

***CHALLENGES IN SUSTAINING A COMPUTER EMERGENCY  
RESPONSE TEAM: MALAYSIA CERT EXPERIENCE***

SHARIFAH ROZIAH MOHD KASSIM  
MYCERT  
CYBERSECURITY MALAYSIA



# Agenda

- Brief Introduction About MyCERT
- Our Services and Achievements
- Challenges in Sustaining our Team
- Lessons Learnt
- Areas of Improvement
- Conclusion
- Q&A



# Brief Introduction to MyCERT



Launched in 1997 as a technical reference centre in Malaysia



Parked and funded under the Ministry of Science, Innovation & Technology, to provide Incident Response for the general public and organizations in Malaysia



Operating with 18 staff with two main services, Incident Response(Reactive) and Malware Research (Pro-active)



Audience: Malaysian Internet User



International Affiliation: Deputy Chair of APCERT, Permanent Secretariat of OICCERT. A member of FIRST – active in FIRST Membership sponsor.

# Services

Reactive	Proactive
<ol style="list-style-type: none"> <li>1. Incident Response and Handling</li> <li>2. Security Operation Centre (SOC)</li> <li>3. Security Advisory &amp; Alerts</li> <li>4. Cyber Security Crisis</li> </ol>	<ol style="list-style-type: none"> <li>1. Watch and Warn / Threat Monitoring</li> <li>2. Applied Research</li> <li>3. Tools development</li> <li>4. Malware Analysis</li> <li>5. Security Advisory &amp; Alerts</li> </ol>



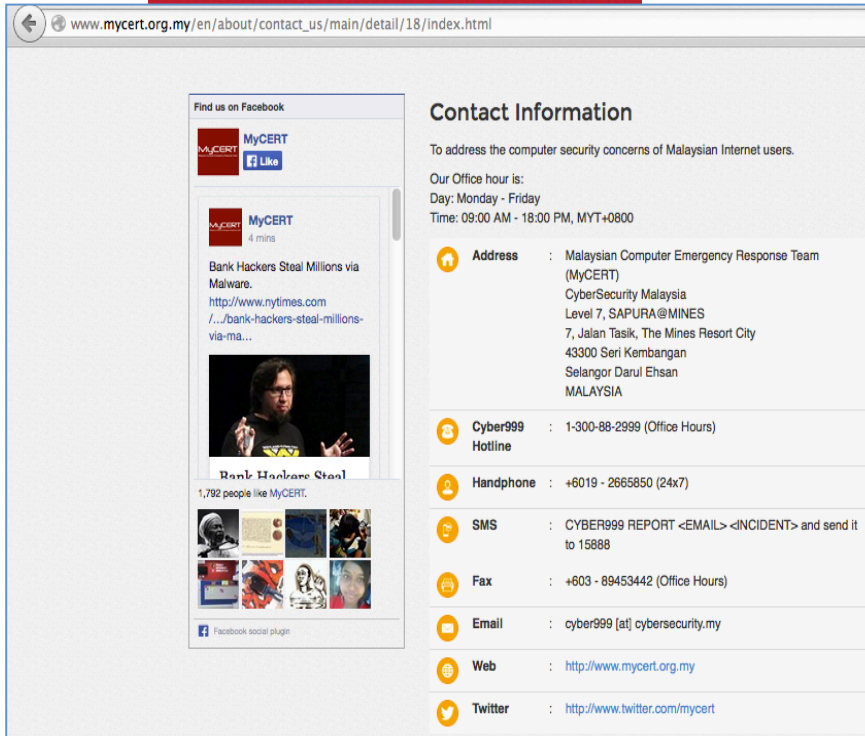
# Incident Reporting Channels

- Email
  - [cyber999@cybersecurity.my](mailto:cyber999@cybersecurity.my)
- Phone/Hotline
  - +603 8992 6888
  - 1 300 88 2999
- Fax
  - +603 8945 3442
- SMS
  - 15888 “Cyber999 Report”
- Mobile (24x7)
  - +6019 266 5850
- Online – <http://www.mycert.org.my>
- Walk In - Office Hours: MYT 0900 – 1800
- Mobile application (iOS and Android)



**ADDRESS**  
 My CyberSecurity Clinic,  
 E-R2, Ground Floor, Block E,  
 The Mines Waterfront Business Park,  
 No 3 Jalan Tasik, The Mines Resort City,  
 43300 Seri Kembangan,  
 Selangor Darul Ehsan, Malaysia.

**contact +603-8946 0811**



www.mycert.org.my/en/about/contact\_us/main/detail/18/index.html

**Contact Information**

To address the computer security concerns of Malaysian Internet users.

Our Office hour is:  
 Day: Monday - Friday  
 Time: 09:00 AM - 18:00 PM, MYT+0800

**Address** : Malaysian Computer Emergency Response Team (MyCERT)  
 CyberSecurity Malaysia  
 Level 7, SAPURA@MINES  
 7, Jalan Tasik, The Mines Resort City  
 43300 Seri Kembangan  
 Selangor Darul Ehsan  
 MALAYSIA

**Cyber999 Hotline** : 1-300-88-2999 (Office Hours)

**Handphone** : +6019 - 2665850 (24x7)

**SMS** : CYBER999 REPORT <EMAIL> <INCIDENT> and send it to 15888

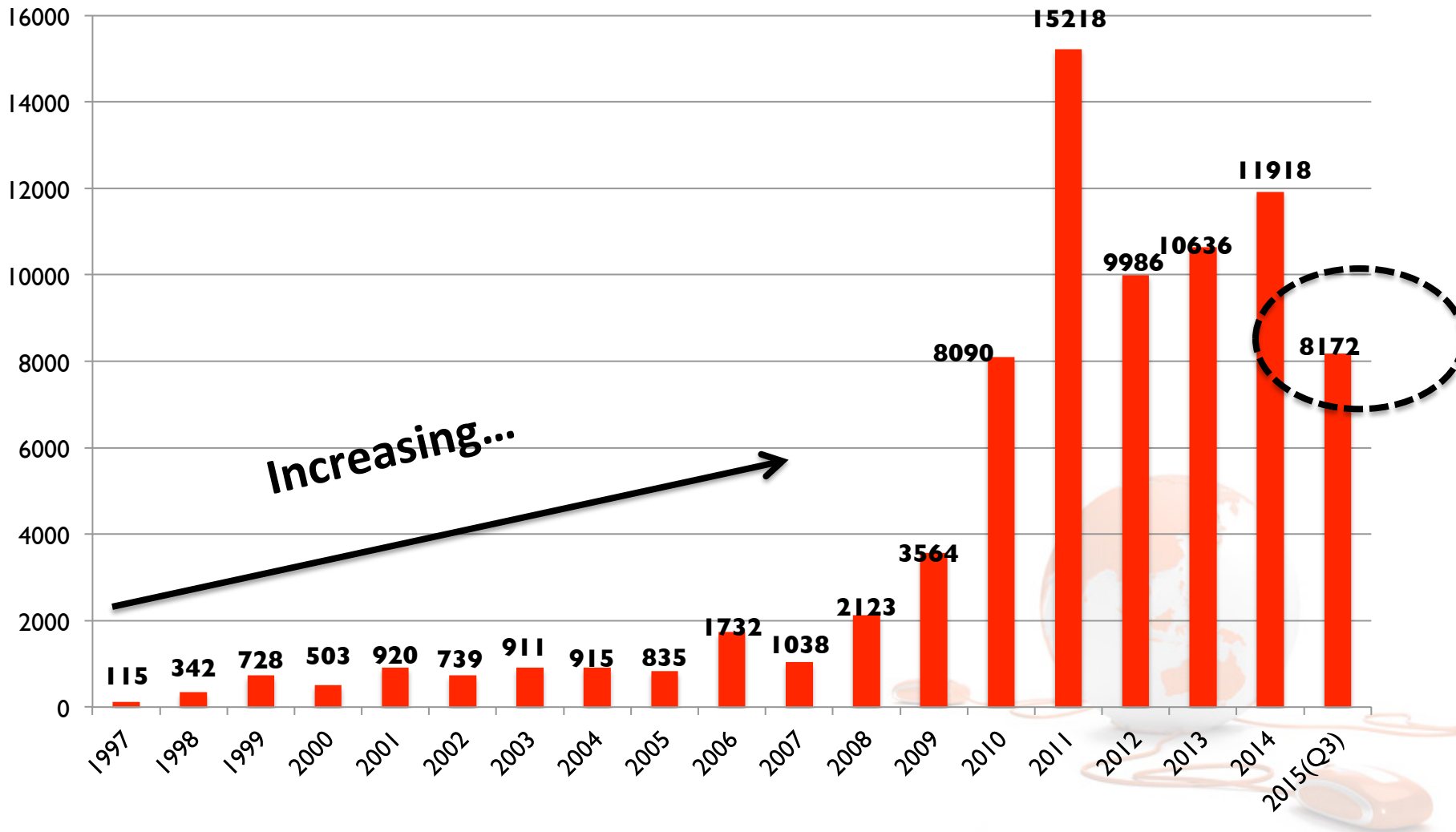
**Fax** : +603 - 89453442 (Office Hours)

**Email** : [cyber999@cybersecurity.my](mailto:cyber999@cybersecurity.my)

**Web** : <http://www.mycert.org.my>

**Twitter** : <http://www.twitter.com/mycert>

# Incidents Handled by MyCERT (1997 – 2015)



# Incidents Handled by Category (2014)

	JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC	TOTAL
Content Related	5	2	2	1	4	2	4	6	3	3			
Cyber Harassment	57	41	45	44	46	48	52	44	53	36			
Denial of Service	1	2	3	2	4	1	3	1	6	3			
<b>Fraud</b>	<b>250</b>	<b>264</b>	<b>280</b>	<b>399</b>	<b>401</b>	<b>519</b>	<b>406</b>	<b>372</b>	<b>435</b>	<b>366</b>	<b>377</b>	<b>408</b>	<b>4477</b>
Intrusion	109	76	216	70	15	26	43	47	104	105	178	134	1125
Intrusion Attempt	3	11	24	157	63	75	21	241	649	12	19	27	1302
Malicious Codes	251	78	101	55	47	48	29	14	22	13	16	42	716
Spam	40	23	32	36	61	55	385	530	548	671	735	534	3650
Vulnerabilities Report	1	1	4	9	4	1	0	3	2	7	1	1	34
	<b>717</b>	<b>498</b>	<b>707</b>	<b>773</b>	<b>645</b>	<b>777</b>	<b>943</b>	<b>1258</b>	<b>1822</b>	<b>1216</b>	<b>1376</b>	<b>1186</b>	<b>11918</b>

*Fraud – phishing, online scam, 419 scam, purchase, impersonation, spoofing*

<http://www.mycert.org.my/statistics/2014.php>

# Incidents Handled by Category (2015)

	JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEP	TOTAL
Content Related	2	3	3	3	0	4				25
Cyber Harassment	30	40	32	51	30	45				26
Denial of Service	1	2	2	5	3	3	5	7	2	30
<b>Fraud</b>	<b>276</b>	<b>235</b>	<b>232</b>	<b>313</b>	<b>303</b>	<b>388</b>	<b>253</b>	<b>252</b>	<b>247</b>	<b>2499</b>
Intrusion	88	508	29	63	21	20	85	233	206	1253
Intrusion Attempt	28	22	21	21	10	6	13	8	13	142
Malicious Codes	21	30	26	26	35	51	43	39	220	491
Spam	389	430	455	434	348	850	338	88	58	3390
Vulnerabilities Report	1	1	2	2	4	0	1	3	2	16
	836	1271	802	918	754	1367	786	665	773	8172

*Fraud – phishing, online scam, 419 scam, purchase, impersonation, spoofing*

<http://www.mycert.org.my/statistics/2015.php>





# Local News Coverage On MyCERT

## Pengguna perlu ada kesedaran keselamatan siber

Kes penipuan atas talian, perbankan semakin serius

**Wartawan:** Revolusi kebebasan internet di seluruh dunia, termasuk Malaysia tidak boleh lari daripada kesan negatif kepada rakyat dan negara. Ia boleh digambarkan untuk pelbagai tajuk termasuk jenayah, buli, penyelewengan kuasa dan pelbagai lagi. Apa penalaran dan komen CyberSecurity Malaysia mengenai perkembangan semasa yang berlaku sekarang?

**Kecanggihannya dan kemudahan teknologi terkini memudahkan urusan perbankan. Melaui urusan perbankan boleh dilakukan di mana saja tanpa mengira masa. Namun, wujud pihak tidak bertanggungjawab memburai dan memindah wang orang lain melalui**

basan mutlak di alam siber kerana ia boleh dilaksanakan oleh pihak tertentu untuk merajutkan keharmonian masyarakat berbilang bangsa dan agama di negara ini. Justeru, peranan internet perlu mempunyai perlakuan yang beretika dan bertanggungjawab supaya tidak menimbulkan kekecohan dan huru-hara dalam kalangan rakyat yang boleh memberi kesan negatif kepada insya negara dan kesejahteraan awam dan keselamatan negara.

**S:** Aplikasi yang banyak digunakan di Malaysia dan yang berisiko untuk mudah ditipu, di-selak guna atau maklumat peribadi mudah diceroboh dan digunakn bagi tujuan tertentu. Bagaimana dengan modus operandi yang digunakan dan contoh kes secara am? **J:** Antara aplikasi internet yang sering menjadi sasaran serangan pem-

rang menarik contohnya telefon mudah alih, tablet dan aksesori wanita. Pengguna telah melakukan pembelian di laman berkenaan menggunakan kredit kad, tetapi selepas munggas sebulan lamanya barisan yang ditengah tidak tiba ke tangan pembeli. Tanpa-cupanya laman itu telah mengambil duit bayaran pembeli tetapi tanpa disedari. Oleh hal demikian, adalah penting untuk pengguna melakukan transaksi di laman yang dipercayai dan selamat untuk melakukan transaksi kewangan dan urusan jual beli.

**S:** Kemudahan e-mel yang pernah dikatakan antara yang selamat juga kerap menjadi mangsa cyberboh atau e-mel palsu. Bagaimana pengguna boleh mengelak daripada terjebak daripada melayan sebarang e-mel yang mengandungi dan tindakan susulan yang perlu ditakutkan seperti apa?



## The SKOP

Home / Berita / Virus Zeus Boleh Serang Maybank2U, CIMB Clicks

# Virus Zeus Boleh Serang Maybank2U, CIMB Clicks

By admin on September 25, 2014

Tweet

Pin It

ADVERTISEMENT



Agensi pakar dalam keselamatan siber yang berada di bawah Kementerian Sains, Teknologi dan Inovasi, CyberSecurity memberi amaran kepada pengguna perbankan internet

**Nation** Home > News > Nation

Published: Wednesday August 20, 2014 MYT 12:00:00 AM

Updated: Wednesday August 20, 2014 MYT 1:53:51 PM

# Hacker targets info on MH370 probe

BY NICHOLAS CHENG



**EXCLUSIVE:** KUALA LUMPUR: The computers of high-ranking officials in agencies involved in the MH370 investigation were hacked and classified information was stolen.

The stolen information was allegedly being sent to a computer in China before CyberSecurity Malaysia – a Ministry of Science, Technology and Innovation agency – had the transmissions blocked and the infected machines shut down.

## JENAYAH

ARKIB : 25/09/2014

# Hantar virus ke telefon lesapkan wang

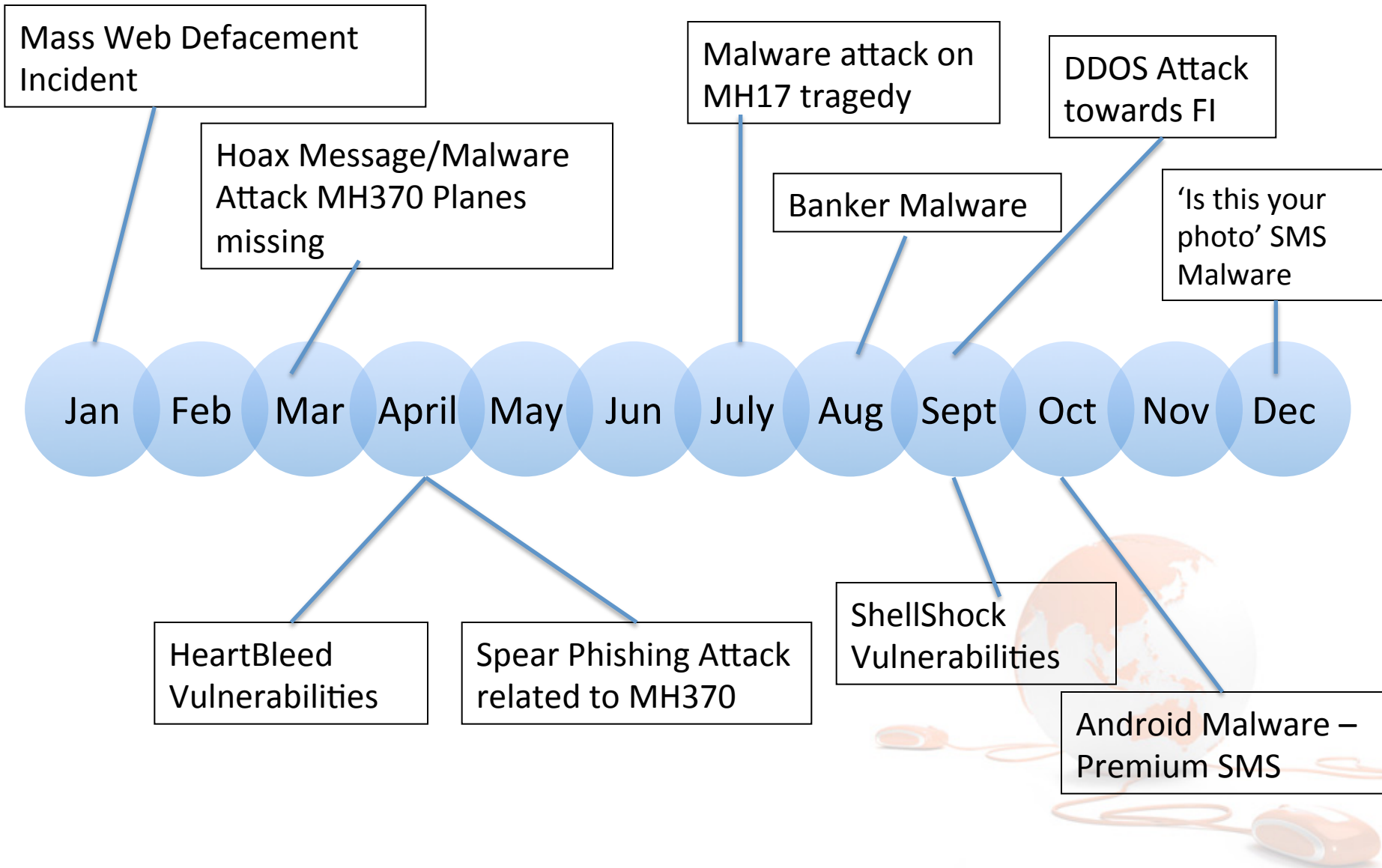
Oleh AZRAI MOHAMMAD  
penarang@utusan.com.my



HAMZA Taib (dua dari kanan) bersama para pegawainya menunjukkan sebahagian barang rampasan selepas sidang akhbar di pejabat Jabatan Siasatan Jenayah Komersial (JSJK) di Kuala Lumpur, semalam. - UTUSAN/FAUZI BAHARUDIN

**KUALA LUMPUR 24 Sept.** - Awas! Hanya dengan menekan satu klik pada pautan yang dihantar ke telefon pintar menerusi pesanan khidmat ringkas (SMS) atau WhatApps, kesemua wang di dalam akaun bank anda mungkin akan lesap dalam

# What we have seen in year 2014

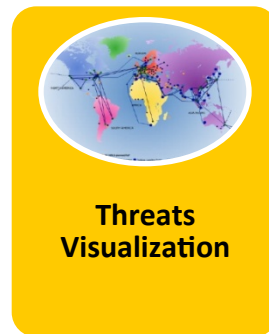
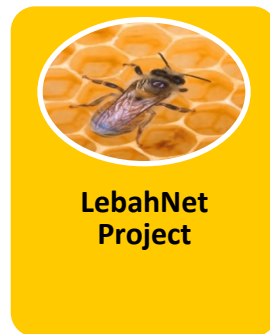
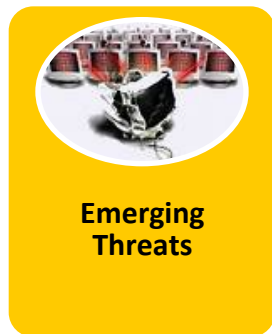
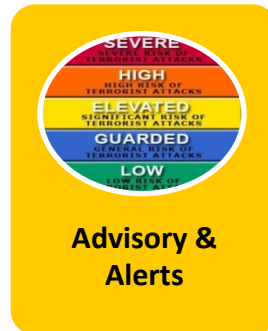


# Malware Research Centre (MRC)



## MRC Projects/Activities

## Advisories and Alerts



- Software vulnerabilities (Advisories)
  - 0-day vulnerabilities (Java, PDF)
  - Patch / Upgrade
  - Security update for Firefox
- Outbreaks 2015 (Alerts)
  - Circulation of Emails Attached with Malicious Document
  - Attack to .my domains

# Advisories and Alerts

## MyCERT Advisories

[2015](#)
[2014](#)
[2013](#)
[2012](#)
[2011](#)
[2010](#)
[2009](#)
[2008](#)
[2007](#)
[2006](#)
[2005](#)
[2004](#)
[2003](#)  
[2002](#)
[2001](#)
[2000](#)
[1999](#)
[1998](#)

---

### MyCERT Advisories, Alerts and Summaries for the year 2015

---

- 08/10/2015** MA-525.102015: MyCERT Vulnerability and Threat Summary - September 2015
- 08/10/2015** MA-524.102015: MyCERT Vulnerability and Threat Summary - August 2015
- 04/10/2015** MA-523.092015: MyCERT Alert – New “Ghost Push” Variants Sport Guard Code
- 28/09/2015** MA-522.092015: MyCERT Advisory – Google Releases Security Update for Chrome
- 23/09/2015** MA-521.092015: MyCERT Advisory - Mozilla Releases Security Updates for Firefox
- 22/09/2015** MA-520.092015: MyCERT Advisory - Adobe Releases Security Updates for Flash Player

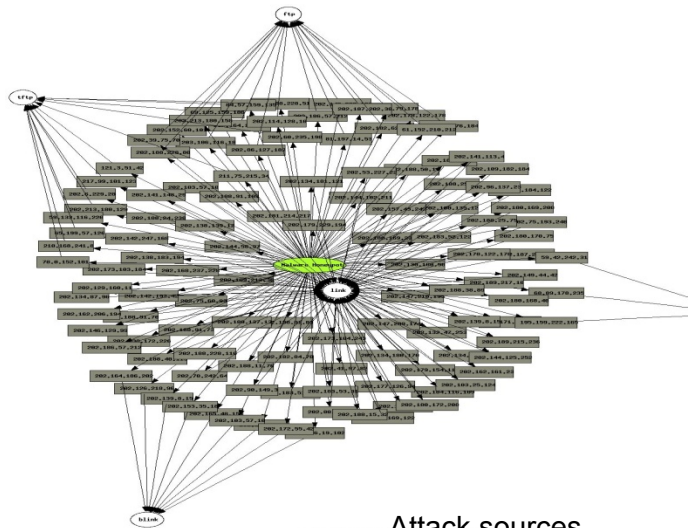
<https://www.mycert.org.my/en/services/advisories/mycert/2015/main/index.html>



Advisory and Alerts

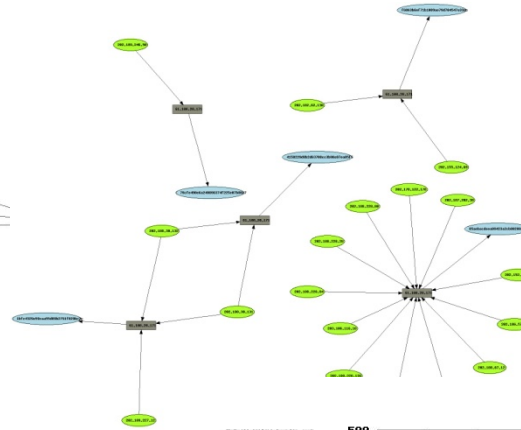


# HoneyNet - LebahNet

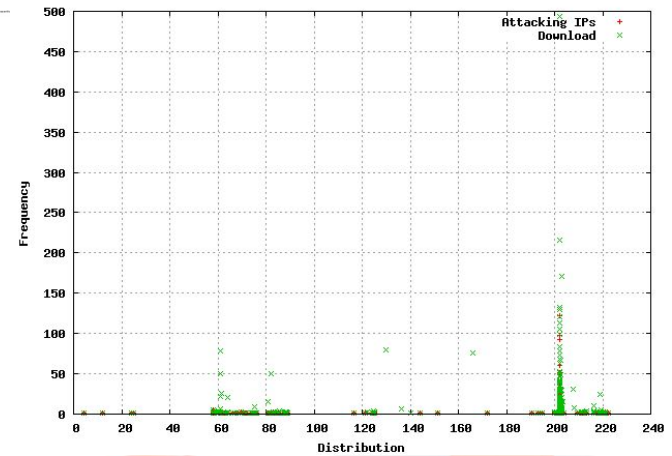


Attack sources

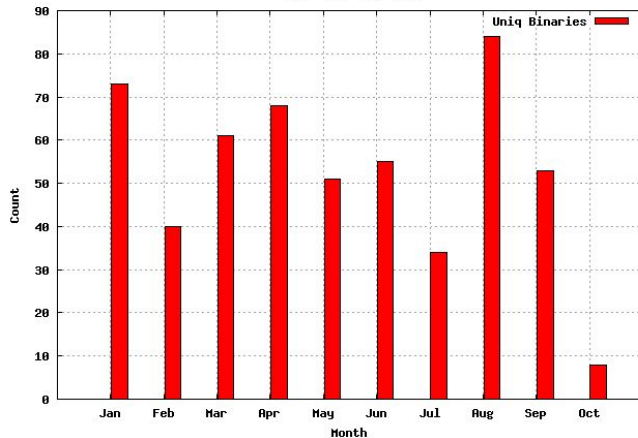
## Malware Analysis



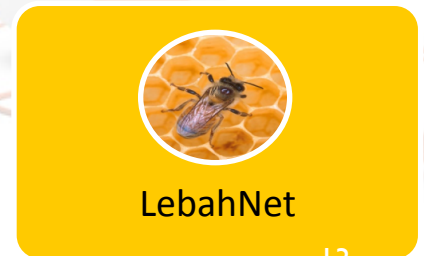
2 Octets IP Distribution Attacking and Download



Malware Collector Unique Binaries Monthly Jan - Oct (12) 2007



Uniq Binaries

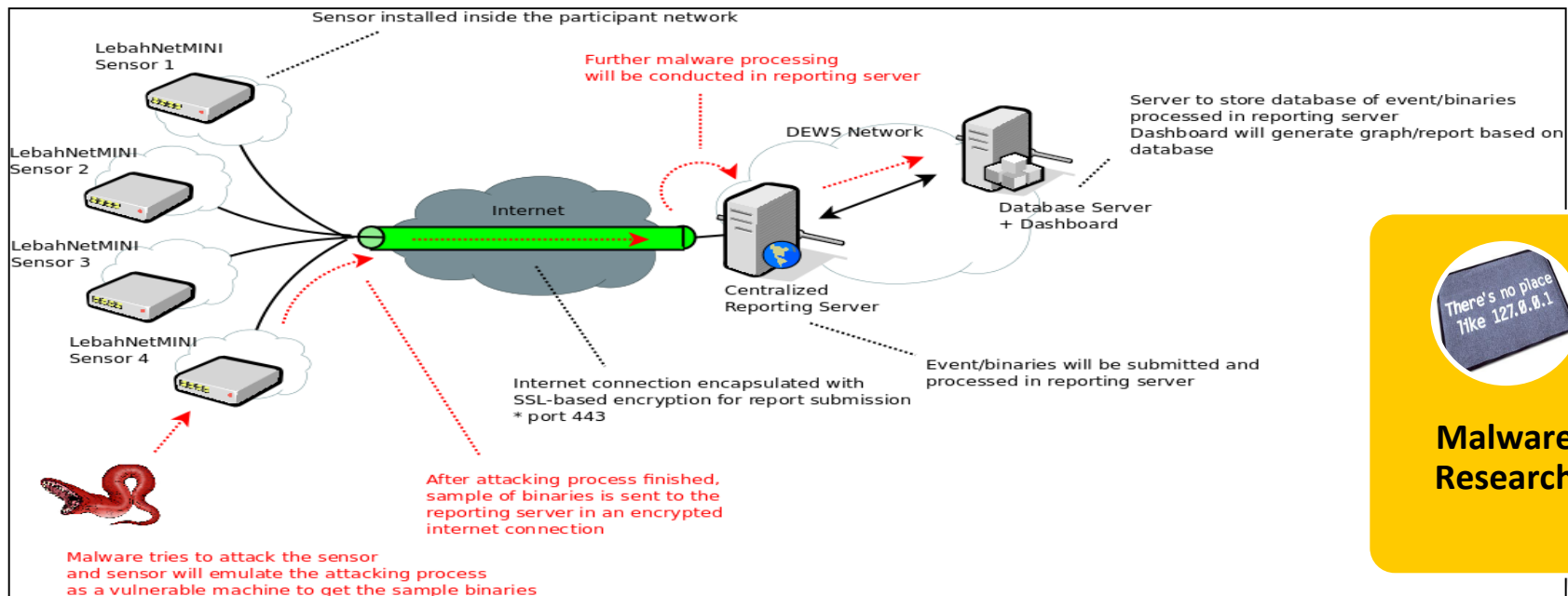


# Malware Distribution Sensor

Lebahnet



CyberSecurity Malaysia Honeynet Project



# Challenges in Sustaining a CERT

Stakeholder  
Buy-In

Cooperation  
from Various  
Parties

Staffing and  
Skills &  
Expertise

Budget

Quality of  
service

Change in  
Nature of  
Incident



# Stakeholders Buy-In

Challenge to convince the roles of CERTS and its capabilities to a constituency

Stakeholder looks into investment that brings return (ROI). CERTs are non-profit organization.

Must achieve targeted Key Performance Indicators





# Cooperation from Various Parties: Local & International

- 1) Cooperation from Law Enforcement Agencies
- 2) Cooperation from Service Providers,
- 3) CERT to CERT cooperation
- 4) Cross border issues: Language, Culture, Law.



# Staffing, Skills and Expertise

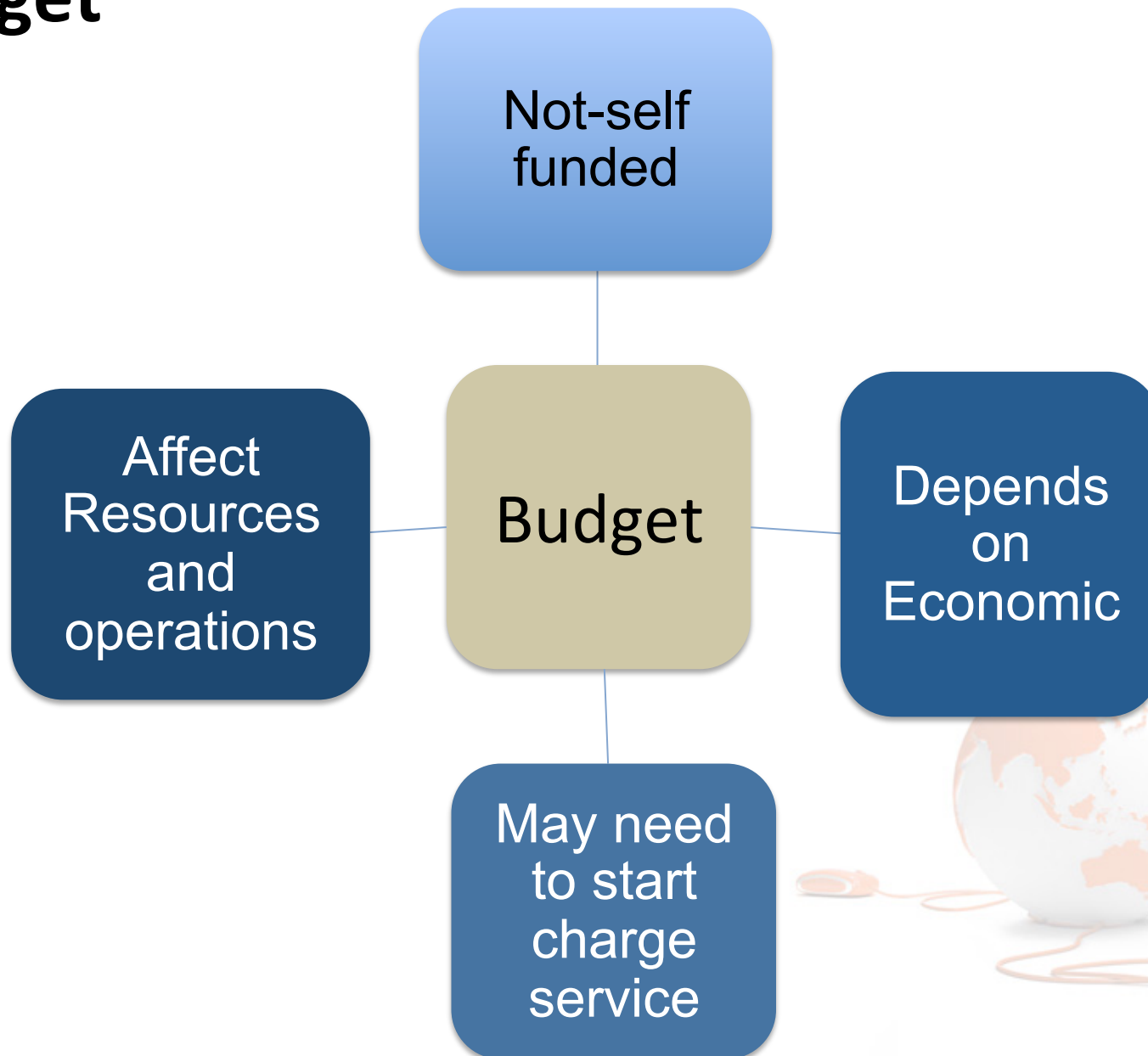
Insufficient staff to meet the growing needs and demands

Developing/maintaining skills and expertise

Reduce staff turn over – improve staff benefits



# Budget



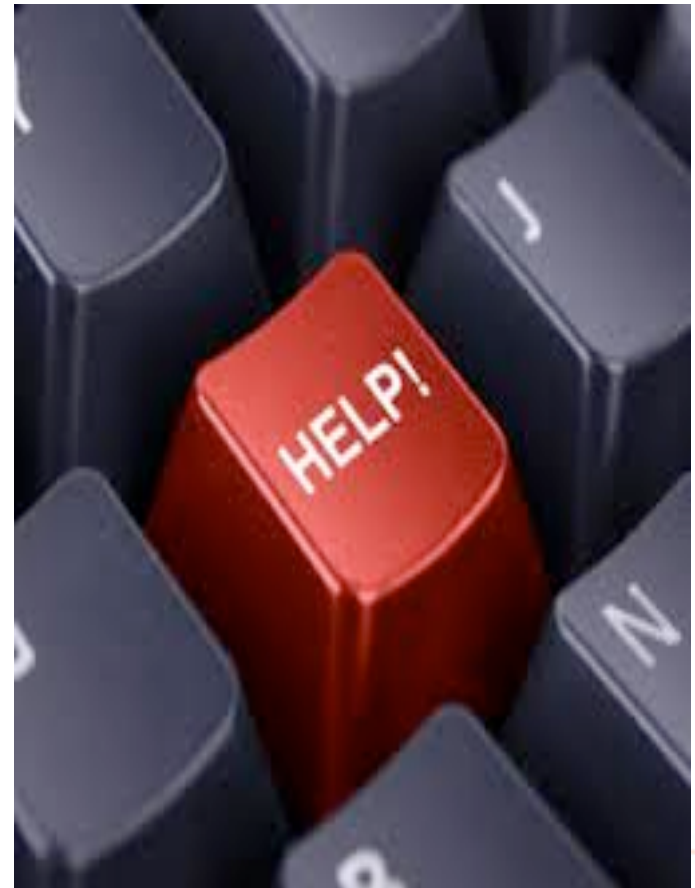
# Quality of Service

- 1) Consistency & improvement to the quality of current service
- 2) Introduce more new value-add service for public
- 3) Customer satisfaction should be a priority
- 4) Develop new tools to support the operation
- 5) Incident resolution rate



# Nature of Incidents Change

- 1) Technical vs Non-technical Incidents
- 2) Challenge to respond to non-technical incidents
- 3) Victims are aggressive
- 4) Escalation to Law Enforcement Agencies – incidents sometimes become less priority for Law Enforcement.



# Areas of Improvement for CERTS

Stakeholders buy-in

Understanding the constituency and its needs

Resources with necessary skills and expertise

Effective Communication with all parties

Efficient Operations and services

# Lessons Learnt

- Communication is essential. Need to communicate well on issue faced by the CERT with relevant parties & communication on operational matters.
- Need to ensure the CERTs direction is well understood by all parties in the constituency to avoid misconception on CERT's roles.
- Selecting right resources with the right skillsets. Always have business contingency plan to address staff turn over issue.
- CERTs need to come up with their own new ideas and solutions to overcome problems and issues related to budget.
- Issues and problems in CERT must not affect the CERTs main functions.



# Conclusion

- MyCERT's presence is needed in our constituency to address the ever growing cyber incidents.
- Good cooperation and collaboration with the APCERT, OIC CERT, South East Asia countries CERTs and FIRST community has further improved our visibility in the global.
- However, there are still many improvements need to be made in order to sustain our continuity and our visibility.
- Need to immediately address challenges and issues by coming up with effective solutions





# Any Questions



# Thank you

## Corporate Office

CyberSecurity Malaysia,  
Level 8, Block A,  
Mines Waterfront Business Park,  
No 3 Jalan Tasik, The Mines Resort City,  
43300 Seri Kembangan,  
Selangor Darul Ehsan, Malaysia.

T : +603 8946 0999  
F : +603 8946 0888  
H : +61 300 88 2999

[www.cybersecurity.my](http://www.cybersecurity.my)  
[info@cybersecurity.my](mailto:info@cybersecurity.my)

## Northern Regional Office

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](http://www.facebook.com/CyberSecurityMalaysia)



[twitter.com/cybersecuritymy](https://twitter.com/cybersecuritymy)



[www.youtube.com/cybersecuritymy](http://www.youtube.com/cybersecuritymy)

