Tracing Volumetric DDoS to its Booter / IPHM Origins

Craig Labovitz

NANOG June 2021
Background and Disclosures

- I work for a router vendor that provides anti-DDoS
- This NANOG presentation provides preliminary result (more to follow)
- This talk anonymizes specific vendors, peers and ISPs
  - Except when public information (i.e., many IPHM and Booters advertise)
  - We do not know motives (i.e., what is malice and what is ignorance)
  - We are discussing results with ISPs & hosting identified in study
- You can run these queries yourself
- You can (and should) filter / rate limit IPHM yourself
This Talk Summary

1. Most DDoS today is unsophisticated IPHM reflection or flood
2. Most IPHM originates in < 50 hosting companies and regional ISP
3. Aggregate IPHM DDoS rates doubled last year (this is bad)
4. We provide techniques to trace IPHM Amplification, TCP SA and Flood
5. We show router filters can block 95%+ of volumetric DDoS
6. We have recommendations for router vendors and ISPs
Background: Four Primary DDoS Attack Vectors

1. **Amplification** (send UDP with spoofed victim source IP to amplifier)
2. **TCP SA** (send spoofed victim TCP IP source to TCP servers like Akamai or Google)
3. **IPHM Flood** (spoof everything to victim destination IP)
4. **Botnet** (application request and sometimes TCP/UDP flood)

<table>
<thead>
<tr>
<th>TTL</th>
<th>Proto</th>
<th>Chksum</th>
</tr>
</thead>
<tbody>
<tr>
<td>SRC</td>
<td>VICTIM</td>
<td></td>
</tr>
<tr>
<td>DST</td>
<td>Amplifier</td>
<td></td>
</tr>
</tbody>
</table>

~40 Bytes

<table>
<thead>
<tr>
<th>TTL</th>
<th>Proto</th>
<th>Chksum</th>
</tr>
</thead>
<tbody>
<tr>
<td>SRC</td>
<td>Amplifier</td>
<td></td>
</tr>
<tr>
<td>DST</td>
<td>VICTIM</td>
<td></td>
</tr>
</tbody>
</table>

Amplifiers

Amplified Response or TCP SA

<table>
<thead>
<tr>
<th>TTL</th>
<th>Proto</th>
<th>Chksum</th>
</tr>
</thead>
<tbody>
<tr>
<td>SRC</td>
<td>Spoofed</td>
<td></td>
</tr>
<tr>
<td>DST</td>
<td>VICTIM</td>
<td></td>
</tr>
</tbody>
</table>

High spoofed source address cardinality

Fully spoofed packet
Background: DDoS Ecosystem

100+ commercial booter services offer range of competitive amplification, spoofed and botnet attacks. Sometimes booters also provide anti-DDoS solutions (in a presumed conflict of interest).

Gamers and extortion as well as gamblers, market manipulation, state sponsored attacks

1M+ home routers, IoT, windows servers and misconfigured DNS servers responding to UDP amplification requests or conscripted in botnet

50+ hosting companies sell high-speed IPHM (IP Header Modification) servers. Many explicitly market their IPHM and anti-DMCA capabilities as features. Often subset of bulletproof hosting
Background: DDoS Ecosystem Booters

Pricing varies but usually around $50 / month paid in BTC. More for longer duration and multiple concurrent attacks

Mostly UDP amplification and TCP SA with explicit focus on game DDoS. Botnet application DDoS typically require higher VIP package spend

Typical booter control panel helpfully offering range of source CIDR spoofing options

Most claim 20-30 servers, including VIP reserved instances
Background: DDoS Ecosystem Booters

HardStresser is one of the most powerful attack Stresser Service sites in 2021, instantly maintaining its position as leader of the 1500Gbit/s Stresser Attack Force

Some advertise up to 2 Tbps (though individual claims may not be reliable)
Background: DDoS Ecosystem IPHM
The business models appear to range from straightforward to more complex. IPHM leverage grey area legal jurisdictions, layered behind several layers of reseller hosting (including DDoS mitigation providers), or hide in IaaS / highly distributed hosting. Significant overlap with Bullet Proof market [21, 23]
The State of DDoS Today

The Problem

1. Number of amplifiers is growing (thanks IoT)
2. Number of botnets is growing quickly (thanks IoT and cloud)
3. DDoS pps / bps peaks is growing (because #1 and #2 and economic motives)
4. DDoS now mainly economic challenge (and less a technical issue)

Graph of 5-minute max daily Tbps amplified response DDoS across collaborating providers in study. Aggregate peak DDoS rates grew from 1.5 to 3 Tbps last year.

Note: Individual peaks may represent multiple simultaneous CIDR / ASN / ISP “attacks”
The State of DDoS Today
Approaches to solve DDoS Economics

1. Fix amplifiers and patch botnets (lost case)

2. Commercial booter take-downs (worthy effort, but not obviously effective)

3. Deploy specialized DDoS hardware (works, but cost and Moore’s law is an issue)

4. Use CDN / Cloud (significant win for many types of traffic)

5. Use community (BCP38, MANRS) to identify and stop IPHM at ISP edge

6. Use existing routers to block DDoS at ISP edge
**Step 1: Trace IPHM**

Trace IPHM using fingerprints and real-time IPFIX from across Internet

In a process similar to IETF DOTS [39], we use DDoS fingerprint hashes to trace amplified DDoS back to the IPHM hosting origins using [40]. While the victim in step (1) only sees amplifier IPs, we can identify the originating IPHM using fingerprint in step (3).
Step 1a: Trace IPHM Example (Amplifiers -> Customer X)

DDoS impacting an anonymized North American ISP customer (Customer X) coming from roughly 65K DNS amplifiers. We show the 10-second average Gbps inbound to customer. The drop in traffic reflects one or more upstream providers blackholing all traffic to the customer (i.e., “completing the attack”). In next slide, we use the attack fingerprint hash to trace the traffic upstream of the victim ISP and amplifiers.
Step 1b: Trace IPHM Example (IPHM -> Amplifiers)

We use a fingerprint hash of attack against “Customer X” to trace DDoS back across the Internet. At 100x amplification attack ranged between 1-2 Tbps downstream of amplifiers. We identify the point where forged source IP traffic (i.e., packets destined to the 65K amplifiers and spoofing the victim source IP) first enter our study sample. In 40–50% of the attacks, we identify a specific IPHM hosting provider. In the remainder of attacks, we identify the closest regional provider or specific transit provider. We use accounts on booter / IPHM and associated service fingerprints to further refine our identification of Booters / IPHM within regional ISPs and transit
Step 1c: Trace IPHM
Plot of packets per second of IPHM with closest identified origin

The same ~50 IPHM hosting companies or regional / national providers consistently generate the majority of IPHM observed both in real-word DDoS attacks as well as commercial booser fingerprints (50+ Mpps). Note that we cannot always attribute motive (i.e., malice versus inadvertent)
Step 2: Fingerprint Booters
Most booters have unique signatures

Some 100-active commercial booter services often sharing administration, code base and amplifier lists

How to Fingerprint Booters

1. Amplifier IP lists (particularly invalids)
2. Amplifier payload (e.g., DNS)
3. ICMP / TCP monitoring during attacks
4. Spoofed IP header choices (TTL, options, etc.)
5. Amplifier honeypots (rate limited!)
6. IPHM hosting or botnet IPs
Step 3: Detect IPHM
Using IPFIX port pairs, TTL, address distribution and routed topology

1. Most IPHM uses improbable port combinations
   • Look for unusual port combinations (especially game -> amplifier)
   • e.g. port.src(3074,80,443,8888) port.dst(11211,123,19,53,1900,389)

2. Most IPHM uses improbable IP header fields
   • Normal TTLs fall within narrow on peering routers (see upcoming slide)
   • Similarly sequence numbers, window, options, etc.
Step 3: Detect IPHM via Improbable TTL

Sample graph of TTL observed in normal and DDoS traffic

Most IPHM includes improbable and readily distinguished TTL as observed in thousands of real-world DDoS attacks and fingerprint traces collected from the top fifty commercial booters.

Normal TTL Distribution Large NA Consumer Provider

IPHM DDoS (CLDAP) at Global Transit -> Amplifiers
Step 3: Detect IPHM via Improbable CIDRs and Topology
Using IPFIX port pairs, TTL, address distribution and routed topology

3. Most fully IPHM chooses improbable src CIDRs
   • Unused *(well, formerly)* address space (DoD)
   • Improbable distribution within CIDR blocks *(next slide)*
   • Improbable topologies
     • e.g., DIA hosting interfaces sourced with EU consumer providers
     • e.g., global transit 1 -> global transit 2

4. Combinations of all above provides high IPHM classification confidence
Step 3: Detect IPHM via Improbable CIDRs and Topology

IPHM TCP Syn Flood as seen via 1/2000 IPFIX

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Rate (Mb)</th>
<th>Protocol</th>
<th>Suffix</th>
<th>Start Time</th>
<th>End Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>100.0.31.228</td>
<td>0.08</td>
<td>tcp</td>
<td>S</td>
<td>50749</td>
<td>30120</td>
</tr>
<tr>
<td>100.12.155.240</td>
<td>0.08</td>
<td>tcp</td>
<td>S</td>
<td>6477</td>
<td>30120</td>
</tr>
<tr>
<td>100.128.194.76</td>
<td>0.08</td>
<td>tcp</td>
<td>S</td>
<td>48111</td>
<td>30120</td>
</tr>
<tr>
<td>100.128.203.74</td>
<td>0.08</td>
<td>tcp</td>
<td>S</td>
<td>38973</td>
<td>30120</td>
</tr>
<tr>
<td>100.128.252.219</td>
<td>0.08</td>
<td>tcp</td>
<td>S</td>
<td>62079</td>
<td>30120</td>
</tr>
<tr>
<td>100.128.40.33</td>
<td>0.08</td>
<td>tcp</td>
<td>S</td>
<td>12136</td>
<td>30120</td>
</tr>
<tr>
<td>100.128.98.94</td>
<td>0.08</td>
<td>tcp</td>
<td>S</td>
<td>4758</td>
<td>30120</td>
</tr>
<tr>
<td>100.131.56.255</td>
<td>0.08</td>
<td>tcp</td>
<td>S</td>
<td>32330</td>
<td>30120</td>
</tr>
<tr>
<td>100.132.144.157</td>
<td>0.08</td>
<td>tcp</td>
<td>S</td>
<td>9170</td>
<td>30120</td>
</tr>
<tr>
<td>100.133.156.104</td>
<td>0.08</td>
<td>tcp</td>
<td>S</td>
<td>6801</td>
<td>30120</td>
</tr>
<tr>
<td>100.134.17.137</td>
<td>0.08</td>
<td>tcp</td>
<td>S</td>
<td>49272</td>
<td>30120</td>
</tr>
<tr>
<td>100.134.85.144</td>
<td>0.08</td>
<td>tcp</td>
<td>S</td>
<td>47309</td>
<td>30120</td>
</tr>
<tr>
<td>100.135.189.56</td>
<td>0.08</td>
<td>tcp</td>
<td>S</td>
<td>24976</td>
<td>30120</td>
</tr>
<tr>
<td>100.136.80.160</td>
<td>0.08</td>
<td>tcp</td>
<td>S</td>
<td>61741</td>
<td>30120</td>
</tr>
<tr>
<td>100.137.183.182</td>
<td>0.08</td>
<td>tcp</td>
<td>S</td>
<td>13215</td>
<td>30120</td>
</tr>
<tr>
<td>100.138.184.231</td>
<td>0.08</td>
<td>tcp</td>
<td>S</td>
<td>12638</td>
<td>30120</td>
</tr>
<tr>
<td>100.139.232.128</td>
<td>0.08</td>
<td>tcp</td>
<td>S</td>
<td>44457</td>
<td>30120</td>
</tr>
<tr>
<td>100.140.98.42</td>
<td>0.08</td>
<td>tcp</td>
<td>S</td>
<td>48676</td>
<td>30120</td>
</tr>
<tr>
<td>100.141.160.53</td>
<td>0.08</td>
<td>tcp</td>
<td>S</td>
<td>44899</td>
<td>30120</td>
</tr>
<tr>
<td>100.141.210.109</td>
<td>0.08</td>
<td>tcp</td>
<td>S</td>
<td>43336</td>
<td>30120</td>
</tr>
<tr>
<td>100.142.146.161</td>
<td>0.08</td>
<td>tcp</td>
<td>S</td>
<td>38634</td>
<td>30120</td>
</tr>
<tr>
<td>100.142.187.98</td>
<td>0.08</td>
<td>tcp</td>
<td>S</td>
<td>41407</td>
<td>30120</td>
</tr>
<tr>
<td>100.142.255.164</td>
<td>0.08</td>
<td>tcp</td>
<td>S</td>
<td>15533</td>
<td>30120</td>
</tr>
<tr>
<td>100.143.208.71</td>
<td>0.08</td>
<td>tcp</td>
<td>S</td>
<td>44429</td>
<td>30120</td>
</tr>
</tbody>
</table>

Usually randomized or sequential from every IP in a block (e.g., TMobile)
Step 4: Solve some mysteries
IPHM potential significantly larger than observed DDoS

1. Nokia amplifier IP list different from most IPHM lists
2. IPHM capacity is 5x size of largest reported DDoS attacks

Why?
Step 4: Solve some mysteries
IPHM potential significantly larger than observed DDoS

1. Limits in amplification availability (i.e., only ~400k memcache)
2. Amplifier frag, port + packet-length policing (and uRPF)
3. Booters are unreliable and attacks diffuse
4. Significant IPHM inefficiencies (bad amplifier lists and payload)
Step 4: Solve some mysteries
Most commercial Booters underperforming by 50% or more

Example of out-of-date amplifier list as seen at a victim with 50% of the IPHM using non-existent amplifiers (resulting in ICMP unreachable) or non-optimal payloads:

IP 191.129.185.195 > XX.XX.198.50: ICMP 191.129.185.195 udp port 123 unreachable, length 44
IP 191.10.179.50 > XX.XX.198.50: ICMP 191.10.179.50 udp port 123 unreachable, length 44
IP 187.82.75.141 > XX.XX.198.50: ICMP 187.82.75.141 udp port 123 unreachable, length 44
IP 191.201.234.37 > XX.XX.198.50: ICMP 191.201.234.37 udp port 123 unreachable, length 44
IP 77.208.242.209 > XX.XX.198.50: ICMP 77.208.242.209 udp port 123 unreachable, length 44
IP 82.96.41.146 > XX.XX.198.50: ICMP 82.96.41.146 udp port 123 unreachable, length 44
IP 177.161.13.224 > XX.XX.198.50: ICMP 177.161.13.224 udp port 123 unreachable, length 44
IP 152.245.150.194 > XX.XX.198.50: ICMP 152.245.150.194 udp port 123 unreachable, length 44
IP 191.208.70.45 > XX.XX.198.50: ICMP 191.208.70.45 udp port 123 unreachable, length 44
IP 179.168.159.139 > XX.XX.198.50: ICMP 179.168.159.139 udp port 123 unreachable, length 44
IP 177.116.32.121 > XX.XX.198.50: ICMP 177.116.32.121 udp port 123 unreachable, length 44
IP 191.16.102.98 > XX.XX.198.50: ICMP 191.16.102.98 udp port 123 unreachable, length 44
IP 179.149.227.81 > XX.XX.198.50: ICMP 179.149.227.81 udp port 123 unreachable, length 44
IP 177.123.15.188 > XX.XX.198.50: ICMP 177.123.15.188 udp port 123 unreachable, length 44
IP 179.147.19.2 > XX.XX.198.50: ICMP 179.147.19.2 udp port 123 unreachable, length 44
IP 191.196.208.76 > XX.XX.198.50: ICMP 191.196.208.76 udp port 123 unreachable, length 44
IP 179.112.92.39 > XX.XX.198.50: ICMP 179.112.92.39 udp port 123 unreachable, length 36
IP 177.175.253.214 > XX.XX.198.50: ICMP 177.175.253.214 udp port 123 unreachable, length 36
IP 179.247.60.13 > XX.XX.198.50: ICMP 179.247.60.13 udp port 123 unreachable, length 44
IP 177.117.250.170 > XX.XX.198.50: ICMP 177.117.250.170 udp port 123 unreachable, length 44
IP 177.160.136.57 > XX.XX.198.50: ICMP 177.160.136.57 udp port 123 unreachable, length 44
Step 5: Stop DDoS using routers

Previous decade

- Routers had limited telemetry (SNMP, IPFIX)
- Routers had limited filter capacity (especially line speed)
- Routers had limited configuration (SNMP, SSH, Rancid)
- Providers had limited trust (e.g., the great FlowSpec winter)
- Net-Sec needed their own hardware

Today

- Routers with copious telemetry from all major vendors (IPFIX, gRPC)
- Significant increases in line-speed filter capacity
- All major vendors supporting FlowSpec and NetConf
- More trust, but safety using routers anti-ddos filters is still key issue
- Net-Sec still wants their own hardware, but management demands sharing
Step 5: Stop DDoS using routers

• Vendor & FlowSpec versus NetConf differences

• But generally possible on most routers
  • Block 100% amplified DDoS via port/pkt-length
  • Block 98% TCP SA using 2K filter entries
  • Block 98% IPHM flood using 2k filter entries
  • Block 95% botnet using 2k filter entries

• Key challenges:
  • Upstream capacity
  • Line-speed number of filters (number of simultaneous mitigations)
  • Safety (including line speed impact and organizational issues)
  • Latency / feedback loop with compute (i.e., de-couple scrubber)
Step 6: Ask for help
Lower cost of defense and increase cost of launching IPHM DDoS

- As a community, we can and should do more to limit IPHM
  - Easy to run IPHM (e.g., IPFIX TTL, port combination, CIDR queries)
  - Share these queries with your peers
  - Deploy basic filters (BCP38, MANRS, amplification policers)
- A little more technology would go a long way
  - Carrier: gRPC / IPFIX / NetConf / FlowSpec adoption
  - Vendor: Low latency packet header sampling (IPFIX without the cache)
  - Vendor: Low latency filter CRUD operations
  - IETF: FlowSpec TTL, filter ordering, prefix list, payload match, mirroring, and grouped counters
Questions

craig.labovitz@nokia.com
Reference: DDoS Attack Trends

More than twenty years of academic, vendor and press reports on trends in DDoS attack frequency, victims and attack vectors. Our findings match recent work and show DDoS (particularly amplification and reflection) attacks are growing in frequency and volume

Reference: Booters


Reference: IPHM / Bulletproof Hosting / Cloud Misuse

Significant number of reports on the prevalence of spoofing. In an extension of earlier work (e.g. [14, 15, 16]), Nokia used IPFIX telemetry, BGP topology and a broad cross section of synthetic IPHM and Booter account traces to identify closest origins of spoofed DDoS amplifier and TCP SA destined traffic. We believe Nokia research is one of the first efforts to experimentally fingerprint and identify the the largest contributors of IPHM used in DDoS attacks across the Internet today.

Reference: IPHM / Bulletproof Hosting / Cloud Misuse

Multiple research efforts have explored experimental measurements of the scale and multiplication factor of different amplification DDoS attack vectors. Nokia’s contribution is using observed IPHM pps rates and large-scale crawling / discovery of Internet amplifiers to estimate latent / potential attack threat posed by Booters and IPHM.

Reference: Mitigating DDoS on Routers

Multiple vendors offer a range of on-premise and cloud-based DDoS mitigation products and service. This work describes Nokia’s use of commodity compute servers and high-speed routers to de-compose the functions of traditional hardware DDoS scrubbers. The Nokia DDoS solution uses gPRC and Flowspec / Netconf for coordination between routers and the managing server cluster. Observations in [37] provide framework for granular protective filters based on Internet and enterprise network architectures. We show our decomposed scrubber approach can mitigate 95%+ of volumetric DDoS attack traffic on peering routers for all attacks observed during our study.