



Practical Workflow for Automation and Orchestration of Addressing Cyber Threat: Case Study of Mirai Botnet in Malaysia

Megat Muazzam Head of Malaysia CERT CyberSecurity Malaysia

Copyright © 2017 CyberSecurity Malaysia



Agenda

- Introduction
- Issues Surrounding Protecting Malaysia Cyber Security
- Important of Threat Intelligent Sharing
- Traditional SOC "And" Threat Intelligent Information Sharing
- Case study Mirai



MyCERT Maysia Computer Emergency Response Tan Cyber 999 Cyber Early Warning Services

Incident Handling

- Cyber Early Warning
 - Technical Coordination Centre
 - Malware Research Center

Email us at: cyber999@cybersecurity.my

REFERENCE CENTRE FOR CYBER SECURITY ASSISTANCE

- for all internet users, including home users and organizations

What steps are taken by the

Malaysian Government

to keep cyber threats under control?



One of the most important step is creating :

National Cyber Security Policy (NCSP) Establishing CyberSecurity Malaysia to implement NCSP



Issues Surrounding Cyber Security in Malaysia

Vastly expanding attack surface area (Mobile, Cloud, Virtualization, IOT etc)

Insufficient reliable data related to cyber threats

No appropriate body or authority that provides reliable data

Insufficient technical resources and expertise to expedite threat intelligence analysis and incident response.



CSIRT's Role in Protecting Critical National Information Infrastructure

- Information sharing about latest threats and mitigation measures against the threats
- Early warning of latest outbreaks, provide Alert and Advisory on the latest outbreak which includes detection and mitigations
- Raise awareness about cybersecurity and critical infrastructure protection issues
- As a platform to promote mutual collaboration between all sectors in CNII, such as Government, Private, Financial sectors. A good example is a National-level Cyber Exercise.
- Engaging with various parties such as with Law Enforcement Agencies, ISPs, security experts on mitigations against cyber attacks against CNII.



Current Malaysia Practise for Mitigating Cyber Threats in Malaysia





What is Threat Intel

"Threat Intelligence (TI) is evidence based knowledge, including context, mechanism, indicator, implications, and actionable advise about an existing or emerging menace or hazard to assets That can be used to inform decisions regarding the subject response to that menace or hazard" - Gartner, 2013

• SANS Institute

- The set of data collected, assessed and applied regarding security threat, threat actors, exploits, malware, vulnerabilities and compromise indicators"



To move threat intelligence sharing to the next level of efficiency and effectiveness, improvement is needed in three areas:

- We need to simplify event triage and provide a better environment for security practitioners to investigate highpriority threats.
- We need to do a better job establishing relationships between indicators of compromise so that we can understand their connections to attack campaigns.
- We need a better way to share threat intelligence among our stakeholders and relevant authorities.



Example of Threat Intelligence / Information Sharing Framework

Technical Platform / Framework

- MISP
- OpenIOC
- STIX / TAXII
- Collective Intelligence Framework (CIF)
- Avalanche/Soltra (FS-ISAC)

SIEM Communities

- Qradar Threat Exchange
- Splunk feeds

National CSIRTs/CERTs info sharing exchange



Traditional SOC Operation











Tools Used for Information Sharing

MyLipas	 Semi-automated escalation tool For mass IP notification
Honeynet	 Source of threat information
Automated Scripts	 Automating the analysis and processing of the threat information
Forensic tools	• Forensic analysis



Case Study - Mirai

Mirai Botnet Infection



https://intel.malwaretech.com/botnet/mirai/?t=24h&bid=all







List of vectors found in source code.

Attack	Description
UDP	UDP flood
VSE	Valve Source Engine query flood
DNS	Recursive DNS query attack
water	
torture	
SYN	SYN packet flood
ACK	ACK packet flood
STOMP	ACK flood with STOMP
GRE IP	GRE flood
GRE	Ethernet encapsulated inside
Ether-	GRE flood
net	
Plain	UDP flood optimized for speed
UDP	
HTTP	HTTP layer 7 flood

root/xc3511 admin/admin root/default root/54321 admin/password user/user admin/admin1234 admin/1111 root/1234 service/service guest/12345 administrator/1234 ubnt/ubnt root/hi3518 root/zlxx. root/system root/user admin/1111111 admin/54321 admin/1234 tech/tech

root/vizxv root/888888 root/juantech support/support root/root admin/(none) root/1111 root/666666 root/klv123 supervisor/supervisor guest/12345 666666/666666 root/klv1234 root/jvbzd root/7ujMko0vizxv root/ikwb root/realtek admin/1234 admin/123456 admin/pass mother/fu r

root/admin root/xmhdipc root/123456 root/(none) root/12345 root/pass admin/smcadmin root/password Administrator/admin guest/guest admin1/password 888888/888888 root/Zte521 root/anko root/7ujMko0admin root/dreambox root/00000000 admin/12345 admin/7ujMko0admin admin/meinsm

Mirai's built-in password dictionary.

The passwords come from the botnet's source code



Security Feeds Information

Mirai infection CC-Port Scan Detected Jan - April 2017





Mirai detection using Honeypot

MTPot – open source honeypot developed by *Cymmetria Research.*

MTPot is written in Python

- the ip and port to which the honeypot shall bind
- a list of commands expected to be sent by the scanners and the responses that MTPot shall give
- the name of the attack (Mirai)
- a session timeout value
- some optional syslog settings to collect the fingerprinted IPs
- Escalation to ISP focus only for .my source of IP that have been infected.



Automated Escalation Process





Automation of escalation

.....

B Customer - enal- external customer - enal- customer - enal- custom									
99 cuctomer - email- customer - email- custo	9	95	customer – email-external	.	Malaysia Computer Emer	gency Res	Botnet Drones daily r	02/03/2017 18:28	(1)
image: intercent in the intercent i	~ -		customer – email-		Malania Orana -) Rotect Russes of "	00/00/0017	(1)
D Customer - email Descie com mul Batest Proves dall D202017 (1) Article #95 - (() Bond Drones dally report on 02-02-2017. Created: 2003/2017 18.28 Prom: Mainysia Computer Emergency Response Team Prom: Mainysia Computer Emergency Response Team Computer Emergency Response Computer Emergency Response Computer Emergency Response Computer Emergency Computer Emergency Computer Emergency Computer Emergency Computer Emergency Computer Computer	ີ 9	96	external	(et-	Malaysia Computer Eme	ergency) Botnet Drones daily	02/03/2017	(1)
OP Description Description Description Description Description Article #95 - (Boinet Drones daily report on 02-02-2017. Image and the second main Ream of the se			customer – email-						(1)
Aricle #95 - (Botnet Drones daily report on 02-02-2017. Constrained and Formal Print Spin Bounce Forward Response Team Print Spin Bounce Forward Response Team Constrained and the second se	7 Q	97		- 14-	Malavsia Computer Eme	argency (m	axis com mv) Rotnet Drones dail	02/03/2017	(1)
<pre>r Article #95 - (</pre>									
And an Formal Print Bpill Bounce Forward PReppyAlls PReppy Prom: Malaysia Computer Emergency Response Team To C: cyber999@cybersecurity.my Signed: Good PGP signature. (Malaysia Computer Emergency Response Team (MyCERT) -cyber999@cybersecurity.my: 8286ED71: SrCDC0081100E03038B0A787D0100370280E0D71) Sudderd Bonnes daily report on 02-02-2017. Attachment: mycel.4788.01, 60.1 KByses Team-BBCIN PCP SIGNED MESSAGE Prepprit on malware, bothet act; 2017-02-02 00:00:01, 125 127-02-02 00:00:01, 125 127-02-02 00:00:01, 126 2017-02-02 00:00:01, 125 2017-02-02 00:00:01, 125 2017-02-	Article	e #95 -	(Botnet Drones of	daily repo	rt on 02-02-2017			Created: 02/03/2017	18.28
an Format Print Split Bounce Forward Reply All= Reply Re	7 4 6010	0 //00	Bothot Brohoo C	adity ropo				oroatod. oerooreo rr	10.20
From: Malaysia Computer Emergency Response Team (MyCERT) - cyber/9996cybersecurity.my-: 8286ED71: C:: cyber/9996cybersecurity.my Signet: Good PCP signature. (Malaysia Computer Emergency Response Team (MyCERT) - cyber/9996cybersecurity.my-: 8286ED71: C:: C:: Cyber/9996cybersecurity.my Signet: Good PCP signature. (Malaysia Computer Emergency Response Team (MyCERT) - cyber/9996cybersecurity.my-: 8286ED71: C:: C:: Cyber/9996cybersecurity.my Signet: Good PCP signature. (Malaysia Computer Emergency Response Team (MyCERT) - cyber/9996cybersecurity.my-: 8286ED71: C:: C:: Cyber/9996cybersecurity.my Minister Cyber/9996cybersecurity.my Minister Cyber/9996cybersecurity.my-: 8286ED71: C:: C:: Cyber/9996cybersecurity.my Minister Cyber/9996cybersecurity.my Minister Cyber/9996cybersecurity.my-: 8286ED71: C:: C:: Cyber/9996cybersecurity.my Minister Cyber/9996cyber/9996cyber/9996cyber/9996cyber/9	ain Form	nat Pri	nt Split Bounce Forward	- Reply	All - Repl	y -			
From: Malayala Computer Emergency Response Team To C: cyber9998cybersecurity.my Bignet: Good PDP Spinature, Malayala Computer Emergency Response Team (MyCERT) - cyber9898cybersecurity.my-: 8286ED71 : S7CDC089180c6083538BDAF97D01005708288ED71) Botnet Dones daily mport on 02-02-2017. Attachment: mimal.4788.tst, 650.1 KBytes Fear-BEGIN FCP SIGNED MESSAGE- Haah : SIA1 Dear Abuse Team, HyCERT : received a report from '2017-02-02 00:00:01,175 LimeStamp jbp, port.450,000,cc, 480.1 Mol / 100,000,000,000,000,000,000,000,000,000									
C: cyber9998cybersecurity.my Signet: Good PGP signature, Kuklaysia Computer Emergency Response Team (MyCERT) -cyber9996cybersecurity.myc: 8286ED71: C: cyber9998cybersecurity.myc: 8286ED71: C: cyber9998cybersecurity.myc: 8286ED71: C: cyber9998cybersecurity.myc: 8286ED71: C: cyber9998cybersecurity.myc: 8286ED71: C: cyber998cybersecurity.myc: 8286ED71: C: cyber998cyber996cybersecurity.myc: 8286ED71: C: cyber998cyber996cy		Fr	om: Malaysia Computer Emergen	icy Respon	se Team				
C: cyber9998cybersecurity.my Signet: Good PGP signature, Malaysia Computer Emergency Response Team (MyCERT) -cyber9998cybersecurity.my-: 8286ED71: Stdperf Botnet Drones daily report on 02-02-2017. Attachment: mirai.4788.td, 669.1 KBytes			Ter						
C:: cyber9996cybersecurity.my Bignet: Good PGP signature. (Malaysia Computer Emergency Response Team (MyCERT) -cyber9996cybersecurity.my: 18286ED71: 57CDC680190E083358BBAF97D01005708286ED71) Subject bother Dones daily report on C2-02-017. Attachment: mmsl 4788.td, 659.1 KBytes BEGIN POP SIGNED MESSAGE- timeStamp, ip, port, asn, geo.region, city, hostname, type, infection, url, agent, cc, cc_port, cc_asn, MyCERT received a report from '2017-02-02 00:00:01, 175 b.22, 20359, My EXERT received a report from '2017-02-02 00:00:01, 115 b.22, 20359, My EXERT received a report from '2017-02-02 00:00:01, 115 b.22, 20359, My EXERT received a report from '2017-02-02 00:00:01, 116 b.5, 15792, 4 y.5, EANGOR, PETALING JAYA, tcp, mirai,, 6789,,, 6789,,, 6789,,,, 6789,,,,,,,, .			18:						
Signed: Good PGP signature. (Makaysia Computer Emergency Response Team (MyCERT) - cyber9998cybersecurity.my: :8288ED71: STCDC8891B0E08338BBDAF97D01005708288ED71) Subject Botnet Dones daily report on 02-02-2017. Attachment: minal 4788.td, 669.1 KBytes			Cc: cyber999@cybersecurity.my						
Signer: Good PGP signature, Mulaysia Computer Emergency Response Team (MyCERT) -coyber9998cybersecurity.my: 12886ED71: Stdject Bothet Dones daily report on 02-02-2017. Attachment: miral 4788.td, 669.1 KBytes BEGIN PGP SIGNED MESSAGE- Haah: BHAI Dear Abuse Team, MyCERT received a report from (2017-02-02 00:00:01, 175 able to capture from the monit. 2017-02-02 00:00:01, 175 able to capture from the monit. 2017-02-02 00:00:01, 115 able to capture from the monit. 2017-02-02 00:00:01, 115 (2017-02-02 00:00:01, 110 Infection type, and these will 2017-02-02 00:00:01, 110 MyCERT received a report from (2017-02-02 00:00:01, 100 (2017-02-02 00:00:01, 115 (2017-02-02 00:00:01, 11									
Subject Botnet Drones daily report on 02-02-2017. Attachment: miral 4788.td. 659.1 KBytes Dear Abuse Team, MyCRRT received a report from report on malware, botnet action discovery of a list of all the able to capture from the monits. miral 4788.tl. txt ~ Bef IN-LOG- infection type, and these will. miral 4788.tl. txt ~ We are contacting you regarding. 2017-02-02 00:00:01.100 15,51072.tl. 2017-02-02 00:00:01.100 15,51072.tl. 22,22359. MWLAYAH PERSEKUTUAN KUALA LUMP,		Sigr	ied: Good PGP signature. (Malays	sia Comput	ter Emergency Response Team	(MyCERT) <cyber999@< td=""><td><pre>@cybersecurity.my> : 82B6ED71 :</pre></td><td></td><td></td></cyber999@<>	<pre>@cybersecurity.my> : 82B6ED71 :</pre>		
Butter Butter Dene daily report on 02-02-2017. Hackmant: mirai.4788.txl, 659.1 KBytes mirai.4788.txl, 659.1 KBytes Hash: SNAI mirai.4788.txl, 659.1 KBytes mirai.4788.txl, 659.1 KBytes Dear Abuse Team, MYCRR received a report from infection to all the daily report of 00:001.175 b.22,203.59, b.22,203.59, concertions to BTTP botnests, connections to BTTP botness, connections to BTTP botn			57CDC6891B0E08353BBDA	F97D01005	57082B6ED71)				
Attachment: mrail4788.bt, 659.1 KBytes Attachment: mrail4788.bt, 659.1 KBytes Dear Abuse Team, MyCRRT received a report from [2017-02-02 00:00:01.166. discovery of a list of all the able to capture from the monit. 2017-02-02 00:00:01.100 BEGIN-LOG		Subi	Rotact Dropas	haily report	02.02.2017				
Attachment: miral 4788.tx, 659.1 KBytes BEGIN FGP SIGNED MESSAGE- Hash: SHA1 Dear Abuse Team, MyCERT received a report from '2017-02-02 00:00:01,175 b.22,20359, MY,JADRR,JOHR BAHRU,,tcp,Miraj,,,6789,,.,6789,,.789,,,789,,.,780,,.789,,.,780,,.		Gubj	Bother Drones C	ally report	01102-02-2017.				
BEGIN PGP SIGNED MESSAGE Hash: SHA1 Dear Abuse Team, myCRRT received a report from '10,000 (001,000) (001,0		Attachm	ent: mirai.4788.txt , 659.1 KBytes	;					
BEGIN PGP SIGNED MESSAGE mirai.4788-1.txt Dear Abuse Team, MyCERT received a report from alware, bothet acti discovery of a list of all the able to capture from the monit infection type, and these will 2017-02-02 00:00:01, 60. b.22,20359, 22,20359, 2017-02-02 00:00:01, 60. mirai.4788-1.txt We are contacting you regarding you regarding you for the infection type, and these will 2017-02-02 00:00:01, 60. b.5,10792,4 2017-02-02 00:00:01, 60. mirai.4788-1.txt We are contacting you regarding you you regarding you you									
BEGIN PGP SIGNED MESSAGE- Hash: SHAI Dear Abuse Team, MyCERT received a report from '2017-02-02 00:00:01,175 5.22,20359, report on malware, bothet acti 2017-02-02 00:00:01,60. 245,5410,47 discovery of a liat of all the 2017-02-02 00:00:01,60. 245,5410,47 wiLAYAH PERSEKUTUAN KUALA LUMP, KU									
Hash: SHAI BEGIN-LOG- Dear Abuse Team, MyCRET received a report from 'insetamp, ip, port, asn, geo, region, city, hostname, type, infection, url, agent, cc, cc, port, cc, asn MyCRET received a report from 'insetamp, ip, port, asn, geo, region, city, hostname, type, infection, url, agent, cc, cc, port, cc, asn MyCRET received a report from 'insetamp, ip, port, asn, geo, region, city, hostname, type, infection, url, agent, cc, cc, port, cc, asn MyCRET received a report from the monit, 2017-02-02 00:00:01,60. bits, 127,023,000,000,000,000,000,000,000,000,000		BEGIN	N PGP SIGNED MESSAGE-					mirai 1788-1 tv	~
Dear Abuse Team, MyCERT received a report from imestamp, ip, port, asn, geo, region, city, hostname, type, infection, url, agent, cc, cc_port, cc_asn MyCERT received a report from infection system the monit of all the 2017-02-02 00:00:01, 175 connections to HTTP botnets, connections to HTTP botnets, connection type, and these will 2017-02-02 00:00:01, 60. 2017-02-02 00:00:01, 100 2017-02-02 00:00:01, 60. 2017-02-02 00:00:01, 75 2017-02-02 00:00:01, 75 2017-02-02 00:00:01, 175 2017-02-02 00:00	Hash	h: SHA						minal.4700-1.tx	•
MyCERT received a report from '2017-02-02 00:00:01,175 report on malware, botnet acti' 2017-02-02 00:00:01,106 discovery of a list of all the 2017-02-02 00:00:01,118 able to capture from the monit' 2017-02-02 00:00:01,118 infection type, and these will 2017-02-02 00:00:01,110 23,,.,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	Dear	r Abuse	e Team.	mostam	in port sch dee r	egion city hos	the type infection unless	ant cc cc nort	
report on malware, bothet act; 2017-02-02 00:00:01,60. 245,5410.47 discovery of a list of all the 2017-02-02 00:00:01,10 19,38935, mile computer from the monits of the monits of the computer from the monits of the compute	MyCE	ERT red	ceived a report from (70	17_02_0	p_{1} p_{2} p_{3} p_{1} p_{2} p_{3} p_{1} p_{2} p_{3} p_{3	22 20350		ten mirai 678	
discovery of a list of all the 2017-02-02 00:00:01,118 able to capture from the monit. 2017-02-02 00:00:01,118 infection type, and these will infection type, and these will 2017-02-02 00:00:01,60. 23,558888,4 WillAYAH PERSEKUTUAN KUALA LUMP, KUALA LUMP, We are contacting you regardin. 2017-02-02 00:00:01,60. 2017-02-02 00:00:01,60. 2017-02-02 00:00:01,60. 2017-02-02 00:00:01,60. 2017-02-02 00:00:01,75 2017-02-02 00:00:01,75 2017-02-02 00:00:01,75 2017-02-02 00:00:01,175 2017-02-02 00:00:01,175 2017-0	repo	ort on	malware, botnet acti 20	17-02-0	02 00:00:01,175	245 5410 47	WILAYAH PERSEKUTUAN K	ΙΔΙΔ Ι ΙΜΡ. ΚΙΙΔΙΔ	
able to capture from the monit. 217-02-02 00:00:01,10 0.5,10792,4 7,SARAWAK,MIRI,,tcp,mirai,,for89,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	disc	covery	of a list of all the 20	17-02-0	02 00:00:01,118	119, 38935	MY, SELANGOR, PETALING 1	YAtcp.mirai	
connections to HTTP botnets, or 2017-02-02 00:00:01,60. 35,58888,4 Y. WILAYAH PERSEKUTUAN KUALA LUMP,	able	e to ca	apture from the monit 20	17-02-0	02 00:00:01.110	5,10792.4	Y.SARAWAK.MIRItcp.mi	rai6789	
<pre>Intection type, and these will 23,,,,,,,,518210,737 We are contacting you regardin.2017-02-02 00:00:01,60. 235,20927,4 APNIC whois database. If you a:2017-02-02 00:00:01,60. 29,51910,4 Can relay this message by forw.2017-02-02 00:00:01,60. 14,38333,47 2017-02-02 00:00:01,175 5.196,15508 2017-02-02 00:00:01,175 5.196,15508 2017-02-02 00:00:01,175 24.32,22405 2017-02-02 00:00:01,175 24.32,22405 2017-02-02 00:00:01,175 24.32,22405 2017-02-02 00:00:01,115 24.32,22405 2017-02-02 00:00:01,115 24.32,22405 2017-02-02 00:00:01,115 24.32,22405 2017-02-02 00:00:01,115 24.32,22405 2017-02-02 00:00:01,115 24.4,28871,4 23,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,</pre>	conr	nection	to HTTP botnets, o: 20	17-02-0	02 00:00:01,60.	35,58888,4	Y,WILAYAH PERSEKUTUAN	WALA LUMP, KUALA	LUMP
We are contacting you regardin.2017-02-02 00:00:01,60. 235,20927,4 Y, SARAWAK, KUCHING, tcp,mirai,.,,23,.,.,, APNIC whois database. If you a: 2017-02-02 00:00:01,60. 14,38333,47 SELANGOR, JALAN TASIK SELATAN, tcp,mirai,.,,23,.,., can relay this message by forw.2017-02-02 00:00:01,175 1.96,15508 MY,SELANGOR, JALAN TASIK SELATAN, tcp,mirai,.,,23,.,., 2017-02-02 00:00:01,175 1.96,15508 MY,PULAU PINANG,BUTTERWORTH, tcp,mirai,.,,23,.,., 2017-02-02 00:00:01,175 2.4,22,25228 MY,PULAU PINANG,BUTTERWORTH, tcp,mirai,.,,23,.,., 2017-02-02 00:00:01,175 2.4,22,25228 MY,PULAU PINANG,BUTTERWORTH, tcp,mirai,.,,23,.,., 2017-02-02 00:00:01,175 2.4,32,22405 MY,PULAU PINANG,BUTTERWORTH, tcp,mirai,.,,23,., 2017-02-02 00:00:01,118 39,13863,4 Y,SELANGOR,PETALING JAYA, tcp,mirai,.,,23,., 2017-02-02 00:00:01,115 2.64,1024, MY,SELANGOR,PETALING JAYA, tcp,mirai,.,,23,., 2017-02-02 00:00:01,115 2.64,25871,4 Y,SELANGOR,PETALING JAYA, tcp,mirai,.,,23,., 2017-02-02 00:00:01,175 34.223,5222 8,MY,SELANGOR,PETALING JAYA, tcp,mirai,.,,23,.,., 2017-02-02 00:00:01,175 34.223,5222 8,MY,SELANGOR,PETALING JAYA, tcp,mirai,.,,23,.,.,, 2017-02-02 00:00:01,175 34.223,5222 8,MY,SELANGOR,PETALING JAYA, tcp,mirai,.,,23,.,.,,	TULE	ection	cype, and chese will 23	3	,,,,,518210,737	Communicati	, , ,		
APNIC whois database. If you a: 2017-02-02 00:00:01,60. can relay this message by forw. 2017-02-02 00:00:01,60. 2017-02-02 00:00:01,175 2017-02-02 00:00:01,175 2017-02-02 00:00:01,175 2017-02-02 00:00:01,175 2017-02-02 00:00:01,175 2017-02-02 00:00:01,175 2017-02-02 00:00:01,175 2017-02-02 00:00:01,175 2017-02-02 00:00:01,175 2017-02-02 00:00:01,115 2017-02-02 00:00:01,115 2017-02-02 00:00:01,115 2017-02-02 00:00:01,115 2017-02-02 00:00:01,115 2017-02-02 00:00:01,175 2017-02-02 00:00:01,175 2017-02	We a	are con	ntacting you regardin, 20	17-02-0	02 00:00:01,60.	235,20927,4	Y, SARAWAK, KUCHING, , tcp	,mirai,,,,23,,,,	, , , , ,
<pre>can relay this message by forw 2017-02-02 00:00:01,175 2017-02-02 00:00:01,175 2017-02-02 00:00:01,175 2017-02-02 00:00:01,175 2017-02-02 00:00:01,175 2017-02-02 00:00:01,175 2017-02-02 00:00:01,175 2017-02-02 00:00:01,175 2017-02-02 00:00:01,175 2017-02-02 00:00:01,115 2017-02-02 00:00:01,115 2017-02-02 00:00:01,115 2017-02-02 00:00:01,115 2017-02-02 00:00:01,115 2017-02-02 00:00:01,175 2017-02-02 00:00:0</pre>	APNI	IC who:	is database. If you a:20	17-02-0	02 00:00:01,60.	29,51910,4	Y, SELANGOR, JALAN TASIK	SELATAN,,tcp,mi	rai,,
2017-02-02 00:00:01,175 5.196,15508 ,MY,SELANGOR,JALAN TASIK SELATAN,,tcp,mirai, 2017-02-02 00:00:01,175 7.7,47877,4 Y,SELANGOR,KJANG,bUTTERWORTH,,tcp,mirai,.,23, 2017-02-02 00:00:01,175 4.32,22405 ,MY,PULAU PINANG,BUKIT MERTAJAM,tcp,mirai, 2017-02-02 00:00:01,118 39,13863,4 Y,SELANGOR,PETALING JAYA,tcp,mirai,.,23, 2017-02-02 00:00:01,115 2.64,1024, MY,SELANGOR,PETALING JAYA,tcp,mirai,.,23, 2017-02-02 00:00:01,60. 54,25871,4 Y,SELANGOR,PETALING JAYA,tcp,mirai,.,23, 2017-02-02 00:00:01,175 34.223,5222 8,MY,SELANGOR,PETALING JAYA,tcp,mirai,.,23, 2017-02-02 00:00:01,175 34.223,5222 8,MY,SELANGOR,PETALING JAYA,tcp,mirai,.,23 2017-02-02 00:00:01,175 34.223,5222 8,MY,SELANGOR,PETALING JAYA,tcp,mirai,.,23 2017-02-02 00:00:01,175 34.223,5222 8,MY,SELANGOR,PETALING JAYA,tcp,mirai,.,23 2017-02-02 00:00:01,175 34.223,5222 8,MY,SELANGOR,PETALING JAYA,tcp,mirai,.,23 2017-02-02 00:00:01,175 204,57521, MY,SELANGOR,PETALING JAYA,tcp,mirai,.,6789,.,., 2017-02-02 00:00:01,175 204,57521, MY,SELANGOR,PETALING JAYA,tcp,mirai,.,6789,.,., 2017-02-02 00:00:01,175 204,57521, MY,SELANGOR,PETALING JAYA,tcp,mirai,.,6789,.,., 2017-02-02 00:00:01,175 00.94,20580 ,MY,SELANGOR,PETALING JAYA,tcp,mirai,.,23, 2017-02-02 00:00:01,175 00.94,20580 ,MY,SELANGOR,PETALING JAYA,tcp,mirai,.,23,.,., 2017-02-02 00:00:01,175 00.94,20580 ,MY,SELANGOR,PETALING JAYA,tcp,mirai,.,23,.,.,, 2017-02-02 00:00:01,175 0.203,60448 ,	can	relay	this message by forward)17-02-0	02 00:00:01,60.	14,38333,47	,SELANGOR, PETALING JAY	A,,tcp,mirai,,,,	23,,,
<pre>2017-02-02 00:00:01,170 7,22,25228 MY,PULAU PINANG,BUTTERWORTH,tcp,mirai,,,,23 2017-02-02 00:00:01,175 7,47877,4 Y,SELANGOR,KAJANG,tcp,mirai,,,23,,,,,20 2017-02-02 00:00:01,175 24.32,22405 MY,PULAU PINANG,BUKIT MERTAJAM,tcp,mirai,,,23,, 2017-02-02 00:00:01,118 39,13863,4 Y,SELANGOR,PETALING JAYA,tcp,mirai,,,23,, 2017-02-02 00:00:01,115 2.64,1024 MY,SELANGOR,VETALING JAYA,tcp,mirai,,,23,, 2017-02-02 00:00:01,60. 54,25871,4 Y,SELANGOR,VETALING JAYA,tcp,mirai,,,23,, 2017-02-02 00:00:01,175 34.223,5222 8,MY,SELANGOR,PETALING JAYA,tcp,mirai,,,23 2017-02-02 00:00:01,175 34.223,5222 8,MY,SELANGOR,PETALING JAYA,tcp,mirai,,,23 2017-02-02 00:00:01,175 34.223,5222 8,MY,SELANGOR,VETALING JAYA,tcp,mirai,,,23 2017-02-02 00:00:01,175 34.223,5222 8,MY,SELANGOR,VETALING JAYA,tcp,mirai,,,23 2017-02-02 00:00:01,175 34.223,5222 8,MY,SELANGOR,PETALING JAYA,tcp,mirai,,,6789,,,,, 2017-02-02 00:00:01,118 0.198,12942 MY,SELANGOR,VETALING JAYA,tcp,mirai,,,6789,,,,, 2017-02-02 00:00:01,115 2.04,57521, MY,SELANGOR,VETALING JAYA,tcp,mirai,,,6789,,,,, 2017-02-02 00:00:01,115 3.220,13400 MY,SELANGOR,VETALING JAYA,tcp,mirai,,,23,, 2017-02-02 00:00:01,175 00.94,20580 MY,SELANGOR,PETALING JAYA,tcp,mirai,,,23,,,,, 2017-02-02 00:00:01,175 00.94,20580 MY,SELANGOR,PETALING JAYA,tcp,mirai,,,23,,,,, 2017-02-02 00:00:01,175 00.94,20580 MY,SELANGOR,PETALING JAYA,tcp,mirai,,,23,,,,, 2017-02-02 00:00:01,175 00.94,20580 MY,SELANGOR,PETALING JAYA,tcp,mirai,,,23,,,,, 2017-02-02 00:00:01,175 00.94,20580 MY,SELANGOR,PUCHONG,tcp,mirai,,,23,,,,,, 2017-02-02 00:00:01,175 00.94,20580 MY,SELANGOR,PUCHONG,tcp,mirai,,,23,,,,,, 2017-02-02 00:00:01,175 00.94,20580 MY,SELANGOR,PUCHONG,tcp,mirai,,,23,,,,,, 2017-02-02 00:00:01,175 00.94,65159 MY,SELANGOR,PUCHONG,tcp,mirai,,,23,,,,,, 2017-02-02 00:00:01,175 0.203,60448 MY,PULAU PINANG,BAYAN LEPAS,tcp,mirai,,,23,,,,,, 2017-02-02 00:00:01,175 0.203,60448 MY,PULAU PINANG,BAYAN LEPAS,tcp,mirai,,,23,,,,,23,24456 MY,DUOR DANDAR DANA LEPAS,tcp,mirai,,,23,24456 MY,DUOR DANDAR DANA LEPAS,tcp,mirai,,,23,24456 MY,DUOR DANDAR DA</pre>			20	17-02-0	02 00:00:01,175	5.196,15508	, MY, SELANGOR, JALAN TAS	[K SELATAN,,tcp,	mirai
<pre>2017-02-02 00:00:01,175 24,32,2405 , MY,PULAU PINANG,BUKIT MERTAJAM, tcp,miraj,,,23,,,,2017-02-02 00:00:01,118 39,13863,4 Y,SELANGOR,PETALING JAYA,tcp,miraj,,,23,,2017-02-02 00:00:01,105 2.64,1024, MY,SELANGOR,PETALING JAYA,tcp,miraj,,,23,,2017-02-02 00:00:01,105 34,25871,4 Y,SELANGOR,PETALING JAYA,tcp,miraj,,,23,,2017-02-02 00:00:01,175 34,223,5222 8, MY,SELANGOR,PETALING JAYA,tcp,miraj,,,23,2017-02-02 00:00:01,175 34,223,522 8, MY,SELANGOR,PETALING JAYA,tcp,miraj,,,23,2017-02-02 00:00:01,175 204,57521, MY,SELANGOR,PETALING JAYA,tcp,miraj,,,6789,,,2017-02-02 00:00:01,175 204,57521, MY,SELANGOR,PETALING JAYA,tcp,miraj,,,6789,,2017-02-02 00:00:01,175 204,57521, MY,SELANGOR,PETALING JAYA,tcp,miraj,,,6789,,2017-02-02 00:00:01,175 204,57521, MY,SELANGOR,PETALING JAYA,tcp,miraj,,,23,2017-02-02 00:00:01,175 204,57521, MY,SELANGOR,PETALING JAYA,tcp,miraj,,,23,2017-02-02 00:00:01,175 204,57521, MY,SELANGOR,PETALING JAYA,tcp,miraj,,,23,2017-02-02 00:00:01,175 204,57521, MY,SELANGOR,PETALING JAYA,tcp,miraj,,,23,2017-02-02 00:00:01,175 00:94,20580 ,MY,SELANGOR,PETALING JAYA,tcp,miraj,,,23,2017-02-02 00:00:01,175 00:94,20580 ,MY,SELANGOR,PETALING JAYA,tcp,miraj,,23,23,2017-02-02 00:00:01,175 00:94,20580 ,MY,J0HOR J0HOR BARRU,tp,Miraj,,23,23,23,23,2017-02-02 00:00:01,175 00:94,20580 ,MY,J0HOR J0HOR PAMPULAU PINANG,BAYAN LEPAS,tp,Miraj,,23,2017-02-02 00:00:01,175 0.203,60448 ,MY,PULAU P</pre>			20	17-02-0	02 00:00:01,210	17.22,25228	,MY, PULAU PINANG, BUTTE	RWORTH,,tcp,mira	1,,,,
2017-02-02 00:00:01,115 2017-02-02 00:00:01,118 2017-02-02 00:00:01,118 2017-02-02 00:00:01,115 2017-02-02 00:00:01,115 2017-02-02 00:00:01,175 2017-02-02 00:00:01,210 2017-02-02 00:00:01,2			20	017-02-0	02 00:00:01,175	9.7,47877,4	Y, SELANGOR, KAJANG, , tcp	miral,,,,23,,,,	, <u>.</u> .
2017-02-02 00:00:01,118 2017-02-02 00:00:01,118 2017-02-02 00:00:01,115 2017-02-02 00:00:01,60. 23,,,,,,,,518210,737 2017-02-02 00:00:01,175 2017-02-02 00:00:01,175 2017-02-02 00:00:01,175 2017-02-02 00:00:01,118 2017-02-02 00:00:01,118 2017-02-02 00:00:01,118 2017-02-02 00:00:01,118 2017-02-02 00:00:01,118 2017-02-02 00:00:01,118 2017-02-02 00:00:01,118 2017-02-02 00:00:01,115 2017-02-02 00:00:01,115 2017-02-02 00:00:01,115 2017-02-02 00:00:01,115 2017-02-02 00:00:01,115 2017-02-02 00:00:01,115 2017-02-02 00:00:01,115 2017-02-02 00:00:01,115 2017-02-02 00:00:01,115 2017-02-02 00:00:01,115 200,13400 MY,SELANGOR, PETALING JAYA, tcp,mirai,.,,6789,.,.,, 2017-02-02 00:00:01,115 2020,13400 MY,SELANGOR, PETALING JAYA, tcp,mirai,.,,23,.,,, 2017-02-02 00:00:01,115 2020,13400 MY,SELANGOR, PETALING JAYA, tcp,mirai,.,,23,.,,, 2017-02-02 00:00:01,115 2020,3400 MY,SELANGOR, PETALING JAYA, tcp,mirai,.,,23,.,,, 2017-02-02 00:00:01,175 203,60448 MY,PULAU PINANG,BAYAN LEPAS, tcp,mirai,.,23,.,,, 2017-02-02 00:00:01,175 204,65159 MY, PULAU PINANG,BAYAN LEPAS, tcp,mirai,.,,23,.,,, 2017-02-02 00:00:01,175 2023,4456 MY, PULAU PINANG,BAYAN LEPAS, tcp,mirai,.,,23,.,,, 2017-02-02 00:00:01,175 2023,4456 MY, PULAU PINANG,BAYAN LEPAS, tcp,mirai,.,,23,.,,,22,23,456 MY, PULAU PINANG,BAYAN LEPAS, tcp,mirai,.,,23,.,,,22,23,456 MY, PULAU PINANG,BAYAN LEPAS, tcp,mirai,.,,23,.,,,22,23,456 MY, PULAU PINANG,BAYAN LEPAS, tcp,mirai,.,,23,.,,,22,23,455 MY, PULAU PINANG,BAYAN LEPAS, tcp,mirai,.,,23,.,,,22,23,456 MY, PULAU PINANG,BAYAN LEPAS, tcp,mirai,.,,23,.,,,22,23,456 MY, PULAU PINANG,BAYAN LEPAS, tcp,mirai,.,,23,.,,,22,23,456 MY, PULAU PINANG,BAYAN LEPAS, tcp,mirai,.,,23,.,,,22,23,456 MY, PULAU PINANG,BAYAN LEPAS, tcp,mirai,.,,23,.,,,22,23,455 MY, PULAU PINANG,BAYAN LEPAS, tcp,mirai,.,,23,.,,,22,23,456 MY, PULAU PINANG,BAYAN LEPAS, tcp,mirai,.,,23,.,,,22,23,456 MY JOHOP JOHOP PAHUPI tcp,mirai,.,,23,.,,,22,23,456 MY JOHOP JOHOP PAHUPI tcp,mirai,.,,23,.,,,22,23,456 MY JOHOP JOHOP PAHUPI tcp			26	017-02-0	02 00:00:01,175	24.32,22405	,MY, PULAU PINANG, BUKIT	MERIAJAM, tcp,	irai,
2017-02-02 00:00:01,60. 2017-02-02 00:00:01,60. 23,,,,,,,518210,737 2017-02-02 00:00:01,175 2017-02-02 00:00:01,175 2017-02-02 00:00:01,175 2017-02-02 00:00:01,175 2017-02-02 00:00:01,118 2017-02-02 00:00:01,118 2017-02-02 00:00:01,175 2017-02-02 00:00:01,210 2017-02-02 00:00:01,210 2017-02-02 00:00:01,210 2017-02-02 00:00:01,210 2017-02-02 00:00:01,210 2017-02-02 00:00:01,215 2017-02-02 00:00:01,215			20	017-02-0	02 00:00:01,118	39,13863,4	Y, SELANGUR, PETALING JA	A,,tcp,miral,,,	,23,,
2017-02-02 00:00:01,737 2017-02-02 00:00:01,175 2017-02-02 00:00:01,175 2017-02-02 00:00:01,175 2017-02-02 00:00:01,175 2017-02-02 00:00:01,175 2017-02-02 00:00:01,118 2017-02-02 00:00:01,175 2017-02-02 00:00:01,1			20		02 00:00:01,115	12.64,1024,	MY, SELANGUR, PETALING J.	AYA,,tcp,mirai,,	,,23,
23,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,			20	017-02-0	02 00:00:01,60.	54,258/1,4	Y, SELANGUR, KLANG, 54, 10	4.50.60.Kl]03-nd	me.tm
2017-02-02 00:00:01,175 34.223,522 8,MT,SELANGOR,PETALING JATA,,tcp,mirai,,,22 2017-02-02 00:00:1,203 7.53,22456, MY,WILAYAH PERSEKUTUAN KUALA LUMP,KUALA LUMP 23,,,,,,518210,737 communicati 2017-02-02 00:00:01,118 9.198,12942 ,MY,SELANGOR,KJANG,,tcp,mirai,,,6789,,,,, 2017-02-02 00:00:01,175 204,57521, MY,SELANGOR,KJANG,,tcp,mirai,,,6789,,,,, 2017-02-02 00:00:01,175 204,57521, MY,SELANGOR,PETALING JATA,,tcp,mirai,,,6789 2017-02-02 00:00:01,115 5.220,13400 ,MY,SELANGOR,PETALING JATA,,tcp,mirai,,,23, 2017-02-02 00:00:01,175 90.94,20580 ,MY,JOHOR,JOHOR BAHRU,,tcp,mirai,,,23,,,,, 2017-02-02 00:00:01,210 99.94,65159 ,MY,SELANGOR,PETALING JATA,,tcp,mirai,,,23,,,,, 2017-02-02 00:00:01,175 1.203,60448 ,MY,PULAU PINANG,BATAN LEPAS,,tcp,mirai,,,23			23	17 02 0	,,,,,518210,/3/	.ommunicati	A MY CELANCOD DETAL INC	14VA ten minoi	2
2017-02-02 00:00:01,135 23,,,,,,,,518210,737 2017-02-02 00:00:01,118 2017-02-02 00:00:01,175 204,57521, MY, SELANGOR, KAJANG,,tcp,mirai,,,,6789,,,,,, 2017-02-02 00:00:01,175 204,57521, MY, SELANGOR, PETALING JAYA,,tcp,mirai,,,,6789 2017-02-02 00:00:01,115 2020,13400 ,MY, SELANGOR, PETALING JAYA,,tcp,mirai,,,,23, 2017-02-02 00:00:01,175 2017-02-02 00:00:01,210 2017-02-02 00:00:01,175 2017-02-02 00:00:01,175 2017-02-02 00:00:01,210 2017-02-02 00:00:01,21			20		02 00:00:01,175	34.223,5222	8, MY, SELANGUR, PETALING	JAYA, tcp, mirai	,,,,,
23,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,			20	017-02-6	62 00:00:01,203	.53,22450,	MY, WILAYAH PERSERUTUAN	KUALA LUMP, KUAL	A LUM
2017-02-02 00:00:01,175 2017-02-02 00:00:01,175 2017-02-02 00:00:01,175 2017-02-02 00:00:01,124 2017-02-02 00:00:01,115 2020,13400 2017-02-02 00:00:01,175 2017-02-02 00:00:01,175 2017-02-0			23	17 02 0	,,,,,518210,737		MY SADAWAK KUCHTNC +	on miroj 6700	
2017-02-02 00:00:01,124 2017-02-02 00:00:01,124 2017-02-02 00:00:01,115 2017-02-02 00:00:01,115 2017-02-02 00:00:01,175 2017-02-02 00:00:01,175 2017-02-02 00:00:01,210 2017-02-02 00:00:01,210 2017-02-02 00:00:01,175 2017-02-02 00:00:01,1			20	17_02_0	02 00:00:01,118	204 57521	MY SELANGOR KAJANG to	p, mirai 6780	, , , , ,
2017-02-02 00:00:01,115 5.220,13400 ,MY,SELANGOR, PETALING JAYA,,tcp,mirai,,.,23, 2017-02-02 00:00:01,175 10.94,20580 ,MY,JOHOR,JOHOR BAHRU,,tcp,mirai,.,,23, 2017-02-02 00:00:01,210 99.94,65159 ,MY,SELANGOR,PUCHONG,,tcp,mirai,.,,23,.,,, 2017-02-02 00:00:01,75 3.203,60448 ,MY,PULAU PINANG BAYAN LEPAS,tcp,mirai,.,,23,.,,, 2017-02-02 00:00:01,175 1.152 3.24556 MY,JOHOR BAHRU, tcp,mirai,.,,23,.,,,,2017-02-02 00:00:01,175 1.152 3.24556 MY, PULAU PINANG BAYAN LEPAS,tcp,mirai,.,,23			20	17_02_0	02 00:00:01,175	164 0331	MY SELANCOR PETALING 1	VA ton mirai	678
2017-02-02 00:00:01,175 00.94,20580 ,MY,DHOR BAHRU,,tcp,mirai,,,,23,,,,, 2017-02-02 00:00:01,210 99.94,65159 ,MY,SELANGOR,PUCHONG,,tcp,mirai,,,,23,,,,, 2017-02-02 00:00:01,175 3.203,60448 ,MY,PULAU PINANG,BAYAN LEPAS,,tcp,mirai,,,,23,,,,, 2017-02-02 00:00:01,175 1.152 3.4456 MY,DHOR DAHPB MAURING, BAYAN LEPAS,,tcp,mirai,,,,23,,,,,2017-02-02 00:00:01,175 1.152 3.4456			20	17_02_0	02 00:00:01,124	220 13400	MY SELANCOR PETALING	1AVA ton mirai	,,0/0
2017-02-02 00:00:01,210 99.94,65159 ,MY, <u>SELANGOR,PUCHONG</u> ,tcp,mirdi,.,,23,,,,, 2017-02-02 00:00:01,175 3.203,60448 ,MY,PULAU PINANG,BAYAN LEPAS,,tcp,mirai,.,,6 2017-02-02 00:00:01,175 1.152 34456 MY,DUHOR JOHOR DAMPUL tcp.mirai,			20	17-02-0	02 00:00:01,115	0.94 20580	MY 10HOR 10HOR BAHRU	tcn mirai 23	,,,25
2017-02-02 00:00:01,175 3.203,60448 ,MY,PULAU PINANG,BAYAN LEPAS,,tcp,mirai,,,6			20	17-02-0	02 00.00.01 210	9 94 65159	MY SELANGOR PUCHONG	rcp, mirai 23	,,,,,
2017-02-02 00:00:01 175 1 152 34456 MY JOHOR JOHOR BAHPU too miraj 23			20	17-02-0	02 00:00:01,175	3,203,60448	MY PULAL PINANG BAYAN	LEPAS. tcp.mira	i
			20	17-02-0	02 00:00:01,175	1,152,34456	MY, JOHOR, JOHOR BAHRU,	tcp.mirai23	****



Mitigate the attacked

- Automated incident escalation to ISP
- Recommend ISPs identify compromised IoT devices by filtering traffic TCP23 / TCP 2323 / TCP 7547
 - ISP action : Isolate and notify legitimate owners of the problem and urge to take corrective action.
- Publish advisory to alert Malaysia Internet user



Recommendation to device owners

- Research the capabilities and security features of an IoT device before purchase
- Stop using default/generic passwords.
- Disable Telnet login and use SSH
- Disable or protect remote access to IoT devices when not needed
- Regularly check the manufacturer's website for firmware updates



What is the challenges

Owner of Devices

- Not straightforward to patch/upgrade
- Not every user know how to resolve infected devices

IoT Manufacture

- Profit Vs Security
- Unnecessary services should be disabled by default
- Best practices: password

ISP

- Difficult to correlate information that have been share / escalate by CERT
- Need proper guidelines to informed affected customers.



Summary

- It worked for us in obtaining valid, reliable threat intelligent information from our trusted partners. This will eventually makes identification and rectification works smoothly.
- It worked in identifying the threats, vulnerabilities to systems belonging to the CNII sector
- It strengthens the working collaboration between CSIRTs and CNII sectors and position CSIRT as an entity that plays an important role in safe guarding the cyber space
- CSIRTs partnership has become an integral part at international network to fight against cyber threats.
- To develop a baseline understanding of common threats and capabilities to enable coordinated actions among the CNII sectors in the event of large scale cyber attacks.



Questions ?



- Find out more
 - www.cybersecurity.my
 - www.mycert.org.my
 - cyber999@cybersecurity.my
- Personal
 - megat@cybersecurity.my





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

ISMS

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



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







