



Promoting a Culture of Cybersecurity among *Critical National Information Infrastructure*

ITU Workshop, Doha, Qatar
February 18-21, 2008
By R.Azrina R.Othman
CyberSecurity Malaysia



Agenda

- Background of Cyber Security Issues
- Introduction to the National Cyber Security Policy
- Awareness level
- Knowledge Sharing Platform
- Cyber Security Exercise
- Way Forward



Recent Incident Of Cyber War Against A Nation

Cyber Attack on Estonia

- Occurred in May 2007
- Estonia was under cyber attacks for 3 weeks
- Attack targeted government, banking, media and police websites
- Paralyzed internet communication.
- Attacks from 128 sources outside Estonia
- US and European countries aided Estonia in overcoming the cyber attacks



Impact:

Huge economic losses incurred as online based transactions were disrupted



Cyber Attacks on Malaysia?



**WHAT IF OUR CRITICAL INFRASTRUCTURE
ARE UNDER ATTACK ?**

ARE WE READY ?

HOW DO WE DEAL WITH IT ?



Agenda

- Background of Cyber Security Issues
- Introduction to the National Cyber Security Policy
- Awareness level
- Knowledge Platform
- Cyber Exercise
- Way Forward



Introduction to The National Cyber Security Policy

In 2006, **National Cyber Security Policy (NCSP)** was initiated by the Ministry of Science Technology and Innovation, to harness national effort to enhance the security of Malaysia's **Critical National Information Infrastructure (CNII)**



Objective of the National Cyber Security Policy

1

To address the risks to the CNII

2

To ensure that critical infrastructure are protected to a level that commensurate the risks faced

3

To develop and establish a comprehensive program and a series of frameworks

NCSP OBJECTIVES



National Cyber Security Framework

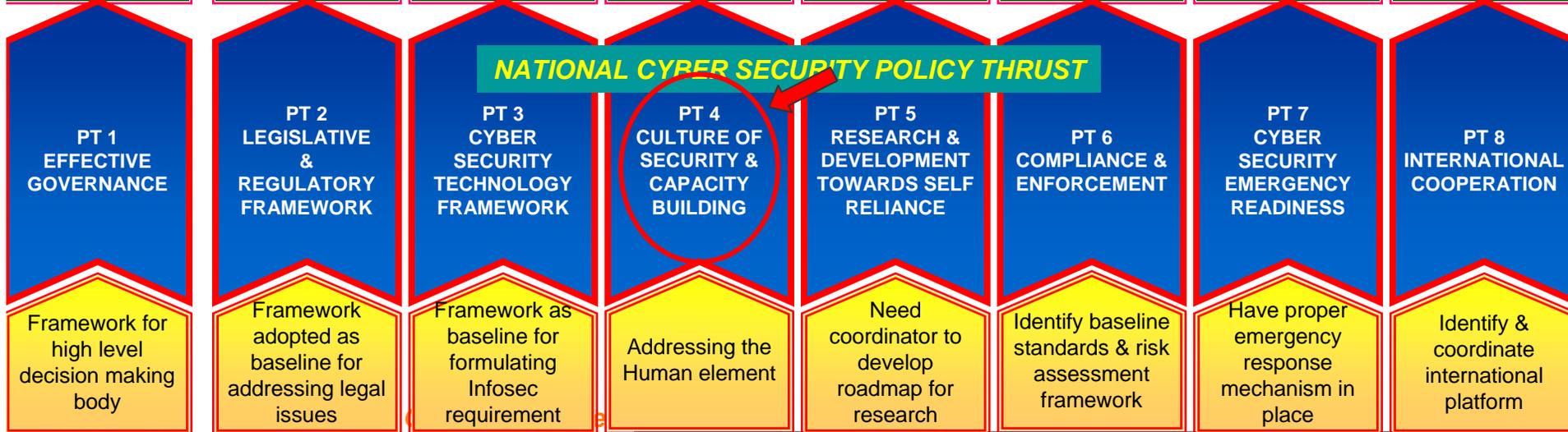
Malaysia's Critical National Information Infrastructure will be secure, resilient and self-reliant. Infused with a culture of security, it will promote stability, social well being and wealth creation'



CRITICAL NATIONAL INFORMATION INFRASTRUCTURE

- Establishment of a national info security coordination centre
- Reduction of & increased in success in, the prosecution in cyber crime.
- Expansion of national certification scheme for infosecgmt & assurance
- Reduced no. of InfoSec incidents through improved awareness & skill level
- Acceptance & utilization of local developed info security products
- Strengthen or include infosec enforcement role in all CNII regulators
- CNII resilience against cyber crime, terrorism, info warfare
- International branding on CNII protection with improved awareness & skill level

NATIONAL CYBER SECURITY POLICY THRUST



NCSP's Policy Thrust 4: Culture of Security & Capacity Building

- Develop, foster and maintain a national culture of security
- Standardise and coordinate cyber security awareness and education programmes across all elements of the CNII
- Establish an effective mechanism for cyber security knowledge dissemination at the national level
- Identify minimum requirements and qualifications for information security professionals



Agenda

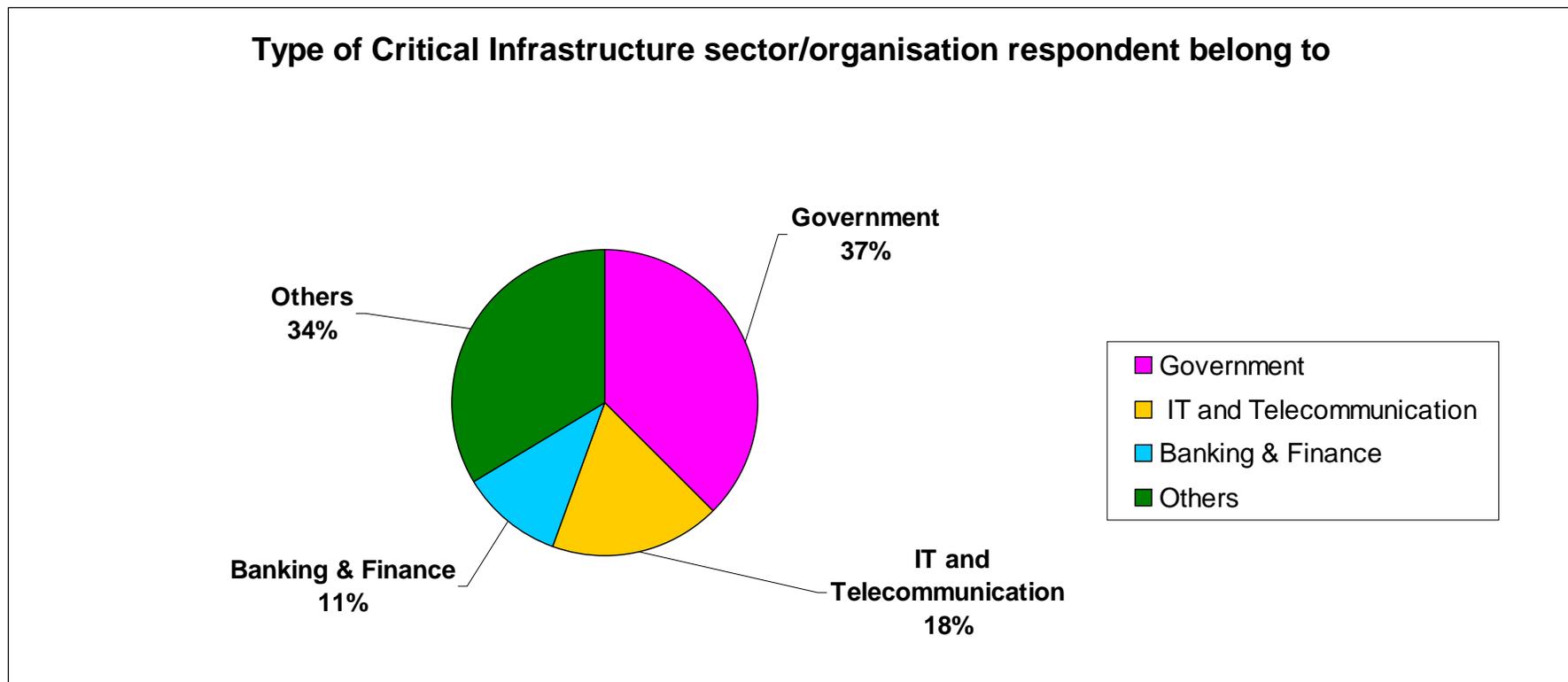
- Background of Cyber Security Issues
- Introduction to the National Cyber Security Policy
- Awareness level
- Knowledge Platform
- Cyber Exercise
- Way Forward



Survey 2007 among CNII Organisations - By Sector

The Conference was targeted at participants from GLCs and CNII organisation, the largest number of turnout is from government linked companies. *Aug 29, 2007*

Total of about 100 respondents



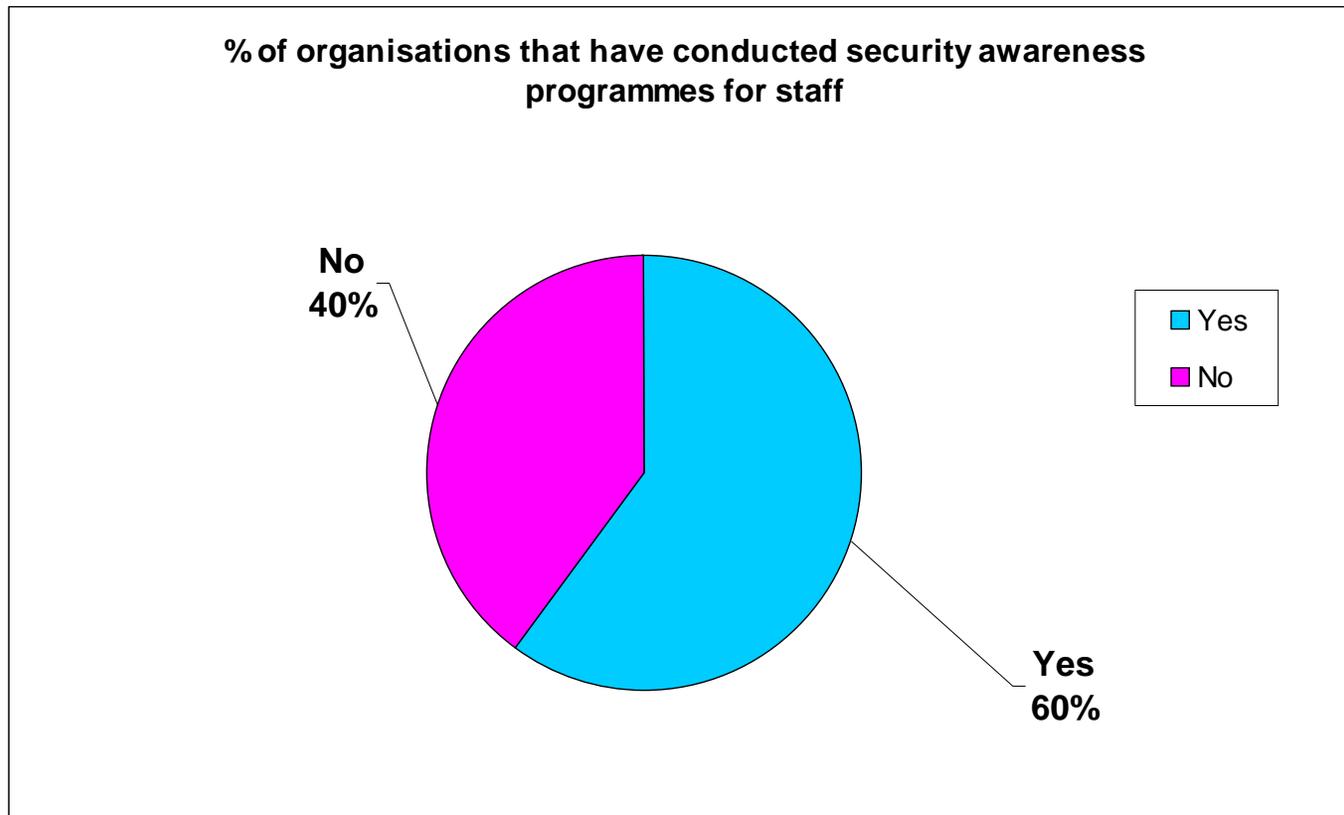
Note: CNII - Critical National Information Infrastructure



Survey 2007 among CNI Organisations - Cyber Security Awareness Initiatives

Does your organisation conduct cyber security awareness programme for all staff?

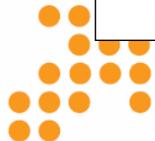
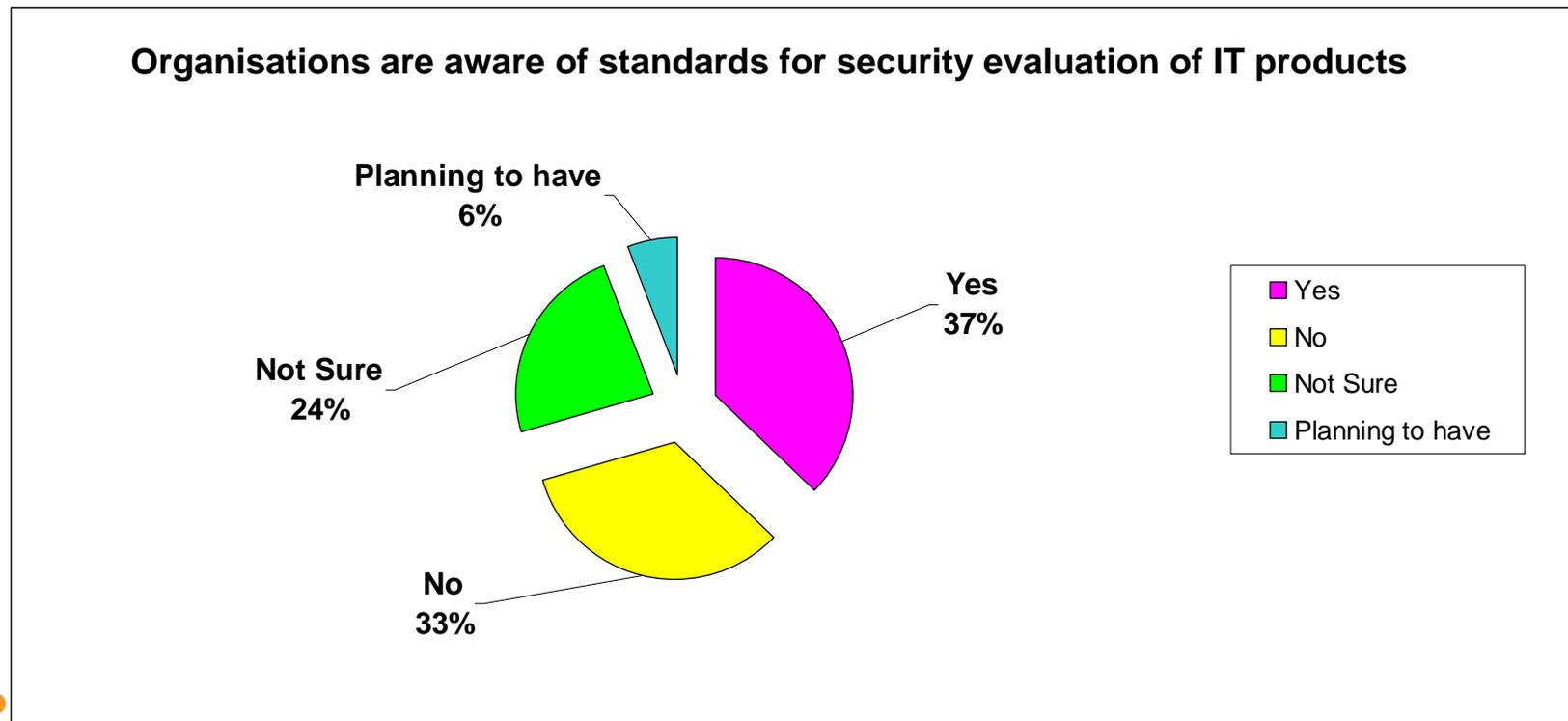
60% of respondents has conducted some form of cyber security awareness programme for staffs.



Survey 2007 among CNI Organisations - Guidelines for Evaluation of IT Products

Do you know that there is a standard guideline (ISO/IEC 15408 Common Criteria for IT Security Evaluation) that can be used to request, develop and evaluate secure IT products?

One third of the respondents are aware that there is such standard guideline to evaluate IT products.



Agenda

- Background of Cyber Security Issues
- Introduction to the National Cyber Security Policy
- Awareness level
- **Knowledge Sharing Platform**
- Cyber Exercise
- Way Forward





Outreach Program

CYBER SECURITY AND INTERNET SAFETY AWARENESS CAMPAIGN

Content Partners



International
CERT
Communities

Other
industry
partners

Content Localization & Packaging



MOSTI



Content Channels



Target Audience



Children / students



Parents/
home users



Organizations

Competency Development Programs

- Promote various platforms for engagement sessions
 - Seminars, forums & roundtable (e.g. **Infosec.my** conducted quarterly)
 - Demos and talks to specific critical sectors
 - Focus group mailing lists discussions
- Encourage hands-on participation
 - Hands-on Workshops
 - Cyber Exercises
 - Expert Lab
- Promote Information Security Professional Certifications



Portal for Critical National Information Infrastructure (CNII)

- **The CNII Portal is a security resource portal designed specifically to meet the needs of security practitioners (management & technical) within Critical National Information Infrastructure organisation.**
- **Platform to share guidelines and best practice among CNII, across sector**
- **Provide latest news on information security and security advisories**



Customized contents for Management & Technical security practitioners

CNII Portal
Critical National Information Infrastructure

| Home | About CNII Portal | FAQ | Contact Us

Information

Security Outlook For **Managers, CIO, CISO**

Technical Information For **System administrators, Developers**

Announcement

- 27 November 2007 [INFOSEC.my Technical Forum](#)
- 31 October 2007 [INFOSEC.my Knowledge Sharing](#)
- 23 October 2007 [Launch of MSC Malaysia CYBERCENTRE@MERU JAYA](#)

About CNII Portal

The CNII Portal is a portal in which the members of critical infrastructure work together by sharing information on security issues which affect critical infrastructure.

About Critical National Information Infrastructure

Critical National Information Infrastructure (CNII) is defined as those assets (real and virtual), systems and functions that are vital to the nations that their incapacity or destruction would have a devastating impact...

Highlight

INFOSEC.my Technical Forum

"In Conjunction with National Innovation Conference & Exhibition (NICE)"

Date And Time
2.00 PM - 5.30 PM, 27th November 2007

Venue
Hall 1, Dewan Tun Hussein Onn, Putra World Trade Centre (PWTC), 41, Jalan Tun Ismail, 50480 Kuala Lumpur.

Registration
<http://www.cybersecurity.org.my/infosec.my/>

Latest News

CERT Announcements

- New Podcast Released
- CERT NetSA Group Participates in Anti-Ph...
- New Podcast Released
- CERT Statistics Updated
- New Podcast Released

Help Net Security - News

- Off the wire: New QuickTime bug opens X...
- Off the wire: Security concerns cloud v...
- Off the wire: Did Microsoft's security ...
- Off the wire: Security chief asks Saudi...
- Off the wire: Useful security and priva...

Front page.

Home > Security Outlook

News

- [Cyber Incident Outside Malaysia Report](#)

Statistic Traffics

- [MyCERT statistics](#)
- [Current Top 10 Remote Hosts](#)

Security Reference

- [Information Guiding Principles](#)
- [Policies & Procedures](#)
- [Tips](#)

Security Outlook page for Managers, CIO, CISO.

Home > Security Outlook > Security Reference > Information Guiding Principles



ICT Sector



Banking & Financial Sector



Health Sector



Water Sector



National Defense & Security Sector



Transportation Sector

ICT Sector

- [Access Control](#)
- [UNIX Host Access Management With CA Access Controls](#)
- [A General & Flexible Access Control System For The Web](#)
- [Identity Based Control](#)
- [Access Control](#)
- [Account Management Policy](#)
- [Best Practices in Info Lifecycle Management Security](#)
- [Best Practices For Management Information Security](#)
- [Implementing Application Security Policies](#)
- [The Future Of secure application access management](#)
- [BC Guideline - A Practical Approach For Emergency Preparedness, Crisis Management And Disaster Recovery](#)
- [Developing A Business Continuity Plan](#)

Information Guiding Principles page.

Home > Technical Information

Security Advisories, Alert & Vulnerability Notes

- [Security Blogs](#)
- [Security Advisories](#)
- [Security Audit](#)
- [Vulnerabilities](#)
- [Malicious Codes](#)

Security Reference

- [Information Guiding Principles](#)
- [Policies & Procedures](#)
- [Tips](#)

Security Tools

- [Clock Synchronization](#)
- [File Integrity Checker](#)
- [Intruder Detection System](#)
- [Password Cracker & Utilities](#)
- [Patch Checkers](#)
- [Scanner](#)
- [Sniffer](#)
- [Other Tools](#)

Technical Information
page for System
Administrators,
Developer.

Home > Security Outlook > Security Reference > Tips

- [Malware Information](#)
- [Anti Virus Database](#)
- [Hoax Database](#)
- [Safe Email Practises](#)
- [Home User PC Security: Know the Threats and Countermeasures](#)
- [Time Synchronization Based on Operating Systems](#)

Tips page.



Agenda

- Background of Cyber Security Issues
- Introduction to the National Cyber Security Policy
- Awareness level
- Knowledge Sharing Platform
- **Cyber Exercise**
- Way Forward



Malaysian Incident Handling Drill @MyDrill 2007

- **Conducted on 22nd Nov 2007 by CyberSecurity Malaysia**
- **Participated by a total of 6 teams**
 - **3 ISPs**
 - **1 Antivirus Vendor**
 - **1 Domain Registrar**
 - **CyberSecurity Malaysia**

High level Objectives

- Prepare for potential cyber-security activity related to the Global event such as Beijing 2008 Olympic Games
- Provide different levels of exercise to suit the needs of the various local teams
- Provide an exercise that can be effectively coordinated by the volunteer exercise control group (EXCON)
- Meet the other high-level objectives within the short timeframe available for the drill.



Drill Scenario Background

Inject 1 – Domain Registrar received report that there's a C&C hosted outside Malaysia using a local domain mylovelybot.my. Request to take down domain

Domain Registrar scenario

Inject 2 - Received report of DDoS targeting udp/random port number attacking their DNS.

Inject 1 - Report from home user informing of slowness in accessing Beijing Olympic website.

Inject 2 - Website no longer accessible, further investigation shows > than 10,000 IP originating from Malaysia accessing the website, suspected botnet infected.

ISP scenario

Inject 3 - ISP received malware analysis report from AV vendor (malware infecting their user's PC – bot) containing several critical information i.e.C&C host domain (mylovelybot.my)



Inject 1 – Antivirus Vendor received report from MyCERT involving thousands of PCs from Malaysia infected by a new malware.

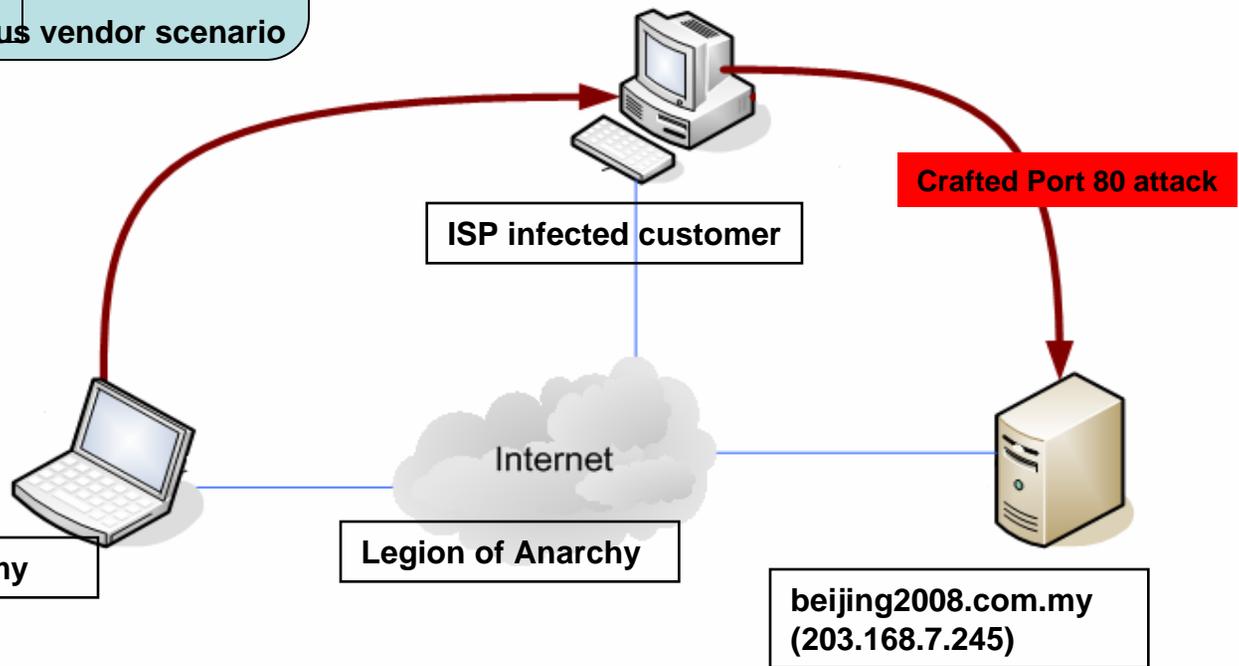


Anti-virus vendor scenario

Inject 1 – Input from MyCERT and to produce press release on attack



Public Relations scenario



Securi



Select language | 日本語 | 简体中文 | 繁體中文(香港) | 繁體中文(臺灣)

Main Index > Security Centre > Descriptions

F-Secure Malware Information Pages: Trojan-Downloader:W32/MyDrill.A

[Summary] | [Detailed Description]

Radar



Name: Trojan-Downloader:W32/MyDrill.A
Size: 130,708
Type: Trojan-Downloader
Category: Malware
Platform: Win32
Date of Discovery: November 22, 2007

Search

Security Guide
 F-Secure World Map
 Security Alerts
 Virus Statistics
 Malware Removal Tools
 Malware Code Glossary
 Submit Malware Sample

Select local site

Global Sites

VIRUS WORLD MAP

Global Alert Level:
 - Medium -

Latest Threat:
 Exploit:W32/AdobeRea

Summary

MyDrill.A is detection for files used as part of a Malaysian Cyber Security Drill that took place during 2007.

MyDrill.A are harmless test files. Detection was added for the purpose of the drill.

[Back to the Top](#)

Detailed Description

On execution this trojan will download a second trojan file from:

- [http://202.190\[REMOVED\]/gaga/2malware.html](http://202.190[REMOVED]/gaga/2malware.html)

It is saved as C:\malware.html and then later renamed and executed as C:\malware2.exe. The second trojan is also detected as Trojan-Downloader:W32/MyDrill.A.

Way Forward

- Innovate and generate materials relevant for the target audience
- Expand partnership with key stakeholders to reach out to target users.
- Device suitable platforms for information sharing among ICT & Information Security practitioners
- Assess effectiveness





-  **Postal Address** : CyberSecurity Malaysia (formerly known as NISER),
Level 7, SAPURA @ MINES,
7, Jalan Tasik, The Mines Resort City,
43300 Seri Kembangan,
Selangor Darul Ehsan,
Malaysia.
-  **Office Hours** : Monday - Friday 08:30 - 17:30 MYT
(Note: Not operational every Saturday and Sunday)
-  **Phone** : +603 - 8992 6888
-  **Fax** : +603 - 8945 3250
-  **Email** : *info [at] cybersecurity.org.my*
-  **Map** : Click here to download CyberSecurity Malaysia location map.



Awareness Portal – www.esecurity.org.my

| Home | Bahasa Malaysia |

eSecurity

TOWARDS BUILDING A SECURITY CULTURE

KIDS/ TEENAGERS

PARENTS/ ADULTS

ORGANISATIONS



About Us



Video



Download



Information Protection
When you are on the Internet
• Don't give out information about yourself to someone you meet online
• Don't send a picture of yourself to people you meet online
• Be alert to what the people you meet online say. If it worries you, ask your parents

Virus & Worms
When you are on the Internet
• Protect your computer current with the automatic updates
• Use an Internet firewall
• Subscribe to industry standard antivirus software and keep it current

Security Best Practices
BACKING UP DATA
• Establish backup schedule on daily, weekly and monthly basis to backup all documents whenever there is a modification to original content, backups should be created instantly
• Maintain backups for a period of time to allow for recovery process or fixing issue that is not revealed instantaneously
• Use automation features, as creating copies manually can be time consuming and tedious
• Run a set of tests on the backup process by periodically restoring the contents and verifying its accuracy

Information Security Management
SECURITY POLICY
When employees have access to the internet at work, there are serious risks involved. They can download viruses, create user logins, gain unauthorized access to critical information and potentially leak it. Good technical security and staff training can help. Good staff/security policies are also important because they make it very clear what is acceptable and what is not.
How to prepare and implement a policy
Sample Security Policies

Contact Us | Sitemap | Disclaimer

© 2007 CyberSecurity Malaysia. All Rights Reserved.

[Back](#)

Awareness Posters

(schools, public & organisations)

Back



IDENTITY THEFT

HOW TO PROTECT YOURSELF!

- Do not send personal information to unknown websites
- Do not respond to unknown emails
- If shopping online, know your sources
- Read website's privacy statement carefully
- Post your resumes only on promisee jobsites
- Always LOG OFF your computer when not in use!

Let's Make The Internet A Safer Place
CyberSecurity Malaysia
MOSTI



PHISHING SCAM

PHISHING SCAM is an act of getting someone into providing private information such as credit card numbers, bank account information, etc. through email, pop up messages and websites that appear to be legitimate.

HOW TO PROTECT YOURSELF!

- Don't reply to emails asking for personal or financial information
- Use an antivirus and firewall software
- Don't email personal or financial information
- Be careful of downloading any attachments or files from emails
- Don't follow links in emails

Let's Make The Internet A Safer Place
CyberSecurity Malaysia
MOSTI



CYBERSTALKING & HARASSMENT

The internet has become an invaluable part of our life. We use it for work, education and leisure. But we must be careful of what we do online to avoid being stalked or harassed on the internet.

Some tips to avoid being stalked or harassed on the internet:

- Don't respond to messages that asking for your information
- Choose a generation (male/female) screen name when chatting
- Don't share your personal banking or messages, unless you're prepared to face the fallout
- Don't click on suspicious messages and report them to the Malaysian Computer Emergency Response Team (M-CERT) at cert@nic.gov.my or www.mocert.org.my
- Do a search on yourself by using a search engine to make sure no personal information is posted for others about you
- If you are stalked or harassed, consider reporting it to the police

Let's Make The Internet A Safer Place
CyberSecurity Malaysia
MOSTI



PROTECT YOUR PASSWORD

- Never reveal your password to anyone
- Never provide your password over phone or email
- Change your password regularly
- Create difficult to guess password
- Mix uppercase and lowercase letters, symbols and numbers (e.g. a!c@Pqst)
- It should be more than 8 characters long

Let's Make The Internet A Safer Place
CyberSecurity Malaysia
MOSTI



SHOP SAFELY ONLINE

- Shop with merchants that you know or trust
- Check that the shopping website is secured
- Be wary of unsolicited phone calls or emails from a merchant
- Read merchant's refund and exchange policy before making purchase
- Do not share your password
- Always print and keep the order confirmation document
- Read the privacy statement
- Use an anti-virus, anti-spyware and personal firewall and keep it updated
- Never enter your personal information in a pop-up screen

Let's Make The Internet A Safer Place
CyberSecurity Malaysia
MOSTI



BEWARE OF SPYWARE

SPYWARE refers to software that performs certain tasks on your computer without your consent. This may include giving you advertisements or collecting personal information about you. (Pop-ups, slow system, system crashes, changes in your system, slow loader or your browser, unwanted software)

HOW TO PREVENT FROM SPYWARE!

- Use a firewall
- Adjust your security setting on your browser for the Internet zone to "Medium"
- Install and update your anti-spyware software
- Download software from website that you trust only

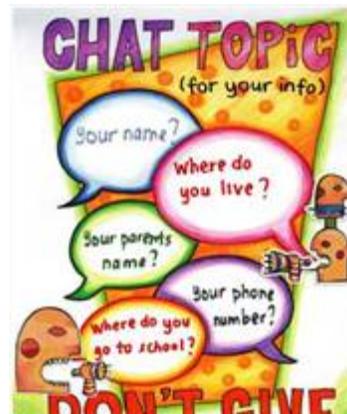
Let's Make The Internet A Safer Place
CyberSecurity Malaysia
MOSTI



SAFETY ON INTERNET CHAT

- Use nicknames as ID instead of real names, e.g. TopKoolie instead of Abdul Hamid
- Never provide personal information that is sensitive
- Do not meet a stranger that you met on internet chat
- Only open or download files from people you know
- When using a public computer key in your ID and password manually

Let's Make The Internet A Safer Place
CyberSecurity Malaysia
MOSTI



CHAT TOPIC (for your info)

Your name?
Where do you live?
Your parents name?
Your phone number?
Where do you go to school?

DON'T GIVE

Let's Make The Internet A Safer Place
CyberSecurity Malaysia
MOSTI



YOUR COMPUTER SECURITY CHECKLIST

- Install and use a personal firewall
- Update your software
- Use an updated anti-virus software
- Use an updated anti-spyware software
- Scan all email attachments
- Scan all your external drives (thumb drives, memory cards, hard disk)
- Back up your files on your computer
- Create and use a strong password and change them regularly

Let's Make The Internet A Safer Place
CyberSecurity Malaysia
MOSTI



SAFE ONLINE BANKING

- Keep your password/PIN code safe and memorize them
- Check that the Online Banking website is secured
- Log out immediately after you have completed your online transaction
- Use an anti-virus, anti-spyware and personal firewall and keep it updated
- Do not copy or click on any links attached in emails
- Do not respond to emails asking for personal information
- Read privacy and policy information before conducting any transactions
- Check your account statements to ensure that no unauthorized transaction has taken place
- When visiting your online banking site, always check that the Date and Time, matches the date and time when you last signed in

Let's Make The Internet A Safer Place
CyberSecurity Malaysia
MOSTI

Awareness Videos

Email & Spam



Safe Chatting



Safe Internet Banking

Cyber Stalking

Back

