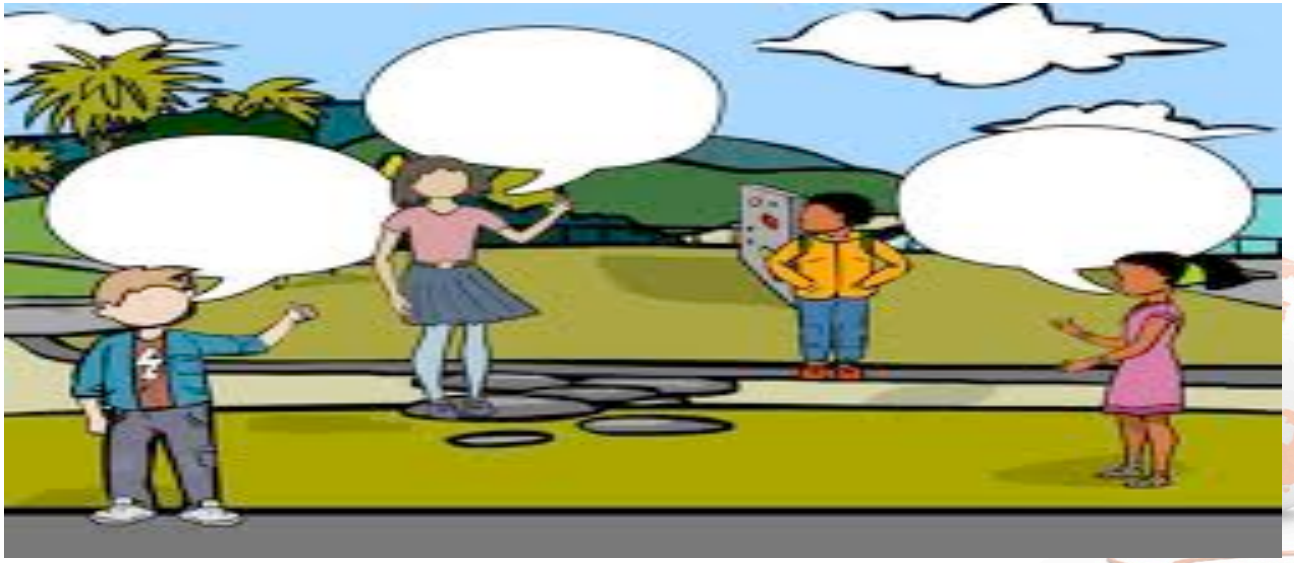
# Unifying Incident Response Teams Via Multi Lateral Cyber Exercise for Mitigating Cros Border Incidents: Malaysia CERT Case Study

Sharifah Roziah Mohd Kassim
MyCERT
CyberSecurity Malaysia

# Agenda

- Introduction
- Multi-lateral Cyber Exercise Preparation
- In-house Developed Tools
- Observations and Expectations
- Reviews and Feedbacks
- Case Study - Examples of Cross Border Incidents
- Areas of Improvement
- Conclusion

# Introduction



# Issues Surrounding Cross Border Incidents


Understanding the Laws and Legislations of the cross border countries. Laws vary considerably from country to country, especially if the incidents involve have undeveloped legal structure, the prosecution is further complicated.


Lack of contacts and mutual colloborations. We may spend unnecessary time to look up the right contacts when comes to responding to cross border incidents.


Lack of common practice and common understanding. Lack of a coordinated action plan that can be used by everyone during an incident.


Challenges to cross-border investigations and prosecutions includes high cost of investigations and lack of technical expertise to expedite analysis and response.

Time consuming. Cross border incidents normally involve well organized syndicate rings, thus investigations may end up time consuming.

# Why Mitigating Cross Border Incidents are Critical

1) Organized cyber incidents are becoming more cross-border in nature. Thus it must be detected, contained and mitigated at early stage otherwise it may have big impacts to economical, social & politics.

2) It is a colloborative work to ensure  that the cyber world is safe for everyone, thus incidents must be responded fast and cyber threats must be eliminated.

3)To contain cyber threats from further spreading across borders, otherwise the threat may become more widespread.

4)To detect, trace and prosecute cyber criminals at earliest stage possible.

5)To cripple down any cyber criminal syndicates or activities that is carried on across borders.

# Common Cross Border Incidents

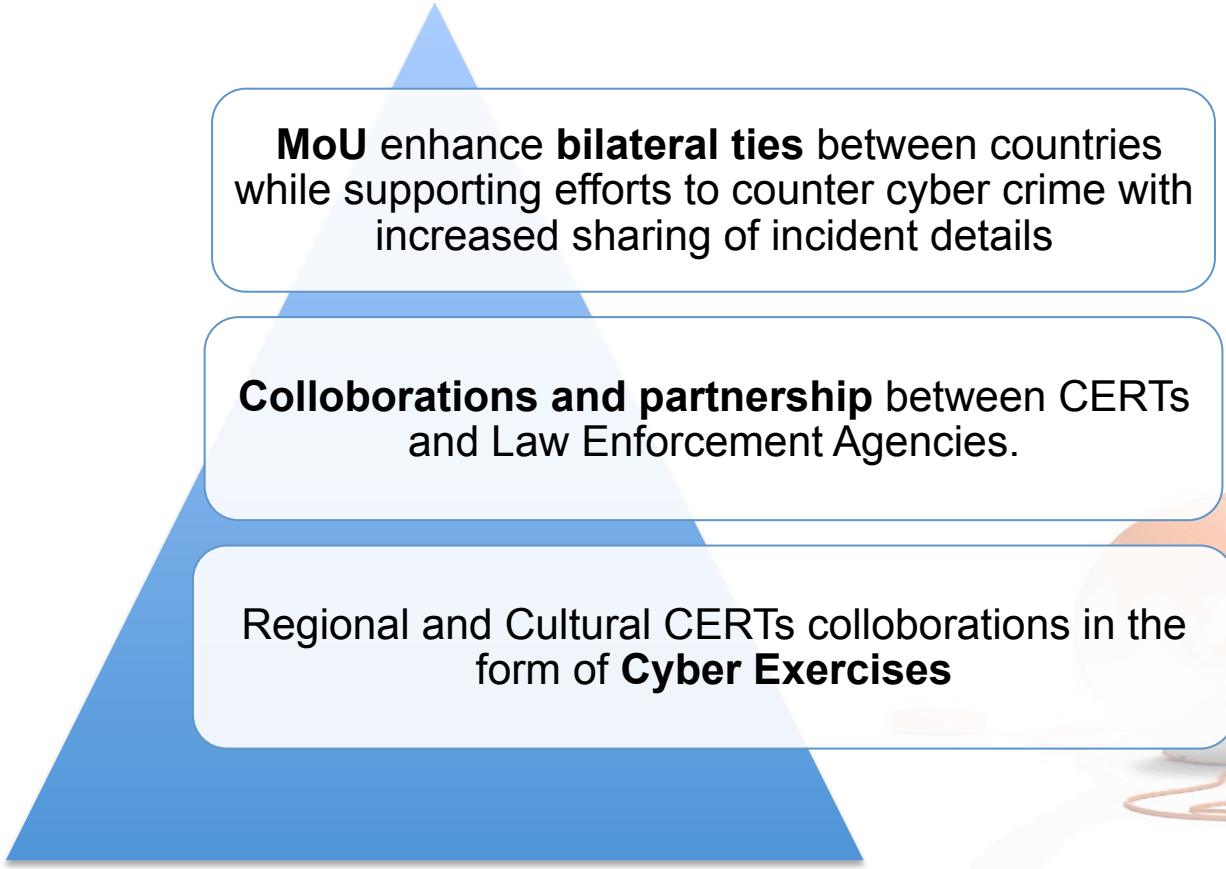
Criminals conducting frauds against banks from a different region

Extorting funds by threatening to release pictures of victims in another country

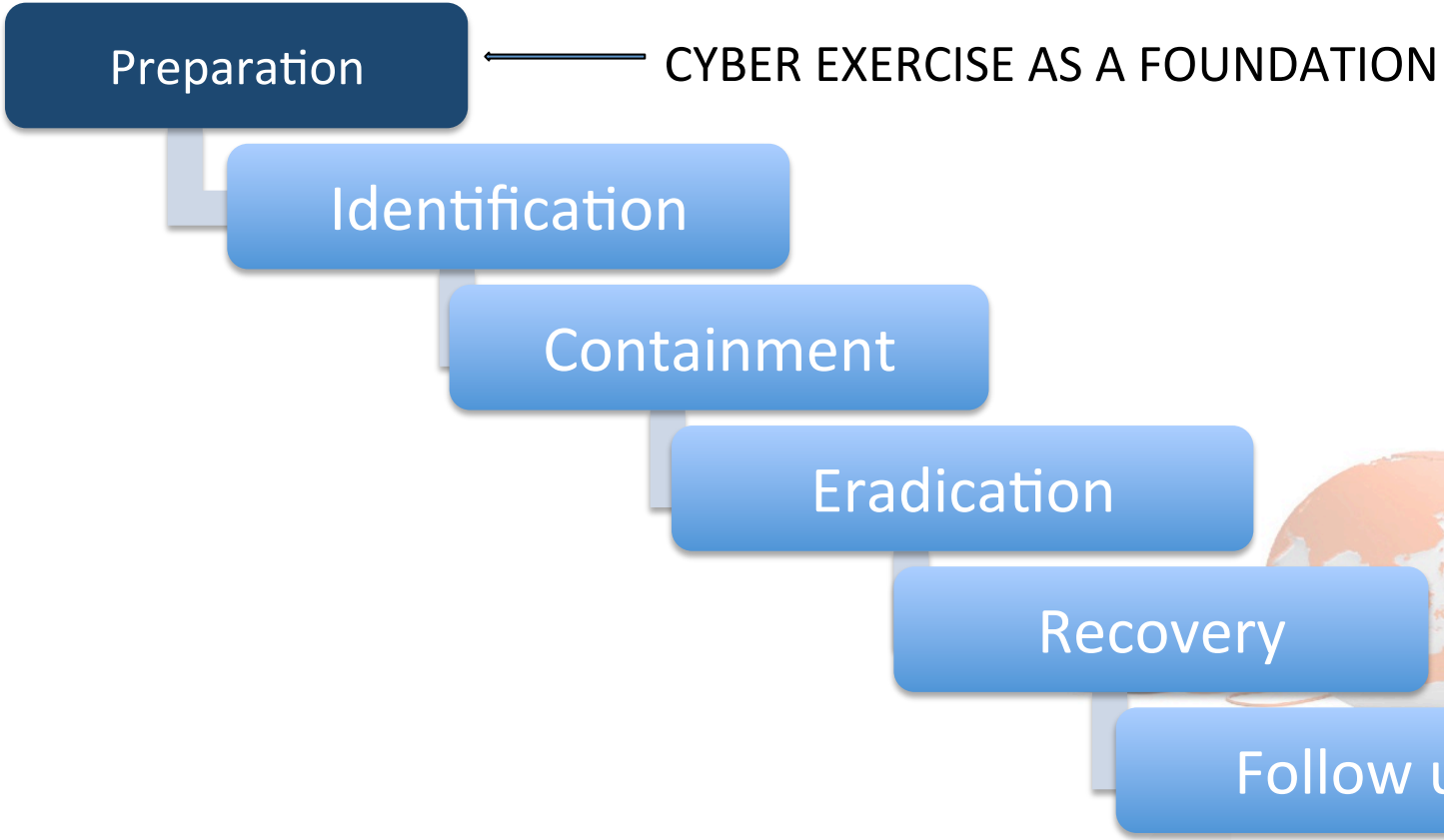
Criminals using Compromised machines in another country as launching pad to attack other machines

C & C servers used in malware activities located in a different country

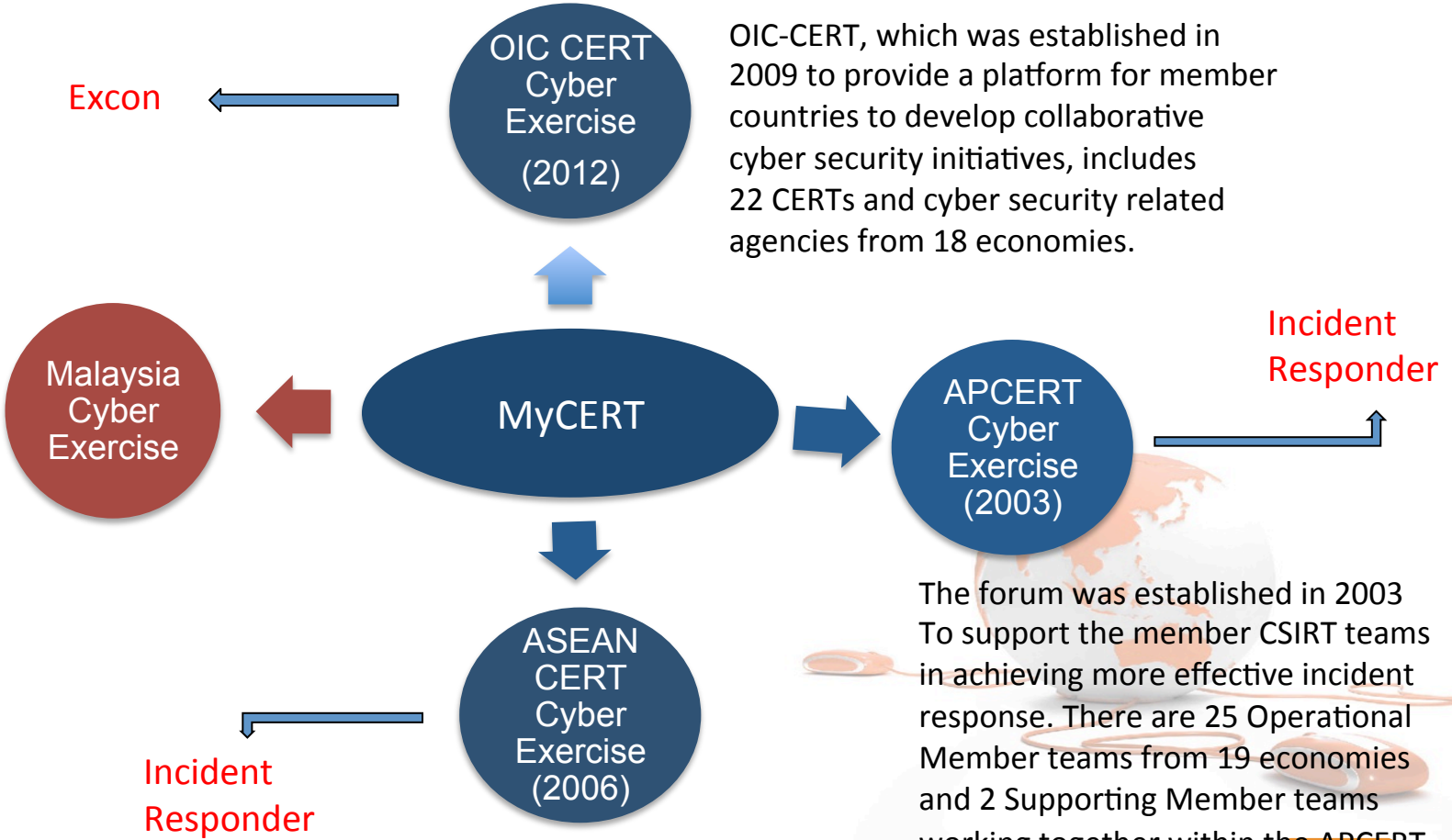
# Current Measures in Place for Mitigating Cross Border Incidents



# Cyber Exercise as Foundation of Incident Response



# Multi-Lateral Cyber Exercise – Why We Are Unique



# What is a Multi Lateral Cyber Exercise

Cyber Exercise that involves between different countries within a geographical region or between countries that have other common sharings

Usually themes are threats that are of cross border in nature and that may possibly affect various countries

Tests specifically on incident response procedures when it comes to responding to cross border incidents.

# Objectives of A Multi Lateral Cyber Exercise

To ensure incidents that happen across borders are correctly escalated and communicated to relevant parties in a short period of time.

Emphasize the need for continuous communication channels between neighbouring countries, as well as enhancing each country's incident response capabilities.

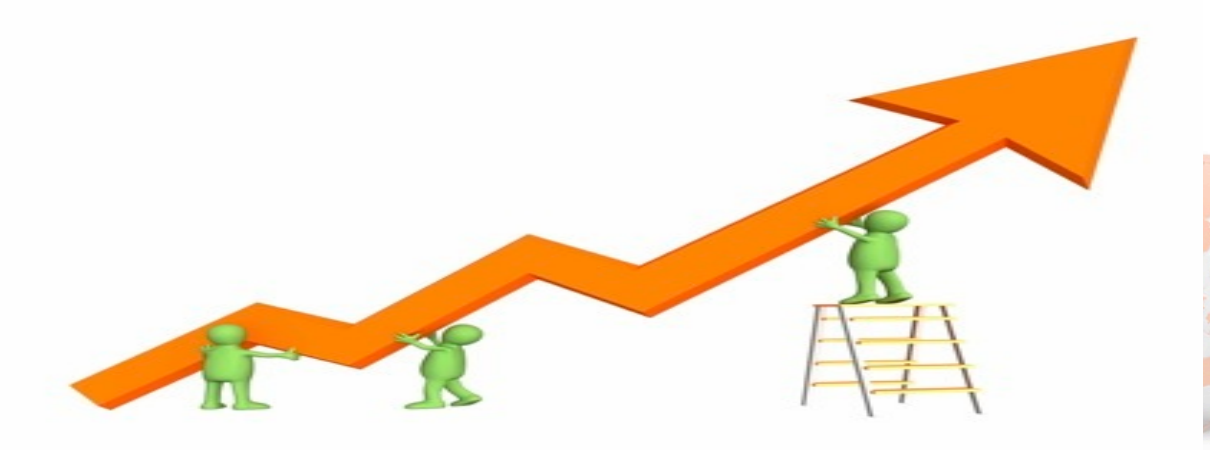
Test incident response capabilities in mitigating and countering cyber attacks especially that affects different borders.

To test the level of readiness of the team in various countries when incidents happen at cross borders and identify future planning and process improvements.

# Why Multi Lateral Cyber Exercise is Important?

- Cyberspace is a interconnected place that provides many advantages to nations, organizations and individuals. As such issues related to cyberspace need to be addressed properly.
- The need for a swift response of cross-border incidents in the event of an emergency is critical.
- To encourage nations coming together with similar intention, goal, vision, and capabilities to defend against cyber threats.
- CERTs partnership has become an integral part at international network to fight against cyber threats and multi lateral Cyber Exercise enhance such patnership.
- To develop a baseline understanding of common threats and capabilities to enable coordinated actions among different countries in the event of cyber incidents across borders.
- To test the regional coordination process and procedures in preparation of a real incident.

# Multi-lateral Cyber Exercise Preparation



# Exercise Plan

- Infrastructure
  - Web Server
  - CRM Ticketing System
  - Email Server
  - IRC Server
  - Dashboard
  - Virtual Machine Image (VMware Image archive)

# Scenario Development

# Infrastructure preparation

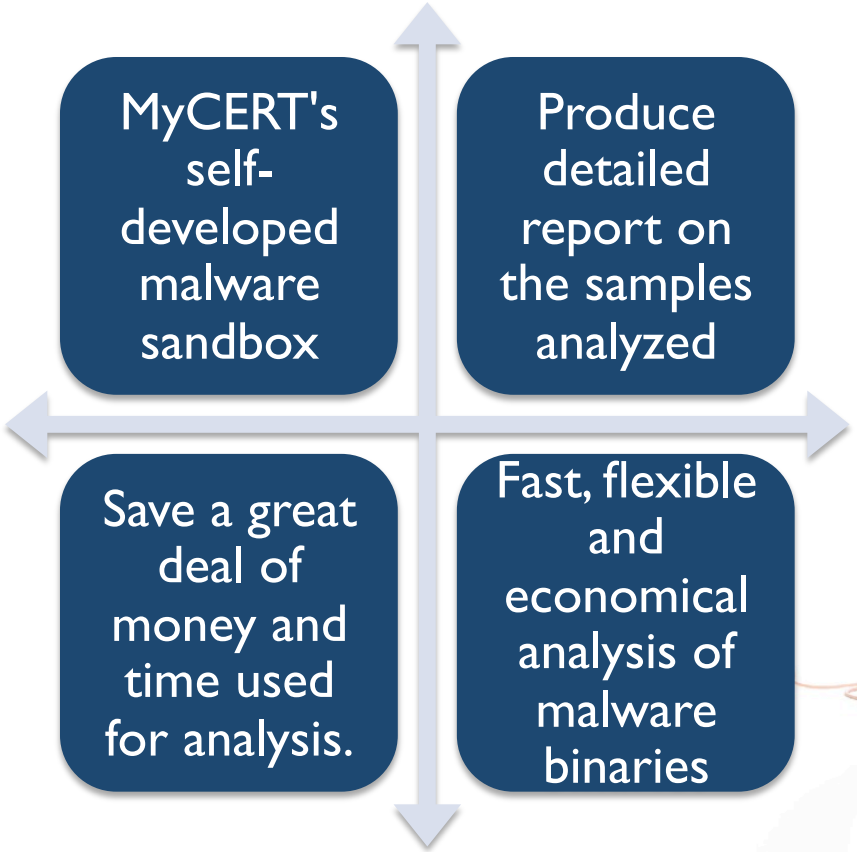
# In-house Developed Tools

# Deployment of In-House Developed Tools

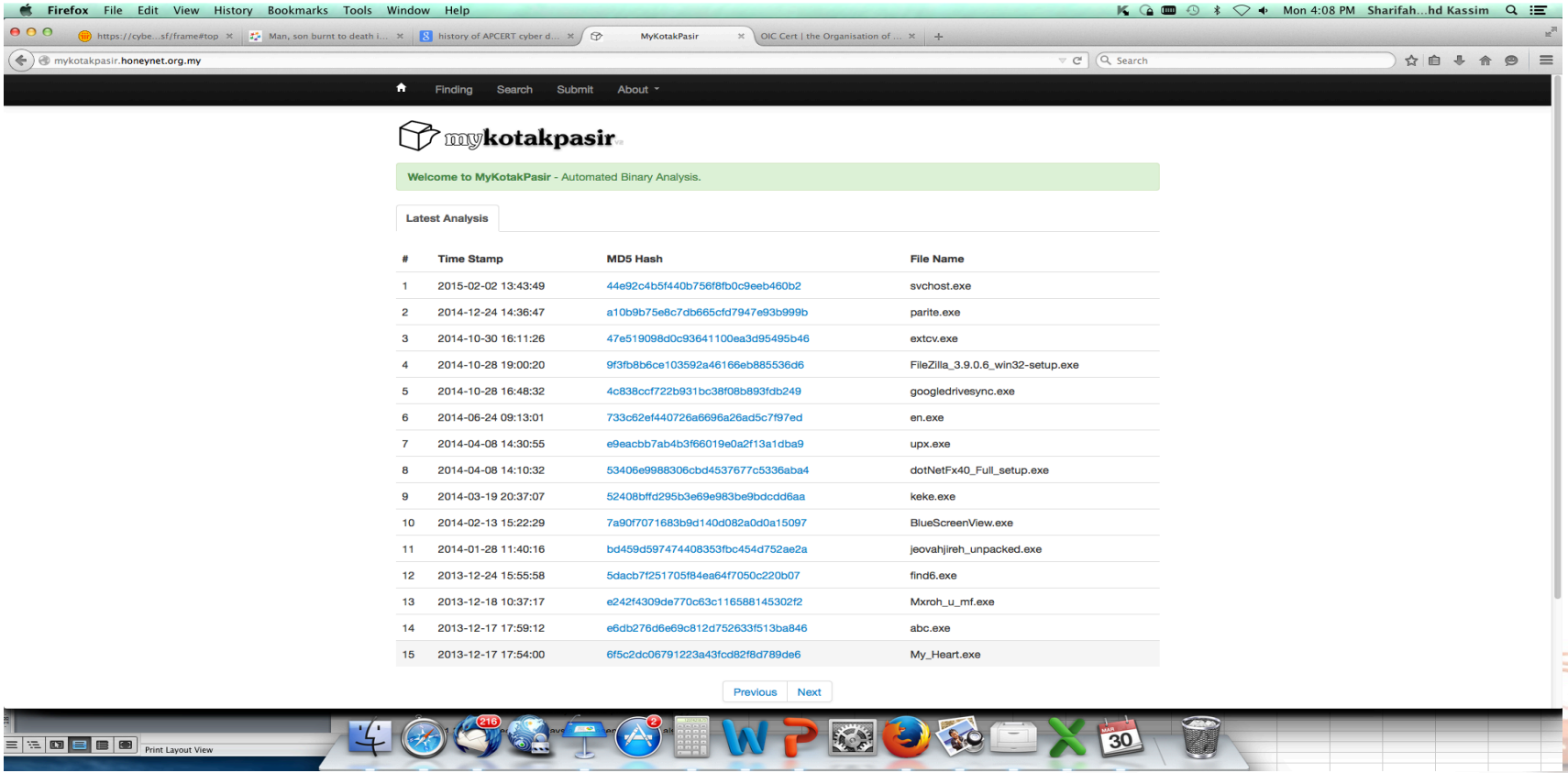
| | |
|---|---|
| Dashboard | • To monitor the Cyber Exercise Status<br>• To monitor Players Status |
| MyKotakPasir | • Players to Submit Malware Binaries<br>• Analyse the binaries and produce findings |
| Malware Checker | • Tool to analyse malware<br>• The tool also can detect and remove malware |
| Andbox | • Automatic android application analysis system |
| Gdecoder | • To deobsfuscate malicious javascript |

# MyKotakPasir

http://mykotakpasir.honeynet.org.my



# MyKotak Pasir Outputs



# Drill Dashboard

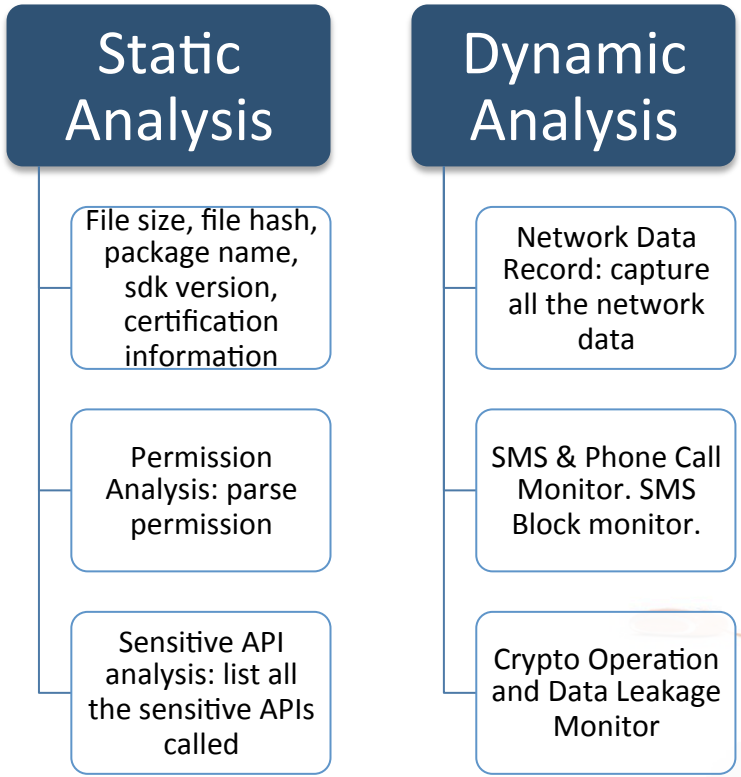
- It's a tool for EXCON to monitor the Cyber Exercise Status
- Helps EXCON to monitor Players Status and may provide assistance
- Provides a complete overall picture of the Cyber Exercise
- Helps to identify if some thing goes wrong during the Cyber Exercise

# Malware Checker

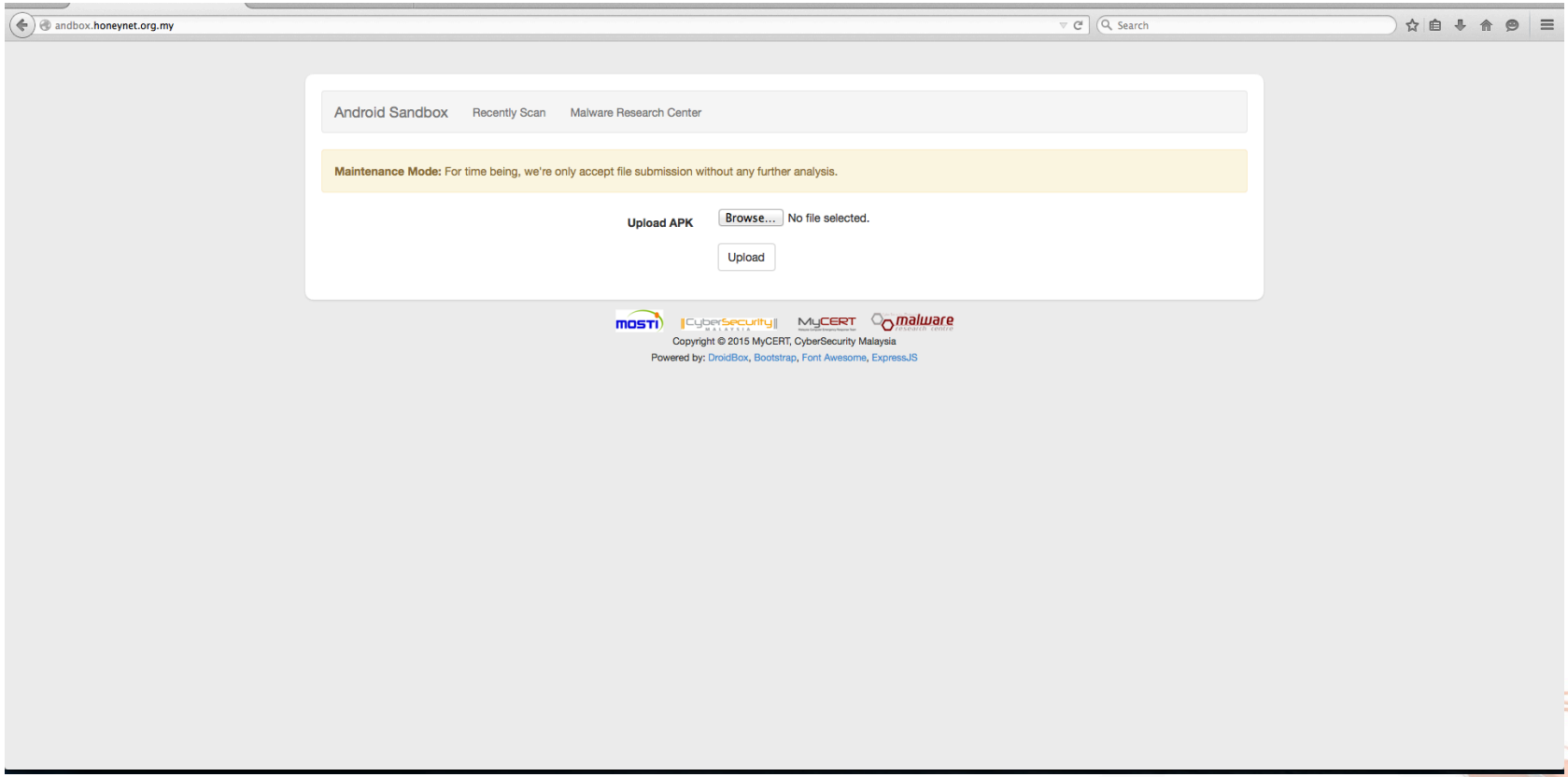
- Simplified in-house developed tool to detect malware presence during Cyber Exercise.
- Notify MyCERT/EXCON about status of infected machine and assist player status whether their machine still infected or not.
- Program are protected from being reverse engineered
- Not a real-time antivirus program.
- This program do not remove the malware. Only for notification to MyCERT/EXCON on infected status on players' infected machines.

# Andbox

Andbox (aka Android Sandbox) an automatic android application analysis system.
URL: andbox.honeynet.org.my



# Andbox Interface



# Gdecoder

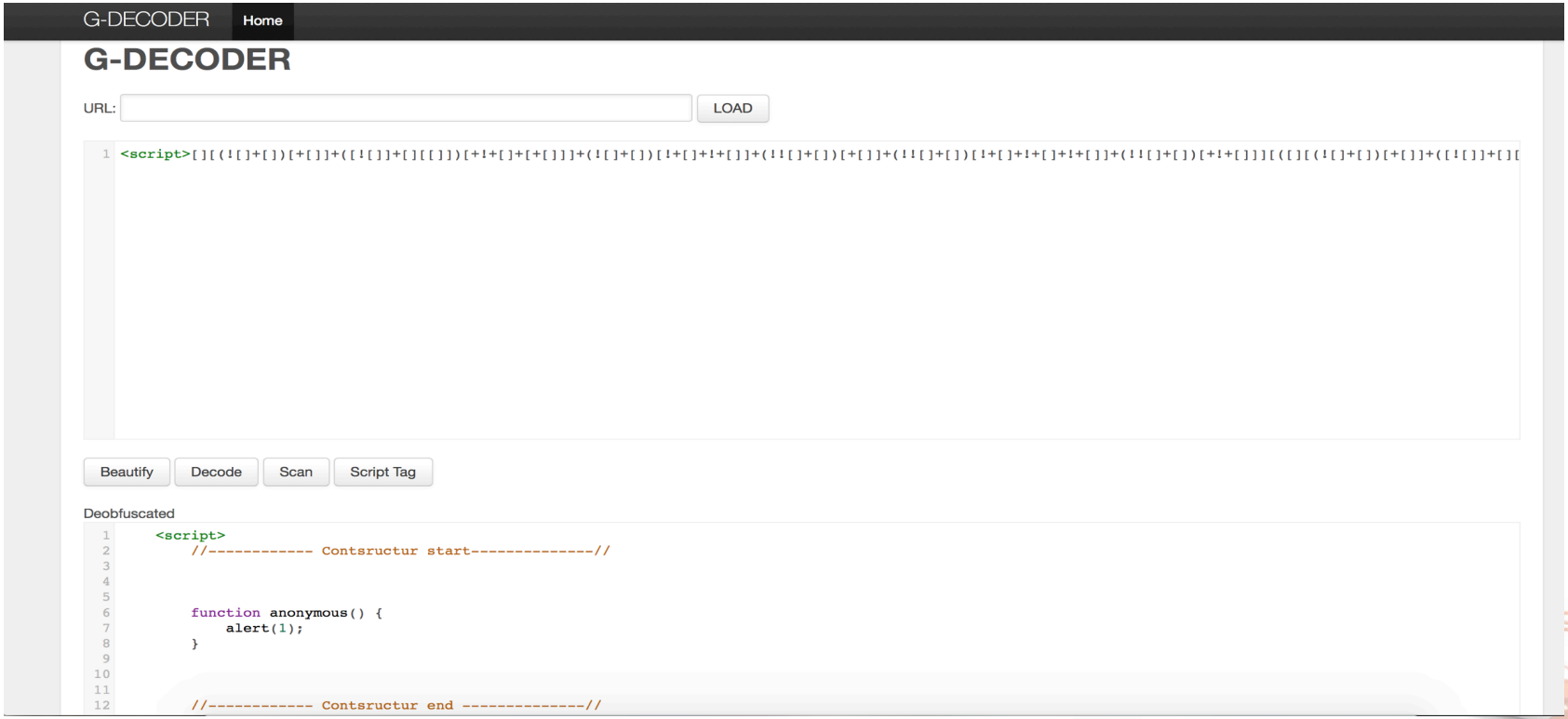
- G-Decoder is a universal javascript deobfuscator which can assist in malicious javascript analysis
- Fully in-house developed for analysis of malicious javascript incidents for quick, fast & economical.

- It comes with HTML DOM emulation engine.
- Intercepts calls to certain functions like eval() or document.write(), and return what would be executed by that function calls.
- The DOM emulation allows the execution of DOM-dependent function calls

- Extensivley used during Cyber Exercises for analysis of malicious javascript
- The Gdecoder is also is allowed for public use. Users can download in the Gdecoder ftr their analysis.

# Gdecoder Interface

https://gdecoder.honeynet.org.my/



# Observations & Expectations

# Observation From Cyber Exercise

| The Good Side | The Bad Side |
|---|---|
| Many player manage to respond to the incident. i.e remove malicious artifacts | Lack of In Depth Analysis Skill among the players and dependent on third party for assistance. |
| Players attended several relevant workshops/trainings prior to the Cyber Exercise | Incompleting the whole Incident response process. |
| Majority of Teams Took Part – Shows Interest, i.e OIC CERT, APCERT. | Lack of Procedures in Incident Response, i.e no prioritizing of incident. |
| Communication amongst players was good using the relevant channels | Contact information was not current and up to date. |

# Common Expectations from Cyber Exercise

1) Common Framework for Incident Response that is well understood and practical for deployment in the event of emergency that affects across borders.

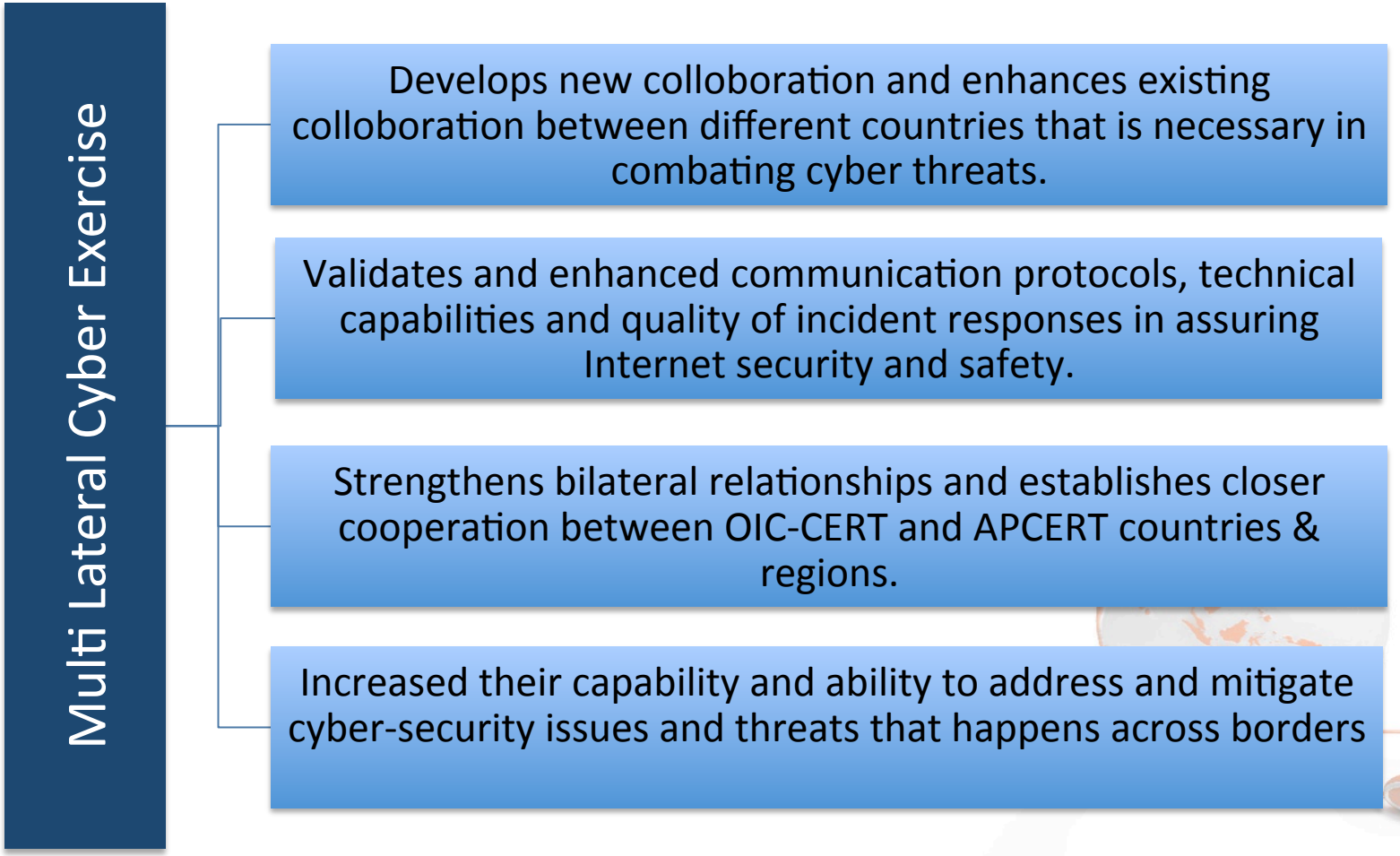
2) Improvement of Processes, Tools and Technology. Improved processes, tools, and training—focused on the analysis and prioritization of physical, economic, and national security impacts of cyber attack scenarios—would enhance the quality, speed, and coordination of response.

3)Information sharing. Analysis and findings may differ between countries. This is the platform that we can look at analysis and findings from different angles presented by different economies.

4) Correlation of Multiple Incidents between countries. Correlation of multiple incidents across the border. We may be efficient in responding to single attacks within our constituency and affecting us only. However, it may be a challenge to respond to mutiple attacks targetting different constituencies and we are part of it.

5) Come up with strategic communications plan that can be used by all teams. The plan will cover the communication among the players, team members and also communication with external parties during an emergency. It is important information flow is properly controlled.

# What We Gained from Multi Lateral Cyber Exercise



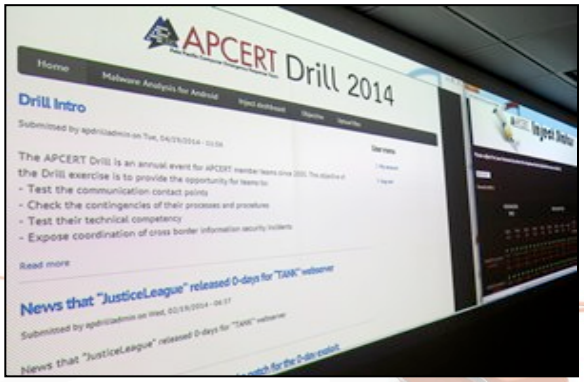
# 2014 Cyber Exercise – APCERT, OIC CERT Colloborates

APCERT today has successfully completed its annual cyber exercise to test the response capability of leading Computer Security Incident Response Teams (CSIRT) from the Asia Pacific economies. APCERT involved the participation of members from the OIC-CERT and the European Government CSIRTs group (EGC) in this drill.

20 CSIRT teams  from 16 economies in APCERT; three CSIRT teams of the OIC-CERT
(Egypt, Pakistan, and Nigeria); and a CSIRT from Germany of the EGC participated in the drill.

Australia, Bangladesh, Brunei, China, Taipei,
Hong Kong, Indonesia, Japan, Korea, Macao, Malaysia, Myanmar, Singapore, Sri Lanka,
Thailand and Vietnam. Malaysia, Brunei and Indonesia are also members of OIC-CERT.

OIC-CERT
The Organisation of The Islamic Cooperation - Computer Emergency Response Team (OIC-CERT)
Computer Emergency Response Team

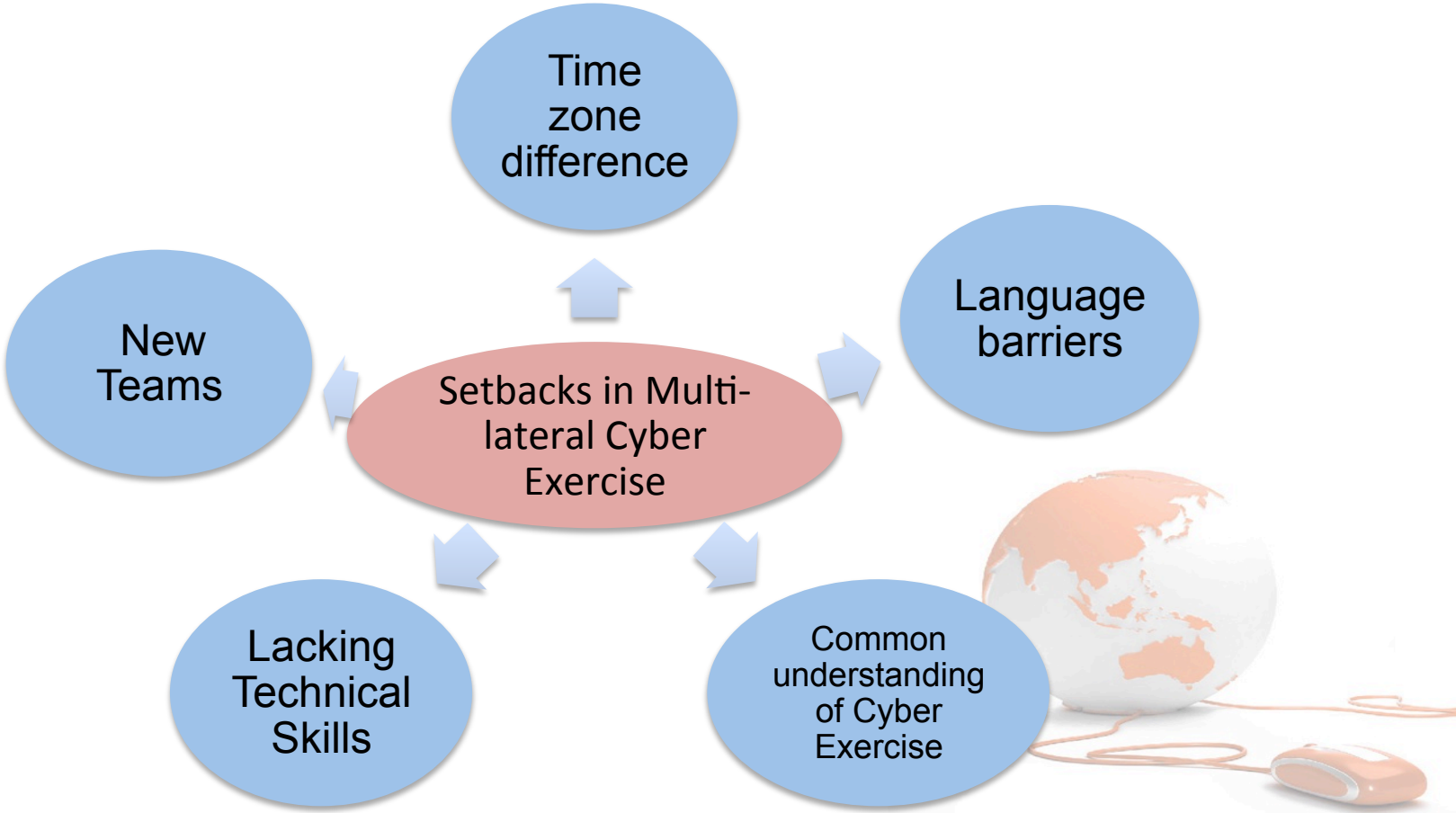


# Findings & Feedbacks

# Sample Findings from OIC-CERT 2014 Multi Lateral Cyber Exercise

- The OIC CERT Drill 2014 was well conducted and met all the intended objectives. 86% meet participants expectation.
- The Drill Organizer (EXCON) were able to coordinate the drill exercise effectively.
- The scenario develop is realistic and relevant with the possible current cyber threats.
- Communication infrastructure prepared i.e. IRC and drill inject were sufficient and well managed.
- The drill exposed the participants to realistic hands-on experience in handling and managing cyber incidents

# Nothing is Perfect



# Sample Feedbacks from Players of OIC-CERT 2014 Cyber Exercise

One of the team suggested for tutorial regarding to solve the drill exercise.

To have more interactions and incident escalation between CERTs and to include forensic investigation.

To include exercise on how to do recovery of infected system and data exercise.

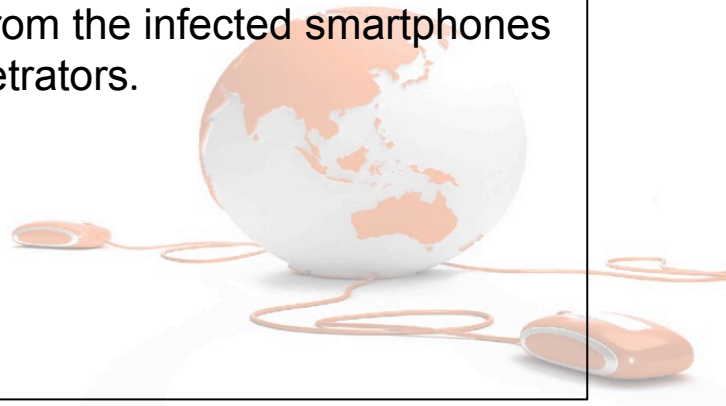
EXCON to provide more assistance before the drill day event.

# Sample Case Studies

# Example 1 of Cross Border Incident: Mobile Botnet Targeting Malaysian Smartphone Users- TwnCERT

***Incident 1***

Mobile botnet that spreads malware via SMS messages targetting Android smartphone users. Users who clicked on the link in the SMS message, installed a malicious Android Package (APK) that took control of their mobile phone. The infected smartphones can be hijacked remotely and potentially used for fraudulent purposes **such** as buying digital goods and services. The smartphones can also be used for spreading the malware to more smartphones by sending SMS with link to malicious APK. Phone numbers extracted from the infected smartphones are stolen and can be used for malicious activities by perpetrators.



# Example 1 of Cross Border Incident: How Multi Lateral Cyber Exercise Assisted in this Incident

**Contact**
- Contacts were easily available for further communication on the incident

**Comm**
- Speed up communication between both parties on responding to this incident

**Escalate**
- Information provided was used for details analysis & findings escalated to local Telcos for eradication

**Advisory.**
- Information provided by TwnCERT was used to publish an Advisory on this malicious mobile botnet to alert the general public in our constituency.

# Example 2 of Cross Border Incidents: Nitol Botnet Infection - CNCERT

***Incident 2***

Received daily feeds report regarding Nitol botnet infections originate from .MY constituency targetting systems in China.
Source of infections are from various .MY IPs. MyCERT analysed the logs to verify the feeds data such as the source of infections. MyCERT notified the infected IP Admins/ISPs for clean up and rectification.

# Example 2 of Cross Border Incidents: Nitol Botnet Infection to China Domains

**Contact**

- CNCERT had communicated well with MyCERT's contact persons on the incidents.

**Comm**

- The incident was well communicated in which feeds data was sent daily to MyCERT that contains infected IPs from .MY constituency

**Speed**

- The incident has also taught MyCERT to respond in fast and speed mode, by automating the escalation to ISPs for immediate remediations.

# Areas of Improvement & Conclusion

# Areas of Improvement from the Multi Lateral Cyber Exercise

- Swift Communication. Communication is very essential during incidents and for fast mitigations of incidents
- Common understanding of laws & regulations across borders. It is essential to know and understand different country's regulations.
- Effective time management. Management of time among the teams that come from different zones
- Diversity in Analysis Tools. Having diversed tools and efficient is important for accurate analysis
- Right Contacts. Having right people and right person in charge will ensure incidents are responded fast and efficiently.
- Breaking the Language & Cultural barriers.

# Conclusion

MyCERT had leveraged our experience in organizing Multi Lateral Cyber Exercise for the Organisation of Islamic Cooperation - Computer Emergency Response Team (OIC-CERT), the Asia Pacific Computer Emergency Response Team (APCERT) as well as for the South East Asia CERTs Cyber Exercise.

From MyCERT point of view, overall the cyber exercise provides opportunity for participants to face realistic incident, testing out internal technical capabilities and analyse cyber threat.
Areas for improvement still exist from both sides, i.e. cyber exercise organizer and participant to ensure future cyber exercise activities will be done successfully and meet all necessary objectives. Most importantly encouraging and getting full participations from the team

MOSTI
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

ISMS SIRIM
CERTIFIED TO ISO/IEC 27001:2005
CERT NO. : AR4656

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

MSC MALAYSIA Status Company

Best Child Online Protection Website