Responding to Security Incident: MyCERT approach and case study

FIRST TC 2012 @ KYOTO
13-15 November 2012

By: Megat Muazzam Abdul Mutalib
Manager Emergency Response (Cyber999), MyCERT
Agenda

- About MyCERT
- Trends + Statistic
- Case Study
- Success and Challenges
MyCERT

• Established in 1997
• Roles:
  – Incident Handling & Response
  – Technical Co-ordination
  – Alert and Advisories
  – National Cyber Security Exercises
• Works closely with various partners, locally and Internationally
• Constituents: ALL Internet users in Malaysia
MyCERT (2)

• 2 Core Groups
  – Cyber999 / Incident Response
  – Malware Research Centre

• Strengths
  – 20 Personnel
  – > 10 until 2007
  – Supported by other departments and initiatives at CyberSecurity Malaysia
MyCERT (3)

• No ‘Enforcement Power’
  – Based on trust
  – Provide technical expertise for assisting victims of cyber security incidents

• Collaboration
  – Vast network of contacts via other security teams, vendors and law enforcement agencies
Cyber999 Statistical Reports
Overview of Stats

• Growth of Incidents reflect ‘changing’ times and more reliance of the Internet
  – i.e. rise of harassment and scam due to prevalence of social networking
  – Ability for the team handle more incidents increased after 2007 due to more resources

• National CERT fills in the gap in dealing with emerging threats – i.e. malware, phishing, targeted attack, cyber harassment and more

• Incident data created awareness, generate interests and pushed forward other initiatives
  – CNII Protection, Cyber Crisis Management, Training and Awareness
Incidents Handled 1997 – 2011

More resources resulting better handling due to automation

Source: www.mycert.org.my
Fraud Incidents 1997 – 2011

Trend: Criminals increasing their efforts to target Internet users due to growth of E-Commerce + Lack of user awareness i.e. Phishing, Advanced Fee Fraud

Source: www.mycert.org.my
Rise of Malware particularly botnet had provide resources to be used for DDoS. Increase of activities of Hacktivism recently led to this increasing trend

Source: www.mycert.org.my
The rise of malware, hacking tools coupled with lack of best practices in deploying and managing servers/computers contributed to the rise in intrusion incidents.
Social networking sites, video, blogs and lack of etiquettes led to the increase in users being abused or harassed.

Source: www.mycert.org.my
Advisories & Alerts Published 1997 - 2011
Statistic by Incident (1st Half 2012)
Case Study
Case Study: Job Scam

- **The Setup**
  - Poses as a recruitment agency
  - Email sent to potential victim that really looking for job
  - Impersonate local MNC – usually in oil and gas industry
  - Victim most of it is not local

- **What actual happen**
  - Email sent usually spoof
  - Entice victim by giving job description / salary / attractive perk
  - Eventually a charge is required as a processing fee for Employment Registration Certificate / Visa / Registration Card

- **The Risk**
  - Money lost
  - Still end up without a job
From: petronas476@xyz.com
Subject: JOB OPPORTUNITIES@ PETRONAS OIL COMPANY MALAYSIA
Date: Wed, 22 Dec 2010 18:23:33 +0000

Dear Employee,

We have confirmed your CV/Resume, in the below mail you will find the current positions where expatriates are needed in our Company.

All the positions include these below benefits:

1. Five Bedroom Flat Duplex
2. Free Medical & Travel Insurance
3. 10 Days Leave / break/ Vacation after every 90 working days
4. Flight Fares (Air Tickets)
5. Free Toyota Camry 2007 Model.

A. Current CV/Resume
B. One Reference Letter.
C. Passport Copy.

The Documents should be provide to us through scan e-mail attachment For fast processing, because all the positions need expatriates" who Can be able to start up employment on January/March 2011, and all the Arrangement need to be made as fast as possible.
Case Study: Job Scam (Sample)

EMPLOYMENT AGREEMENT

We refer to your earlier forwarded application for job engagement with relations to
SAPURACREST PETROLEUM BERHAD (MALAYSIA)

On the above subject matter SAPURACREST PETROLEUM BERHAD
(MALAYSIA) hereby congratulates you on your successful emergence based on
detailed by our career department

Further details are as follows:

JOB REFERENCE NUMBER:
SCP/01310/KLM
Case Study : Fraud Purchase

- **The Setup**
  - Send in your money and get nothing

- **What actual happen**
  - Never get the product promised
  - Promises don’t match the product
  - Product description may be vague, incomplete or completely fake

- **The Risk**
  - Get ripped off
  - Losing time and money
Case Study: Nigerian Scam

- **The Setup**
  - Receive an email written in screaming capital letter or very lengthy
    Example - "DEAR SIR/MADAM: I REPRESENT THE RECENTLY DEPOSED MINISTER OF AGRICULTURE FOR NODAMBIZIA, WHO HAS EMBEZZLED 30 MILLION DOLLARS FROM HIS STARVING COUNTRYMEN AND NOW NEEDS TO GET IT OUT OF THE COUNTRY..."
  - Scammers are seeking an accomplice to transfer funds and you will get the cut – 10%
  - But before transfer can be finalized you must pay for unnecessary advance fees

- **What actually happens**
  - There is no minister and no money
  - Except the money victim have put in advance

- **The Risk**
  - Serious financial loss or worse
  - Losing time and could probably threaten
Case Study: Fraud Site + Lottery/Sweepstake Scams

- The Setup
  - Selling product or services to potential victim
  - Company not legally registered
  - Perpetrated via mail which contain colorful brochure or scratch card

- What actually happen
  - One of the card always a winning card
  - To claim price always asked to provide payment for various fees via wire transfer

- The Risk
  - Serious financial loss
  - Losing time
Welcome to Pro-Link

As UK & New Zealand’s leading express courier, logistics and distribution company, Direct Post brings you ‘The Whole Package.’

Combining the capabilities of Pace, Courier Post, Roadstar and Contract Logistics, with the transport strength of New Zealand Post, our Whole Package brings you speed, reach and control within a customized solution for your business.

Direct Post is the partner of choice for a number of UK companies including ACP Media, Poste Plus, Ezibuy and OfficeMax. We proudly support worthwhile causes such as the Starship Foundation and KidsCan Charitable Trust as a way to support the New Zealand communities we operate in everyday.
What We Are Seeing
The Source of all—A Lot of Evil

- Information Loss
- Financial Loss
- Badness
  - Denial of Service Attacks
- Your PC might be hosting malware or serving malware
Malware Research Centre

• Malware Response since 1997
  – Infected Machines feeds
  – Command and Control take downs / Monitoring
  – Removing evilness* from servers/sites
  – Tracking and Analysis
  – Advisory and Alerts
  – “I think I got something in My PC” requests
  – Malware samples & Feed Exchange
Malware Incident 2011
Malware Research Centre (MRC)

Projects/Activities

Emerging Threats
LebahNet Project
Threats Visualization
Malware Research
Advisory & Alerts

Innovative Tools Produced

Malware Sandbox
AntiPhishing Plugin
Malicious PHP Analyzer
PHP WebApp IPS
PDF Analyzer
AntiPhishing Portal
.My Malware Project
DNS Watch – Site detection
(FREE) Tools from the Lab

DontPhishMe!  DNSWatch  PKaji

Dontphishme: Plugin for Firefox and Chrome

Mozilla Add-On: https://addons.mozilla.org/en-us/firefox/addon/dontphishme/

Chrome Add-On: https://chrome.google.com/webstore/detail/ekhmajimailppllbglbkopdjfenocpnl

Currently support local Financial Instituion / Bank at Malaysia
Why Are You Here

WARNING!

The web page you tried to visit might have been trying to steal your personal information. That page was removed after being identified as a "phishing" web page. A phishing web page tricks people out of bank account information, passwords and other confidential information.

How You Were Tricked

This email is from my bank. It asks me to update my information. I better click on the link and update it.

STOP!
Don't fall for it.

How to Help Protect Yourself

1. Don't trust links in an email.
2. Never give out personal information upon email request.
3. Don't call company phone numbers in emails or instant messages. Check a reliable source such as a phone book or credit card statement.
4. Name:[Jane Smith]
Submit to us the suspicious links and let us verify

Received a phishing email? Send it to us by forwarding the email that contains the URL. Our incident response team will help in verifying the submitted URLs and taking necessary actions.

MyCERT collects and handles URLs related to phishing. In the table below, you can find the latest URLs used in phishing scams.

Daily Phish Stats

- Local Brand hosted in Domestic Server
- Local Brand hosted in Foreign Server
- International Brand hosted in Domestic Server
- International Brand hosted Foreign Server

Quick Stats

7 days phish

Upcoming Events

counter ecrime operations summit
DNSWatch (Service)

- Released in August 2011 as a service
- Started initially as a different project (DNSMon) as a result of monitoring conficker infected clients querying known_malicious_dns
- What do we do with a list of known ‘bad’ URLs?
  - From honeypots and other public/non-public sources
- We offer a DNS Service, when users visit a potentially malicious site that has been blacklisted, redirect to a landing page
  - This will alert and hopefully get user curious enough to fix the problem
Opps.. you are redirected to DNSwatch landing page

The page that you are trying to access is known to be hosting malware

You are trying to access a [redacted] which is associated with known malicious domain. For more information please contact us.

WARNING: visiting this site may harm your computer

False positive? Report to honeynet@cybersecurity.my

DNSwatch (alpha version)
Brought to you by

[Logos of MOSTI, CyberSecurity Malaysia, MyCERT]
DNSChanger Malware Cleanup

• What is DNSChanger
  – malware that infect computers with the purpose of diverting traffic to potentially illegal and malicious websites. The malware modifies the infected computer's DNS server setting replacing it with DNS server belonging to the attackers.

• MyCERT Advisory
DNSChanger Malware Cleanup

- Detection (http://dnschanger.detect.my)

- Removal Step available at MyCERT website
DNSChanger Malware Cleaning
DNS Changer: IP Addresses Count – Based on Reports from Shadow Server Foundation
Awareness

• CyberSAFE Project
  – Cyber Security Awareness for Everyone
  – http://www.cybersafe.my

• Addresses amongst other things, Phishing and ID Theft issues

• Engagement with Media and Public to promote the message

• Production of educational materials (feel free to re-use)
Publish Advisory / Alert / News

• Came out with advisory

“MA-228.042010:MyCERT Advisory - Phishing Attempts Targeting Public Bank Malaysia Users”


• Publish newspaper article

“Steer clear of phishing sites”
Mode of Incident Reporting

- Email
  - cyber999@cybersecurity.my
- Phone/Hotline
  - +603 8992 6969
  - 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 0830 – 1730
Success and Challenges (I)

• A “1-Stop-Centre” work to a certain extent. Incidents experienced by Public and Private Organizations and Individuals provided the bigger picture for the stakeholders.

• Cost savings is there but no hard data.

• End-to-end resolution is challenging both locally and internationally. Often stops at escalation and does not translate to prosecution (or money returned in the case of Fraud).
Success and Challenges (2)

• Being able to focus allow expertise to be developed. The CERT were able to release tools and services to deal with problem of the day – i.e. DontPhishMe!, PDF Analyzer, LebahnetMini (Honeypot)

• Lessons learned can be translated into awareness materials. But how do we measure the state of awareness? Number of incidents keep to continue – See [www.cybersafe.my](http://www.cybersafe.my)
Conclusion

• Security incidents happen!
• Managing security incidents is critical both at the enterprise, country and global level
• Having a dedicated team to handle incidents will ensure that potential damaged is contained and lessons can applied for improvements to steer other initiatives
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 80 2999

www.cybersecurity.my
info@cybersecurity.my

www.facebook.com/CyberSecurityMalaysia
twitter.com/cybersecuritymy
www.youtube.com/cybersecuritymy