@HUNOG_1

Using AI/ML for Network-optimized DDoS Mitigation

Daniel Beszkid

12 October 2023

NOKIA

Some facts:

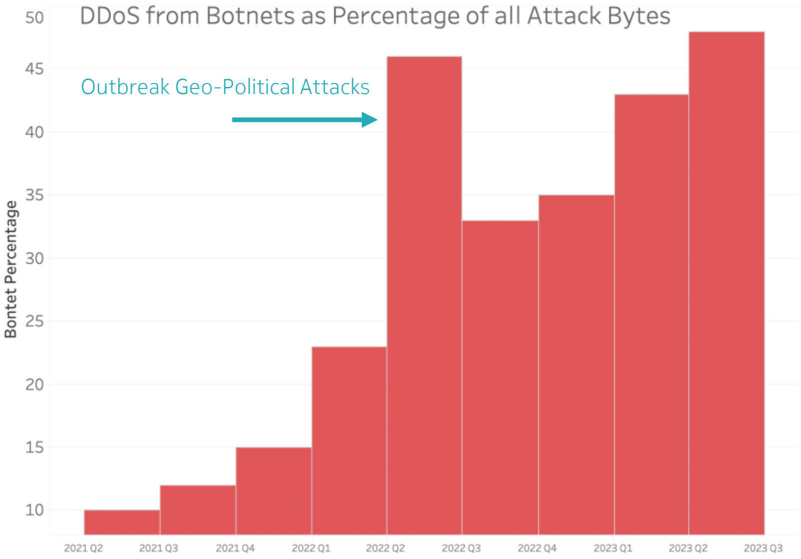
#1: Botnets have taken over the (DDoS) world

2002 - 2022

- Majority of DDoS is spoofed / IPHM
- Originates from 50 EU / AP hosting providers
- Abuses misconfigured NTP / DNS servers

2023

- Botnets are now **majority** of all DDoS bytes
- Botnets now represent **90% of complex attacks**
- **Botnet circumvent traditional anti-DDoS systems**



Nokia data showing botnet originated DDoS traffic as percentage of all attack traffic over last year. Data from GDTA participating service and cloud providers around the world with Nokia commercial DDoS defense solution

Booter services

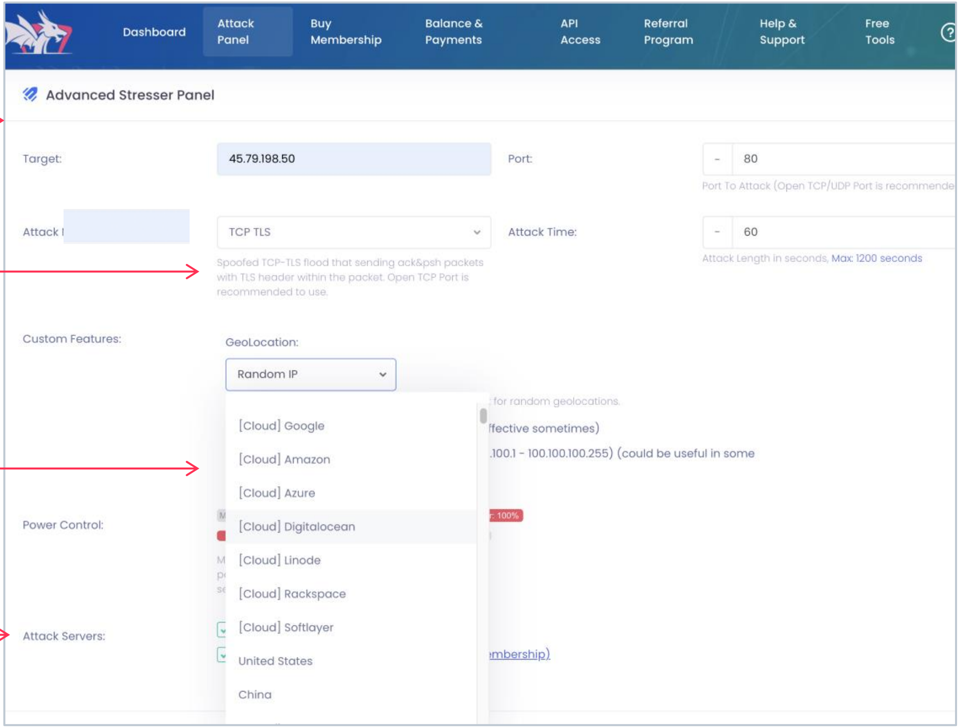
As easy as “click, pay and launch”

Pricing varies, but usually around $50/month paid in cryptocurrency - 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 spend (“VIP package”)

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

Most claim 20-30 servers, including VIP reserved instances



Advanced Stresser Panel

Target: 45.79.198.50

Port: - 80

Port To Attack (Open TCP/UDP Port is recommende

Attack I TCP TLS

Spoofed TCP-TLS flood that sending ack&psh packets with TLS header within the packet. Open TCP Port is recommended to use.

Attack Time: - 60

Attack Length in seconds, Max: 1200 seconds

Custom Features:

GeoLocation:

Random IP

- [Cloud] Google
- [Cloud] Amazon
- [Cloud] Azure
- [Cloud] Digitalocean
- [Cloud] Linode
- [Cloud] Rackspace
- [Cloud] Softlayer
- United States
- China

for random geolocations.

ffective sometimes)

.100.1 - 100.100.100.255) (could be useful in some

Power Control:

: 100%

Attack Servers:

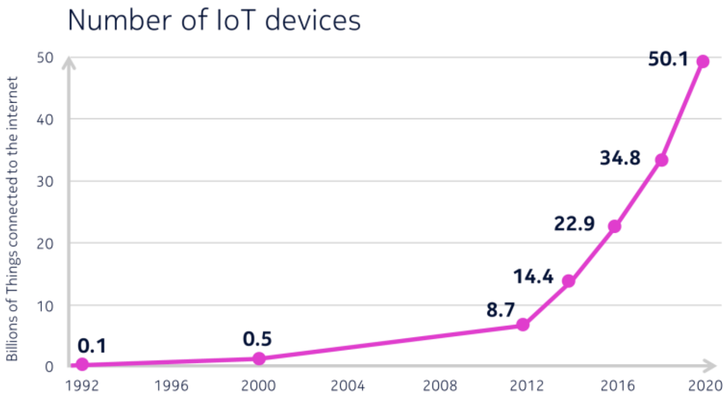
mbership)

Some facts:

#2: There are many bots…

IoT and Cloud are now everywhere in the enterprise

- Surveillance / NVR / DVR
- HVAC, PoS
- Medical imaging



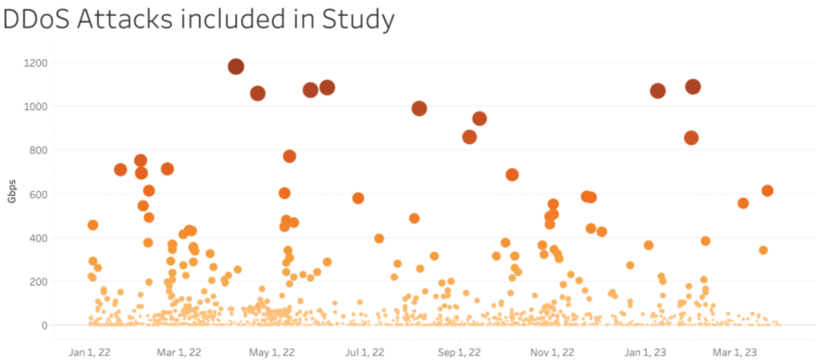
https://www.comptia.org/content/research/sizing-up-the-internet-of-things

99% of enterprise IoT and properly patched, firewalled and secure, but….

1% of many billion devices is significant.

Today, based on Nokia data (and others), botnet DDoS represents:

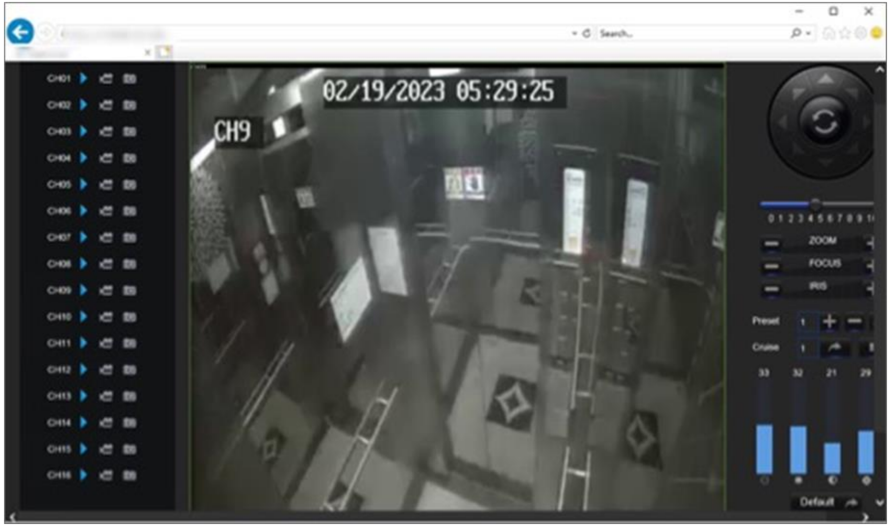
- **500k – 1M active IoT hosts**
- **50 - 100 Tbps** aggregate capacity
- **1 - 2 Tbps peak** observed attacks

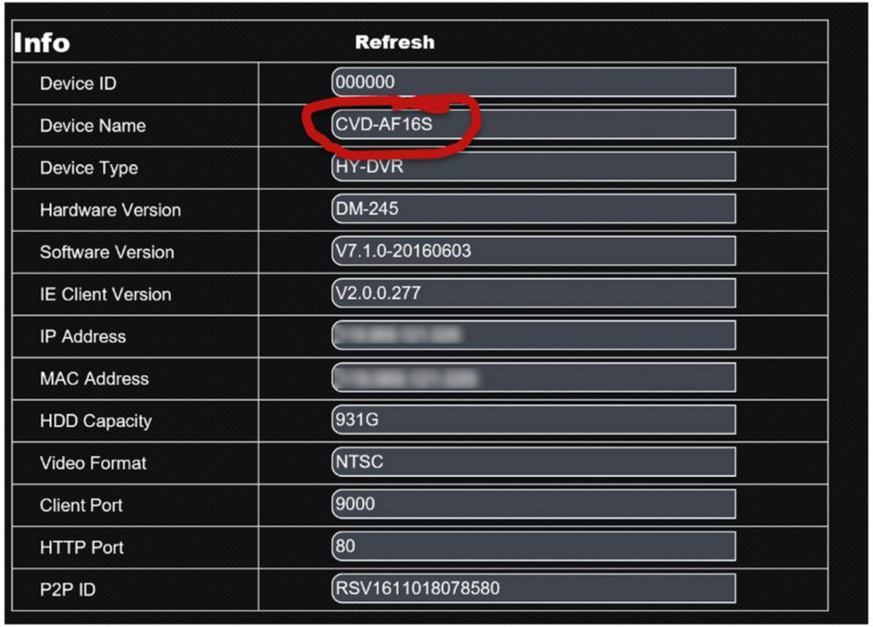


Some facts:

#2: There are many bots…

- Unsecured DVR easily discoverable via crawling
- Running 2016 firmware - easy to exploit
- From model number, you can find CVE
- From CVE, you can find GitHub exploit code
- With exploit code, **you have a bot…**





Info	Refresh
Device ID	000000
Device Name	CVD-AF16S
Device Type	HY-DVR
Hardware Version	DM-245
Software Version	V7.1.0-20160603
IE Client Version	V2.0.0.277
IP Address	[redacted]
MAC Address	[redacted]
HDD Capacity	931G
Video Format	NTSC
Client Port	9000
HTTP Port	80
P2P ID	RSV1611018078580

Some facts:

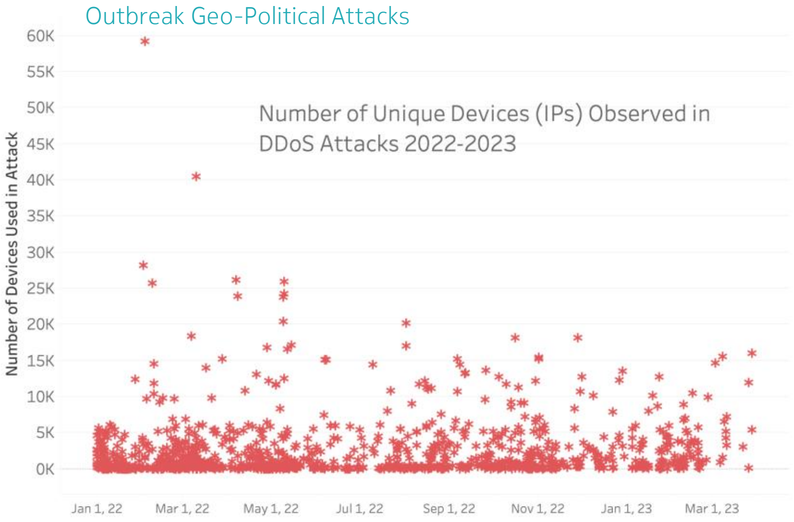
#3: …and (almost as) many botnets

Majority attacks < 5,000 devices and effective against many server / applications

Large networks of **> 60k devices** and geo-political attacks included previously unknown botnet devices

On device types:

- Most botnet are compromised CPE (e.g., Mikrotik router) followed by one of 30-40 brands of DVR
- Botnets tend to attack in "packs" of like devices and topologies
- Cloud is not largest by number of devices, but one of fastest growing in terms of bps / pps capacity



Some facts:

#4: Yet we're still in the early stages of botnet-driven DDoS impact

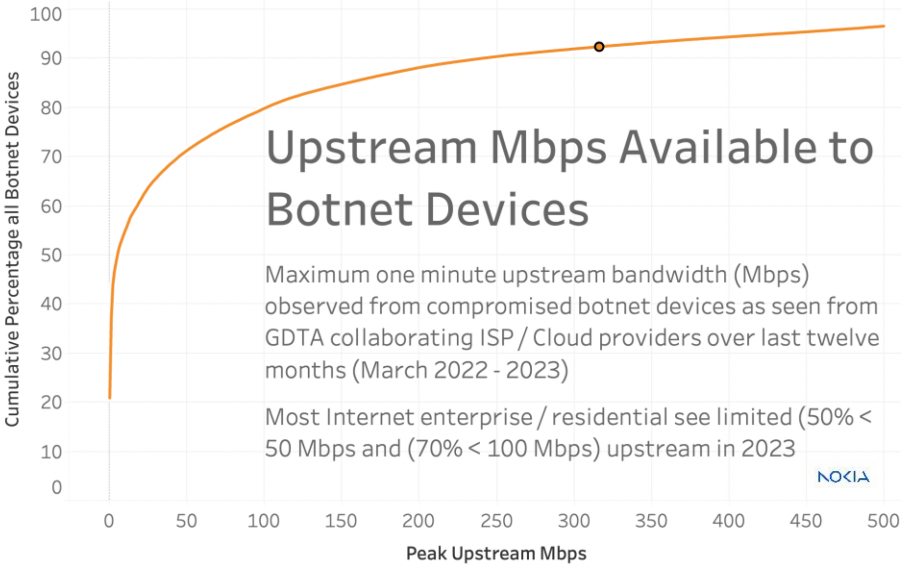
Last 20 years of Internet history

- Most access via Cable / DSL
- Asymmetric access 90 / 10 (down / up)

Botnet threat still limited

- Botnet bps matches industry averages
- 70% of all botnets < 50 Mbps today

i.e., **botnets limited by upstream today's bandwidth** — while race to Gbps symmetrical bandwidth is already well under way.



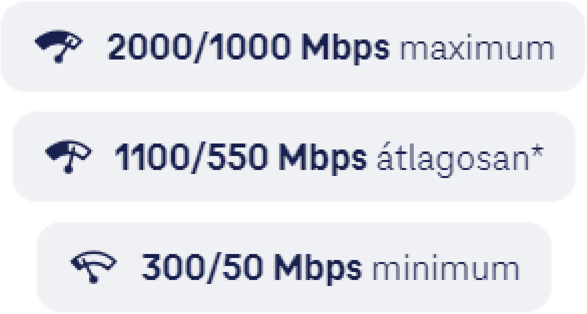
Upstream Mbps Available to Botnet Devices

Maximum one minute upstream bandwidth (Mbps) observed from compromised botnet devices as seen from GDTA collaborating ISP / Cloud providers over last twelve months (March 2022 - 2023)

Most Internet enterprise / residential see limited (50% < 50 Mbps and (70% < 100 Mbps) upstream in 2023

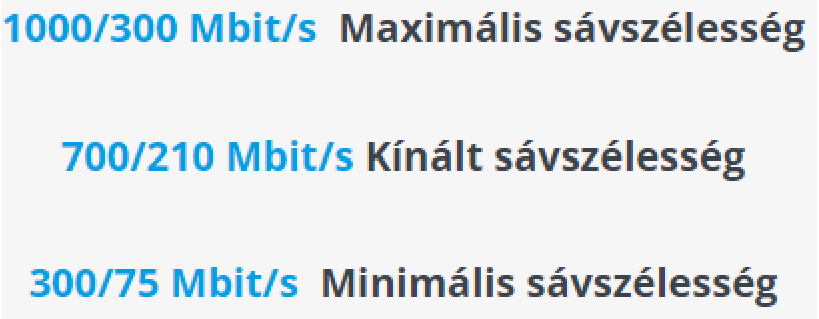
Some facts:

#4: Yet we’re still in the early stages of botnet-driven DDoS impact


2000/1000 Mbps maximum

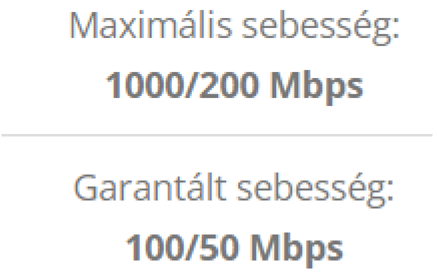
1100/550 Mbps átlagosan*

300/50 Mbps minimum


1000/300 Mbit/s **Maximális sávszélesség**

700/210 Mbit/s **Kínált sávszélesség**

300/75 Mbit/s **Minimális sávszélesség**


Maximális sebesség:

1000/200 Mbps

Garantált sebesség:

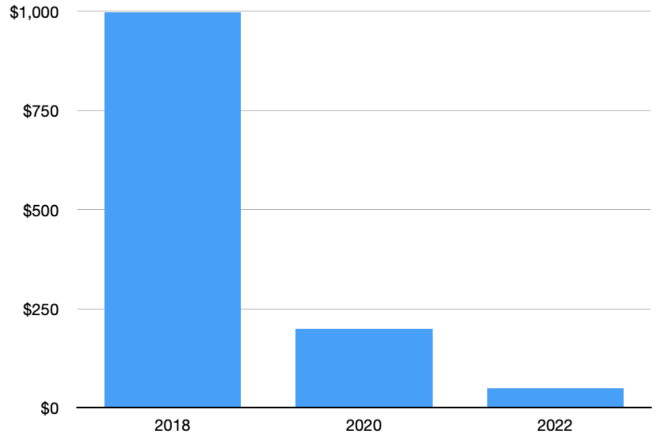
100/50 Mbps

1000 Mbps maximális letöltési és 40 Mbps feltöltési sebesség
Rendes körülmények között elérhető le/feltöltési sebesség 700/28 Mbps

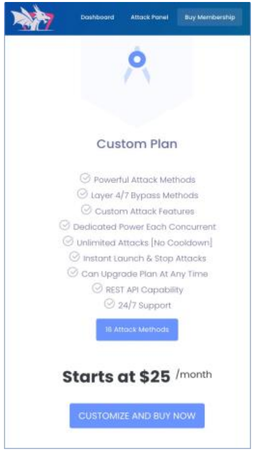
Some facts:

#5: Increasingly Competitive Booter Market and cheap IoT botnets

Average Price for Buying DDoS Attacks



Collapse in daily average US price for launching a 100 Gbps DDoS using illegal booter web sites 2018 - 2022

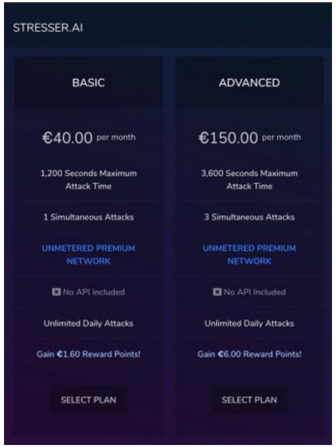


Custom Plan

- 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

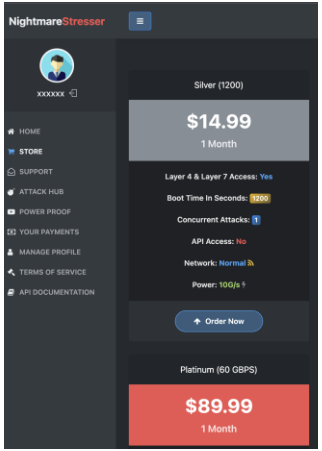
Starts at $25 /month

www.cybervm.io



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!

www.stresser.ai



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

Platinum (60 GBPS)

$89.99
1 Month

www.nightmarestresser.com

Why botnet attacks are such a problem

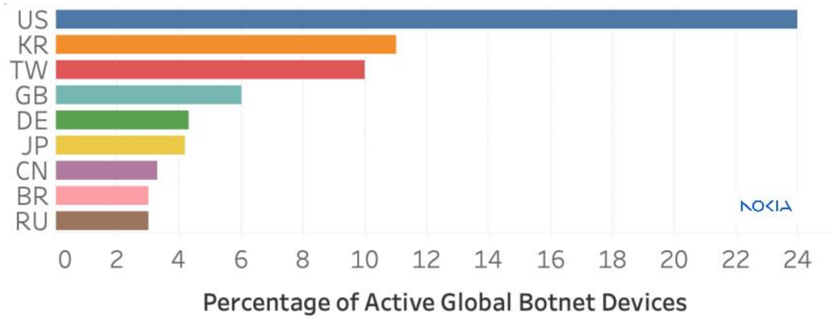
“The call is coming from inside the house”

Traditional ISP / CSP security model assumed:

- Protect external edges of network from inbound attacks, especially problematic eastern EU / Asia countries
- Protect against spoofed or amplified traffic
  - Active countermeasure (e.g., SYN cookie, HTTP redirect)
  - Shaping DNS, NTP, LDAP

The reality in 2023:

- In 2023, majority of botnet problem is North America / Europe
- **Largest threat for many ISP is from their own customers**



The technical challenge with botnet DDoS

Traditional payload pattern detection techniques become less effective

Traditional DDoS (till 2022)

- Spoofed IP addresses to trigger reflected amplified responses
- Or floods of crafted packets
- Often from well-known domains

From threshold-based detection

Botnet-based DDoS

- Real devices, real IP-addresses and full TCP stack
- Appears as "regular" HTTP(s) or applications bypassing scrubbing payload ML
- Growing armies of devices connected anywhere

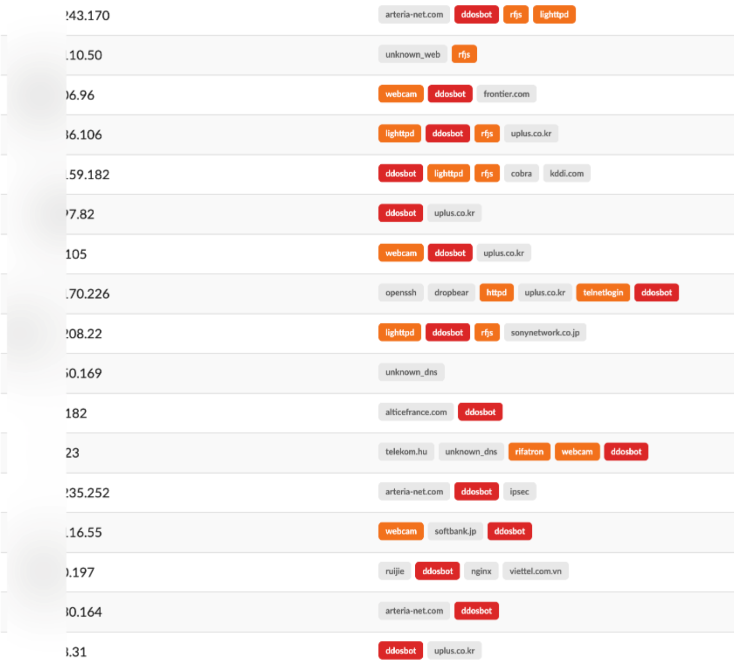
to big-data **knowledge-based** detection

How can we (really) address this?

#1 Anomaly detection

For >95% of DDoS, it's no longer about looking at what's inside the packet — but instead what is sending the packet.

- bps/pps thresholds and baselines are insufficient, and not adapted to most of today's traffic (including flash crowd events)
- A big data-driven approach that correlates network traffic in real-time with broader Internet context (in this case, which type of device is behind a source IP address) is much more effective in reducing DDoS false-positive



43.170	arteria-net.com ddosbot rfjs lighttpd
10.50	unknown_web rfjs
6.96	webcam ddosbot frontier.com
6.106	lighttpd ddosbot rfjs uplus.co.kr
59.182	ddosbot lighttpd rfjs cobra kddi.com
7.82	ddosbot uplus.co.kr
105	webcam ddosbot uplus.co.kr
70.226	openssh dropbear httpd uplus.co.kr telnetlogin ddosbot
08.22	lighttpd ddosbot rfjs sonynetwork.co.jp
0.169	unknown_dns
182	alticefrance.com ddosbot
23	telekom.hu unknown_dns rifatron webcam ddosbot
35.252	arteria-net.com ddosbot ipsec
16.55	webcam softbank.jp ddosbot
.197	ruijie ddosbot nginx viettel.com.vn
0.164	arteria-net.com ddosbot
.31	ddosbot uplus.co.kr

Nokia data top sources of traffic in DNS amplification attack to a consumer IP. Data from GDTA participating service and cloud providers around the world with Nokia commercial DDoS defense solution

How can we (really) address this?

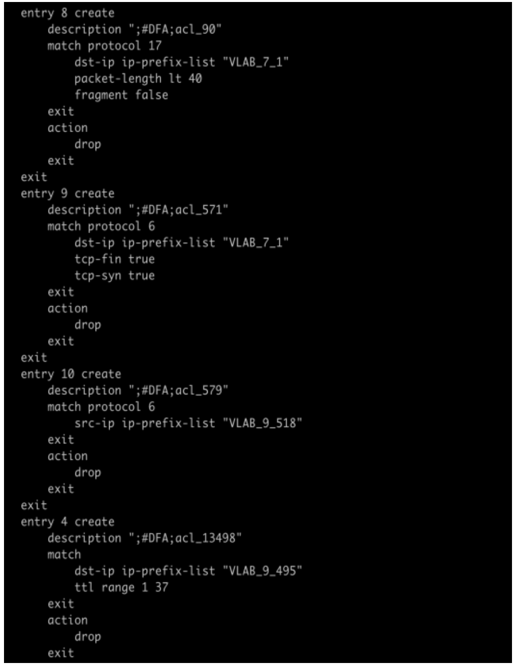
#2 AI-based auto-mitigation

Once an attack is detected, a system can generate an automated response based on multiple parameters, which will create an optimized model for **that attack**, at **that time**, on **that network**.

For example:

- What's the attack vector mix?
- What mitigation devices are available on the network? At what scale and cost per bit?
- How can these devices be programmed?
- What's the botnet cluster launching that attack?

>95% attacks can be mitigated on existing (modern) routers, thanks to progress on silicon performance & programmability (particularly NETCONF).



```
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
```

Output of mitigation strategy model to a router through NETCONF

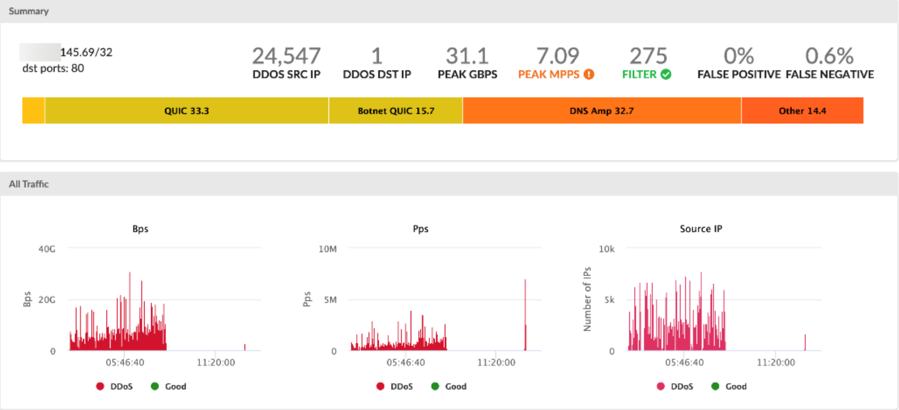
How can we (really) address this?

#3 Adaptive mitigation & collaborative learning

Instead of being driven by FUD:

- Mitigation effectiveness can be **measured** against body of real-world attacks
- Model can be **trained** on new attacks to optimize countermeasures
- False-negative/false-positive rates can be understood and optimized

This does require **active collaboration between CSPs**, to share (anonymized) DDoS treat intelligence data in real-time.



Summary

[redacted]145.69/32
dst ports: 80

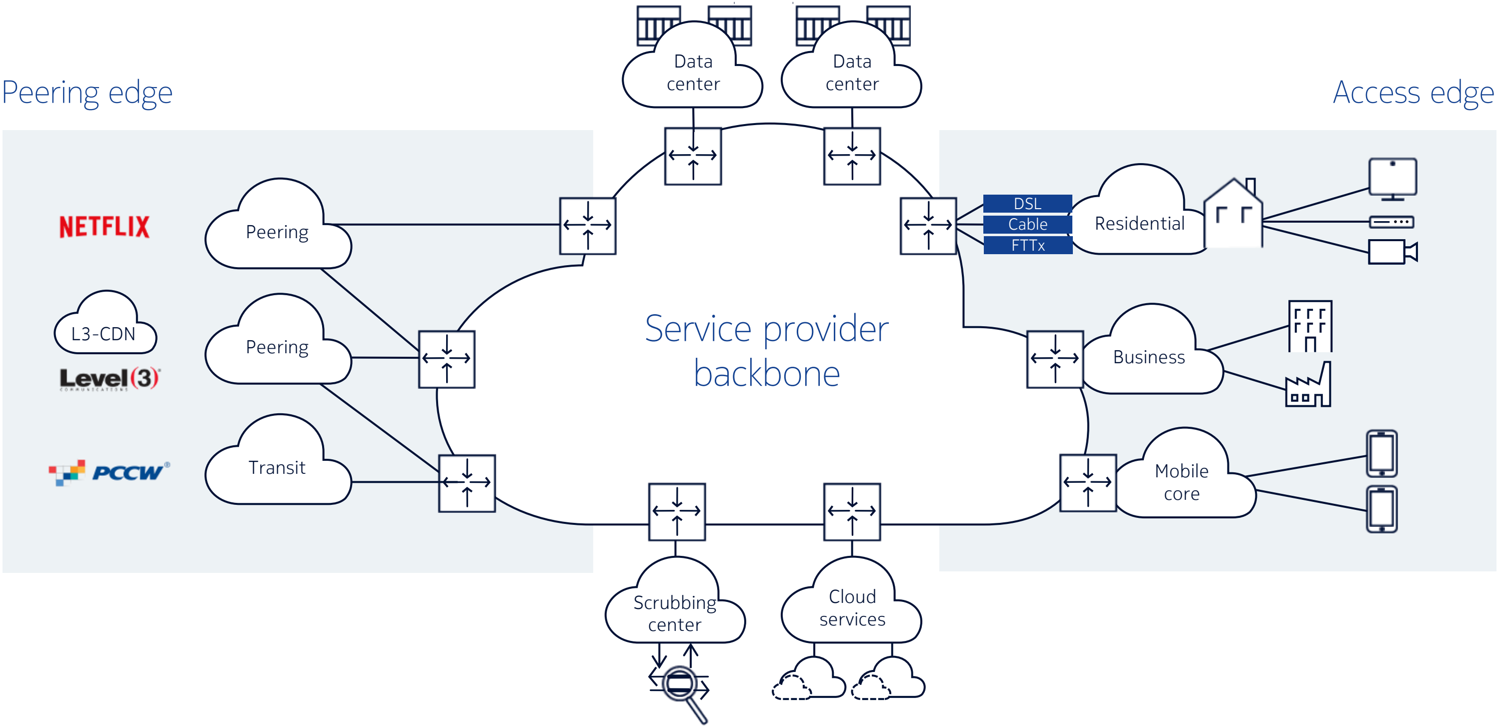
24,547 DDOS SRC IP
1 DDOS DST IP
31.1 PEAK GBPS
7.09 PEAK MPPS
275 FILTER ✓
0% FALSE POSITIVE
0.6% FALSE NEGATIVE

QUIC 33.3 | Botnet QUIC 15.7 | DNS Amp 32.7 | Other 14.4

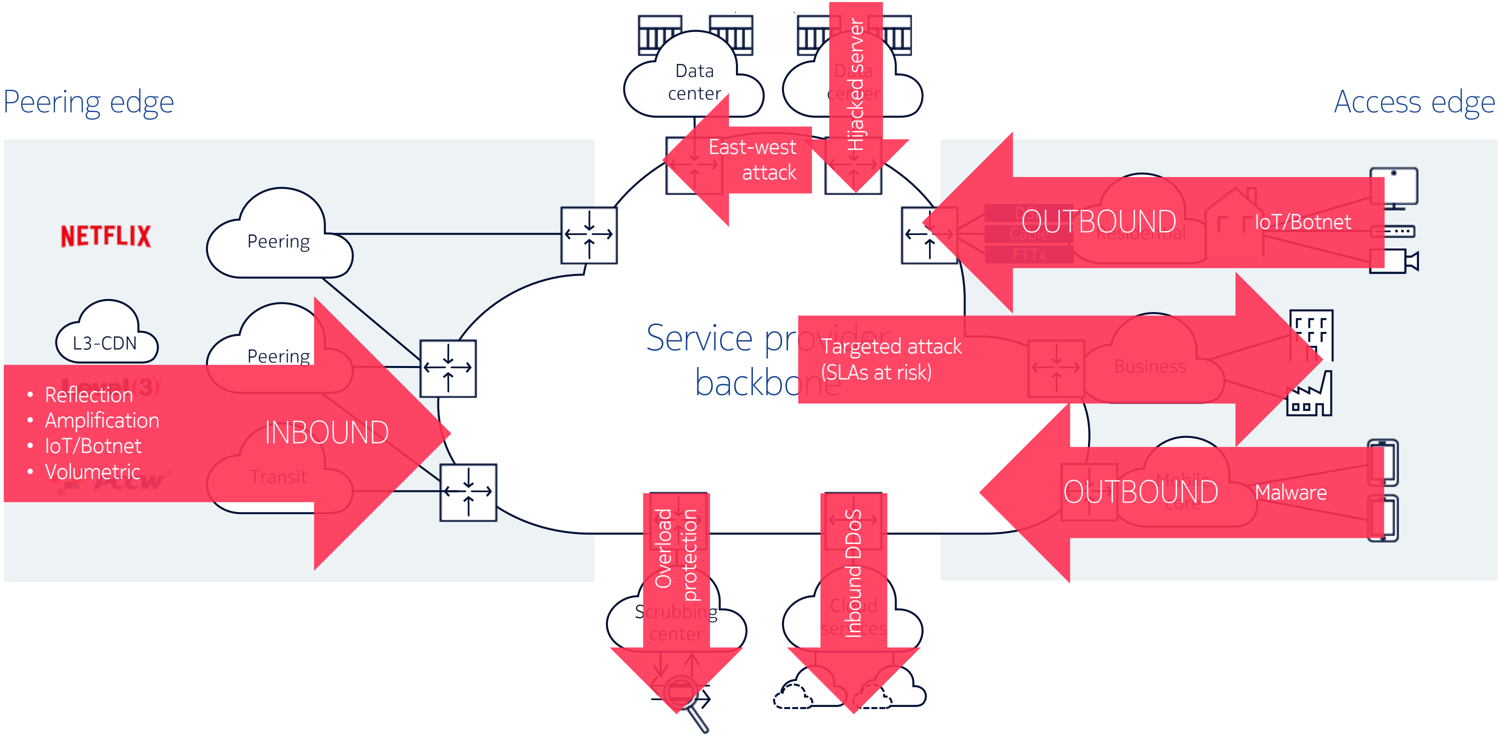
All Traffic

Summary from DDoS attack in April 2023 to an EU government host. Data from GDTA participating service and cloud providers around the world with Nokia commercial DDoS defense solution

What is today’s security perimeter?



What is today's security perimeter?



- Reflection
- Amplification
- IoT/Botnet
- Volumetric

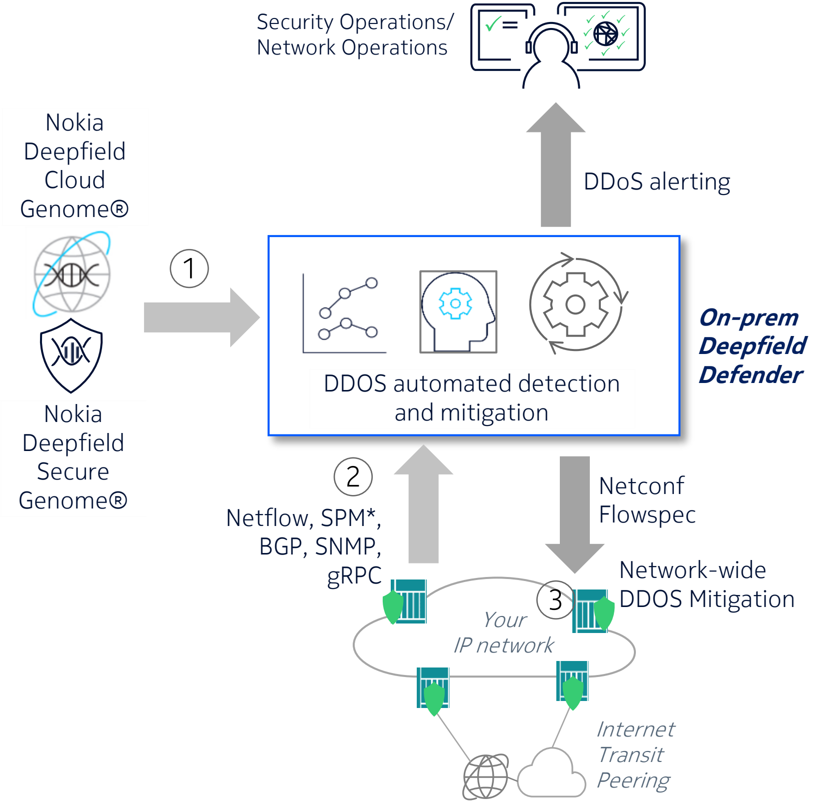
Nokia Deepfield Defender in a nutshell

A high-scalable **software platform** that combines

1. Nokia Deepfield Genome® - a **big data** based Supply-Chain and Security map of the Internet
2. **Telemetry** from your routers
3. with the power of **high-performance Router silicon**

to provide **DDoS protection**

- **at every edge** – the most efficient point
- and **for every customer**
- **at a fraction of the cost** of appliance-based solutions



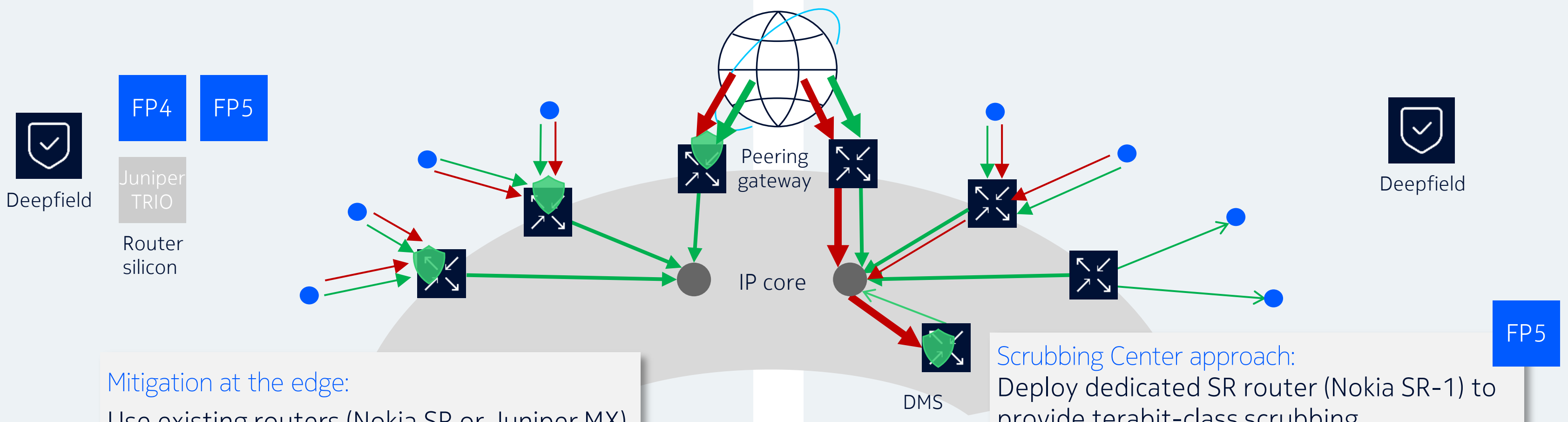
Security Operations/
Network Operations
Nokia Deepfield Cloud Genome®
Nokia Deepfield Secure Genome®
1
DDoS alerting
DDOS automated detection and mitigation
On-prem Deepfield Defender
2
Netflow, SPM*, BGP, SNMP, gRPC
Netconf Flowspec
3
Network-wide DDOS Mitigation
Your IP network
Internet Transit Peering

* SPM (Sample Packet Mirroring) - Only supported fpr Nokia SR and Juniper MX

Deepfield Router based DDoS mitigation – Implementation options

Edge router-based mitigation

Alternative: Off-ramp to Defender Mitigation System (DMS)



Mitigation at the edge:

Use existing routers (Nokia SR or Juniper MX) to drop DDoS traffic at the edge.

Scrubbing Center approach:

Deploy dedicated SR router (Nokia SR-1) to provide terabit-class scrubbing in a controlled SW environment.

Both options match or exceed scrubber-based mitigation efficacy

Summary

DDoS botnets are nascent, but already most of DDoS traffic today

- Exponential growth of enterprise IoT
- ISP symmetrical 1Gbps marketing arms race
- Nation-state attacks with large botnet networks

Enterprise IoT botnets are everyone's problem

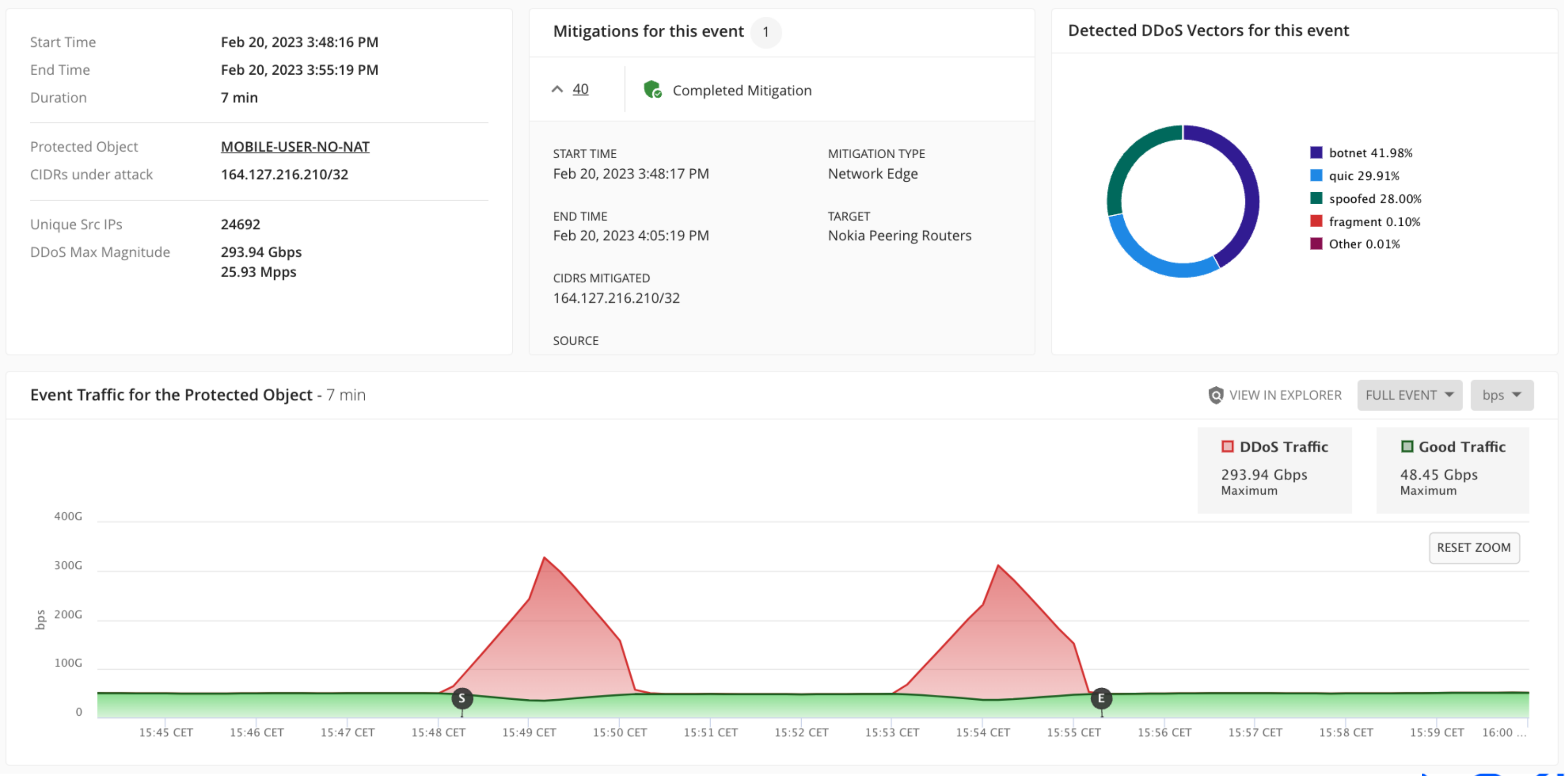
- ISP, enterprise, vendors must take proactive IoT threat mitigation

AI/ML provide us tools to more effectively address that threat

- Models can (and should) be trained on real-world data sets
- More collaboration is essential to share current DDoS data

NOKIA

With Nokia Deepfield, DDoS gets automatically classified…



Start Time	Feb 20, 2023 3:48:16 PM
End Time	Feb 20, 2023 3:55:19 PM
Duration	7 min
Protected Object	MOBILE-USER-NO-NAT
CIDRs under attack	164.127.216.210/32
Unique Src IPs	24692
DDoS Max Magnitude	293.94 Gbps 25.93 Mpps

Mitigations for this event 1

^ 40 Completed Mitigation

START TIME
Feb 20, 2023 3:48:17 PM

MITIGATION TYPE
Network Edge

END TIME
Feb 20, 2023 4:05:19 PM

TARGET
Nokia Peering Routers

CIDRS MITIGATED
164.127.216.210/32

SOURCE

Detected DDoS Vectors for this event

- botnet 41.98%
- quic 29.91%
- spoofed 28.00%
- fragment 0.10%
- Other 0.01%

Event Traffic for the Protected Object - 7 min

VIEW IN EXPLORER | FULL EVENT | bps

DDoS Traffic
293.94 Gbps
Maximum

Good Traffic
48.45 Gbps
Maximum

RESET ZOOM

Copyright and confidentiality

The contents of this document are proprietary and confidential property of Nokia. This document is provided subject to confidentiality obligations of the applicable agreement(s).

This document is intended for use by Nokia's customers and collaborators only for the purpose for which this document is submitted by Nokia. No part of this document may be reproduced or made available to the public or to any third party in any form or means without the prior written permission of Nokia. This document is to be used by properly trained professional personnel. Any use of the contents in this document is limited strictly to the use(s) specifically created in the applicable agreement(s) under which the document is submitted. The user of this document may voluntarily provide suggestions, comments or other feedback to Nokia in respect of the contents of this document ("Feedback").

Such Feedback may be used in Nokia products and related specifications or other documentation. Accordingly, if the user of this document gives Nokia Feedback on the contents of this document, Nokia may freely use, disclose, reproduce, license, distribute and otherwise commercialize the feedback in any Nokia product, technology, service, specification or other documentation.

Nokia operates a policy of ongoing development. Nokia reserves the right to make changes and improvements to any of the products and/or services described in this document or withdraw this document at any time without prior notice.

The contents of this document are provided "as is". Except as required by applicable law, no warranties of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose, are made in relation to the accuracy, reliability or contents of this document. NOKIA SHALL NOT BE RESPONSIBLE IN ANY EVENT FOR ERRORS IN THIS DOCUMENT or for any loss of data or income or any special, incidental, consequential, indirect or direct damages howsoever caused, that might arise from the use of this document or any contents of this document.

This document and the product(s) it describes are protected by copyright according to the applicable laws.

Nokia is a registered trademark of Nokia Corporation. Other product and company names mentioned herein may be trademarks or trade names of their respective owners.