# Are Cyber Security Exercises Useful? The Malaysian Case Study

Adli Wahid
Head of Malaysia CERT (MyCERT)
Email adli@cybersecurity.my
Twitter: adliwahid


ARCTIC OCEAN
Greenland
Svalbard (Nor.)
ARCTIC OCEAN
United States of America
Canada
Iceland
Norway
Sweden
Finland
Russia
United Kingdom
Denmark
Ireland
Neth.
Ger.
Pol.
Estonia
Latvia
Belarus
Ukraine
Kazakhstan
Mongolia
France
Italy
Rom.
Georgia
Bulgaria
Azer.
Uzb.
Turkm.
Kyrgyzstan
Tajikistan
Portugal
Spain
Turkey
Greece
Tunisia
Syria
Lebanon
Iraq
Iran
Afg.
Pakistan
China
N. Korea
S. Korea
Japan
Nepal
Bhutan
Morocco
Algeria
Libya
Israel
Jordan
Kuwait
Egypt
Saudi Arabia
U.A.E.
Oman
India
Laos
Taiwan
Western Sahara
Mauritania
Mali
Niger
Chad
Eritrea
Yemen
Djibouti
Sudan
Bangl.
Burma
Thailand
Vietnam
Philippines
Cambodia
Senegal
Guinea-Bissau
Sierra Leone
Liberia
Cote d' Ivoire
Ghana
Togo
Nigeria
Cam.
C.A.R.
Ethiopia
Somalia
Sri Lanka
Malaysia
Gabon
Dem. Rep of Congo
Uganda
Kenya
Tanzania
Rep. of the Congo
Indonesia
Papua New Guinea
Solomon Islands
Fiji
Angola
Zambia
Malawi
Madagascar
Namibia
Zimbabwe
Botswana
Mozambique
Swaziland
Lesotho
South Africa
Australia
New Zealand
Mexico
Guatemala
Honduras
Nicaragua
Costa Rica
Panama
Colombia
Ven.
Guyana
French Guiana
Suriname
Ecuador
Peru
Brazil
Bolivia
Paraguay
Chile
Argentina
Uruguay
PACIFIC OCEAN
ATLANTIC OCEAN
INDIAN OCEAN
PACIFIC OCEAN
ATLANTIC OCEAN
I am HERE ☹

# Key Points

1. Cyber Security Exercises in MY
2. What the Players Say?
3. Useful? Yes or No
4. The June 2011 Incident
5. Lessons Learned

# Cyber Security Exercises in MY

| Year | Exercise Name | # Participants / Organizations |
|---|---|---|
| 2007 | MYDRILL07 | 7-8 orgs |
| 2008 | X-MAYA | 10 |
| 2009 | X-MAYA 2 | 28 |
| 2010 | X-MAYA 3 | 34 |
| 2011 | X-MAYA 4 | 66 |

# Who is Involved ?

1. National Security Council (Lead Organizer)
2. CyberSecurity Malaysia / MyCERT – Exercise Controller / Scenarios + Artifacts
   Developer / Backend / Overall DrillFoo
3. Players – Critical Information Infrastructure Agencies

MOSTI

CyberSecurity MALAYSIA

# National Cyber Security Policy (NSCP)

**Thrust 1:**
Effective Governance

**Thrust 2:**
Legislative & Regulatory Framework

**Thrust 3:**
Cyber Security Technology Framework

**Thrust 4:**
Culture of Security & Capacity Building

**Vision:**

"Malaysia's CNII shall be secured, resilient and self-reliant. Infused with a culture of security it will promote stability, social well being and wealth creation"


**Thrust 5:**
R&D Towards Self Reliance

**Thrust 6:**
Compliance & Enforcement

**Thrust 7:**
Cyber Security Emergency Readiness

**Thrust 8:**
International Cooperation

# Exercise Objectives

1. Get the agencies to familiarize with the National Cyber Crisis Management Procedures (NCCMP) *
2. Improve overall cyber security readiness of CNII agencies
3. Encourage sharing of information between agencies

# How we (MyCERT) got involved

1. National Cyber Security Response Center (Got Incidents?)

   * 8 – 12 people involved

2. Participated and help co-ordinate APCERT Exercises in the past

# Evolution

| Year | Exercise Name | # | Nature / Backend Work |
|---|---|---|---|
| 2007 | MYDRILL07 | 8 orgs | Desktop Exercise |
| 2008 | X-MAYA | 10 | Hands-on / 'Blackbox' |
| 2009 | X-MAYA 2 | 28 | Hands-on / Progress Tracking |
| 2010 | X-MAYA 3 | 34 | Hands-on / Progress Tracking/ Automation |
| 2011 | X-MAYA 4 | 66 | All of the above + Infrastructure Hosting (The Cloud?) |

# Back-End Stuff

| Details | The Return of Anonymous LulzDrill | 0% |
|---|---|---|
| 2011-11-15 09:06:09 | - Senario started - | |
| 2011-11-15 09:18:12 | Anonymous LulzDrill's video | |
| 2011-11-15 14:11:57 | Analysis of Infected Web Server Released | |
| 2011-11-15 15:06:09 | Lulzdrillz IRC Information Released | |
| 2011-11-15 16:37:12 | Joomla Advisory Provided | |
| **Details** | **The Malware** | **0%** |
| 2011-11-15 11:28:38 | - Senario started - | |
| 2011-11-15 15:24:01 | Infected Machine's PCAP Provided | |
| 2011-11-15 16:51:02 | Infected Machine's Analysis Provided | |

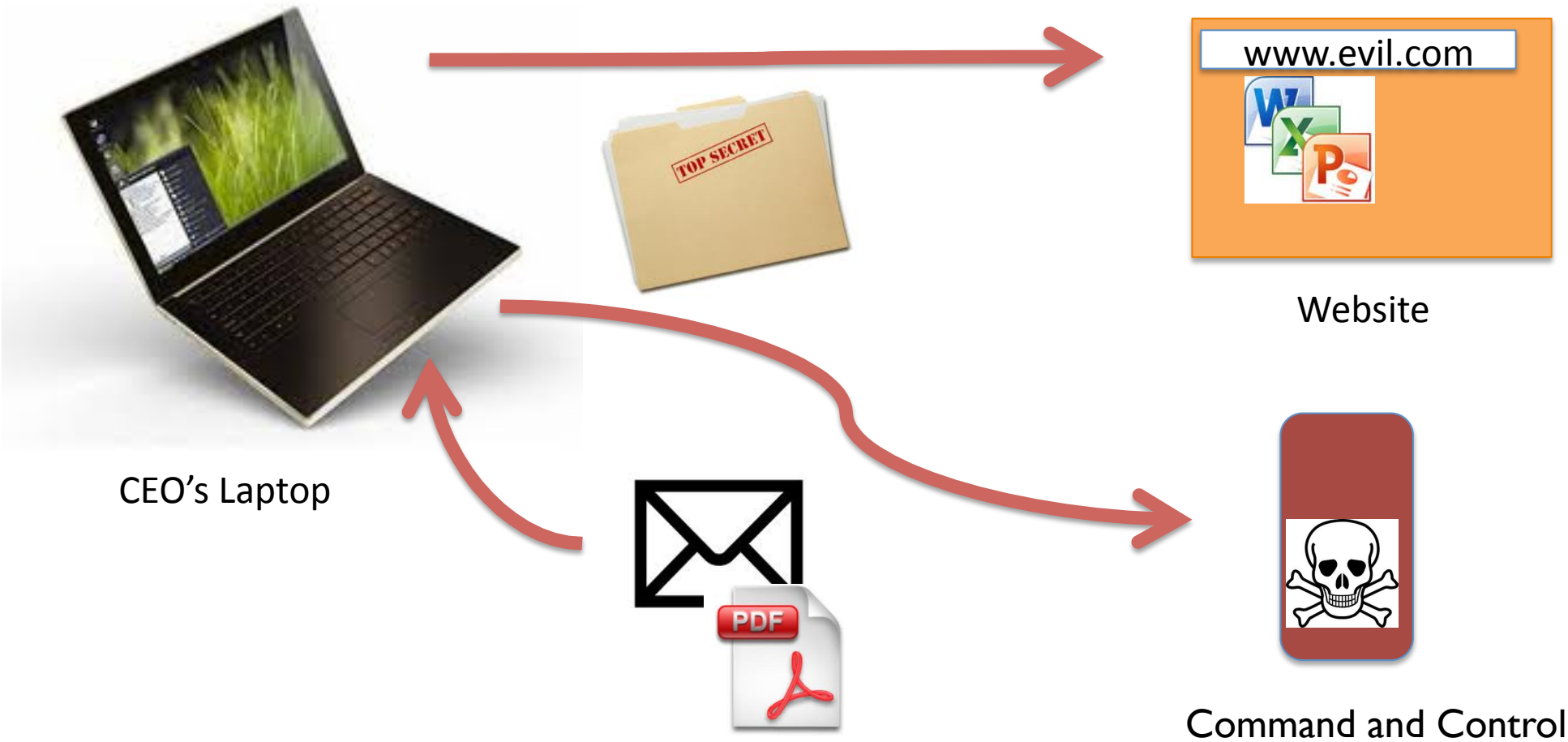
# Activities

1. Overall Planning, Call for Players
2. Training for Players (Procedures, Incident Response, Mini Drills)
3. Scenario & Artifacts Development
4. Infrastructure Building
5. D-Day
6. Post-Drill Stuff

* Takes many months

# Example of Scenarios

# Who Pwn3d Our CEO ?




Scenario from National Cyber Security Exercise 2010 (X-Maya 3)

# #OpsLulzDrillzMY

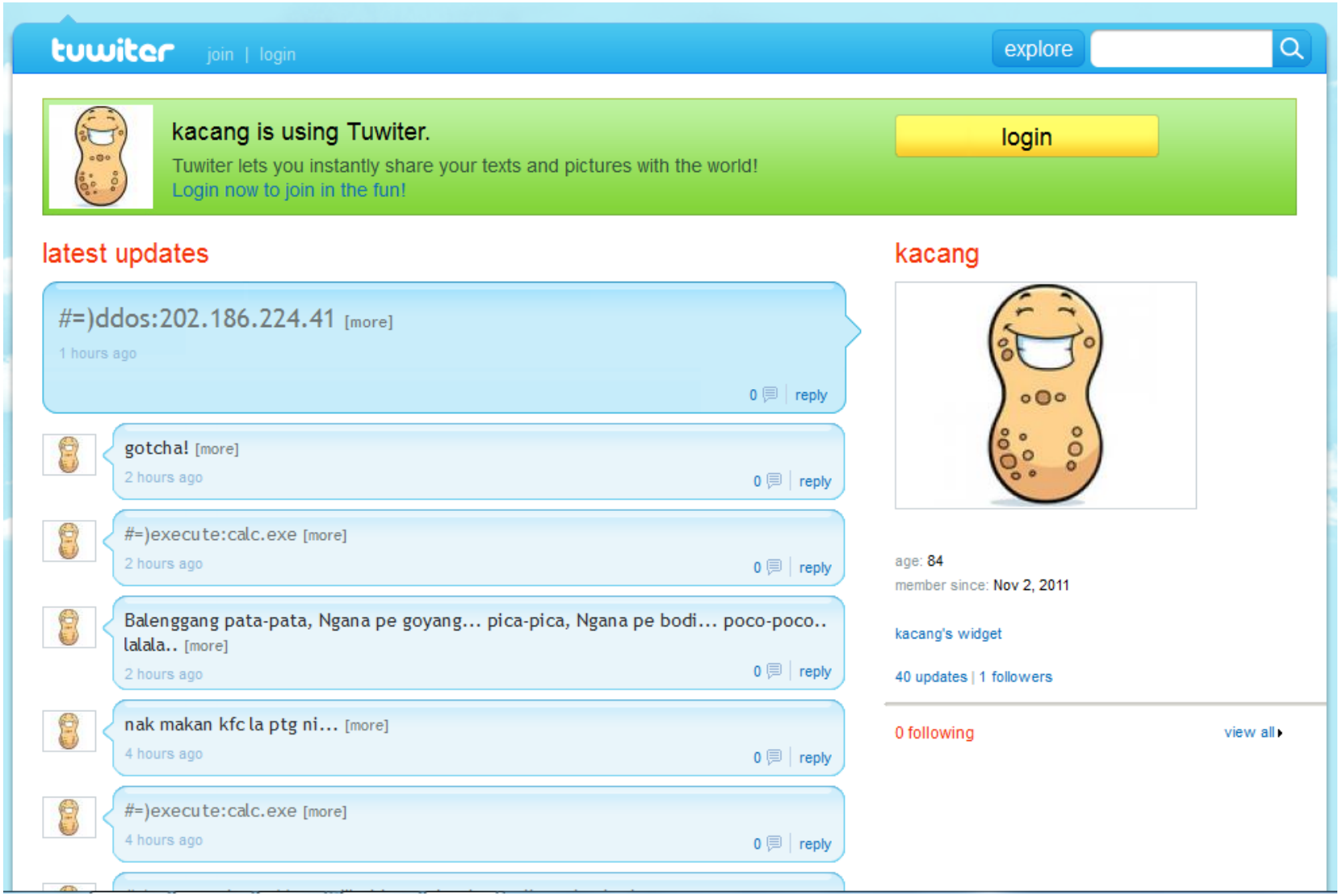
1. (Fictitious) Group LulzDrillzMY wants to attack .MY (again)
2. DDoS Sites of Agencies
3. Release DDoS Tool that is backdoored
4. Infected computers can be controlled by Twitter like service
5. Attacks announced in real time in #irc channel

Scenario from National Cyber Security Exercise 2011 (X-Maya 4)

# Video on MayaTube

# Crowd Sourcing

# Tuwitter: Infected machine management



# Scenarios Expectations

1. Most important is adherence to procedures i.e. escalation, threat levels declaration etc
2. Technical – fixing the problem

[redacted]

| Details | The Return of Anonymous LulzDrill | 100% |
|---|---|---|
| 2011-11-15 09:06:09 | - Senario started - | |
| 2011-11-15 09:18:12 | Anonymous LulzDrill's video | |
| 2011-11-15 10:38:09 | Backdoor account removed | |
| 2011-11-15 10:40:18 | Web Shell removed | |
| 2011-11-15 14:11:56 | Analysis of Infected Web Server Released | |
| 2011-11-15 14:15:29 | SQL Injection vulnerability patched | |
| 2011-11-15 14:15:29 | -- Senario ended -- | |
| 2011-11-15 16:37:12 | Joomla Advisory Provided | |
| **Details** | **The Malware** | **100%** |
| 2011-11-15 11:28:38 | - Senario started - | |
| 2011-11-15 15:24:00 | Infected Machine's PCAP Provided | |
| 2011-11-15 16:51:00 | Infected Machine's Analysis Provided | |
| 2011-11-15 16:51:15 | CnC of malware reported | |
| 2011-11-15 16:53:57 | Infected machine cleaned | |
| 2011-11-15 16:59:07 | URL of malware identified | |

# What do the Players Say?

Positive

1. Exercise is good and realistic
2. Practical way to learn about the National Cyber Crisis Procedures
3. Helps to develop internal CSIRTs capabilities/ understanding
4. Let's do this more than ONCE a year

* Score 85-95% Satisfaction for all exercises

# What do the Players Say (2)

Not So Positive

1. We Don't Use X (software/servers/etc) in our infrastructure so Not Fair
2. How do we know if we are done? (And what is our rank/position)
3. We didn't do A, B, C because it is not in our SOP

# Some Challenges

MyCERT

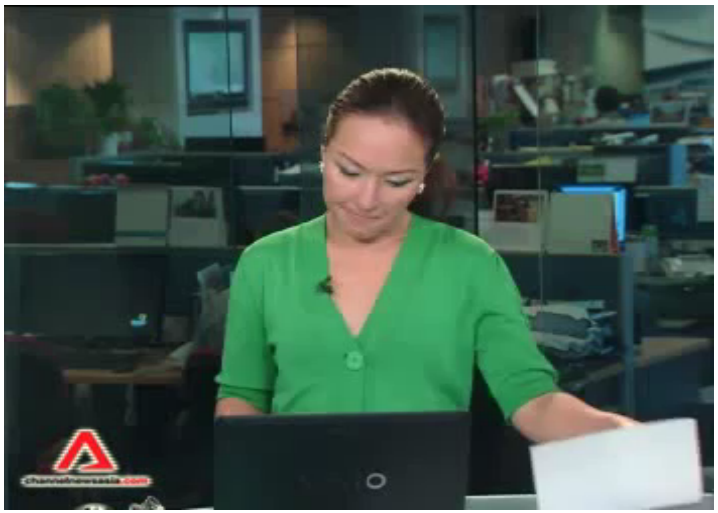
1. Keeping things real
2. Players = Players + Vendors
3. Managing a large Game

Players

1. Same as Not-So-Positive Comments in Previous slide

# A Good/Real Test – June 2011

# Anonymous vs Malaysia (June 15 2011)

# So Are Cyber Security Exercises Useful?

# Lessons Learned

1. YES, useful to a certain extent, but
2. Effective for organizations that have security in place *
3. Everybody does not have to 'play' at the same time
4. Keep the objectives in mind, don't go overboard with the scenarios


Panasonic
To do
(1) Define Roles


malware
research centre
MyCERT
Malaysia Computer Emergency Response Team

# Thank You for Listening!

- Find out More
  - www.cybersecurity.my
  - www.mycert.org.my
- Personal
  - adli@cybesecurity.my
  - Twitter: adliwahid