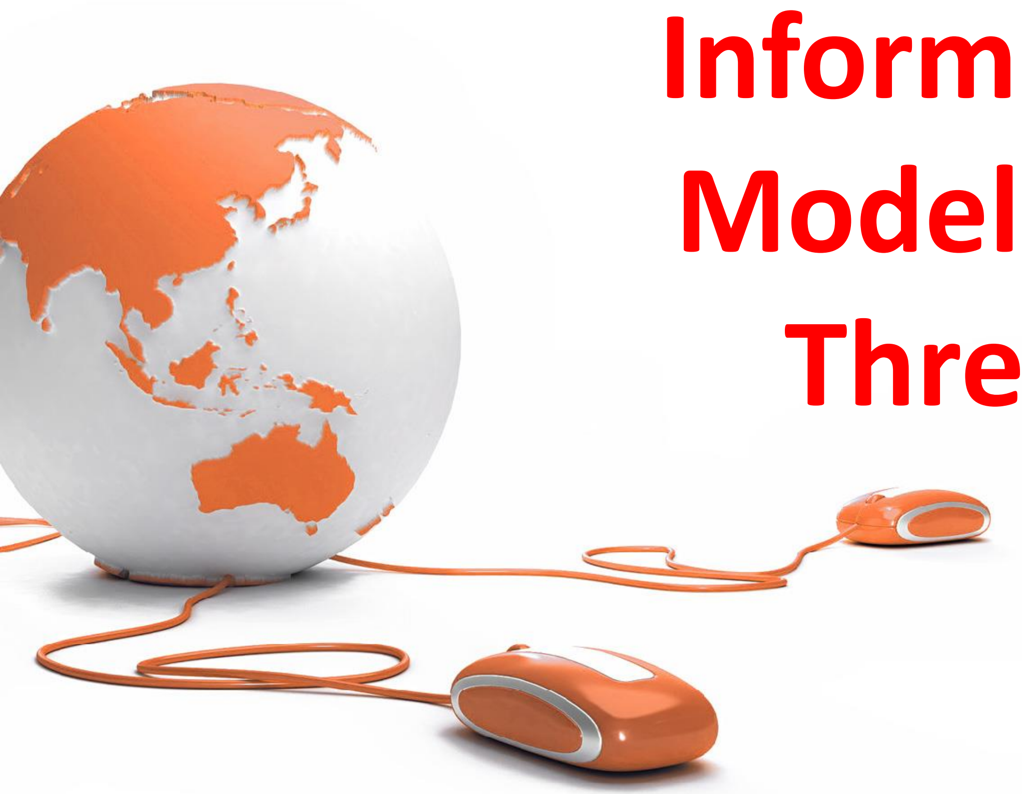
KEMENTERIAN SAINS, TEKNOLOGI DAN INOVASI
MINISTRY OF SCIENCE, TECHNOLOGY AND INNOVATION

CyberSecurity
MALAYSIA
An agency under MOSTI

CyberDEF

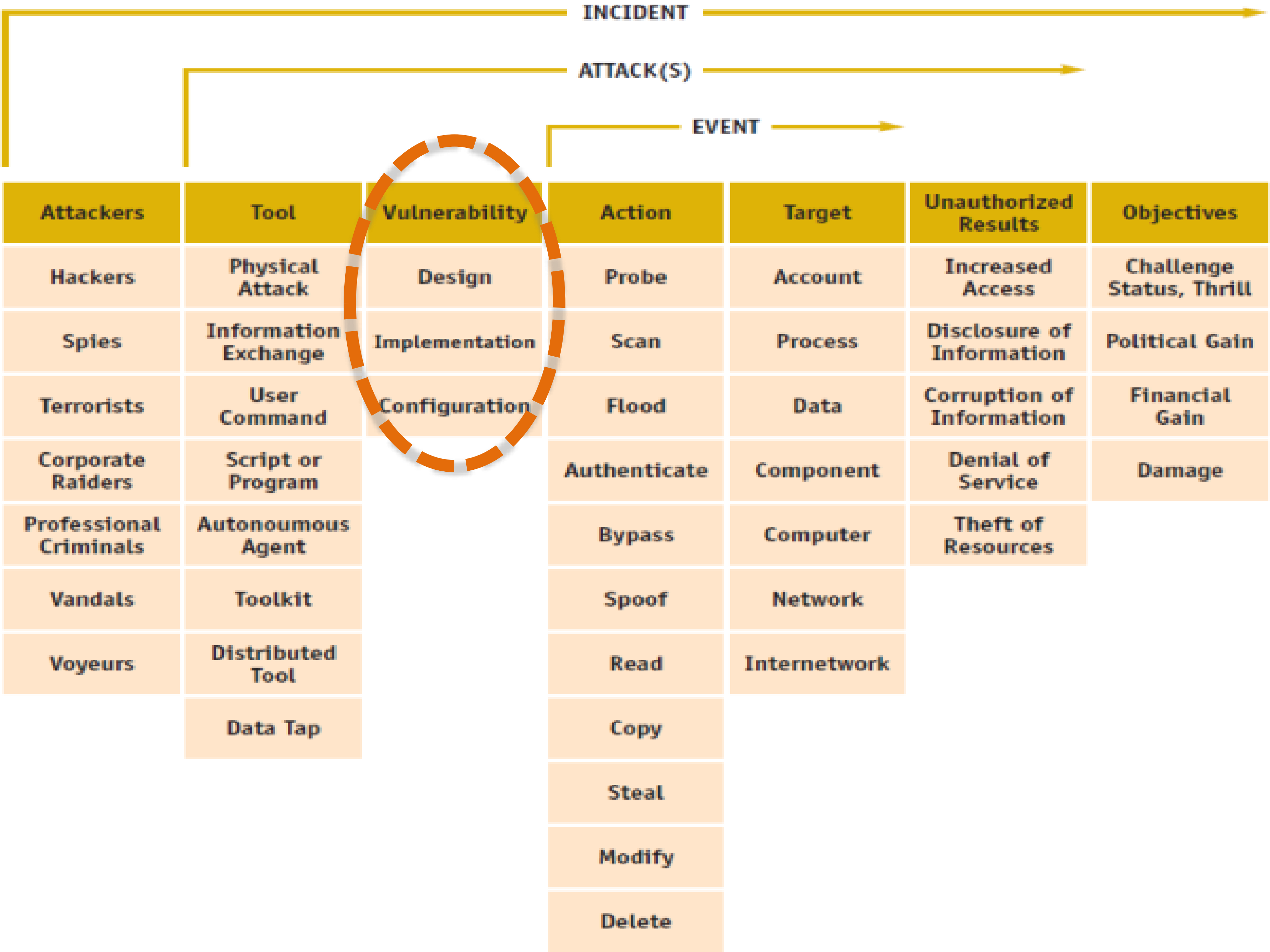
Collaborative Information Sharing Model for Malware Threat Analysis



DrAA (Dr Aswami Ariffin)
SVP & Digital Forensics Scientist
Cyber Security Responsive Services
CyberSecurity Malaysia
aswami@cybersecurity.my

Agenda

1. Current problem
2. Malware Mitigation Working Group and CyberDEF Intelligent System – CDIS
3. Findings



INCIDENT

ATTACK(S)

EVENT

Attackers	Tool	Vulnerability	Action	Target	Unauthorized Results	Objectives
Hackers	Physical Attack	Design	Probe	Account	Increased Access	Challenge Status, Thrill
Spies	Information Exchange	Implementation	Scan	Process	Disclosure of Information	Political Gain
Terrorists	User Command	Configuration	Flood	Data	Corruption of Information	Financial Gain
Corporate Raiders	Script or Program		Authenticate	Component	Denial of Service	Damage
Professional Criminals	Autonomous Agent		Bypass	Computer	Theft of Resources	
Vandals	Toolkit		Spoof	Network		
Voyeurs	Distributed Tool		Read	Internetwork		
	Data Tap		Copy			
			Steal			
			Modify			
			Delete			

National Cyber Security Policy (NCSP)

CyberSecurity MALAYSIA
An agency under MOSTI

Thrust 1:
Effective Governance

Thrust 2:
Legislative & Regulatory Framework

Thrust 3:
Cyber Security Technology Framework

Thrust 4:
Culture of Security & Capacity Building

Vision:

"Malaysia's CNII 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 (CNII)

Thrust 5:
R&D Towards Self Reliance

Thrust 6:
Compliance & Enforcement

Thrust 7:
Cyber Security Emergency Readiness

Thrust 8:
International Cooperation

Malware mitigation WG

Malaysia would like to initiate

Honeynet / Lebahnet

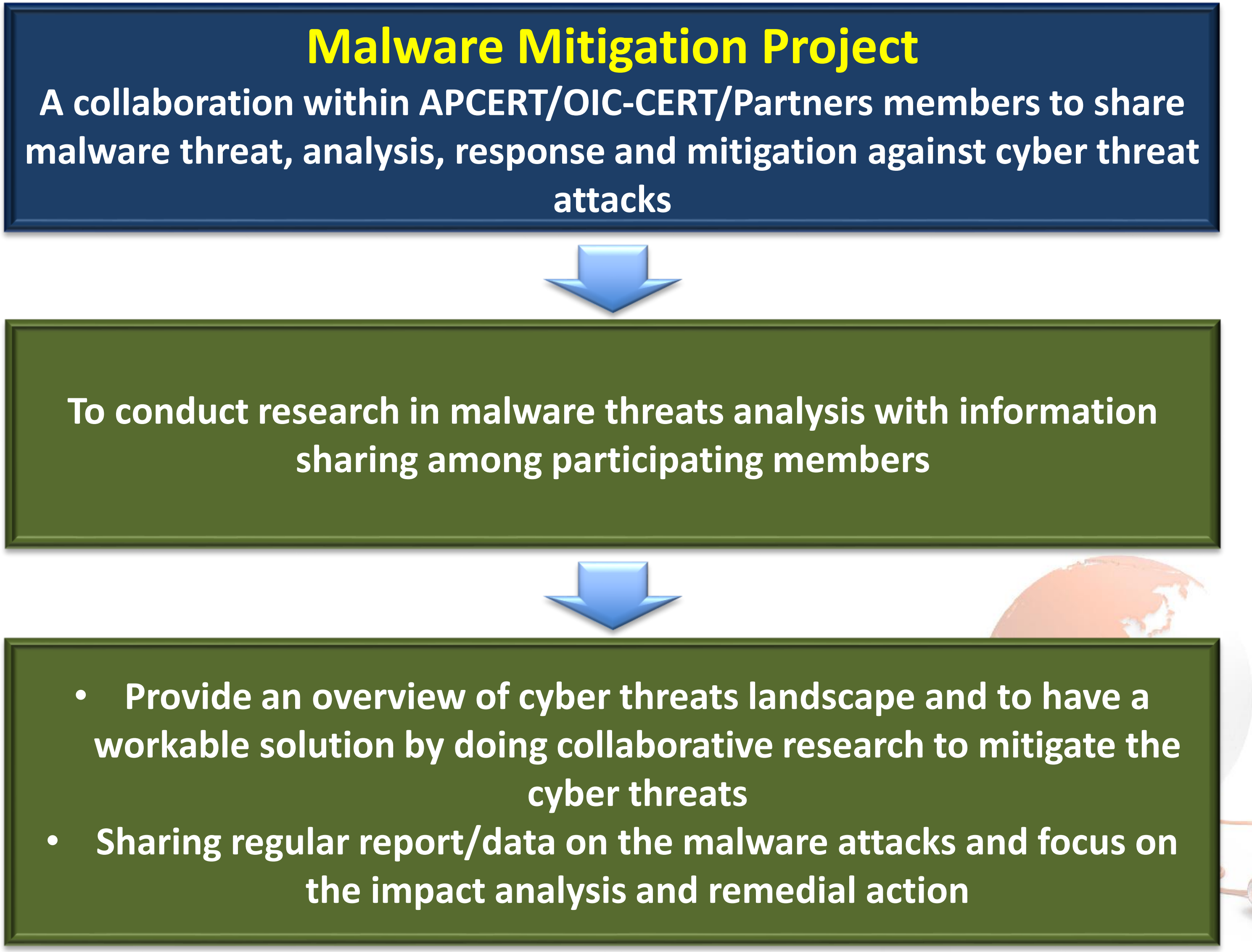
LebahNET.MY
CyberSecurity Malaysia Honeynet Project

POWERED BY MyCERT
Malaysia Computer Emergency Response Team

under

Malware Mitigation Working Group

The project



Malware Mitigation Project

A collaboration within APCERT/OIC-CERT/Partners members to share malware threat, analysis, response and mitigation against cyber threat attacks

To conduct research in malware threats analysis with information sharing among participating members

- Provide an overview of cyber threats landscape and to have a workable solution by doing collaborative research to mitigate the cyber threats
- Sharing regular report/data on the malware attacks and focus on the impact analysis and remedial action

Project plan

Phase I

- Data Collection / Repository

Phase II

- Data Analysis & Sharing

Phase III

- Malware Mitigation

Commitment from participating members

LOCATION

Determine the location to install/host the honeypot sensor

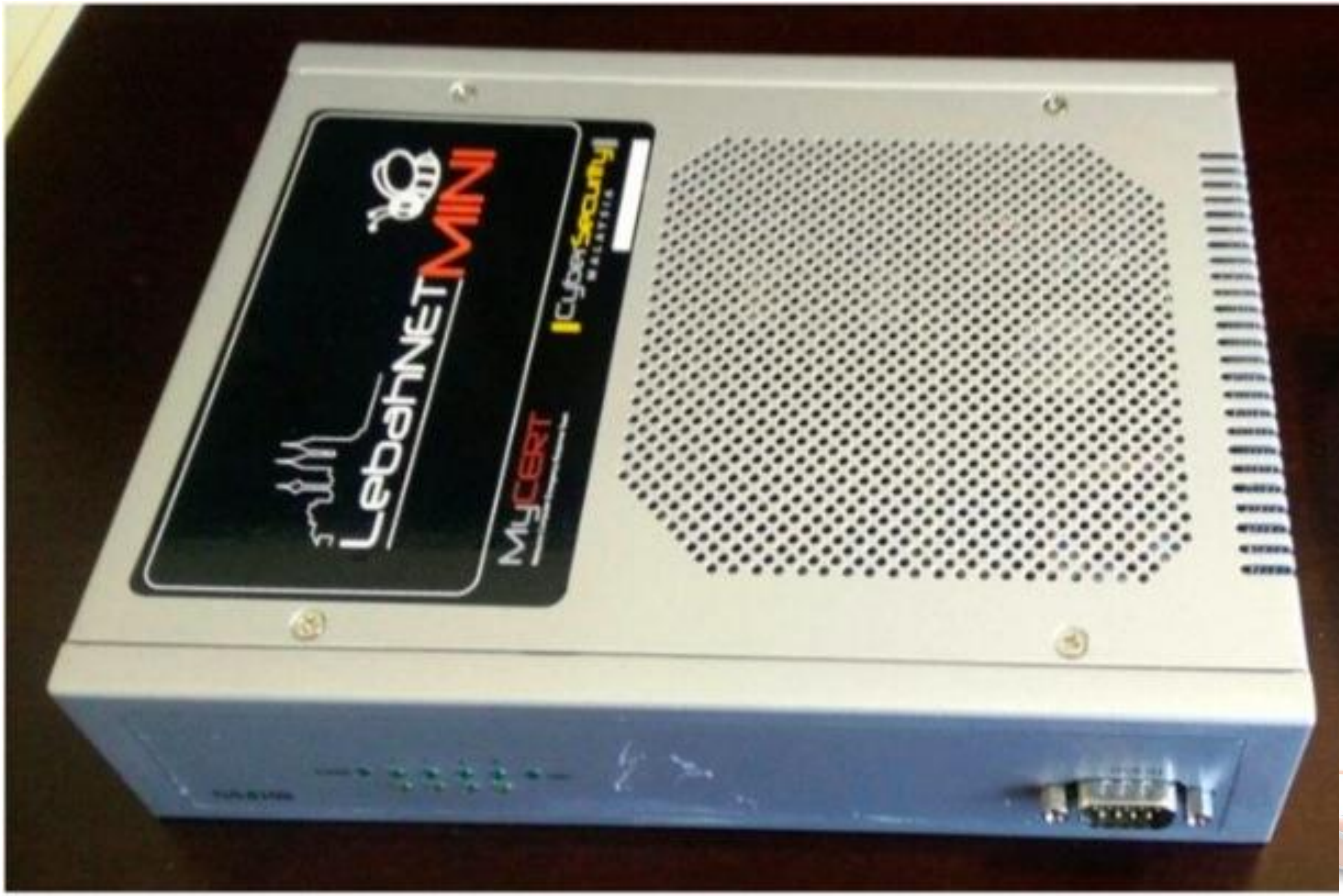
LOCAL TECHNICAL

Provide the local technical support

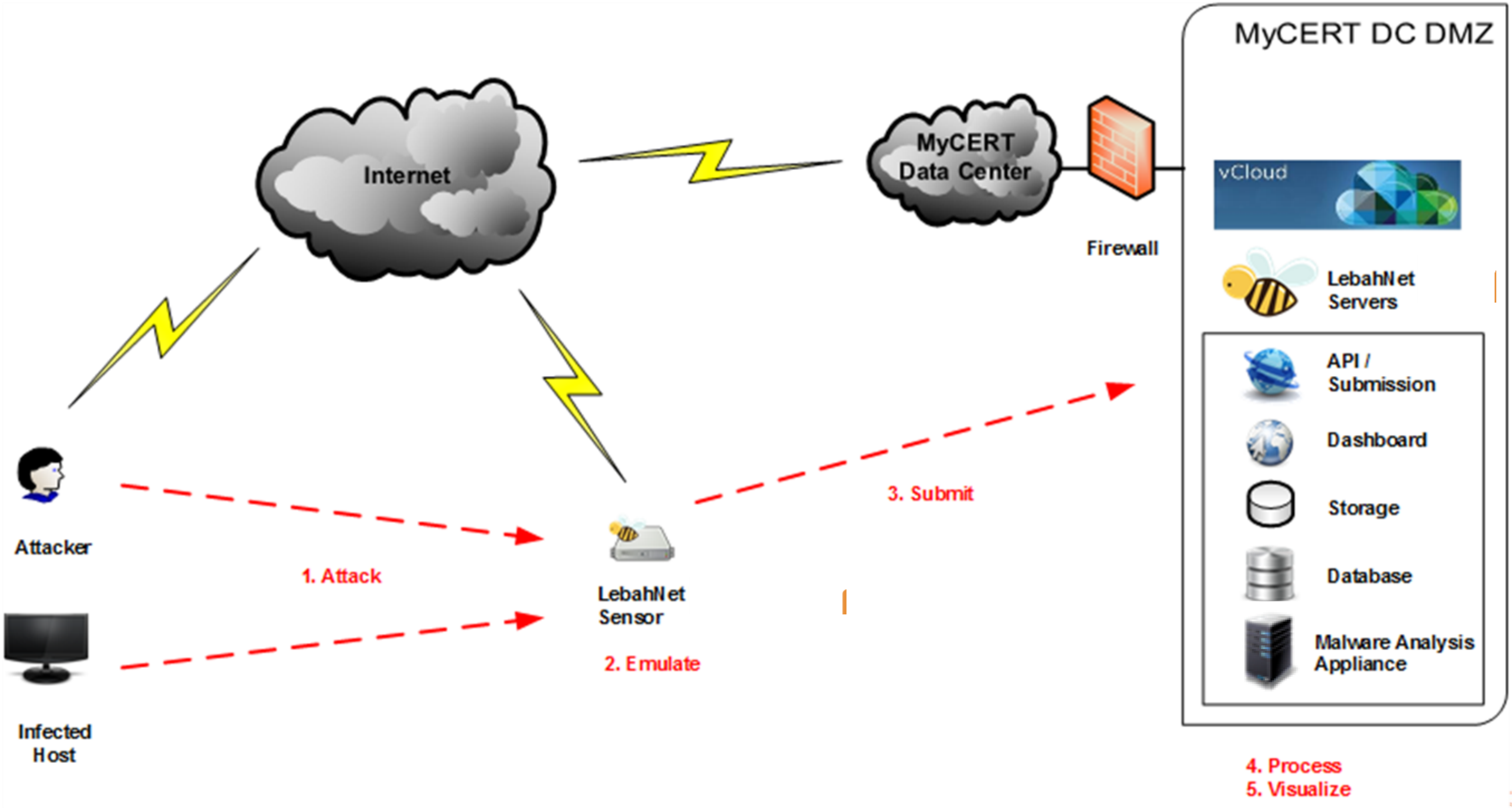
SHARE REPORT

Share reports and findings related to the project

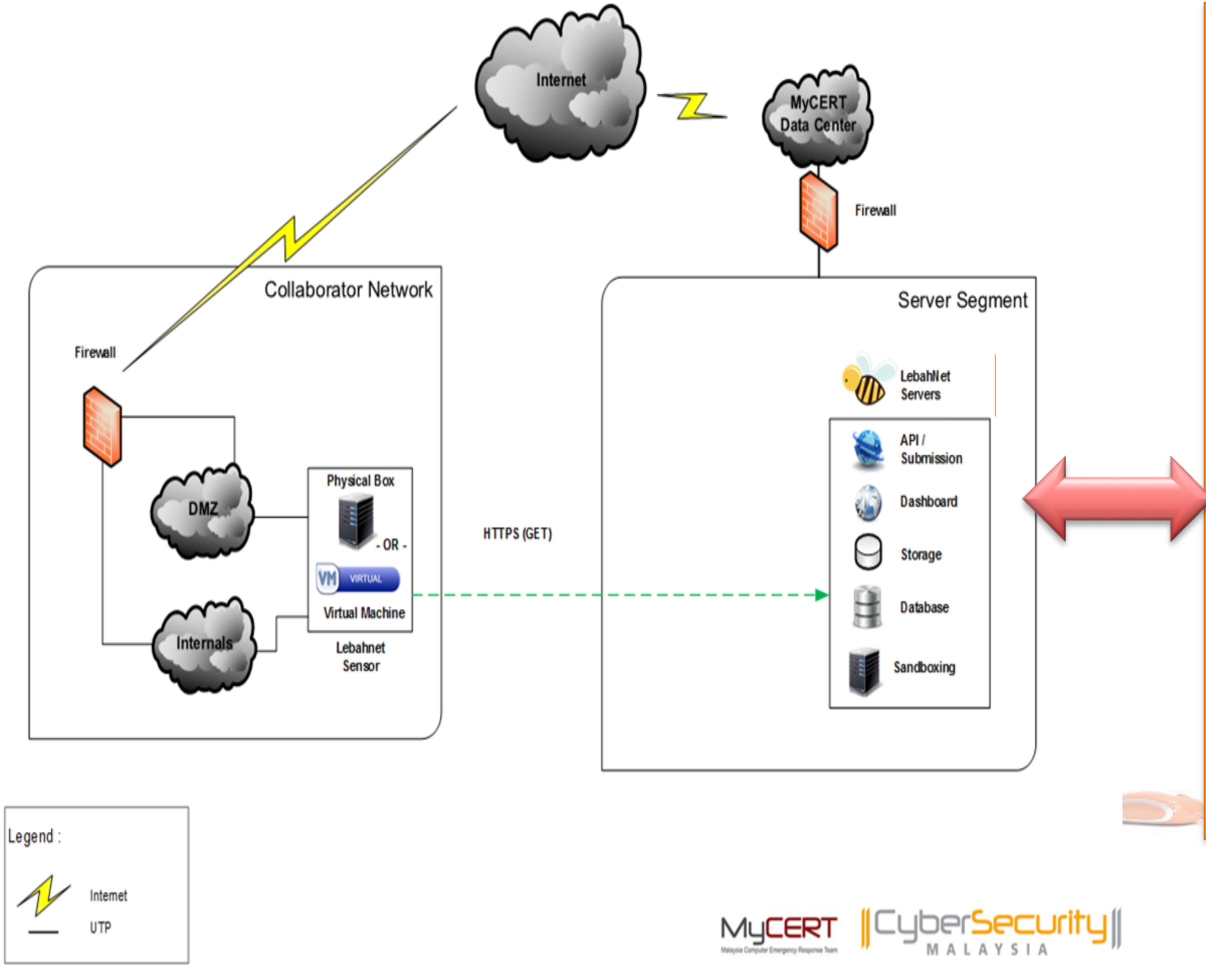
LebahNet sensor



LebahNet process flow



Architecture and participation



Regional Participant/Member

APCERT/OIC-CERT MEMBER Sensor Deployment

DATA from LebahNet

TYPE OF INFORMATION THAT WILL BE CAPTURED BY LEBAHNET SENSORS

Malware

Remote access login attempt (SSH, Telnet, etc.)

Web application attack (SQLi, RFI, LFI, etc.)

Important Note: Sensors will not capture sensitive information from the organization network (passive mode)

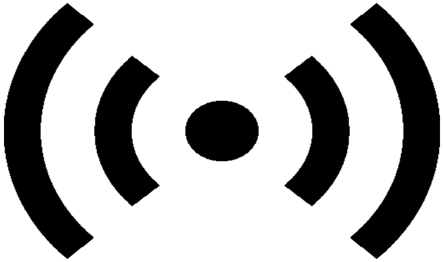
LebahNet requirements

MONITORING

For monitoring threats from the **Public / Internet**, the sensor will require public IP (or mapped from public IP) with allow ANY incoming ports configure from Firewall.

For monitoring threats from the **Internal (LAN / VLAN / Secured),** the sensor will require internal IP related to the segment being monitored with allow ANY incoming ports configure from Firewall.

SENSOR



The sensor will be prepared in **two (2) forms**, a Physical box and a Virtual Machine. Participant can choose either form suite to their environment.

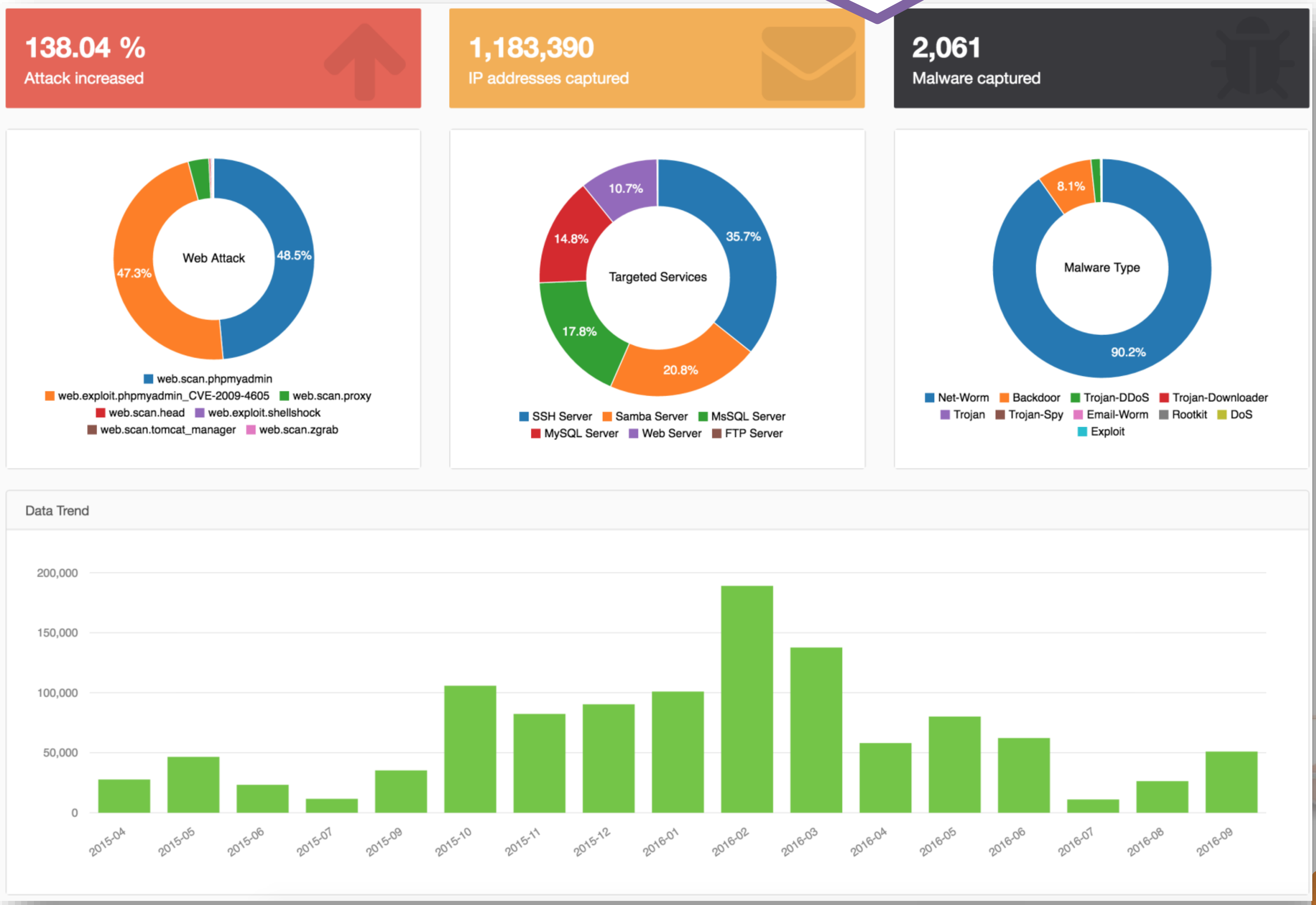
USER / PARTICIPATION

Participant have to **allow information sending through secured protocol (HTTPS 443/TCP)** over the Internet between the sensor and MyCERT centralized server (api.honeynet.org.my).

User/Participant will have access to their **dedicated Dashboard** that require access credential.

User dashboard: LebahNet user interface

Participant will view information according to their sensors deployed

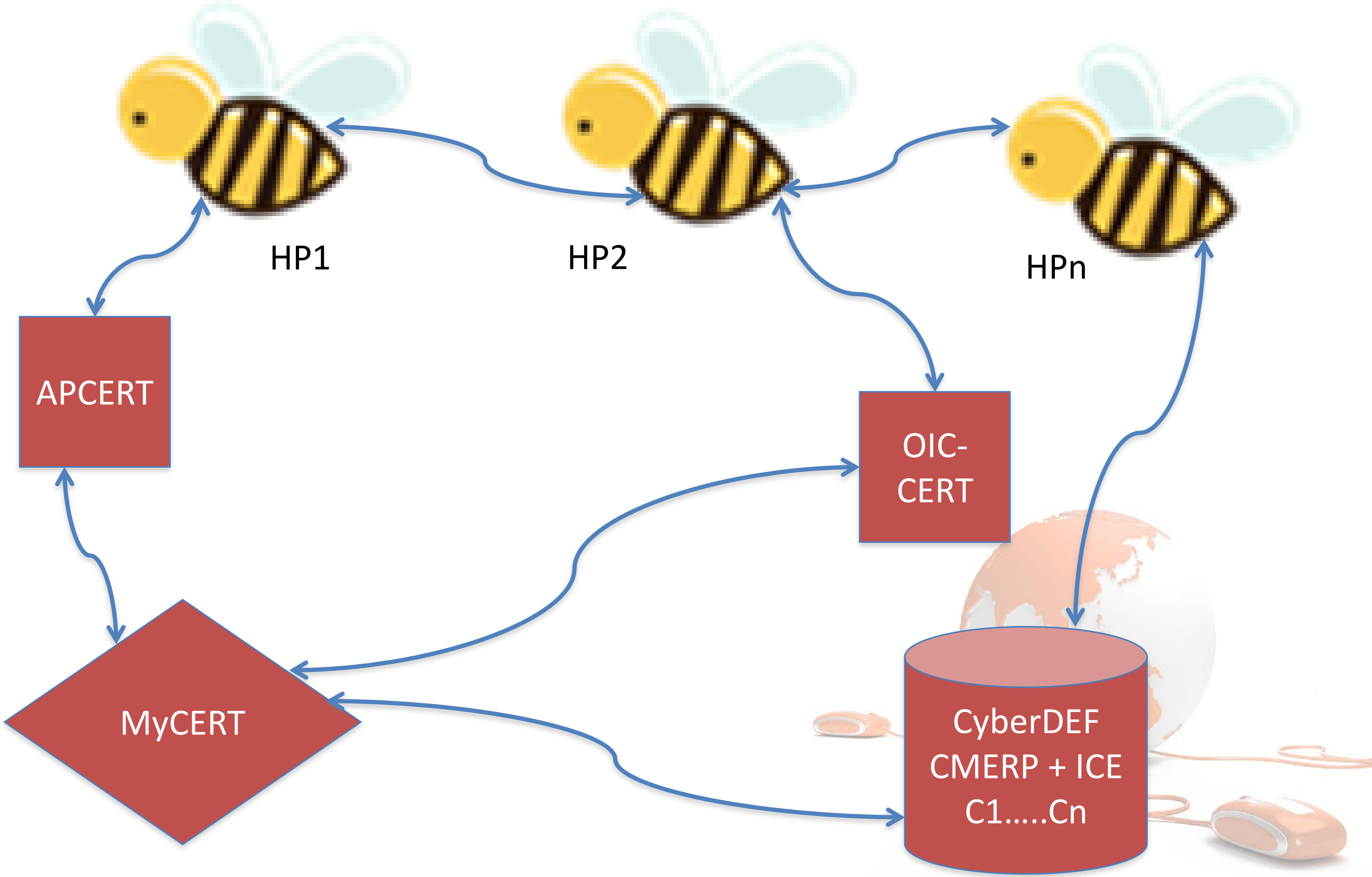


138.04 %
Attack increased

1,183,390
IP addresses captured

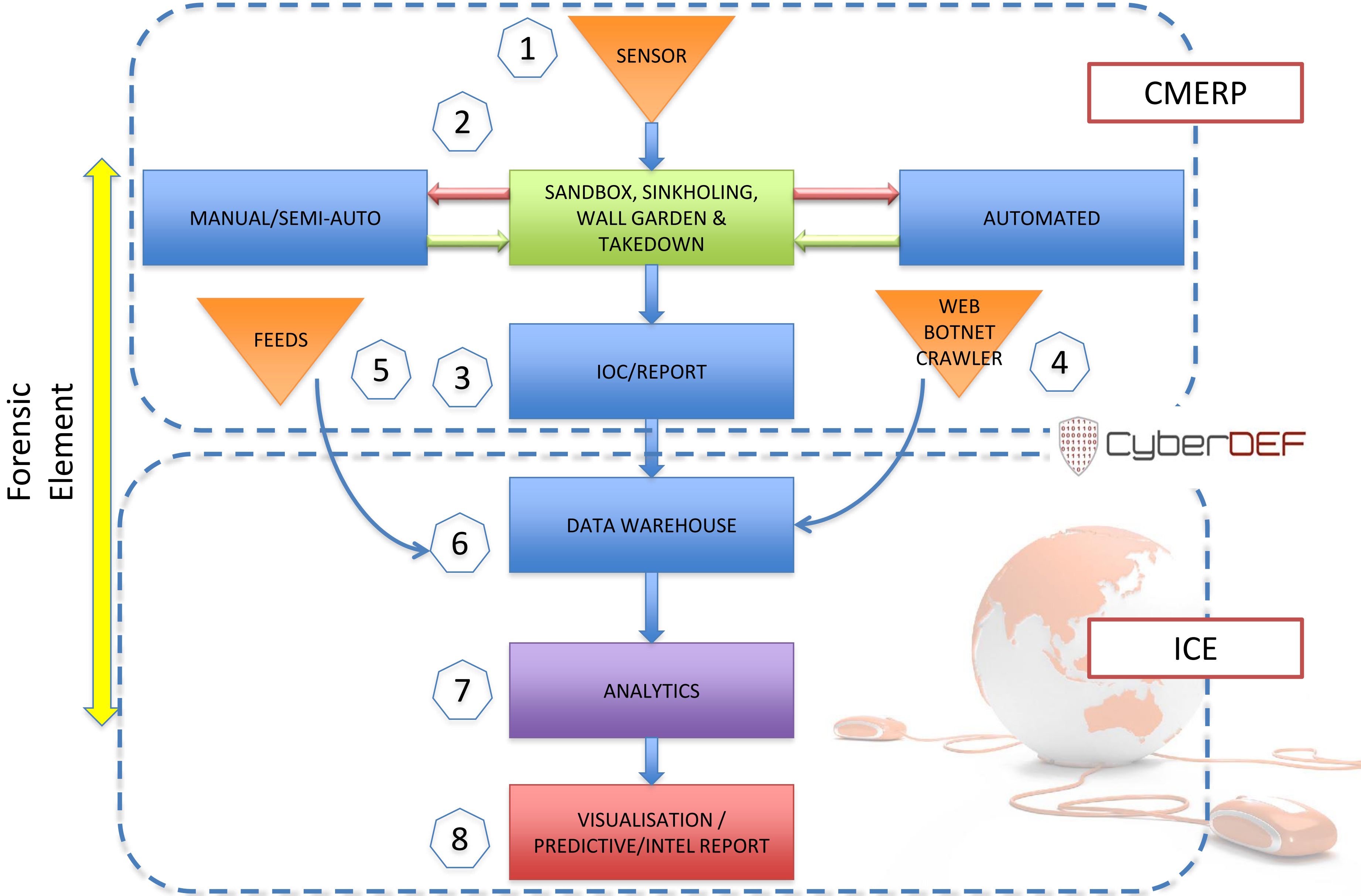
2,061
Malware captured

Collaborative Model

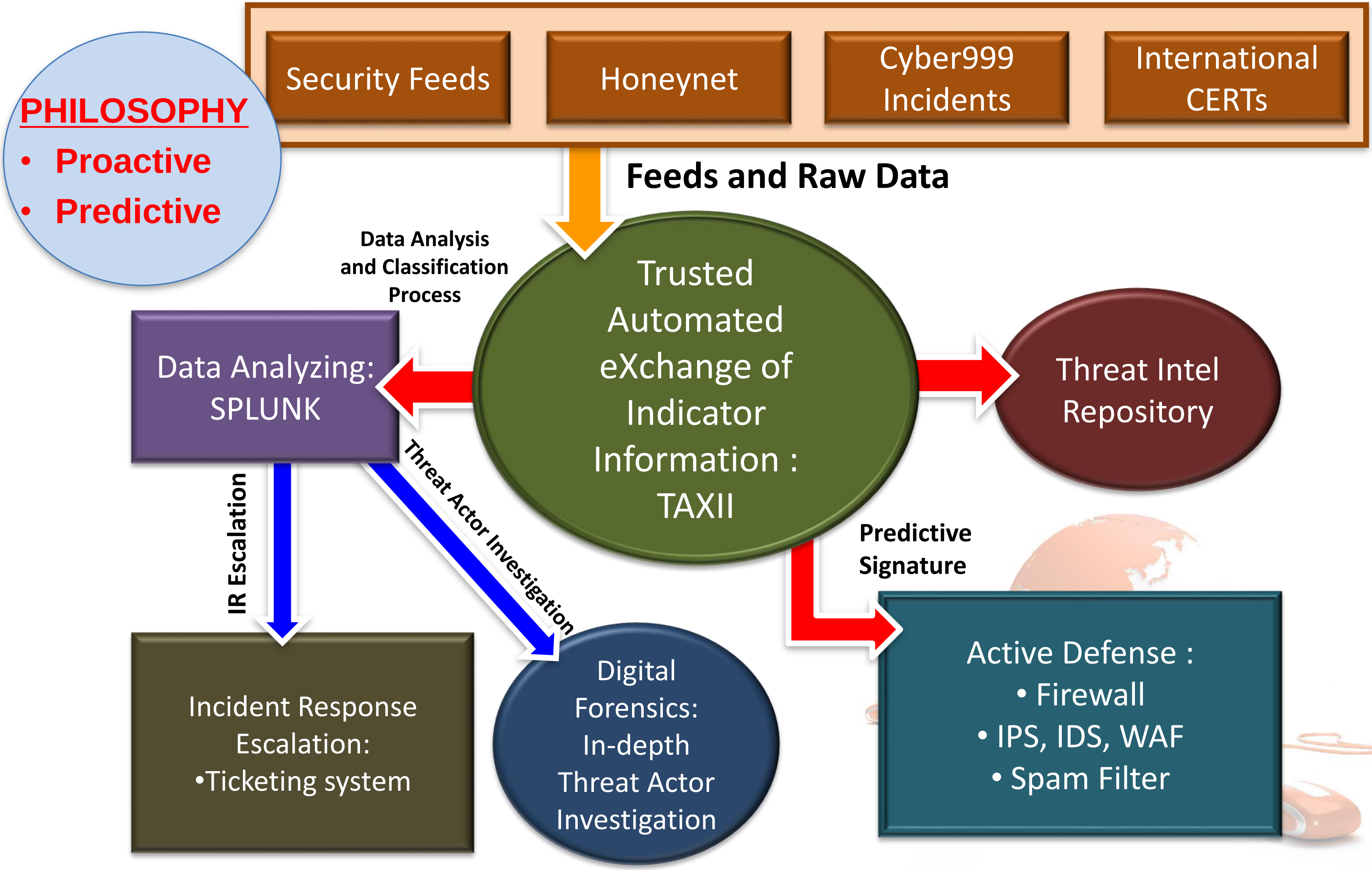


CyberDEF Intelligent System - CDIS

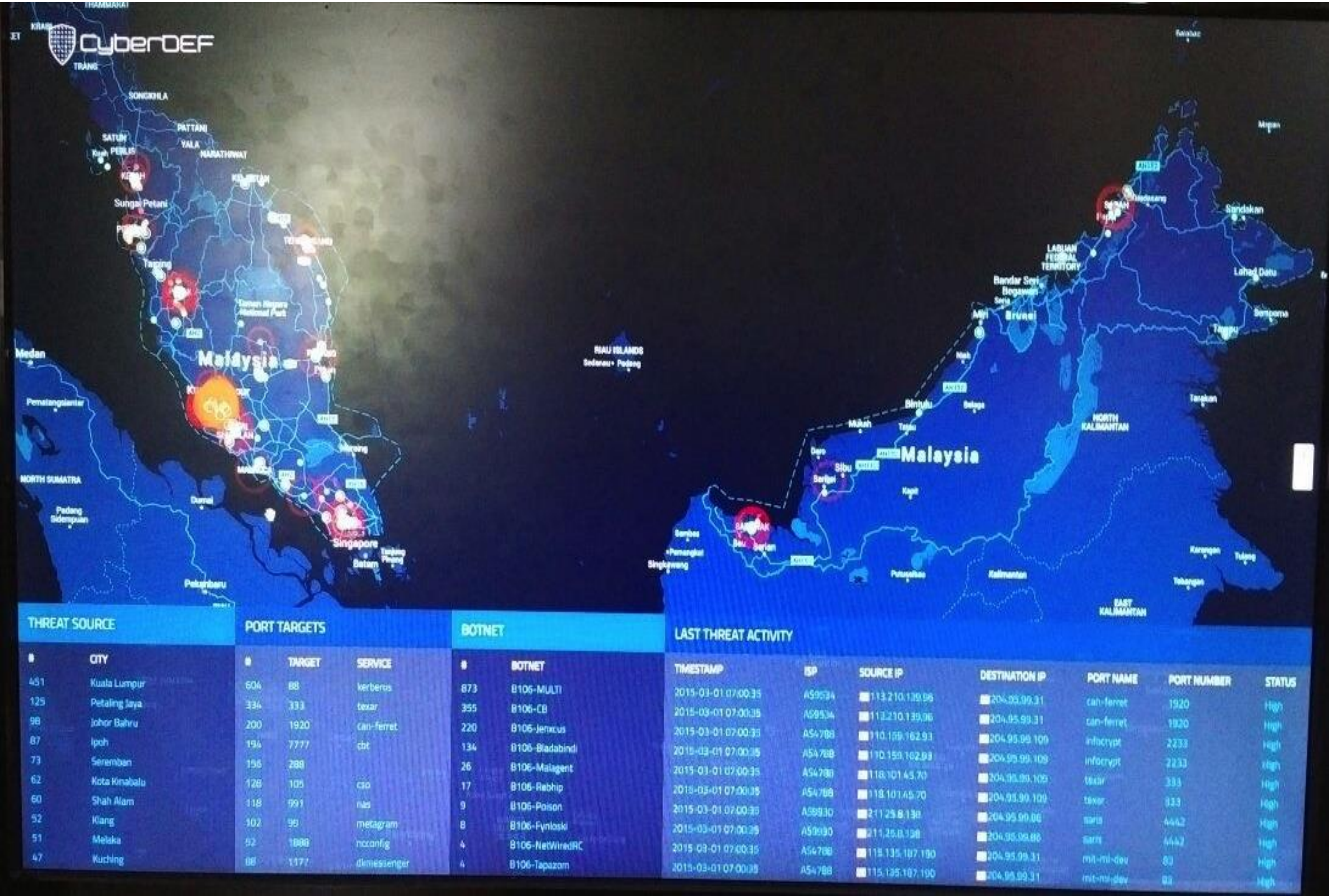
CyberSecurity MALAYSIA
An agency under MOSTI



SOC operation V2.0 - SIC



Botnet infection heat map



THREAT SOURCE

#	CITY
451	Kuala Lumpur
125	Petaling Jaya
98	Johor Bahru
87	Ipoh
73	Seremban
62	Kota Kinabalu
60	Shah Alam
52	Klang
51	Melaka
47	Kuching

PORT TARGETS

#	TARGET	SERVICE
604	88	kerberos
334	333	texar
200	1920	can-ferret
194	7777	cbt
156	288	
128	105	cso
118	991	nas
102	99	metagram
92	1888	ncconfig
88	1177	dkmessenger

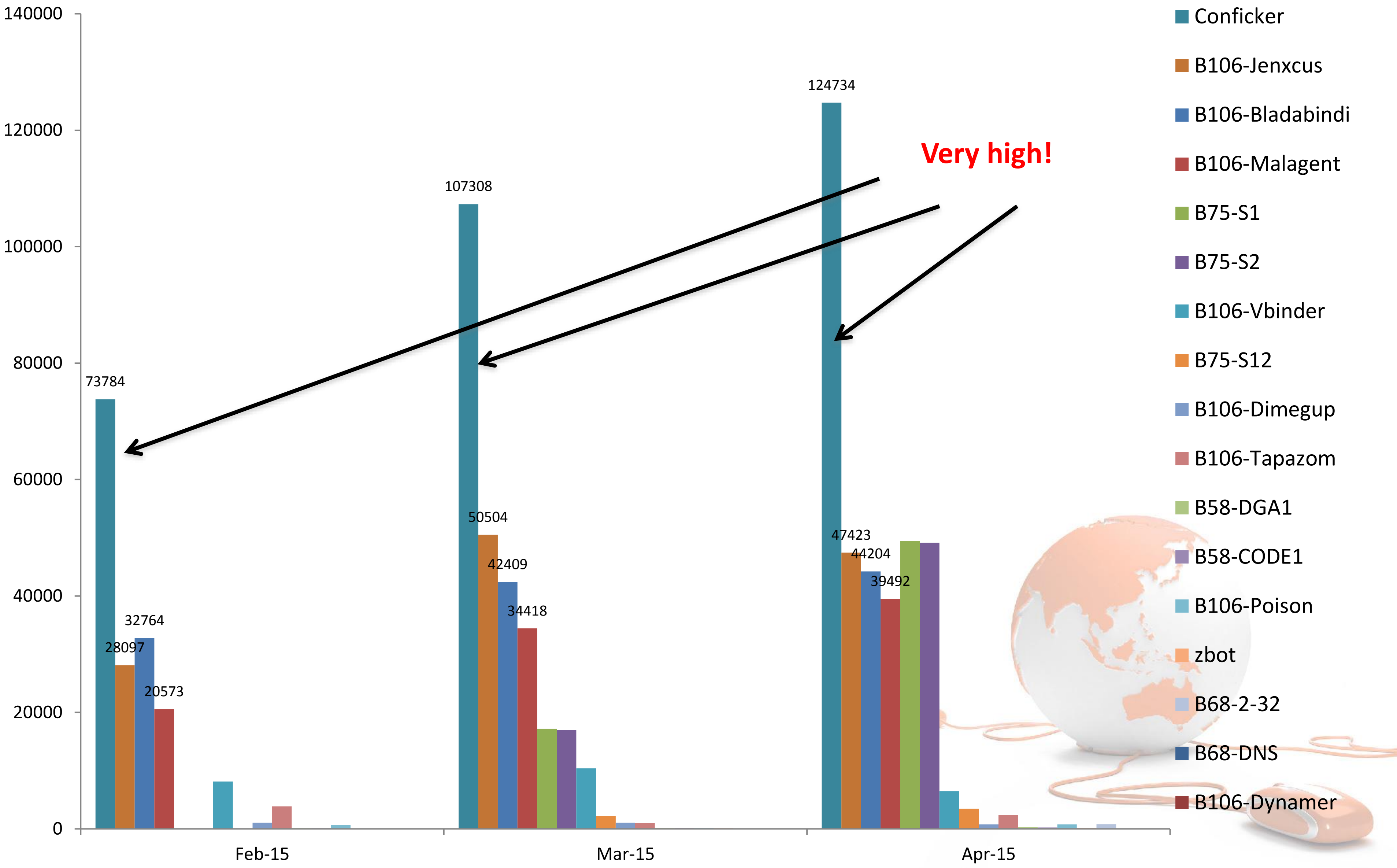
BOTNET

#	BOTNET
873	B106-MULTI
355	B106-CB
220	B106-Jenxcus
134	B106-Bladabindi
26	B106-Malagent
17	B106-Rebhip
9	B106-Poison
8	B106-Fynloski
4	B106-NetWiredRC
4	B106-Tapazom

LAST THREAT ACTIVITY

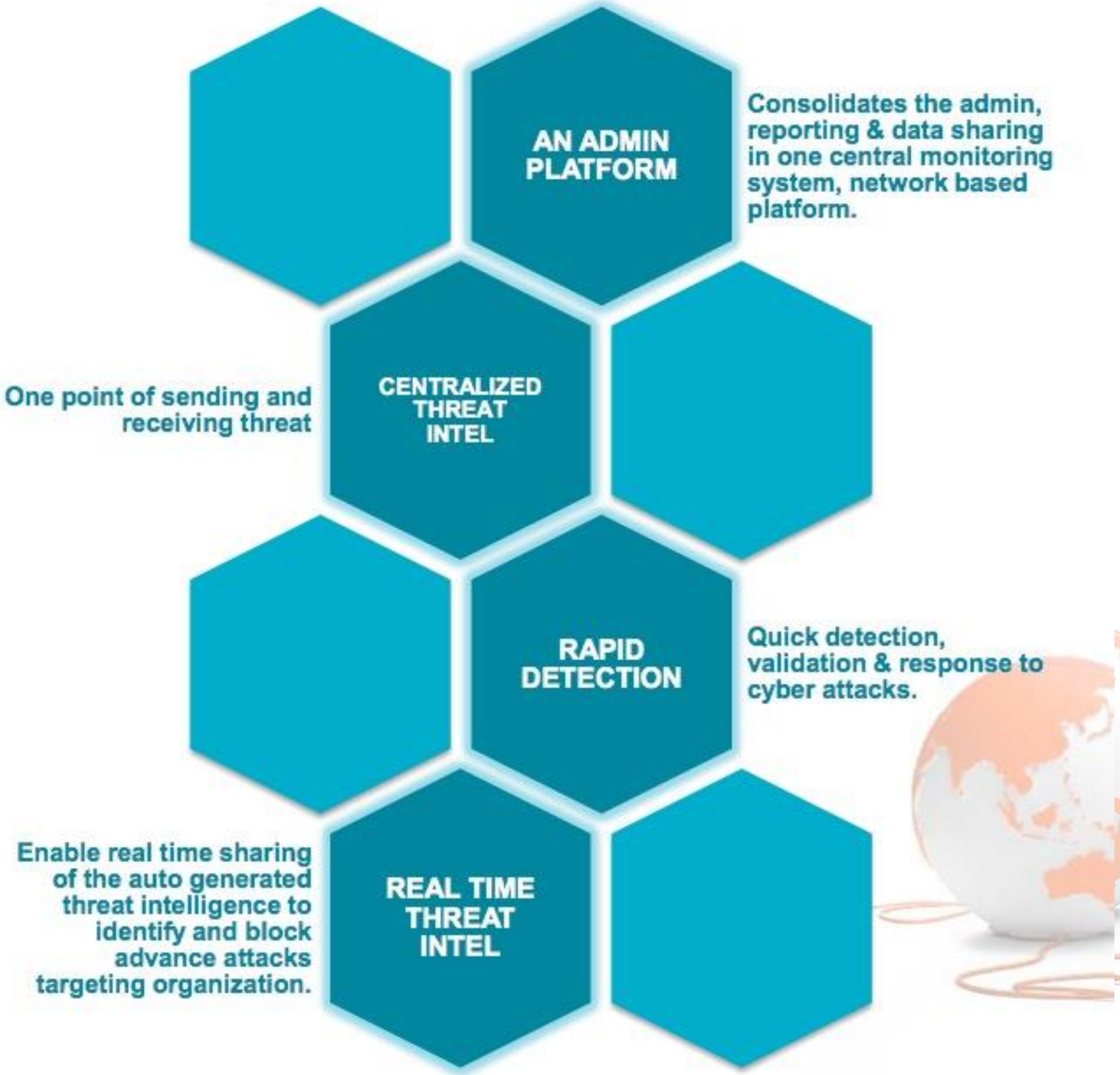
TIMESTAMP	ISP	SOURCE IP	DESTINATION IP	PORT NAME	PORT NUMBER	STATUS
2015-03-01 07:00:35	AS9534	113.210.139.96	204.95.99.31	can-ferret	1920	High
2015-03-01 07:00:35	AS9534	113.210.139.96	204.95.99.31	can-ferret	1920	High
2015-03-01 07:00:35	AS4788	110.159.162.93	204.95.99.109	infocrypt	2233	High
2015-03-01 07:00:35	AS4788	110.159.162.93	204.95.99.109	infocrypt	2233	High
2015-03-01 07:00:35	AS4788	118.101.45.70	204.95.99.109	texar	333	High
2015-03-01 07:00:35	AS4788	118.101.45.70	204.95.99.109	texar	333	High
2015-03-01 07:00:35	AS9930	211.25.8.138	204.95.99.86	sans	4442	High
2015-03-01 07:00:35	AS9930	211.25.8.138	204.95.99.86	sans	4442	High
2015-03-01 07:00:35	AS4788	115.135.107.190	204.95.99.31	mit-ml-dev	83	High
2015-03-01 07:00:35	AS4788	115.135.107.190	204.95.99.31	mit-ml-dev	83	High

Monthly statistic of malware infection



Very high!

Objective



AN ADMIN PLATFORM

Consolidates the admin, reporting & data sharing in one central monitoring system, network based platform.

CENTRALIZED THREAT INTEL

One point of sending and receiving threat

RAPID DETECTION

Quick detection, validation & response to cyber attacks.

REAL TIME THREAT INTEL

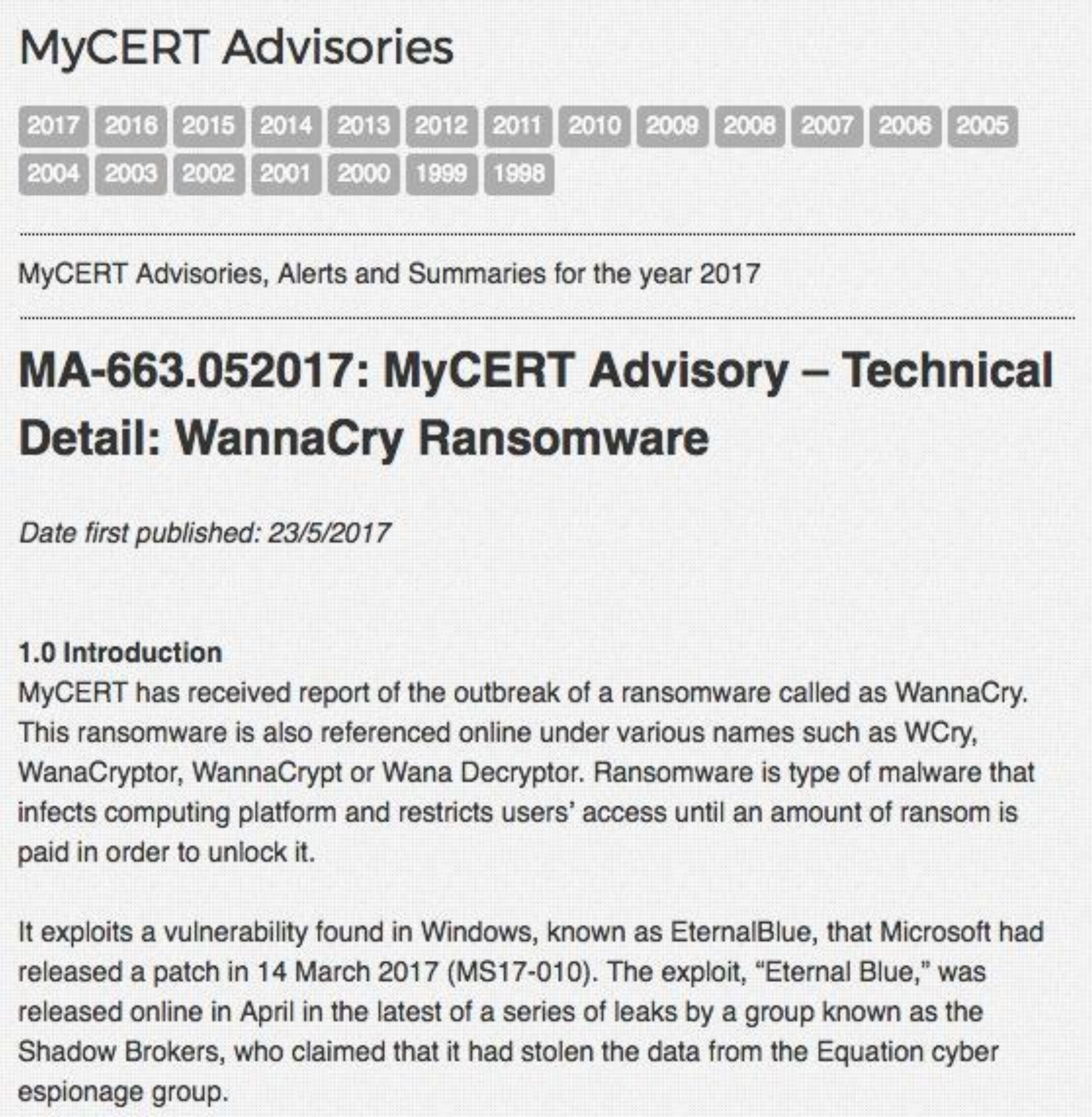
Enable real time sharing of the auto generated threat intelligence to identify and block advance attacks targeting organization.

Threat report

MALWARE TREND REPORT

H2 2016 : July – December 2016

Advisories



MyCERT Advisories

MyCERT Advisories, Alerts and Summaries for the year 2017

MA-663.052017: MyCERT Advisory – Technical Detail: WannaCry Ransomware

Date first published: 23/5/2017

1.0 Introduction

MyCERT has received report of the outbreak of a ransomware called as WannaCry. This ransomware is also referenced online under various names such as WCry, WanaCryptor, WannaCrypt or Wana Decryptor. Ransomware is type of malware that infects computing platform and restricts users' access until an amount of ransom is paid in order to unlock it.

It exploits a vulnerability found in Windows, known as EternalBlue, that Microsoft had released a patch in 14 March 2017 (MS17-010). The exploit, "Eternal Blue," was released online in April in the latest of a series of leaks by a group known as the Shadow Brokers, who claimed that it had stolen the data from the Equation cyber espionage group.

Findings

- Such analysis and landscape report will provide early detection of malware and the appropriate advisories allow organizations and government to react against the malware threats and protecting critical national information infrastructure, intellectual property and economy against the detrimental effect of malware intrusion and attacks.
- People; operational + research (training & experience)
- Process; coordination
- Technology; facilitation
- **TRUST <- need to resolve this!**

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

CyberSecurity MALAYSIA
An agency under MOSTI

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

Best Brand Internet Security 2008 & 2009

MS ISO/IEC 17021: 2011
ISMS 02082013 CB 02

MSC MALAYSIA Status Company

Best Child Online Protection Website