



The Problem with North American Botnets

Craig Labovitz
June 2022

Conventional Wisdom

1. DDoS is growing
2. Most DDoS is due to amplification
3. Most DDoS in North America comes from Asia / EU
4. FlowSpec is good for amplification but not other types of DDoS

Conventional Wisdom

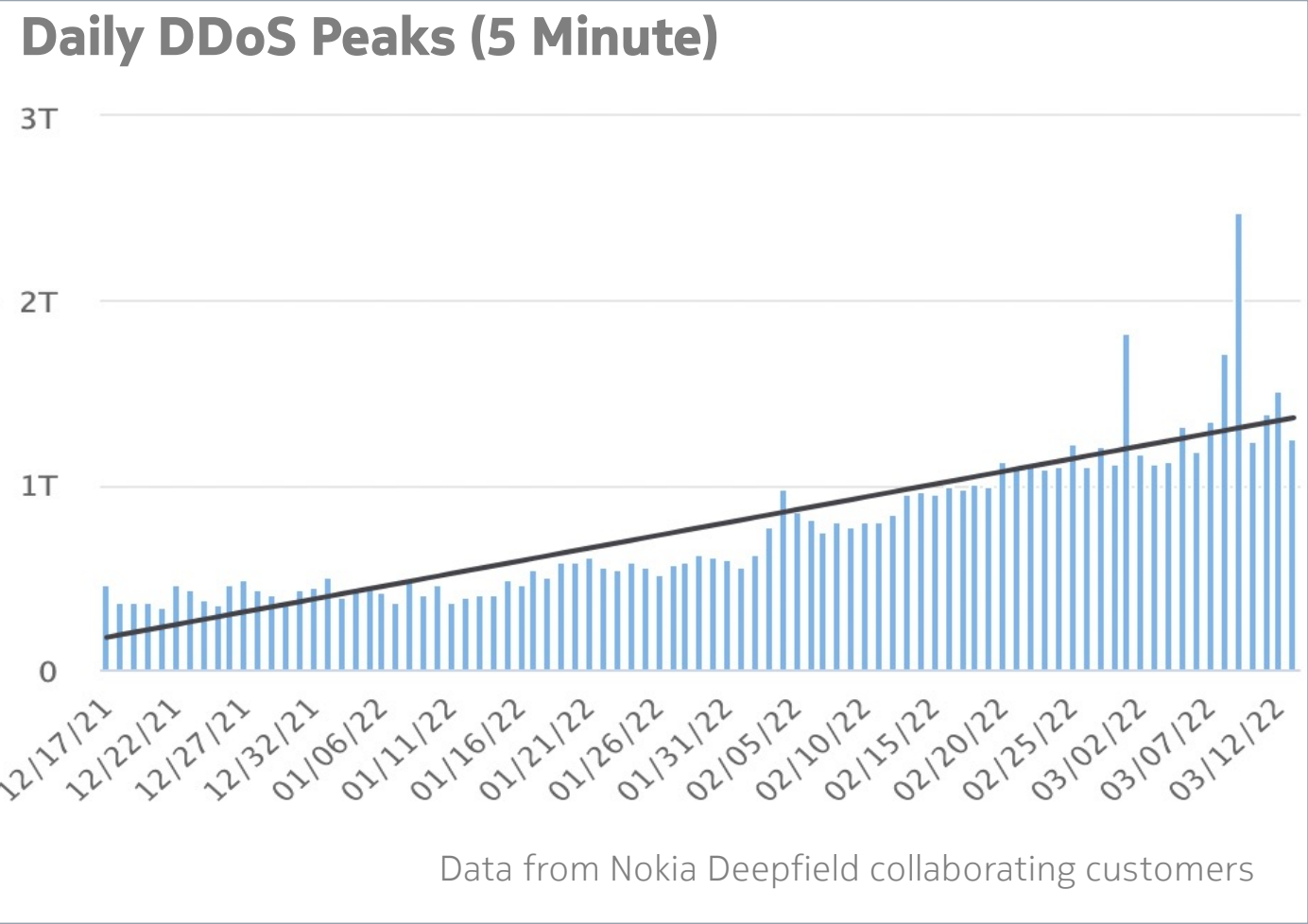
1. DDoS is growing
2. Most DDoS is due to amplification
3. Most DDoS in North America comes from Asia / EU
4. FlowSpec is good for amplification but not other types of DDoS

Only first is true

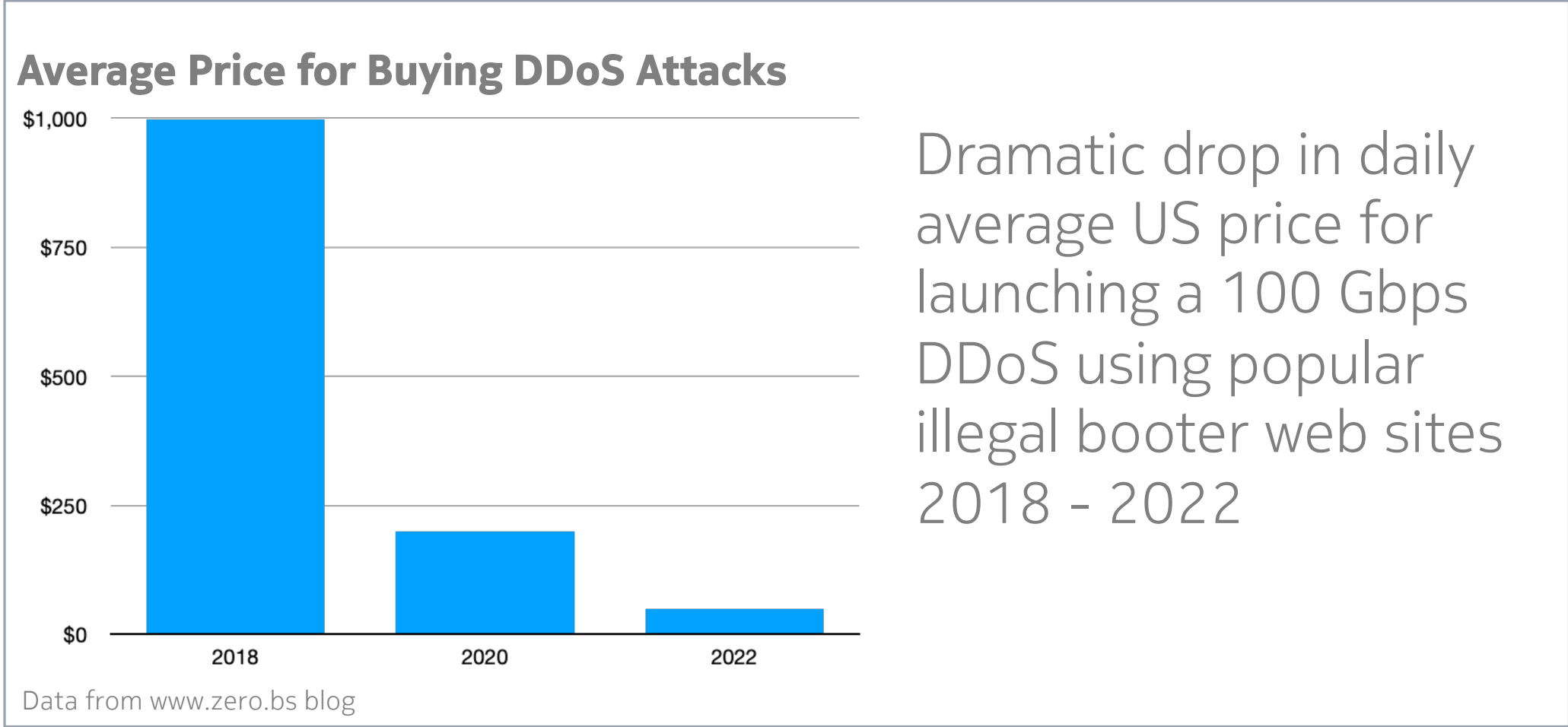
DDoS Traffic is Growing

Key Drivers

- 1. Extortion (bitcoin)
- 2. Theft
- 3. Gamers (Booters)
- 4. Fixed Gigabit and 5G
- 5. IoT Botnets



DDoS Attack Prices are Declining



DDoS Attack Prices are Declining

Dashboard Attack Panel Buy Membership

Custom Plan

- Powerful Attack Methods
- Layer 4/7 Bypass Methods
- Custom Attack Features
- Dedicated Power Each Concurrent
- Unlimited Attacks [No Cooldown]
- Instant Launch & Stop Attacks
- Can Upgrade Plan At Any Time
- REST API Capability
- 24/7 Support

18 Attack Methods

Starts at \$25 /month

CUSTOMIZE AND BUY NOW

www.cybervm.io

STRESSER.AI

BASIC	ADVANCED
€40.00 per month	€150.00 per month
1,200 Seconds Maximum Attack Time	3,600 Seconds Maximum Attack Time
1 Simultaneous Attacks	3 Simultaneous Attacks
UNMETERED PREMIUM NETWORK	UNMETERED PREMIUM NETWORK
No API Included	No API Included
Unlimited Daily Attacks	Unlimited Daily Attacks
Gain €1.60 Reward Points!	Gain €6.00 Reward Points!
SELECT PLAN	SELECT PLAN

www.stresser.ai

NightmareStresser

Silver (1200)

\$14.99
1 Month

Layer 4 & Layer 7 Access: Yes

Boot Time In Seconds: 1200

Concurrent Attacks: 1

API Access: No

Network: Normal

Power: 10G/s

Order Now

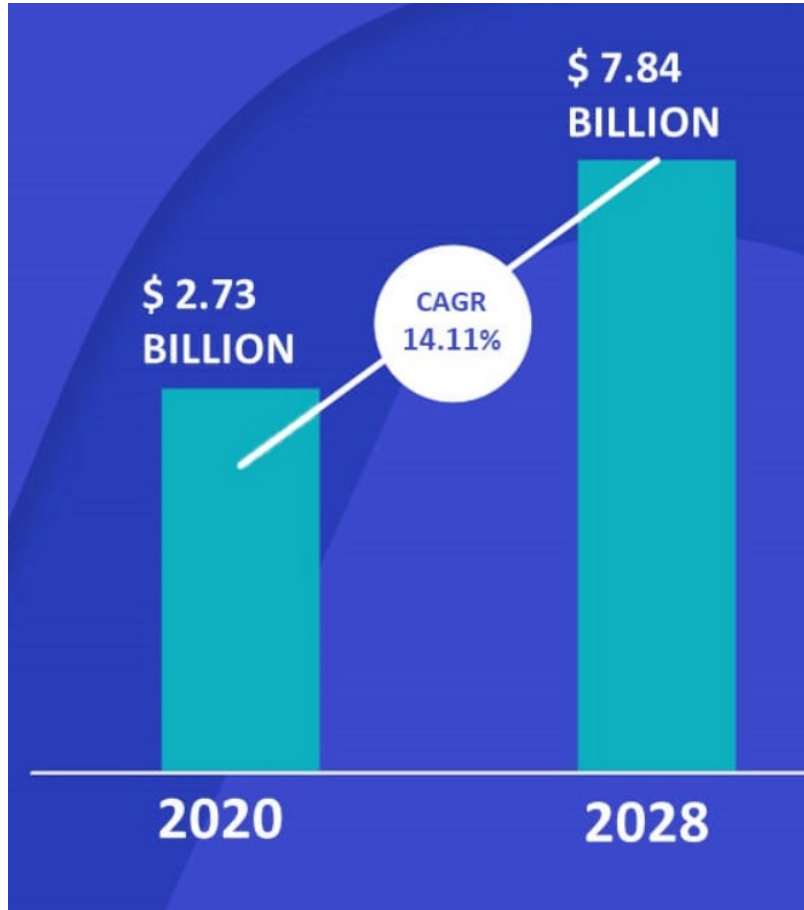
Platinum (60 GBPS)

\$89.99
1 Month

www.nightmarestresser.com

DDoS Defense Prices Increasing 2020 - 2028

Price per Gbps Anti-DDoS not declining at same rate as router / port



Market spend on DDoS solutions

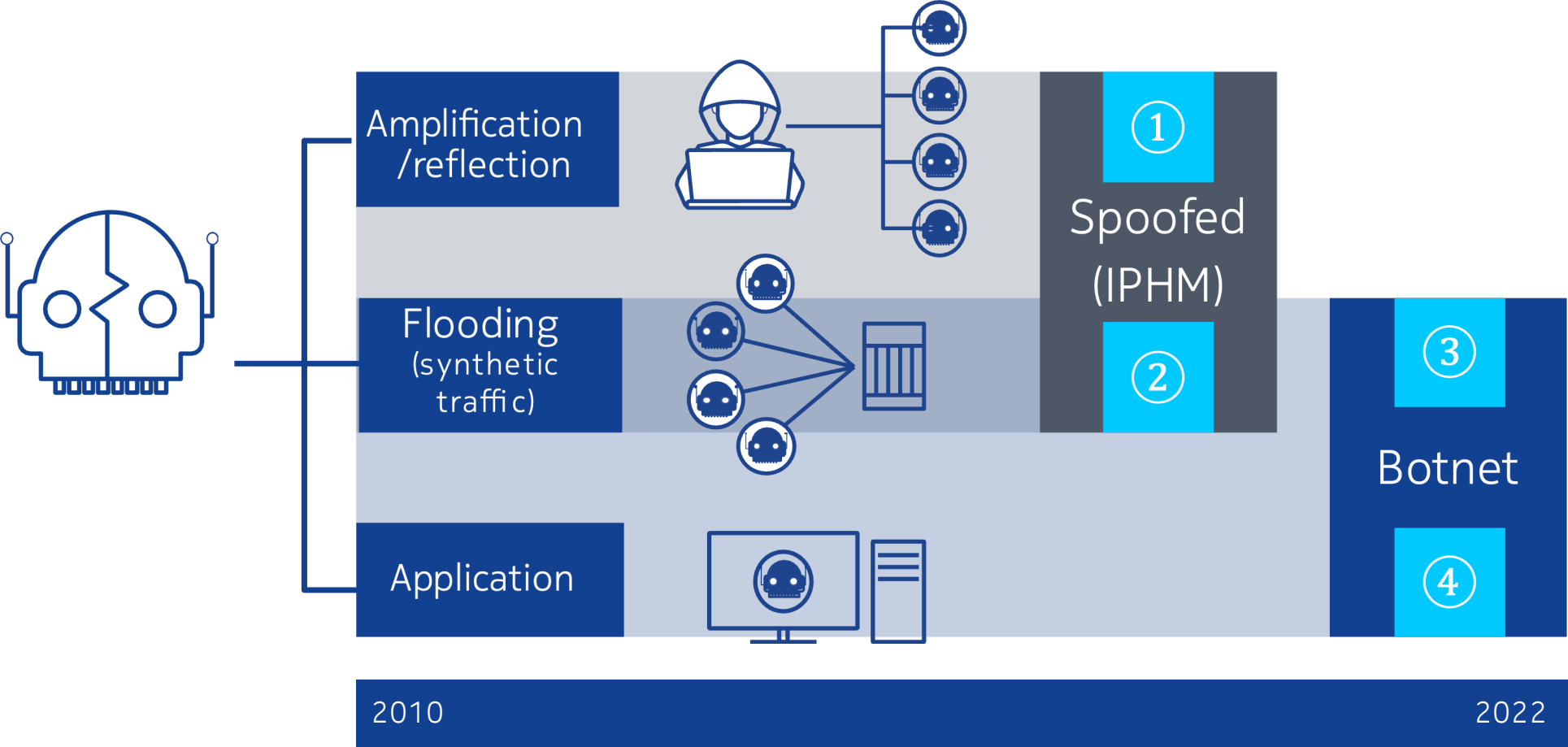
A great market for anti-DDoS vendors (and criminals!)

A commercial challenge for CSP

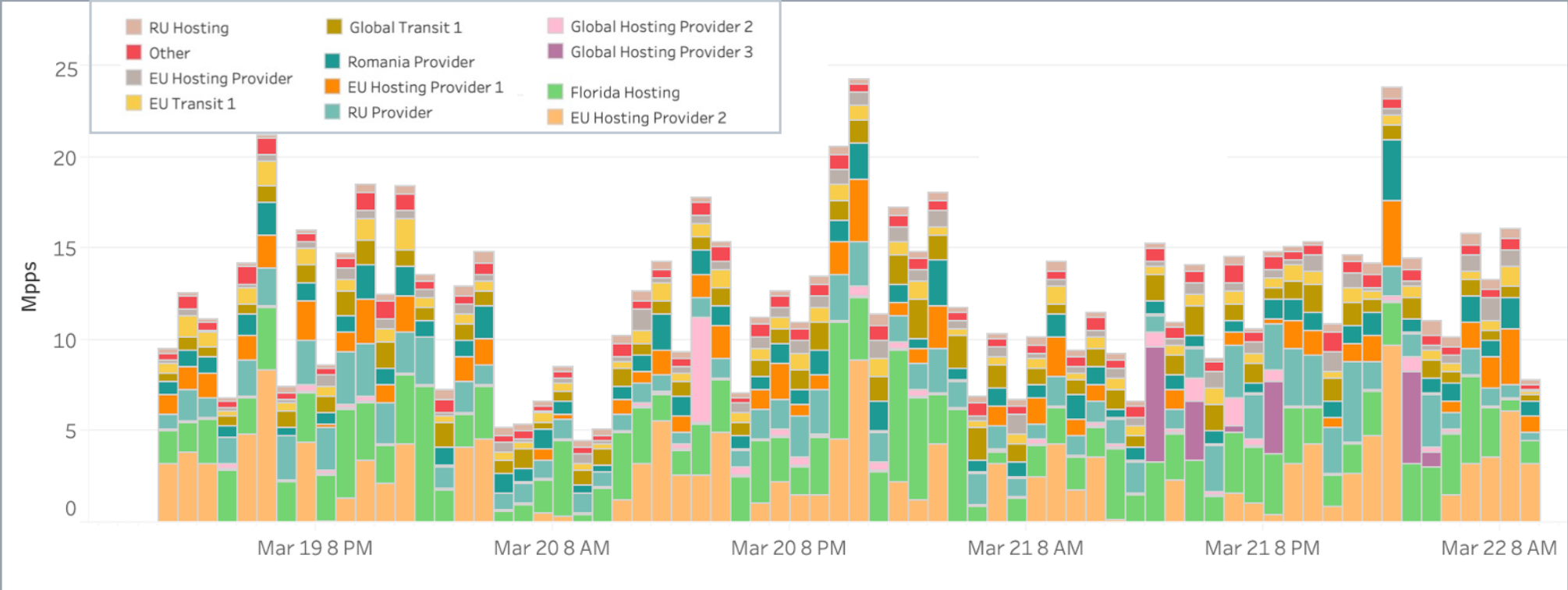
Data from ww.verifiedmarketresearch.com

Changes to DDoS Market

2010– 2020 Most DDoS Amplification of Synthetic Floods from IPHM



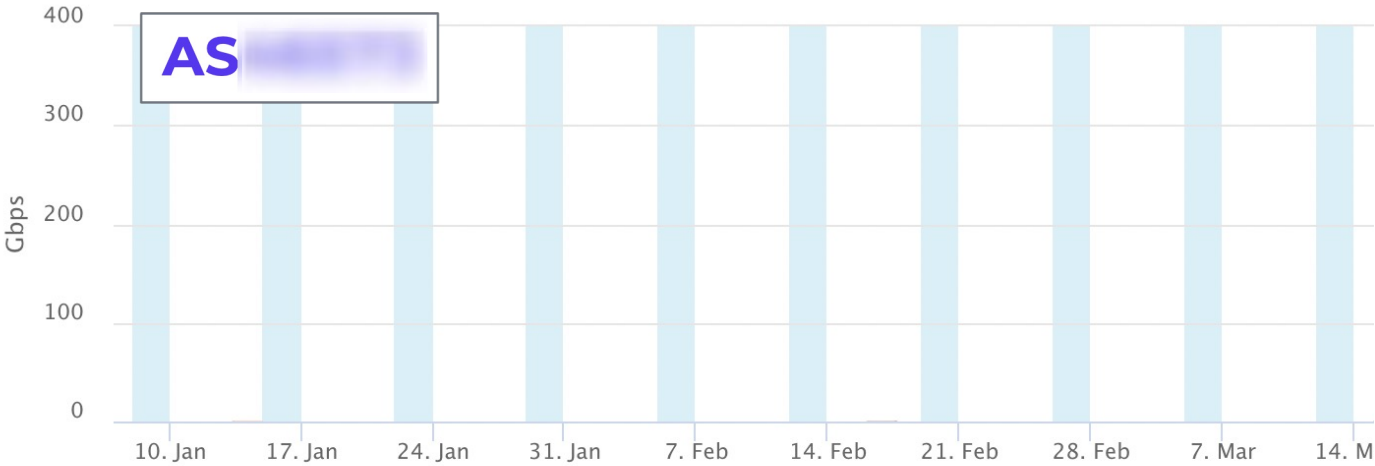
Most DDoS from Small Number of Hosting (2010 – 2020)



March 2021 spoofed traffic – majority of IPHM originates from 50 hosting companies / ASN

Data from June NANOG 2021 presentation showing obvious spoofed traffic including amplifier port pairs and invalid source CIDR

Dramatic Drop IPHM / Spoofing (2022)

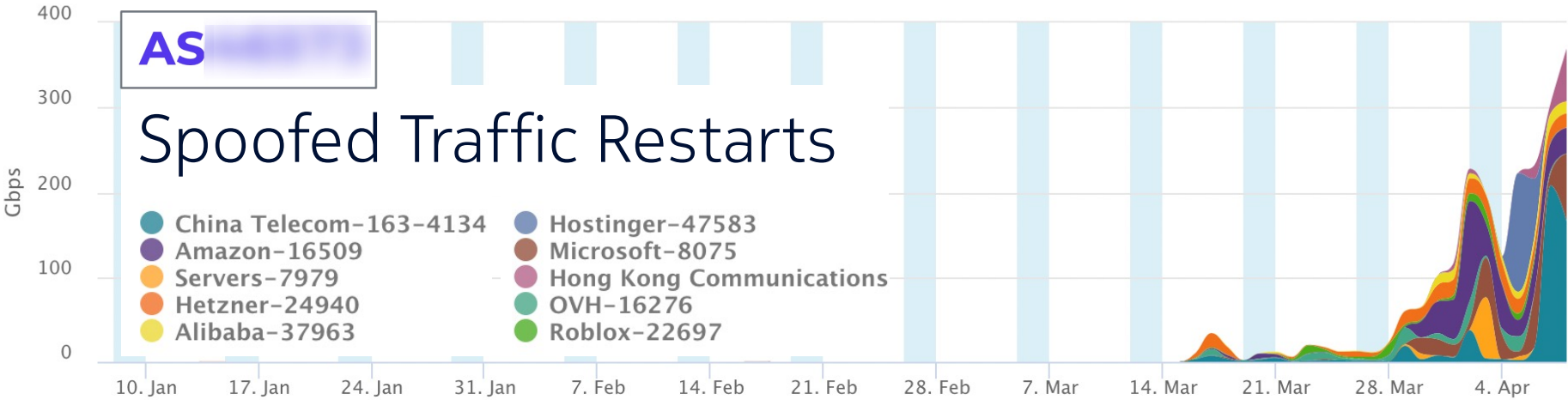


Spoofed traffic (invalid source ASN) observed outbound from one of largest global IPHM hosting companies

Good News! Spoofed traffic from several of top IPHM DDoS hosting stopped in H2 2021!

Thanks to NANOG / RIPE community and BCP 38

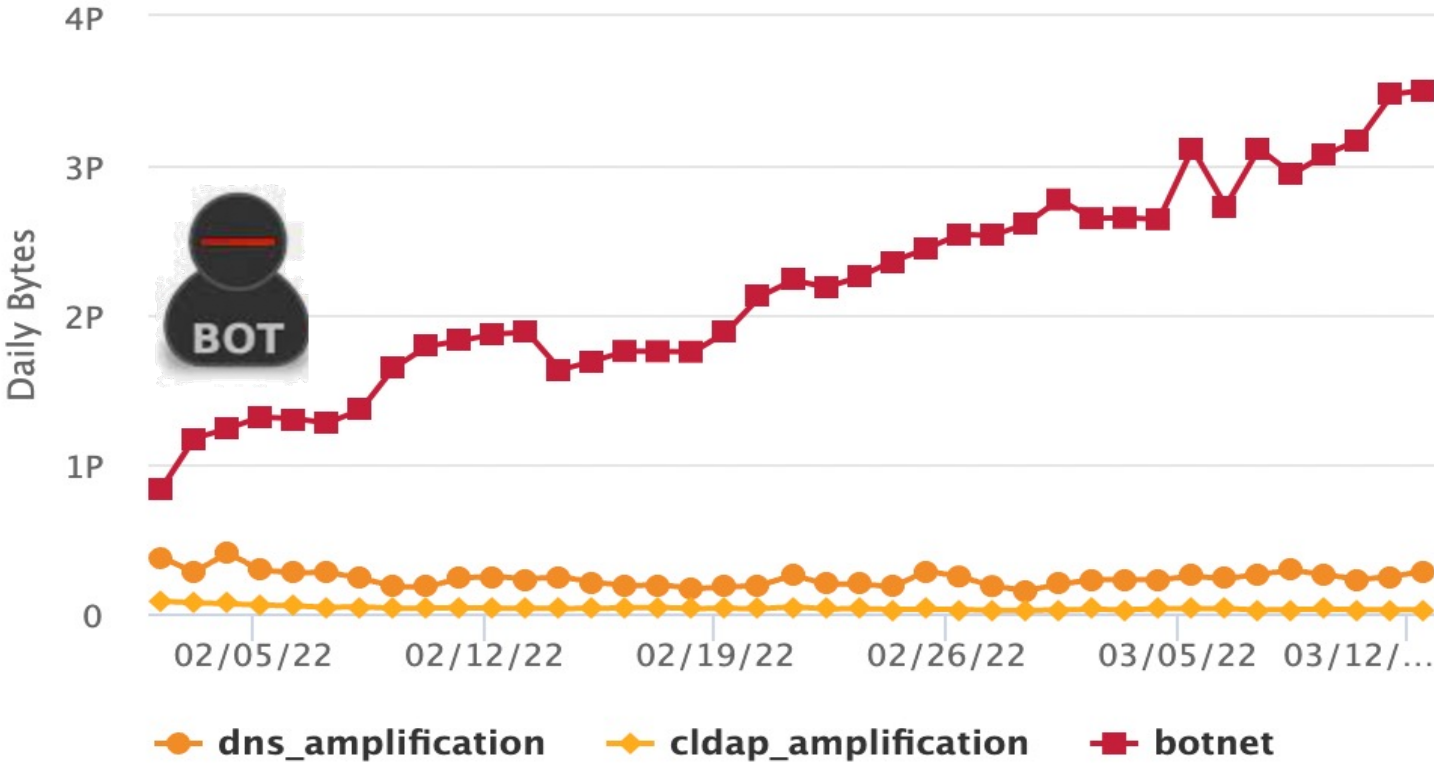
Dramatic Drop IPHM / Spoofing (2022)



Source CIDR of peering traffic from medium size hosting company that does not actually provide transit to Alibaba, OVH, Roblox, Microsoft

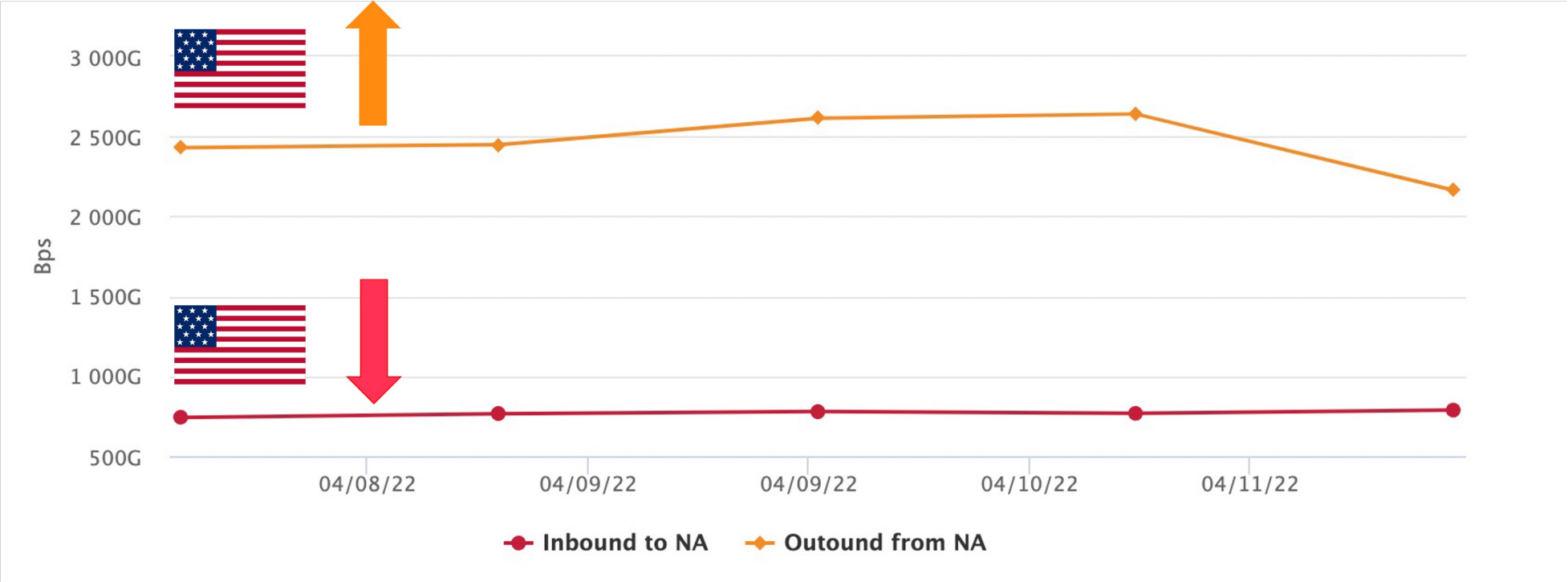
Less Good - Some IPHM hosting returned H1 2022
Please check your peers and customers!

Botnets now dominant source of DDoS in North America



Less Good – Decline in IPHM spoofed (flood and amp) offset by Botnet DDoS

North America Net Producer of DDoS 2022



2010-220 North America victim / consumer of DDoS from EU / Asia
2022 North America is a net producer of DDoS traffic!

Too many DVR and IoT

300k+ IoT / Servers active in Commercial Botnets (24 hours)

DVR x.x.5.9 is a DDOS botnet member

Hybrid Video Recorder

IRV- Series 3年保証

Model 4ch IRV- 8ch IRV-

主な製品特長

- TVI 最大 4K、AHD 最大 5MP、CVI 最大 2MP 及び CVBS 対応
- ネットワークカメラ最大 **4MP**
- 映像出力：VGA / HDMI / CVBS SPOT の **3 系統**
- 音声入力：4
- 画像圧縮：H.264/H.265 対応（出荷時は H.264）
- IRV-AT6004N **1**トレイ、AT6008N **2**トレイ **ビデオ用 HDD** を標準使用。最大 **8TB**
- 検索 / 再生：カレンダー検索 / イベント検索 / 前回からの再生
- Alarm 入力：IRV-AT6004N **4 系統**、AT6008N **8 系統**
- 倍速再生：2 倍速、4 倍速、8 倍速、16 倍速、32 倍速、300 倍速
- P2P 対応、DDNS (PowerDDNS) 対応、NTP 対応、
- その他：HDD 自動計算、自動再起動、設定情報 Export/import、管理者を含む登録ユーザー 15、Push 通知、UTC 対応

Web Service

専用のソフトをインストールする事無く、Web ブラウザ (Internet Explorer 11 以上) によって、IRV-AT6000N シリーズの設定確認や変更を行うことが出来ます。テキストのみの構成となっている為、低スペック PC やモバイル PC、帯域の狭いネットワークや通信速度の遅い環境からでも操作可能。

※Web Service でライブ映像や録画再生を確認したり、バックアップ (ダウンロード) を行ったなどの高度な機能は備わっておりません。

※Microsoft Edge、Firefox、Google Chrome、Safari、Opera、Vivaldi、Cyberfox、Kina、Tale Moon、Sleepin' などの一部のブラウザには一部対応しておりません。

※Web Service をご利用頂く場合、IRV-AT6000N シリーズのネットワーク設定内の Web ポート設定と、IRV-AT6000N シリーズが接続されている現場のルータのポートフォワーディング設定 (ポート開放) が必要です。



Parking meter

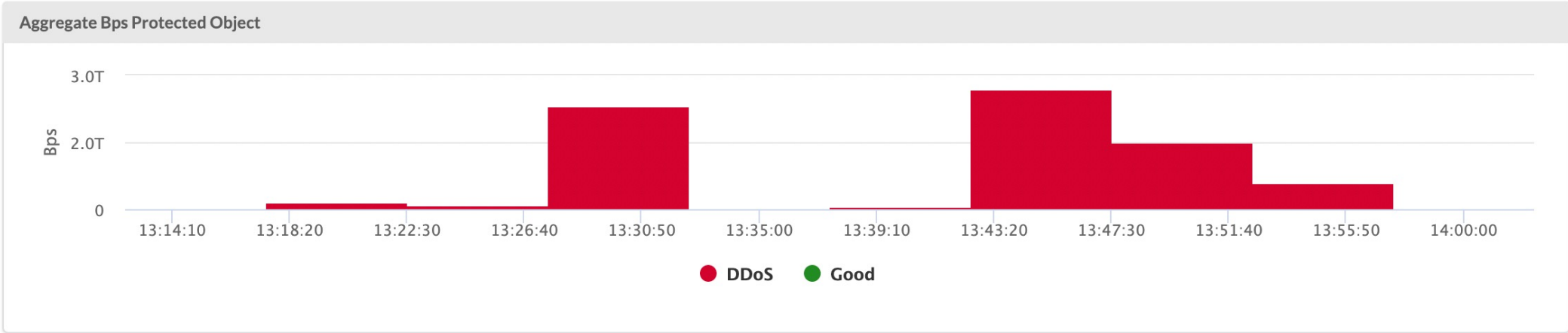
Y.Y.17.23 is a DDoS botnet member



- Other 'popular' members:
- Home routers, IP cameras, thermostats
- Other connected consumer devices
- Cloud servers & appliances, ...

Example: North America Residential Botnet Attack to EU

Dec 28, 2021



Example: North America Residential Botnet Attack to EU

Dec 28, 2021

Time	TTL	Proto	TCP Flag	Peer	Src IP	SPort	Dst IP	DPort	Drop	Src Genome	Bytes	Len
13:45:00	60	17			.99.238	22897	2.18	7778	44	lighttpd webcam k.jp ddosbot 🇯🇵	536094310	1,428
13:45:00	58	17			.86.130	61792	2.18	7778	44	commax webcam ulwsd ddosbot	536094310	1,428
13:30:00	60	17			.250.12828157		2.18	7778	16	ddosbot	534757427	1,427
13:45:00	61	17			.1.105	5306	2.18	7778	16	unknown_web fujitsu.com ddosamp rfs ddosbot	534757427	1,427
13:45:00	61	17			.1.196	48338	2.18	7778	16	ntt.com ddosbot 🇯🇵	534757427	1,427
13:45:00	60	17			.37.76	41311	2.18	7778	44	commax webcam ulwsd speco .on.net com ddosbot 🇺🇸	534024294	1,428
13:50:00	55	17			.7.33	27181	2.18	7778	16	app-webs httpd webcam .e.com unknown_dns hikvision myfritz ddosbot 🇩🇪	533827788	1,427
13:55:00	62	17			.28	2823	2.18	7778	44	ddosbot 🇯🇵	533722419	1,428
13:45:00	58	17			.86	37387	2.18	7778	44	lighttpd webcam k.jp ddosbot 🇯🇵	533420544	1,428

A Month in the Life of One North American Webcam

Default CIDRs **History** JSON

Show 50 entries Search:

Date	Event
02/13/22	om lighttpd webcam
02/13/22	om lighttpd webcam om ddosbot lighttpd webcam
02/16/22	ner.com UDP Flood Botnet (1368)
03/14/22	ames.com Botnet UDP Flood (1242)
05/02/22	214)
05/03/22	it.com Botnet QUIC (2121)
05/08/22	ined (2176)
05/08/22	me.ru (2436)
05/10/22	net Botnet QUIC (2469)
05/13/22	rd.com Botnet QUIC (2512)
05/23/22	m Botnet QUIC + TCP (2508)
05/24/22	om Botnet QUIC (2189)
05/24/22	ok.com Botnet Syn + QUIC (2479)
05/24/22	Botnet QUIC (2530)

This camera part of commercial botnet
Used in multiple DDoS campaigns per day
Outbound DDoS traffic frequently 1 Gbps

The Problem with North American Botnets

1. Growth in IoT trending towards super linear
2. IoT security not improving
3. IoT Botnet DDoS challenging to mitigate
4. Structural problem / CSP incentive gap

The Problem with North American Botnets

Payload / Header (e.g. HTTP(S)) are otherwise legitimate

The image shows a Wireshark network traffic capture. The top pane displays a list of packets. The selected packet (99.441880) is an HTTP GET request from source IP 152.231.62.172 to destination IP 129.128.212. The bottom pane shows the details of this packet, including the Hypertext Transfer Protocol section with the following content:















```
GET / HTTP/1.1\r\nHost: 129.128.212\r\nConnection: keep-alive\r\nPragma: no-cache\r\nCache-Control: no-cache\r\nUpgrade-Insecure-Requests: 1\r\nUser-Agent: Mozilla/5.0 (Linux; Android 10; RMX2032 Build/QKQ1.200209.002) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.101 Mobile Safari/537.36\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\nAccept-Encoding: gzip, deflate\r\nAccept-Language: en-US\r\n\r\n[Full request URI: http://129.128.212/]\r\n[HTTP request 1/1]
```

Solving North American Botnet Problem

- Structural / CSP Incentives
- Track the Botnets
 - Crawling (multiple vendors)
 - Threat Sharing (real-time DDoS botnet reporting)
 - Library of every DDoS (make public)
- 10x Reduce DDoS Mitigation Cost and Increase Scale
 - Take advantage of existing router silicon (multiple vendors)
 - Crawling data + Botnet Data + Compiler + Netconf / Flowspec

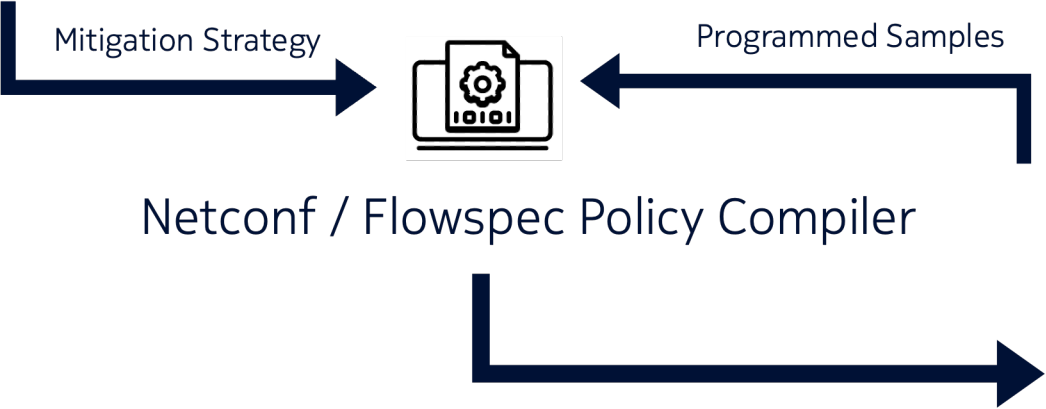
Library of DDoS Attacks 2021 - Present

10K+ attacks from commercial booters and collaborating Nokia customers

GID	Attack	Src IP	Dst IP	Bps	Pps	Filters	False Positive	Status
3	 PPS Spoofed UDP ecksum -- arrients	43,323,931	1	7.2 Gbps	31.2 Gpps	1	0%	
10	 ACK TCP ACK Flood with mos res	39,705,864	1	9.4 Gbps	28.8 Gpps	1	0%	
102	 ICMP-Echo Badly spoofed ICMP Echo Flood with IPs randomized from	33,310,986	1	5.3 Gbps	23.5 Gpps	1	0%	
81	 TCP-Bypass Badly spoofed TCP Syn flood wi y e	18,134,655		103 Mbps	313 Kbps	0	0%	
2	 ExoFlag Spoofed TCP XMAS flood with measures	14,467,644	1	3.7 Gbps	9.5 Gpps	3	0%	
75	 Bomb UDP Flood with most 1 ge. IP	13,344,478		57 Mbps	223 Kbps	0	0%	
45	 VSE Yet another UDP Flood with	12,985,611	1	2.5 Gbps	8.3 Gpps	1	0%	

Netconf / Flowspec Mitigation Performance

Possible to block all DDoS on Routers (multiple vendors)



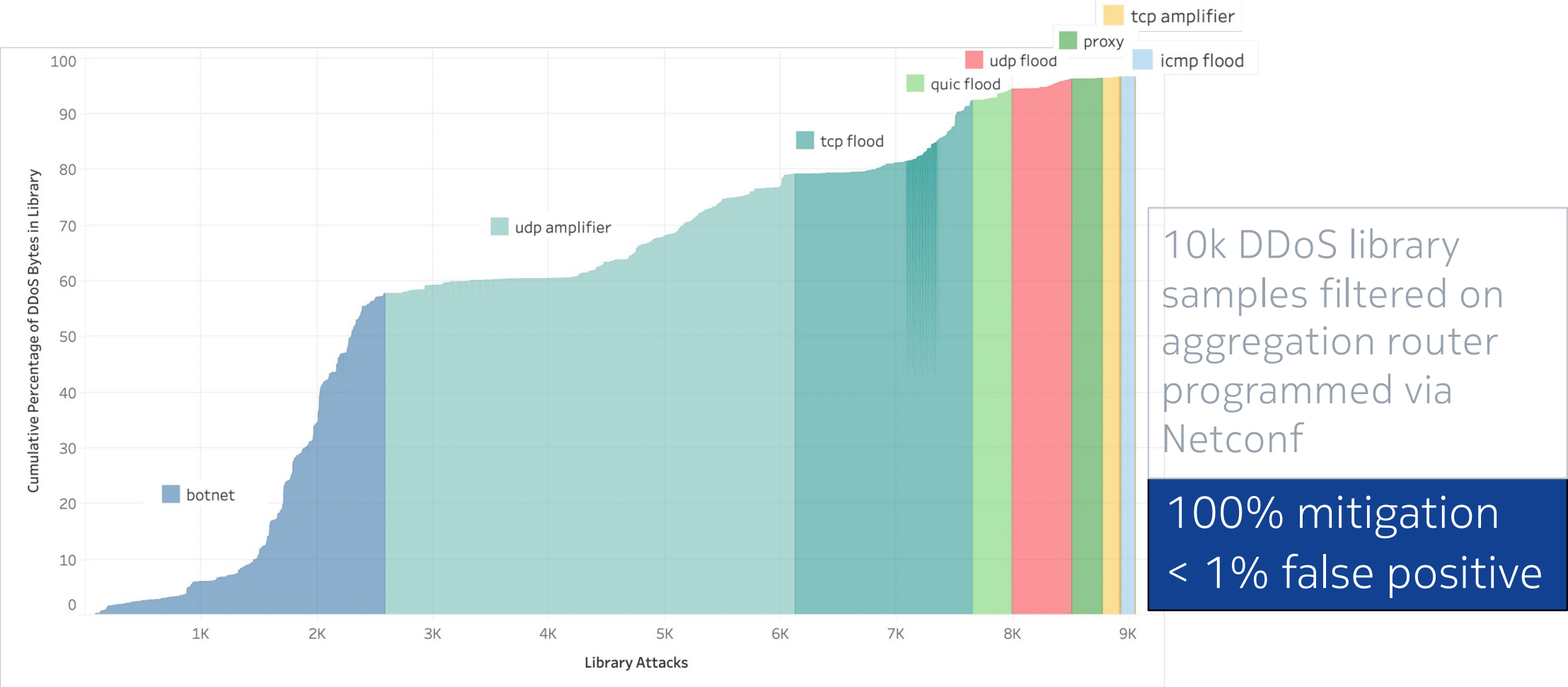
```
entry 8 create
description "#DFA;acl_90"
match protocol 17
  dst-ip ip-prefix-list "VLAB_7_1"
  packet-length lt 40
  fragment false
exit
action
drop
exit
exit
entry 9 create
description "#DFA;acl_571"
match protocol 6
  dst-ip ip-prefix-list "VLAB_7_1"
  tcp-fin true
  tcp-syn true
exit
action
drop
exit
exit
entry 10 create
description "#DFA;acl_579"
match protocol 6
  src-ip ip-prefix-list "VLAB_9_518"
exit
action
drop
exit
exit
entry 4 create
description "#DFA;acl_13498"
match
  dst-ip ip-prefix-list "VLAB_9_495"
  ttl range 1 37
exit
action
drop
exit
```

Linecard

Linecard

Netconf / Flowspec Mitigation Performance

Possible to block all DDoS on Routers (multiple vendors)



NOKIA