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

CyberSecurity MALAYSIA
An agency under MOSTI

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

Agenda

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

Cyber999™
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

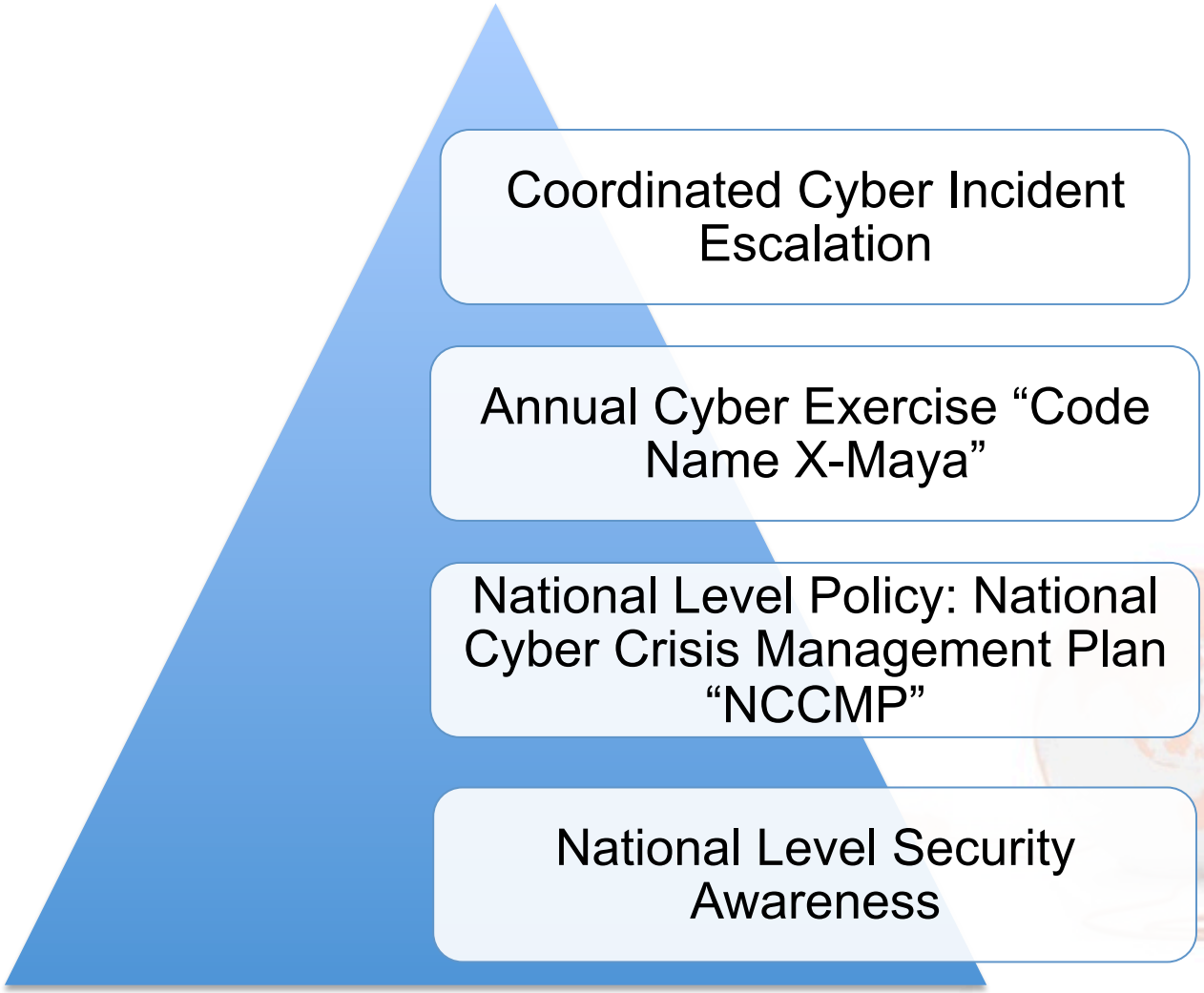
Issues Surrounding Cyber Security in Malaysia

- 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"

Importance of Threat Intelligence

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 high-priority 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

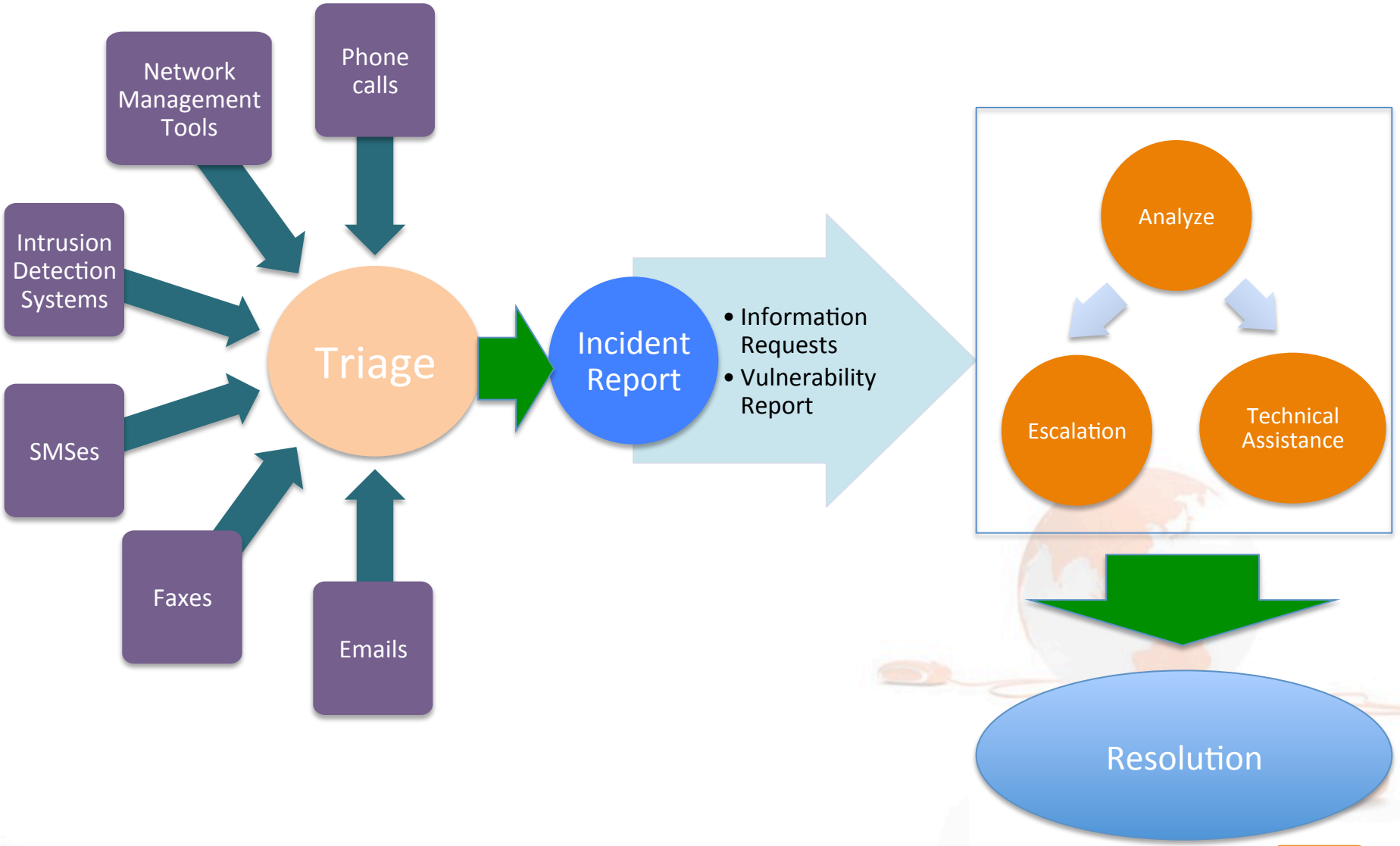
- MISP
- OpenIOC
- STIX / TAXII
- Collective Intelligence Framework (CIF)
- Avalanche/Soltra (FS-ISAC)

SIEM Communities

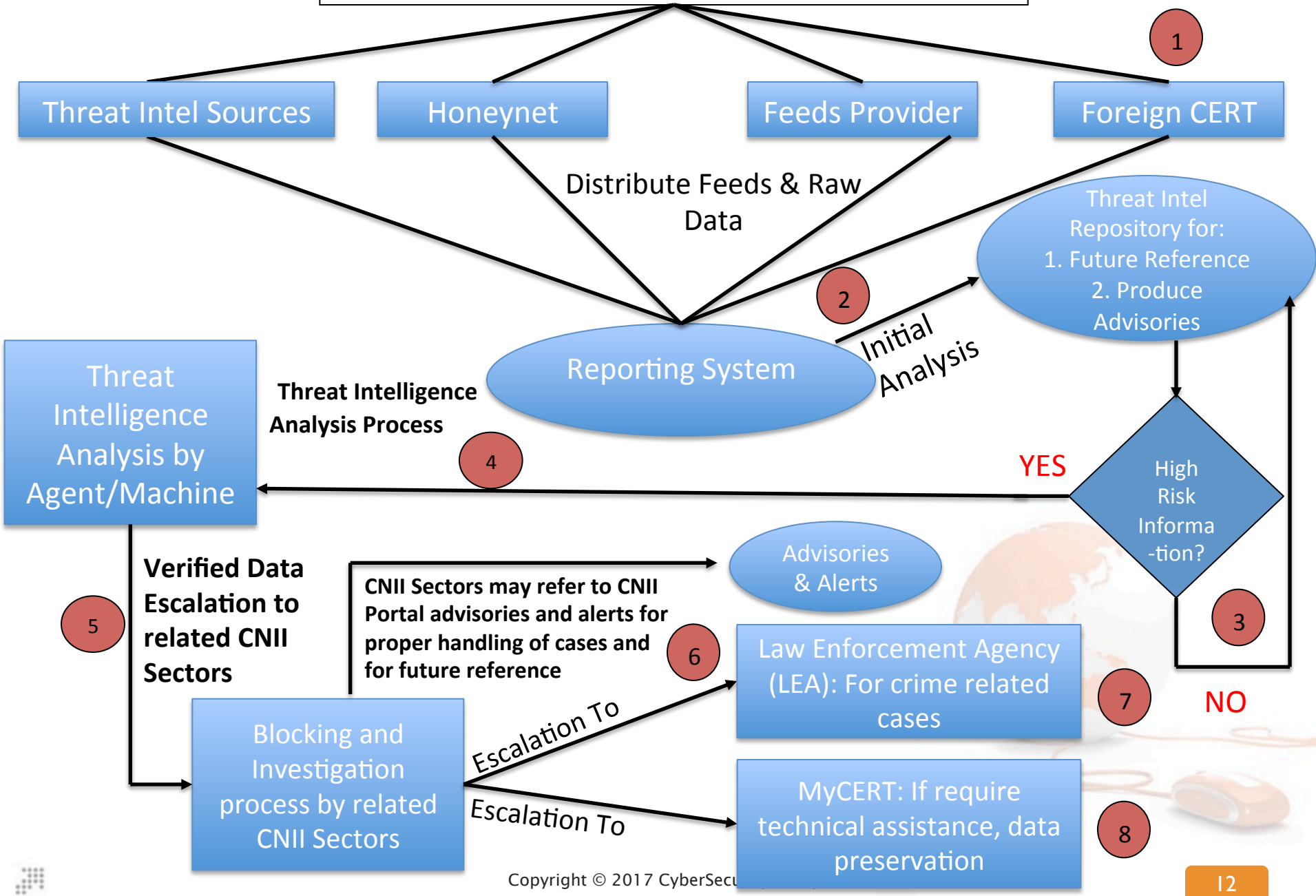
- Qradar Threat Exchange
- Splunk feeds

National CSIRTs/CERTs info sharing exchange

Traditional SOC Operation



Threat Intelligence Information Sharing Model

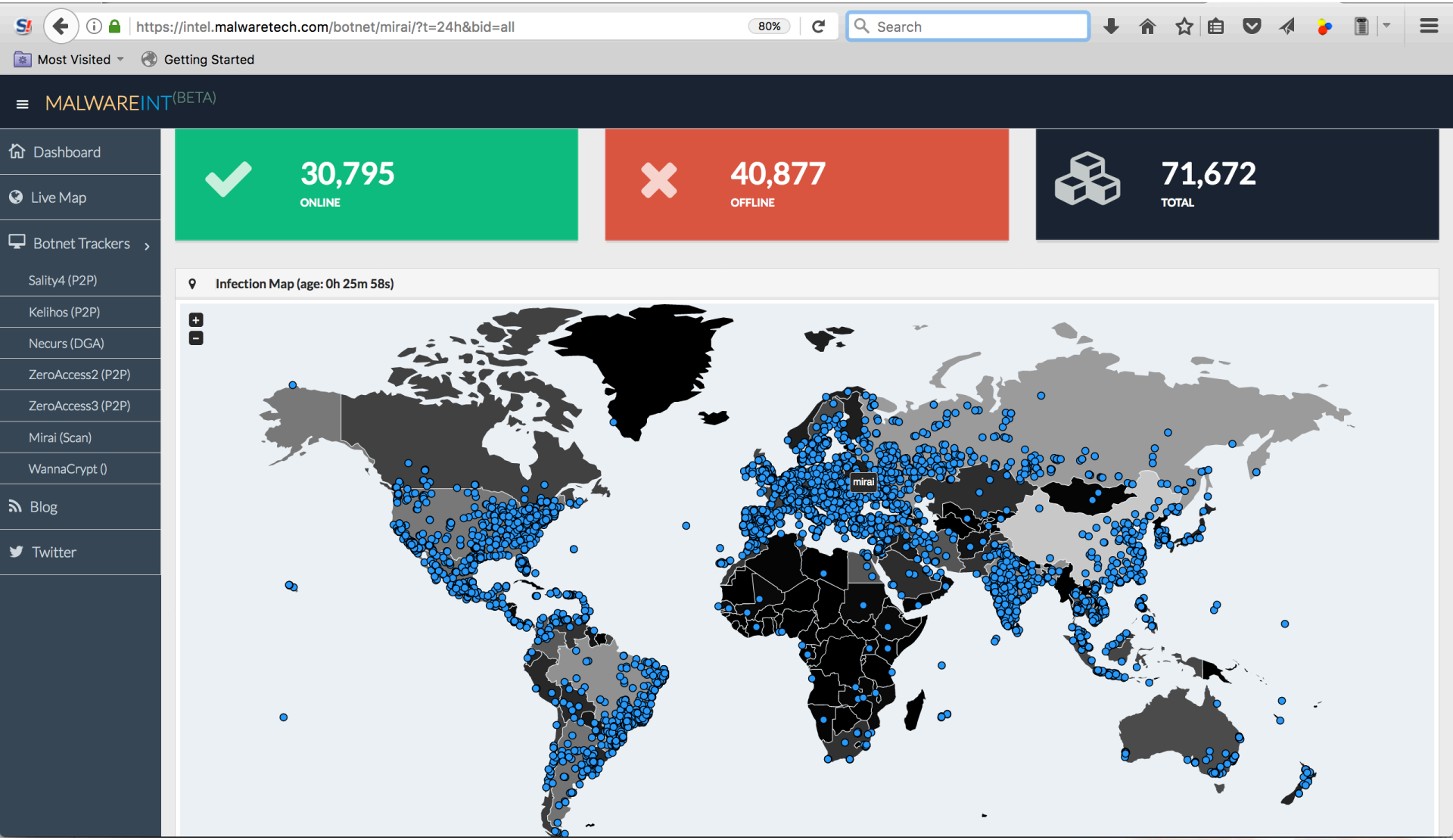


Tools Used for Information Sharing

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

Shodan | Developers | Book | View All...

SHODAN | port:7547 country:my | Explore | Downloads | Reports | Enterprise Access | Contact Us

Exploits | Maps | Share Search | Download Results | Create Report

TOTAL RESULTS

20,585

TOP COUNTRIES

Malaysia	20,585

TOP CITIES

Kuala Lumpur	6,762
Petaling Jaya	2,020
Shah Alam	1,183
Klang	776
Kajang	362

TOP ORGANIZATIONS

TM Net	17,073
Maxis Broadband Sdn Bhd	1,447
Central	313
TM Business	208
Tt Dotcom Sdn Bhd	130

210.186.135.252
TM Net
Added on 2017-05-29 04:59:48 GMT
Malaysia, Kuala Lumpur
Details

175.139.242.105
TM Net
Added on 2017-05-29 04:58:43 GMT
Malaysia, Alma
Details

175.142.235.79
TM Net
Added on 2017-05-29 04:58:39 GMT
Malaysia, Kuala Lumpur
Details

TOTAL RESULTS

20,585

TOP COUNTRIES

Malaysia	20,585

TOP CITIES

Kuala Lumpur	6,762
Petaling Jaya	2,020
Shah Alam	1,183
Klang	776
Kajang	362

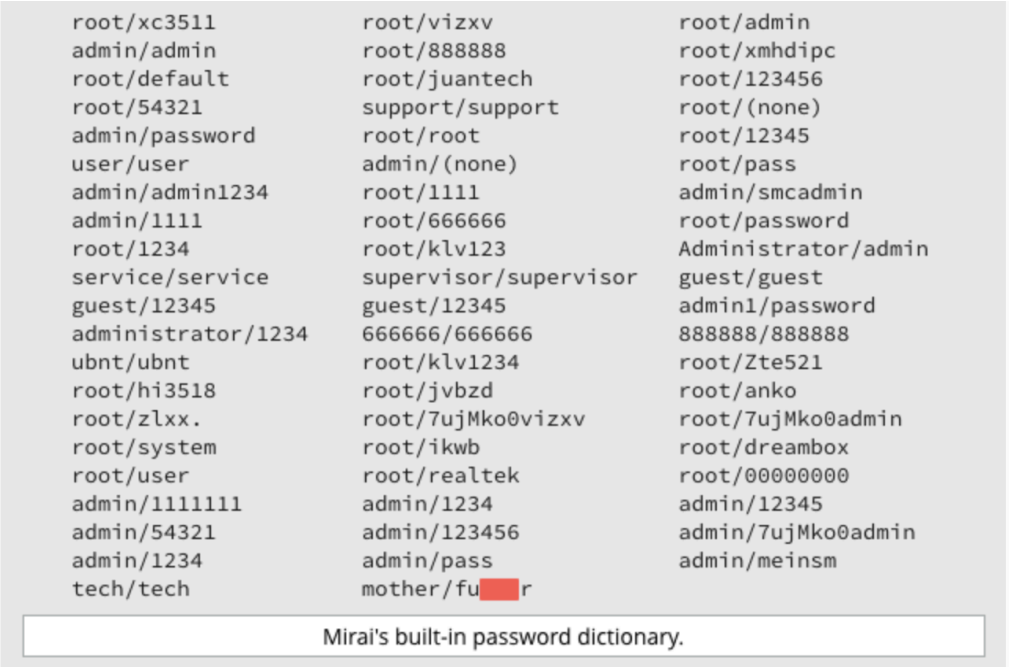
TOP ORGANIZATIONS

TM Net	17,073
Maxis Broadband Sdn Bhd	1,447
Central	313
TM Business	208
Tt Dotcom Sdn Bhd	130

https://www.shodan.io/

List of vectors found in source code.

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

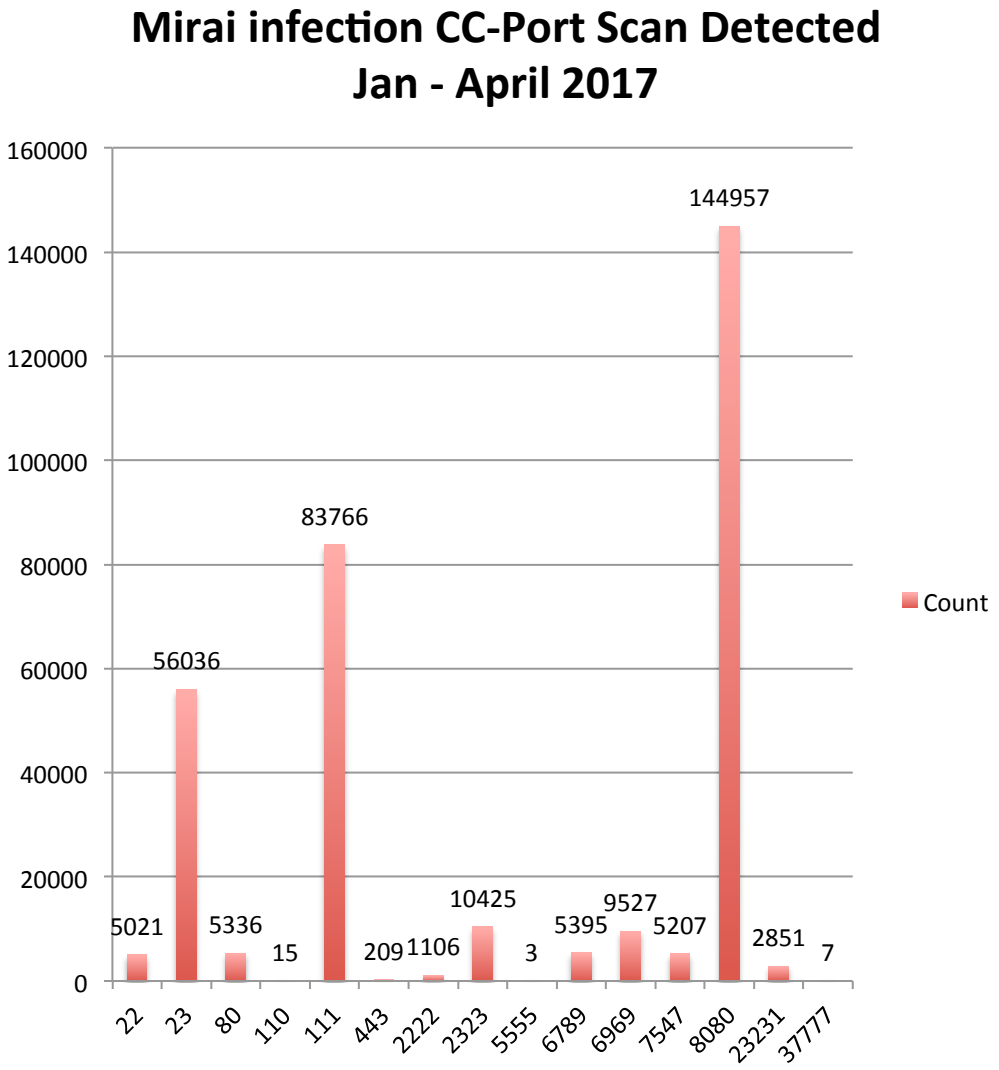


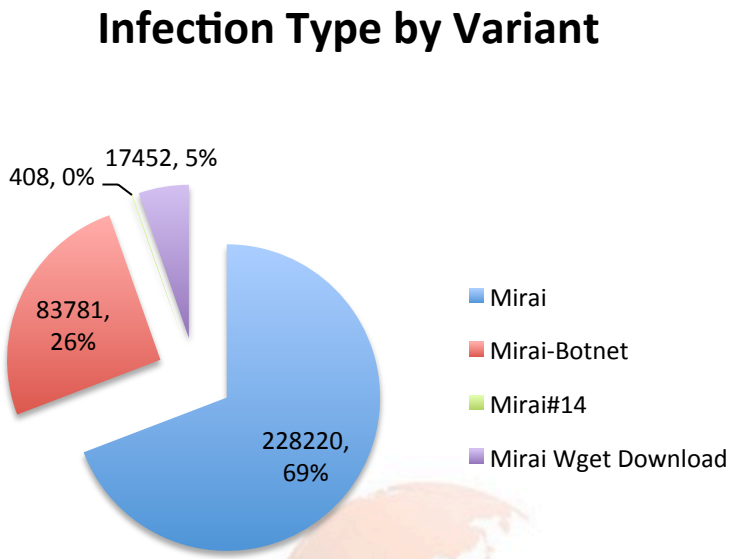
root/xc3511	root/vizxv	root/admin
admin/admin	root/888888	root/xmhdipc
root/default	root/juantech	root/123456
root/54321	support/support	root/(none)
admin/password	root/root	root/12345
user/user	admin/(none)	root/pass
admin/admin1234	root/1111	admin/smcadmin
admin/1111	root/666666	root/password
root/1234	root/klv123	Administrator/admin
service/service	supervisor/supervisor	guest/guest
guest/12345	guest/12345	admin1/password
administrator/1234	666666/666666	888888/888888
ubnt/ubnt	root/klv1234	root/Zte521
root/hi3518	root/jvbzd	root/anko
root/zlxx.	root/7ujMko0vizxv	root/7ujMko0admin
root/system	root/ikwb	root/dreambox
root/user	root/realtek	root/00000000
admin/1111111	admin/1234	admin/12345
admin/54321	admin/123456	admin/7ujMko0admin
admin/1234	admin/pass	admin/meinsm
tech/tech	mother/fu[redacted]r	

Mirai's built-in password dictionary.

The passwords come from the botnet's source code

Security Feeds Information





Mirai detection using Honeypot

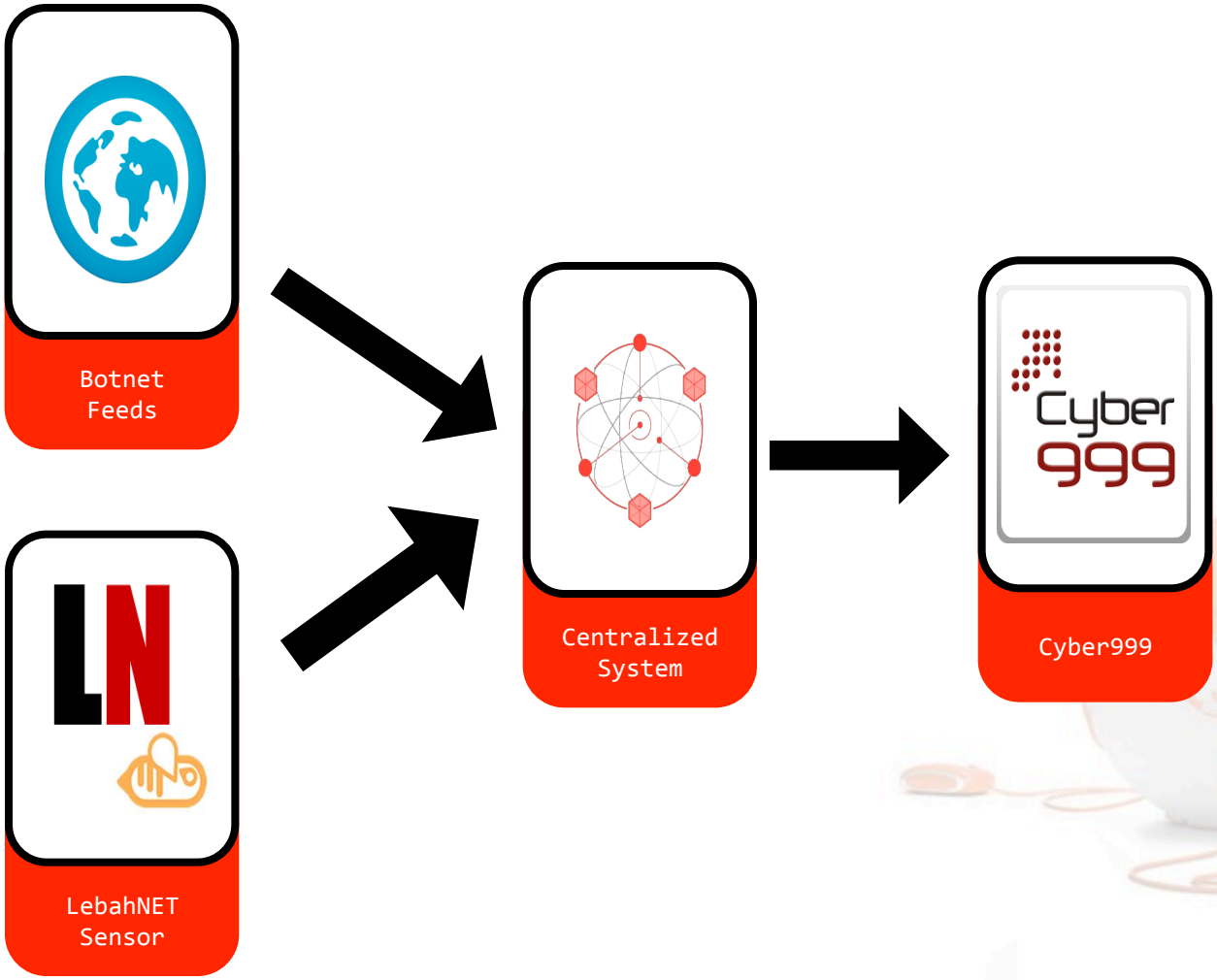
MTPot – open source honeypot developed by *Cymmetria Research.*

MTPot is written in Python

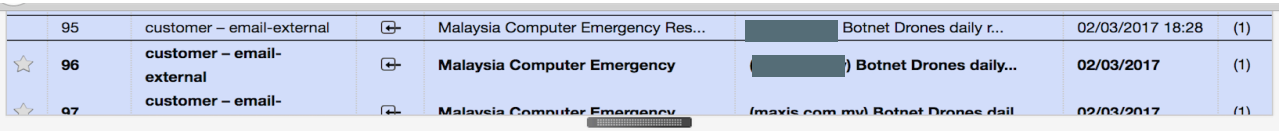
- the ip and port to which the honeypot shall bind
- a list of commands expected to be sent by the scanners and the responses that MTPot shall give
- the name of the attack (Mirai)
- a session timeout value
- some optional syslog settings to collect the fingerprinted IPs

- Escalation to ISP focus only for .my source of IP that have been infected.

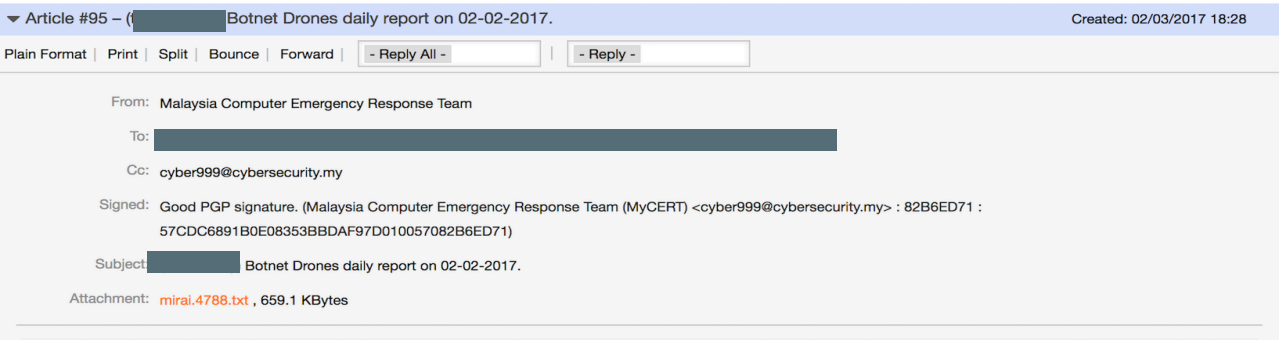
Automated Escalation Process



Automation of escalation



95	customer – email-external		Malaysia Computer Emergency Res...	[redacted] Botnet Drones daily r...	02/03/2017 18:28	(1)
96	customer – email-external		Malaysia Computer Emergency	([redacted]) Botnet Drones daily...	02/03/2017	(1)
97	customer – email-		Malaysia Computer Emergency	(maxis.com.my) Botnet Drones dail	02/03/2017	(1)



Article #95 – ([redacted] Botnet Drones daily report on 02-02-2017. Created: 02/03/2017 18:28

Plain Format | Print | Split | Bounce | Forward | - Reply All - | - Reply -

From: Malaysia Computer Emergency Response Team

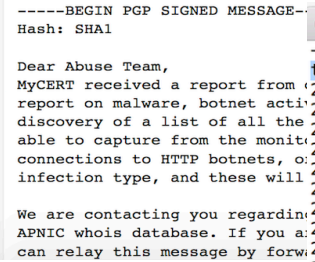
To: [redacted]

Cc: cyber999@cybersecurity.my

Signed: Good PGP signature. (Malaysia Computer Emergency Response Team (MyCERT) <cyber999@cybersecurity.my> : 82B6ED71 : 57CDC6891B0E08353BBDAF97D010057082B6ED71)

Subject: [redacted] Botnet Drones daily report on 02-02-2017.

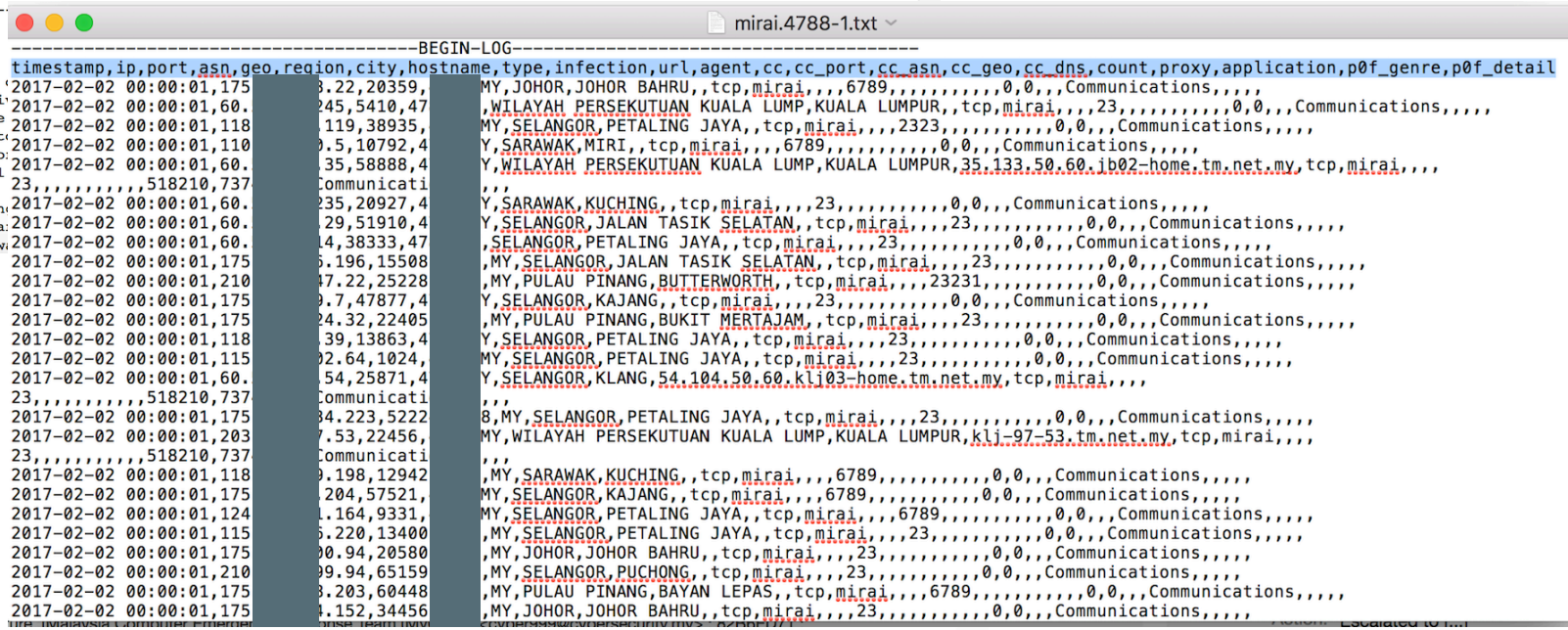
Attachment: mirai.4788.txt , 659.1 KBytes



```
-----BEGIN PGP SIGNED MESSAGE-
Hash: SHA1

Dear Abuse Team,
MyCERT received a report from
report on malware, botnet acti
discovery of a list of all the
able to capture from the monit
connections to HTTP botnets, o
infection type, and these will

We are contacting you regardin
APNIC whois database. If you a
can relay this message by forw
```



mirai.4788-1.txt

```
-----------------------------------BEGIN-LOG-----------------------------------
timestamp,ip,port,asn,geo,region,city,hostname,type,infection,url,agent,cc,cc_port,cc_asn,cc_geo,cc_dns,count,proxy,application,p0f_genre,p0f_detail
2017-02-02 00:00:01,175[redacted]3.22,20359,[redacted]MY,JOHOR,JOHOR BAHRU,,tcp,mirai,,,,6789,,,,,,,,,,0,0,,,Communications,,,,,
2017-02-02 00:00:01,60.[redacted]245,5410,47[redacted],WILAYAH PERSEKUTUAN KUALA LUMP,KUALA LUMPUR,,tcp,mirai,,,,23,,,,,,,,,,0,0,,,Communications,,,,,
2017-02-02 00:00:01,118[redacted].119,38935,[redacted]MY,SELANGOR,PETALING JAYA,,tcp,mirai,,,,2323,,,,,,,,,,0,0,,,Communications,,,,,
2017-02-02 00:00:01,110[redacted]9.5,10792,4[redacted]Y,SARAWAK,MIRI,,tcp,mirai,,,,6789,,,,,,,,,,0,0,,,Communications,,,,,
2017-02-02 00:00:01,60.[redacted]35,58888,4[redacted]Y,WILAYAH PERSEKUTUAN KUALA LUMP,KUALA LUMPUR,35.133.50.60.jb02-home.tm.net.my,tcp,mirai,,,,
23,,,,,,,,,,518210,737[redacted]Communicati[redacted],,,
2017-02-02 00:00:01,60.[redacted]235,20927,4[redacted]Y,SARAWAK,KUCHING,,tcp,mirai,,,,23,,,,,,,,,,0,0,,,Communications,,,,,
2017-02-02 00:00:01,60.[redacted]29,51910,4[redacted]Y,SELANGOR,JALAN TASIK SELATAN,,tcp,mirai,,,,23,,,,,,,,,,0,0,,,Communications,,,,,
2017-02-02 00:00:01,60.[redacted]14,38333,47[redacted],SELANGOR,PETALING JAYA,,tcp,mirai,,,,23,,,,,,,,,,0,0,,,Communications,,,,,
2017-02-02 00:00:01,175[redacted]5.196,15508[redacted],MY,SELANGOR,JALAN TASIK SELATAN,,tcp,mirai,,,,23,,,,,,,,,,0,0,,,Communications,,,,,
2017-02-02 00:00:01,210[redacted]7.22,25228[redacted],MY,PULAU PINANG,BUTTERWORTH,,tcp,mirai,,,,23231,,,,,,,,,,0,0,,,Communications,,,,,
2017-02-02 00:00:01,175[redacted]9.7,47877,4[redacted]Y,SELANGOR,KAJANG,,tcp,mirai,,,,23,,,,,,,,,,0,0,,,Communications,,,,,
2017-02-02 00:00:01,175[redacted]24.32,22405[redacted],MY,PULAU PINANG,BUKIT MERTAJAM,,tcp,mirai,,,,23,,,,,,,,,,0,0,,,Communications,,,,,
2017-02-02 00:00:01,118[redacted].39,13863,4[redacted]Y,SELANGOR,PETALING JAYA,,tcp,mirai,,,,23,,,,,,,,,,0,0,,,Communications,,,,,
2017-02-02 00:00:01,115[redacted]2.64,1024,[redacted]MY,SELANGOR,PETALING JAYA,,tcp,mirai,,,,23,,,,,,,,,,0,0,,,Communications,,,,,
2017-02-02 00:00:01,60.[redacted].54,25871,4[redacted]Y,SELANGOR,KLANG,54.104.50.60.klj03-home.tm.net.my,tcp,mirai,,,,
23,,,,,,,,,,518210,737[redacted]Communicati[redacted],,,
2017-02-02 00:00:01,175[redacted]34.223,5222[redacted]8,MY,SELANGOR,PETALING JAYA,,tcp,mirai,,,,23,,,,,,,,,,0,0,,,Communications,,,,,
2017-02-02 00:00:01,203[redacted]7.53,22456,[redacted]MY,WILAYAH PERSEKUTUAN KUALA LUMP,KUALA LUMPUR,klj-97-53.tm.net.my,tcp,mirai,,,,
23,,,,,,,,,,518210,737[redacted]Communicati[redacted],,,
2017-02-02 00:00:01,118[redacted]9.198,12942[redacted],MY,SARAWAK,KUCHING,,tcp,mirai,,,,6789,,,,,,,,,,0,0,,,Communications,,,,,
2017-02-02 00:00:01,175[redacted].204,57521,[redacted]MY,SELANGOR,KAJANG,,tcp,mirai,,,,6789,,,,,,,,,,0,0,,,Communications,,,,,
2017-02-02 00:00:01,124[redacted]1.164,9331,[redacted]MY,SELANGOR,PETALING JAYA,,tcp,mirai,,,,6789,,,,,,,,,,0,0,,,Communications,,,,,
2017-02-02 00:00:01,115[redacted]5.220,13400[redacted],MY,SELANGOR,PETALING JAYA,,tcp,mirai,,,,23,,,,,,,,,,0,0,,,Communications,,,,,
2017-02-02 00:00:01,175[redacted]0.94,20580[redacted],MY,JOHOR,JOHOR BAHRU,,tcp,mirai,,,,23,,,,,,,,,,0,0,,,Communications,,,,,
2017-02-02 00:00:01,210[redacted]9.94,65159[redacted],MY,SELANGOR,PUCHONG,,tcp,mirai,,,,23,,,,,,,,,,0,0,,,Communications,,,,,
2017-02-02 00:00:01,175[redacted]3.203,60448[redacted],MY,PULAU PINANG,BAYAN LEPAS,,tcp,mirai,,,,6789,,,,,,,,,,0,0,,,Communications,,,,,
2017-02-02 00:00:01,175[redacted]1.152,34456[redacted],MY,JOHOR,JOHOR BAHRU,,tcp,mirai,,,,23,,,,,,,,,,0,0,,,Communications,,,,,
```

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

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

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

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

Status Company

Best Child Online Protection Website