Articulus

Detecting IP Hijacking Through Server Fingerprinting
Research Question

How can we detect BGP IP hijacking by probing the at-risk subnets to detect suspect change to hosts and subnets.
(Slightly) related work

- BGPmon
- Cyclops by UCLA
- Uptrends SSL monitoring
- Unnamed Eric & Mick tool
The problem
What are the possibilities

- Man-in-the-middle attacks
- Downgrade attacks
- False information
Terminology

- Sentinel
  - Globally spread out
  - Executes fingers

- Node
  - At-risk host in need of protection

- Server
  - Command & control server
  - Result comparison

- Fingers
  - Commands executed on Sentinels

Intro - Fingerprinting - Avoiding Detection - Technical Details - Demo - Questions
Our solution

Get Fingerprints

Compare results
Fingerprinting

- Identifying software used
- Identifying software version used
- Identifying specific host characteristics
Fingerprinting - DNS

- Response only
- DNS censorship/hijacking detection.
Fingerprinting - Mail services

- SMTP / IMAP / POP

- STARTTLS

- 25/tcp open smtp
  Postfix smtpd
  smtp-commands: haarm.y-dmeer.nl, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
  ssl-cert: Subject: commonName=mail.y-dmeer.nl
  Issuer: commonName=PositiveSSL CA 2/organizationName=COMODO CA Limited
  /stateOrProvinceName=Greater Manchester/countryName=GB
  Public Key type: rsa
  Public Key bits: 2048
  Not valid before: 2012-12-28 00:00:00
  Not valid after: 2013-12-28 23:59:59
  MD5: 99d3 2b23 96f0 2dec 595f 8da8 9491 cef4
  SHA-1: f8be 2267 8923 c508 ed11 4217 fd14 96e3 8c0d f68b
Fingerprinting - Secure Shell

- RSA Fingerprint

- OpenSSH version

- Distribution

22/tep open ssh
OpenSSH 6.4p1 Debian 2 (protocol 2.0)
ssh-hostkey:
2048 a8:fe:3a:70:7f:e7:2e:1d:89:b2:35:e7:16:1a:77:11 (RSA)
Fingerprinting - Webservices

- WordPress 3.8
- Apache 2.2.16
- jQuery 1.10.2
Fingerprinting - Secure Webservices

- Nginx 1.4.4
- SHA-1 of certificate

```
443/tcp open  http
syn-ack 14.1.4.4
http-methods: No Allow or Public header in OPTIONS|response (status code 400)
http-title: 400 The plain HTTP request was sent to HTTPS port
ssl-cert: Subject: commonName=pretwolk.nl/organizationName=pretwolk.nl/
stateOrProvinceName=NH/countryName=NL/localityName=Dankort/
organizationalUnitName=pretwolk.nl/countryName=NL
Issuer: commonName=pretwolk.nl/organizationName=pretwolk.nl/
stateOrProvinceName=NH/countryName=NL/organizationalUnitName=pretwolk.nl/
emailAddress=contact@pretwolk.nl
Public Key type: rsa
Public Key bits: 4096
Not valid before: 2013-06-23T12:13:10+00:00
Not valid after: 2015-06-23T12:13:10+00:00
MD5: 9e1a 074d adfe cfe8 44de 965f d45a df51
SHA-1: 5df5 92e2 6ff9 4136 145a 12bb dc4b 4815 3328 8d1d
```
### Fingerprinting - Traceroute

- ICMP / UDP / TCP port 80

<table>
<thead>
<tr>
<th></th>
<th>IP Address</th>
<th>1st RTT</th>
<th>2nd RTT</th>
<th>3rd RTT</th>
<th>4th RTT</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>145.100.102.97</td>
<td>38.407 ms</td>
<td>40.024 ms</td>
<td>41.305 ms</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>145.100.99.17</td>
<td>1.254 ms</td>
<td>1.793 ms</td>
<td>2.313 ms</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>145.145.19.190</td>
<td>0.431 ms</td>
<td>0.439 ms</td>
<td>0.435 ms</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>195.69.145.245</td>
<td>0.820 ms</td>
<td>0.820 ms</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>91.121.131.169</td>
<td>6.333 ms</td>
<td>6.597 ms</td>
<td>6.548 ms</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>91.121.215.187</td>
<td>6.197 ms</td>
<td>91.121.128.37</td>
<td>13.795 ms</td>
<td>*</td>
</tr>
<tr>
<td>7</td>
<td>37.59.51.20</td>
<td>6.127 ms</td>
<td>6.143 ms</td>
<td>6.119 ms</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>37.59.51.20</td>
<td>6.488 ms</td>
<td>6.463 ms</td>
<td>6.416 ms</td>
<td></td>
</tr>
</tbody>
</table>
Fingerprinting - TCP/IP

- Uptime Guess

Device type: general purpose
Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
OS details: Linux 2.6.32 - 3.9, Linux 2.6.32 - 3.6, Linux 3.0 - 3.9
TCP/IP fingerprint:
OS:SC=\x4E%6E%E4%61%74%89%70%E5%B9%BE%E5%80%BB
OS:SC=\x4E%6E%E4%61%74%89%70%E5%B9%BE%E5%80%BB
OS:SC=\x4E%6E%E4%61%74%89%70%E5%B9%BE%E5%80%BB
Uptime guess: 162.618 days (since Thu Aug 22 01:49:39 2013)
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: All zeros
Final times for host: rtt: 4594 rttvar: 2611 to: 100000

- TCP characteristics

- TCP Sequence difficulty
Reporting

- Three levels
  - Paranoid
  - System administrator
  - User

- Alerts
  - Email
  - SMS
## Fingerprinting - Avoiding detection

<table>
<thead>
<tr>
<th>Service</th>
<th>Possibilities of hiding</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS</td>
<td>Alternate replies for Articulus and victim</td>
</tr>
<tr>
<td></td>
<td>Forward to original</td>
</tr>
<tr>
<td>DNSsec</td>
<td>Access to upstream tld and alternate replies for Articulus and victim</td>
</tr>
<tr>
<td></td>
<td>Forward to original</td>
</tr>
<tr>
<td>Mail services</td>
<td>Same software and modules enabled</td>
</tr>
<tr>
<td></td>
<td>MITM</td>
</tr>
<tr>
<td></td>
<td>Forward to original</td>
</tr>
<tr>
<td>Web server</td>
<td>Same software and modules enabled</td>
</tr>
<tr>
<td></td>
<td>MITM</td>
</tr>
<tr>
<td></td>
<td>Forward to original</td>
</tr>
<tr>
<td>TLS services</td>
<td>Access to the certificate and private key</td>
</tr>
<tr>
<td></td>
<td>Possible downgrade attack</td>
</tr>
<tr>
<td></td>
<td>Forward to original</td>
</tr>
<tr>
<td>Traceroute</td>
<td>Needs to be directly connected to a router in the original path</td>
</tr>
<tr>
<td>Openports</td>
<td>Port scan original and set up all of the above for enabled services</td>
</tr>
<tr>
<td>TCP/IP characteristics</td>
<td>Run nmap and running appropriate kernel modules</td>
</tr>
</tbody>
</table>
Comparing Fingerprints

- All output saved
- RegEx fingerprint
- Compare result to previous result
Technical details

- **Command and Control server**
  - Python API
  - Only works for approved UUID’s
  - HTTPS webserver with Python support (Apache, Nginx, …)
  - MySQL database (MariaDB should work as well)

- **Sentinels**
  - Python
  - Hardcoded server and certificate (-pinning)
  - POST requests to C&C API
  - Generates UUID
  - Parallel command execution
Technical details

- Secure
- Lightweight
- Scalable
Modular setup

- Add commands for execution on the fly
  - Sentinel needs commands to be installed though

- Add nodes dynamically

- IPv4 and IPv6 support
http://sne.pretwolk.nl:81
Thank you for your attention

» Are there any questions?
### Sentinels

<table>
<thead>
<tr>
<th>UUID:</th>
<th>IP / Hostname:</th>
<th>Added at:</th>
<th>Last seen:</th>
<th>Username:</th>
<th>Auth:</th>
<th>Enabled:</th>
</tr>
</thead>
<tbody>
<tr>
<td>07864b9a-7de8-11e3-990b-1803731facaab</td>
<td>145.100.102.101</td>
<td>Jan 20 2014 12:04</td>
<td>Jan 31 2014 16:04</td>
<td>mmeer</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>c55850de-7c56-11e3-b7a1-1803731fbb17</td>
<td>145.100.102.102</td>
<td>Jan 21 2014 14:19</td>
<td>Jan 31 2014 17:32</td>
<td>ebijnen</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>2e4ae8de-8343-11e3-858d-005056893a2c</td>
<td>162.219.4.50</td>
<td>Jan 22 2014 9:59</td>
<td>Jan 22 2014 9:59</td>
<td>root</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>0c6a5934-8343-11e3-903b-000c29472fda</td>
<td>85.17.176.216</td>
<td>Jan 22 2014 9:59</td>
<td>Jan 22 2014 9:59</td>
<td>root</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>a340f2f2-88c8-11e3-b447-000c29c6f80a</td>
<td>37.59.51.20</td>
<td>Jan 29 2014 10:35</td>
<td>Feb 4 2014 22:04</td>
<td>root</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>a2547dec-8b4c-11e3-b224-00163e24f6c0</td>
<td>197.85.187.1</td>
<td>Feb 1 2014 15:25</td>
<td>Feb 4 2014 22:04</td>
<td>root</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>0314a20a-8b4e-11e3-82b3-00163e357094</td>
<td>213.108.108.49</td>
<td>Feb 1 2014 15:34</td>
<td>Feb 1 2014 15:35</td>
<td>root</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>52faacee-8b4e-11e3-8711-35b71043f631</td>
<td>49.213.24.4</td>
<td>Feb 1 2014 15:37</td>
<td>Feb 1 2014 15:37</td>
<td>root</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>
### Nodes

<table>
<thead>
<tr>
<th>IP address</th>
<th>Hostname</th>
<th>Description</th>
<th>Fingers</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>213.108.104.135</td>
<td>greenhost.nl</td>
<td>Greenhost public website</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>213.239.154.20</td>
<td>tweakers.net</td>
<td>1337 Tech site</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>194.71.107.15</td>
<td>thepiratebay.se</td>
<td>Infinite music &amp; TV supplier</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>145.100.96.70</td>
<td>os3.nl</td>
<td>asdf</td>
<td>2</td>
<td></td>
</tr>
</tbody>
</table>

Add new node:

**IP Address:**

**Hostname:**

**Name / description:**
### Commands

<table>
<thead>
<tr>
<th>Service name:</th>
<th>Program:</th>
<th>Parameters:</th>
<th>Description:</th>
<th>Root:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Whatweb</td>
<td>whatweb</td>
<td>&quot;--colour=never&quot;</td>
<td>Whatweb checker</td>
<td>No</td>
</tr>
<tr>
<td>TCP Traceroute port 80</td>
<td>traceroute</td>
<td>&quot;-T&quot;, &quot;-p&quot;, &quot;80&quot;, &quot;-n&quot;</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Nmap server fingerprinting</td>
<td>nmap</td>
<td>&quot;-O&quot;</td>
<td></td>
<td>Yes</td>
</tr>
</tbody>
</table>

#### Add new command:
- **Command:**
- **Parameters:**
  
  Example: "-p80, -T, --verbose, --destination=1.2.3.4"

- **Service name:**
- **Description:**
- **Weight:** 100
- **Refresh time:** 30 seconds
- **Root:**

[Submit]
<table>
<thead>
<tr>
<th>#</th>
<th>IP Address</th>
<th>Website</th>
</tr>
</thead>
<tbody>
<tr>
<td>34</td>
<td>213.239.154.20</td>
<td>tweakers.net</td>
</tr>
<tr>
<td></td>
<td>197.85.187.1</td>
<td></td>
</tr>
</tbody>
</table>

<p>|     | 37.59.51.20    |             |
|     | 2014-02-04 22:06:59 |             |
|     | 2014-02-04 22:06:55 |             |
|     | 2014-02-04 22:04:51 |             |
|     | 2014-02-04 22:03:48 |             |
|     | 2014-02-04 22:02:44 |             |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Intro - Fingerprinting - Avoiding Detection - Technical Details - Demo - Questions</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The table contains various entries, each with a hexadecimal string and a timestamp. The timestamps are in the format `2014-02-04 22:30:24`.
Intro - Fingerprinting - Avoiding Detection - Technical Details - Demo - Questions
Thank you for your attention

- Are there any questions?