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

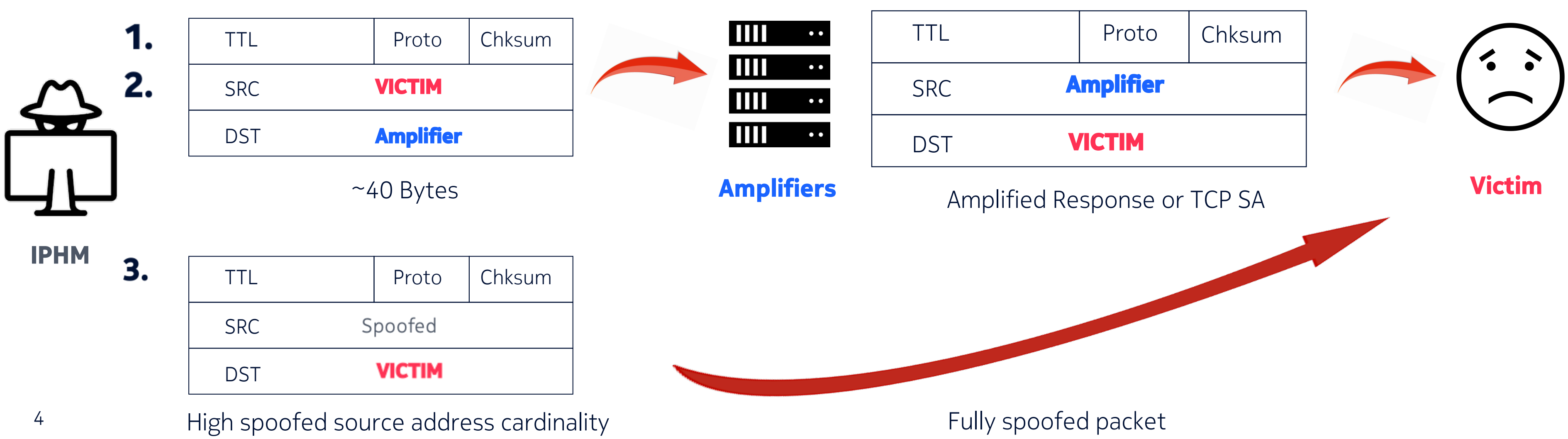
This Talk Summary

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

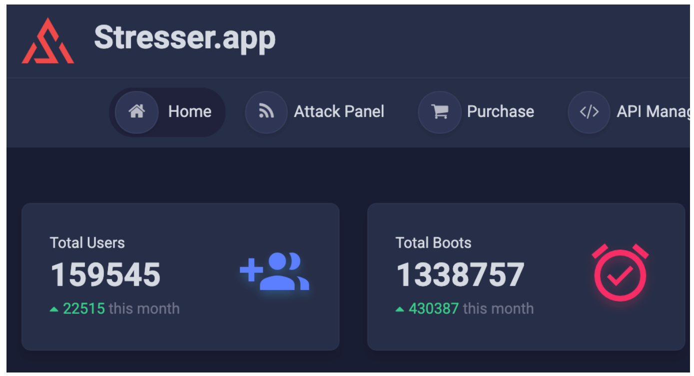
Focus of Talk

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)

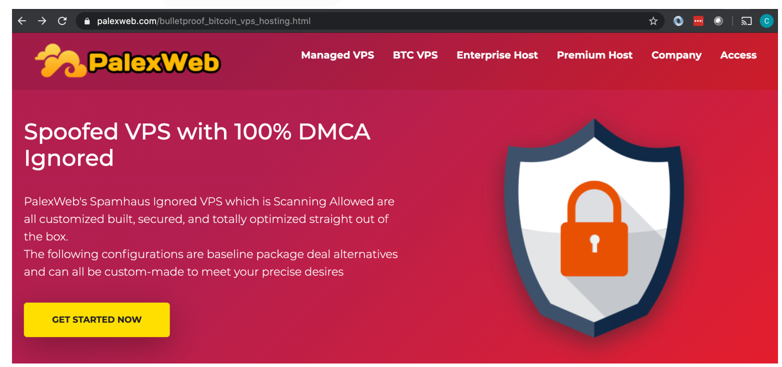


Background: DDoS Ecosystem

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



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)



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

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

1-3 Tbps DDoS

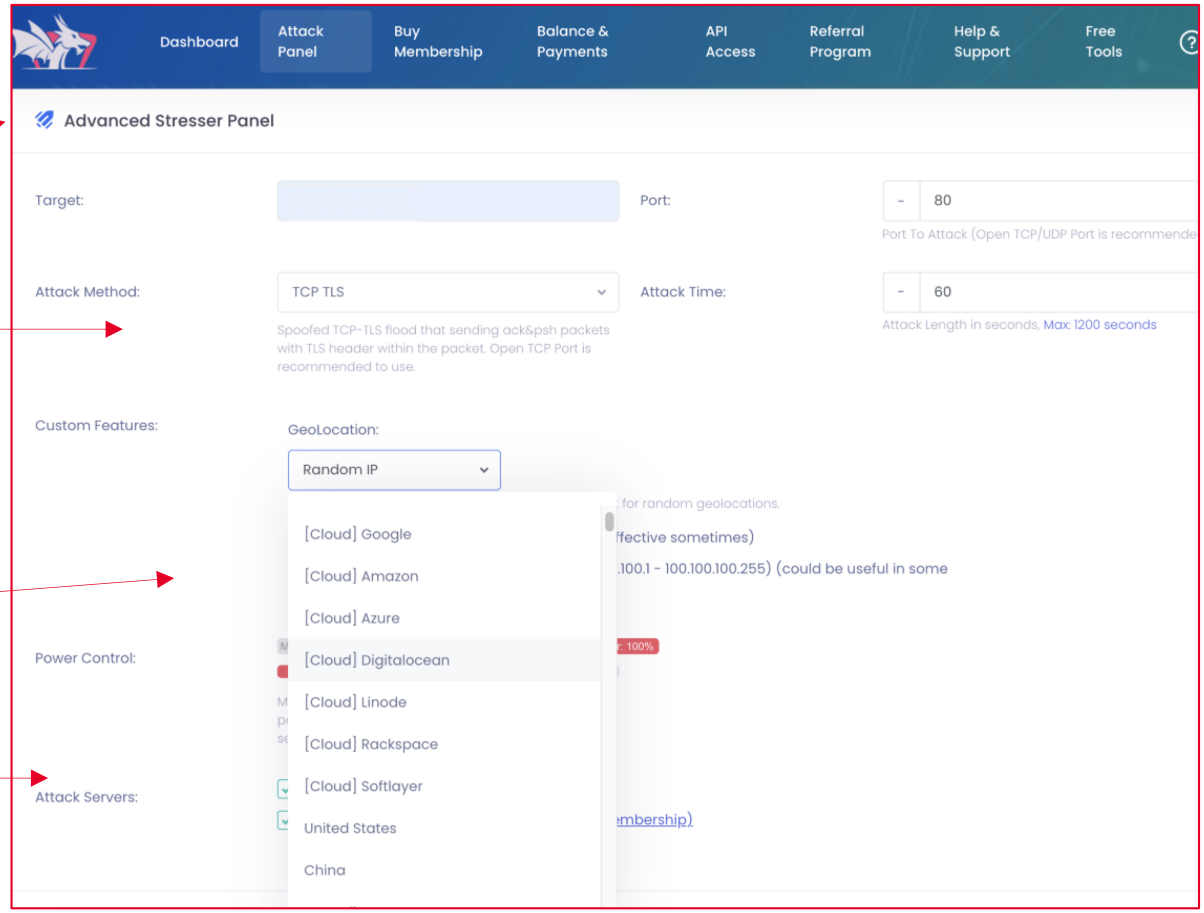
Background: DDoS Ecosystem Booters

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

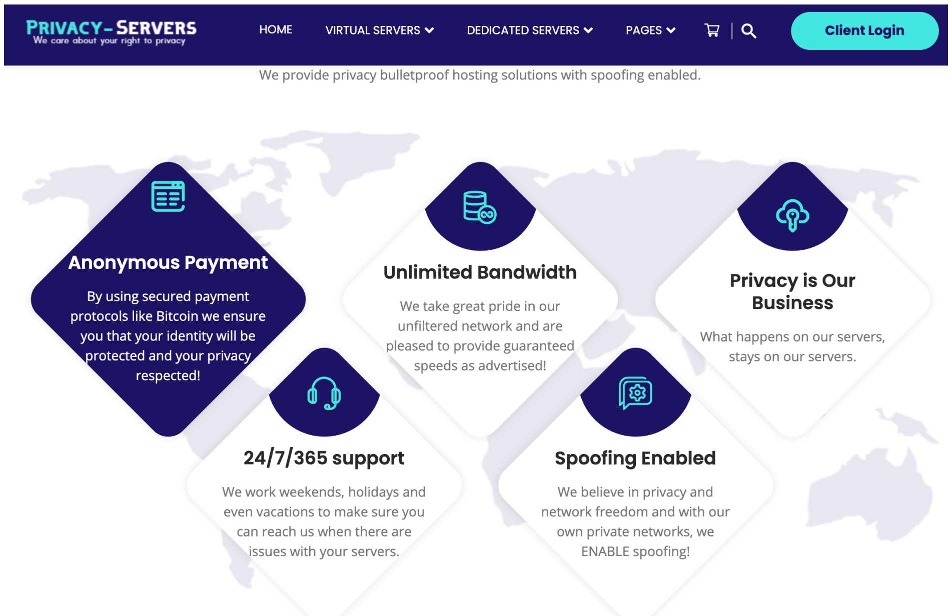


Background: DDoS Ecosystem Booters

Some advertise up to 2 Tbps (though individual claims may not be reliable)

Background: DDoS Ecosystem IPHM

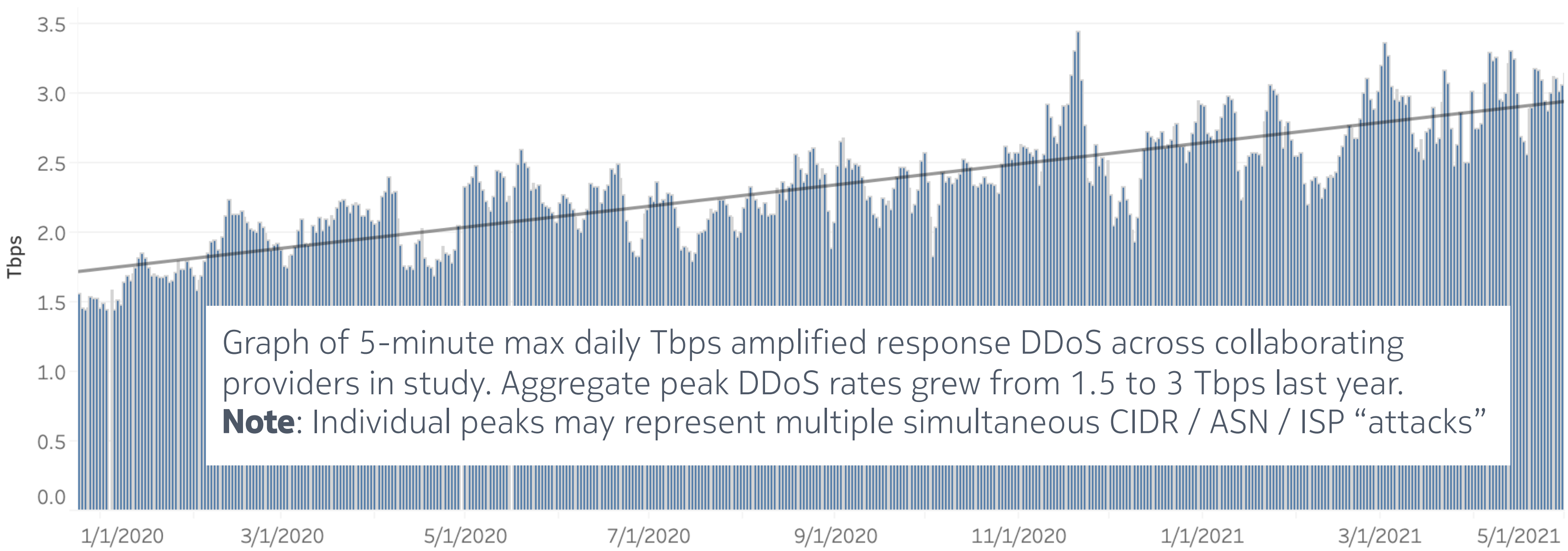
The business models appear to range from straightforward to more complex



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 <u>economic</u> 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

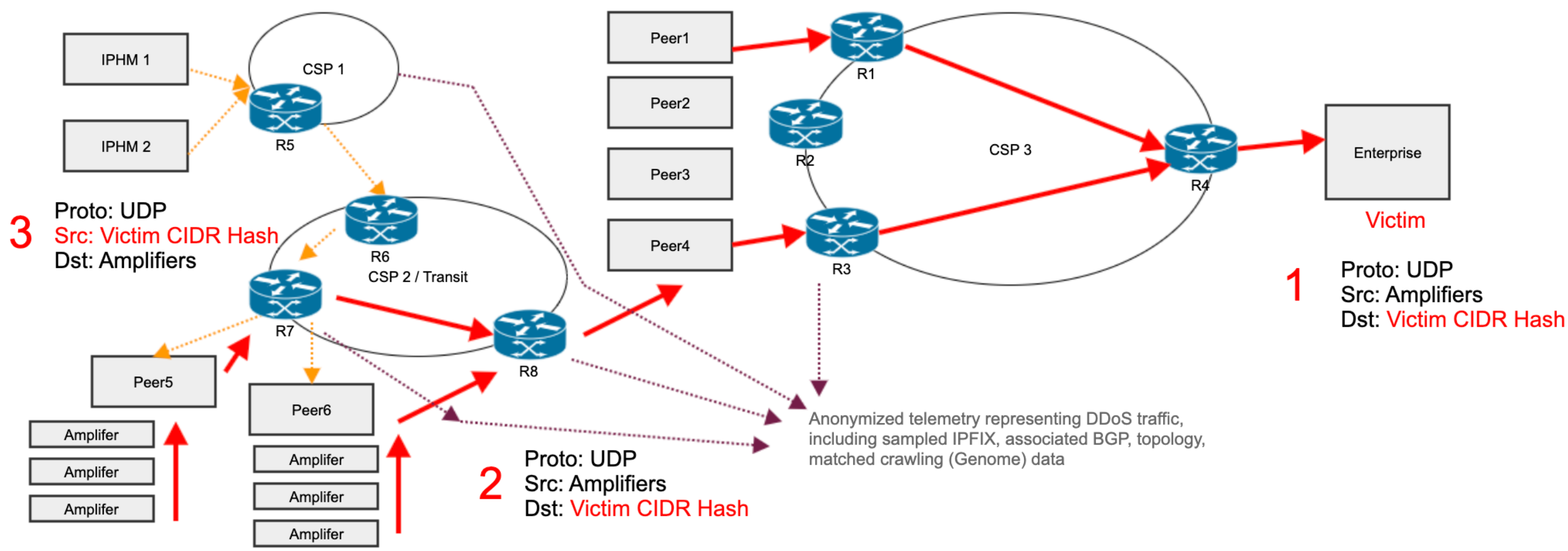
Less Tractable

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

More Tractable

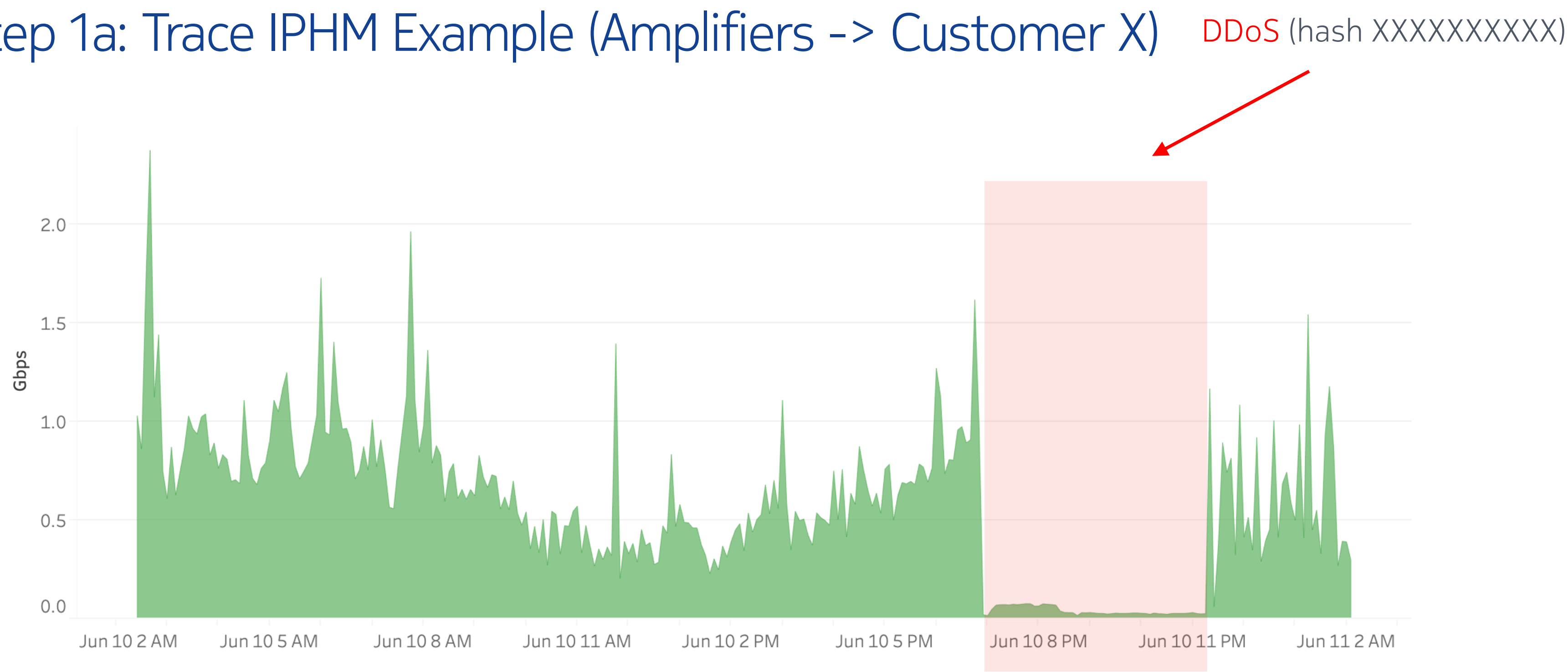
Step 1: Trace IPHM

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



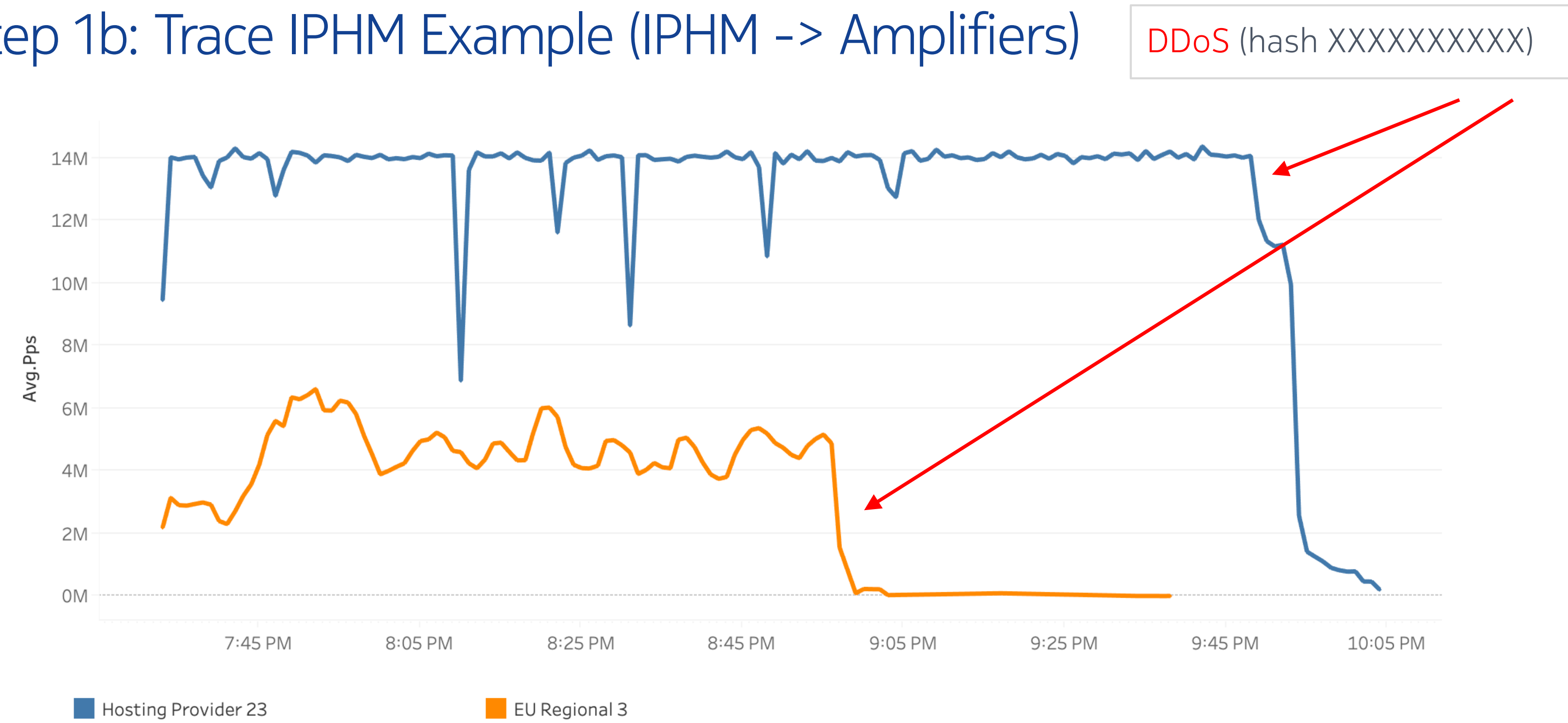
In a process similar to IETF DOTS [39], we use DDoS fingerprint hashes to trace amplified DDoS back to the IPHM hosting origins using [40]. While the victim in step (1) only sees amplifier IPs, we can identify the originating IPHM using fingerprint in step (3)

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

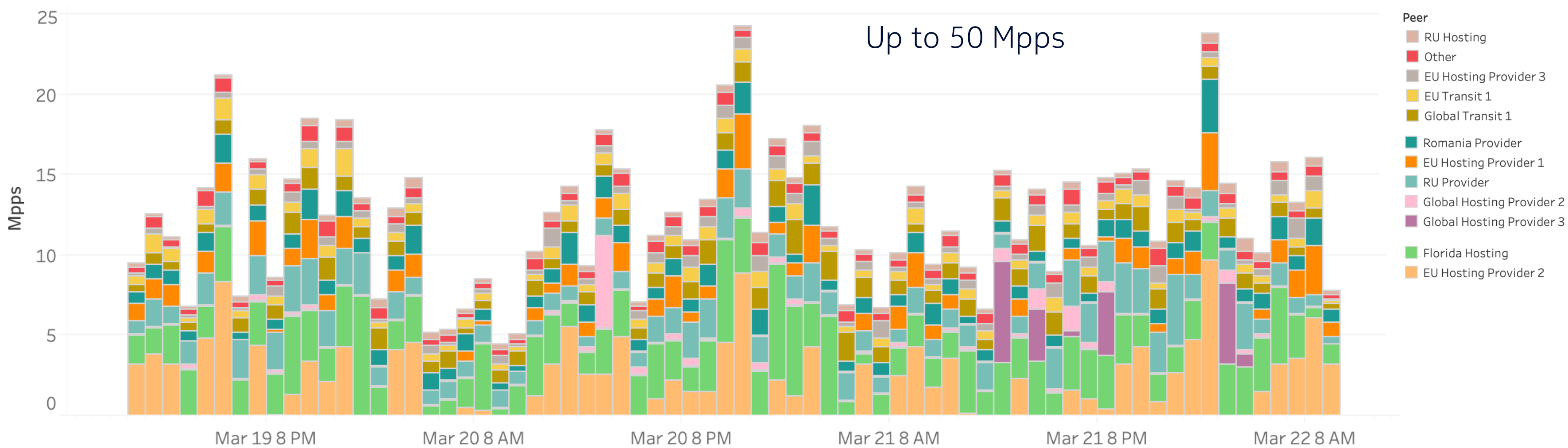
Step 1b: Trace IPHM Example (IPHM -> Amplifiers)



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 booter fingerprints (50+ Mpps). Note that we cannot always attribute motive (i.e., malice versus inadvertent)

Step 2: Fingerprint Booters

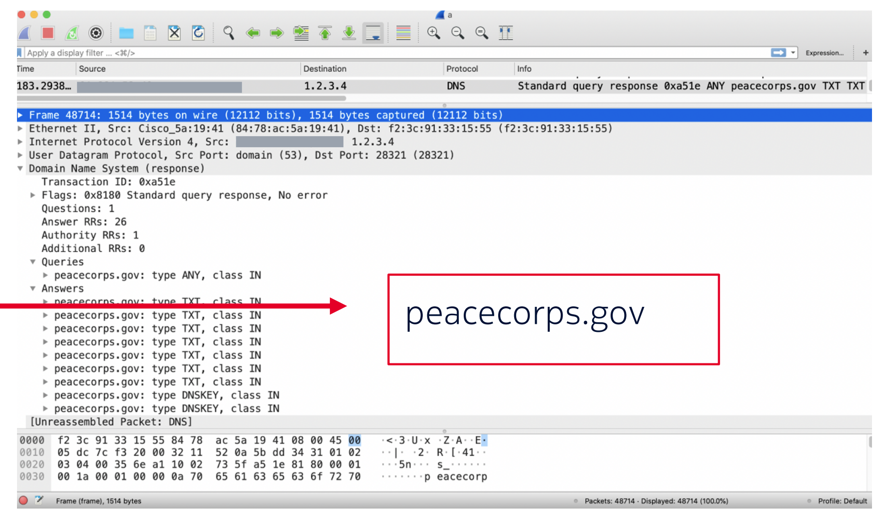
Most booters have unique signatures

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

Stresser.app
AstroStress
Atom Stresser
NightmareStresser
Str3ssed Booter
CyberVM
HardStresser

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



Sample DNS amplification PCAP from former SynStresser booter

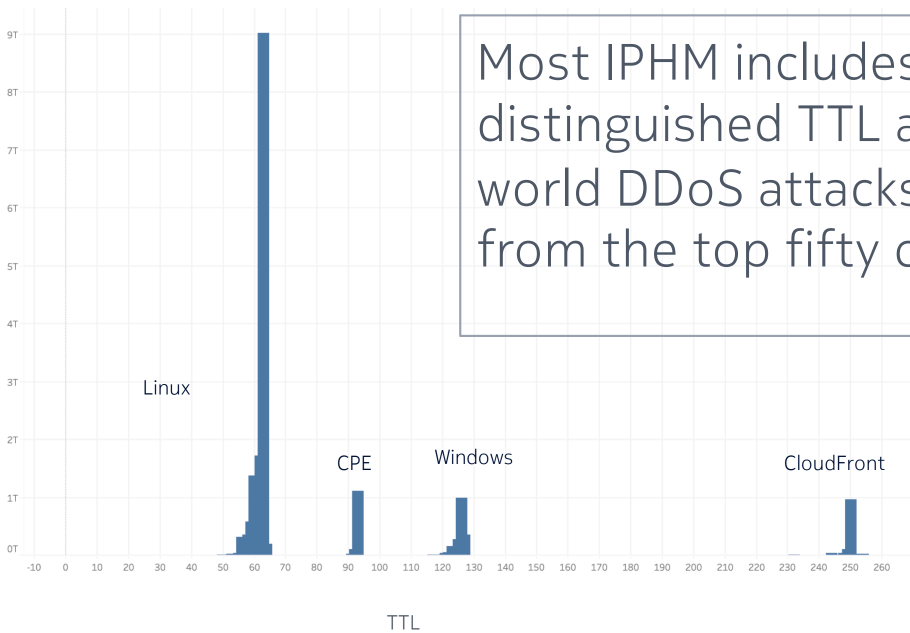
Step 3: Detect IPHM
Using IPFIX port pairs, TTL, address distribution and routed topology

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.

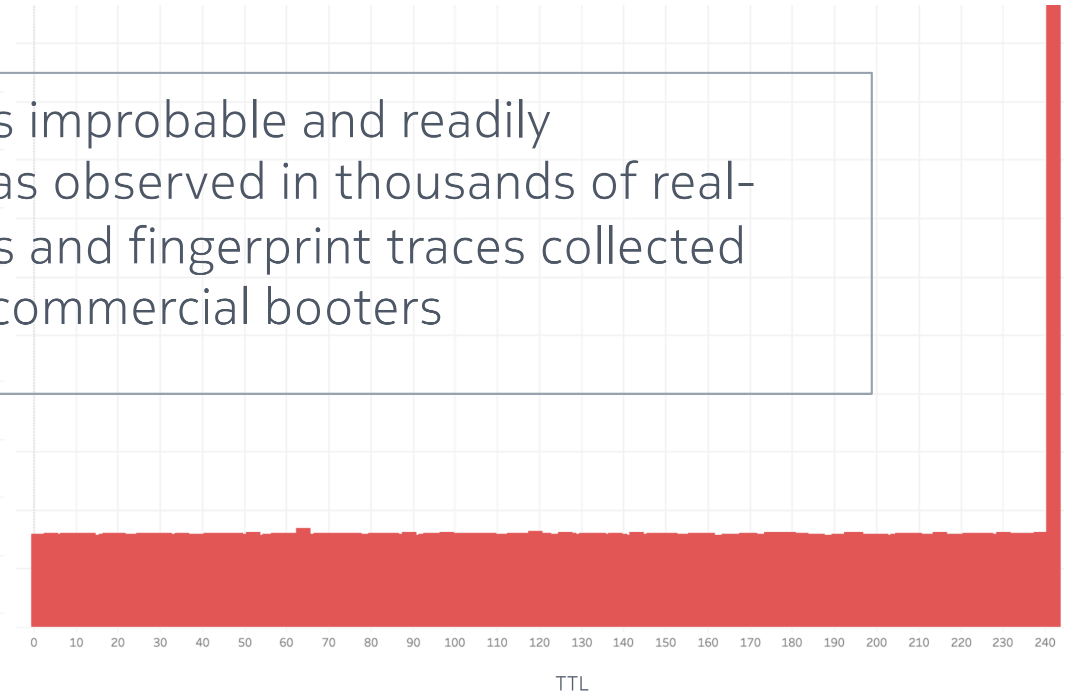
Step 3: Detect IPHM via Improbable TTL

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

```
<-  100.0.31.228        0.08 Mb    S   tcp   50749  30120
<-  100.12.155.240      0.08 Mb    S   tcp    6477  30120
<-  100.128.194.76      0.08 Mb    S   tcp   48111  30120
<-  100.128.203.74      0.08 Mb    S   tcp   38973  30120
<-  100.128.252.219     0.08 Mb    S   tcp   62079  30120
<-  100.128.40.33       0.08 Mb    S   tcp   12136  30120
<-  100.128.98.94       0.08 Mb    S   tcp    4758  30120
<-  100.131.56.255      0.08 Mb    S   tcp   32330  30120
<-  100.132.144.157     0.08 Mb    S   tcp    9170  30120
<-  100.133.156.104     0.08 Mb    S   tcp    6801  30120
<-  100.134.17.137      0.08 Mb    S   tcp   49272  30120
<-  100.134.85.144      0.08 Mb    S   tcp   47309  30120
<-  100.135.189.56      0.08 Mb    S   tcp   24976  30120
<-  100.136.80.160      0.08 Mb    S   tcp   61741  30120
<-  100.137.183.182     0.08 Mb    S   tcp   13215  30120
<-  100.138.184.231     0.08 Mb    S   tcp   12638  30120
<-  100.139.232.128     0.08 Mb    S   tcp   44457  30120
<-  100.140.98.42       0.08 Mb    S   tcp   48676  30120
<-  100.141.160.53      0.08 Mb    S   tcp   44899  30120
<-  100.141.210.109     0.08 Mb    S   tcp   43336  30120
<-  100.142.146.161     0.08 Mb    S   tcp   38634  30120
<-  100.142.187.98      0.08 Mb    S   tcp   41407  30120
<-  100.142.255.164     0.08 Mb    S   tcp   15533  30120
<-  100.143.208.71      0.08 Mb    S   tcp   44429  30120
```

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

```
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 187.116.193.168 > XX.XX.198.50: ICMP 187.116.193.168 udp port 123 unreachable, length 36
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
```

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

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

1. "Famous DDoS attacks: The largest DDoS attacks of all time", CloudFlare Learning Center. https://www.cloudflare.com/learning/ddos/famous-ddos-attacks
2. T. Emmons, "Volumetric DDOS Attacks Rising Fast", Akamai Blog. March 29, 2021. https://blogs.akamai.com/2021/03/in-our-2020-ddos-retrospective
3. C. Labovitz, "Bots, DDoS and Ground Truth", NANOG 50. https://archive.nanog.org/meetings/nanog50/presentations/Tuesday/NANOG50.Talk58.groundtruth.pdf
4. NetScout Worldwide Infrastructure Security Report. April 2021. https://www.netscout.com/threatreport

Reference: Booters

5. J. Cardoso de Santanna, "DDoS-as-a-Service: Investigating Booter Websites". PhD Thesis, University of Twente, Enschede 2017. https://doi.org/10.3990/1.9789036544290
6. Anonymous, "Top Booter / Top Stresser List. Web site: https://ddosforhire.net
7. B. Collier et al., "Booting the Booters: Evaluating the Effects of Police Interventions in the Market for Denial-of-Service Attacks". IMC, October 2019, Amsterdam, Netherlands. https://doi.org/10.1145/3355369.3355592
8. B. Krebs, "Bomb Threat, DDoS Purveyor Gets Eight Years". KrebsOnSecurity Blog, December 1, 2020. https://krebsonsecurity.com/category/ddos-for-hire
9. D. Kopp et al., "DDoS Hide & Seek: On the Effectiveness of a Booter Services Takedown. IMC 2019. https://doi.org/10.1145/3355369.3355590
10. R. Musotto et al., "More Amazon than Mafia: analysing a DDoS stresser service as organised cybercrime". Trends Organized Crime (2020). https://doi.org/10.1007/s12117-020-09397-5
11. United States v. Sergiy P. Usatyuk. February 2019. https://www.justice.gov/usao-ednc/united-states-v-sergiy-usatyuk

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

12. M. Majkowski, “The real cause of large DDoS - IP Spoofing”. CloudFlare Blog, June 2018. https://blog.cloudflare.com/the-root-cause-of-large-ddos-ip-spoofing/
13. CAIDA Spoofer Project, https://www.caida.org/projects/spoofer
14. R. Beverly, S. Bauer, “The Spoofer Project: Inferring the Extent of Source Address Filtering on the Internet”, SRUTI 2005. Cambridge, MA, July 2005. http://www.cmand.org/papers/spoofer-sruti05.pdf
15. H. Wang, C. Jin, K. Shin, “Defense against spoofed IP traffic using hop-count filtering”, IEEE/ACM Transaction on Networking, 2007 https://dl.acm.org/doi/10.1109/TNET.2006.890133
16. I. Mopari et al., “Detection of DDoS attack and defense against IP spoofing”. ICAC3 2009, https://doi.org/10.1145/1523103.1523200
17. F. Lichtblau et al., “Detection, classification, and analysis of inter-domain traffic with spoofed source IP addresses”. IMC 2017. https://doi.org/10.1145/3131365.3131367
18. O. Fonseca et al., “Tracking Down Sources of Spoofed IP Packets”. CoNEXT 2019. https://doi.org/10.1145/3360468.3368175
19. N. Vlajic et al., “IP Spoofing In and Out of the Public Cloud: From Policy to Practice”. Computers 2019. https://doi.org/10.3390/computers8040081

Reference: IPHM / Bulletproof Hosting / Cloud Misuse

20. Anonymous, “Spoofed Hosting Providers”. https://s1ck.pw/spoofed.php
21. Intel471 Blog, “Here’s who is powering the bulletproof hosting market”. May 20201. https://www.intel471.com
22. Hacker Forums, “IPHM Hosts”. May 2021. https://hackforums.net
23. A. Noroozian, et al., “Platforms in everything: analyzing ground-truth data on the anatomy and economics of bullet-proof hosting”. SEC 2019. https://www.usenix.org/system/files/sec19-noroozian.pdf
24. Anonymous, “How To Host Questionable Websites”. https://weboas.is/media/host.pdf
25. Spamhaus Drop List. June 2021. https://www.spamhaus.org/drop
26. R. Tandon et al., "Quantifying Cloud Misbehavior”. CloudNet 2020. https://steel.isi.edu/Projects/Cloud_Misbehavior/

Reference: Measuring Amplifiers and IoT

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

27. S. Moon, et al., "Accurately Measuring Global Risk of Amplification Attacks using AmpMap", USENIX Security, 2021. https://www.usenix.org/conference/usenixsecurity21/presentation/moon
28. A. Lavrenovs, "Towards Measuring Global DDoS Attack Capacity". CyCon 2019. https://ieeexplore.ieee.org/abstract/document/8756851
29. D. Kopp et al., "DDoS Never Dies? An IXP Perspective on DDoS Amplification Attacks". PAM 2021. https://arxiv.org/pdf/2103.04443.pdf
30. H. Guo and J. Heidemann, "Detecting IoT Devices in the Internet". IEEE/ACM Trans. Networking. October, 2020. https://doi.org/10.1109/TNET.2020.3009425
31. C. Labovitz et al., "System and method for management of cloud-based systems". US Patent 20160043956A1
32. J. Czyz et al., "Taming the 800 Pound Gorilla: The Rise and Decline of NTP DDoS Attacks". IMC 2014. https://doi.org/10.1145/2663716.2663717

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.

33. P. Ferguson ad D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing". IETF RFC2827 / BCP38, MAY 2000. https://tools.ietf.org/html/bcp38
34. N. Hinze, et al., "On the Potential of BGP Flowspec for DDoS Mitigation at Two Sources: ISP and IXP". SIGCOMM 2018 https://doi.org/10.1145/3234200.3234209
35. Ralf Weber, "Better than Best Practices for DNS Amplification Attacks". NANOG https://archive.nanog.org/sites/default/files/mon_general_weber_defeat_23.pdf
36. D. Gassen et al., "BGP Flow Specification Deployment Experience". NANOG 38. https://archive.nanog.org/meetings/nanog38/presentations/labovitz-bgp-flowspec.pdf
37. C. Labovitz et al., "Internet inter-domain traffic". SIGCOMM 20201. https://doi.org/10.1145/1851182.1851194
38. C. Dietzel et al., "Stellar: network attack mitigation using advanced blackholing" CoNEXT 2018. https://doi.org/10.1145/3281411.3281413
39. A. Mortensen et al, "DDoS Open Threat Signaling (DOTS) Requirements". IETF RFC 8612.May 2019. https://www.rfc-editor.org/rfc/rfc8612.html
40. Nokia Defender. Commercial software home page. June 2021. https://www.nokia.com/networks/products/deepfield-defender/