Exit from Hell? – Reducing the Impact of Amplification DDoS Attacks

Marc Kührer
Thomas Hupperich
Christian Rossow
Thorsten Holz

1 Ruhr-University Bochum
2 Saarland University

USENIX Security, August 2014
Technical Details Behind a 400Gbps NTP Amplification DDoS Attack

Published on February 13, 2014 01:00AM by Matthew Prince.

On Monday we mitigated a large DDoS that targeted one of our customers. The attack peaked just shy of 400Gbps. We've seen a handful of other attacks at this scale, but this is the largest attack we've seen that uses NTP amplification. This style of attacks has grown dramatically over the last six months and poses a significant new threat to the web.
Amplification DDoS Attacks

Exit from Hell? Reducing the Impact of Amplification DDoS Attacks
Contents

- Can we mitigate the UDP-based amplifications?
- Are there other amplifiers than UDP?
- Can we identify spoofing-enabled networks?
## Amplifier Classification

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Unix</th>
<th>Linux</th>
<th>Ubuntu</th>
<th>FreeBSD</th>
<th>Windows</th>
<th>ZyNOS</th>
<th>Cisco IOS</th>
<th>Junos</th>
<th>NetOS</th>
<th>Others</th>
<th>Unknown</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS</td>
<td>3.6</td>
<td>3.4</td>
<td>0.0</td>
<td>0.0</td>
<td>0.8</td>
<td>7.5</td>
<td>0.1</td>
<td>0.0</td>
<td>0.0</td>
<td>1.1</td>
<td>83.5</td>
</tr>
<tr>
<td>NetBIOS</td>
<td>0.4</td>
<td>0.1</td>
<td>0.0</td>
<td>0.0</td>
<td>87.3</td>
<td>0.3</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.7</td>
<td>11.2</td>
</tr>
<tr>
<td>NTP</td>
<td>18.2</td>
<td>26.8</td>
<td>0.0</td>
<td>4.7</td>
<td>0.2</td>
<td>0.0</td>
<td>40.8</td>
<td>2.9</td>
<td>0.0</td>
<td>1.7</td>
<td>4.7</td>
</tr>
<tr>
<td>SNMP</td>
<td>1.5</td>
<td>11.4</td>
<td>0.1</td>
<td>0.1</td>
<td>0.8</td>
<td>17.8</td>
<td>2.2</td>
<td>0.0</td>
<td>0.0</td>
<td>8.7</td>
<td>57.4</td>
</tr>
<tr>
<td>SSDP</td>
<td>1.8</td>
<td>36.0</td>
<td>5.5</td>
<td>0.0</td>
<td>1.3</td>
<td>0.7</td>
<td>0.0</td>
<td>0.0</td>
<td>19.3</td>
<td>1.8</td>
<td>33.6</td>
</tr>
</tbody>
</table>
NTP Amplification Case Study

- **NTP: Network Time Protocol**
  - Optional `monlist` debug feature
  - 8B request and 44kB response $\rightarrow$ >1000x amplification
  - In Dec ‘13: **1.6 million amplifiers**

- Timeline of vulnerability discovery
  - Aug ‘13: Notified vendors, reserved CVE
  - Jan ‘14: Released CVE + coop with CERTs/ISPs
  - Feb ‘14: Presented vulnerabilities at NDSS
Exit from Hell? Reducing the Impact of Amplification DDoS Attacks:
Exit from Hell? Reducing the Impact of Amplification DDoS Attacks:

Contents

- Can we mitigate the UDP-based amplifications?
- Are there other amplifiers than UDP?
- Can we identify spoofing-enabled networks?
TCP and Reflection

TCP 3-Way Handshake

- Reflection
- No amplification

Exit from Hell? Reducing the Impact of Amplification DDoS Attacks:
TCP and Reflection

SYN/ACK Amplifiers

- Keep repeating SYN/ACK until ACK
- Default, e.g., in *nix
- Reason: packet loss
TCP and Reflection (also see WOOT ‘14 paper)

PSHy hosts

RST storms

C

S

C

S

SYN

SYN/ACK

PSH

PSH

PSH

...

SYN

RST

RST

RST

RST

...

Exit from Hell? Reducing the Impact of Amplification DDoS Attacks:
Methodology

Scan
- IPv4 Address Range
- TCP SYN Packets

Filter
- Amplification >20
- Prevalent Protocols

Stats
- Amplifier Classification
- Evaluate Countermeasures
## Amplification Statistics

<table>
<thead>
<tr>
<th>Protocol</th>
<th>SYN/ACK</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td># Ampl.</td>
<td>AF</td>
<td># Ampl.</td>
<td>AF</td>
<td># Ampl.</td>
<td>AF</td>
</tr>
<tr>
<td>FTP</td>
<td>2,907,279</td>
<td>22x</td>
<td>274</td>
<td>103x</td>
<td>5,577</td>
<td>53,927x</td>
</tr>
<tr>
<td>HTTP</td>
<td>421,487</td>
<td>60x</td>
<td>241</td>
<td>147x</td>
<td>3,411</td>
<td>432x</td>
</tr>
<tr>
<td>NetBIOS</td>
<td>8,863</td>
<td>54x</td>
<td>64</td>
<td>71x</td>
<td>3,087</td>
<td>78,042x</td>
</tr>
<tr>
<td>SIP</td>
<td>16,496</td>
<td>1,596x</td>
<td>2</td>
<td>696x</td>
<td>6,306</td>
<td>32,411x</td>
</tr>
<tr>
<td>SSH</td>
<td>81,256</td>
<td>80x</td>
<td>391</td>
<td>57x</td>
<td>5,889</td>
<td>29,705x</td>
</tr>
<tr>
<td>Telnet</td>
<td>2,112,706</td>
<td>28x</td>
<td>2,353</td>
<td>3,272x</td>
<td>4,242</td>
<td>79,625x</td>
</tr>
</tbody>
</table>
## Attack Frequency

- Response packets per X seconds

<table>
<thead>
<tr>
<th>Protocol</th>
<th>SYN/ACK</th>
<th>PSH</th>
<th>RST</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>&lt; 10</td>
<td>&lt; 30</td>
<td>&lt; 60</td>
</tr>
<tr>
<td>FTP</td>
<td>2</td>
<td>5</td>
<td>10</td>
</tr>
<tr>
<td>HTTP</td>
<td>2</td>
<td>6</td>
<td>11</td>
</tr>
<tr>
<td>NetBIOS</td>
<td>8</td>
<td>17</td>
<td>22</td>
</tr>
<tr>
<td>SIP</td>
<td>2</td>
<td>6</td>
<td>12</td>
</tr>
<tr>
<td>SSH</td>
<td>3</td>
<td>6</td>
<td>11</td>
</tr>
<tr>
<td>Telnet</td>
<td>2</td>
<td>5</td>
<td>10</td>
</tr>
</tbody>
</table>
Amplifier Classification

DEVICE TYPE
- Networking Equipment
- Misc
- Unknown

OS
- Unknown
- Linux
- ZyNOS
Can we mitigate the UDP-based amplifications?

Are there other amplifiers than UDP?

Can we identify spoofing-enabled networks?
Remote Spoofer Test via DNS

University

S: Scanner

7.7.7.7

Unknown Netw.

P: DNS Proxy

1.2.3.4

Public Resolver

R: Recursive DNS Resolver

8.8.8.8

A? 1.2.3.4.rub.de

srcIP: 7.7.7.7
dstIP: 1.2.3.4

A? 1.2.3.4.rub.de

srcIP: 7.7.7.7
dstIP: 8.8.8.8

A 1.2.3.4.rub.de: x.x.x.x

srcIP: 8.8.8.8
dstIP: 7.7.7.7

Exit from Hell? Reducing the Impact of Amplification DDoS Attacks:
Active Defense

- **SYN/ACK storms**: send RST segments
  - Stops about 99.9% of the SYN/ACK streams

- **RST storm**: send ICMP port unreachable messages
  - Stops about 80% of the RST streams
## Remote Spoofer Test Results

<table>
<thead>
<tr>
<th>Filter</th>
<th>#P</th>
<th>#AS_P</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top 4 Resolver</td>
<td>42,691</td>
<td>301</td>
</tr>
<tr>
<td>Top 10 Resolver</td>
<td>45,072</td>
<td>352</td>
</tr>
<tr>
<td>Distinct AS</td>
<td>170,451</td>
<td>2,692</td>
</tr>
</tbody>
</table>
Conclusion

- Mitigation of NTP amplifiers (largely) successful
- TCP amplification may cause issues in the future
- Remote test finds at least 300 spoofing ASes
Q & A ???
Thank You!!!

- Presented By -
Narayanan Seshan