ThaiCERT Incident Response
&
Phishing cases in Thailand

By

Kitisak Jirawannakool

Thai Computer Emergency Response team

(ThaiCERT)

Agenda

❑ About ThaiCERT

❑ ThaiCERT IR

❑ Phishing in Thailand

About ThaiCERT

- Ministry of Science and Technology
  - National Science and Development Agency (NSTDA)
    - National Electronics and Computer Technology Center (NECTEC)
      - Thai Computer Emergency Response Team (ThaiCERT)
- Thailand National CERT
- Full member of FIRST, APCERT

Objectives of ThaiCERT

- To handle the computer crime and coordinate with the related organization.

- To gain the knowledge and skill in the information security which is the factor effect to the stability of Thailand.

- To establish the team, which can handle the incidence of computer security and develop team personnel’s skill.

Current ThaiCERT

Dr. Komain

Dr. Siwaruk

Dr. Banchong

Dr. Kitti

Dr. Kamol

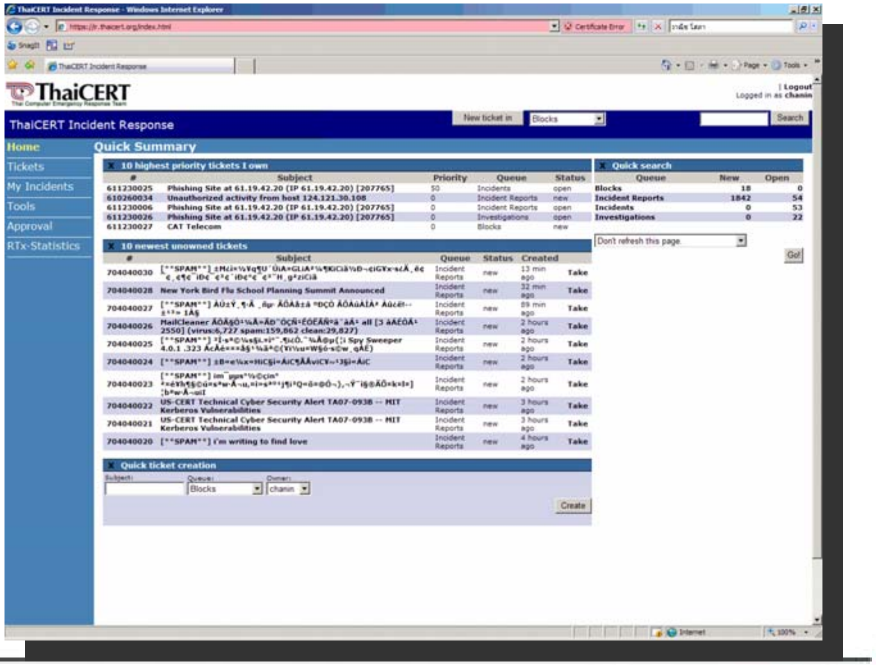
- 5 Ph.D.
- 30 Staffs

Current ThaiCERT

- ThaiCERT Services
- ThaiCERT R&D (3 research area)
  - Wireless Broadband Security Research and Development
  - Information Security Standard Research and Development
  - National Security Technology Research and Development

ThaiCERT Services

- Public Services
  - User security awareness raising
    - i.e. publication of security knowledge on the web, and Safety-Net Booklet
    - E-learning on computer security
  - Incident Response
    - Virus Alert
    - Security Advisory
  - Incident Coordinator



ThaiCERT Incident Response - Windows Internet Explorer
https://ir.thaicert.org/index.html
Certificate Error
ThaiCERT Incident Response
Page
Tools
ThaiCERT
Thai Computer Emergency Response Team
| Logout
Logged in as chanin
New ticket in
Blocks
Search
Home
Tickets
My Incidents
Tools
Approval
RTx-Statistics
Internet
100%

ThaiCERT Incident Response

Quick Summary

10 highest priority tickets I own

#	Subject	Priority	Queue	Status
611230025	Phishing Site at 61.19.42.20 (IP 61.19.42.20) [207765]	50	Incidents	open
610260034	Unauthorized activity from host 124.121.30.108	0	Incident Reports	new
611230006	Phishing Site at 61.19.42.20 (IP 61.19.42.20) [207765]	0	Incident Reports	open
611230026	Phishing Site at 61.19.42.20 (IP 61.19.42.20) [207765]	0	Investigations	open
611230027	CAT Telecom	0	Blocks	new

Quick search

Queue	New	Open
Blocks	18	0
Incident Reports	1842	54
Incidents	0	53
Investigations	0	22

Don't refresh this page. Go!

10 newest unowned tickets

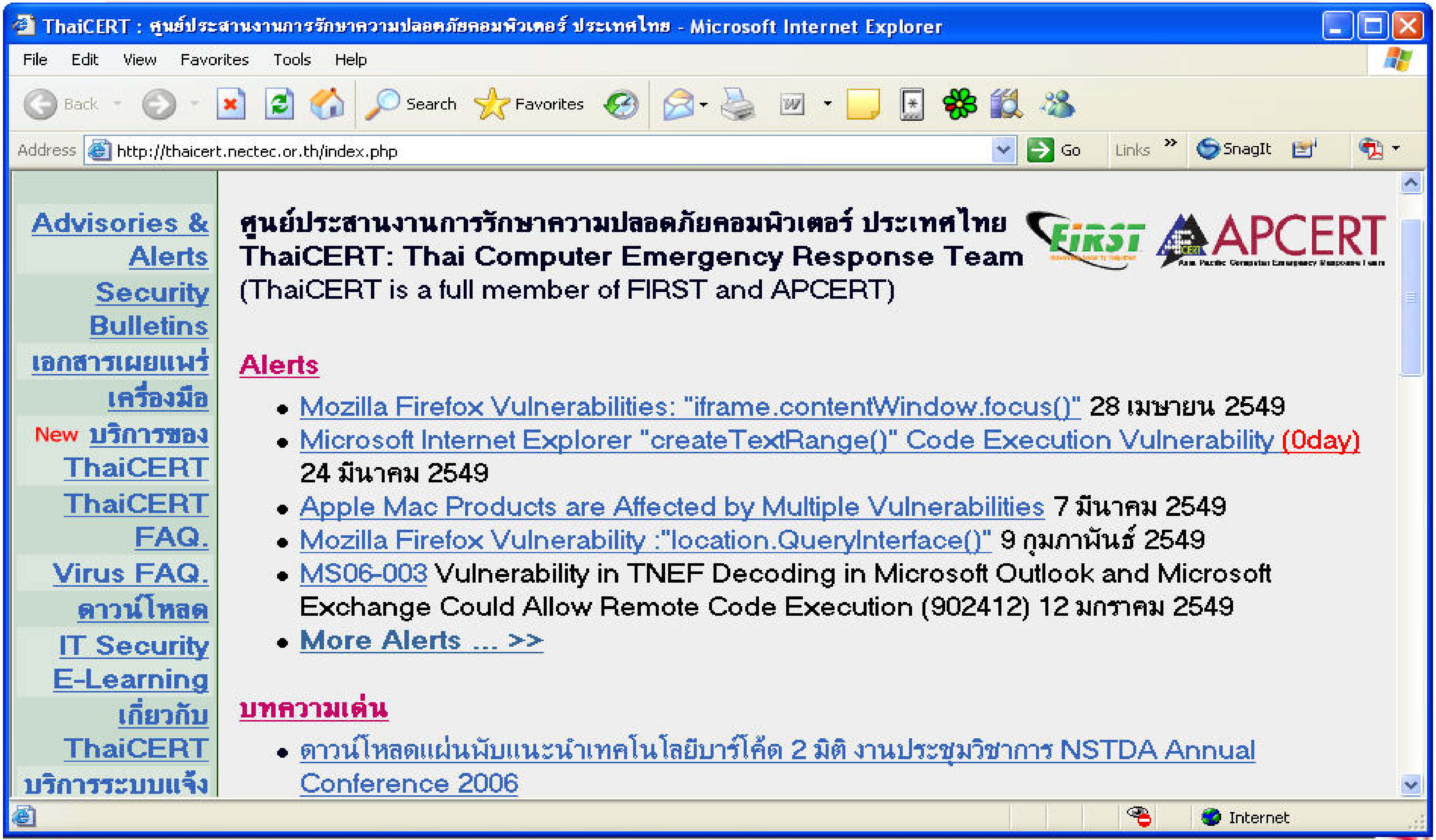
#	Subject	Queue	Status	Created	
704040030	[**SPAM**] [illegible]	Incident Reports	new	13 min ago	Take
704040028	New York Bird Flu School Planning Summit Announced	Incident Reports	new	32 min ago	Take
704040027	[**SPAM**] [illegible]	Incident Reports	new	89 min ago	Take
704040026	MailCleaner [illegible] all [3 [illegible] 2550] (virus:6,727 spam:159,862 clean:29,827)	Incident Reports	new	2 hours ago	Take
704040025	[**SPAM**] [illegible] Spy Sweeper 4.0.1 .323 [illegible]	Incident Reports	new	2 hours ago	Take
704040024	[**SPAM**] [illegible]	Incident Reports	new	2 hours ago	Take
704040023	[**SPAM**] [illegible]	Incident Reports	new	2 hours ago	Take
704040022	US-CERT Technical Cyber Security Alert TA07-093B -- MIT Kerberos Vulnerabilities	Incident Reports	new	3 hours ago	Take
704040021	US-CERT Technical Cyber Security Alert TA07-093B -- MIT Kerberos Vulnerabilities	Incident Reports	new	3 hours ago	Take
704040020	[**SPAM**] i'm writing to find love	Incident Reports	new	4 hours ago	Take

Quick ticket creation

Subject: Queue: Blocks Owner: chanin

Create

ThaiCERT Website



ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ ประเทศไทย
ThaiCERT: Thai Computer Emergency Response Team
(ThaiCERT is a full member of FIRST and APCERT)

Alerts

- Mozilla Firefox Vulnerabilities: "iframe.contentWindow.focus()" 28 เมษายน 2549
- Microsoft Internet Explorer "createTextRange()" Code Execution Vulnerability (0day) 24 มีนาคม 2549
- Apple Mac Products are Affected by Multiple Vulnerabilities 7 มีนาคม 2549
- Mozilla Firefox Vulnerability :"location.QueryInterface()" 9 กุมภาพันธ์ 2549
- MS06-003 Vulnerability in TNEF Decoding in Microsoft Outlook and Microsoft Exchange Could Allow Remote Code Execution (902412) 12 มกราคม 2549
- **More Alerts ... >>**

บทความเด่น

- ดาวน์โหลดแผ่นพับแนะนำเทคโนโลยีบาร์โค้ด 2 มิติ งานประชุมวิชาการ NSTDA Annual Conference 2006

ThaiCERT
Thai Computer Emergency Response Team

NECTEC
a member of NSTDA

Publication

Electronic • Computing • Telecommunication • Information • Instruments NECTEC

มาตรฐานการรักษาความมั่นคงปลอดภัย
ในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชัน 1)
ประจำปี 2547

จัดพิมพ์เพื่อเผยแพร่โดย
คณะอนุกรรมการด้านความมั่นคง
ภายใต้ คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

Electronic Transaction Security Standard (version 1) (based on BS 7799 / ISO 17799:2000 Standard)

NECTEC
a member of NSTDA

มาตรฐานการรักษาความมั่นคงปลอดภัย
ในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชัน 2)
ประจำปี 2549

จัดพิมพ์เพื่อเผยแพร่โดย
คณะอนุกรรมการด้านความมั่นคง
ใน คณะอนุกรรมการธุรกรรมทางอิเล็กทรอนิกส์

Electronic Transaction Security Standard (version 2) (based on ISO 27001 / ISO 17799:2005 Standard

ThaiCERT Services

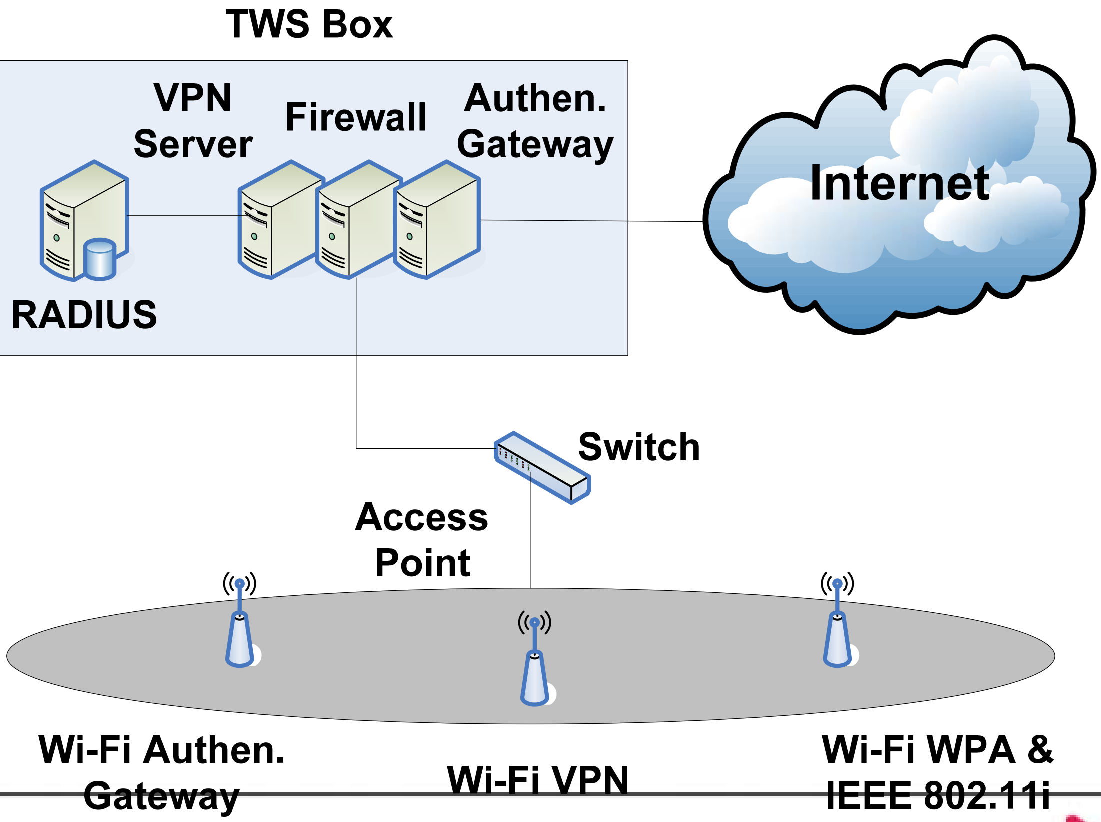
- Incident Response Services
  - E-mail
  - Telephone
- IT Security Audit Services
  - Penetration Test
  - Vulnerability Scanning
  - Information Security Assessment (ISA)
    - ISO/IEC27001 and ISO/IEC17799 std
  - IT Security Plan Development Service

ThaiCERT Services

- Security Training
  - i.e. OS Hardening, Wireless Security, Security Standard Implementation
- Wireless Security Services
  - Design and Implementation Services
- Virus Protection Services
  - Virus Alert Service
  - Virus Buster Service
  - E-Mail Antivirus Gateway

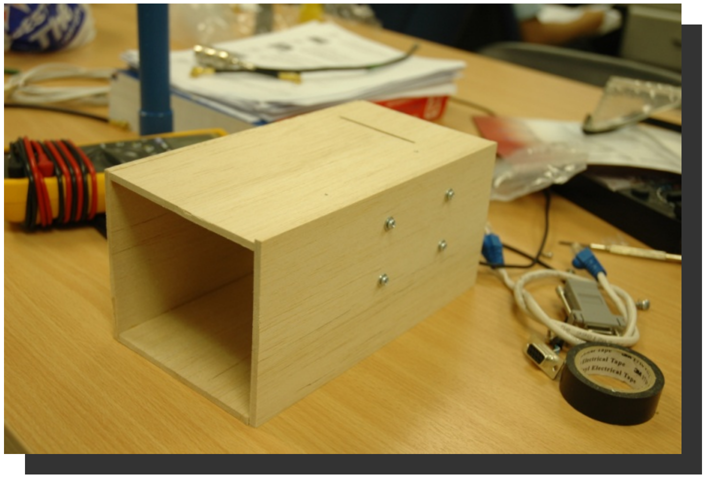
ThaiCERT R&D

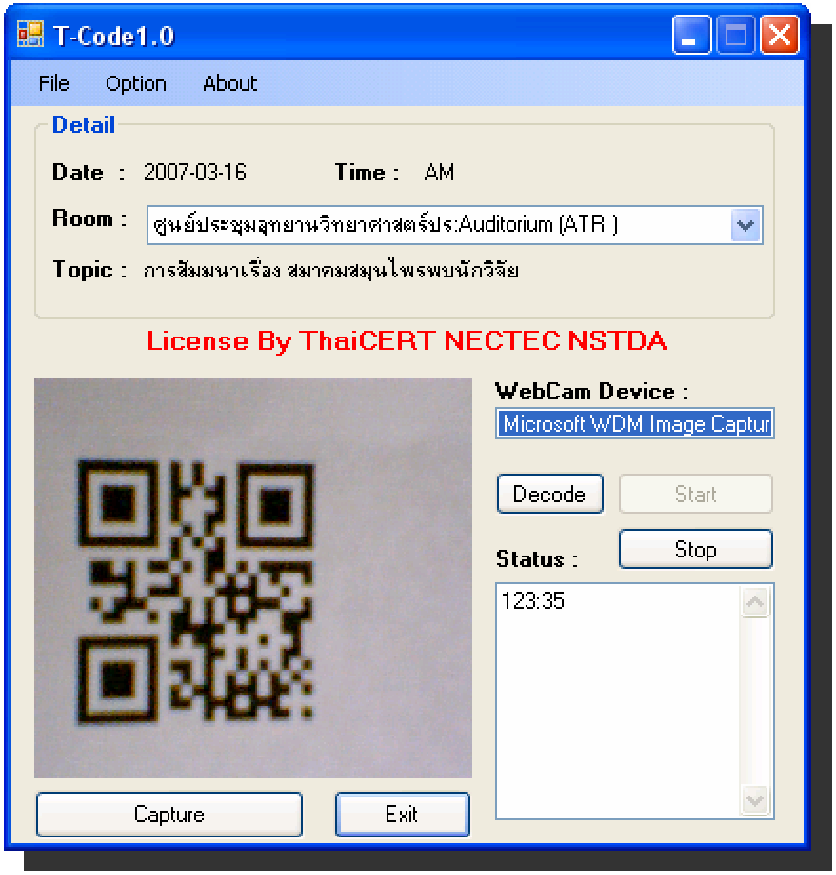
- IT Security Standard
- Wireless Security



ThaiCERT R&D

- 2-D Barcode Security
- Malware Analysis Lab
- Fingerprint Software
- Security Sensor





Detail

Date : 2007-03-16 **Time** : AM

Room : ศูนย์ประชุมอุทยานวิทยาศาสตร์ปร:Auditorium (ATR)

Topic : การสัมมนาเรื่อง สมาคมสมุนไพรพบนักวิจัย

License By ThaiCERT NECTEC NSTDA

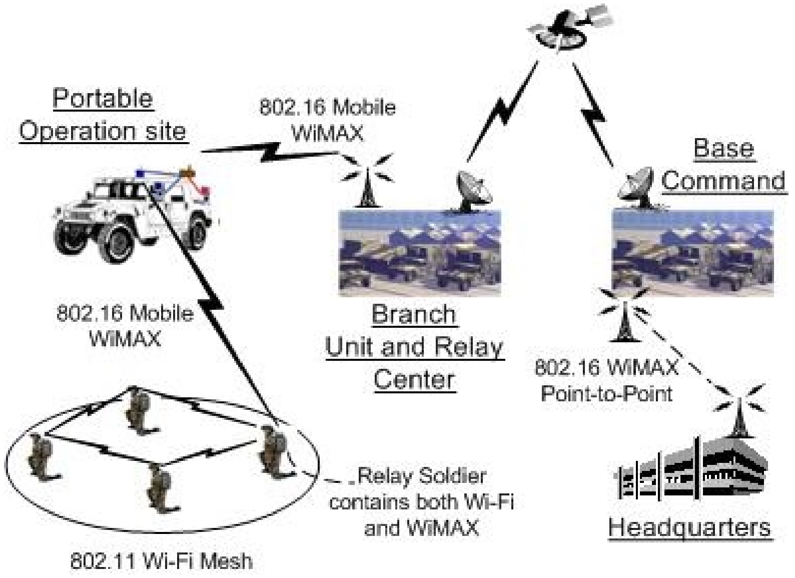
WebCam Device : Microsoft WDM Image Captur

Status :

123:35

ThaiCERT R&D

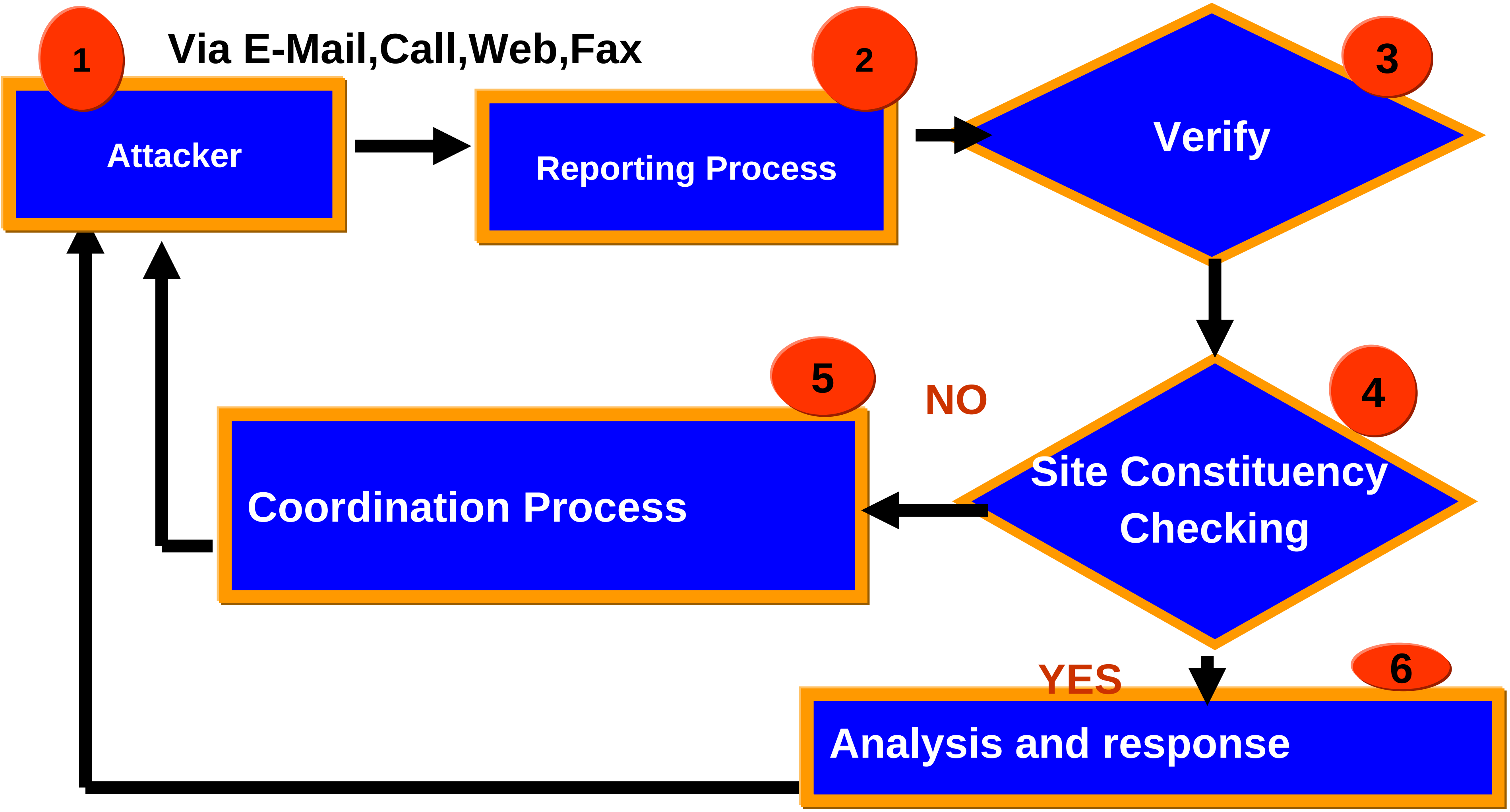
- Broadband Wireless for National Security



ThaiCERT IR

- ❑ General IR Process
- ❑ Constituency
- ❑ Statistics

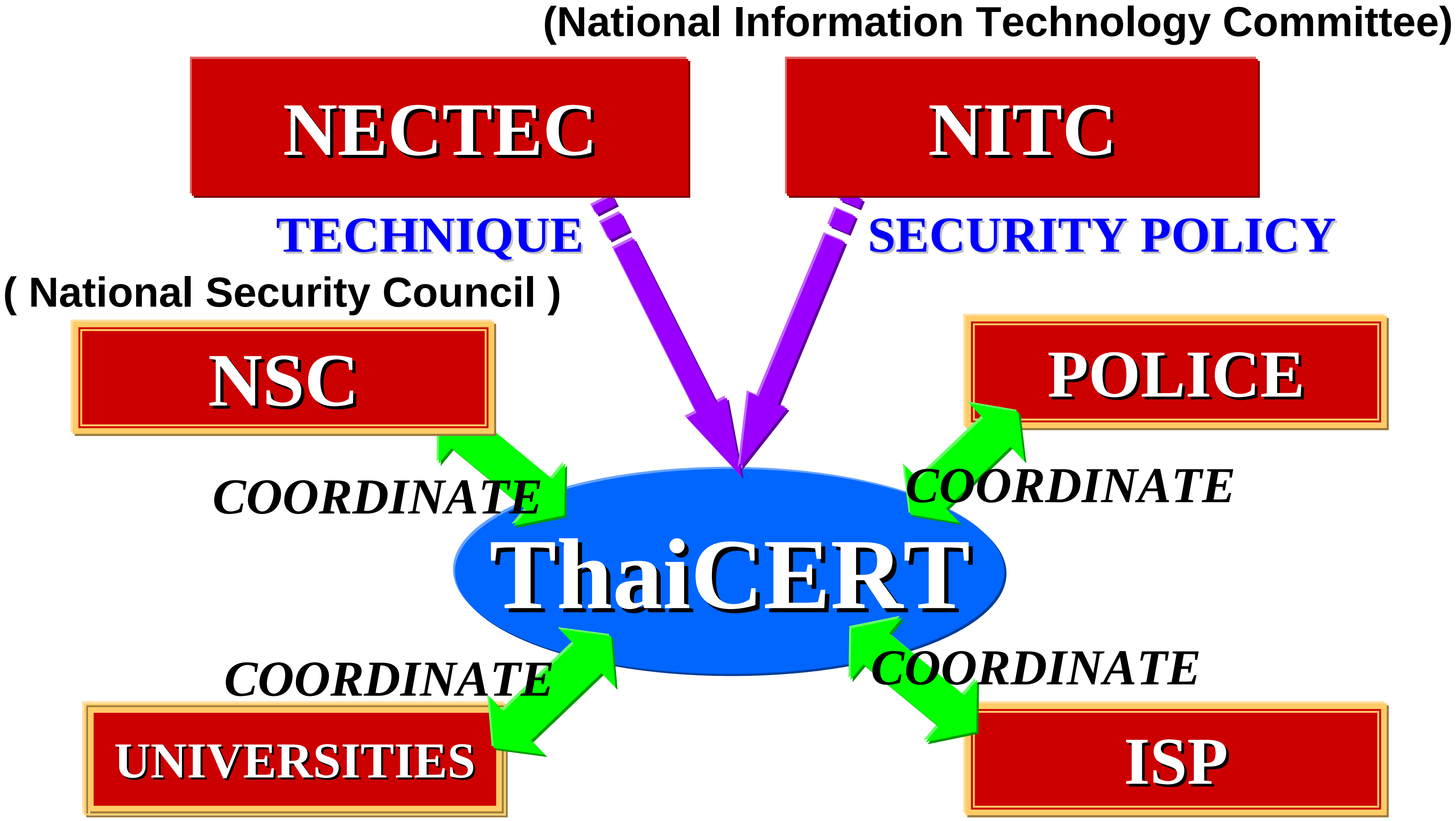
Incident Response Process



Constituency

- NSTDA and under
  - NECTEC
  - BIOTEC
  - MTEC
  - NANOTEC
- Government organizations
- some ISPs
- other organizations by request

Collaboration



(National Information Technology Committee)

NECTEC

NITC

TECHNIQUE

SECURITY POLICY

(National Security Council)

NSC

POLICE

COORDINATE

COORDINATE

ThaiCERT

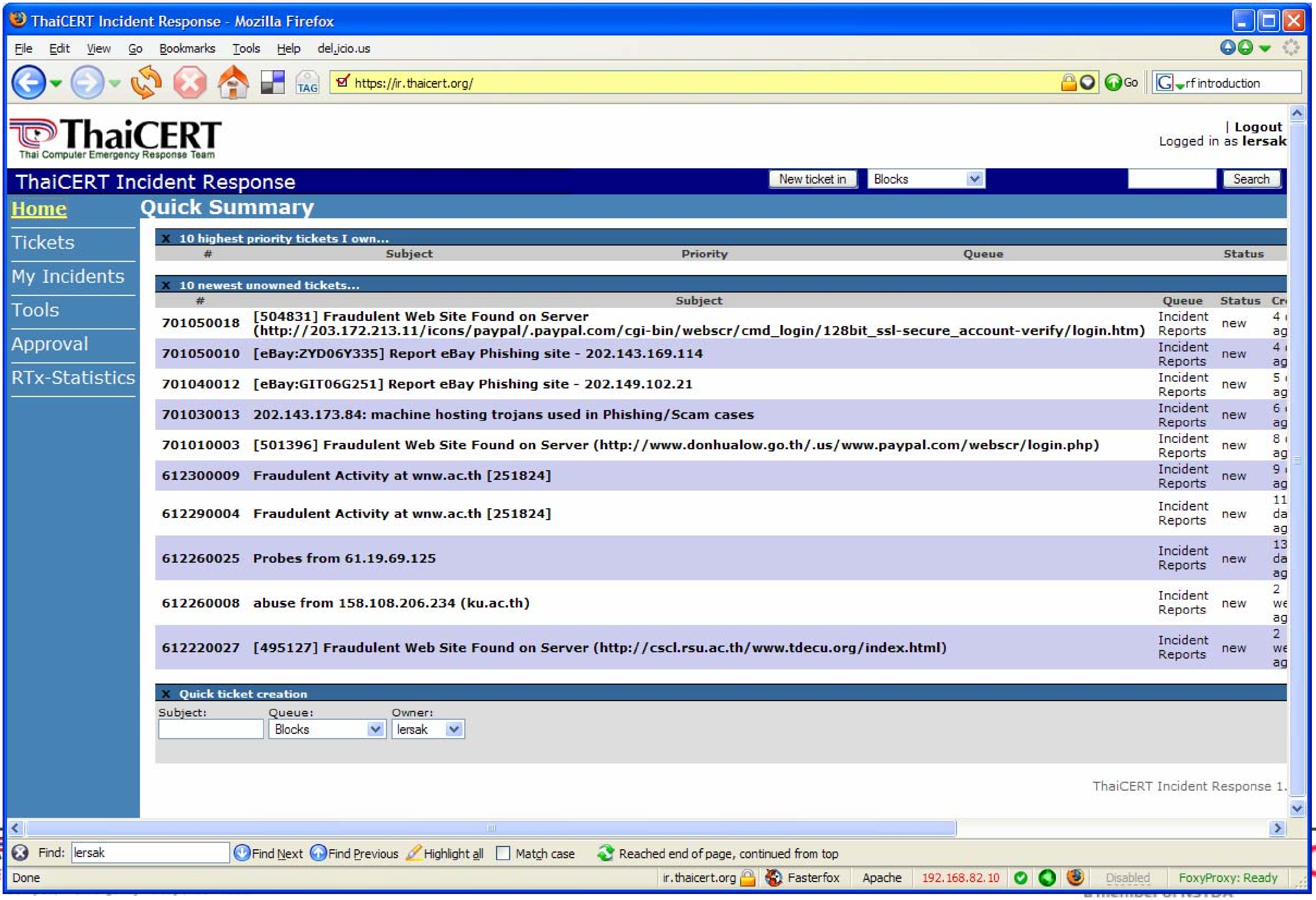
COORDINATE

COORDINATE

UNIVERSITIES

ISP

Incident Management System


ThaiCERT Incident Response - Mozilla Firefox
File Edit View Go Bookmarks Tools Help del.icio.us
https://ir.thaicert.org/
Go
rf introduction
ThaiCERT
Thai Computer Emergency Response Team

| Logout
Logged in as lersak

ThaiCERT Incident Response

New ticket in | Blocks | Search

Home
Tickets
My Incidents
Tools
Approval
RTx-Statistics

Quick Summary

X 10 highest priority tickets I own...

#	Subject	Priority	Queue	Status

X 10 newest unowned tickets...

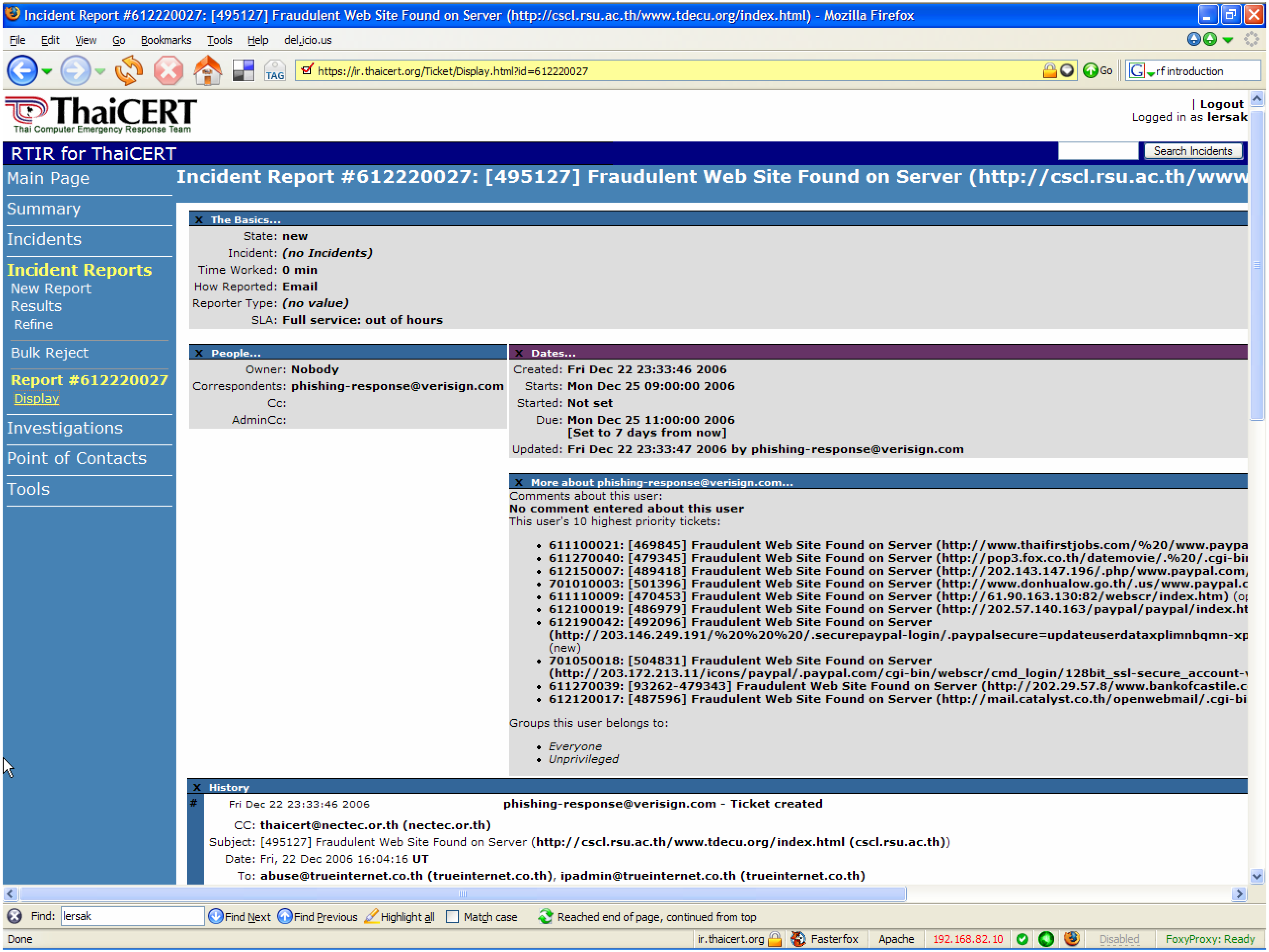
#	Subject	Queue	Status	Cr
701050018	[504831] Fraudulent Web Site Found on Server (http://203.172.213.11/icons/paypal/.paypal.com/cgi-bin/webscr/cmd_login/128bit_ssl-secure_account-verify/login.htm)	Incident Reports	new	4 ag
701050010	[eBay:ZYD06Y335] Report eBay Phishing site - 202.143.169.114	Incident Reports	new	4 ag
701040012	[eBay:GIT06G251] Report eBay Phishing site - 202.149.102.21	Incident Reports	new	5 ag
701030013	202.143.173.84: machine hosting trojans used in Phishing/Scam cases	Incident Reports	new	6 ag
701010003	[501396] Fraudulent Web Site Found on Server (http://www.donhualow.go.th/.us/www.paypal.com/webscr/login.php)	Incident Reports	new	8 ag
612300009	Fraudulent Activity at wnw.ac.th [251824]	Incident Reports	new	9 ag
612290004	Fraudulent Activity at wnw.ac.th [251824]	Incident Reports	new	11 da ag
612260025	Probes from 61.19.69.125	Incident Reports	new	13 da ag
612260008	abuse from 158.108.206.234 (ku.ac.th)	Incident Reports	new	2 we ag
612220027	[495127] Fraudulent Web Site Found on Server (http://cscl.rsu.ac.th/www.tdecu.org/index.html)	Incident Reports	new	2 we ag

X Quick ticket creation

Subject:	Queue:	Owner:
	Blocks	lersak

ThaiCERT Incident Response 1.

Reached end of page, continued from top



Incident Report #612220027: [495127] Fraudulent Web Site Found on Server (http://cscl.rsu.ac.th/www.tdecu.org/index.html) - Mozilla Firefox

https://ir.thaicert.org/Ticket/Display.html?id=612220027

| Logout
Logged in as **lersak**

RTIR for ThaiCERT

- Main Page
- Summary
- Incidents
- **Incident Reports**
  - New Report
  - Results
  - Refine
- Bulk Reject
- **Report #612220027**
  - Display
- Investigations
- Point of Contacts
- Tools

Incident Report #612220027: [495127] Fraudulent Web Site Found on Server (http://cscl.rsu.ac.th/www

X The Basics...

State:	**new**
Incident:	***(no Incidents)***
Time Worked:	**0 min**
How Reported:	**Email**
Reporter Type:	***(no value)***
SLA:	**Full service: out of hours**

X People...

Owner:	**Nobody**
Correspondents:	**phishing-response@verisign.com**
Cc:	
AdminCc:	

X Dates...

Created:	**Fri Dec 22 23:33:46 2006**
Starts:	**Mon Dec 25 09:00:00 2006**
Started:	**Not set**
Due:	**Mon Dec 25 11:00:00 2006** **[Set to 7 days from now]**
Updated:	**Fri Dec 22 23:33:47 2006 by phishing-response@verisign.com**

X More about phishing-response@verisign.com...

Comments about this user:
No comment entered about this user
This user's 10 highest priority tickets:

- **611100021: [469845] Fraudulent Web Site Found on Server (http://www.thaifirstjobs.com/%20/www.paypa**
- **611270040: [479345] Fraudulent Web Site Found on Server (http://pop3.fox.co.th/datemovie/.%20/.cgi-bi**
- **612150007: [489418] Fraudulent Web Site Found on Server (http://202.143.147.196/.php/www.paypal.com,**
- **701010003: [501396] Fraudulent Web Site Found on Server (http://www.donhualow.go.th/.us/www.paypal.c**
- **611110009: [470453] Fraudulent Web Site Found on Server (http://61.90.163.130:82/webscr/index.htm)** (o
- **612100019: [486979] Fraudulent Web Site Found on Server (http://202.57.140.163/paypal/paypal/index.ht**
- **612190042: [492096] Fraudulent Web Site Found on Server (http://203.146.249.191/%20%20%20/.securepaypal-login/.paypalsecure=updateuserdataxplimnbqmn-xp** (new)
- **701050018: [504831] Fraudulent Web Site Found on Server (http://203.172.213.11/icons/paypal/.paypal.com/cgi-bin/webscr/cmd_login/128bit_ssl-secure_account-**
- **611270039: [93262-479343] Fraudulent Web Site Found on Server (http://202.29.57.8/www.bankofcastile.c**
- **612120017: [487596] Fraudulent Web Site Found on Server (http://mail.catalyst.co.th/openwebmail/.cgi-bi**

Groups this user belongs to:

- *Everyone*
- *Unprivileged*

X History

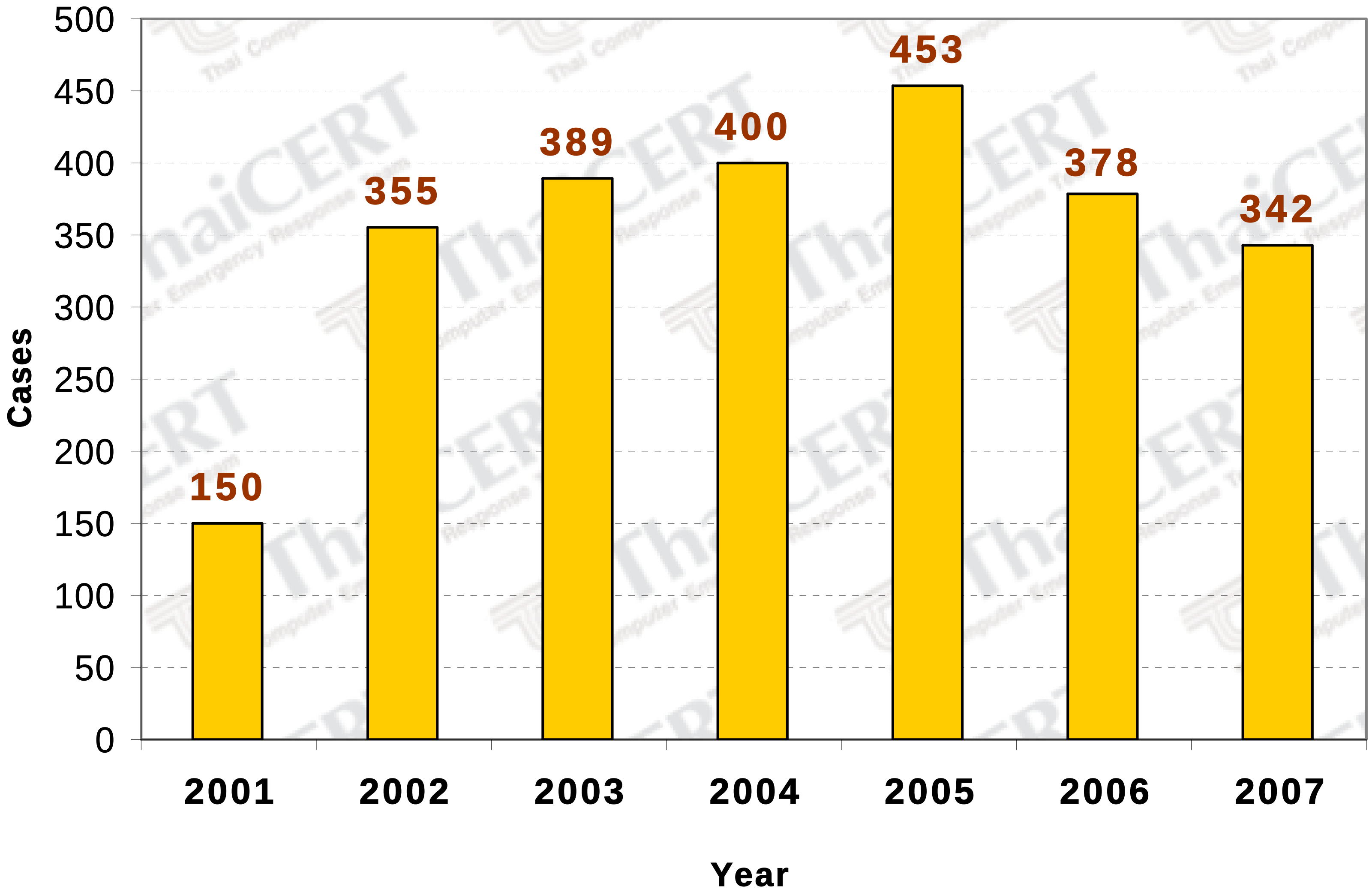
Fri Dec 22 23:33:46 2006 **phishing-response@verisign.com - Ticket created**

CC: **thaicert@nectec.or.th (nectec.or.th)**
Subject: [495127] Fraudulent Web Site Found on Server (**http://cscl.rsu.ac.th/www.tdecu.org/index.html (cscl.rsu.ac.th)**)
Date: Fri, 22 Dec 2006 16:04:16 **UT**
To: **abuse@trueinternet.co.th (trueinternet.co.th), ipadmin@trueinternet.co.th (trueinternet.co.th)**

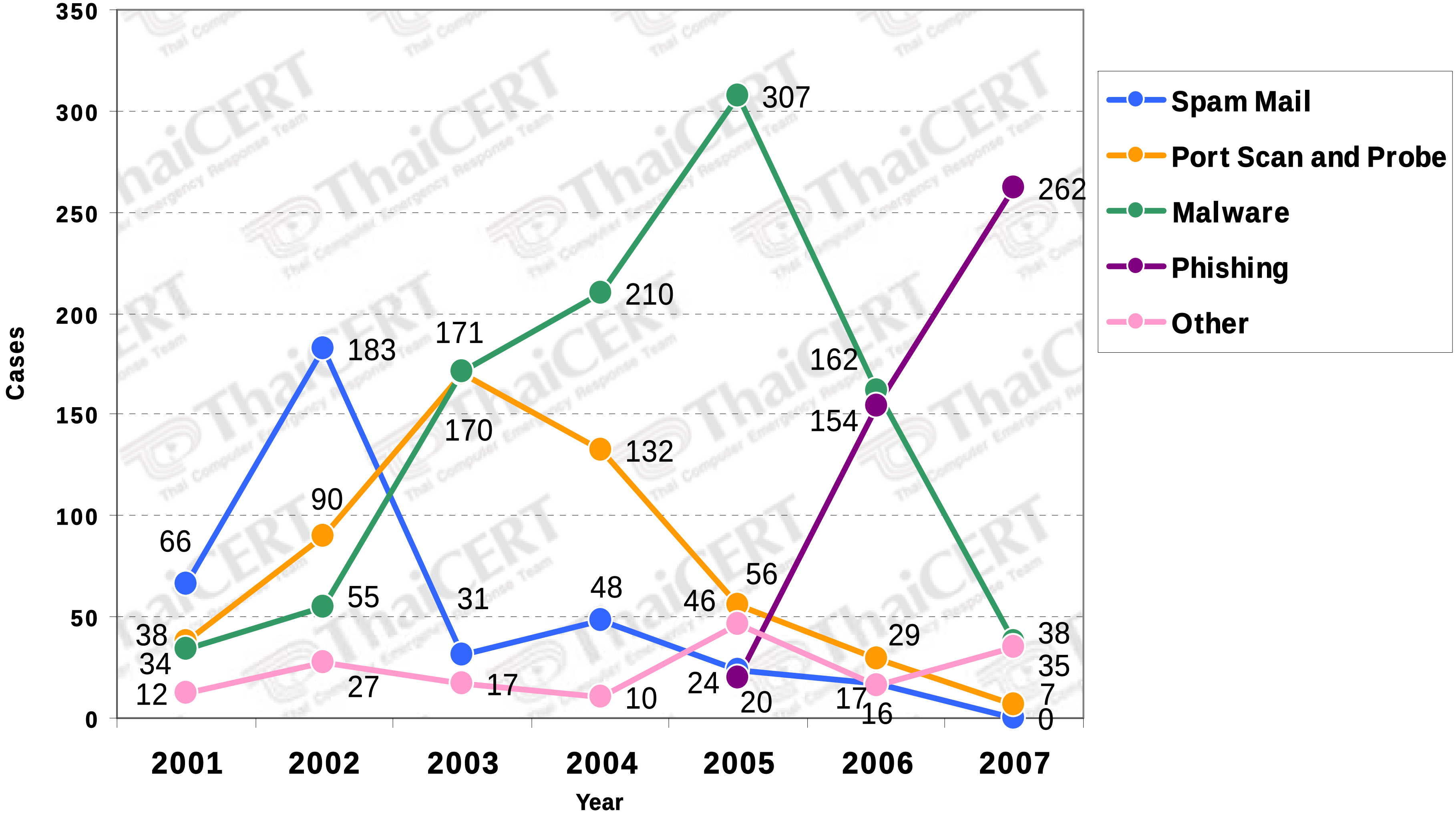
Find: lersak
Reached end of page, continued from top

Done
ir.thaicert.org
192.168.82.10

Statistics - Overall



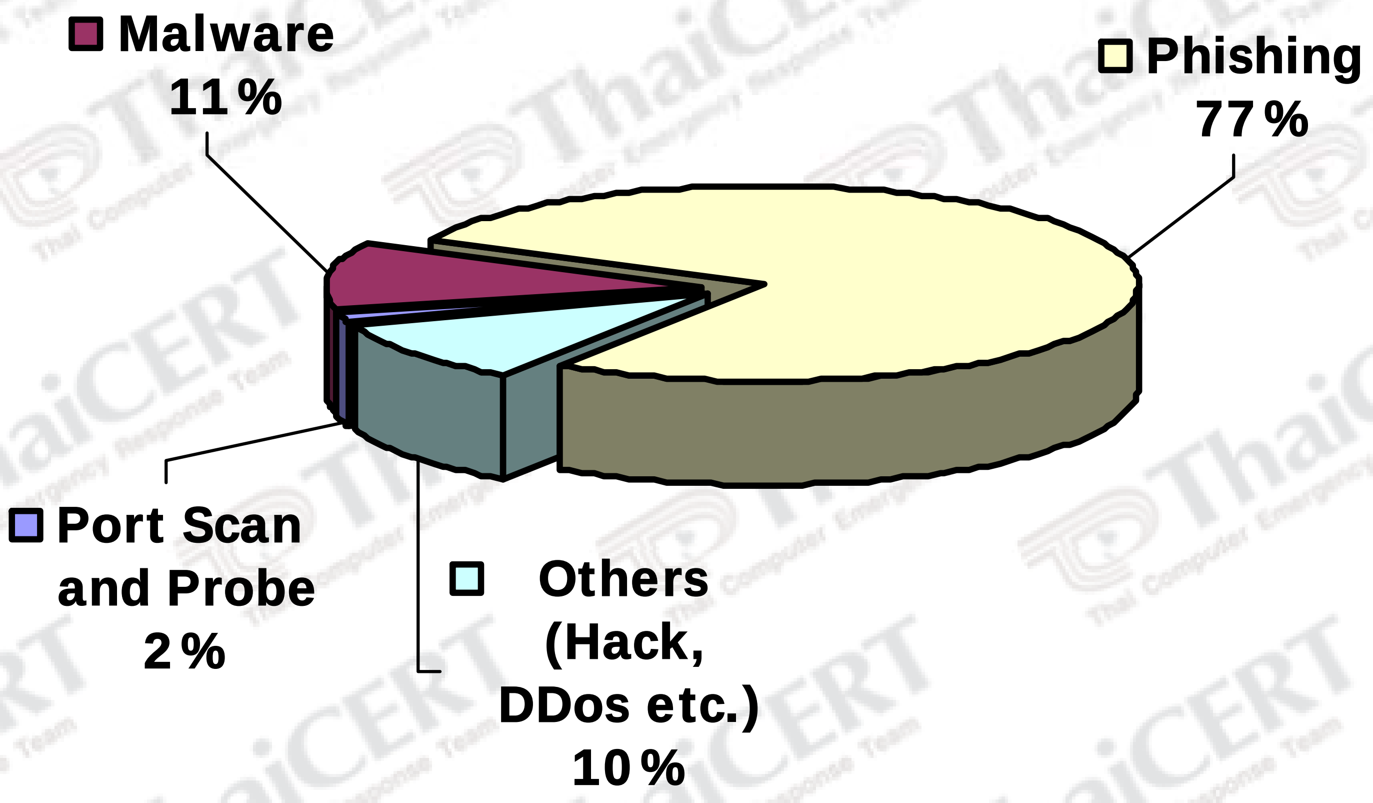
Types of Incident



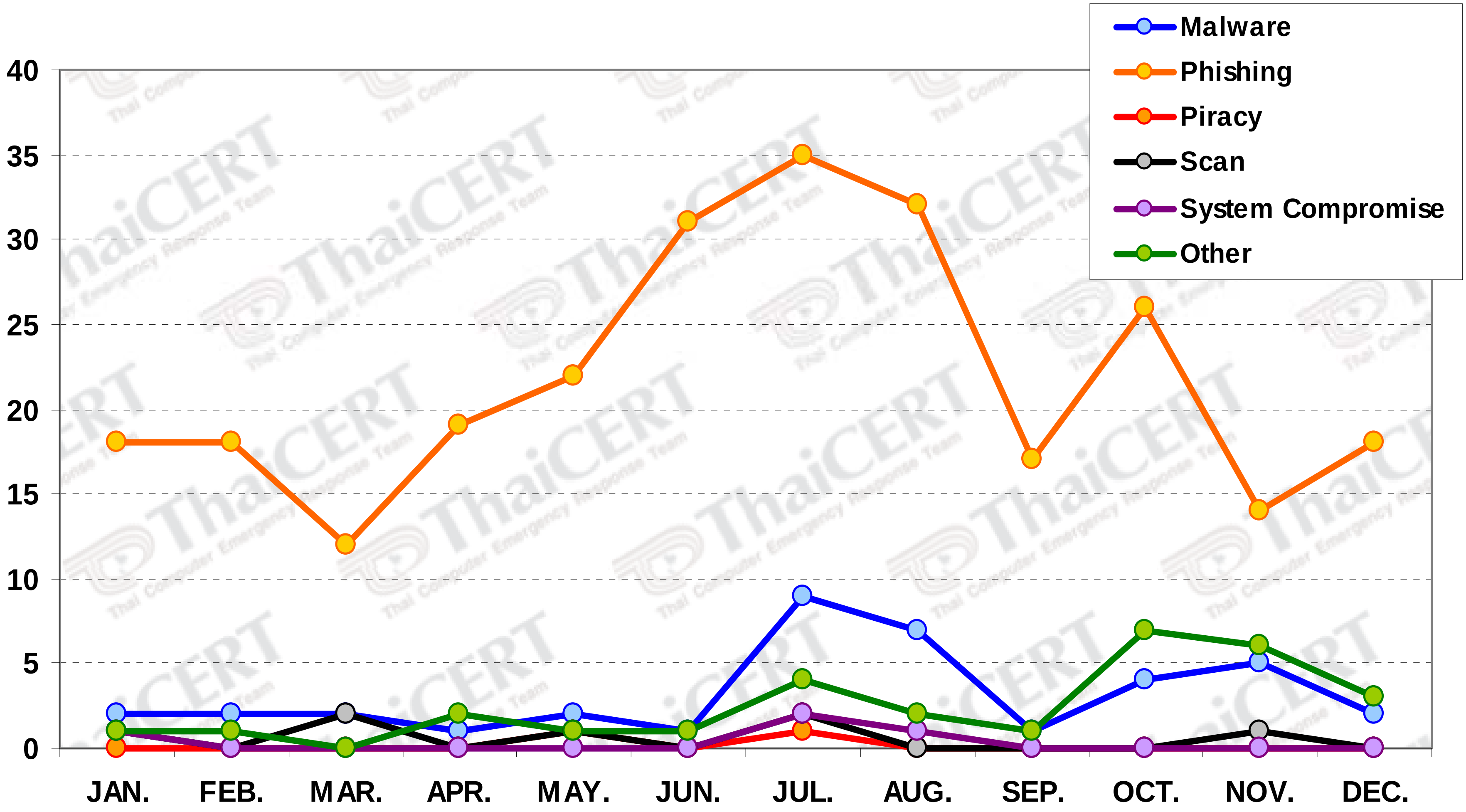
ThaiCERT
Thai Computer Emergency Response Team

NECTEC
a member of NSTDA

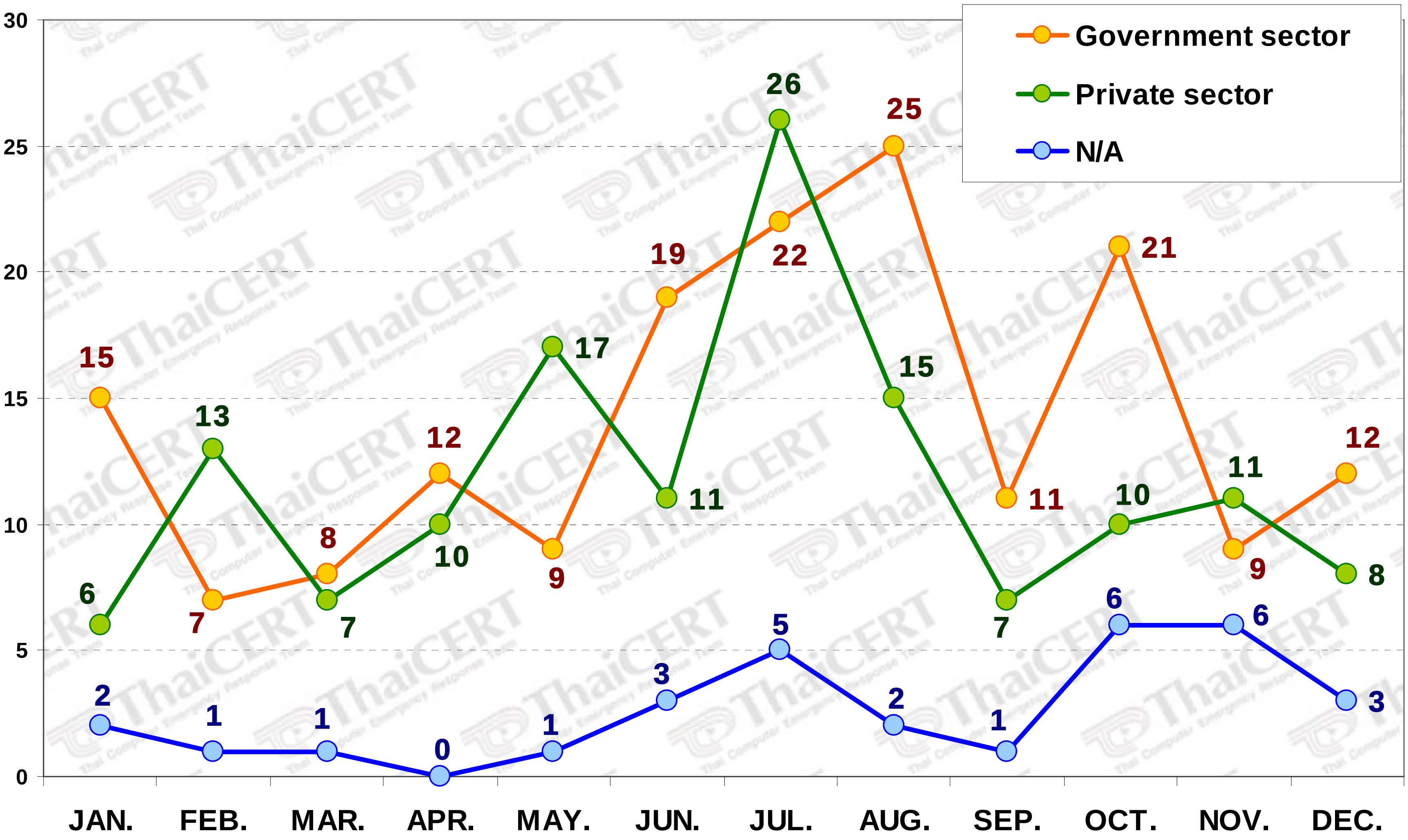
Types of Incident 2007



Monthly - 2007



Organization type

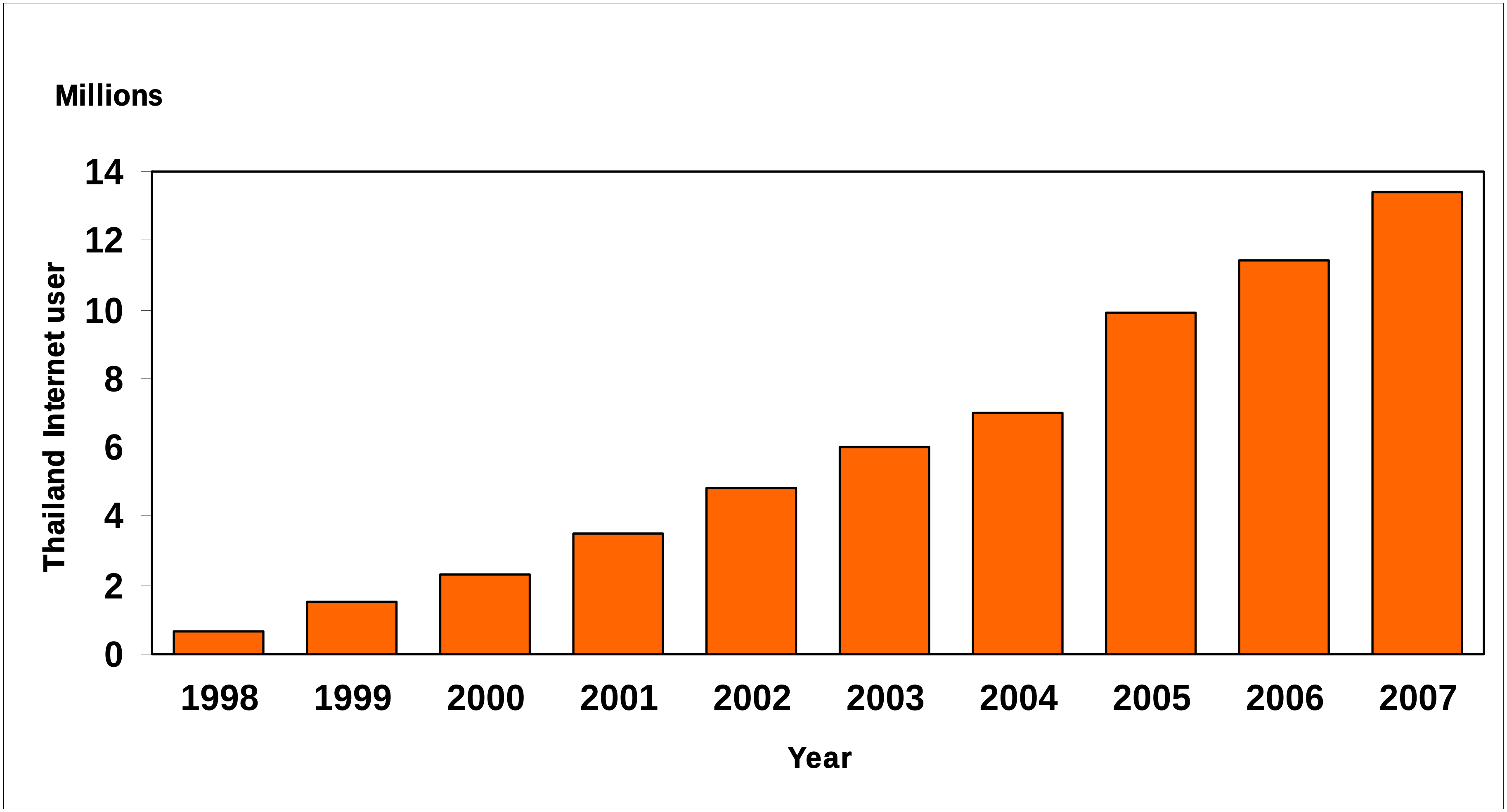


	JAN.	FEB.	MAR.	APR.	MAY.	JUN.	JUL.	AUG.	SEP.	OCT.	NOV.	DEC.
Government sector	15	7	8	12	9	19	22	25	11	21	9	12
Private sector	6	13	7	10	17	11	26	15	7	10	11	8
N/A	2	1	1	0	1	3	5	2	1	6	6	3

Phishing Cases in Thailand

- ❑ Overview
- ❑ Types of Phishing Incidents
- ❑ Discussion

Internet Usage in Thailand

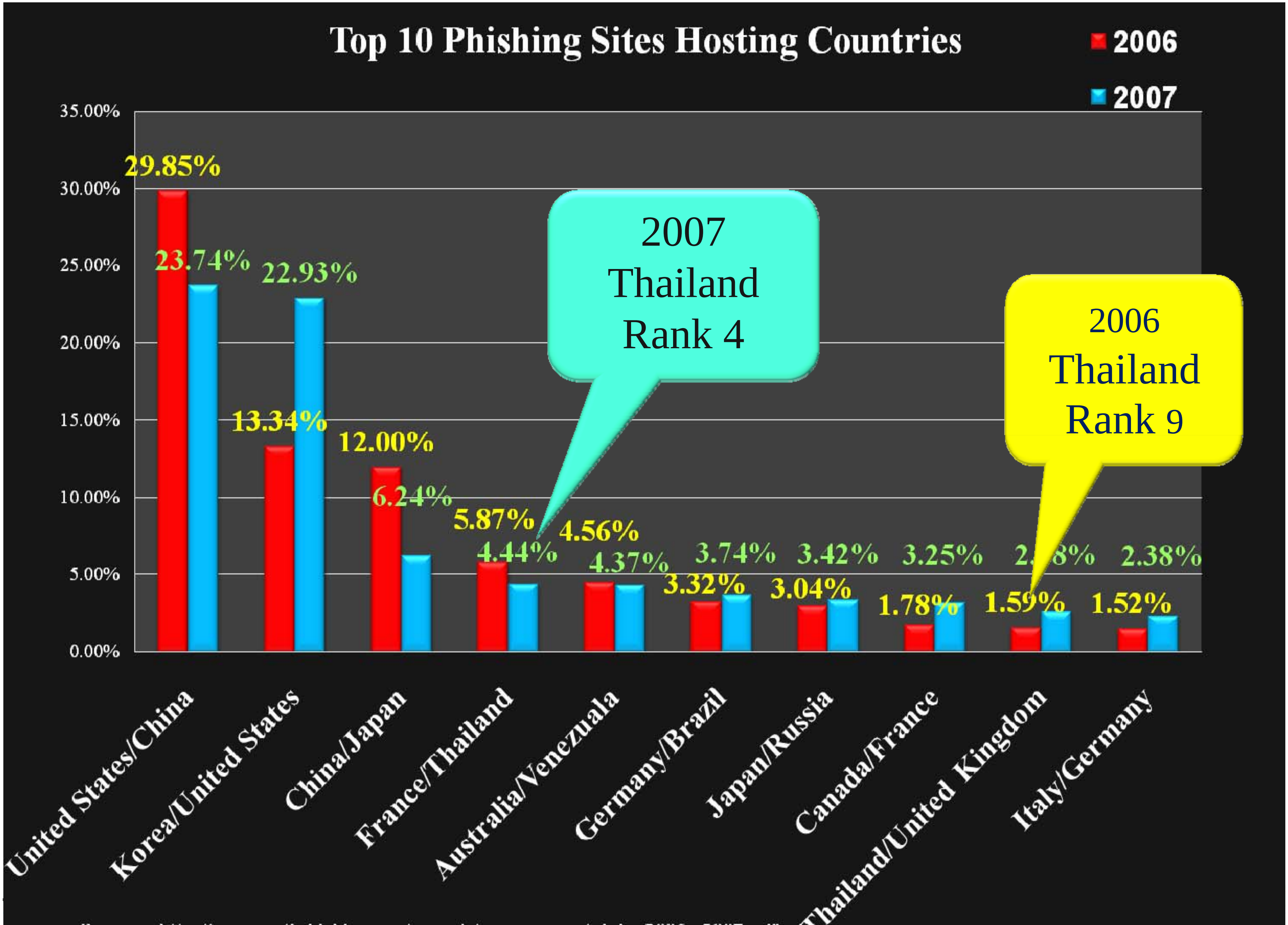


Source : http://internet.nectec.or.th/webstats/internetuser.iir?Sec=internetuser

ThaiCERT
Thai Computer Emergency Response Team

NECTEC
a member of NSTDA

Top 10 Phishing Sites Hosting Countries



2007
Thailand
Rank 4

2006
Thailand
Rank 9

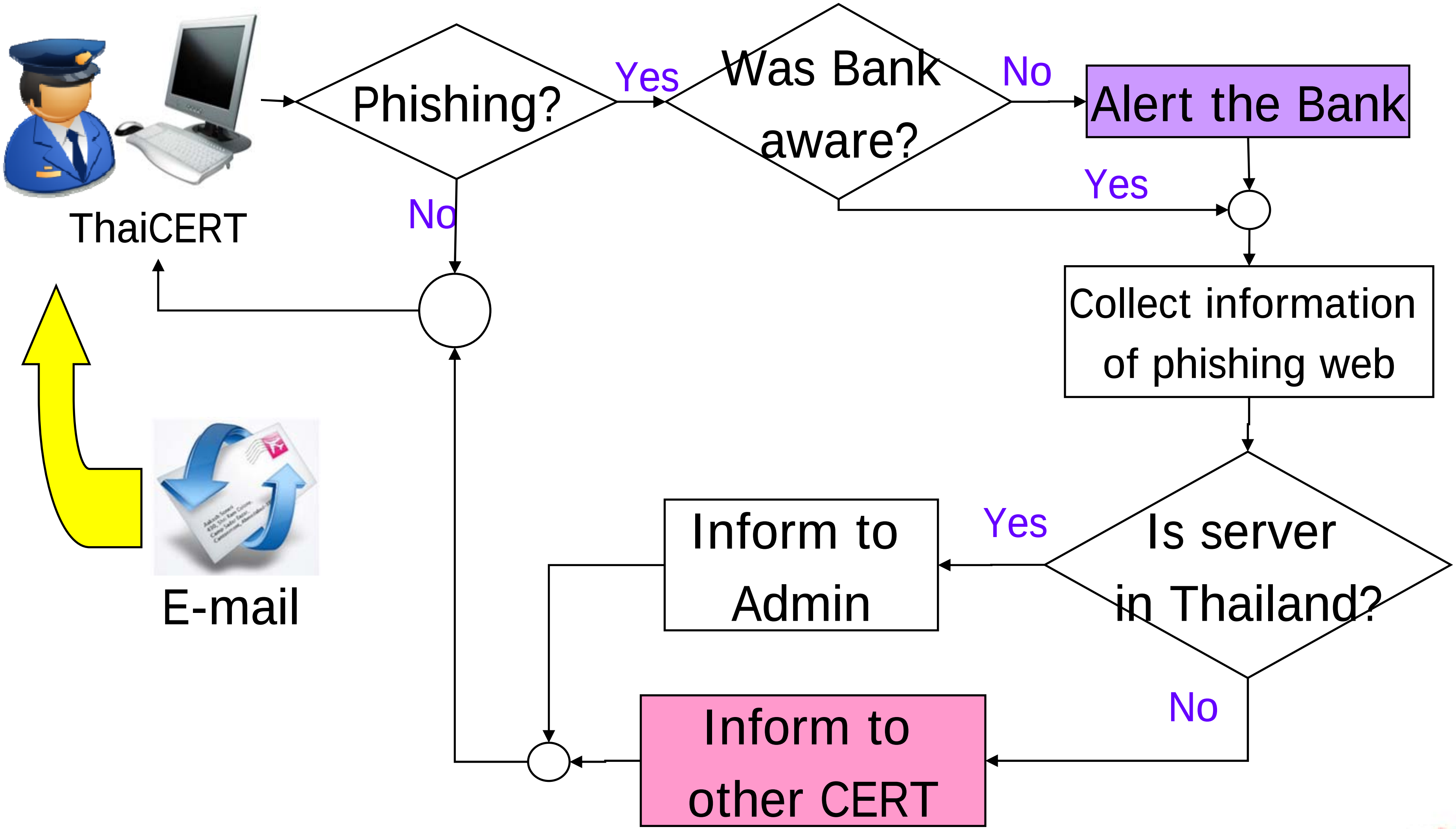
Source : http://www.antiphishing.org/reports/apwg report july 2006 - 2007.pdf

Types of phishing incidents

- Hosting phishing site
  - > 90% of ThaiCERT incidents
  - Servers were hacked
  - handle by using general IR process

- Thai banks-related phishing site
  - Servers were in outside Thailand
  - Thai banks fell victim too

How do we handle?



Discussion

- The Phishing cases are increasing.
- Phishing has little impact in Thailand.
- Thai people ignore English e-mail.
- Thai people don’t trust security in e-transaction.
- There are a lot of off-line banks and ATMs branches, which are convenient.

ThaiCERT
Thai Computer Emergency Response Team

NSTi
National Security
Technology & Innovation
Laboratory

Thai Computer Emergency Response Team

National Security Technology and Innovation Laboratory

NECTEC Building

112 Thailand Science Park Phahon Yothin Rd.,

Klong 1, Klong Luang, Pathumthani 12120. THAILAND.

TEL: **+66 (0) 2-564-6868**
FAX: **+66 (0) 2-564-6871**
E-MAIL: **thaicert@nectec.or.th**
WEBSITE: **http://www.thaicert.org**

Q/A