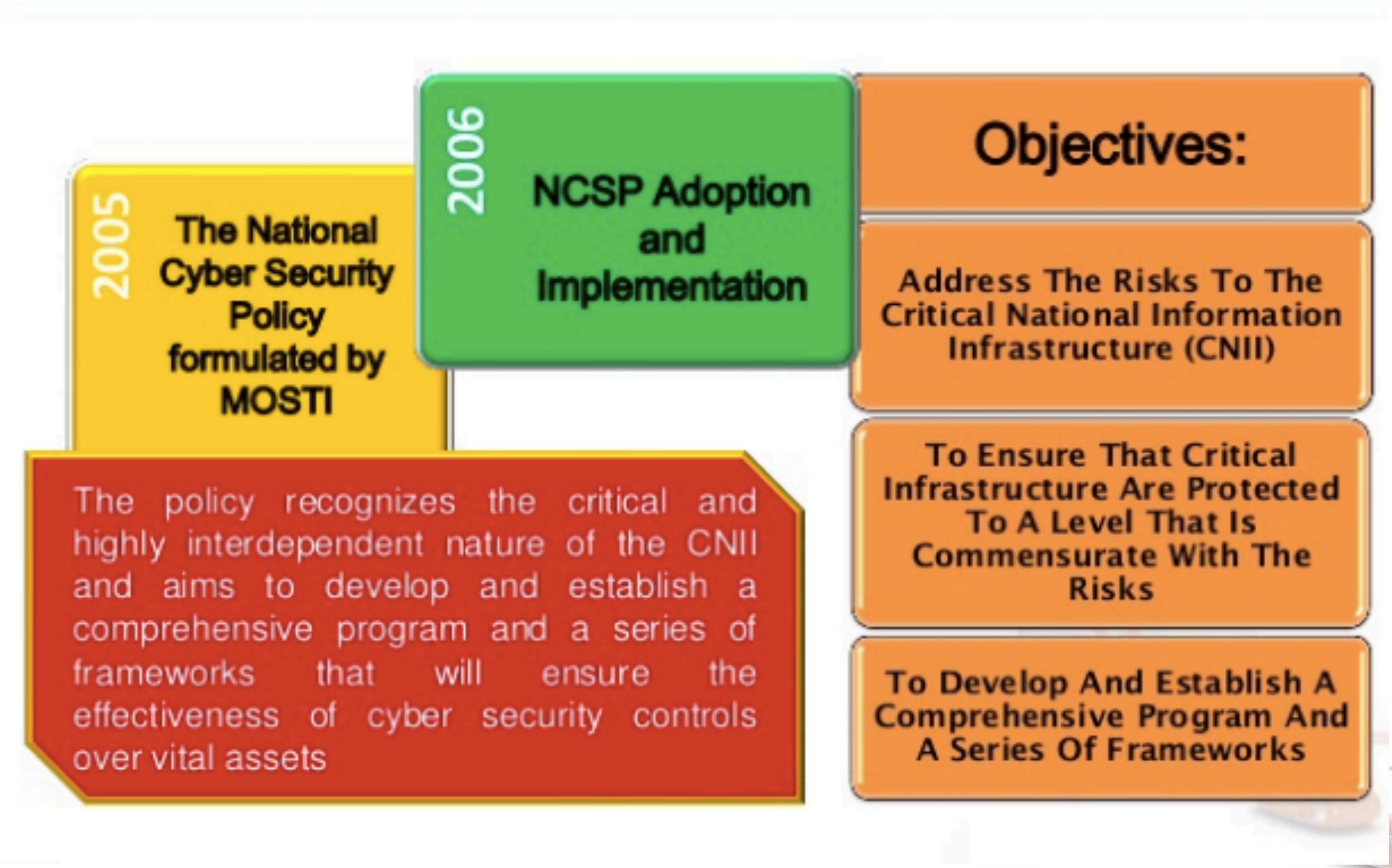
2) Technical challenges

- Anti forensics technology
- Anonymizer technology
- Internet of Things technology

3) Governance challenges

- Inter-working relationship
- Budget and funding
- Syndicate / organized crime network

THE NATIONAL CYBER SECURITY POLICY



2005

The National Cyber Security Policy formulated by MOSTI

2006

NCSP Adoption and Implementation

The policy recognizes the critical and highly interdependent nature of the CNII and aims to develop and establish a comprehensive program and a series of frameworks that will ensure the effectiveness of cyber security controls over vital assets

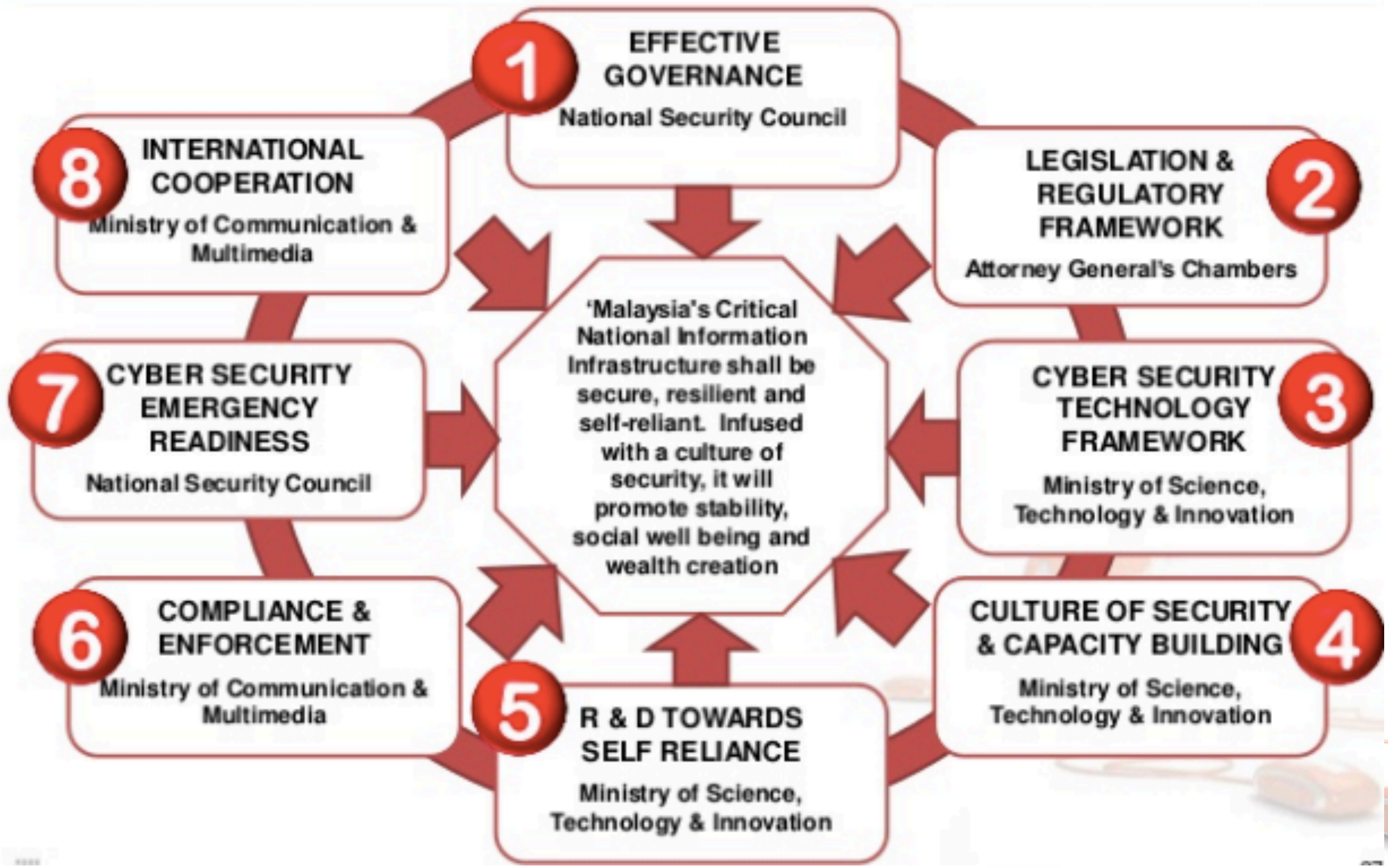
Objectives:

Address The Risks To The Critical National Information Infrastructure (CNII)

To Ensure That Critical Infrastructure Are Protected To A Level That Is Commensurate With The Risks

To Develop And Establish A Comprehensive Program And A Series Of Frameworks

THE NATIONAL CYBER SECURITY POLICY (POLICY THRUST)



'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

1 EFFECTIVE GOVERNANCE
National Security Council

2 LEGISLATION & REGULATORY FRAMEWORK
Attorney General's Chambers

3 CYBER SECURITY TECHNOLOGY FRAMEWORK
Ministry of Science, Technology & Innovation

4 CULTURE OF SECURITY & CAPACITY BUILDING
Ministry of Science, Technology & Innovation

5 R & D TOWARDS SELF RELIANCE
Ministry of Science, Technology & Innovation

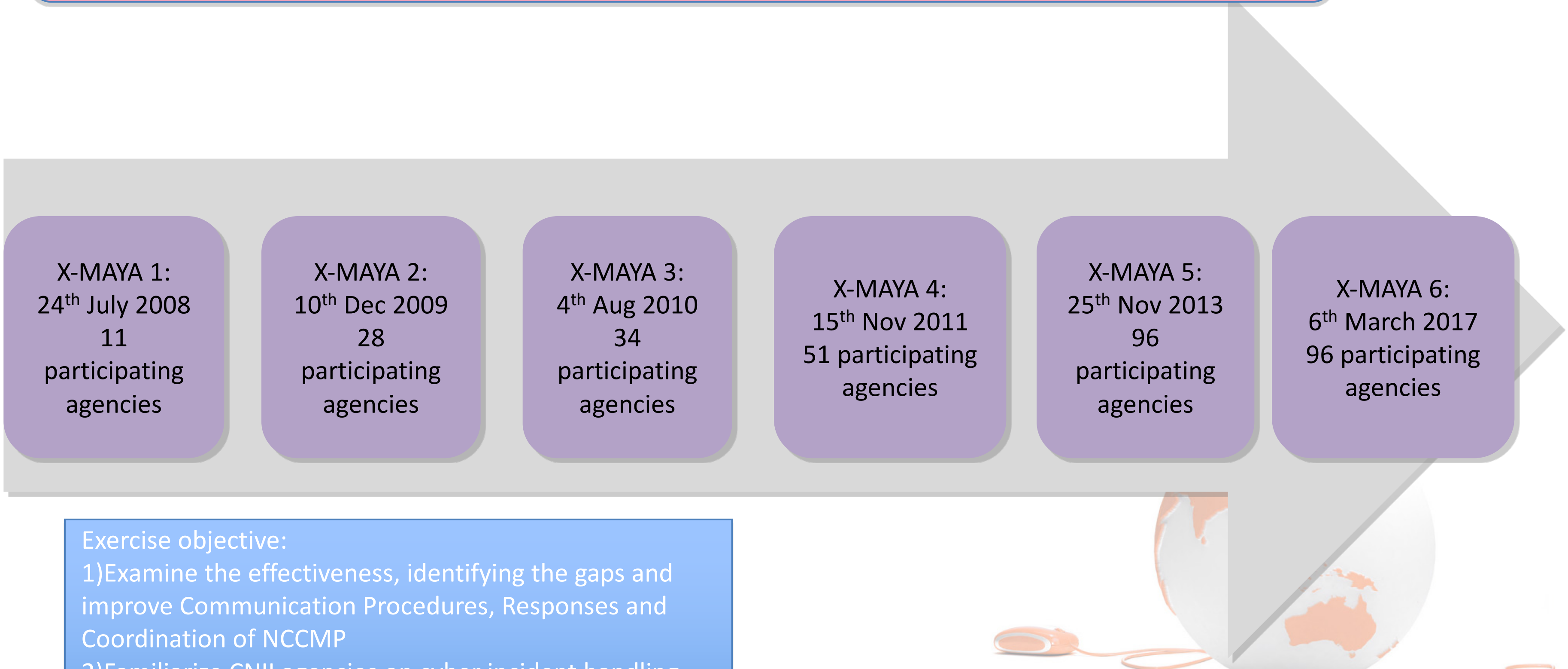
6 COMPLIANCE & ENFORCEMENT
Ministry of Communication & Multimedia

7 CYBER SECURITY EMERGENCY READINESS
National Security Council

8 INTERNATIONAL COOPERATION
Ministry of Communication & Multimedia

NATIONAL CYBER CRISIS MANAGEMENT PLAN

Framework that outline the strategy for cyber attacks mitigation & response among malaysia's CNII through public & private collaboration and coordination



X-MAYA 1:
24th July 2008
11 participating agencies

X-MAYA 2:
10th Dec 2009
28 participating agencies

X-MAYA 3:
4th Aug 2010
34 participating agencies

X-MAYA 4:
15th Nov 2011
51 participating agencies

X-MAYA 5:
25th Nov 2013
96 participating agencies

X-MAYA 6:
6th March 2017
96 participating agencies

Exercise objective:

1)Examine the effectiveness, identifying the gaps and improve Communication Procedures, Responses and Coordination of NCCMP

2)Familiarize CNII agencies on cyber incident handling mechanisms

3) Familiarize communication between CNII agencies during cyber incidents.

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*

CyberDEF

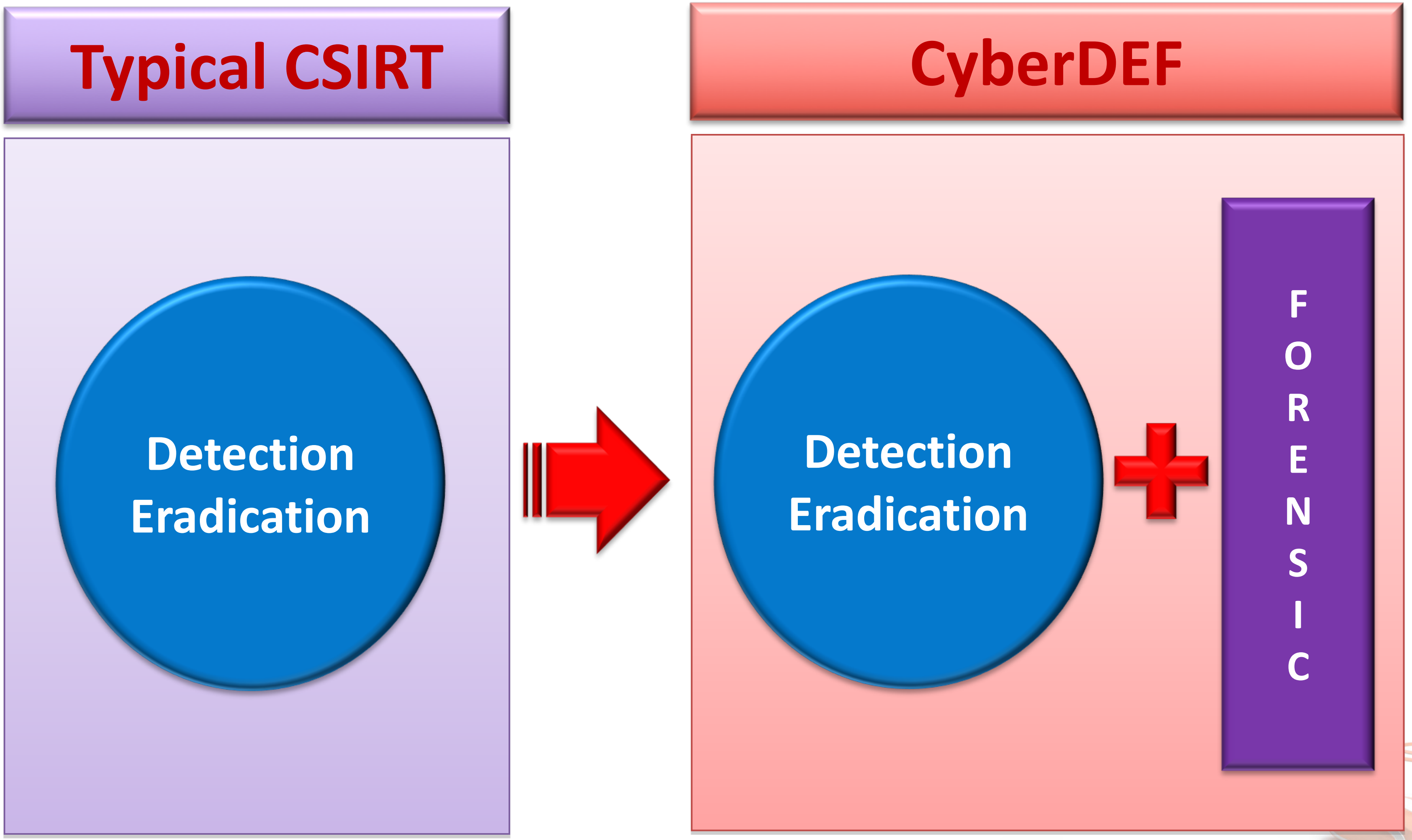
D *“detection of cyber threat”*

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 (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

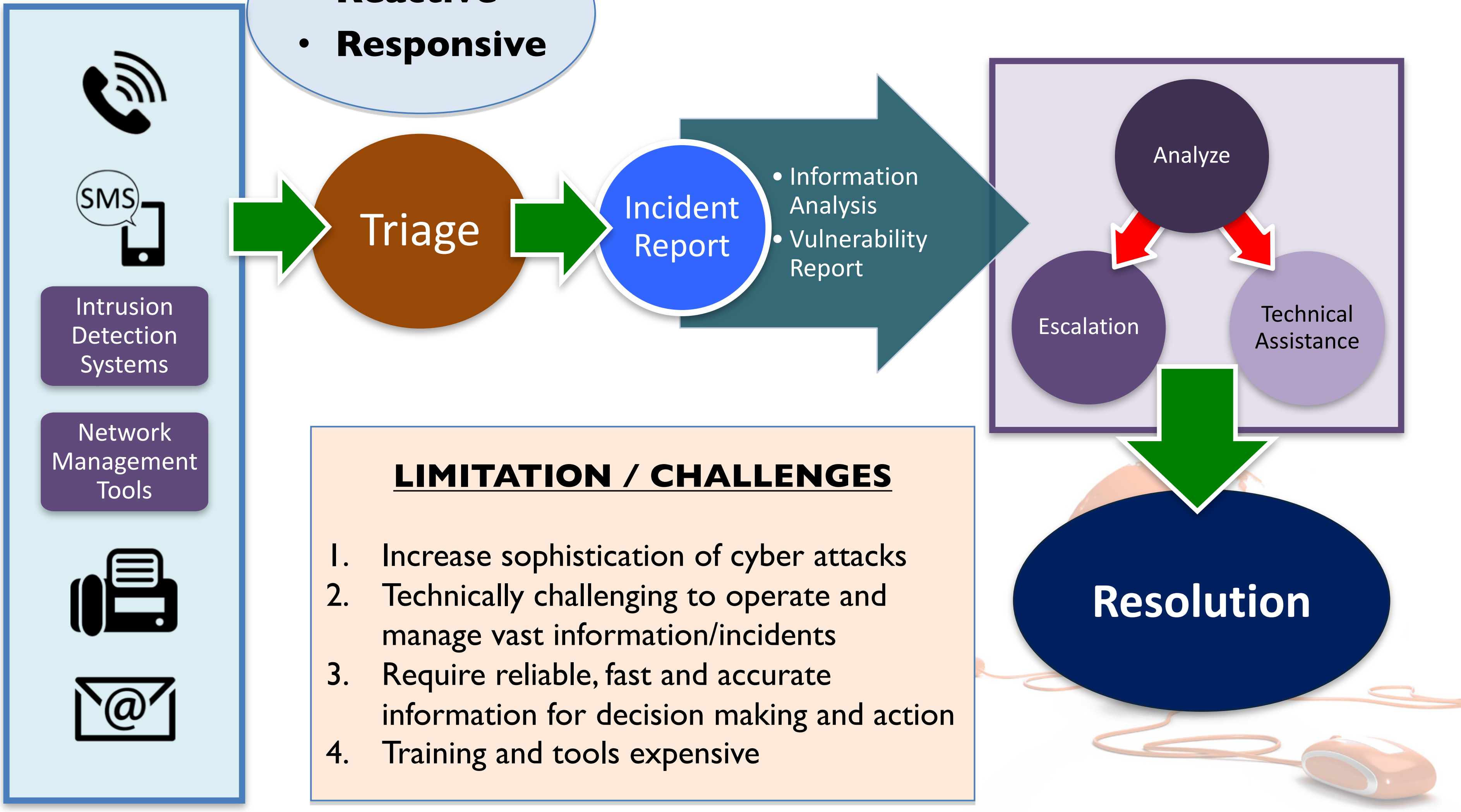
Forensics

1. E-Discovery
2. Root cause analysis
3. Investigation
4. Forensics readiness
5. Forensic compliance

TRADITIONAL SOC OPERATION

PHILOSOPHY

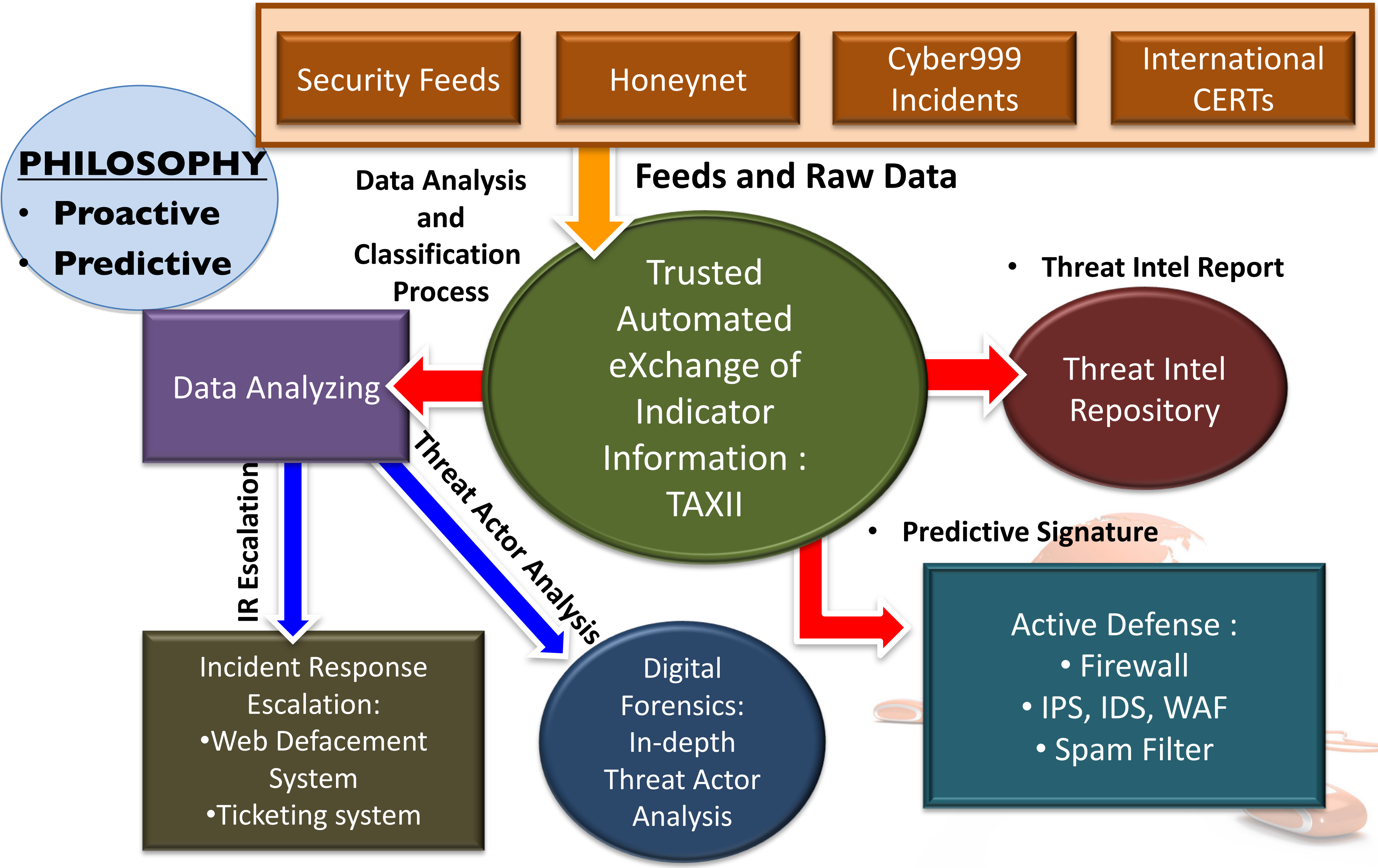
- **Reactive**
- **Responsive**



LIMITATION / CHALLENGES

1. Increase sophistication of cyber attacks
2. Technically challenging to operate and manage vast information/incidents
3. Require reliable, fast and accurate information for decision making and action
4. Training and tools expensive

PROPOSED SOC OPERATION V2.0



INTENDED OUTCOME SOC V2.0

To have better ways of addressing the broad category of cyber security threats

To improve current framework/system that can proactively provide early warning mechasim about cyber security threats in real-time

To enhance the service in terms of expertise and information sharing with relevant authorities and partners

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

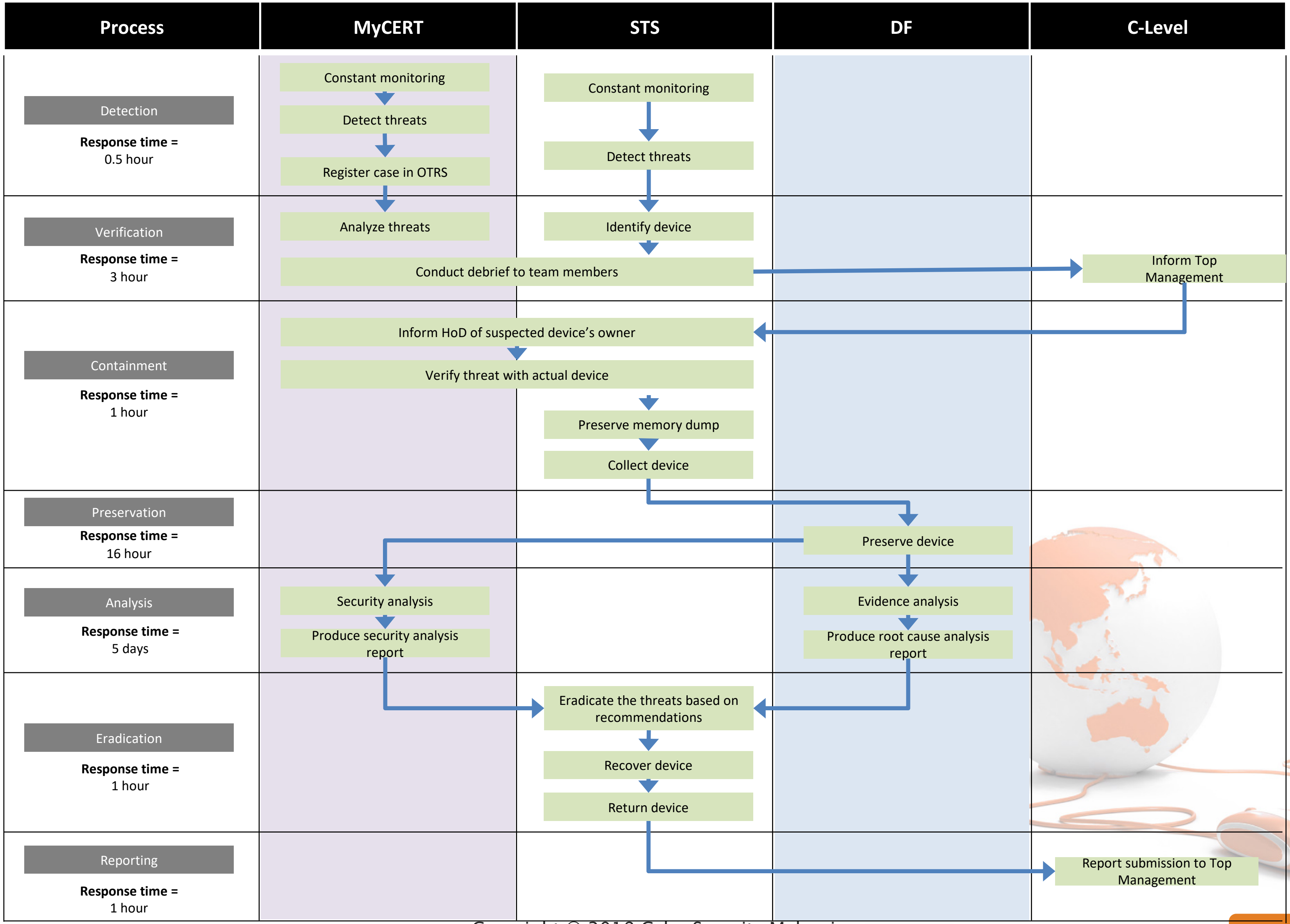
Effective **centralized governance** because all of the 3 involved departments report directly to Vice President of Cyber Security Responsive Services.

Forensic Element

Forensic element **incorporated** in the services offered

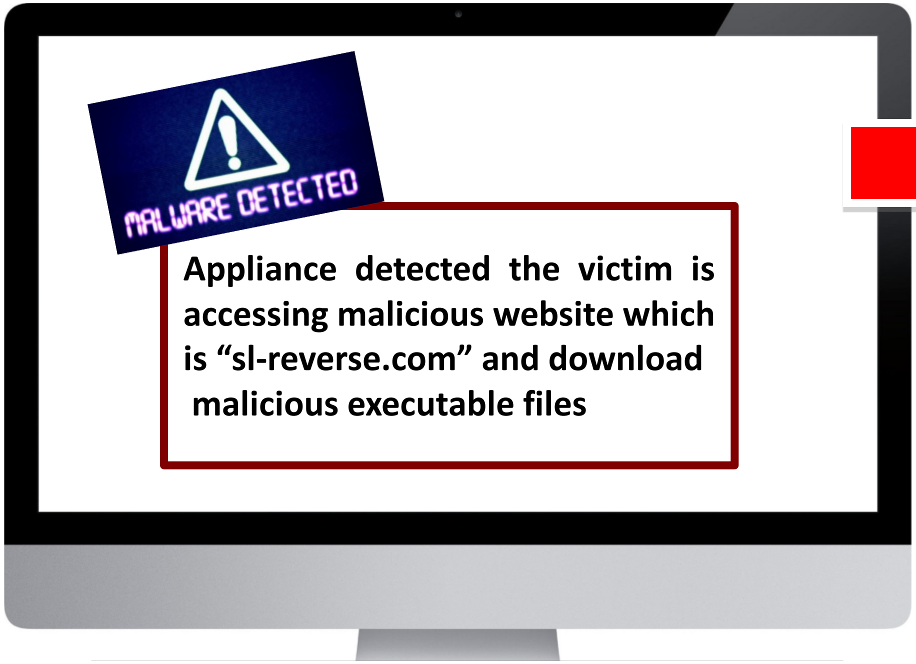
Cyber 999

CSIRT MANAGEMENT WORKFLOW

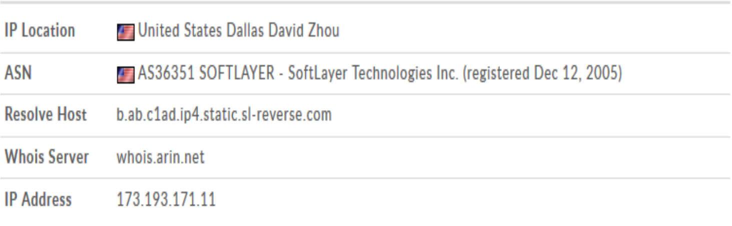


Process	MyCERT	STS	DF	C-Level
Detection **Response time =** 0.5 hour	Constant monitoring Detect threats Register case in OTRS	Constant monitoring Detect threats		
Verification **Response time =** 3 hour	Analyze threats Conduct debrief to team members	Identify device		Inform Top Management
Containment **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

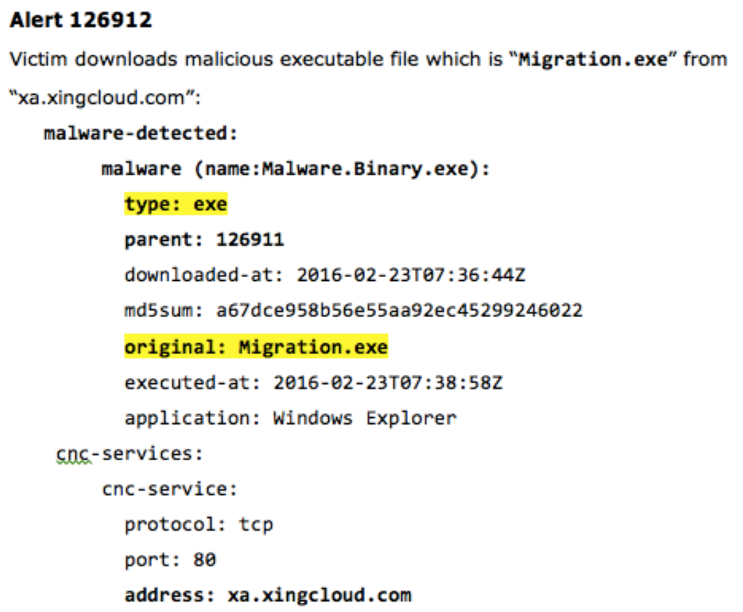
CASE STUDY: DETECTION



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



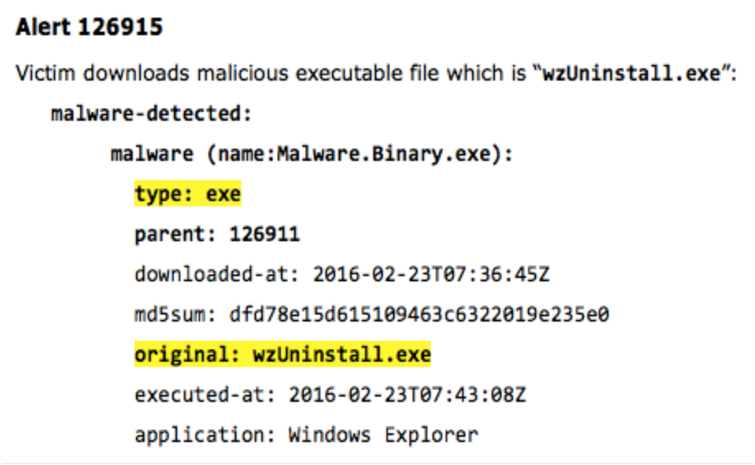
IP Location	United States Dallas David Zhou
ASN	AS36351 SOFTLAYER - SoftLayer Technologies Inc. (registered Dec 12, 2005)
Resolve Host	b.ab.c1ad.ip4.static.sl-reverse.com
Whois Server	whois.arin.net
IP Address	173.193.171.11



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
```



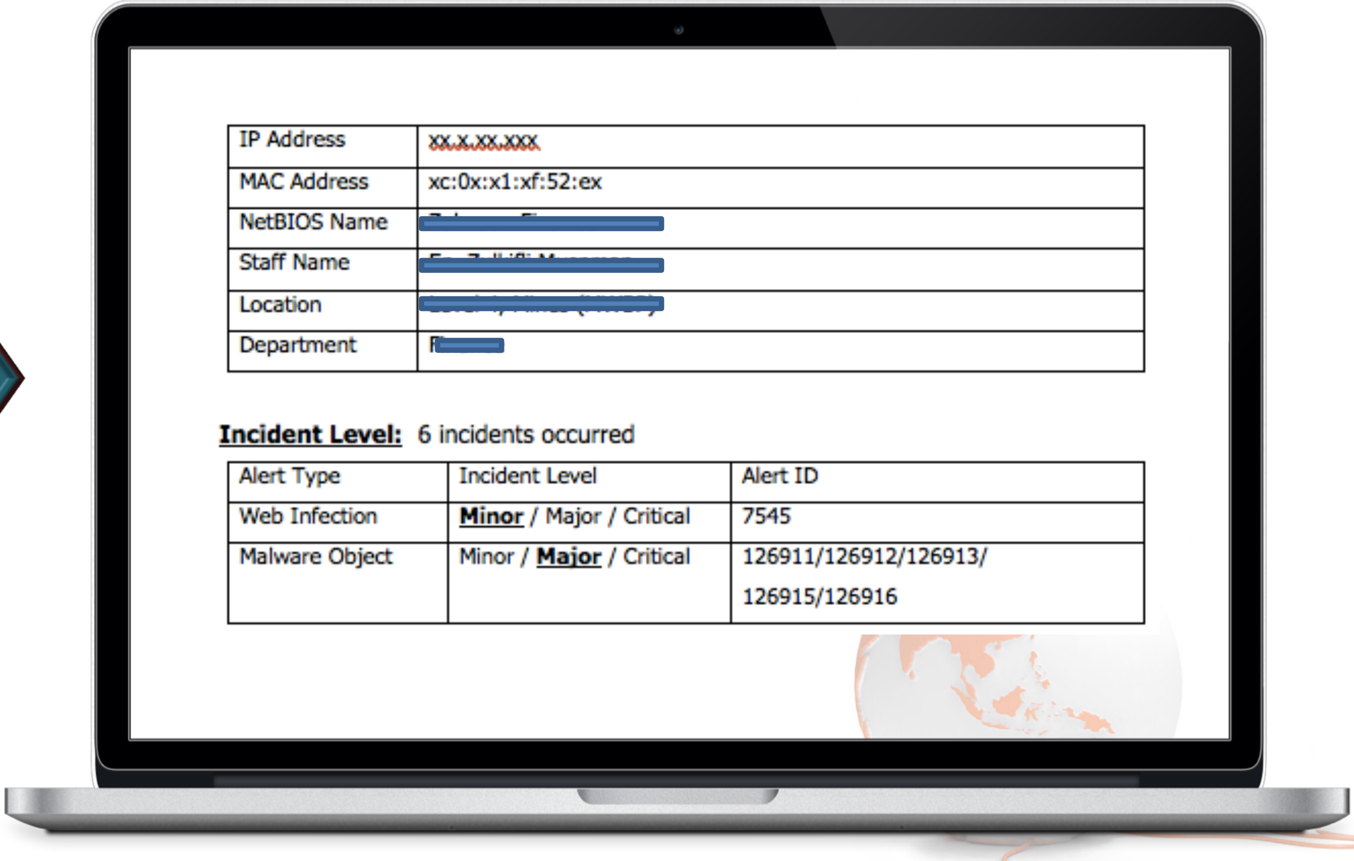
Alert 126915

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



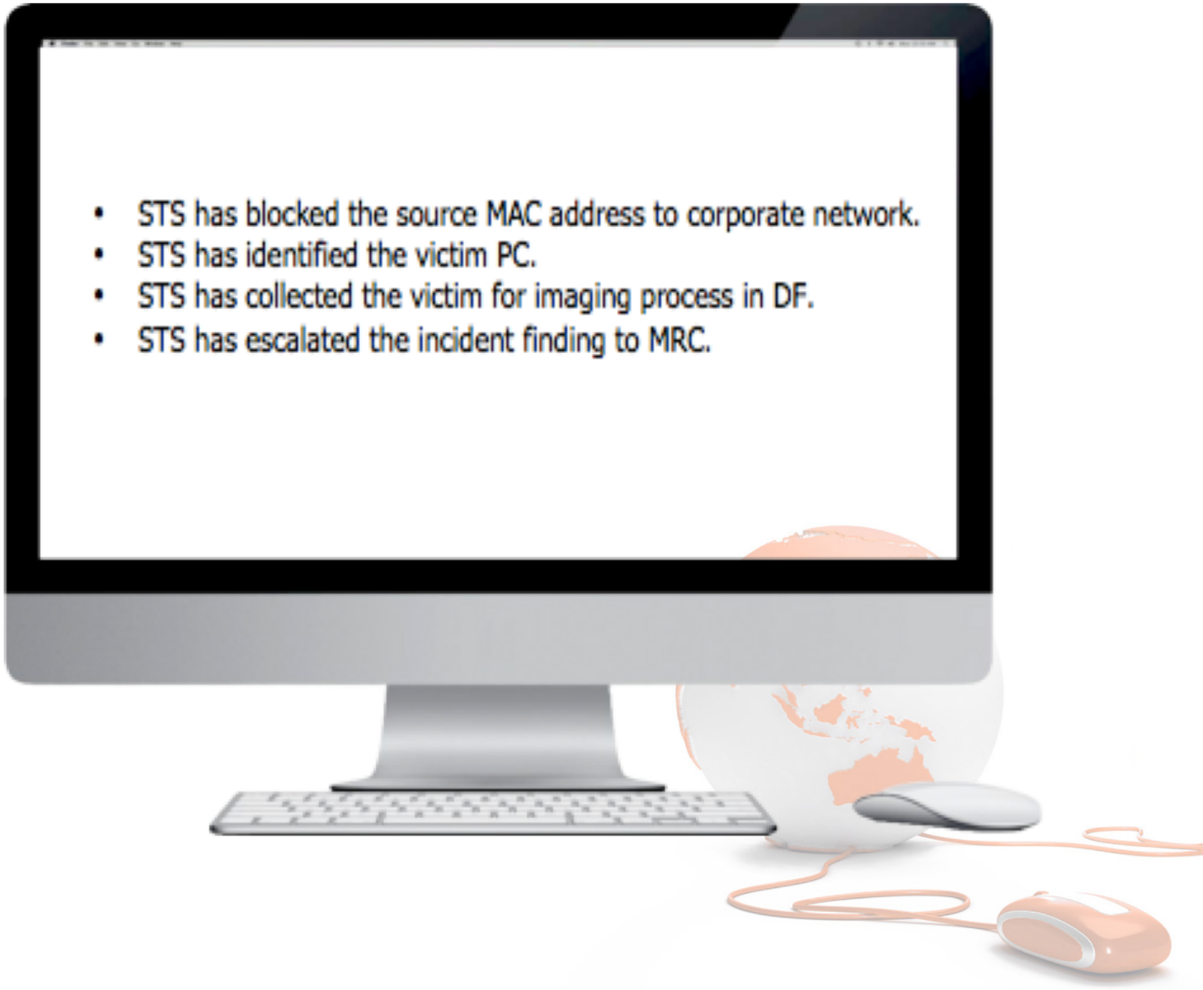
IP Address	xx.x.xx.xxx
MAC Address	xc:0x:x1:xf:52:ex
NetBIOS Name	[redacted]
Staff Name	[redacted]
Location	[redacted]
Department	[redacted]

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

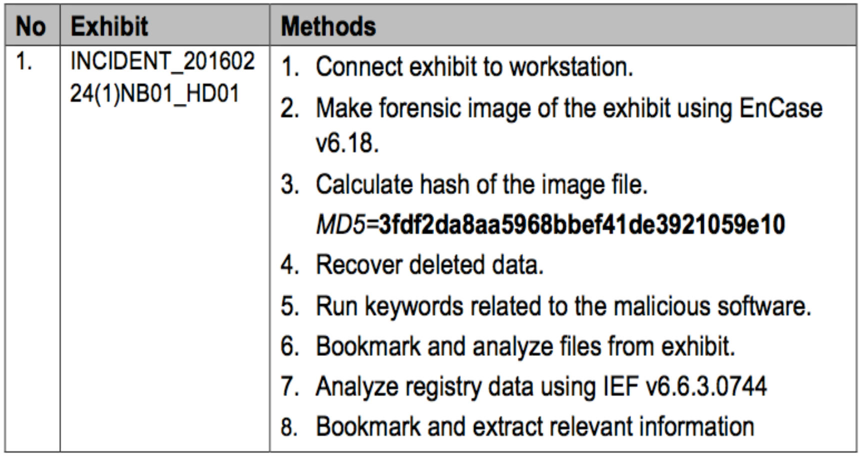


- STS has blocked the source MAC address to corporate network.
- STS has identified the victim PC.
- STS has collected the victim for imaging process in DF.
- STS has escalated the incident finding to MRC.

CASE STUDY: FORENSICS

Analysis

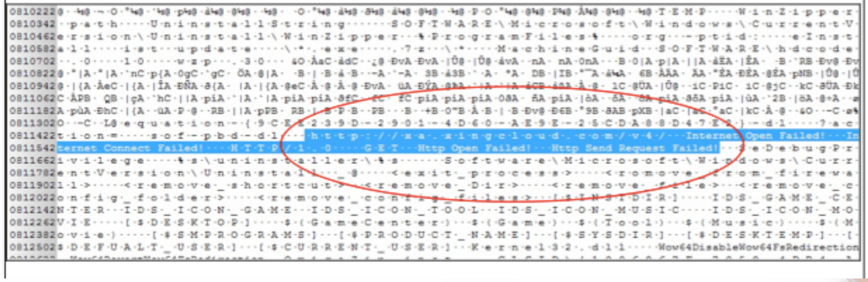
Extract metadata & registry info from malicious file and analyze it using available tools



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:

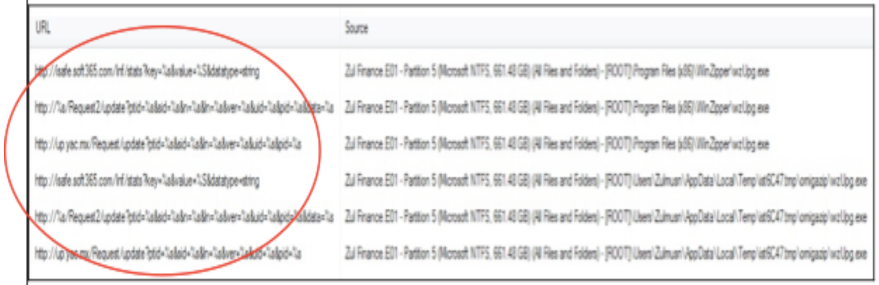


```
0810222@··¼@·¬·O·"¼@·'¼@·p¼@·â¼@·@¼@··¼@··O·"¼@·â¼@·ð¼@·â¼@·@¼@··¼@·P·O·"¼@·@¼@·Þ¼@·Å¼@·@¼@··¼@·T·E·M·P····W·i·n·Z·i·p·p·e·r·
0810342··p·a·t·h····U·n·i·n·s·t·a·l·l·S·t·r·i·n·g······S·O·F·T·W·A·R·E·\·M·i·c·r·o·s·o·f·t·\·W·i·n·d·o·w·s·\·C·u·r·r·e·n·t·V·
0810462e·r·s·i·o·n·\·U·n·i·n·s·t·a·l·l·\·W·i·n·Z·i·p·p·e·r···%·P·r·o·g·r·a·m·F·i·l·e·s·%····o·r·g···–·p·t·i·d·:····e·I·n·s·t·
0810582a·l·l····i·s·t···u·p·d·a·t·e····\·*·.·e·x·e····.·7·z···\·*····M·a·c·h·i·n·e·G·u·i·d···S·O·F·T·W·A·R·E·\·h·d·c·o·d·e·
0810702··.·0·····1·0·····w·z·p···.·3·0···¿O·ÅaC·ådC··¿@·ÐvA·ÐvA·|Û@·|Û@·åvA··nA· nA·0nA···B·0|A·p|A·||A·åÊA·|ÊA· ·B·'RB·Ðv@·Ðv
0810822@·"|A·"|A·'nC·p{A·0gC·'gC· ÖA·@|A· ·B·|·B·å·B··–A·'–A· 3B·å3B·'·A· "A· DB·|IB·"¯A·å¼A· 6B·ÅÅA· ÅA·"ÊA·ÐÊA·@ÊA·pNB·|Û@·|Û
0810942@·|{A·ÅeC·|{A·|ÎA·ÐÑA·ð{A· |A·|{A·@eC·Å·@·Å·@·ÐvA· ùA·ÐÝA·@ÑA··|A··|A·åCB·åûA·Å·@· 1C·@ÜA·|Û@··1C·P1C· 1C·@jC··kC·ðÜA·Ðk
0811062C·ÅPB· QB·|çA·'hC·||A·piA·'|A·'|A·piA·piA·ðfC··fC· fC·piA·piA·piA·0ðA· ñA·piA·|òA··õA··õA·piA·ðõA·piA·|ùA·'2B·|õA·@+A··ø
0811182A·pùA·ÐhC·|{A··ûA·P·@··RB·||A·pPB· RB·|·B·P·B··PB···B··+B·0"B·Å·B·|·B·Ðv@·Ð6B·"9B·ðAB·pXB·|aC·|aC·"aC·|kC·Å·@··¿O··–C·ø¼
0811302O··–C··L@·e·q·u·a·t·i·o·n·–·{·9·C·E·E·2·3·9·D·–·2·9·0·1·–·4·D·6·0·–·A·E·9·E·–·2·5·C·D·A·8·8·D·4·7·E·2·}·–·d·l····?·a·c·
0811422t·i·o·n·=·····s·o·f·–·p·b·d·–·d·l····h·t·t·p·:·/·/·x·a·.·x·i·n·g·c·l·o·u·d·.·c·o·m·/·v·4·/···Internet Open Failed!···In
0811542ternet Connect Failed!···H·T·T·P·/·1·.·0·····G·E·T···Http Open Failed!···Http Send Request Failed!···S·e·D·e·b·u·g·P·r·
0811662i·v·i·l·e·g·e·····%·s·\·u·n·i·n·s·t·a·l·l·e·r·\·%·s······S·o·f·t·w·a·r·e·\·M·i·c·r·o·s·o·f·t·\·W·i·n·d·o·w·s·\·C·u·r·r·
0811782e·n·t·V·e·r·s·i·o·n·\·U·n·i·n·s·t·a·l·l···_·@····<·e·x·i·t·_·p·r·o·c·e·s·s·>·····<·r·o·m·o·v·e·_·f·r·o·m·_·f·i·r·e·w·a·
0811902l·l·>·····<·r·e·m·o·v·e·_·s·h·o·r·t·c·u·t·>···<·r·e·m·o·v·e·_·D·i·r·>·····<·r·e·m·o·v·e·_·f·i·l·e·>···<·r·e·m·o·v·e·_·c·
0812022o·n·f·i·g·_·f·o·l·d·e·r·>·····<·r·e·m·o·v·e·_·c·o·n·f·i·g·_·f·i·l·e·s·>···[·$·I·N·S·T·D·I·R·]·····I·D·S·_·G·A·M·E·_·C·E·
0812142N·T·E·R···I·D·S·_·I·C·O·N·_·G·A·M·E···I·D·S·_·I·C·O·N·_·T·O·O·L···I·D·S·_·I·C·O·N·_·M·U·S·I·C·····I·D·S·_·I·C·O·N·_·M·O·
0812262V·I·E·····[·$·D·E·S·K·T·O·P·]·····$·(·G·a·m·e·C·e·n·t·e·r·)···$·(·T·o·o·l·)···$·(·M·u·s·i·c·)·····$·(·M·
0812382o·v·i·e·)·····[·$·S·M·P·R·O·G·R·A·M·S·]···[·$·P·R·O·D·U·C·T·_·N·A·M·E·]···[·$·S·Y·S·D·I·R·]···[·$·D·E·S·K·T·E·M·P·]···[·
0812502$·D·E·F·U·A·L·T·_·U·S·E·R·]···[·$·C·U·R·R·E·N·T·_·U·S·E·R·]···K·e·r·n·e·l·3·2·.·d·l·l·····Wow64DisableWow64FsRedirection
```

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:

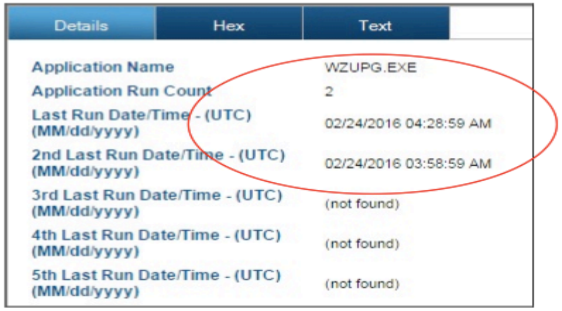


URL	Source
http://safe.soft365.com/inf/stats?key=%s&value=%S&datatype=string	Zul Finance.E01 - Partition 5 (Microsoft NTFS, 661.43 GB) (All Files and Folders) - [ROOT]\Program Files (x86)\WinZipper\wzUpg.exe
http://%s/Request2/update?ptid=%s&sid=%s&ln=%s&lh=%s&ver=%s&uid=%s&pid=%s&data=%s	Zul Finance.E01 - Partition 5 (Microsoft NTFS, 661.43 GB) (All Files and Folders) - [ROOT]\Program Files (x86)\WinZipper\wzUpg.exe
http://up.yac.mx/Request/update?ptid=%s&sid=%s&ln=%s&ver=%s&uid=%s&pid=%s	Zul Finance.E01 - Partition 5 (Microsoft NTFS, 661.43 GB) (All Files and Folders) - [ROOT]\Program Files (x86)\WinZipper\wzUpg.exe
http://safe.soft365.com/inf/stats?key=%s&value=%S&datatype=string	Zul Finance.E01 - Partition 5 (Microsoft NTFS, 661.43 GB) (All Files and Folders) - [ROOT]\Users\Zulmuri\AppData\Local\Temp\is6C47.tmp\omigazip\wzUpg.exe
http://%s/Request2/update?ptid=%s&sid=%s&ln=%s&lh=%s&ver=%s&uid=%s&pid=%s&data=%s	Zul Finance.E01 - Partition 5 (Microsoft NTFS, 661.43 GB) (All Files and Folders) - [ROOT]\Users\Zulmuri\AppData\Local\Temp\is6C47.tmp\omigazip\wzUpg.exe
http://up.yac.mx/Request/update?ptid=%s&sid=%s&ln=%s&ver=%s&uid=%s&pid=%s	Zul Finance.E01 - Partition 5 (Microsoft NTFS, 661.43 GB) (All Files and Folders) - [ROOT]\Users\Zulmuri\AppData\Local\Temp\is6C47.tmp\omigazip\wzUpg.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)



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
- If we can predict attacks, we can be well prepared and provided early alerts to computer users

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

CyberSecurity MALAYSIA

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

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

Best Brand Internet Security 2008 & 2009

CERTIFIED TO ISO/IEC 27001:2013
CERT. NO. : AR 4656

MS ISO/IEC 17025 TESTING
SAMM NO. 456
(MySEF LABORATORY)

MSC MALAYSIA Status Company

Best Child Online Protection Website