Botnet Statistical Analysis Tool

for Limited Resource Computer Emergency Response Team

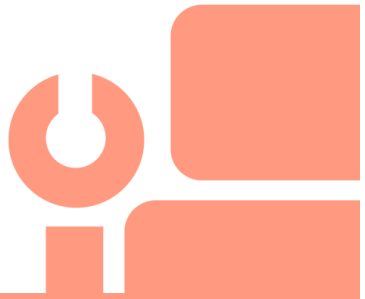
Presenter: Nuttapong Sanglerdsinlapachai

Authors: Kamol K., Nawattapon Y., Kitisak J.,
Nuttapong S. and Chanin L.
Thai Computer Emergency Response Team (ThaiCERT)
National Electronics and Computer Technology Center

IMF 2009: 5th International Conference on IT Security Incident Management & IT Forensics
September 15, 2009 @ Stuttgart, GERMANY

Outline

- Motivation
- Introduction to Botnet
- Existing Statistics about Botnet
- Statistical Analysis Tool
- Thailand's Botnet Report
- Conclusion

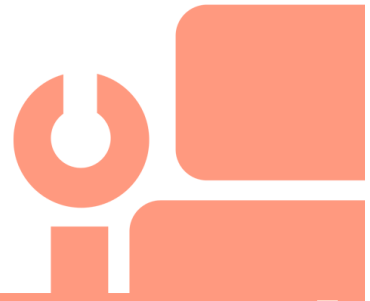


Motivation

- Botnet, fastest growing threats on Internet
- Need to monitor and handle incidents of botnets
- Some CERTs have limited resources for sensors and capturing tools
- Need to know country specific botnet's activities
- Luckily, available help from Shadowserver Foundation
- Build software tool for better incident handling and statistical analysis on botnets

What is Botnet?

- Malicious codes compromise online computers and secretly install “bot” to gain control
- Compromised computers linked into network called “botnet” a.k.a. “robot network”
- Botnet is controlled remotely for malicious attacks such as
  - DDoS, mass spamming, phishing, harvesting confidential information



Entities in Botnet

Bot

= program controls compromised computer

Zombie/drone

= compromised computer

C&C

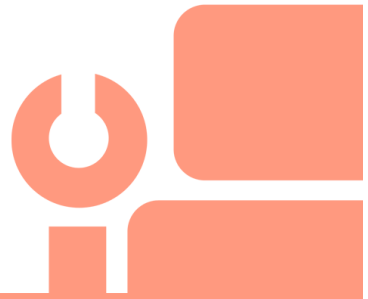
= command and control server

Bot herder

= attacker who controls network of bots

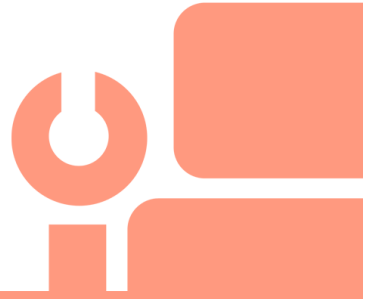
Characteristics of Botnets

- **Blending threats**
  - Self-propagation
  - Evading detection
  - Exploitation
  - Integrated command and control system
- **Categories of botnets based on communication**
  - IRC-based
  - HTTP-based
  - DNS-based
  - P2P-based
- **Topologies of botnets**
  - Centralized
  - Peer-to-peer
  - Unstructured network

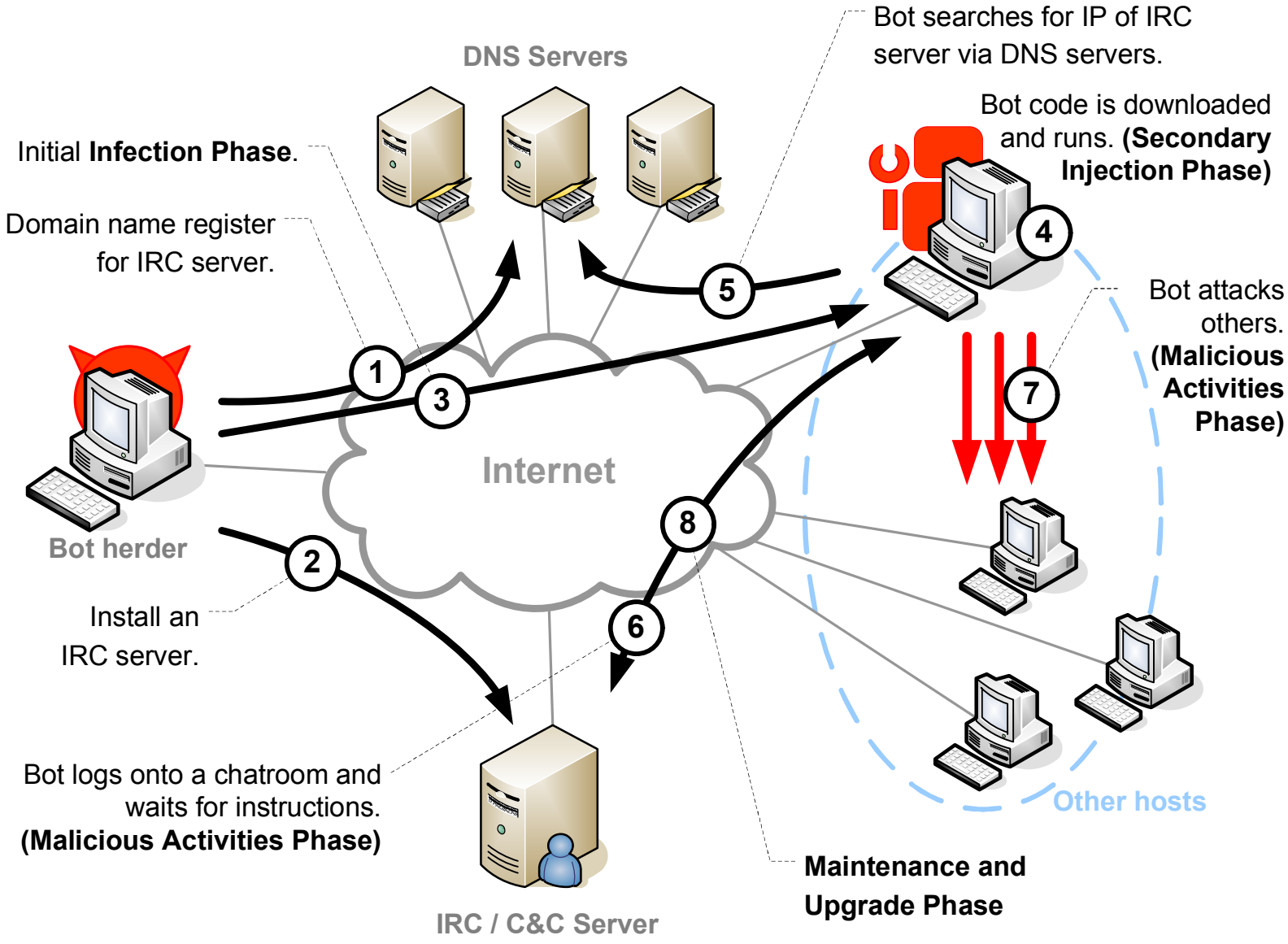


IRC-based Botnet's Life Cycle

- Setting up an IRC server
  - Prepare C&C server and register with DNS
  - Create secret chat room
- **Initial infection**
  - compromise initial machine
- **Secondary injection**
  - Download bot code and run on host (became drone or zombie)
- **Malicious activities**
  - Bots connect back to C&C for further instruction from bot herder
- **Maintenance and upgrade**
  - Change bot's code by downloading upgrade



How Botnet works?



Defense Against Botnets

- No measure is effective so far
- Use of typical firewall, antivirus, and antispyware
- Educated users
- Practicing safe-surfing habits
- Keep software up-to-date
- Bring down C&C ASAP
  - effective against centralized or IRC-based botnet
- P2P-based botnet is more difficult to take down

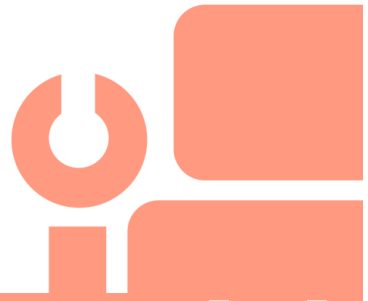
Shadowserver.org

- Shadowserver Foundation
  - Group of volunteer security professionals
  - track and report on malware, botnet activity, and electronic fraud
- **Mission:** to improve security of the Internet
- Provide valuable data for its subscribers
  - Especially on botnet's statistics
  - Via e-mails

shadowserver

Existing Botnet's Statistics

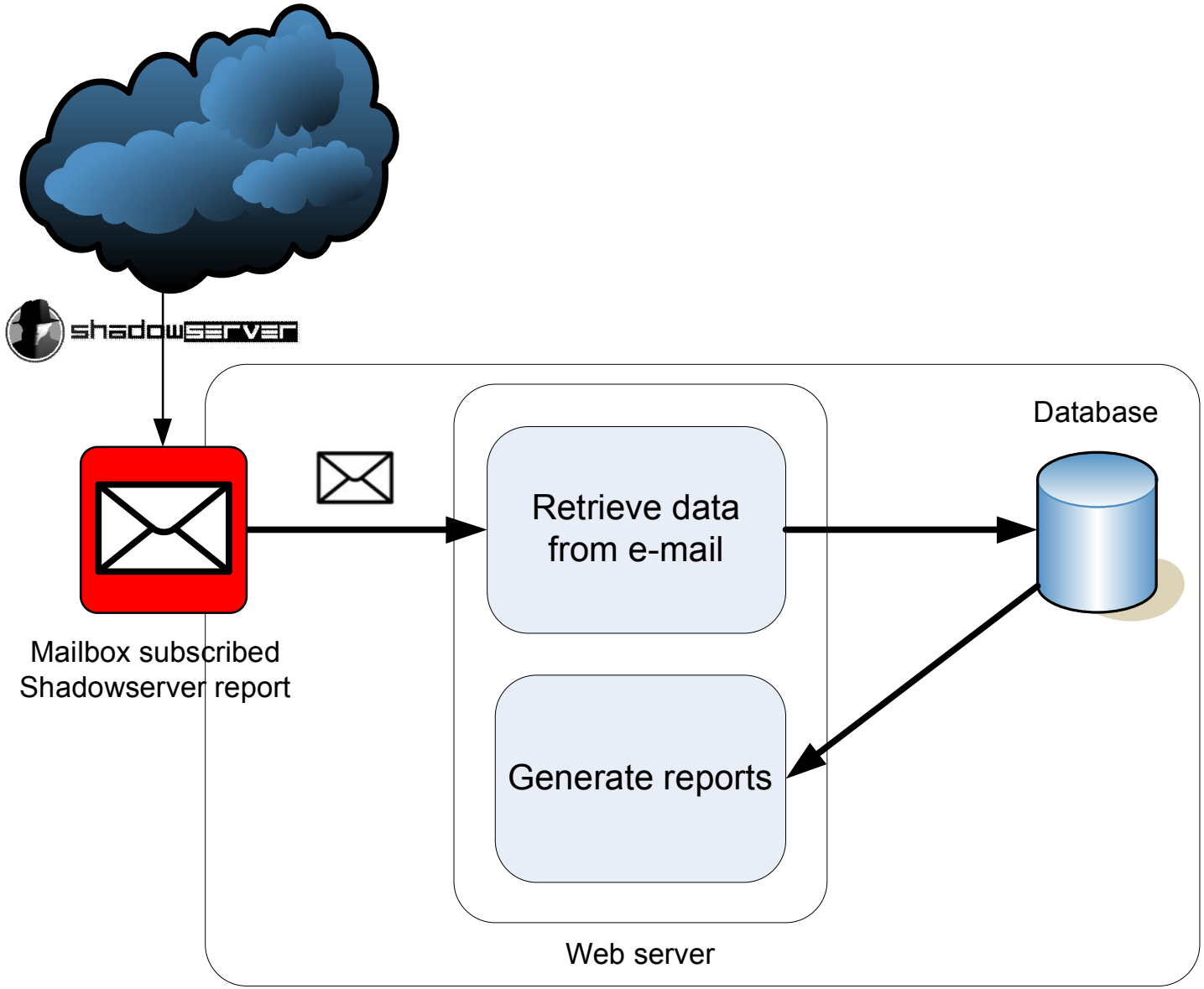
- Big pictures are available as seen by Shadowserver
  - Daily botnet size ~ total # of bits
  - Daily botnet status ~ total # of active C&C servers
- Other available data on Shadowserver.org are
  - Autonomous system numbers (ASNs)
  - Bots
  - Botnets
  - DDoS
  - Geographical locations
  - IRC ports
  - Malware
  - Scans
  - URLs
  - Viruses
- Details can be found on www.shadowserver.org



Botnet's Statistical Analysis Tool

- Approach
  - Import daily digest from e-mails into database
  - Retrieve data to create Thai's constituency report
  - Analyze data for incident handling
- Our tool consists of 3 parts
  - **Mailbox:** POP3 or IMAP protocol
  - **Database:** MySQL with 15 + 3 tables
  - **Web server:** Aphache 2.2.x + PHP 5.2.x + JpGraph
    - **Parsing module** (e-mails → database's tables)
    - **Reporting module** (database query + graphical representation procedure)

Diagram of Our Tool



Database

- Each table for each report type received from Shadowserver → Total 15 tables
- Extra 3 tables for management:

  [**asn-apnic**] – used for converting ASNs to ISPs which they were assigned to

  [**lastupdate**] – stored latest time both ASN converting table update and report retrieval

  [**user**] – keep username & password of the users

Example: Data in Database

asn	isp
1	Level 3 Communications, Inc.
2	University of Delaware
3	Massachusetts Institute of Technology
4	University of Southern California
6	Bull HN Information Systems Inc.
7	UK Defence Research Agency
8	Rice University
9	Carnegie Mellon University
10	CSNET Coordination and Information Center (CSNET-C...
11	Harvard University
12	New York University
13	Army Ballistic Research Laboratory
14	Columbia University

[**asn-apnic**] table

[**botnet_drone**] table:

keep “Drone” reports’ data

timestamp	drone	asn	geo	hostname
2007-09-08 13:06:23	125.26.2.233	9737	TH	125-26-2-233.adsl.totbb.net
2007-09-08 13:13:07	125.26.3.8	9737	TH	125-26-3-8.adsl.totbb.net
2007-09-08 13:15:17	125.26.3.12	9737	TH	125-26-3-12.adsl.totbb.net

rbl	cc	cc_asn	cc_geo	cc_dns	cc_port	infection
	124.38.150.118	17506	JP	fire.nurs.or.jp	6667	-
	124.38.150.118	17506	JP	fire.nurs.or.jp	6667	-
	124.38.150.118	17506	JP	fire.nurs.or.jp	6667	-

Parsing Module

Steps for data insertion:

- Retrieve e-mail with ZIP attachment from mailbox via IMAP
- Identify type of report by using e-mail's subject
- Extract ZIP file to get CSV report file
- Insert all extracted data into the database at proper table

About ThaiCERT

- Thailand's Computer Emergency Response Team
- Non-profit organization
- Unit under Research Institute called National Electronics and Computer Technology Center (NECTEC)
- Small number of staffs and limited budget
- Major missions
  - Incident handling and coordination
  - Computer security research
  - Raise awareness on computer security for Thais
  - Publish alerts, advisories, and articles for Thai people

Thailand's Botnet Report

THAILAND BOTNET REPORT

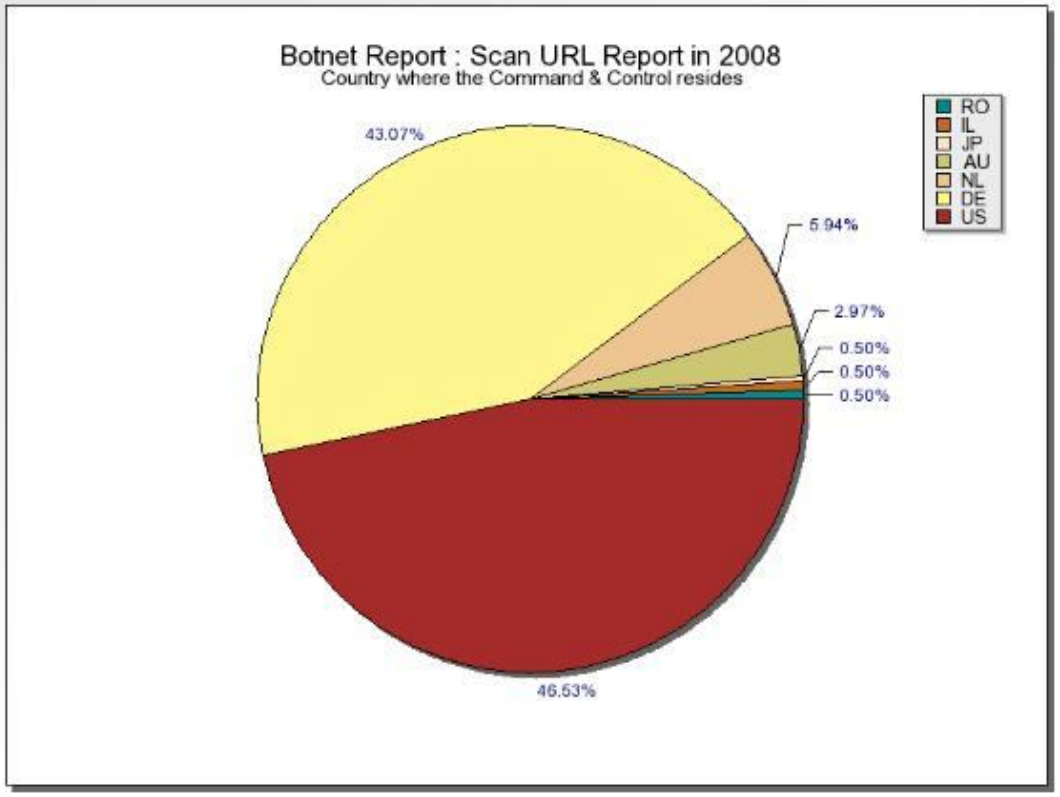
Dashboard | Profile | User management | Settings | Update | Log out

Header

- Botnet URL Report
- Compromised Host Report
- Click-Fraud Report
- Command and Control Report
- DDoS Report
- Drone Report
- Honeypot URL Report
- Proxy Report
- Scan Report
- Sandbox URL Report (Daily HTTP Report)
- Sandbox Connection Report
- Sandbox IRC Report (Daily Digest Report)
- Sinkhole HTTP Drone Report
- Sinkhole HTTP Referer Report
- Spam-URL Report

Botnet Scan Report

dashboard / Botnet Scan Report



DESCRIPTION

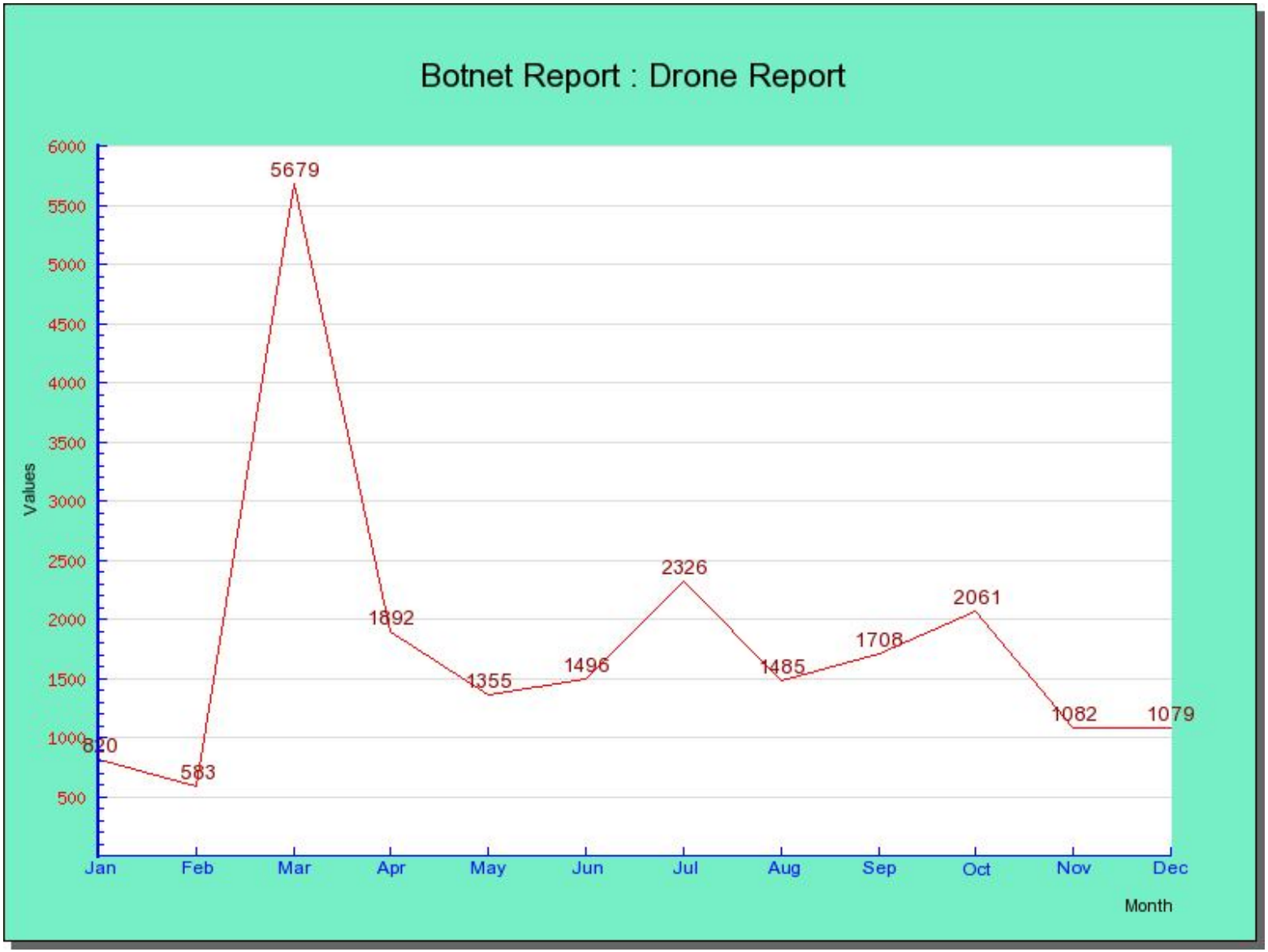
Vulnerbility scanning is a standard part of any botnet arsenal. We report on these as a warning that specific network blocks are being targeted

INTRODUCTION

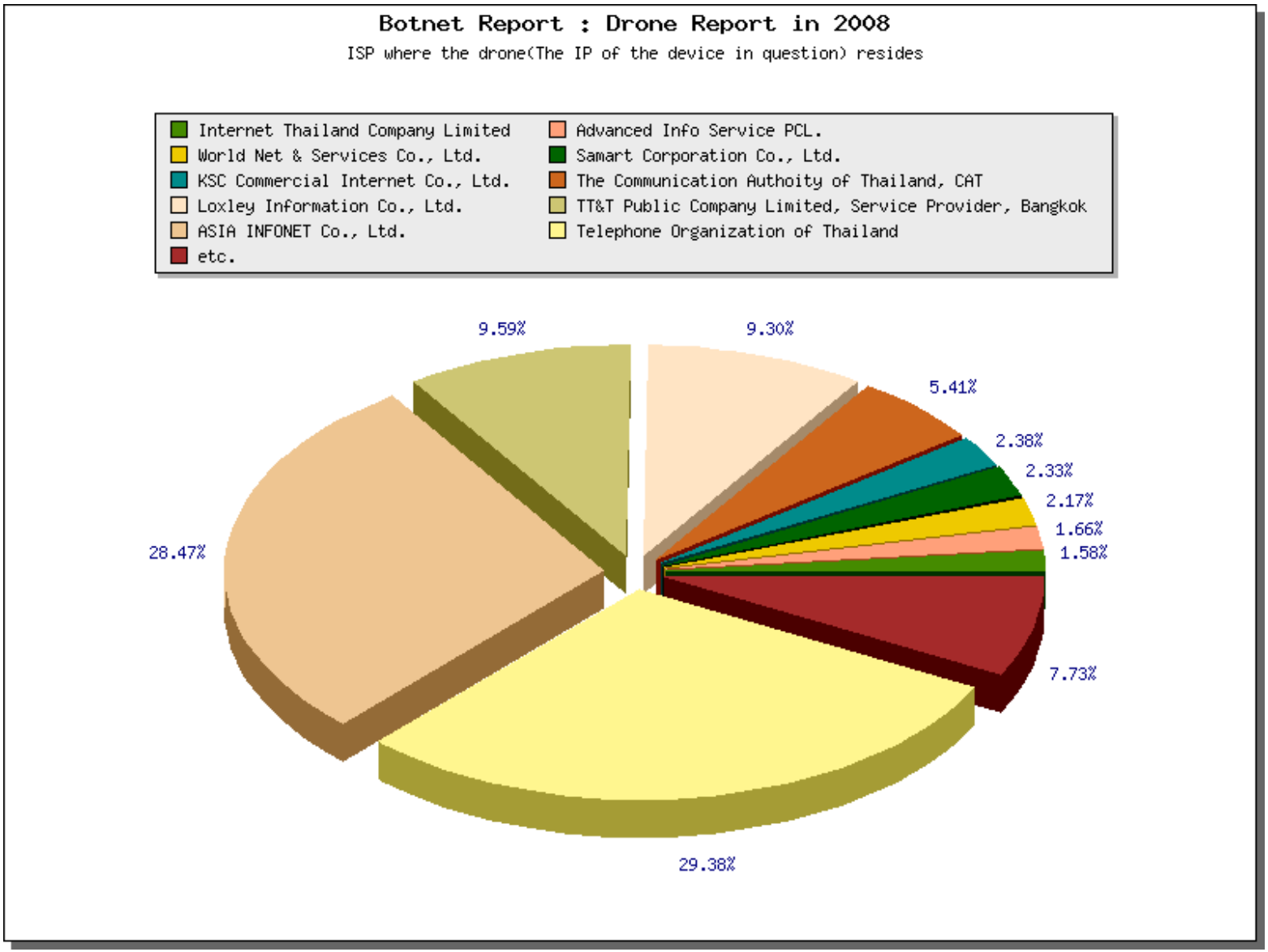
Directly related to remote exploits is the scanning of different network blocks. It is very useful to know when and what is being targeted.

DEMO

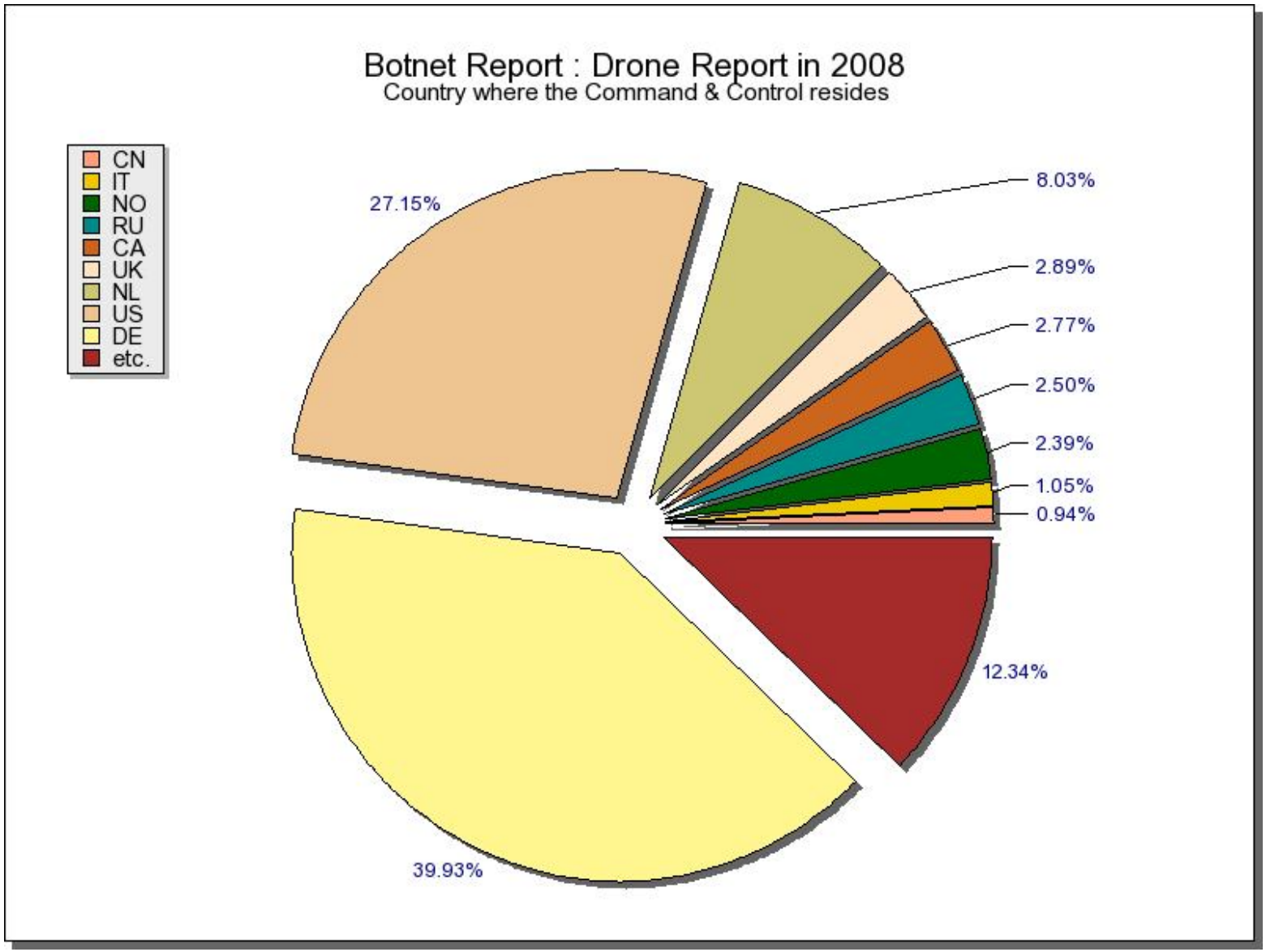
Number of Drones in Thailand (2008)



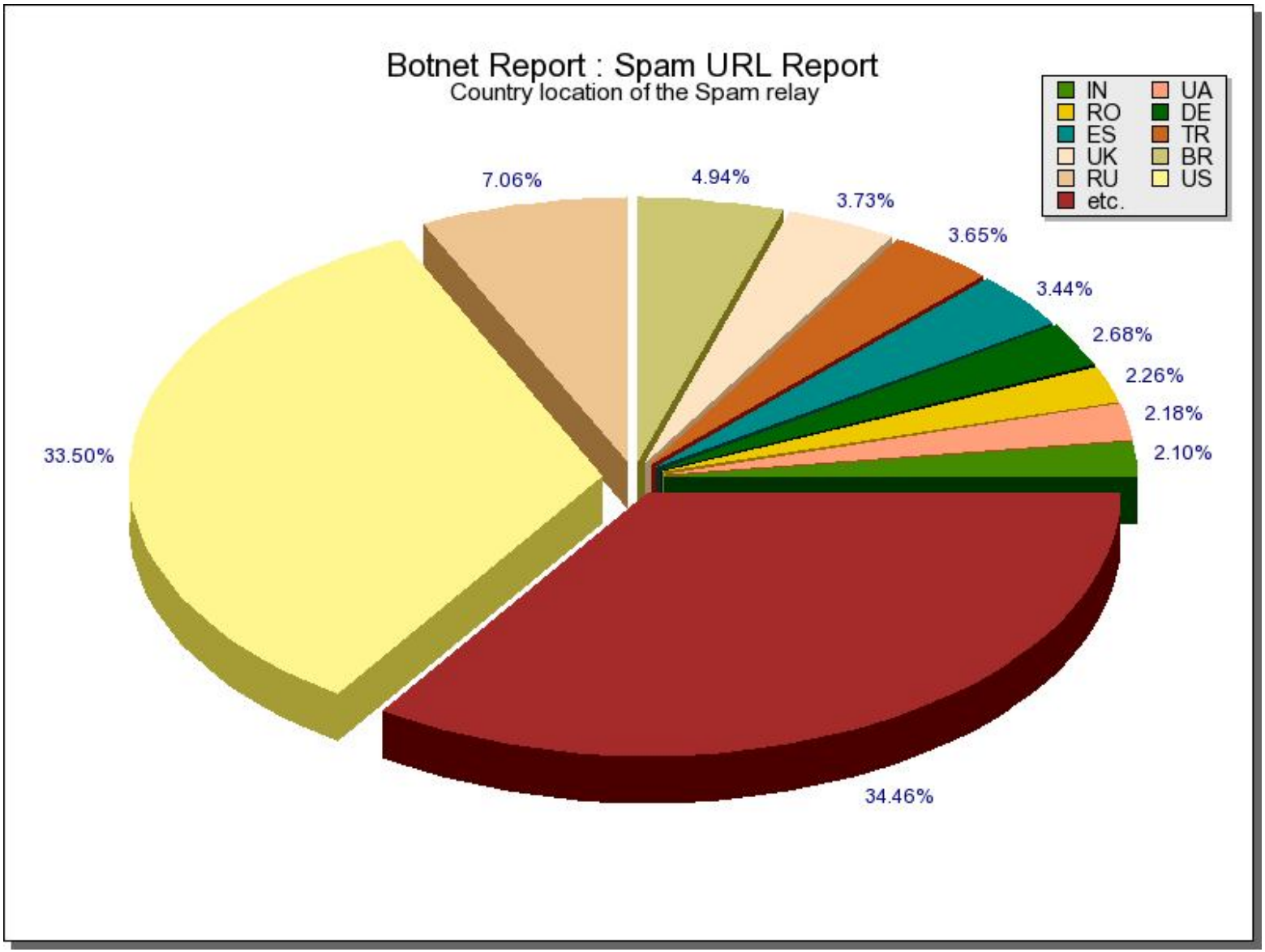
ISPs which hosted Drones in Thailand



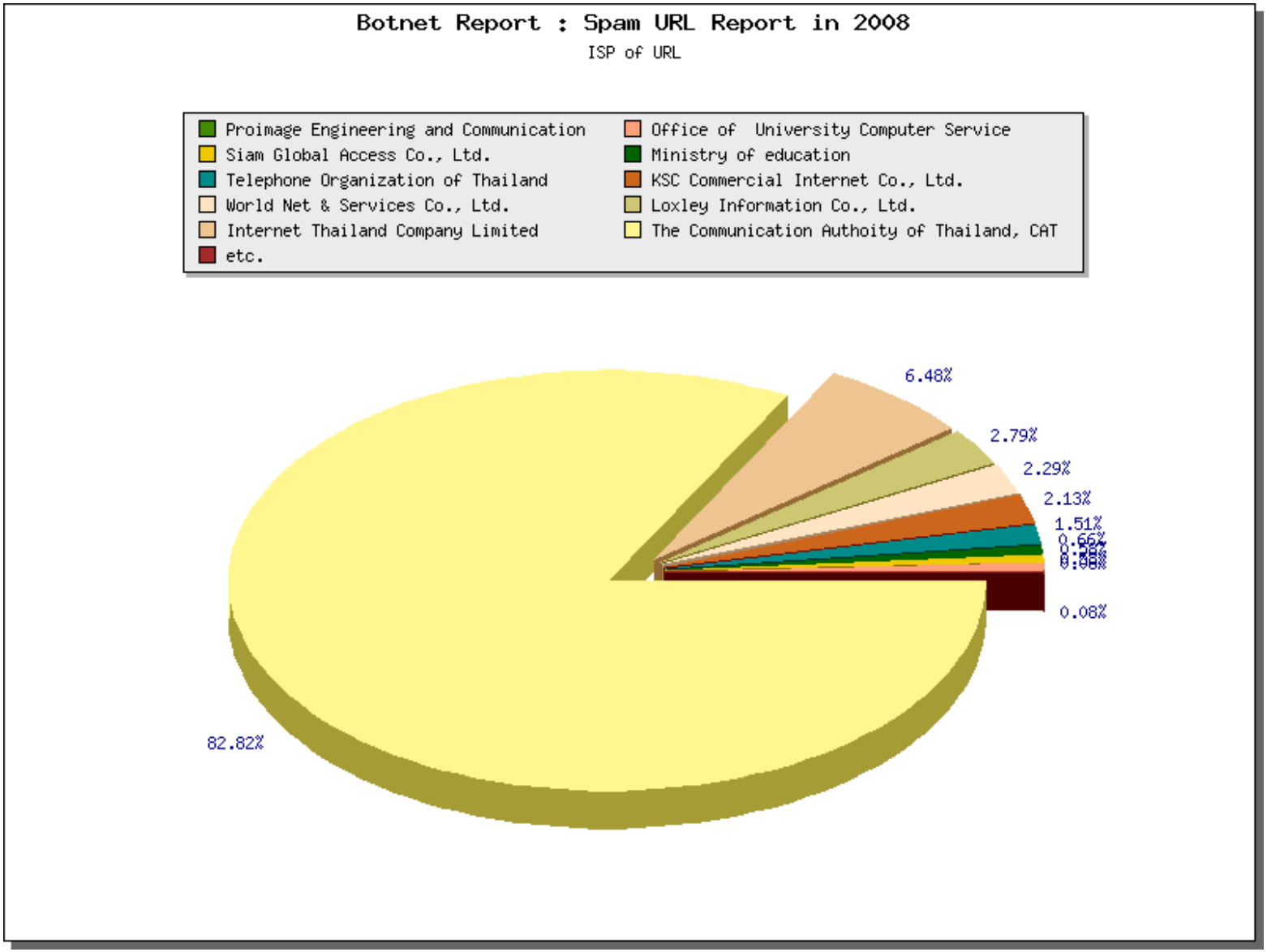
Countries which hosted C&C servers that controls bots in Thailand



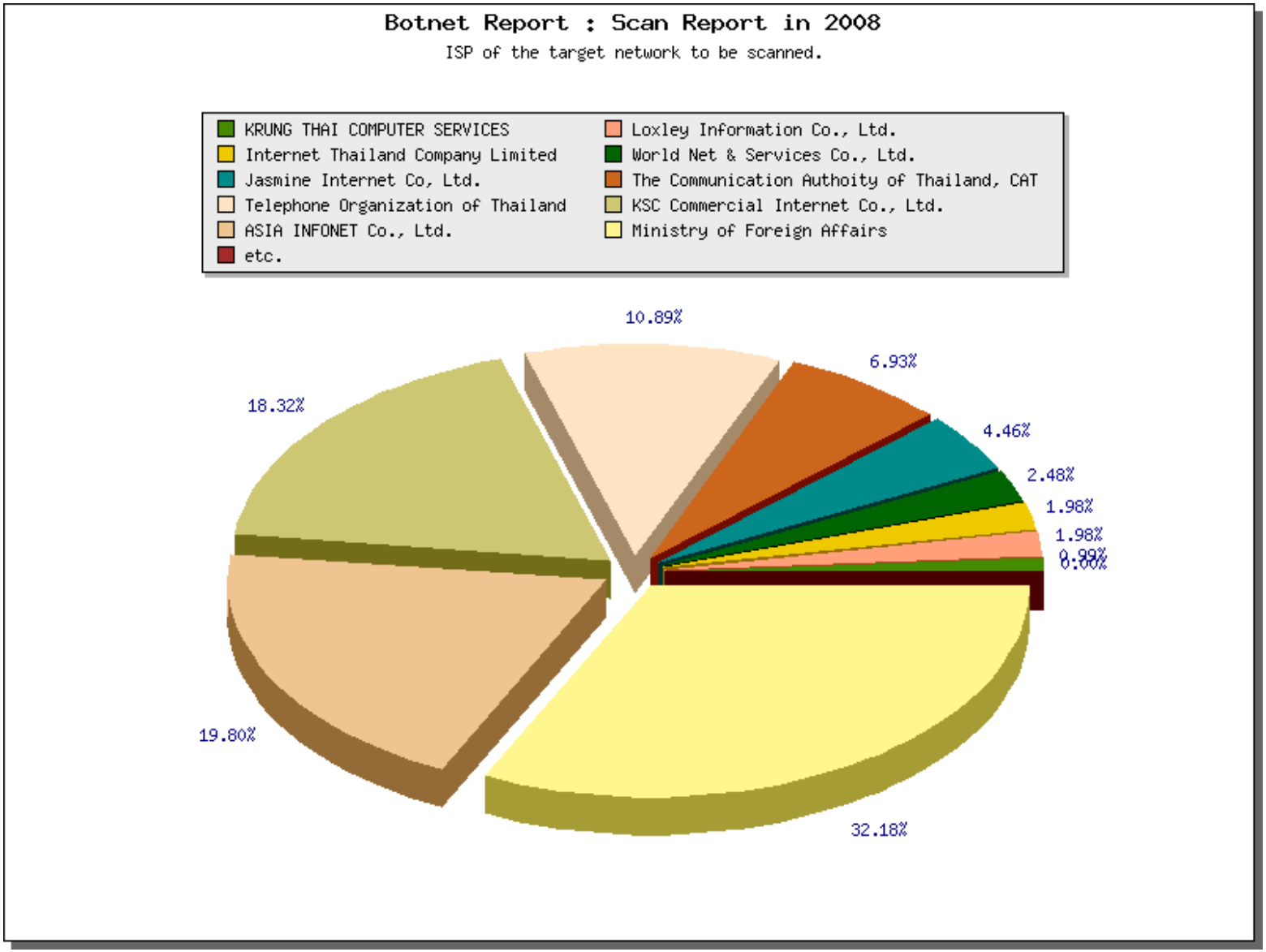
Countries of URLs in spams from Thailand



ISPs of URLs included in spam mails



Targeted networks scanned by botnets



Conclusion

- Mitigating effect of botnets require in-sight information on statistics
- Without sensors and monitoring tools, there is a passive approach and help over the Internet
- Existing information available at Shadowserver Foundation can be useful for CERTs
- Software tool can help reveal country specific information as demonstrated in this work
- Fight against botnets require collaboration

Acknowledgement

Special thank to dedicated and voluntary security professionals at the **Shadowserver Foundation**

shadowserver

Thank you

- Contact us

Thai Computer Emergency Response Team

E-mail: thaicert@nectec.or.th

Website: www.thaicert.org

Address: 112 Thailand Science Park,
Phahonyothin road, Klong 1, Klong Luang,
Pathumthani, 12120, Thailand

Tel: +66-02-564-6868

Fax: +66-02-564-6871