Taming the 800 Pound Gorilla: The Rise and Decline of NTP DDoS Attacks

Jakub (Jake) Czyz, University of Michigan
Michael Kallitsis, Merit Network, Inc.
Manaf Gharaiibeh, Colorado State University
Christos Papadopoulos, Colorado State University
Michael Bailey, University of Michigan and University of Illinois
Manish Karir, Merit Network, Inc.

Internet Measurement Conference
Vancouver, BC, Canada
November 5-7, 2014
The DDoS “Hockey Stick Era”
Agenda & Overview

• Introduce NTP Reflected/Amplified DDoS mechanics
• Summarize Key Measurements
  – **Goal:** to understand the attack:
    Mechanics, size and evolution, impacts, enablers, victims, attacker clues and motivations, and mitigation progress
  – Six datasets: global and local perspectives
    • Global DDoS attack counts/types: Nov.’13 – Apr. ’14
    • Global NTP traffic: Nov.’13 – Apr. ’14
    • Darknet (IPv4, ~/8): Sep. ‘13 – Apr. ‘14
    • Two Local ISP/campus netflow: Dec. ‘13 – Feb. ‘14
    • IPv4-wide NTP monlist & version probes: Jan. ‘14 – Apr. ‘14
• A strange discovery
• Summary and conclusion
Reflected & Amplified DDoS Attacks

- **Volumetric** attacks that seek to overwhelm victim with traffic
- Often rely on properties of several **UDP-based protocols**:  
  - **Spoofability**, **broad deployment**, and **large responses** to small requests
Reflected & Amplified DDoS Attacks
NTP DDoS Attack Mechanics

• Network Time Protocol: for synchronizing system clocks
  – Widely deployed on servers, workstations, & network gear

• Normal Use:
  – small client and small server packets (symmetric)
  – typically one exchange every 1 to 12 minutes
  – NTP protocol normal modes (mode 3 or 4)

• Attacks:
  – small requests, large responses (asymmetric)
  – typically many times per second
  – NTP protocol special diagnostic modes (6 or 7); most egregiously: monlist command (out of several):
    • Request: 1pkt, ~100B
    • Response: up to 40pkt, ~20,000B; ~200x amplification
NTP Attacks

There are ~300k monthly DDoS attacks.

- **Majority of Large Attacks**
- **Negligible Fraction of all DDoS**
NTP monlist Amplifier Population

See also: Kührer et al. 2014@USENIX

Drop: 93%
Amplifier Power

Handful of “Mega Amplifiers”:
Top 20 avg.: > 60,000,000x

Pool of 1k: > 10,000x

Pool of ~100k: 200x

Median: 942; 95th percentile: 90K

Median: 10x
# The monlist Table

<table>
<thead>
<tr>
<th>remote address</th>
<th>port</th>
<th>local address</th>
<th>count</th>
<th>m</th>
<th>ver</th>
<th>rstr</th>
<th>avgint</th>
<th>lstint</th>
</tr>
</thead>
<tbody>
<tr>
<td>204</td>
<td>37164</td>
<td>0.0.0.0</td>
<td>5</td>
<td>7</td>
<td>2</td>
<td>0</td>
<td>3835</td>
<td>0</td>
</tr>
<tr>
<td>217</td>
<td>123</td>
<td>0.0.0.0</td>
<td>1041759</td>
<td>7</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>204</td>
<td>80</td>
<td>0.0.0.0</td>
<td>135</td>
<td>7</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>31.1</td>
<td>27</td>
<td>0.0.0.0</td>
<td>35843</td>
<td>7</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>192.1</td>
<td>8088</td>
<td>0.0.0.0</td>
<td>52071</td>
<td>7</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>198.1</td>
<td>27016</td>
<td>0.0.0.0</td>
<td>21282</td>
<td>7</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>75.1</td>
<td>3074</td>
<td>0.0.0.0</td>
<td>1</td>
<td>7</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>128</td>
<td>43009</td>
<td></td>
<td>29430</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>63</td>
<td>2</td>
</tr>
<tr>
<td>75.1</td>
<td>80</td>
<td>0.0.0.0</td>
<td>10</td>
<td>7</td>
<td>2</td>
<td>0</td>
<td>9</td>
<td>2</td>
</tr>
<tr>
<td>174.1</td>
<td>9987</td>
<td>0.0.0.0</td>
<td>281</td>
<td>7</td>
<td>2</td>
<td>0</td>
<td>11</td>
<td>3</td>
</tr>
<tr>
<td>101.1</td>
<td>3074</td>
<td>0.0.0.0</td>
<td>2</td>
<td>7</td>
<td>2</td>
<td>0</td>
<td>6</td>
<td>4</td>
</tr>
<tr>
<td>98.1</td>
<td>53</td>
<td>0.0.0.0</td>
<td>2</td>
<td>7</td>
<td>2</td>
<td>0</td>
<td>6</td>
<td>4</td>
</tr>
<tr>
<td>5.1</td>
<td>25565</td>
<td>0.0.0.0</td>
<td>1163</td>
<td>7</td>
<td>2</td>
<td>0</td>
<td>5</td>
<td>4</td>
</tr>
<tr>
<td>108.1</td>
<td>3074</td>
<td>0.0.0.0</td>
<td>2</td>
<td>7</td>
<td>2</td>
<td>0</td>
<td>12</td>
<td>4</td>
</tr>
<tr>
<td>198</td>
<td>3074</td>
<td>0.0.0.0</td>
<td>11</td>
<td>7</td>
<td>2</td>
<td>0</td>
<td>11</td>
<td>5</td>
</tr>
</tbody>
</table>
First Table Sampled Jan. 10
Day Peak on Feb. 12th, During Reported OVH Attack
# Top Attacked Ports

<table>
<thead>
<tr>
<th>Rank</th>
<th>Attacked Port</th>
<th>Fraction</th>
<th>Common UDP Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>80</td>
<td>0.362</td>
<td>None. via TCP:HTTP (g)</td>
</tr>
<tr>
<td>2</td>
<td>123</td>
<td>0.238</td>
<td>NTP server port</td>
</tr>
<tr>
<td>3</td>
<td>3074</td>
<td>0.079</td>
<td>XBox Live (g)</td>
</tr>
<tr>
<td>4</td>
<td>50557</td>
<td>0.062</td>
<td>Unknown</td>
</tr>
<tr>
<td>5</td>
<td>53</td>
<td>0.025</td>
<td>DNS; XBox Live (g)</td>
</tr>
<tr>
<td>6</td>
<td>25565</td>
<td>0.021</td>
<td>Minecraft (g)</td>
</tr>
<tr>
<td>7</td>
<td>19</td>
<td>0.012</td>
<td>chargen protocol</td>
</tr>
<tr>
<td>8</td>
<td>22</td>
<td>0.011</td>
<td>None. via TCP:SSH</td>
</tr>
<tr>
<td>9</td>
<td>5223</td>
<td>0.007</td>
<td>Playstation (g); other</td>
</tr>
<tr>
<td>10</td>
<td>27015</td>
<td>0.006</td>
<td>Steam/e.g. Half-Life (g)</td>
</tr>
<tr>
<td>11</td>
<td>43594</td>
<td>0.004</td>
<td>Runescape (g)</td>
</tr>
<tr>
<td>12</td>
<td>9987</td>
<td>0.004</td>
<td>TeamSpeak3 (g)</td>
</tr>
<tr>
<td>13</td>
<td>8080</td>
<td>0.004</td>
<td>None. via TCP:HTTP alt.</td>
</tr>
<tr>
<td>14</td>
<td>6005</td>
<td>0.003</td>
<td>Unknown</td>
</tr>
<tr>
<td>15</td>
<td>77777</td>
<td>0.003</td>
<td>Several games (g); other</td>
</tr>
<tr>
<td>16</td>
<td>2052</td>
<td>0.003</td>
<td>Star Wars (g)</td>
</tr>
<tr>
<td>17</td>
<td>1025</td>
<td>0.002</td>
<td>Win RPC; other</td>
</tr>
<tr>
<td>18</td>
<td>1026</td>
<td>0.002</td>
<td>Win RPC; other</td>
</tr>
<tr>
<td>19</td>
<td>88</td>
<td>0.002</td>
<td>XBox Live (g)</td>
</tr>
<tr>
<td>20</td>
<td>90</td>
<td>0.002</td>
<td>DNSIX (military)</td>
</tr>
</tbody>
</table>

10+ of Top-20 Ports are Gaming-related
# Mega Amplifiers in Monlist Table

<table>
<thead>
<tr>
<th>IP</th>
<th>...</th>
<th>Count</th>
<th>Inter-arrival</th>
</tr>
</thead>
<tbody>
<tr>
<td>ONP Scanner IP</td>
<td>...</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Other IP X</td>
<td>...</td>
<td>123456</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IP</th>
<th>...</th>
<th>Count</th>
<th>Inter-arrival</th>
</tr>
</thead>
<tbody>
<tr>
<td>ONP Scanner IP</td>
<td>...</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>Other IP X</td>
<td>...</td>
<td>123456</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IP</th>
<th>...</th>
<th>Count</th>
<th>Inter-arrival</th>
</tr>
</thead>
<tbody>
<tr>
<td>ONP Scanner IP</td>
<td>...</td>
<td>204242</td>
<td>0</td>
</tr>
<tr>
<td>Other IP X</td>
<td>...</td>
<td>123456</td>
<td>0</td>
</tr>
</tbody>
</table>
Mega Amplifiers Follow-Up

Not exactly hoisted by our own petard, but ...

Mega2: ~400Mbps for 6 hrs.

Mega1: 50Mbps for 7 days!

• Top twenty amplifiers in original 15-week study:

<table>
<thead>
<tr>
<th>Rank</th>
<th>Bytes Per Query</th>
<th>Country</th>
<th>Rank</th>
<th>Bytes Per Query</th>
<th>Country</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>45,449,582,522</td>
<td>JP</td>
<td>11</td>
<td>66,412,500</td>
<td>KR</td>
</tr>
<tr>
<td>2</td>
<td>28,278,811,947</td>
<td>JP</td>
<td>12</td>
<td>65,637,308</td>
<td>KR</td>
</tr>
<tr>
<td>3</td>
<td>15,071,819,517</td>
<td>JP</td>
<td>13</td>
<td>63,433,678</td>
<td>CN</td>
</tr>
<tr>
<td>4</td>
<td>9,925,296,893</td>
<td>JP</td>
<td>14</td>
<td>63,291,795</td>
<td>NL</td>
</tr>
<tr>
<td>5</td>
<td>1,970,253,817</td>
<td>JP</td>
<td>15</td>
<td>60,817,152</td>
<td>KR</td>
</tr>
<tr>
<td>6</td>
<td>376,813,551</td>
<td>JP</td>
<td>16</td>
<td>59,024,394</td>
<td>CN</td>
</tr>
<tr>
<td>7</td>
<td>360,527,290</td>
<td>JP</td>
<td>17</td>
<td>53,974,154</td>
<td>IN</td>
</tr>
<tr>
<td>8</td>
<td>82,340,368</td>
<td>KR</td>
<td>18</td>
<td>48,236,262</td>
<td>KR</td>
</tr>
<tr>
<td>10</td>
<td>69,745,016</td>
<td>KR</td>
<td>20</td>
<td>47,563,494</td>
<td>CN</td>
</tr>
</tbody>
</table>

• Asia prominently represented in top mega amps
• Contacted JP-CERT and others in Japan with most remediating; but no explanation of root cause
Local ISP Perspective: NTP Darknet and ISP Traffic at Merit

![Graph showing NTP egress volume and number of unique scanners over time]

- **Scanners**
  - Number of unique scanners

- **NTP egress volume (UDP sport=123)**
  - MBytes/sec

UTC time:
- 2013-12-01 to 2014-02-01
Local ISP Perspective:
NTP Traffic at CSU & FRGP

![Graph showing NTP traffic over time for CSU and FRGP, with distinct lines for UDP sport=123 and dport=123]
Summary

• NTP DDoS attacks had significant global impact
  – Top large DDoS vector in Q1 2014
  – 1.4 M monlist amplifiers measured at peak
• monlist table allowed studying global DDoS victims
  – 437 K measured unique victims; est. several PB of traffic
  – Gaming targets are large fraction
• “Mega amplifiers” an interesting rarity allowing devastating power
• Local perspective illuminates response to mitigation and some attacker clues
• Global mitigation of monlist swift, but threats remain
  – e.g., monlist unpatched long tail and other NTP commands
Thank You!

Questions?

Jake Czyz
University of Michigan
jczyz [at] umich
BACKUP SLIDES
NTP Traffic

700 Gbps of global NTP

1000x increase in 3 months

Daily Internet traffic sample averages 71.5 Tbps.
Amplifier Power

monlist Command

On-wire Bandwidth Amplification Factor
Amplifier Power
version Command

On-wire Bandwidth Amplification Factor

Sample Date

02-21 02-28 03-07 03-14 03-21 03-28 04-04 04-11 04-18

1 10 100 1K 10K 100K 1M 10M 100M 1G 10G
February Attacks

Day Peak on Feb. 12th: During Reported QVH Attack
Using monlist table to Study Attacks and Victims

(a) monlist Table A  Mostly Normal and Probe Clients

<table>
<thead>
<tr>
<th>Address</th>
<th>Src. Port</th>
<th>Count</th>
<th>Mode</th>
<th>Inter-arrival</th>
<th>Last Seen</th>
</tr>
</thead>
<tbody>
<tr>
<td>ONP-IP</td>
<td>57915</td>
<td>6</td>
<td>7</td>
<td>526929</td>
<td>0</td>
</tr>
<tr>
<td>client.a1</td>
<td>10151</td>
<td>19</td>
<td>6</td>
<td>154503</td>
<td>310</td>
</tr>
<tr>
<td>client.a2</td>
<td>123</td>
<td>3281</td>
<td>4</td>
<td>1024</td>
<td>345</td>
</tr>
<tr>
<td>client.a3</td>
<td>54660</td>
<td>2</td>
<td>7</td>
<td>823</td>
<td>20795</td>
</tr>
<tr>
<td>client.a4</td>
<td>36008</td>
<td>1</td>
<td>3</td>
<td>0</td>
<td>104063</td>
</tr>
</tbody>
</table>

(b) monlist Table B  Mostly Victim and Probe Clients

<table>
<thead>
<tr>
<th>Address</th>
<th>Src. Port</th>
<th>Count</th>
<th>Mode</th>
<th>Inter-arrival</th>
<th>Last Seen</th>
</tr>
</thead>
<tbody>
<tr>
<td>ONP-IP</td>
<td>47188</td>
<td>1</td>
<td>7</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>client-b1</td>
<td>59436</td>
<td>3358227026</td>
<td>7</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>client-b2</td>
<td>43395</td>
<td>25361312</td>
<td>7</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>client-b3</td>
<td>50231</td>
<td>158163232</td>
<td>7</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>client.b4</td>
<td>80</td>
<td>2189</td>
<td>7</td>
<td>0</td>
<td>2</td>
</tr>
</tbody>
</table>
Amplifiers Per Victim

Sample Date

1M 100K 10K 1K 100

Maximum  Mean
95th Pct.  Median

Amplifiers per Victim

01-10 01-17 01-24 01-31 02-07 02-14 02-21 02-28 03-07 03-14 03-21 03-28 04-04 04-11 04-18

Sample Date

IMC'14

NTP DDoS
Total Packets Victims Were Sent
Darknet Scanning

Month

- 2013-09
- 2013-10
- 2013-11
- 2013-12
- 2014-01
- 2014-02
- 2014-03
- 2014-04

Benign Packets (fraction above bar)

Other Packets

Monthly Average Packets Seen per Darknet /24 Block

- 0
- 2000
- 4000
- 6000
- 8000
- 10000
- 12000

27
Vast Majority Unique IPs **Non-Benign**

### IPs (Thousands)

- **2013-09**: 1
- **2013-10**: 1
- **2013-11**: 2
- **2013-12**: 37
- **2014-01**: 22
- **2014-02**: 57
- **2014-03**: 27
- **2014-04**: 44

**Month**

- **2013-09**
- **2013-10**
- **2013-11**
- **2013-12**
- **2014-01**
- **2014-02**
- **2014-03**
- **2014-04**

**All IPs (benign count above bar)**

**IMC'14**

**NTP DDoS**
Remediation / Mitigation

Follow-up confirms: monlist remediation
Flatlines between first 10 weeks 😊

- DNS Open Resolvers (at peak: 33.9M)
- NTP version Amplifiers (at peak: 4.9M)
- NTP monlist Amplifiers (at peak: 1.4M)
All Traffic at Merit Network

Traffic volume (Bps)

Traffic types:
- NTP
- DNS
- HTTP
- HTTPS
- OTHER

100x increase

UTC Time

01-25 01-27 01-29 01-31 02-02 02-04