



An agency under MOSTI

WHAT HAPPEN IN OUR BACKYARDS?

CYBER SECURITY THREATS LANDSCAPE



Megat Muazzam Abdul Motalib
Head of MyCERT
CyberSecurity Malaysia



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

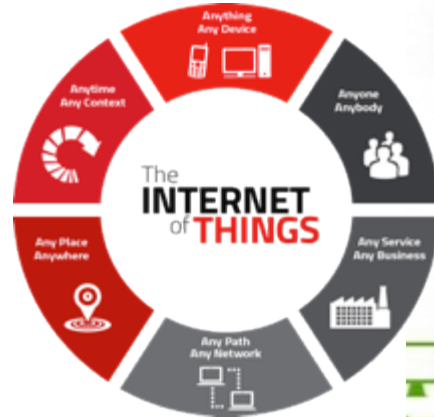
- for all internet users, including home users and organizations

Services

Reactive	Proactive
<ol style="list-style-type: none">1. Incident Response and Handling2. Advisories	<ol style="list-style-type: none">1. Watch and Warn / Threat Monitoring2. Research and Development3. Training and Outreach/Awareness4. Cyber Security Crisis



DIGITAL ENVIRONMENT IS ALREADY COMPLEX



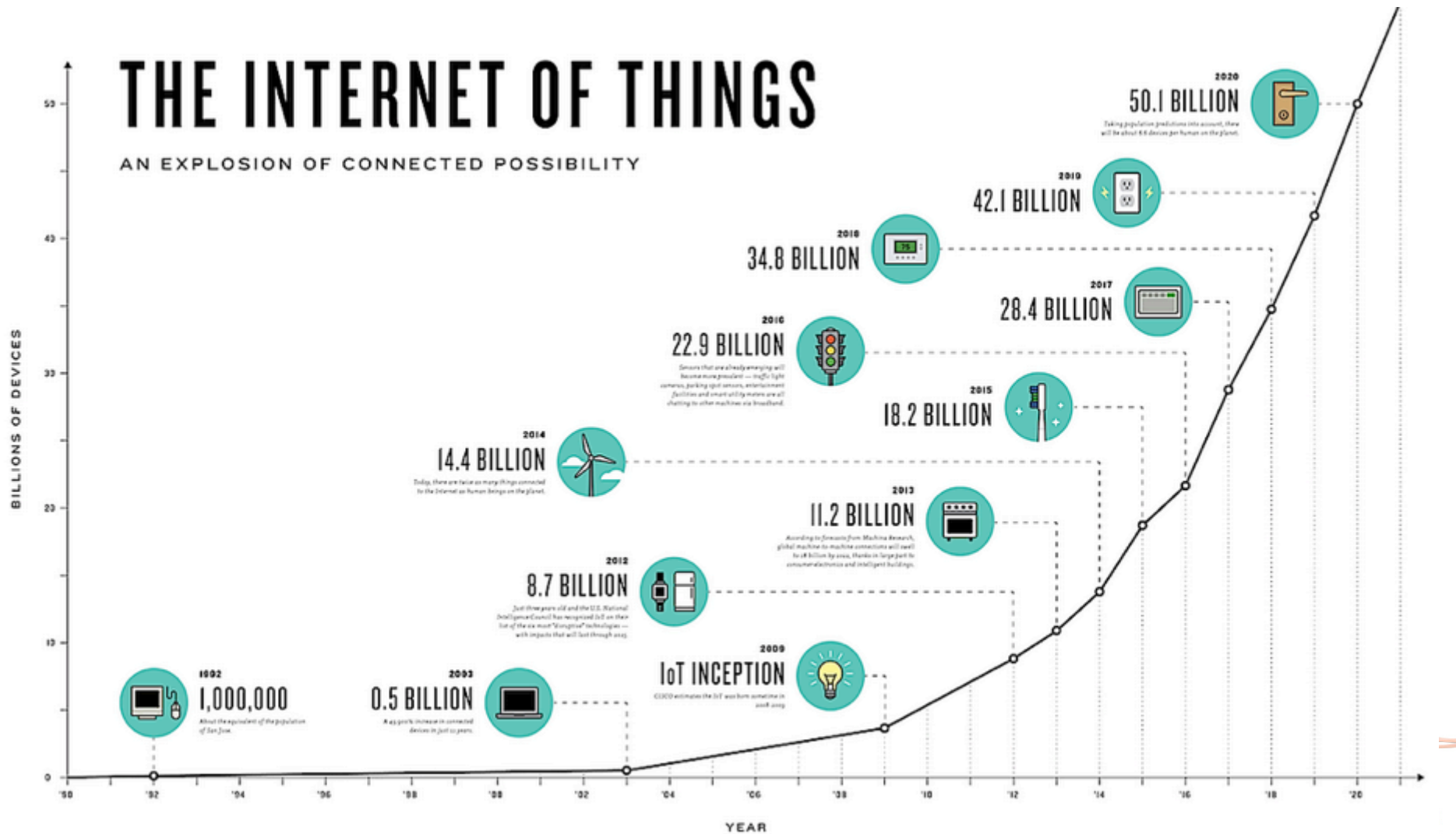
CONVERGENCE OF NEW TECHNOLOGIES INTO CYBER SPACE

- Add More Complexities

The collage features several key elements:

- The Internet of Things:** A circular graphic with segments for "Anything Any Device", "Anyone Anybody", "Any Service Any Business", and "Any Place Anywhere".
- Cloud Computing:** A central cloud labeled "Cloud computing" connected to icons for "Television", "Tablets", "SMS", "Internet", "Server", and "Desk".
- Autonomous Driving:** A section titled "Autonomous Driving" with sub-sections: "Google's modified Toyota Prius uses an driver. Other components, not shown, in", "LIDAR: A rotating sensor on the roof scans more than 200 feet in all directions to generate a precise three-dimensional map of the car's surroundings.", and "VIDEO CAMERA: A camera mounted near the mirror helps onboard".
- Artificial Intelligence:** A graphic showing a human head profile with neural network patterns and the text "ARTIFICIAL INTELLIGENCE".
- Industry 4.0:** A circular graphic with segments for "INDUSTRY 4.0" and "BLOCK CHAIN TECHNOLOGY".
- Technology is Changing Business:** A large blue banner with the text "TECHNOLOGY IS CHANGING BUSINESS".
- Other Elements:** A stack of smartphones, a robot head, and a molecular structure.

WE ARE MOVING INTO A MORE INTERCONNECTED CYBERSPACE



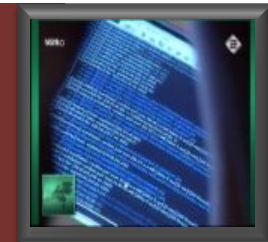
CYBER THREATS ALSO EVOLVING



Large scale, wide spreading incident
(e.g. virus, worm outbreak)



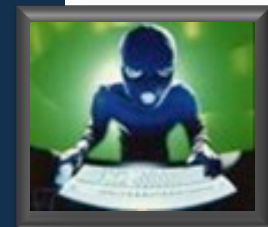
Specific targeted attack, powerful tool
(e.g. Botnet, Stuxnet)



Script kiddies, crackers



Professionals, Criminals



Motivation: for fun, peer recognition, prestige



Specific Motivation: for economic gain, industrial espionage, cyber terrorism



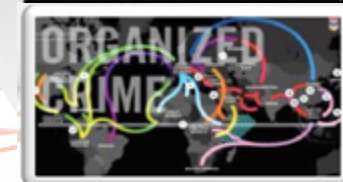
The More We're Interconnected To The Cyber Space, The More We Are At Risk To Cyber Threats ...

TREND OF MALAYSIA CYBER SECURITY THREATS IN 2016 - 2017 (AS OF 30 SEPTEMBER 2017)



14,608

Cyber Security
Incidents
Reported



FRAUD!



5,353,050

Malware & Botnet Drones
Infections

Info: www.mycert.my

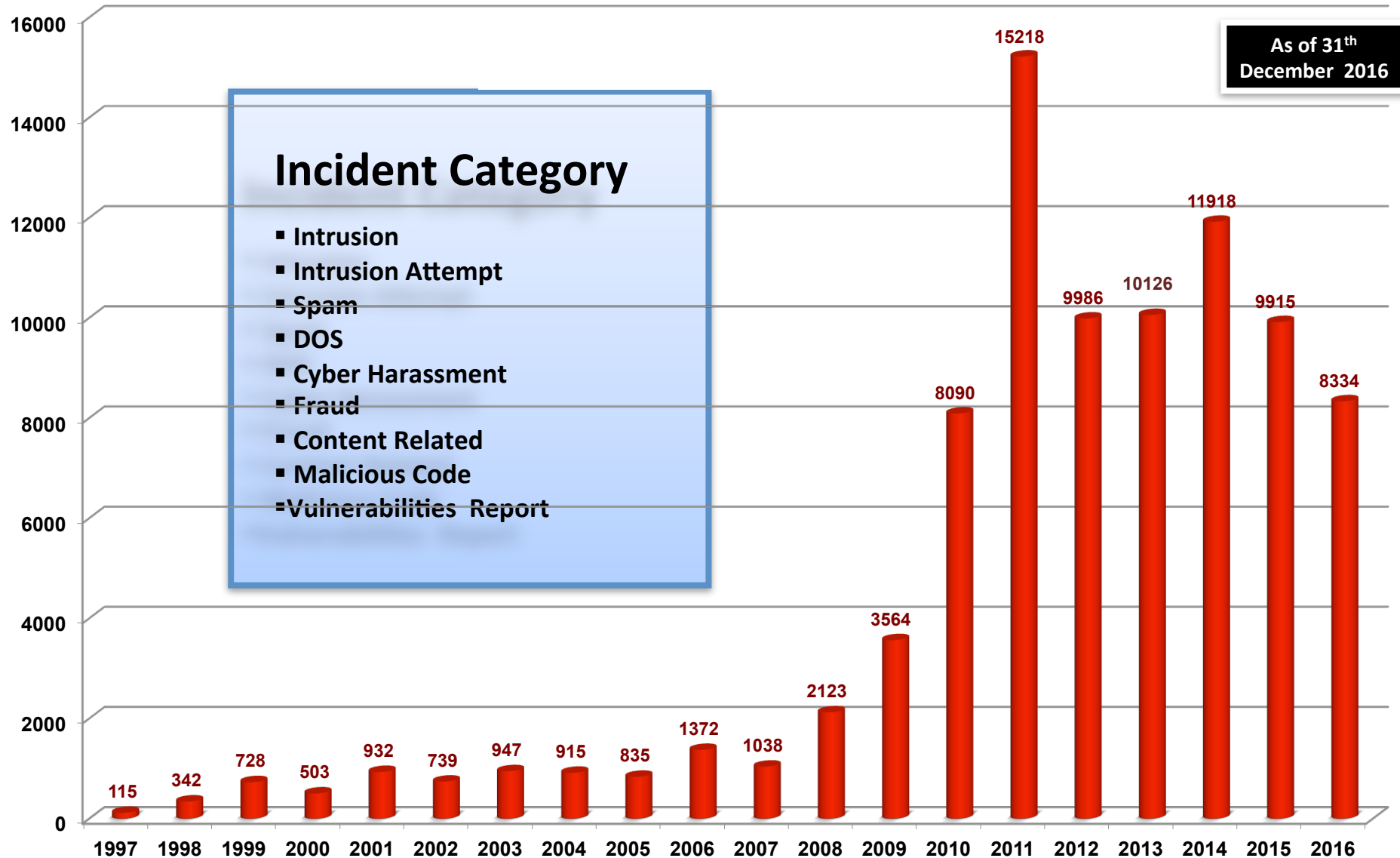


1,580,014

Spam Emails



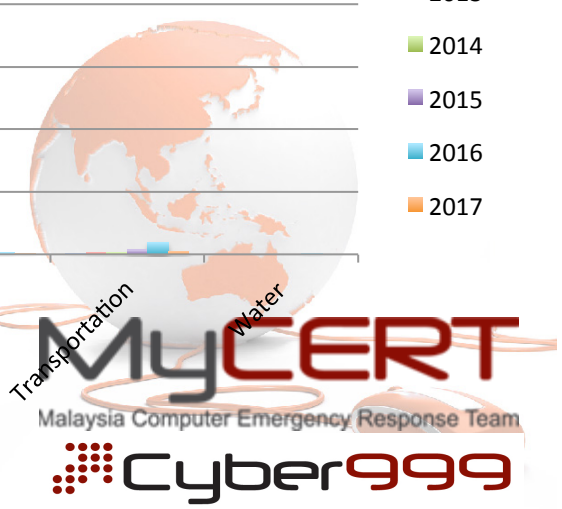
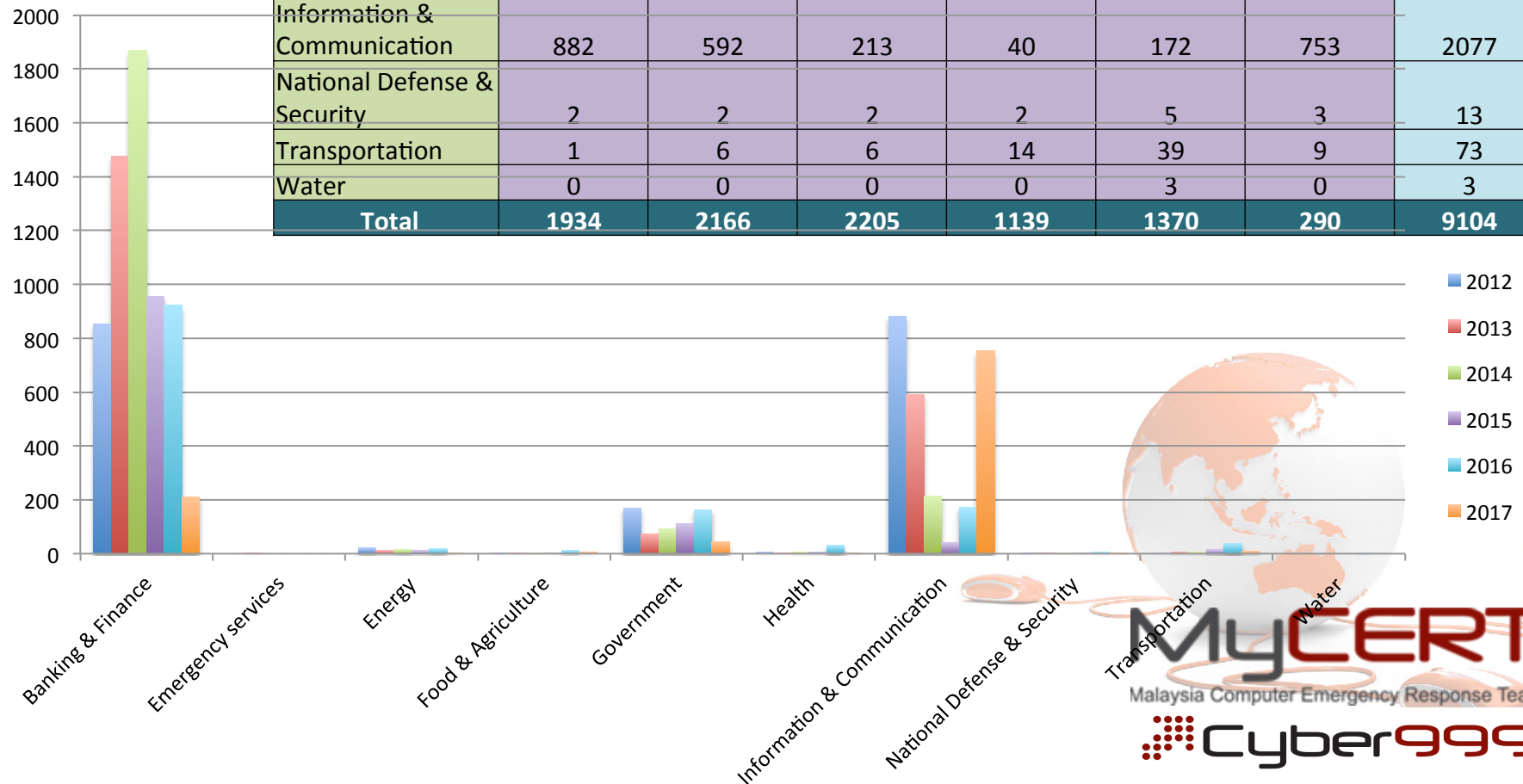
CYBER SECURITY INCIDENT (1997 – 2016)



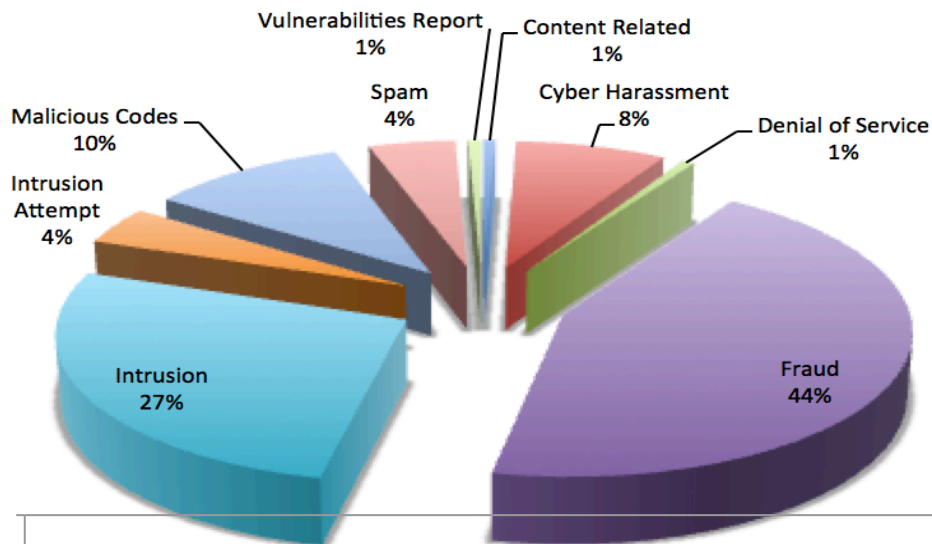
CYBER INCIDENTS BY SECTOR (2012-2017)

	2012	2013	2014	2015	2016	2017	TOTAL
Banking & Finance	852	1476	1868	954	922	211	6156
Emergency services	0	1	0	0	0	0	1
Energy	21	12	17	11	19	4	81
Food & Agriculture	1	1	1	2	13	5	20
Government	170	74	92	110	164	45	625
Health	5	2	6	6	33	4	55
Information & Communication	882	592	213	40	172	753	2077
National Defense & Security	2	2	2	2	5	3	13
Transportation	1	6	6	14	39	9	73
Water	0	0	0	0	3	0	3
Total	1934	2166	2205	1139	1370	290	9104

Source : www.mycert.org.my



Incident Reported 2017



Top 3 incidents:

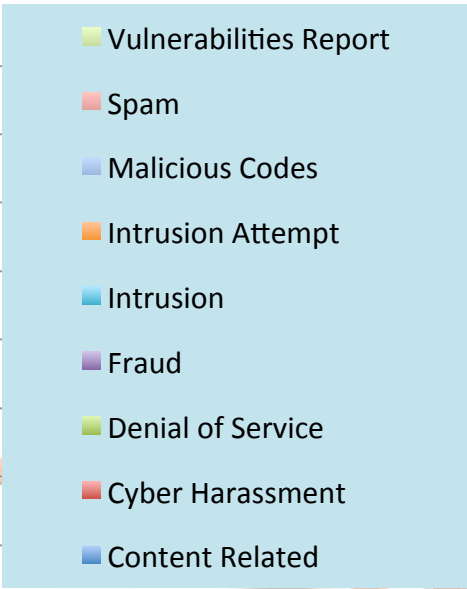
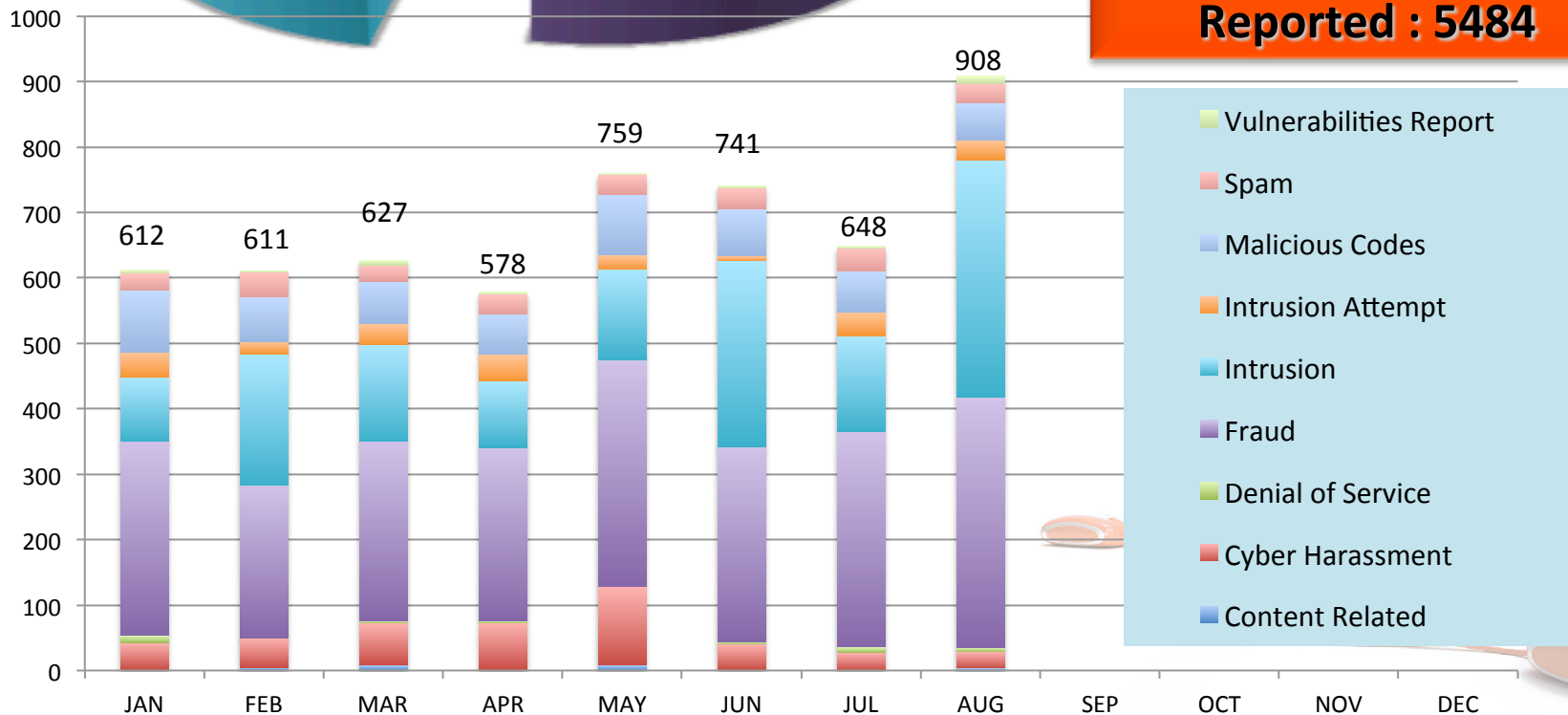
1. Fraud

2. Intrusion

3. Malicious Code

Total Incident Reported : 5484

Source : www.mycert.org.my



As Malaysia's economy goes high tech, so do cyber threats

Friday, 2 June 2017, 10:52 AM

NEW STRAITS TIMES

NEWS BUSINESS LIFESTYLE SPORTS WORLD OPINION PROPERTY

Malaysian hackers busted after RM30,000 online shopping spree

Cyber threats on the rise in Malaysia



Monday, July 24th, 2017 at , News



By NG MIN SHEN

The country's internet security agencies and experts are enhancing Malaysia's defence against the threat of cyber criminals.

Science, Technology and Innovation (Mosti) Deputy Minister Datuk Wira Dr Abu Bakar Mohamad Diah said cyber crimes including fraud, hacktivism, online scams, espionage and harassment have been on the rise over the last decade.



Malaysia

Cyber Security Incident (1 Jan -30 Sept 2017)

Cyber Security Incident	Jan	Feb	Mar	Apr	May	June	July	Aug	Sept	Total
Content Incidents:										
Fraud	296	233	274	265	346	298	329	382	466	2889
Cyber Harassment	41	45	64	71	119	39	27	25	32	463
Content Related	2	5	9	2	9	2	1	4	2	36
Technical Incidents:										
Intrusion Attempt	39	19	32	41	22	8	37	31	8	237
Intrusion	98	201	148	101	138	284	146	363	181	1660
Malicious Code	94	68	65	62	92	71	62	56	64	634
Spam	26	38	24	30	31	32	36	30	29	276
DDoS	11	0	3	3	1	3	8	6	2	37
Vulberabilities	5	2	8	3	1	4	2	11	6	42
Total	612	611	627	578	759	741	648	908	790	6274



MALAYSIANS ARE VULNERABLE TO CYBER FRAUDS

One in three Malaysian internet users have personally experienced cybercrime in the past year - *Norton Cybersecurity Insights Report 2016*

Friday, 11 March 2016 | MYT 2:48 PM

Malaysia is the most vulnerable country to internet scams in this region

FACEBOOK TWITTER GOOGLE+ LINKEDIN

mStar

UTAMA HIBURAN BERITA NIAGA SUKAN KOLUMNIS LAIN-LAIN MSTAR.TV

Utama > Berita > Berita Jenayah > Kes Jenayah Siber

f t G+ Print Email

Kes Penipuan Dalam Talian Meningkat - Madius

Diterbitkan: Selasa, 7 Februari 2017 1:36 PM

Biggest credit card syndicate in Malaysia foiled

Mariah Ahmad, Astro Awani | April 19, 2016 17:00 MYT

Saturday, 26 March 2016

RM1bil lost to online scammers

BY FARIK ZOLKEPLI and AUSTIN CAMOENS

FACEBOOK TWITTER GOOGLE+ LINKEDIN

Fraud makes up almost 50% of cyber crimes, says MyCERT

Posted on 2 June 2016 - 02:33pm
Last updated on 2 June 2016 - 03:47pm
Lee Choon Fai

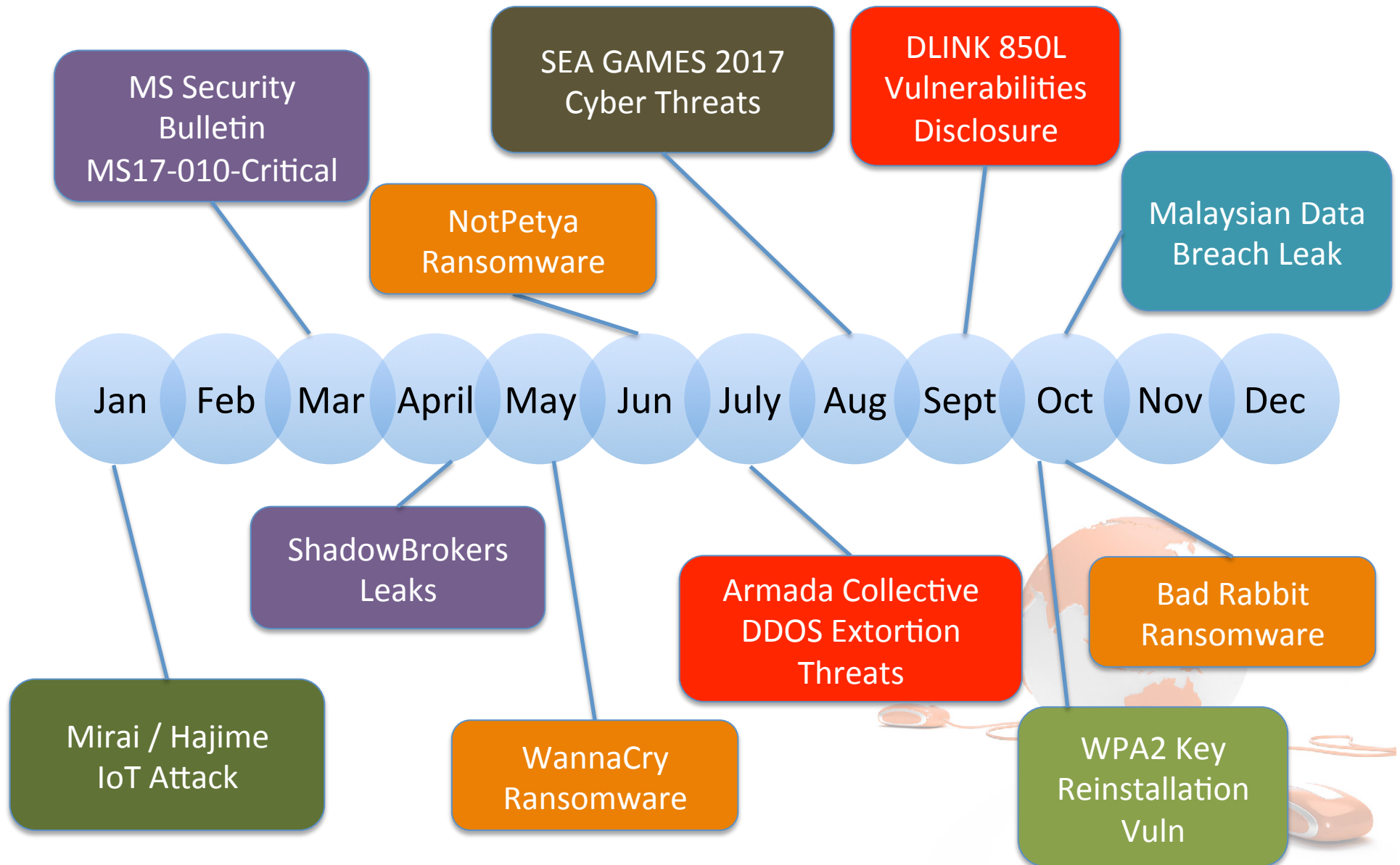
SHARE f t +1 Print

Kerugian RM70.1 juta dalam tempoh dua tahun akibat African Scam

1,095 mangsa penipuan cinta siber

crime reported in the first quarter of 2016 involves fraud, agency and Response Team (MyCERT) disclosed at the

What we have seen in year 2017



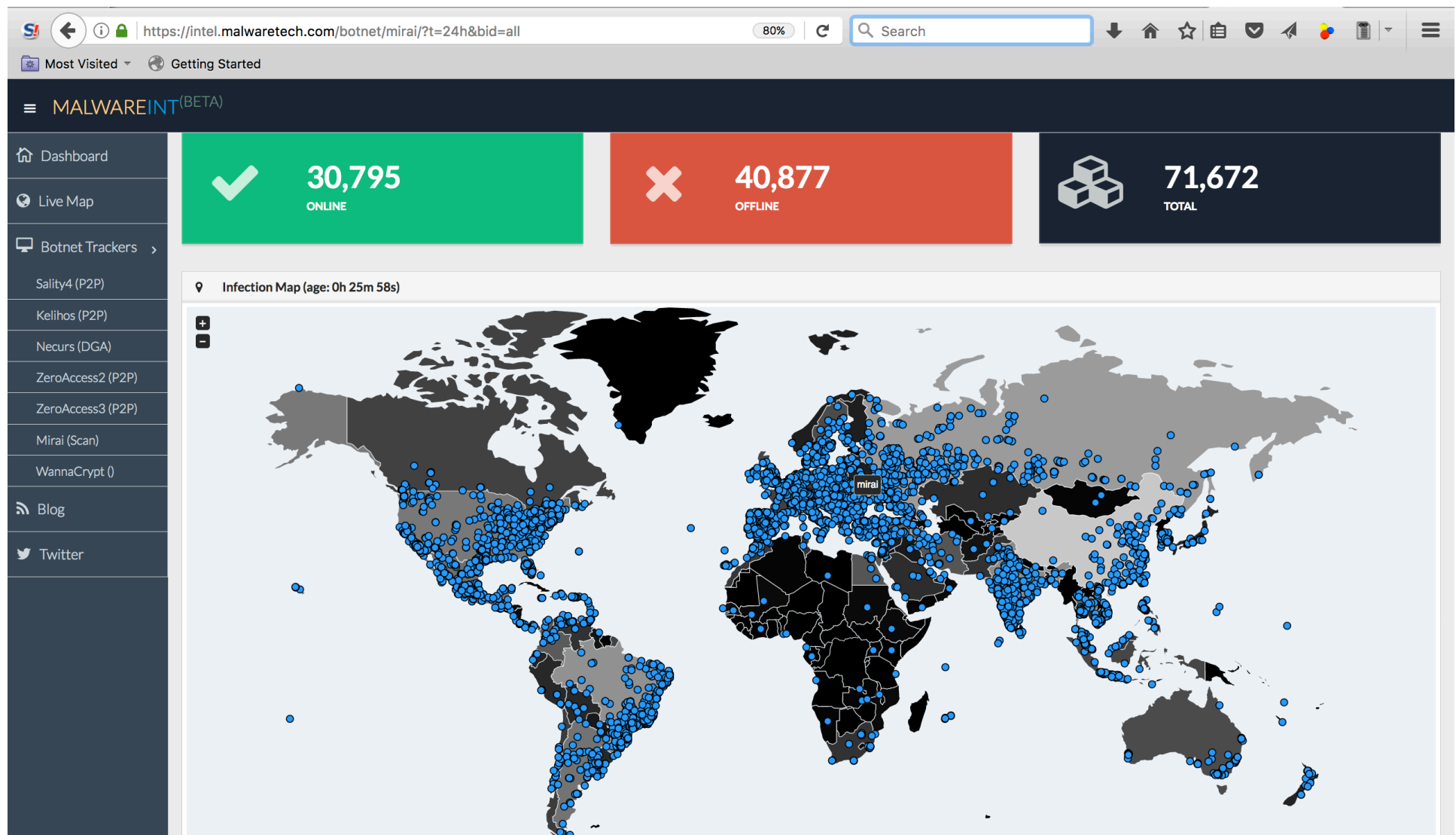


CASE STUDY

IoT Threats



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 water torture	Recursive DNS query attack
SYN	SYN packet flood
ACK	ACK packet flood
STOMP	ACK flood with STOMP
GRE IP	GRE flood
GRE Ethernet	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/8888888       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/12345        guest/12345       guest/guest
administrator/1234 666666/666666    admin1/password
ubnt/ubnt         root/klv1234      888888/888888
root/hi3518       root/klv1234      root/Zte521
root/zlxx.        root/jvbzd        root/anko
root/system       root/7ujMko0vizxv root/7ujMko0admin
root/user         root/ikwb         root/dreambox
admin/1111111     root/realtek      root/00000000
admin/54321       admin/1234        admin/12345
admin/1234        admin/123456     admin/7ujMko0admin
tech/tech        admin/pass       admin/meinsm
mother/fu r

```

Mirai's built-in password dictionary.

The passwords come from the botnet's source code

Botnet Infection (Mirai) – Feeds ShadowsServer

timestamp	ip	port	asn	geo	region	city	type	infection	cc_port	sector
06/10/16 20:34		59618	4788	MY	SELANGOR	BATU CAVES	tcp	mirai	23	Communications
06/10/16 20:34		44890	4788	MY	JOHOR	JOHOR BAHRU	tcp	mirai	2323	Communications
06/10/16 20:34		49327	4788	MY	PULAU PINANG	BAYAN LEPAS	tcp	mirai	23	Communications
06/10/16 20:34		43219	4788	MY	SELANGOR	PETALING JAYA	tcp	mirai	23	Communications
06/10/16 20:34		39140	4788	MY	SELANGOR	PETALING JAYA	tcp	mirai	23	Communications
06/10/16 20:34		44395	38322	MY	JOHOR	JOHOR BAHRU	tcp	mirai	23	Communications
06/10/16 20:34		47455	4788	MY	SELANGOR	KLANG	tcp	mirai	23	Communications
06/10/16 20:34		30351	4788	MY	SELANGOR	BATU CAVES	tcp	mirai	23	Communications
06/10/16 20:34		44379	9930	MY	WILAYAH PERSEKUTUAN KUALA LUMPUR	KUALA LUMPUR	tcp	mirai	23	Communications
06/10/16 20:34		34479	4788	MY	WILAYAH PERSEKUTUAN KUALA LUMPUR	KUALA LUMPUR	tcp	mirai	23	Communications
06/10/16 20:34		35367	4788	MY	SELANGOR	PETALING JAYA	tcp	mirai	23	Communications
06/10/16 20:34		6561	4788	MY	SELANGOR	PETALING JAYA	tcp	mirai	23	Communications
06/10/16 20:34		46603	4788	MY	PULAU PINANG	BUKIT MERTAJAM	tcp	mirai	23	Communications
06/10/16 20:34		63906	4788	MY	PULAU PINANG	LORONG SERI AMAN 3 - 5	tcp	mirai	23	Communications
06/10/16 20:34		38887	4788	MY	PULAU PINANG	LEBUH DOWNING	tcp	mirai	23	Communications
06/10/16 20:34		13365	38322	MY	SELANGOR	SERI KEMBANGAN	tcp	mirai	23	Communications
06/10/16 20:34		16829	4788	MY	PULAU PINANG	BUKIT MERTAJAM	tcp	mirai	23	Communications
06/10/16 20:34		2953	4788	MY	SELANGOR	KAJANG	tcp	mirai	23	Communications
06/10/16 20:34		24143	4788	MY	WILAYAH PERSEKUTUAN KUALA LUMPUR	KUALA LUMPUR	tcp	mirai	23	Communications
06/10/16 20:34		33837	4788	MY	JOHOR	JOHOR BAHRU	tcp	mirai	23	Communications
06/10/16 20:34		55026	4788	MY	SELANGOR	BATU CAVES	tcp	mirai	23	Communications
06/10/16 20:34		64299	4788	MY	SELANGOR	SHAH ALAM	tcp	mirai	23	Communications
06/10/16 20:34		19866	4788	MY	WILAYAH PERSEKUTUAN KUALA LUMPUR	KUALA LUMPUR	tcp	mirai	2323	Communications
06/10/16 20:34		30232	45960	MY	SELANGOR	RAWANG	tcp	mirai	23	Communications
06/10/16 20:34		52553	4788	MY	SELANGOR	PUCHONG	tcp	mirai	23	Communications
06/10/16 20:34		42098	4788	MY	WILAYAH PERSEKUTUAN KUALA LUMPUR	KUALA LUMPUR	tcp	mirai	23	Communications
06/10/16 20:34		38318	4788	MY	WILAYAH PERSEKUTUAN KUALA LUMPUR	KUALA LUMPUR	tcp	mirai	23	Communications
06/10/16 20:34		51511	132435	MY	SELANGOR	SHAH ALAM	tcp	mirai	23	Communications
06/10/16 20:34		31311	4788	MY	WILAYAH PERSEKUTUAN KUALA LUMPUR	KUALA LUMPUR	tcp	mirai	23	Communications
06/10/16 20:34		6820	4788	MY	PULAU PINANG	PERAI	tcp	mirai	23	Communications
06/10/16 20:34		50892	4788	MY	NEGERI SEMBILAN	SEREMBAN	tcp	mirai	23	Communications
06/10/16 20:34		34145	4788	MY	SELANGOR	PETALING JAYA	tcp	mirai	23	Communications



Automation of escalation

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

Article #95 – () 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: ()
 Cc: cyber999@cybersecurity.my
 Signed: Good PGP signature. (Malaysia Computer Emergency Response Team (MyCERT) <cyber999@cybersecurity.my> : 82B6ED71 : 57CDC6891B0E08353BBDAF97D010057082B6ED71)
 Subject: () Botnet Drones daily report on 02-02-2017.
 Attachment: mirai.4788.txt , 659.1 KBytes

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

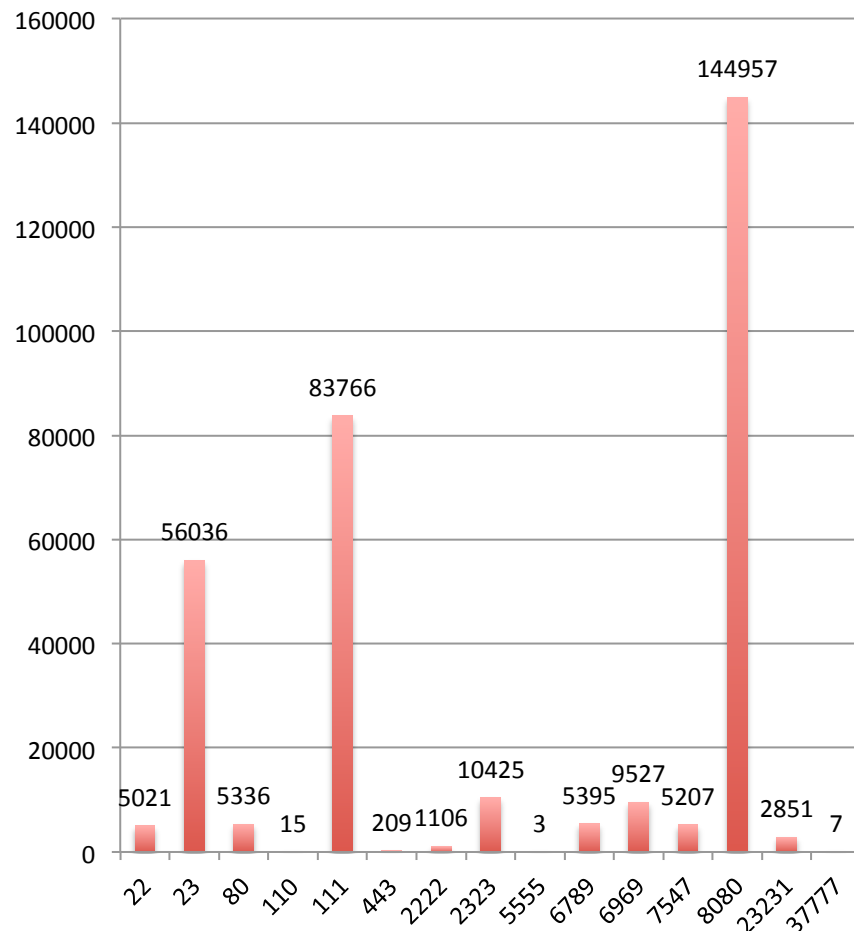
Dear Abuse Team,
 MyCERT received a report from ()
 report on malware, botnet acti
 discovery of a list of all the
 able to capture from the monit
 connections to HTTP botnets, o
 infection type, and these will
 23, , , , , , , , , , 518210,737
 We are contacting you regardin
 APNIC whois database. If you a
 can relay this message by forw

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	8.22,20359,						MY,JOHOR,JOHOR BAHRU,	tcp,mirai,	6789,			0,0,							Communications,		
2017-02-02 00:00:01,60,	245,5410,47						WILAYAH PERSEKUTUAN KUALA LUMPUR,KUALA LUMPUR,	tcp,mirai,	23,			0,0,							Communications,		
2017-02-02 00:00:01,118	119,38935,						MY,SELANGOR,PETALING JAYA,	tcp,mirai,	2323,			0,0,							Communications,		
2017-02-02 00:00:01,110	0.5,10792,4						Y,SARAWAK,MIRI,	tcp,mirai,	6789,			0,0,							Communications,		
2017-02-02 00:00:01,60,	35,58888,4						Y,WILAYAH PERSEKUTUAN KUALA LUMPUR,KUALA LUMPUR,	35.133.50.60.jb02-home.tm.net.my,	tcp,mirai,												
2017-02-02 00:00:01,60,	235,20927,4						Y,SARAWAK,KUCHING,	tcp,mirai,	23,			0,0,							Communications,		
2017-02-02 00:00:01,60,	29,51910,4						Y,SELANGOR,JALAN TASIK SELATAN,	tcp,mirai,	23,			0,0,							Communications,		
2017-02-02 00:00:01,60,	4,38333,47						SELANGOR,PETALING JAYA,	tcp,mirai,	23,			0,0,							Communications,		
2017-02-02 00:00:01,175	6.196,15508						MY,SELANGOR,JALAN TASIK SELATAN,	tcp,mirai,	23,			0,0,							Communications,		
2017-02-02 00:00:01,210	7.22,25228						MY,PULAU PINANG,BUTTERWORTH,	tcp,mirai,	23231,			0,0,							Communications,		
2017-02-02 00:00:01,175	0.7,47877,4						Y,SELANGOR,KAJANG,	tcp,mirai,	23,			0,0,							Communications,		
2017-02-02 00:00:01,175	24.32,22405						MY,PULAU PINANG,BUKIT MERTAJAM,	tcp,mirai,	23,			0,0,							Communications,		
2017-02-02 00:00:01,118	39,13863,4						Y,SELANGOR,PETALING JAYA,	tcp,mirai,	23,			0,0,							Communications,		
2017-02-02 00:00:01,115	02.64,1024,						MY,SELANGOR,PETALING JAYA,	tcp,mirai,	23,			0,0,							Communications,		
2017-02-02 00:00:01,60,	54,25871,4						Y,SELANGOR,KLANG,	54.104.50.60.kli03-home.tm.net.my,	tcp,mirai,												
2017-02-02 00:00:01,175	34.223,5222						8,MY,SELANGOR,PETALING JAYA,	tcp,mirai,	23,			0,0,							Communications,		
2017-02-02 00:00:01,203	7.53,22456,						MY,WILAYAH PERSEKUTUAN KUALA LUMPUR,KUALA LUMPUR,	kli-97-53.tm.net.my,	tcp,mirai,												
2017-02-02 00:00:01,118	0.198,12942						MY,SARAWAK,KUCHING,	tcp,mirai,	6789,			0,0,							Communications,		
2017-02-02 00:00:01,175	204,57521,						MY,SELANGOR,KAJANG,	tcp,mirai,	6789,			0,0,							Communications,		
2017-02-02 00:00:01,124	1.164,9331,						MY,SELANGOR,PETALING JAYA,	tcp,mirai,	6789,			0,0,							Communications,		
2017-02-02 00:00:01,115	6.220,13400						MY,SELANGOR,PETALING JAYA,	tcp,mirai,	23,			0,0,							Communications,		
2017-02-02 00:00:01,175	00.94,20580						MY,JOHOR,JOHOR BAHRU,	tcp,mirai,	23,			0,0,							Communications,		
2017-02-02 00:00:01,210	09.94,65159						MY,SELANGOR,PUCHONG,	tcp,mirai,	23,			0,0,							Communications,		
2017-02-02 00:00:01,175	8.203,60448						MY,PULAU PINANG,BAYAN LEPAS,	tcp,mirai,	6789,			0,0,							Communications,		
2017-02-02 00:00:01,175	1.152,34456						MY,JOHOR,JOHOR BAHRU,	tcp,mirai,	23,			0,0,							Communications,		

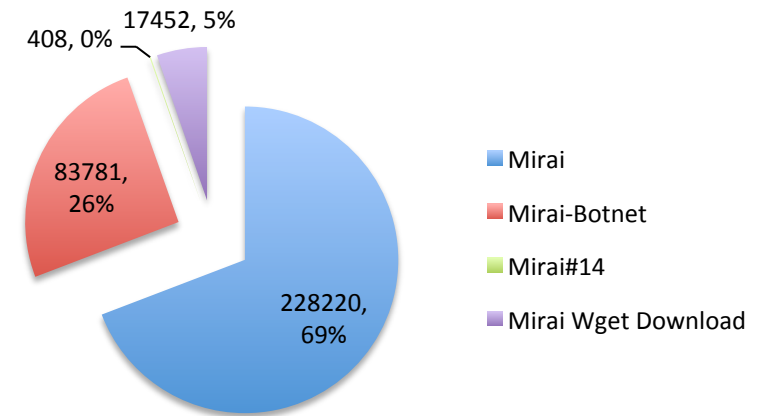


Security Feeds Information

Mirai infection CC-Port Scan Detected
Jan - April 2017



Infection Type by Variant

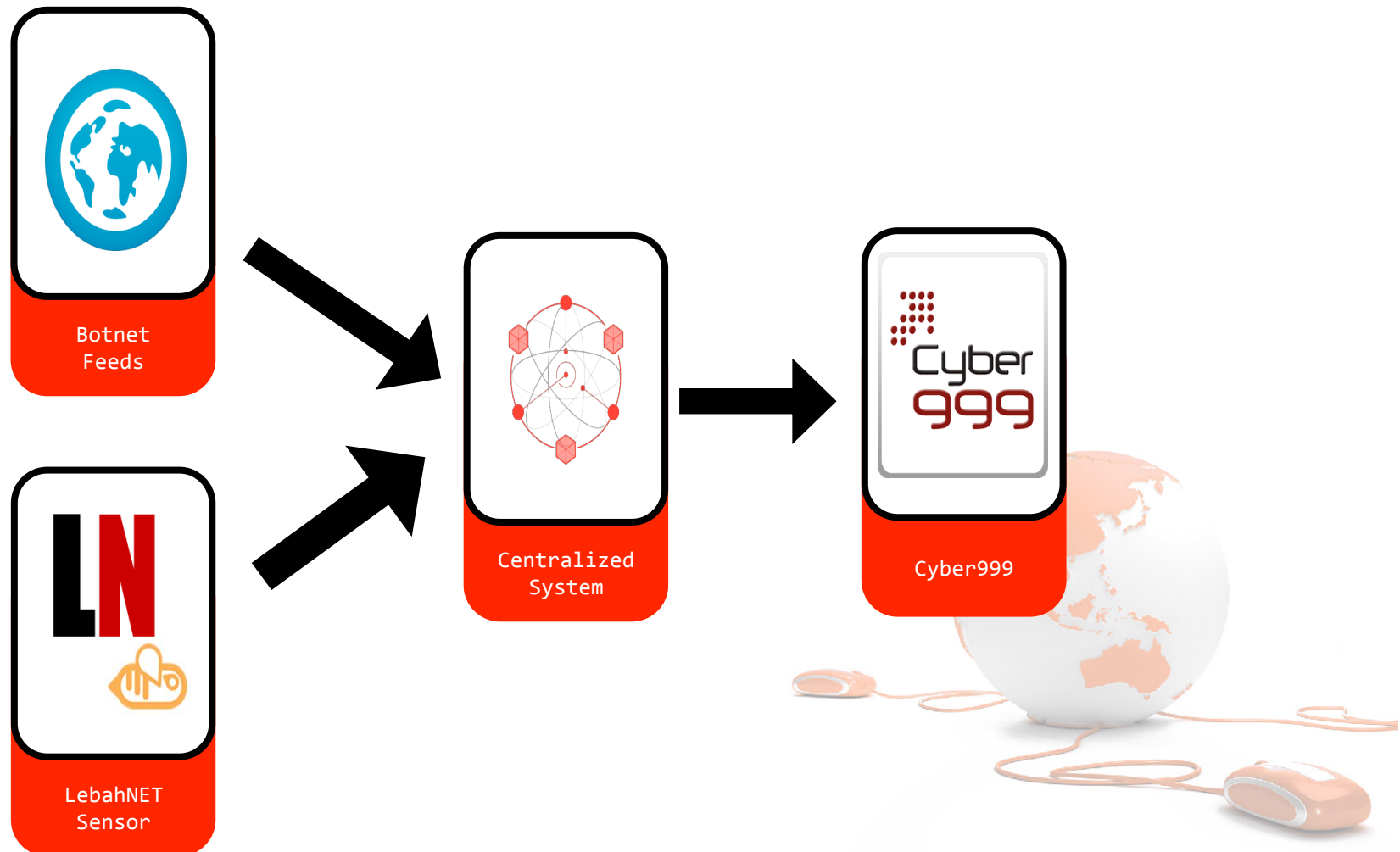


Count

Year	Total Mirai Infection
2016	149335
2017	305740



Automated Escalation Process





Ransomware



WHAT IS IT?

Ransomware is a serious security threat that has **data-kidnapping** capabilities. It limits access to files or system functions, or even render systems totally useless. Then it forces victims to **pay ransom** to regain access to their files/systems.

WHY IS IT A SECURITY THREAT?

Ransomware is no longer just a scareware. From when it was first sighted, it has gone a long way from just issuing empty threats. It is now known for its sophisticated **file-encrypting ability**.

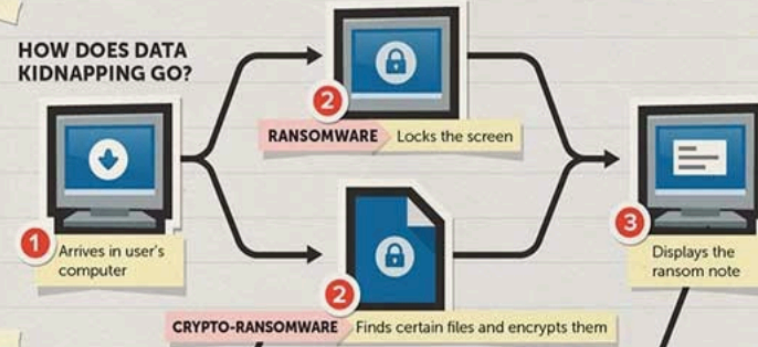


Source infographic: www.pinterest.com

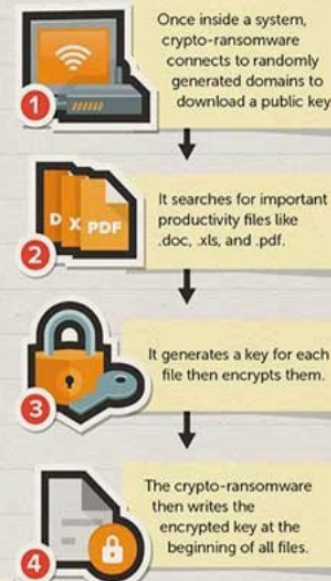
You can be infected when you unknowingly download ransomware from



HOW DOES DATA KIDNAPPING GO?



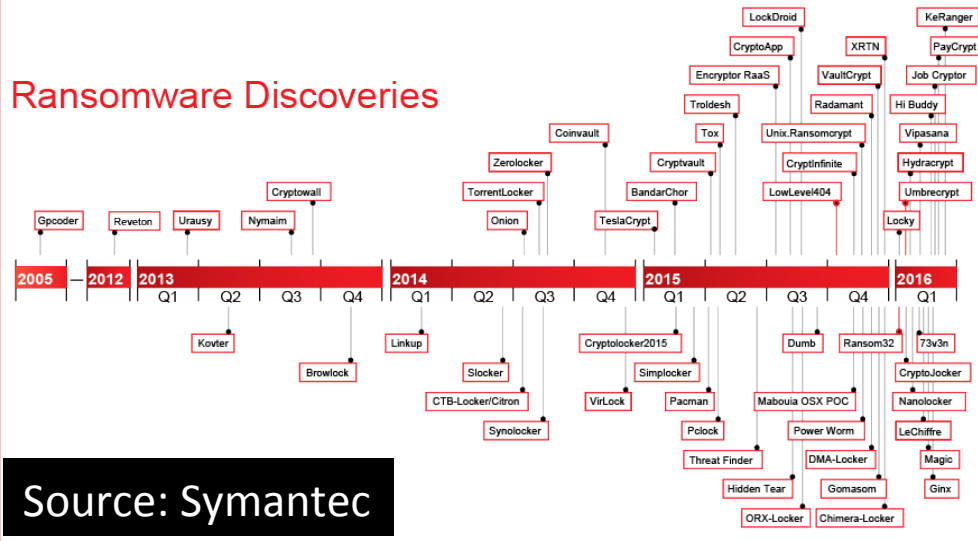
HOW DOES THE FILE ENCRYPTION WORK?



HOW IS THE RANSOM PAID?

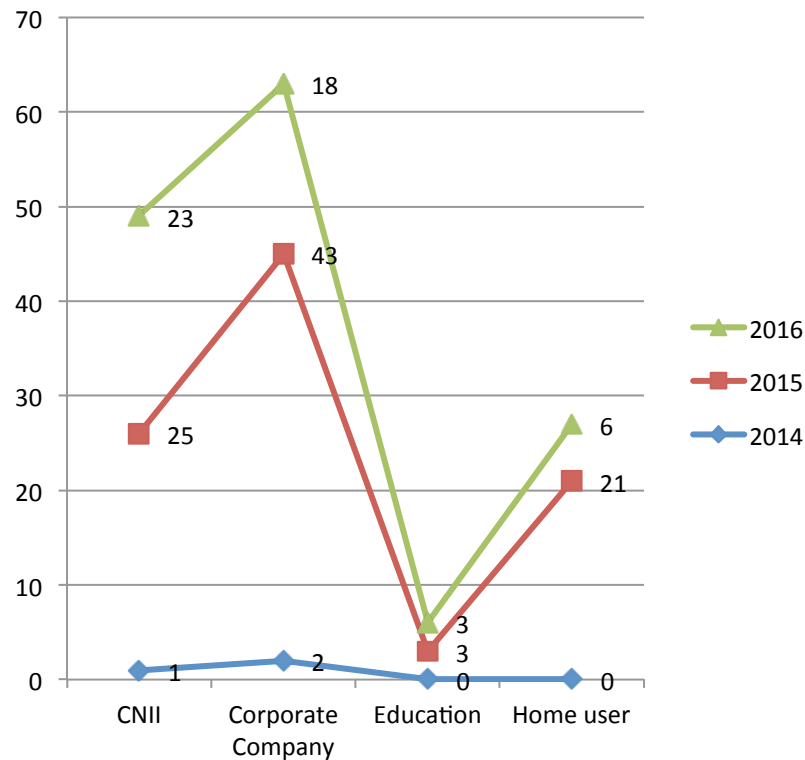


Ransomware Discoveries



Source: Symantec

Ransomware statistic and footprint – Reported to CSM: Cyber999 (2014-2016)



Year	# of incidents
2014	3
2015	92
2016	80
2017 (as of September)	111

Observed ransomware	Date detected / reported
CryptoLocker	9 October 2013
CryptoWall	7 August 2014
CTB-Locker	24 January 2015
TeslaCrypt	15 April 2015
TorrentLocker	19 April 2015
Locker v5.30	25 May 2015
AlphaCrypt	2 Jun 2015
Cerber	31 March 2016
Locky	18 March 2016
Troldesh (Shade or XTBL)	23 May 2016
UltraCrypter	31 May 2016
.777 Ransomware	2 June 2016

The situation with WannaCry / Wcry / WannaCrypt

Wana Decrypt0r 2.0



Ooops, your files have been encrypted!

English

What Happened to My Computer?

Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time. You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever. We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window. After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Payment will be raised on

5/17/2017 16:59:56

Time Left

02: 23: 59: 15

Your files will be lost on

5/21/2017 16:59:56

Time Left

06: 23: 59: 15

Send \$300 worth of bitcoin to this address:

115p7UMMngo1pMvvpHijcRdfJNXj6LrLn

Copy

[About bitcoin](#)

[How to buy bitcoins?](#)

Contact Us

Check Payment

Decrypt



What Happened?



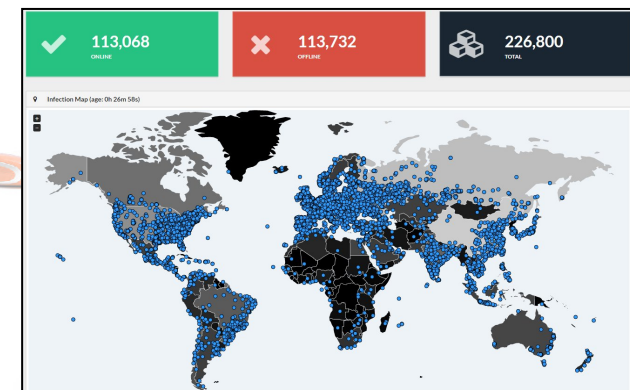
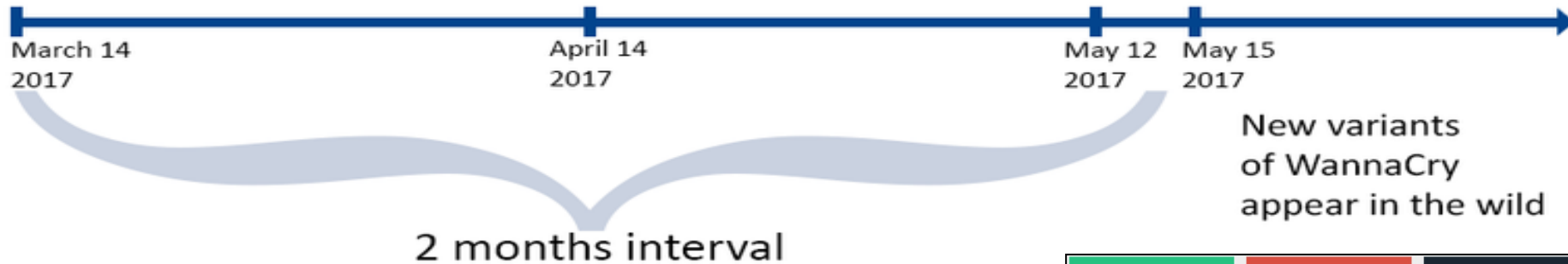
Microsoft Security Bulletin MS17-010 - Critical



ShadowBrokers leak



WannaCry 2.0 ransomware outbreak started appearing in the wild.



Malware tracking by MalwareTech



What to do if infected?

1

Immediately isolate **infected system from the network**

- Temporary disable all network shared drives in the network

2

Alert/report to **CSM / Cyber999**

3

Backup all **.WNCRY files** on the hard drive for offline usage once the decryption keys are available. The decryption process can apply to restore the files .

Used undelete software to recover encrypted files.

4

Install an anti-ransomware software removal tools suggested: Windows Defender, Microsoft Safety Scanner, reputable Antivirus removal tools, scan the infected system and clean it.

5


Reinstall the **Windows OS** with latest patch.

Restore from the last backup. If any backup available.


Alert and Advisory (WannaCry)



<https://www.mycert.org.my/assets/xml/news.rss>



KEMENTERIAN SAINS, TEKNOLOGI DAN INOVASI



CyberSecurity
MALAYSIA
An agency under MOSTI

MEDIA RELEASE

**13 May 2017
FOR IMMEDIATE RELEASE**


**CYBERSECURITY MALAYSIA ISSUES ALERT ON
'WANNACRY RANSOMWARE'**

SERI KEMBANGAN (13 MAY 2017) – CyberSecurity Malaysia, the national cyber security specialist agency under the Ministry of Science, Technology, and Innovation (MOSTI), today issued an alert on ransomware attack known as 'WanaCrypt0r 2.0'.

The ransomware uses a vulnerability first revealed to the public as part of a leaked stash of NSA-related documents to infect Windows PCs and encrypt their contents before demanding a ransom for the key to decrypt the encrypted files. The co-ordinated attack had managed to infect large numbers of computers across the health service around the world after it was first noticed by security researchers on 12 May 2017, in part due to its ability to spread within networks from PC to PC.

According to Dato' Dr. Haji Amirudin Abdul Wahab, Chief Executive Officer, CyberSecurity Malaysia, the ransomware attack used Server Message Block (SMB) exploit leaked by the Shadow Brokers. The malware may spread to vulnerable systems through a security hole in Windows that has been recently patched by Microsoft. In view of this attack, we have recently released an advisory alert to highlight steps and suggestion to address Shadow Brokers exploits.

"In the meantime, we would like to urge system administrators to patch their systems as soon as possible and keep their users aware of the new ransomware in order to prevent them to open suspicious emails/files. Currently, CyberSecurity Malaysia is monitoring the situation of the ransomware attack in Malaysia and will take necessary action by providing technical assistance to the affected organizations and individual users on remediation and preventions through our Cyber999 service" added Dato' Dr. Amirudin.




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
M 1 300 88 2999
www.cybersecurity.my




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
M 1 300 88 2999
www.cybersecurity.my

Securing Our Cyberspace



KEMENTERIAN SAINS, TEKNOLOGI DAN INOVASI



CyberSecurity
MALAYSIA
An agency under MOSTI

SIARAN MEDIA


**16 MEI 2017
UNTUK SIARAN SEGERA**

PERKEMBANGAN ISU 'RANSOMWARE WANNACRY'


SERI KEMBANGAN (16 MEI 2017) - CyberSecurity Malaysia, agensi pakar keselamatan siber nasional di bawah Kementerian Sains, Teknologi dan Inovasi (MOSTI) ingin memaklumkan perkembangan semasa mengenai serangan 'Ransomware WannaCry' yang melanda dunia pada 12 Mei 2017.

Perkembangan adalah seperti berikut: -

- CyberSecurity Malaysia telah menerima satu (1) laporan rasmi daripada institusi akademi dan beranggapan bahawa terdapat lebih banyak insiden yang tidak dilaporkan.
- Kami ingin menggesa semua organisasi (pentadbir sistem) untuk berwaspada dan meneruskan tindakan yang perlu untuk melindungi dan menjamin infrastruktur rangkaian mereka daripada terjejas;
- Pentadbir sistem digesa untuk *patch* sistem komputer mereka dan mengingatkan pengguna mereka agar sentiasa berwaspada mengenai serangan Ransomware baharu untuk menghalang mereka daripada memetik (klik) pautan yang dihantar bersama e-mel yang mencurigakan / fail.
- Orang awam boleh merujuk kepada amaran serta nasihat CyberSecurity Malaysia menerusi laman web korporat di bawah MyCERT sebagai langkah pencegahan:-
<https://www.mycert.org.my/en/services/advisories/mycert/2017/main/detail/1263/index.html>
- Kami ingin menggesa orang ramai (organisasi dan pengguna individu) untuk melaporkan apa jua serangan Ransomware kepada CyberSecurity Malaysia dengan menghubungi pusat bantuan Cyber999. Laporan boleh dilakukan melalui saluran berikut:
 - E-mel: cyber999@cybersecurity.my atau mycert@mycert.org.my



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
M 1 300 88 2999
www.cybersecurity.my



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
M 1 300 88 2999
www.cybersecurity.my

Securing Our Cyberspace

MyCERT Advisories

2017201620152014201320122011201020092008200720062005
2004200320022001200019991998

MyCERT Advisories, Alerts and Summaries for the year 2017

MA-661.052017: MyCERT Alert – WannaCry Ransomware

Date first published: 13/5/2017

1.0 Introduction
MyCERT is aware of the outbreak of a ransomware called as WannaCry. This ransomware is also referenced online under various names – 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. Victims got infected through emails that contains malicious attachment. Once the ransomware infected a system, the malware scans and infects other vulnerable systems within the network.

It exploits a vulnerability found in Windows, known as EternalBlue, that Microsoft patched in March (MS17-010). The vulnerability is in the Windows Server Message Block (SMB) service.

- <https://technet.microsoft.com/en-us/library/security/ms17-010.aspx>

2.0 Impact

- Files on infected computer are encrypted and the owner is unable to access the files until a ransom of \$300 worth of Bitcoin is paid.
- Individuals and organizations are discouraged from paying the ransom, as this does not guarantee access will be restored. Figure 1 shows the ransomnote found on infected computer. Figure 2 shows the text file created by the ransomware that

http://www.cybersecurity.my/data/content_files/44/1674.pdf

http://www.cybersecurity.my/data/content_files/44/1680.pdf

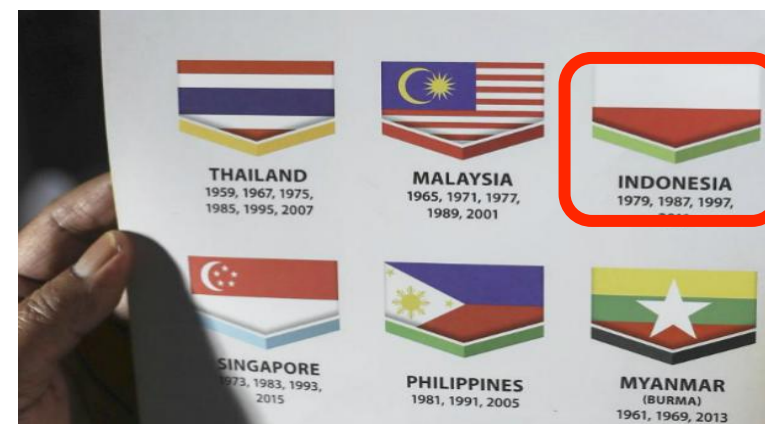
<https://www.mycert.org.my/en/services/advisories/mycert/2017/main/detail/1263/index.html>





OPs BENDERA

- Flag blunder in the Kuala Lumpur SEA Games souvenir booklet (escalated to cyber attack)
- Cyber999 received incident (from 20 August)
- Type of cyber attack:-
 - 1) Web Defacement
 - 2) Confidential Info Leak
 - 3) Distributed Denial of Service (DDOS) attacked



TRENDS OF HACKTIVISM IN MALAYSIA

- Traditional conflicts are spread into cyberspace



Tech News

Monday, 21 August 2017 | MYT 1:58 PM

Indonesian hacker group defaces Malaysian websites following flag blunder



Indonesia: Hackers deface Malaysian websites after SEA Games flag blunder



Government Websites Hacked - Again

Published on Thursday, 02 January 2014 10:29



KUALA LUMPUR: Hackers launched a slew of websites in Malaysia last night, at least two government portals on New Year's Eve.

The Education Ministry(MOE) portal appeared to be replaced with a plain black background which said "Hacked", with one "EvilShade" claiming responsibility.

At the time of writing, the MOE website was inaccessible, though various screen captures depicting the defacement was posted on social media.

33 Malaysian websites hacked following SEA Games error: Experts reaffirm security musts for Sysadmins

Malaysian websites and internet services have been defaced in what is believed to be a hacktivism attack following an error in the official souvenir booklet of the Kuala Lumpur SEA Games 2017.

By AvantiKumar
Aug. 23, 2017





Nasib Puluhan Website Malaysia yang Kena Retas Hacker Karena Insiden Bendera Terbalik di SEA Games



27 Malaysian Websites Hacked After Indonesian Flag Wrongly Printed in SEA Games Booklet



Media Release and Alert (SEA GAMES KL)

MEDIA STATEMENT

21 August 2017

ATTACKS ON MALAYSIAN WEBSITES AND INTERNET SERVICES

CyberSecurity Malaysia, the national cyber security specialist and technical agency has been receiving several incidents targeting Malaysian websites, confidential information leaks and possible Distributed Denial of Services (DDoS) attacks.


The incident is real and we are doing the investigation, monitoring and working closely with other agencies to mitigate this incident.


As of today, 21 August 2017 (3.40pm), a total of 33 Malaysian sites have been defaced.

For preventive measure, we have released an alert to advise System Administrators to take necessary steps to secure their systems against unwanted incidents as well from other security threats.

Some advises are as follows:

- Organizations are recommended to apply defense in depth strategy to protect their networks. Make sure systems, applications and third party add-ons are updated with latest upgrades and security patches.
- If you're running on older versions of operating systems or software, kindly ensure that they are upgraded to the latest versions - older versions may have some vulnerability that can be manipulated by intruders.
- Please make sure that your web based applications and network based appliances are patched accordingly.
 - You may refer to your respective vendors' websites for the latest patches, service packs and upgrades.
 - You may also refer to CyberSecurity Malaysia website under MyCERT for information on the latest patches, service packs and upgrades by referring to our latest advisories at: <https://www.mycert.org.my/en/services/advisories/mycert/2017/main/index.html>
- If you do not prepare for a DDoS incident in advance, contact your ISP to understand the DDoS mitigation it offers and what process you should follow.





T +603 8992 6888
F +603 8992 6841
H 1 300 88 2999

Corporate Office:
Level 5, Sapura@Mines
No 7, Jalan Tasik
The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan
Malaysia.
www.cybersecurity.my

http://www.cybersecurity.my/data/content_files/44/1716.pdf

MyCERT Advisories

2017201620152014201320122011201020092008200720062005
2004200320022001200019991998

MyCERT Advisories, Alerts and Summaries for the year 2017

MA-679.082017: MyCERT Special Alert - Recent Attacks to Malaysian websites

Date first published: 21/8/2017

1.0 Introduction
MyCERT has been receiving several incidents targeting Malaysian websites, confidential information leaks and possible Distributed Denial of Services (DDoS) attacks. As a preventive measure, MyCERT release this alert to advise System Administrators to take necessary steps to secure their systems against unwanted incidents as well from other security threats.

2.0 Recommendation
Attached below are some recommendations for System Administrators as preventive measures and mitigation steps against these attacks:

- Organizations are recommended to apply defense in depth strategy in protecting their networks. Firewalls, intrusion prevention systems (IPS), network and host based intrusion detection systems (IDS) can prevent and log most of the generic attacks.

Make sure systems, applications and third party add-ons are updated with latest upgrades and security patches.
- If you're running older versions of operating systems or software, make sure they are upgraded to the latest versions as older versions may have some vulnerability that can be manipulated by intruders. Aside from that, please make sure that your web based applications and network based appliances are patched accordingly.

You may refer to your respective vendors' websites for the latest patches, service packs and upgrades. You may also refer to MyCERT's website for information on the latest patches, service packs and upgrades by referring to our latest advisories at:

<https://www.mycert.org.my/en/services/advisories/mycert/2017/main/index.html>

<https://www.mycert.org.my/en/services/advisories/mycert/2017/main/detail/1281/index.html>



Malware Research Centre (MRC)

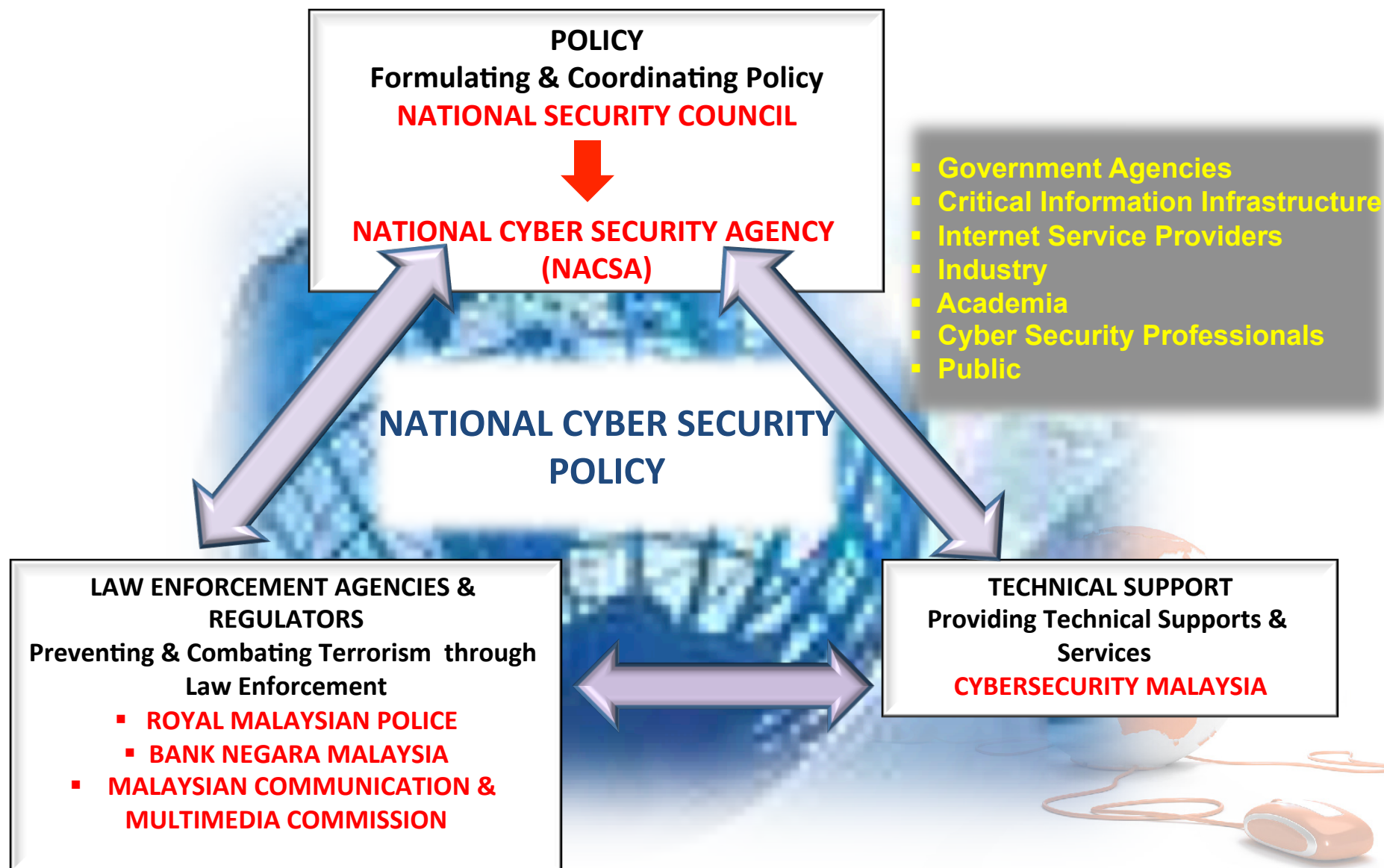
Projects/Activities



Innovative Tools Produced



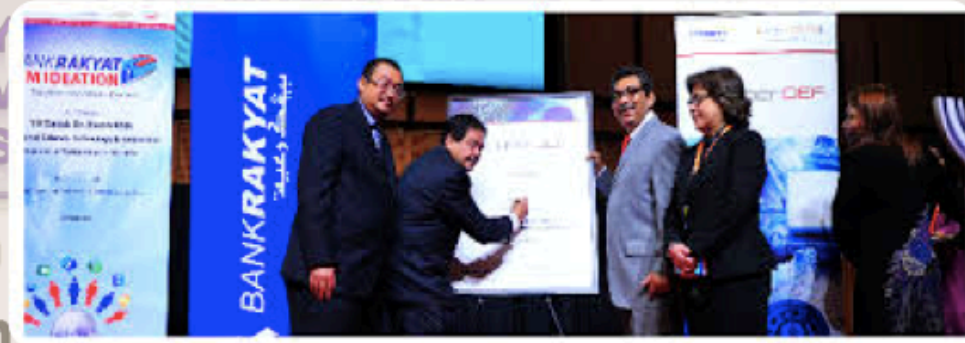
Cyber Security Eco System in Malaysia



CyberSecurity Malaysia: Operational Services – CyberDEF services (latest product)



CyberDEF
A comprehensive solution for detection, eradication and forensic in cyberspace



Key Components of Service

CyberD.E.F will look at the resources, skills, policies and SOPs required in an organisation. Key components of the solutions are as below:

- + CSIRT Consultation**
- + Policies and SOPs study
- + Hands-on training
- + Cyber Exercise
- + Remediation and Eradication Measures
- + CyberDISCOVERY (Digital Forensic)

**for organisations without CSIRT Team/Facility



Cyber Security Certification

REPORTING CHANNEL

Contact Us



Cyber999 Help Centre:

Cyber999 Hotline:
1-300-88-2999

Email:
cyber999@cybersecurity.my

Fax:
+603-8945 3442

Handphone:
+6019 - 266 5850 (24X7 - Emergency)

Online: Fill up online form at
http://www.mycert.org.my/report_incidents/online_form.html

SMS:
CYBER999 REPORT <EMAIL><COMPLAINT> to
15888



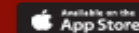
USE INTERNET PRUDENTLY. YOU DO WANT TO BECOME VICTIMS ON MISCONDUCT OF INTERNET

If you encounter any cyber security threats or incidents, report it to the help center CYBER999



CYBER999 APP

App Store - Apple iOS



<https://itunes.apple.com/us/app/cyber999-mobile-application/id888552400?mt=8>

Google Play - Android



<https://play.google.com/store/apps/details?id=my.cyber999.mobile&hl=en>



Corporate Office:
CyberSecurity Malaysia, Level 5, Sapura@Mines, No 7, Jalan Tasik, The Mines Resort City, 43300 Seri Kembangan, Selangor Darul Ehsan, Malaysia.
Tel: +603 - 8992 6888 | Fax: +603 - 8992 6841 | Email: info@cybersecurity.my Customer Service Hotline: 1300-88-2999 | www.cybersecurity.my

Our Office hour is:

Day: Monday - Friday

Time: 09:00 AM - 18:00 PM, MYT+0800



CONCLUSION AND WAY FORWARD

- Our approach to cope with emerging new technologies should be **equally intelligent by adopting holistic strategy and through the use of new cyber tools**
- To effectively **apply cyber security fundamentals with innovative features and techniques**
- Strengthening **Public-Private-Academia Partnership and International Collaboration**
- **To evolve in parallel with technology** by enhancing:
 - Sharing of Information amongst relevant parties
 - Cyber Incidents Response and Coordination
 - Innovative & Collaborative Research
 - Capacity Building
 - Cyber Security Awareness and Education





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

