CyberProbe: Towards Internet-Scale Active Detection of Malicious Servers

A. NAPPA, Z. XU, M.Z. RAFIQUE, J.CABALLERO, G.GU
IMDEA SOFTWARE INSTITUTE
SUCCESS LAB, TEXAS A&M UNIVERSITY
Cybercriminals use geographically distributed servers to run their malicious operations

- Exploit servers -> Malware distribution
- Payment servers -> Monetization
- Redirectors -> Anonymity
- C&C servers -> Control botnets
- P2P bots (server functionality)
What is CyberProbe

Paunch's Operation

MALICIOUS

BENIGN
Existing detection techniques: Passive

- Honeypots
- Spamtraps

**LIMITATIONS**
- Slow
- Incomplete (i.e., limited view)
Existing detection techniques: Active

- Run malware samples
- Honeyclient farms (i.e. Google Safebrowsing)

**LIMITATIONS**

- Expensive
- Incomplete (i.e., Safebrowsing focuses on exploit servers)
Contributions

• Novel active probing approach for Internet-scale detection of malicious servers
• Novel adversarial fingerprint generation technique
• Implement approach into CyberProbe
• Use CyberProbe for 24 localized and Internet-wide scans
  • Identifies 151 malicious servers
  • 75% of the servers unknown to databases of malicious activity (e.g., VirusTotal, UrlQuery)
  • Identifies provider locality property
Cyberprobe in a nutshell

- Network traces
- Benign Traffic

Adversarial Fingerprint Generation

- Fingerprints
- Seed Servers

- Port
- Target Ranges
- Fingerprint

Scanning

- Malicious Servers
Fingerprints

• A fingerprint for each operation & server type
• A fingerprint comprises:
  • A probe construction function ➔ Packet
  • A classification function ➔ Snort signature

Clickpayz1
**Probe:** GET /td?aid=e9xmkgg5h6&said=26427
**Signature:**
  content: “302”; http_stat_code;
  content: “\r\n\r\nLoading...”
Adversarial Fingerprint Generation: Goals

- Minimize traffic
- Generate inconspicuous probes
Adversarial Fingerprint Generation: Architecture
Generation details

- Replay
  - VPN for: anonymity, IP diversity and for new states
  - Check result against random resource from the server
Scanning

- 3 scanners:
  - Horizontal \(\rightarrow\) SYN scan
  - AppTCP scanner (sends app-level probe)
  - UDP scanner
- 3 scan ranges:
  - Localized-reduced
  - Localized-extended
  - Internet-wide
- Signature matching uses Snort
AppTCP and UDP scanners

CyberProbe

INTERNET

Malicious Family A

Benign Server
Scanning summary

TCP
- TCP horizontal scanner (fast, polite)
- TCP sniffer (reliable to get responses to our probes)
- AppTCP scanner (Asynchronous + Snort)

UDP
- UDP scanner (fast, polite) + Snort
Ethical Considerations

To scan as politely as possible we:

• Rate-limit scanners
• Set up forward and backward DNS entries for scanners
• Set up a webpage in the scanners to explain our experiment
• Remove from whitelist provider’s ranges that request so
• Manually check fingerprints
Adversarial fingerprint generation results

<table>
<thead>
<tr>
<th>Type</th>
<th>Source</th>
<th>Families</th>
<th>Pcaps</th>
<th>RRP$s$</th>
<th>RRP$s$ Replay</th>
<th>Seeds</th>
<th>Fingerprints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware</td>
<td>VirusShare</td>
<td>152</td>
<td>918</td>
<td>1,639</td>
<td>193</td>
<td>19</td>
<td>18</td>
</tr>
<tr>
<td>Malware</td>
<td>MALICIA</td>
<td>9</td>
<td>1,059</td>
<td>764</td>
<td>602</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Honeyclient</td>
<td>MALICIA</td>
<td>6</td>
<td>1,400</td>
<td>42,160</td>
<td>9,497</td>
<td>5</td>
<td>2</td>
</tr>
<tr>
<td>Honeyclient</td>
<td>UrlQuery</td>
<td>1</td>
<td>4</td>
<td>11</td>
<td>11</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>
AppTCP Scan Results

- 151 total servers found with the scans
- Virustotal knew only about 25% of the servers
- UrlQuery 15%
- MalwareDomainList and VxVault 1%

4x Better Coverage
# Servers Operations

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>bestav</td>
<td>3</td>
<td>4</td>
<td>23</td>
<td>7</td>
<td>3.3</td>
</tr>
<tr>
<td>bh2-adobe</td>
<td>1</td>
<td>1</td>
<td>13</td>
<td>7</td>
<td>1.8</td>
</tr>
<tr>
<td>bh2-ngen</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>1.0</td>
</tr>
<tr>
<td>blackrev</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>1.0</td>
</tr>
<tr>
<td>clickpayz</td>
<td>2</td>
<td>2</td>
<td>51</td>
<td>6</td>
<td>8.5</td>
</tr>
<tr>
<td>doubleighty</td>
<td>1</td>
<td>1</td>
<td>18</td>
<td>9</td>
<td>2.0</td>
</tr>
<tr>
<td>kovter</td>
<td>2</td>
<td>2</td>
<td>9</td>
<td>4</td>
<td>2.2</td>
</tr>
<tr>
<td>ironsource</td>
<td>1</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td>1.7</td>
</tr>
<tr>
<td>optinstaller</td>
<td>1</td>
<td>1</td>
<td>18</td>
<td>4</td>
<td>2.0</td>
</tr>
<tr>
<td>soft196</td>
<td>1</td>
<td>1</td>
<td>8</td>
<td>4</td>
<td>2.0</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>14</strong></td>
<td><strong>15</strong></td>
<td><strong>151</strong></td>
<td><strong>47</strong></td>
<td><strong>3.2(avg.)</strong></td>
</tr>
</tbody>
</table>
Once a relationship has been established with a provider it is very likely that more than one malicious server will be setup with this provider
# P2P bots Scan Results

<table>
<thead>
<tr>
<th>Type</th>
<th>Start-Date</th>
<th>Port</th>
<th>Fingerprint</th>
<th>Targets</th>
<th>SC</th>
<th>Rate</th>
<th>Time</th>
<th>Found</th>
</tr>
</thead>
<tbody>
<tr>
<td>R</td>
<td>2013-03-19</td>
<td>UDP/16471</td>
<td>zeroaccess</td>
<td>40,448</td>
<td>1</td>
<td>10</td>
<td>1.2h</td>
<td>55 (0.13%)</td>
</tr>
<tr>
<td>I</td>
<td>2013-05-03</td>
<td>UDP/16471</td>
<td>zeroaccess</td>
<td>2,6B</td>
<td>4</td>
<td>50,000</td>
<td>3.6h</td>
<td>7,884 (0.0003%)</td>
</tr>
</tbody>
</table>
Related Work

Scanning:
- Leonard et al. IMC ‘10
- Heninger et al. Usenix Security ‘12
- Zmap

Fingerprinting:
- FiG
- PeerPress

Signature Generation:
- Honeycomb, Autograph, EarlyBird, Polygraph, Hamsa
- Botzilla, Perdisci et al., Firma
Conclusion

• Novel active probing approach for Internet-scale detection of malicious servers
• Novel adversarial fingerprint generation technique
• Implement approach into CyberProbe
• Use CyberProbe for 24 localized and Internet-wide scans
  • Identifies 151 malicious servers
  • 75% of the servers unknown to databases of malicious activity (e.g., VirusTotal, UrlQuery)
  • Identifies provider locality property
Thanks!
Future Work

- Scanner IP diversity
- Completeness
- Shared hosting (i.e. CDN)
- Complex protocol semantics