NOKIA

Using AI/ML for network-optimized DDoS mitigation

The nature of DDoS landscape changed dramatically over last years

2000–2021:

- Majority **DDoS is crafted or spoofed** using amplification/reflection
  - ‘Easy’ to mitigate based on pattern match or protocol challenges

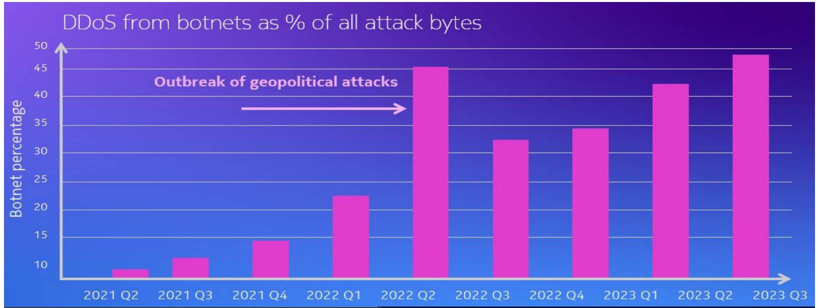
Today:

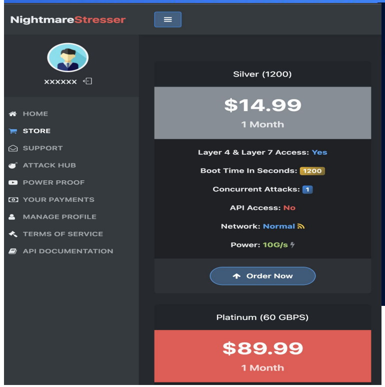
- **Botnets** generate most complex attacks and most DDoS volume
  - Top Botnet device types: webcams, DVRs, routers, NAS, business IOT,…
  - Catalysts: Exponential growth in **IOT devices,** often running old SW stacks
    - Growth in **CVE’s**
    - Booter services: DDoS-SaaS dramatic drop in **DDoS black market prices**

Trends:

- Roll-out of **symmetric GE/10GE access will make things worse…**
- **AI** increases attack variability & realistic HTTPS/DNS/QUIC requests
- Use of **residential Proxy** to mask sources

Source: Nokia Deepfield





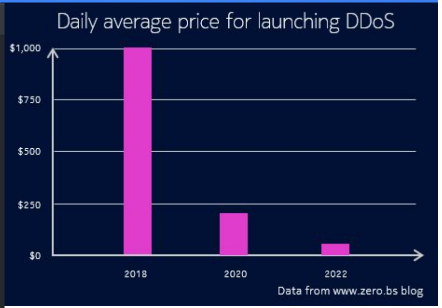
Silver (1200)

$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

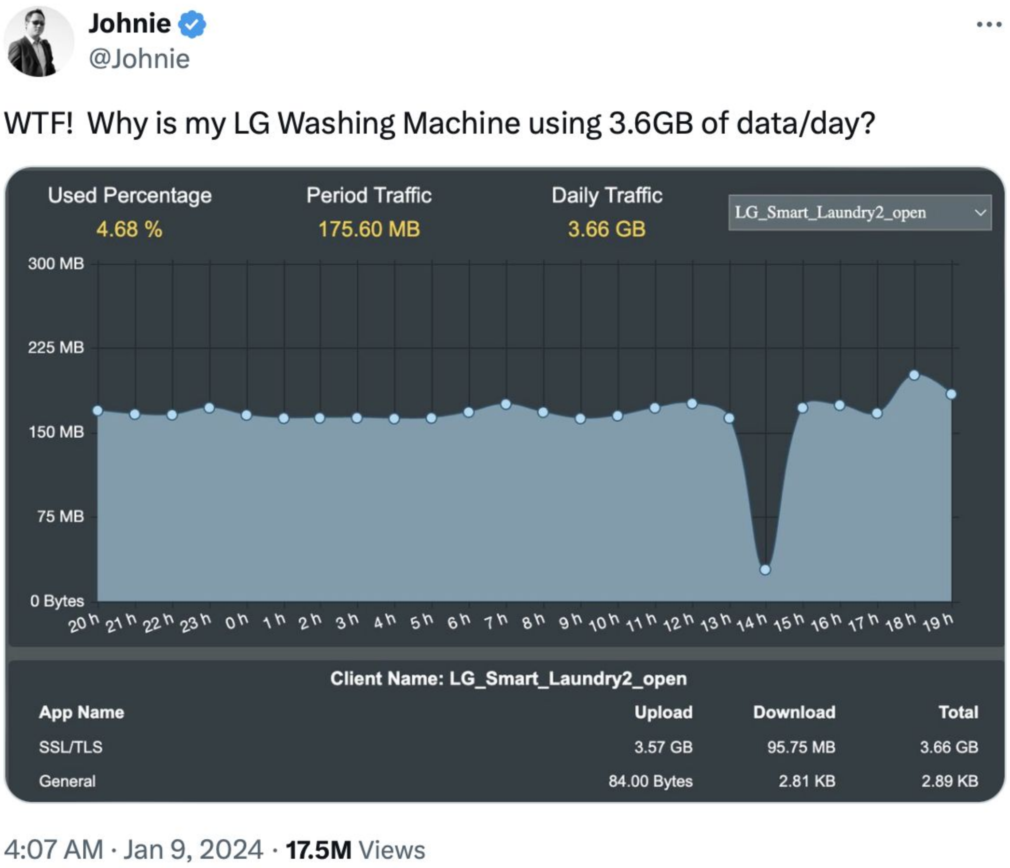


Today’s DDoS

2020s

- Broadband subscribers *love* IoT devices and (multi-)gigabit FTTH uplinks…

- … and so do botnet DDoS operators.



Johnie
@Johnie

WTF! Why is my LG Washing Machine using 3.6GB of data/day?

Used Percentage	Period Traffic	Daily Traffic
4.68 %	175.60 MB	3.66 GB

LG_Smart_Laundry2_open

Client Name: LG_Smart_Laundry2_open

App Name	Upload	Download	Total
SSL/TLS	3.57 GB	95.75 MB	3.66 GB
General	84.00 Bytes	2.81 KB	2.89 KB

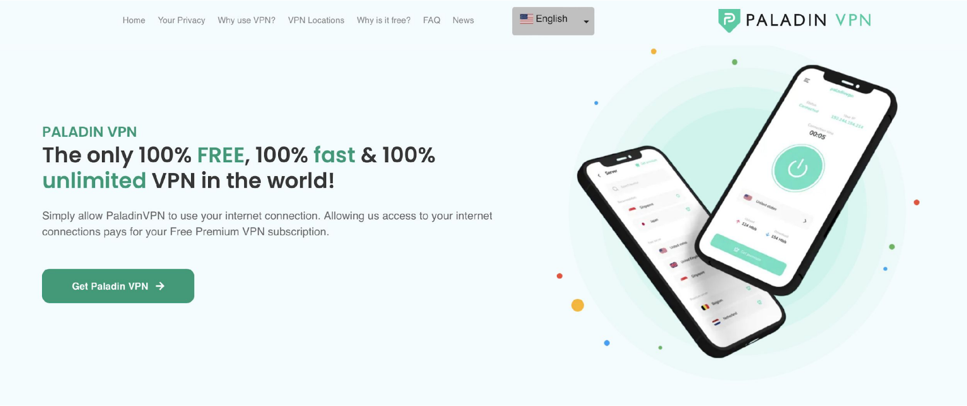
4:07 AM · Jan 9, 2024 · **17.5M** Views

Today’s DDoS

2023+

- People also like free VPNs
- Which often provide backdoor access to subscriber devices as proxy with a “clean” IP reputation
- Initially used for spam, credit card fraud, credential stuffing, click-fraud, buying sneakers, and **more recently: DDoS**

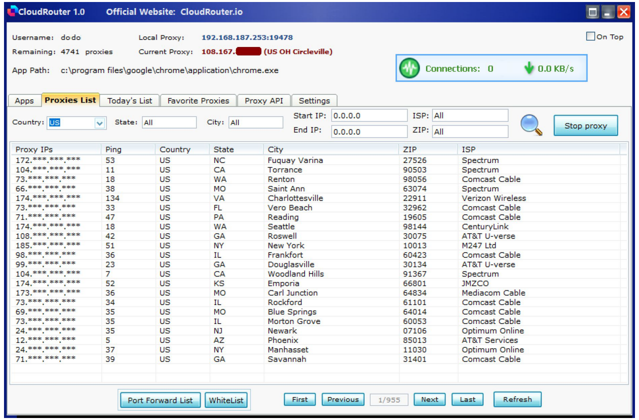
Source: https://spur.us/cloudrouter-911-proxy-resurrected/



PALADIN VPN

The only 100% FREE, 100% fast & 100% unlimited VPN in the world!

Simply allow PaladinVPN to use your internet connection. Allowing us access to your internet connections pays for your Free Premium VPN subscription.



Username: dodo
Remaining: 4741 proxies
Local Proxy: 192.168.187.253:19478
Current Proxy: 108.167.[redacted] (US OH Circleville)
App Path: c:\program files\google\chrome\application\chrome.exe
Connections: 0 0.0 KB/s

Country: US State: All City: All Start IP: 0.0.0.0 End IP: 0.0.0.0 ISP: All ZIP: All

Proxy IPs	Ping	Country	State	City	ZIP	ISP
172.***.***.***	53	US	NC	Fuquay Varina	27526	Spectrum
104.***.***.***	11	US	CA	Torrance	90503	Spectrum
73.***.***.***	18	US	WA	Renton	98056	Comcast Cable
66.***.***.***	38	US	MO	Saint Ann	63074	Spectrum
174.***.***.***	134	US	VA	Charlottesville	22911	Verizon Wireless
73.***.***.***	33	US	FL	Vero Beach	32962	Comcast Cable
71.***.***.***	47	US	PA	Reading	19605	Comcast Cable
174.***.***.***	18	US	WA	Seattle	98144	CenturyLink
108.***.***.***	42	US	GA	Roswell	30075	AT&T U-verse
185.***.***.***	51	US	NY	New York	10013	M247 Ltd
98.***.***.***	36	US	IL	Frankfort	60423	Comcast Cable
99.***.***.***	23	US	GA	Douglasville	30134	AT&T U-verse
104.***.***.***	7	US	CA	Woodland Hills	91367	Spectrum
174.***.***.***	52	US	KS	Emporia	66801	JMZCO
173.***.***.***	36	US	MO	Carl Junction	64834	Mediacom Cable
73.***.***.***	34	US	IL	Rockford	61101	Comcast Cable
69.***.***.***	35	US	MO	Blue Springs	64014	Comcast Cable
73.***.***.***	35	US	IL	Morton Grove	60053	Comcast Cable
24.***.***.***	35	US	NJ	Newark	07106	Optimum Online
12.***.***.***	5	US	AZ	Phoenix	85013	AT&T Services
24.***.***.***	37	US	NY	Manhasset	11030	Optimum Online
71.***.***.***	39	US	GA	Savannah	31401	Comcast Cable

How do most out-of-band DDoS solutions detect DDoS attacks?

Steps usually required to configure DDoS detection

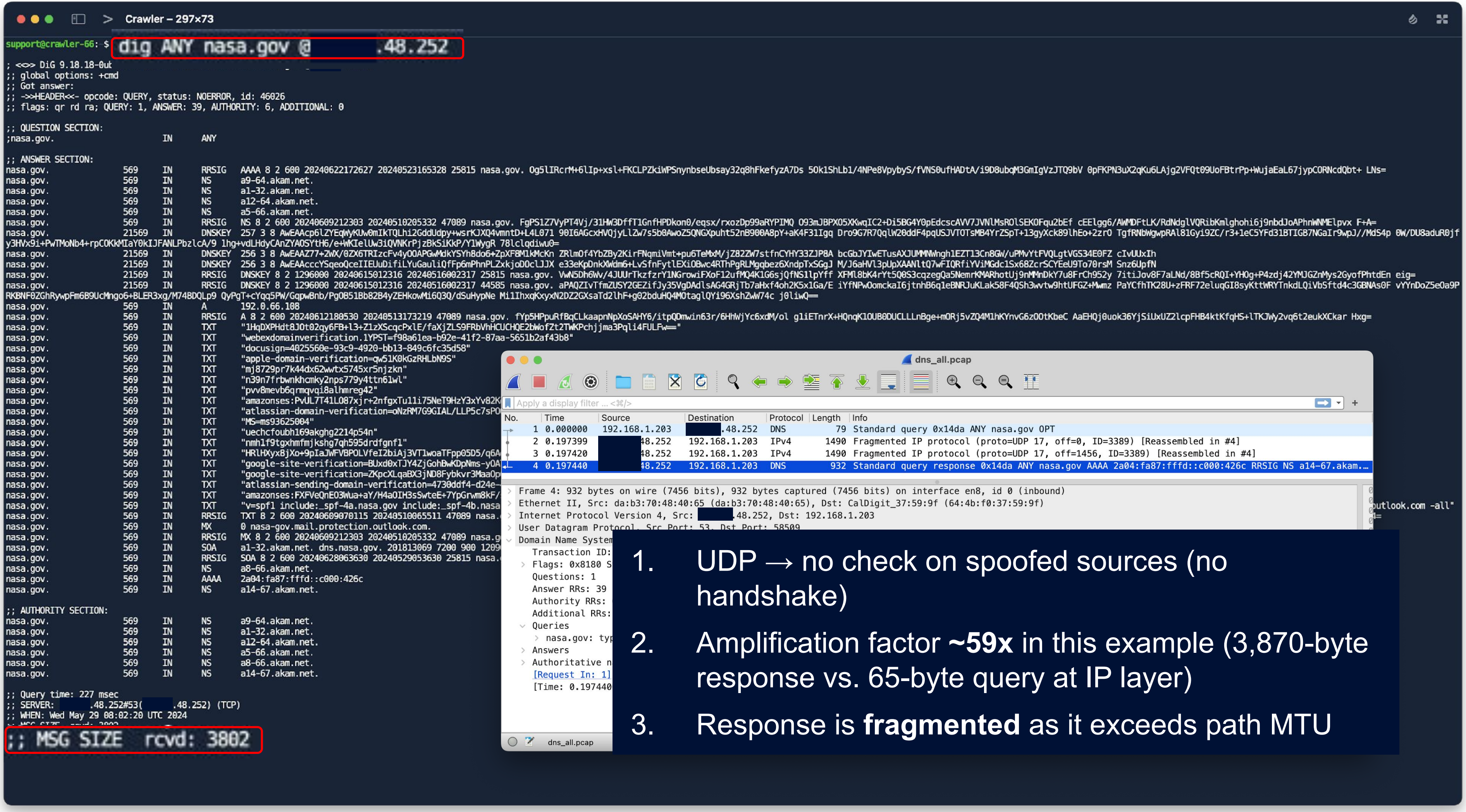
Misuse Type | Trigger Rate | High Severity Ra

- chargen Amplification (bps) | 250 Mbps | Mbps
- chargen Amplification (pps) | 25 Kpps | 50 K
- CLDAP Amplification (bps) | 250 Mbps | 500 Mbps
- CLDAP Amplification (pps) | 25 Kpps | 50 Kpps
- DNS | 10 Kpps | 30 Kpps
- DNS Amplification (bps) | 250 Mbps | 500 Mbps
- DNS Amplification (pps) | 25 Kpps | 50 Kpps
- ICMP | 5 Kpps | 10 Kpps
- IP Fragment | 25 Kpps | 50 Kpps
- IP Private | 5 Kpps | 10 Kpps
- IPy4 Protocol 0 | 5 Kpps | 10 Kpps
- L2TP (bps) | 25 Mbps | 50 Mbps
- L2TP (pps) | 25 Kpps | 50 Kpps

- mDNS (bps) | 25 Mbps | 50 Mbps
- NS (pps) | 25 Kpps | 50 Kpps
- ched Amplification (bps) | 25
- mplification (p
- MS bps | 500 Mbps
- MS SQL R | 25 Kpps | 50 Kpps
- NetBIO ps
- Net
- (bps) | 2 bps
- ation (pps) | 25 K
- ps) | 25 Mbps | 50 Mbps
- 1 (pps) | 25 Kpps | 50 Kpps

- bind (bps) | 25 Mbps | 50 Mbps
- bind (pps) | 25 Kpps | 50 Kpps
- SNMP Amplification (bps) | 25 Mbps | 50 Mbps
- SNMP Amplification (pps) | 25 Kpps | 50 Kpps
- SSDP Amplification (bps) | 250 Mbps | 500 Mbps
- SSDP Amplification (pps) | 25 Kpps | 50 Kpps
- TCP null | 1.5 Kpps | 20 Kpps
- TCP RST | 1.5 Kpps | 20 Kpps
- TCP SYN | 1.5 Kpps | 20 Kpps
- TCP SYN/ACK Amplification (bps) | 125 Mbps | 150 Mbps
- TCP SYN/ACK Amplification (pps) | 125 Kpps | 150 Kpps
- UDP | 30 Kpps | 400 Kpps

Protecting against amplification **attacks**



```
support@crawler-66: $ dig ANY nasa.gov @[redacted].48.252

; <<>> DiG 9.18.18-0ub
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46026
;; flags: qr rd ra; QUERY: 1, ANSWER: 39, AUTHORITY: 6, ADDITIONAL: 0

;; QUESTION SECTION:
;nasa.gov.                      IN      ANY

;; ANSWER SECTION:
nasa.gov.               569     IN      RRSIG   AAAA 8 2 600 20240622172627 20240523165328 25815 nasa.gov. Og5lIRcrM+6lIp+xsl+FKCLPZkiWPSnynbseUbsay32q8hFkefyzA7Ds 5Ok1ShLb1/4NPe8VpybyS/fVNS0ufHADtA/i9D8ubqM3GmIgVzJTQ9bV 0pFKPN3uX2qKu6LAjg2VFQt09UoFBtrPp+WujaEaL67jypCORNcdQbt+ LNs=
nasa.gov.               569     IN      NS      a9-64.akam.net.
nasa.gov.               569     IN      NS      a1-32.akam.net.
nasa.gov.               569     IN      NS      a12-64.akam.net.
nasa.gov.               569     IN      NS      a5-66.akam.net.
nasa.gov.               569     IN      RRSIG   NS 8 2 600 20240609212303 20240510205332 47089 nasa.gov. FgPS1Z7VyPT4Vj/31HW3DffT1GnfHPDkon0/eqsx/rxozDp99aRYPIMQ O93mJBPXO5XKwqIC2+Di5BG4Y0pEdcscAVV7JVNlMsROlSEKOFqu2bEf cEElgg6/AWMDFtLK/RdNdglVQRibKmlghohi6j9nbdJoAPhnWNMElpvx F+A=
nasa.gov.               21569   IN      DNSKEY  257 3 8 AwEAAcp6lZYEqWyKUw0mIkTQLhi2GddUdpy+wsrKJXQ4vmntD+L4L071 90I6AGcxHVQjyLlZw7s5b0AwoZ5QNGXpuht52nB900A8pY+aK4F31Igq Dro9G7R7QqlW20ddF4pqUSJVTOTsMB4YrZSpT+13gyXck89lhEo+2zrO TgfRNbWgwpRAl81Gyi9ZC/r3+1eC5YFd31BTIGB7NGaIr9wpJ//MdS4p 0W/DU8aduR0jf
y3HVx9i+PwTMoNb4+rpCOKkMIaY0kIJFANLPbzlcA/9 1hg+vdLHdyCAnZYA0SYtH6/e+WKIelUw3iQVNKrPjzBkSiKkP/Y1WygR 78lclqdiwu0=
nasa.gov.               21569   IN      DNSKEY  256 3 8 AwEAAZ77+2WX/0ZX6TRIzcFv4yO0APGwMdkYSYh8do6+ZpXF8M1kMcKn ZRlmOf4YbZBy2KirFNqmiVmt+pu6TeMxM/jZ82ZW7stfnCYHY33ZJP8A bcGbJYIwETusAXJUMMNWngh1EZT13Cn8GW/uPMvYtFVQLgtVGS34E0FZ cIvUUxIh
nasa.gov.               21569   IN      DNSKEY  256 3 8 AwEAAcccYSqeoQceIIEUuDifiLYuGauliQfFp6mPhnPLZxkjoDOclJJX e33eKpDnkXWdm6+LvSfnFytlEXiOBwc4RThPgRLMgqbez6XndpTxSGgJ M/J6aHVl3pUpXAANltQ7wFIQRfiYViMGdc1Sx68ZcrSCYEeU9To70rsM Snz6UpfN
nasa.gov.               21569   IN      RRSIG   DNSKEY 8 2 1296000 20240615012316 20240516002317 25815 nasa.gov. VwN5Dh6Wv/4JUUrTkzfzrY1NGrowiFXoF12ufMQ4K1G6sjQfNS1lpYff XFMl8bK4rYt5Q0S3cqzegQa5NemrKMARhotUj9nMMnDkY7u8FrCh952y 7itiJov8F7aLNd/8Bf5cRQI+YH0g+P4zdj42YMJGZnMys2GyofPhtdEn eig=
nasa.gov.               21569   IN      RRSIG   DNSKEY 8 2 1296000 20240615012316 20240516002317 44585 nasa.gov. aPAQZIvTfmZUSY2GEZifJy35VgDAdlsAG4GRjTb7aHxf4oh2K5x1Ga/E iYfNPw0omckaI6jtnhB6q1eBNRJuKLak58F4QSh3wvtw9htUFGZ+Mwmz PaYCfhTK28U+zFRF72eluqGI8syKttWRYTnkdLQiVbSftd4c3GBNAs0F vYYnDoZ5e0a9P
RKBNF0ZGhRywpFm6B9UcMngo6+BLER3xg/M74BDQLp9 QyPgT+cYqq5PW/GqpwBnb/Pg0B51Bb82B4yZEHkowMi6Q3Q/dSuHypNe Mi1IhxqKxyxN2DZ2GXsaTd2lhF+g02bduHQ4M0taglQYi96XshZwW74c j0liwQ==
nasa.gov.               569     IN      A       192.0.66.108
nasa.gov.               569     IN      RRSIG   A 8 2 600 20240612180530 20240513173219 47089 nasa.gov. fYp5HPpuRfBqCLkaapnNpXoSAHY6/itpQDmwin63r/6HhWjYc6xdM/ol gliETnrX+HQnqK1OUB0DUCLLLnBge+mORj5vZQ4M1hKYnvG6zO0tKbeC AaEHQj0uok36YjSiUxUZ2lcpFHB4ktKfqHS+lTKJWy2vq6t2eukXCkar Hxg=
nasa.gov.               569     IN      TXT     "1HqDXPHdt8JOt02qy6FB+l3+Z1zXScqcPxlE/faXjZLS9FRbVhHCUCHQE2bWofZt2TWKPchjjma3Pqli4FULFw=="
nasa.gov.               569     IN      TXT     "webexdomainverification.1YPST=f98a61ea-b92e-41f2-87aa-5651b2af43b8"
nasa.gov.               569     IN      TXT     "docusign=4025560e-93c9-4920-bb13-849c6fc35d58"
nasa.gov.               569     IN      TXT     "apple-domain-verification=qw51K0kGzRHLbN9S"
nasa.gov.               569     IN      TXT     "mj8729pr7k44dx62wwtx5745xr5njzkn"
nasa.gov.               569     IN      TXT     "n39n7frbwnkhcmky2nps779y4ttn61wl"
nasa.gov.               569     IN      TXT     "pvv8mevb6qrmqvqi8alhmreg42"
nasa.gov.               569     IN      TXT     "amazonses:PvUL7T41L087xjr+2nfgxTu11i75NeT9HzY3xYv82K
nasa.gov.               569     IN      TXT     "atlassian-domain-verification=oNzRM7G9GIAL/LLP5c7sPO
nasa.gov.               569     IN      TXT     "MS=ms93625004"
nasa.gov.               569     IN      TXT     "uechcfoubh169akghg2214p54n"
nasa.gov.               569     IN      TXT     "nmh1f9tgxhmfmjkshg7qh595drdfgnfl"
nasa.gov.               569     IN      TXT     "HRlHXyx8jXo+9pIaJWFVBPOLVfeI2biAj3VT1woaTFpp05D5/q6A
nasa.gov.               569     IN      TXT     "google-site-verification=BUxd0xTJY4ZjGohBwKDpNms-yOA
nasa.gov.               569     IN      TXT     "google-site-verification=ZKpcXLqaBX3jND8Fybkvr3MaaOp
nasa.gov.               569     IN      TXT     "atlassian-sending-domain-verification=4730ddf4-d24e-
nasa.gov.               569     IN      TXT     "amazonses:FXFVeQnEO3Wua+aY/H4aOIH3sSwteE+7YpGrwm8kF/
nasa.gov.               569     IN      TXT     "v=spf1 include:_spf-4a.nasa.gov include:_spf-4b.nasa                                                                        outlook.com -all"
nasa.gov.               569     IN      RRSIG   TXT 8 2 600 20240609070115 20240510065511 47089 nasa.                                                                         =
nasa.gov.               569     IN      MX      0 nasa-gov.mail.protection.outlook.com.
nasa.gov.               569     IN      RRSIG   MX 8 2 600 20240609212303 20240510205332 47089 nasa.g
nasa.gov.               569     IN      SOA     a1-32.akam.net. dns.nasa.gov. 201813069 7200 900 1209
nasa.gov.               569     IN      RRSIG   SOA 8 2 600 20240628063630 20240529053630 25815 nasa.
nasa.gov.               569     IN      NS      a8-66.akam.net.
nasa.gov.               569     IN      AAAA    2a04:fa87:fffd::c000:426c
nasa.gov.               569     IN      NS      a14-67.akam.net.

;; AUTHORITY SECTION:
nasa.gov.               569     IN      NS      a9-64.akam.net.
nasa.gov.               569     IN      NS      a1-32.akam.net.
nasa.gov.               569     IN      NS      a12-64.akam.net.
nasa.gov.               569     IN      NS      a5-66.akam.net.
nasa.gov.               569     IN      NS      a8-66.akam.net.
nasa.gov.               569     IN      NS      a14-67.akam.net.

;; Query time: 227 msec
;; SERVER: [redacted].48.252#53([redacted].48.252) (TCP)
;; WHEN: Wed May 29 08:02:20 UTC 2024
;; MSG SIZE  rcvd: 3802
```

```
No.  Time      Source          Destination     Protocol Length Info
  1  0.000000  192.168.1.203   [redacted].48.252  DNS     79  Standard query 0x14da ANY nasa.gov OPT
  2  0.197399  [redacted]48.252   192.168.1.203   IPv4  1490  Fragmented IP protocol (proto=UDP 17, off=0, ID=3389) [Reassembled in #4]
  3  0.197420  [redacted]48.252   192.168.1.203   IPv4  1490  Fragmented IP protocol (proto=UDP 17, off=1456, ID=3389) [Reassembled in #4]
  4  0.197440  [redacted]48.252   192.168.1.203   DNS    932  Standard query response 0x14da ANY nasa.gov AAAA 2a04:fa87:fffd::c000:426c RRSIG NS a14-67.akam.…
```

```
> Frame 4: 932 bytes on wire (7456 bits), 932 bytes captured (7456 bits) on interface en8, id 0 (inbound)
> Ethernet II, Src: da:b3:70:48:40:65 (da:b3:70:48:40:65), Dst: CalDigit_37:59:9f (64:4b:f0:37:59:9f)
> Internet Protocol Version 4, Src: [redacted].48.252, Dst: 192.168.1.203
> User Datagram Protocol, Src Port: 53, Dst Port: 58509
v Domain Name System
    Transaction ID:
  > Flags: 0x8180 S
    Questions: 1
    Answer RRs: 39
    Authority RRs:
    Additional RRs:
  v Queries
    > nasa.gov: typ
  > Answers
  > Authoritative n
    [Request In: 1]
    [Time: 0.197440
```

1. UDP → no check on spoofed sources (no handshake)
2. Amplification factor **~59x** in this example (3,870-byte response vs. 65-byte query at IP layer)
3. Response is **fragmented** as it exceeds path MTU

Fast protection against amplification attacks

Why amplification?

- While relatively basic, DNS amplification is still a very popular attack vector
  - In short-lived attacks (e.g., gaming) as more than enough to congest a residential connection
  - As complement in more complex attacks (to fill pipes while other vectors can target in-line appliances or application servers)
  - (and unlike more esoteric UDP services like TFTP or QOTD, DNS is still somewhat useful for most subscribers)

`dns_port_combo` detection rule

- Secure Genome rules are expressed with the **Deepfield Model Language**.
- Some of the traffic from this attack matches:
  - Protocol **UDP**, and
  - Source port **53**, and
  - Destination ports **22** or **23** or **53** or…
- Straightforward as only operates on 5-tuple metadata

```
(df['protocol'] == 17) &

(df['port.src'].isin([53])) &

(df['port.dst'].isin([22,23,53
,80,110,161,427,443]))
```

dns_amplifier_fragment detection rule

- Slightly more complex as this relies on **Genome context for the source IPs**
- Some of the traffic from this attack matches:
  - Protocol **UDP**, and
  - Source port **0**, and
  - Source IP is **known as a DNS amplifier**
  - Source IP is <u>not</u> part of major public DNS resolvers, DNS root servers, main DNS gTLD/ccTLD servers, and major authoritative nameservers
- Additional criteria with source cardinality (per /24 destination)

```
(df['protocol'] == 17) &

(df['port.src'].isin([0])) &

(df['genome.src'].isin([
GENOME_AMPLIFIER_DNS ])) &

(~df['genome.src'].isin([
GENOME_PUBLIC_DNS,
GENOME_DNS_ROOT, GENOME_DNS_GTLD,
GENOME_DNS_CCTLD,
GENOME_DNS_NAMESERVERS ]))
```

Deepfield Secure Genome

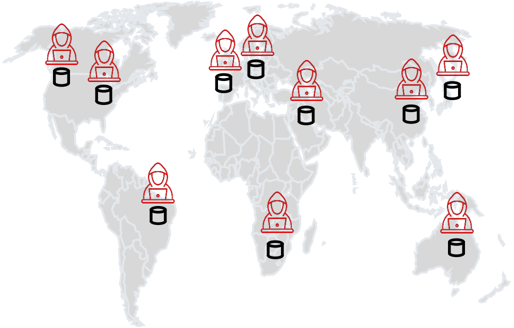
AI powered "DDoS threat map" of the Internet

Internet-wide security context

- **Crawling** over 5 billion IPv4+IPv6 addresses scanned and categorizing Ports, UDP-based reflectors, applications, device type, CVEs, etc.
- DDoS samples – **from GDTA** customers and honeypots
- Open and commercial data feeds

Up-to-date visibility into:

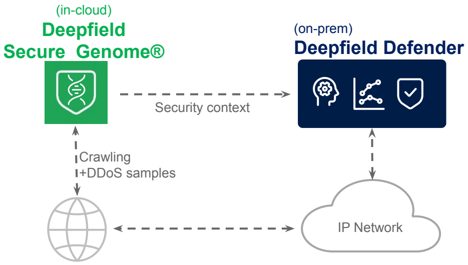
- DDoS vectors and details
- Botnets and residential proxies
- Known/open reflectors
- Booter & spoofed fingerprints
- IoT device details
- Device software versions and CVEs



Knowing the Bad actors

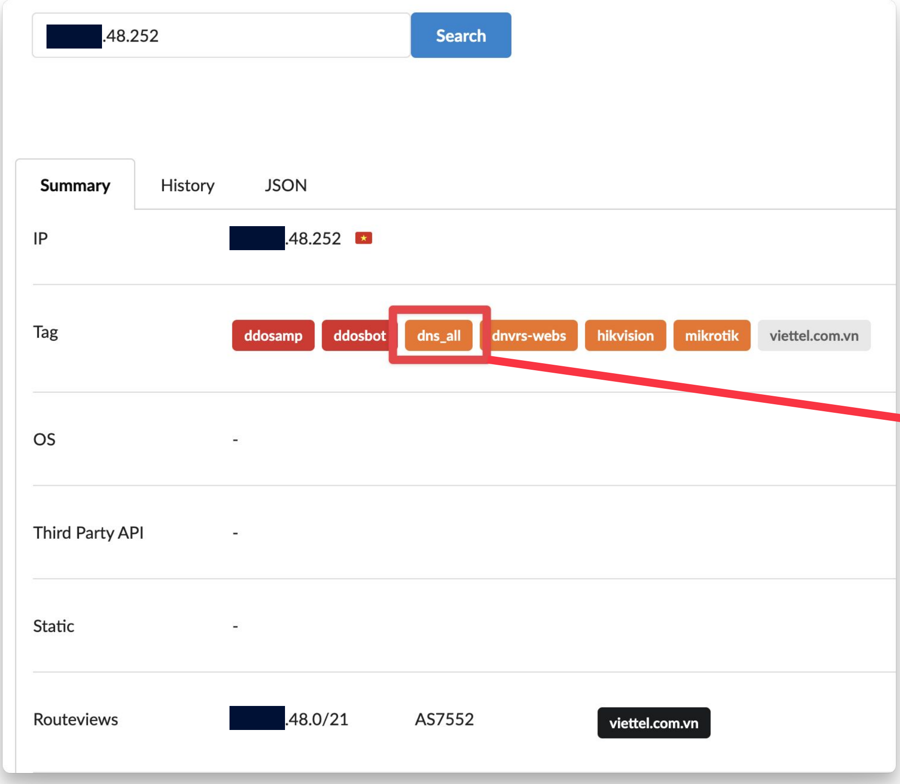
Supervised learning + model training for Defender

- DDoS Detection Engine
- DDoS Mitigation Compiler Engine



Fast protection against amplification attacks

Amplification 101



[redacted].48.252 Search

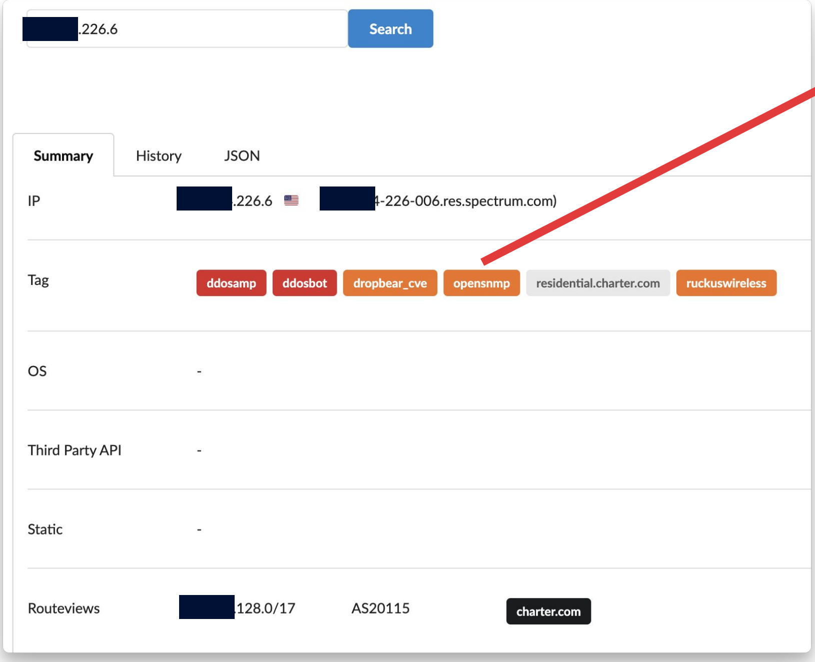
Summary History JSON

IP	[redacted].48.252 🇻🇳		
Tag	ddosamp ddosbot dns_all dnvrs-webs hikvision mikrotik viettel.com.vn		
OS	-		
Third Party API	-		
Static	-		
Routeviews	[redacted].48.0/21	AS7552	viettel.com.vn

```
dig ANY nasa.gov @[redacted].48.252
```

Why Genome awareness

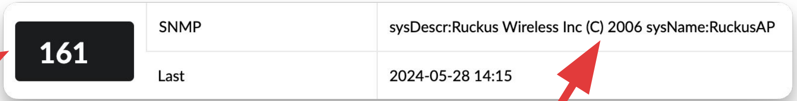
Reflector/amplifier awareness



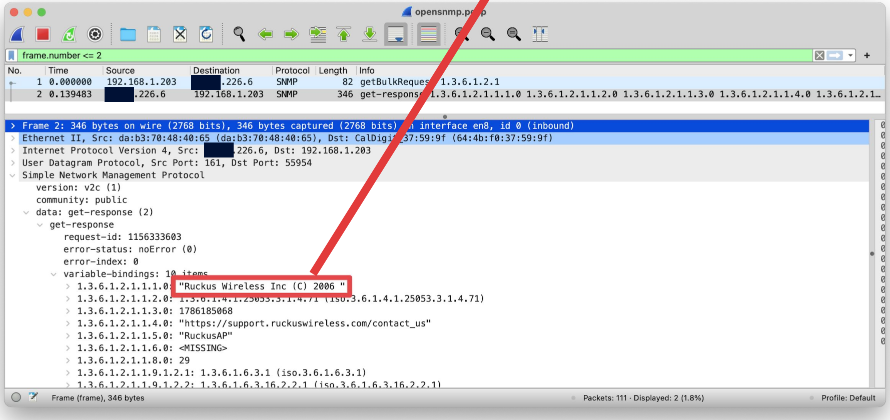
[redacted].226.6 Search

Summary | History | JSON

IP	[redacted].226.6 🇺🇸	[redacted]-226-006.res.spectrum.com)	
Tag	ddosamp ddosbot dropbear_cve opensnmp residential.charter.com ruckuswireless		
OS	-		
Third Party API	-		
Static	-		
Routeviews	[redacted]128.0/17	AS20115	charter.com



161	SNMP	sysDescr:Ruckus Wireless Inc (C) 2006 sysName:RuckusAP
	Last	2024-05-28 14:15



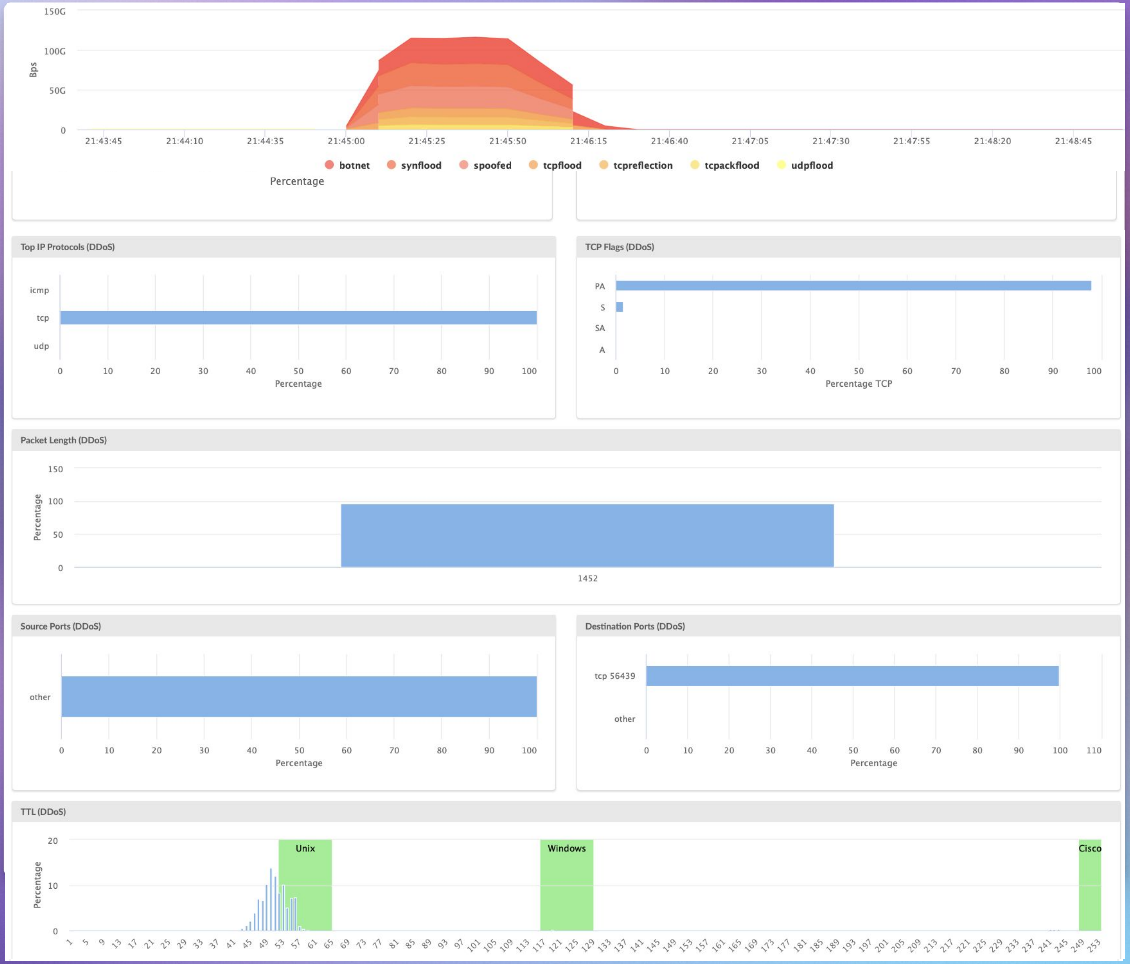
```
frame.number <= 2

No.  Time       Source          Destination     Protocol Length Info
   1 0.000000   192.168.1.203   [redacted].226.6    SNMP       82 getBulkReques 1.3.6.1.2.1
   2 0.139483   [redacted].226.6    192.168.1.203   SNMP      346 get-respons 1.3.6.1.2.1.1.1.0 1.3.6.1.2.1.1.2.0 1.3.6.1.2.1.1.3.0 1.3.6.1.2.1.1.4.0 1.3.6.1.2.1…

> Frame 2: 346 bytes on wire (2768 bits), 346 bytes captured (2768 bits) n interface en8, id 0 (inbound)
> Ethernet II, Src: da:b3:70:48:40:65 (da:b3:70:48:40:65), Dst: CalDigi 37:59:9f (64:4b:f0:37:59:9f)
> Internet Protocol Version 4, Src: [redacted].226.6, Dst: 192.168.1.203
> User Datagram Protocol, Src Port: 161, Dst Port: 55954
v Simple Network Management Protocol
    version: v2c (1)
    community: public
  v data: get-response (2)
    v get-response
        request-id: 1156333603
        error-status: noError (0)
        error-index: 0
      v variable-bindings: 10 items
        > 1.3.6.1.2.1.1.1.0: "Ruckus Wireless Inc (C) 2006 "
        > 1.3.6.1.2.1.1.2.0: 1.3.6.1.4.1.25053.3.1.4.71 (iso.3.6.1.4.1.25053.3.1.4.71)
        > 1.3.6.1.2.1.1.3.0: 1786185068
        > 1.3.6.1.2.1.1.4.0: "https://support.ruckuswireless.com/contact_us"
        > 1.3.6.1.2.1.1.5.0: "RuckusAP"
        > 1.3.6.1.2.1.1.6.0: <MISSING>
        > 1.3.6.1.2.1.1.8.0: 29
        > 1.3.6.1.2.1.1.9.1.2.1: 1.3.6.1.6.3.1 (iso.3.6.1.6.3.1)
        > 1.3.6.1.2.1.1.9.1.2.2: 1.3.6.1.6.3.16.2.2.1 (iso.3.6.1.6.3.16.2.2.1)

Frame (frame), 346 bytes          Packets: 111 · Displayed: 2 (1.8%)          Profile: Default
```

Protecting against Botnet-based **attacks**

Attack Profile

Botnet TCP

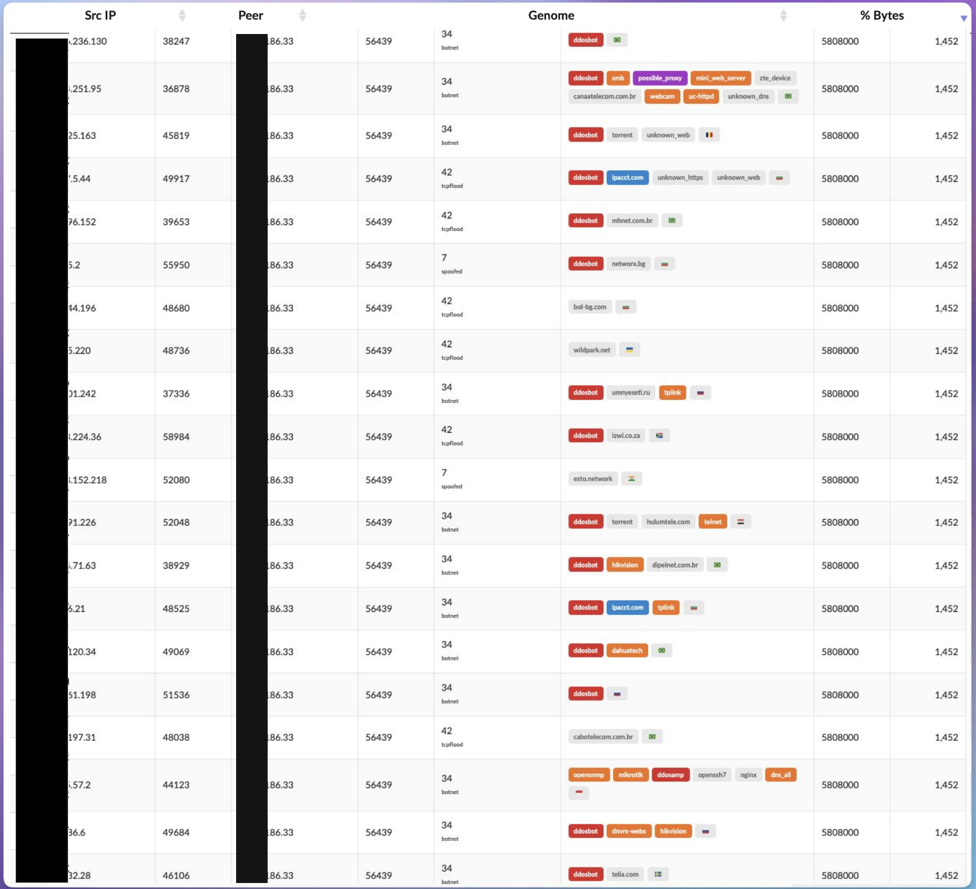
- **4K** sources
- **117 Gbps** / **16Mpps** in original attack
- Attack vectors:
  - Botnet TCP
- Randomized source ports
- Large packet length
- Topologically-close bots



Attack Profile #4

Botnet TCP random

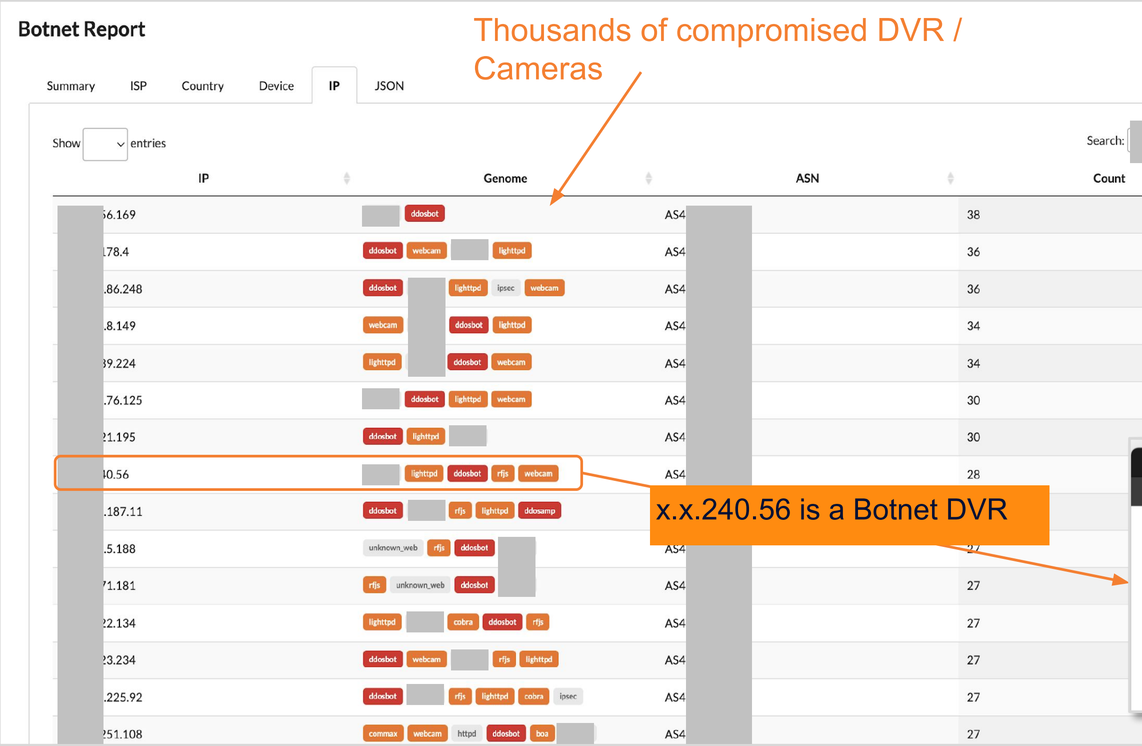
- Mix of webcams/DVRs, routers (TP-Link, Intelbras, ZTE, etc.)



Src IP		Peer			Genome	% Bytes	
[redacted].236.130	38247	[redacted]86.33	56439	34 botnet	ddosbot 🇧🇷	5808000	1,452
[redacted].251.95	36878	[redacted]86.33	56439	34 botnet	ddosbot smb possible_proxy mini_web_server zte_device canaatelecom.com.br webcam uc-httpd unknown_dns 🇧🇷	5808000	1,452
[redacted]25.163	45819	[redacted]86.33	56439	34 botnet	ddosbot torrent unknown_web 🇷🇴	5808000	1,452
[redacted].5.44	49917	[redacted]86.33	56439	42 tcpflood	ddosbot ipacct.com unknown_https unknown_web 🇧🇬	5808000	1,452
[redacted]96.152	39653	[redacted]86.33	56439	42 tcpflood	ddosbot mhnet.com.br 🇧🇷	5808000	1,452
[redacted]5.2	55950	[redacted]86.33	56439	7 spoofed	ddosbot networx.bg 🇧🇬	5808000	1,452
[redacted]44.196	48680	[redacted]86.33	56439	42 tcpflood	bol-bg.com 🇧🇬	5808000	1,452
[redacted]5.220	48736	[redacted]86.33	56439	42 tcpflood	wildpark.net 🇺🇦	5808000	1,452
[redacted]01.242	37336	[redacted]86.33	56439	34 botnet	ddosbot umnyeseti.ru tplink 🇷🇺	5808000	1,452
[redacted].224.36	58984	[redacted]86.33	56439	42 tcpflood	ddosbot izwi.co.za 🇿🇦	5808000	1,452
[redacted].152.218	52080	[redacted]86.33	56439	7 spoofed	esto.network 🇮🇳	5808000	1,452
[redacted]91.226	52048	[redacted]86.33	56439	34 botnet	ddosbot torrent hulumtele.com telnet 🇪🇬	5808000	1,452
[redacted].71.63	38929	[redacted]86.33	56439	34 botnet	ddosbot hikvision dipelnet.com.br 🇧🇷	5808000	1,452
[redacted].21	48525	[redacted]86.33	56439	34 botnet	ddosbot ipacct.com tplink 🇧🇬	5808000	1,452
[redacted]120.34	49069	[redacted]86.33	56439	34 botnet	ddosbot dahuatech 🇧🇷	5808000	1,452
[redacted]61.198	51536	[redacted]86.33	56439	34 botnet	ddosbot 🇷🇺	5808000	1,452
[redacted]197.31	48038	[redacted]86.33	56439	42 tcpflood	cabotelecom.com.br 🇧🇷	5808000	1,452
[redacted].57.2	44123	[redacted]86.33	56439	34 botnet	opensnmp mikrotik ddosamp openssh7 nginx dns_all 🇮🇩	5808000	1,452
[redacted]36.6	49684	[redacted]86.33	56439	34 botnet	ddosbot dnvrs-webs hikvision 🇷🇺	5808000	1,452
[redacted]32.28	46106	[redacted]86.33	56439	34 botnet	ddosbot telia.com 🇸🇪	5808000	1,452

Example botnet info in Deepfield Secure Genome

Active DDoS botnet IP’s over last days

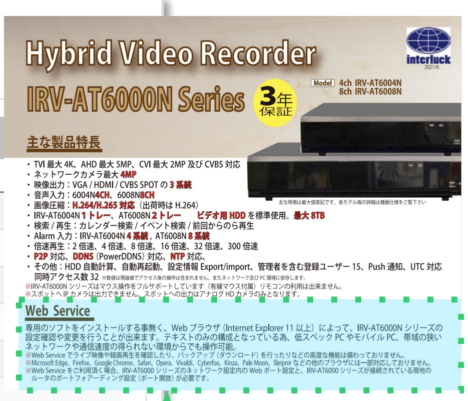


Botnet Report

IP	Genome	ASN	Count
[redacted]56.169	[redacted] ddosbot	AS4[redacted]	38
[redacted]178.4	ddosbot webcam [redacted] lighttpd	AS4[redacted]	36
[redacted].86.248	ddosbot [redacted] lighttpd ipsec webcam	AS4[redacted]	36
[redacted].8.149	webcam [redacted] ddosbot lighttpd	AS4[redacted]	34
[redacted]39.224	lighttpd [redacted] ddosbot webcam	AS4[redacted]	34
[redacted].76.125	[redacted] ddosbot lighttpd webcam	AS4[redacted]	30
[redacted]21.195	ddosbot lighttpd [redacted]	AS4[redacted]	30
[redacted]40.56	[redacted] lighttpd ddosbot rfjs webcam	AS4[redacted]	28
[redacted].187.11	ddosbot [redacted] rfjs lighttpd ddosamp	AS4[redacted]	
[redacted].5.188	unknown_web rfjs ddosbot [redacted]	AS4[redacted]	27
[redacted]71.181	rfjs unknown_web ddosbot [redacted]	AS4[redacted]	27
[redacted]22.134	lighttpd [redacted] cobra ddosbot rfjs	AS4[redacted]	27
[redacted]23.234	ddosbot webcam [redacted] rfjs lighttpd	AS4[redacted]	27
[redacted].225.92	ddosbot [redacted] rfjs lighttpd cobra ipsec	AS4[redacted]	27
[redacted]251.108	commax webcam httpd ddosbot boa [redacted]	AS4[redacted]	27

Thousands of compromised DVR / Cameras

x.x.240.56 is a Botnet DVR



interluck
2021/6
3年保証

Hybrid Video Recorder

IRV-AT6000N Series

Model 4ch IRV-AT6004N
8ch IRV-AT6008N

主な製品特長

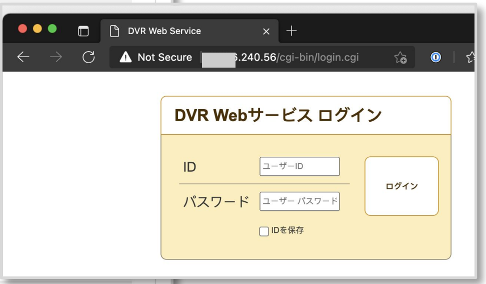
- TVI 最大 4K、AHD 最大 5MP、CVI 最大 2MP 及び CVBS 対応
- ネットワークカメラ最大 4MP
- 映像出力：VGA / HDMI / CVBS SPOT の 3 系統
- 音声入力：6004N4CH、6008N8CH
- 画像圧縮：H.264/H.265 対応（出荷時は H.264）
- IRV-AT6004N 1 トレー、AT6008N 2 トレー　ビデオ用 HDD を標準使用。最大 8TB
- 検索 / 再生：カレンダー検索 / イベント検索 / 前回からのら再生
- Alarm 入力：IRV-AT6004N 4 系統，AT6008N 8 系統
- 倍速再生：2 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 同時アクセス数 32 ※数値は理論値でアクセス後の操作は含まれません。またネットワーク及び PC 環境に依存します。

主な特徴は最大値表記です。各モデル毎の詳細は機器仕様をご覧下さい

※IRV-AT6000N シリーズはマウス操作をフルサポートしています（有線マウス付属）リモコンの利用は出来ません。
※スポットへ IP カメラは出力できません。スポットへの出力はアナログ HD カメラのみとなります。

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得られな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）を行ったり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、Kinza、Pale Moon、Sleipnir などの他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-AT6000 シリーズのネットワーク設定内の Web ポート設定と、IRV-AT6000 シリーズが接続されている現地のルータのポートフォアーディング設定（ポート開放）が必要です。



[redacted].240.56/cgi-bin/login.cgi

DVR Webサービス ログイン

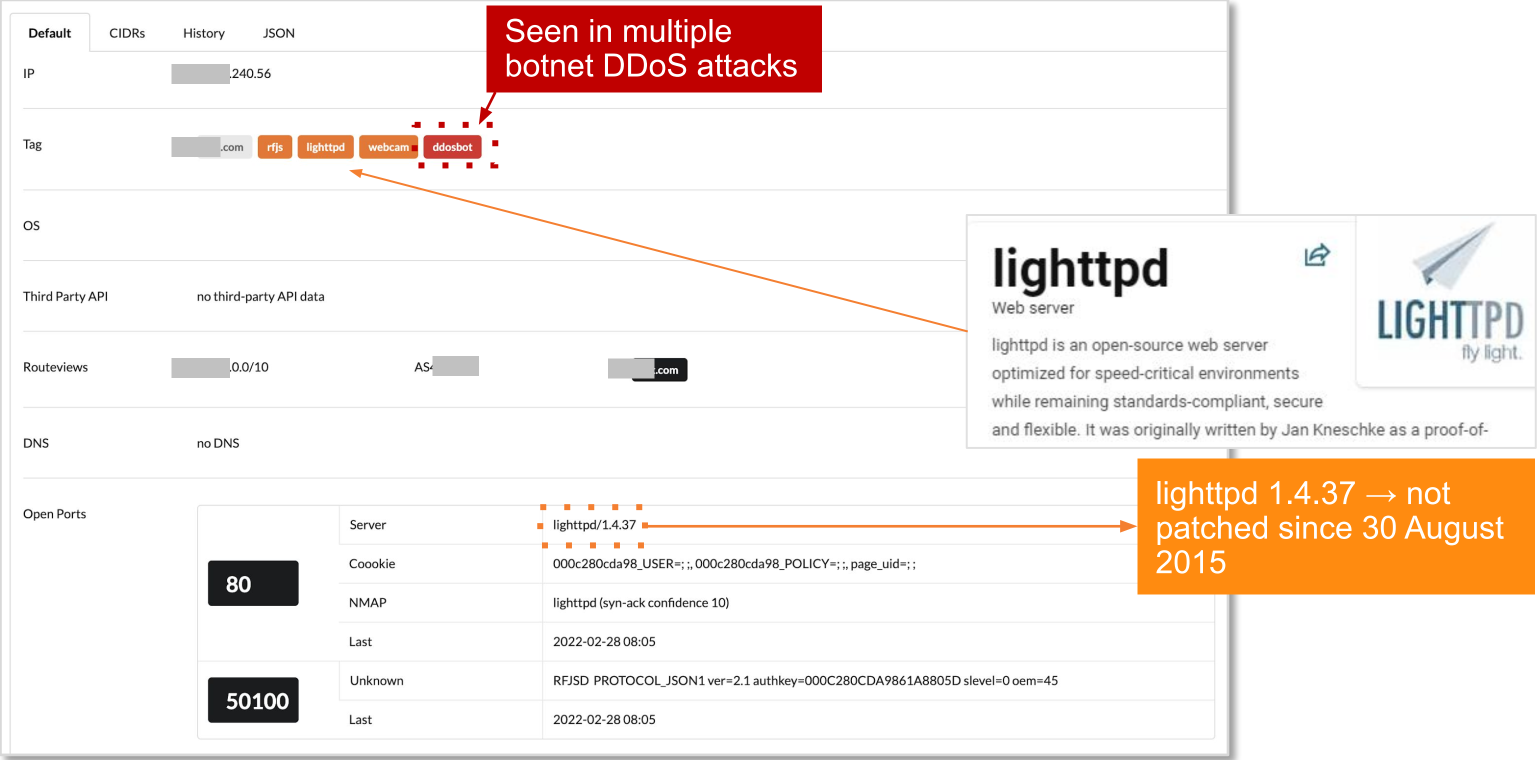
ID ユーザーID

パスワード ユーザー パスワード

□ IDを保存

Example bot info in Deepfield Secure Genome

What does Secure Genome know about this botnet DVR?



Default CIDRs History JSON

IP [redacted].240.56

Tag [redacted].com rfjs lighttpd webcam ddosbot

OS

Third Party API no third-party API data

Routeviews [redacted].0.0/10 AS[redacted] [redacted].com

DNS no DNS

Open Ports

Port		
80	Server	lighttpd/1.4.37
	Coookie	000c280cda98_USER=; ;, 000c280cda98_POLICY=; ;, page_uid=; ;
	NMAP	lighttpd (syn-ack confidence 10)
	Last	2022-02-28 08:05
50100	Unknown	RFJSD PROTOCOL_JSON1 ver=2.1 authkey=000C280CDA9861A8805D slevel=0 oem=45
	Last	2022-02-28 08:05

Seen in multiple botnet DDoS attacks

lighttpd

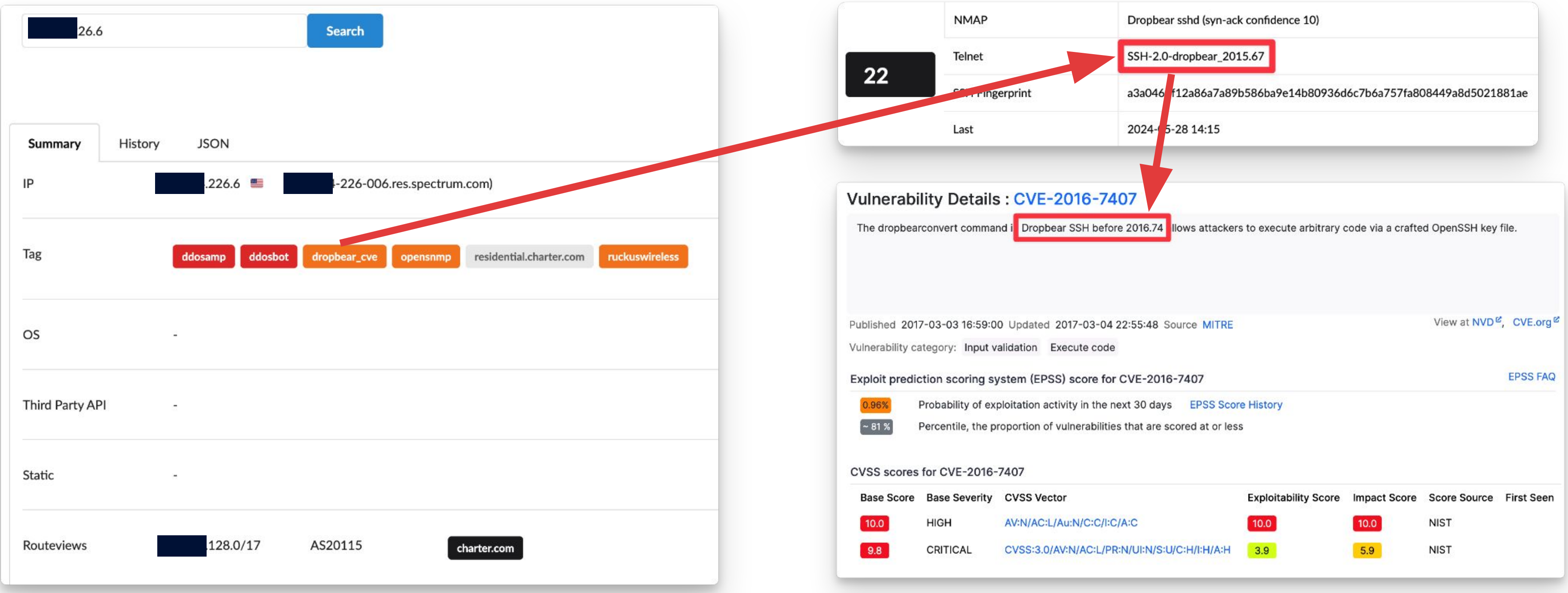
Web server

lighttpd is an open-source web server optimized for speed-critical environments while remaining standards-compliant, secure and flexible. It was originally written by Jan Kneschke as a proof-of-

lighttpd 1.4.37 → not patched since 30 August 2015

Example bot info in Deepfield Secure Genome

CVE awareness to assess risk even before we see the IPs/device in attacks



[redacted]26.6 Search

Summary History JSON

IP	[redacted].226.6 🇺🇸 [redacted]-226-006.res.spectrum.com)
Tag	ddosamp ddosbot dropbear_cve opensnmp residential.charter.com ruckuswireless
OS	-
Third Party API	-
Static	-
Routeviews	[redacted]128.0/17 AS20115 charter.com

22	NMAP	Dropbear sshd (syn-ack confidence 10)
	Telnet	SSH-2.0-dropbear_2015.67
	SSH Fingerprint	a3a046 f12a86a7a89b586ba9e14b80936d6c7b6a757fa808449a8d5021881ae
	Last	2024- 5-28 14:15

Vulnerability Details : CVE-2016-7407

The dropbearconvert command i Dropbear SSH before 2016.74 llows attackers to execute arbitrary code via a crafted OpenSSH key file.

Published 2017-03-03 16:59:00 Updated 2017-03-04 22:55:48 Source MITRE View at NVD, CVE.org

Vulnerability category: Input validation Execute code

Exploit prediction scoring system (EPSS) score for CVE-2016-7407 EPSS FAQ

0.96%	Probability of exploitation activity in the next 30 days	EPSS Score History
~ 81 %	Percentile, the proportion of vulnerabilities that are scored at or less	

CVSS scores for CVE-2016-7407

Base Score	Base Severity	CVSS Vector	Exploitability Score	Impact Score	Score Source	First Seen
10.0	HIGH	AV:N/AC:L/Au:N/C:C/I:C/A:C	10.0	10.0	NIST	
9.8	CRITICAL	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	3.9	5.9	NIST	

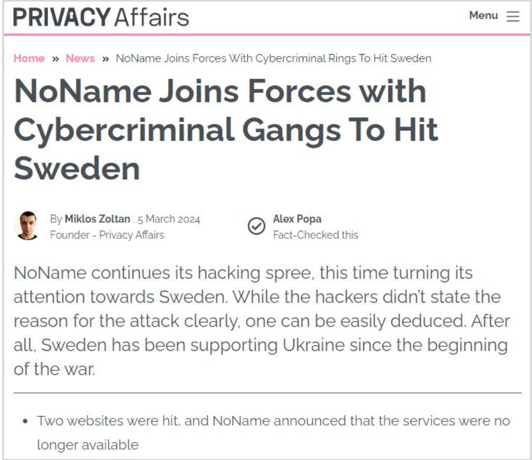
Benefits of ML-based detection

- Thresholds-based detection primarily relies on 5-tuple measurements: **imprecise** because you need to **guess** what is an “acceptable” value
  - **High false-positive rate** (flash crowd events, sudden changes of traffic patterns, etc.)
  - **High false-negative rate**, especially with botnet-based traffic (which can look like legitimate traffic)
  - Thresholds are different per customer type (and change over time!)

- Through ML techniques, Genome **enriches** flows in real-time, and adds additional context/signal:
  - Fragmented traffic is unusual but is safe to drop if we know it originates from DNS servers that we know are used for amplification attacks
  - Similarly (as we will see later), it’s easier to feel more confident to drop UDP traffic if we see it originates from 150 similar webcams and directed to a subscriber IP
- This provides much more **accuracy** (and **explainability**)

Protecting against Proxy-based **attacks**

State-sponsored DDoS attacks



PRIVACY Affairs

Menu

Home » News » NoName Joins Forces With Cybercriminal Rings To Hit Sweden

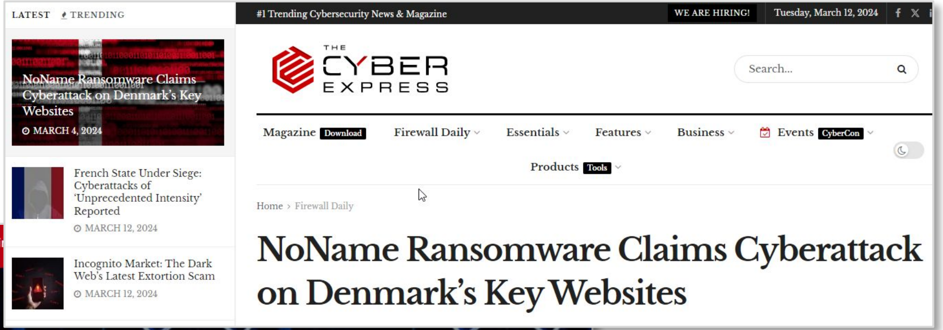
NoName Joins Forces with Cybercriminal Gangs To Hit Sweden

By Miklos Zoltan . 5 March 2024
Founder - Privacy Affairs

Alex Popa
Fact-Checked this

NoName continues its hacking spree, this time turning its attention towards Sweden. While the hackers didn't state the reason for the attack clearly, one can be easily deduced. After all, Sweden has been supporting Ukraine since the beginning of the war.

- Two websites were hit, and NoName announced that the services were no longer available

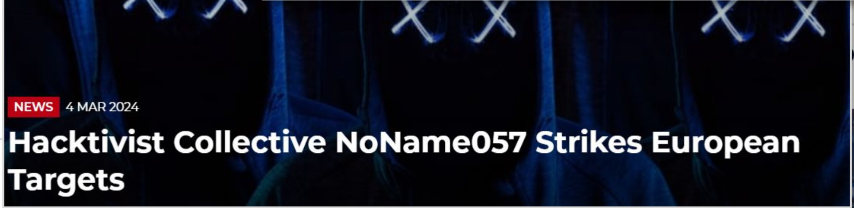


NoName Ransomware Claims Cyberattack on Denmark's Key Websites
MARCH 4, 2024

French State Under Siege: Cyberattacks of 'Unprecedented Intensity' Reported
MARCH 12, 2024

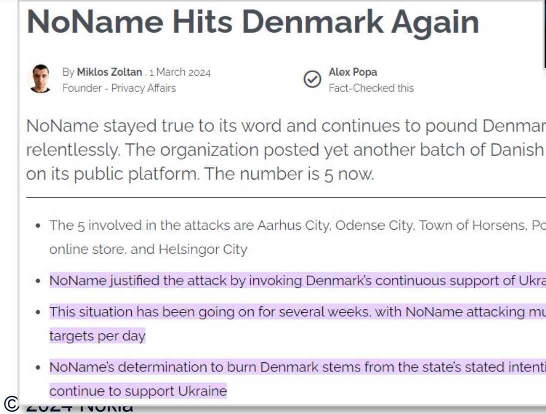
Incognito Market: The Dark Web's Latest Extortion Scam
MARCH 12, 2024

NoName Ransomware Claims Cyberattack on Denmark's Key Websites



NEWS 4 MAR 2024

Hacktivist Collective NoName057 Strikes European Targets



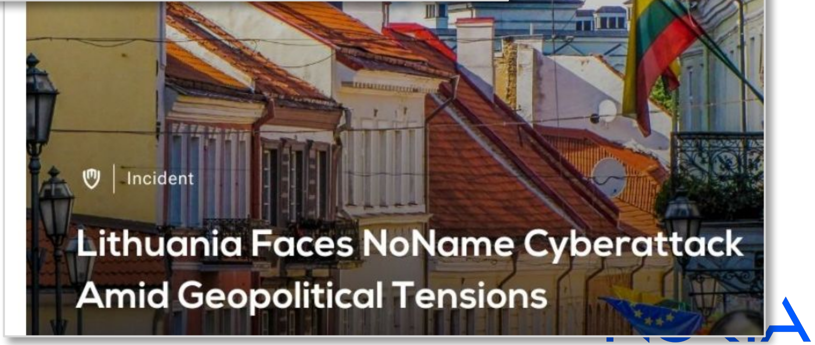
NoName Hits Denmark Again

By Miklos Zoltan . 1 March 2024
Founder - Privacy Affairs

Alex Popa
Fact-Checked this

NoName stayed true to its word and continues to pound Denmark relentlessly. The organization posted yet another batch of Danish victims on its public platform. The number is 5 now.

- The 5 involved in the attacks are Aarhus City, Odense City, Town of Horsens, Postnord online store, and Helsingor City
- NoName justified the attack by invoking Denmark's continuous support of Ukraine
- This situation has been going on for several weeks, with NoName attacking multiple Danish targets per day
- NoName's determination to burn Denmark stems from the state's stated intention to continue to support Ukraine



Incident

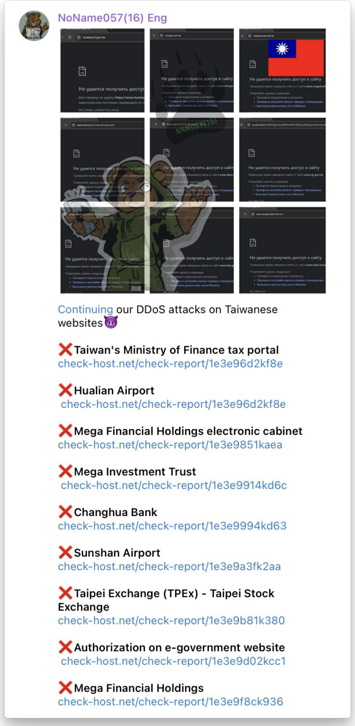
Lithuania Faces NoName Cyberattack Amid Geopolitical Tensions

Threat actor & primary attack type

- Conducts DDoS attacks against various websites from organizations (both governmental and private)
- Uses Telegram channels to claim responsibility for attacks, issue threats, and share tools like their custom DDoS software “DDoSia”
- Developed a cryptocurrency payment system to reward contributors (volunteer-based system as opposed to malware/exploitation)
- Attacks primarily rely on Web DDoS, i.e. **crafted HTTPS GET/POST requests that can overwhelm a server even with a relatively low number of sources/requests**

This attack type presents multiple challenges:

- **Low number of sources**
- **Low bps/pps**
- **TLS-encrypted**
- Using **valid parameters** (URI endpoint, headers, etc.)
- **Not originating directly from known botnets** (but from residential proxies)



NoName057(16) Eng

Continuing our DDoS attacks on Taiwanese websites😈

❌**Taiwan's Ministry of Finance tax portal**
check-host.net/check-report/1e3e96d2kf8e

❌**Hualian Airport**
check-host.net/check-report/1e3e96d2kf8e

❌**Mega Financial Holdings electronic cabinet**
check-host.net/check-report/1e3e9851kaea

❌**Mega Investment Trust**
check-host.net/check-report/1e3e9914kd6c

❌**Changhua Bank**
check-host.net/check-report/1e3e9994kd63

❌**Sunshan Airport**
check-host.net/check-report/1e3e9a3fk2aa

❌**Taipei Exchange (TPEx) - Taipei Stock Exchange**
check-host.net/check-report/1e3e9b81k380

❌**Authorization on e-government website**
check-host.net/check-report/1e3e9d02kcc1

❌**Mega Financial Holdings**
check-host.net/check-report/1e3e9f8ck936

https://t.me/noname05716eng/4294

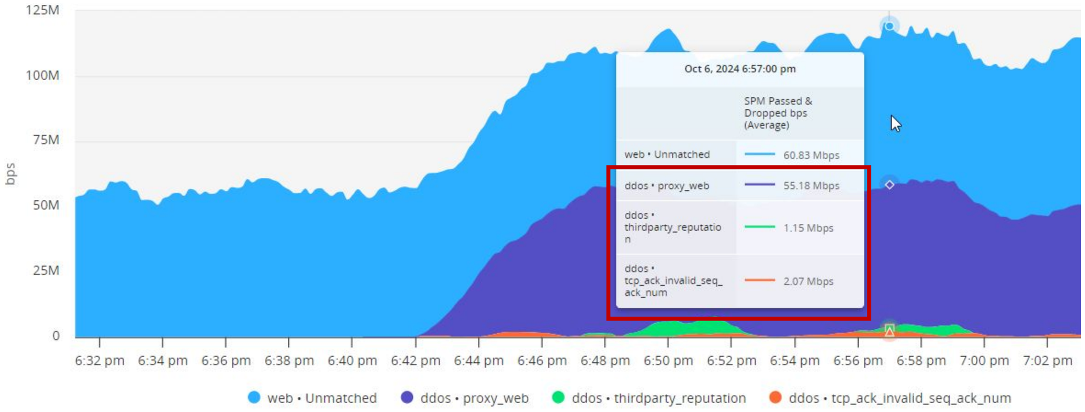
How to detect and protect?

Typical response from NoName targets is to enforce a **geo-block**

Problems with geo-blocking approach:

- attack traffic sourced from **residential proxies** across the world
- Large proportion attack traffic from **European countries,** Significant % attack **sourced from within country**

□ **Better approach** is to add awareness of residential proxies for network traffic flows to detect these anomalies



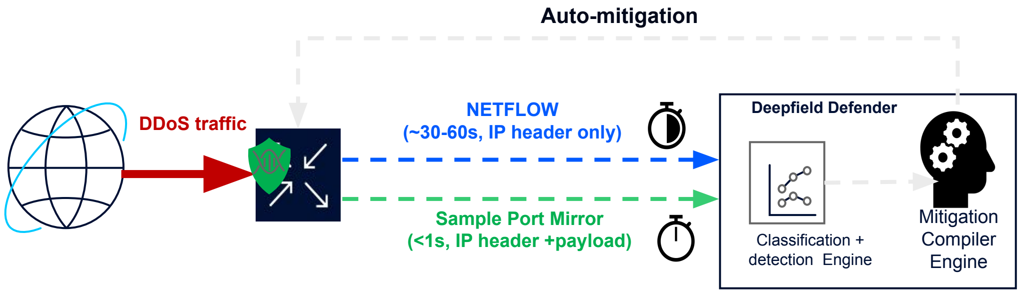
Oct 6, 2024 6:57:00 pm

	SPM Passed & Dropped bps (Average)
web • Unmatched	60.83 Mbps
ddos • proxy_web	55.18 Mbps
ddos • thirdparty_reputation	1.15 Mbps
ddos • tcp_ack_invalid_seq_ack_num	2.07 Mbps

Faster Detection

Ultra-fast detection and mitigation with streamed traffic samples

Sampled Port Mirroring (SPM) – or IPFIX 315

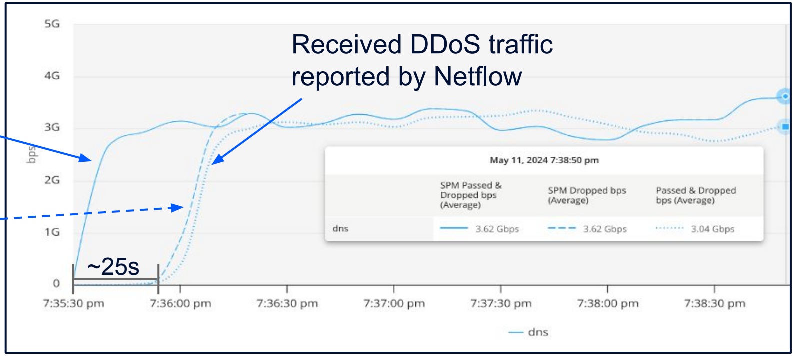

Auto-mitigation
DDoS traffic
NETFLOW
(~30-60s, IP header only)
Sample Port Mirror
(<1s, IP header +payload)
Deepfield Defender
Classification + detection Engine
Mitigation Compiler Engine

SPM based detection:

- Eliminates flow-cache induced delay due to router flow-cache inherent to Netflow
- □ Attack dropped in less than 30 seconds
- Enables advanced detection using full header & payload

Received DDoS traffic reported by SPM

Dropped DDoS traffic (reported by SPM)

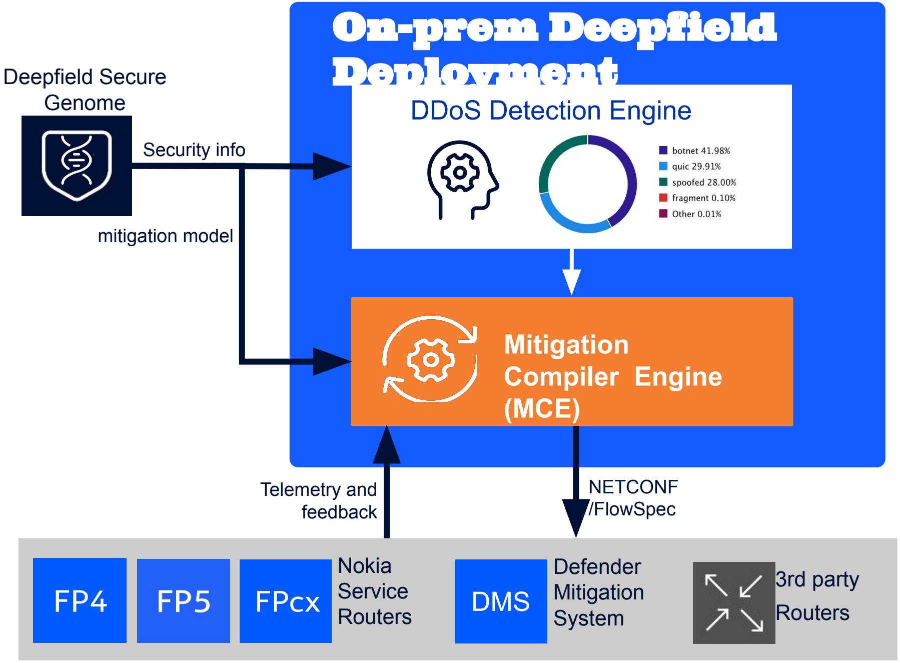


Deepfield solution architecture

(Brief) recap

Defender mitigates attacks using the most efficient strategy

For the observed attack and the deployed hardware



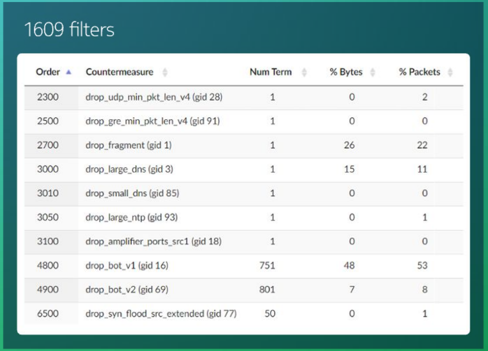
Mitigation Compiler Engine

The **intelligence** to build in real-time the AI optimized mitigation strategy

- Using Deepfield Secure Genome ML models trained on real-world attack samples
- Compiles surgical filters and countermeasures for deployed hardware
- Effective against all known DDoS and emerging vectors

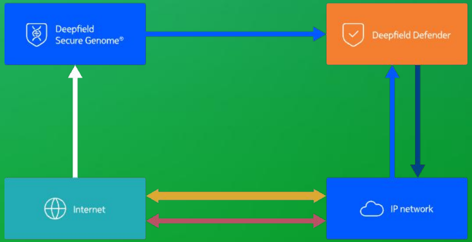
NOKIA

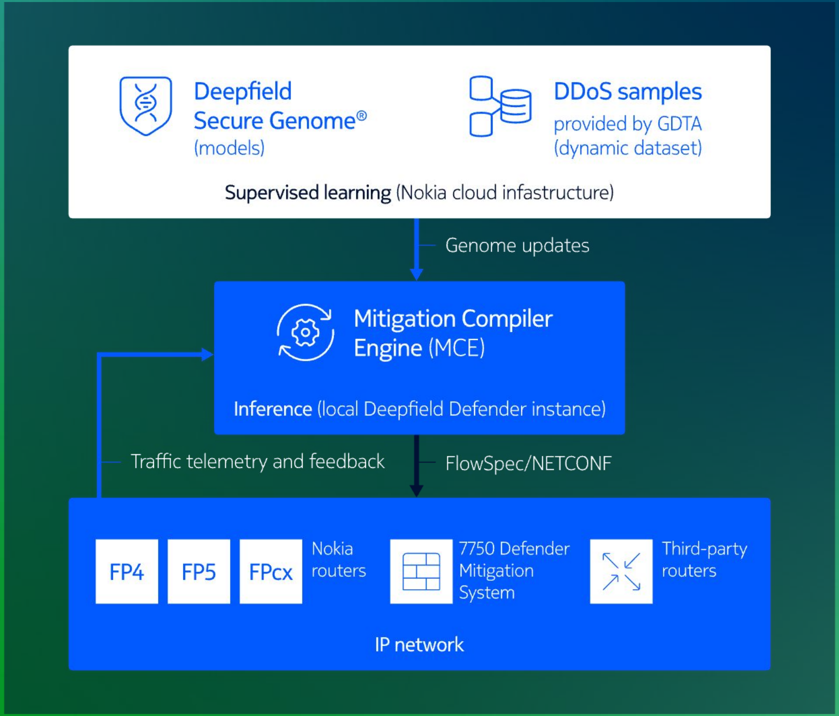
ML-based network-optimized mitigation



1609 filters

Order	Countermeasure	Num Term	% Bytes	% Packets
2300	drop_udp_min_pkt_len_v4 (gid 28)	1	0	2
2500	drop_gre_min_pkt_len_v4 (gid 91)	1	0	0
2700	drop_fragment (gid 1)	1	26	22
3000	drop_large_dns (gid 3)	1	15	11
3010	drop_small_dns (gid 85)	1	0	0
3050	drop_large_ntp (gid 93)	1	0	1
3100	drop_amplifier_ports_src1 (gid 18)	1	0	0
4800	drop_bot_v1 (gid 16)	751	48	53
4900	drop_bot_v2 (gid 69)	801	7	8
6500	drop_syn_flood_src_extended (gid 77)	50	0	1





Deepfield Secure Genome® (models)

DDoS samples provided by GDTA (dynamic dataset)

Supervised learning (Nokia cloud infastructure)

Genome updates

Mitigation Compiler Engine (MCE)

Inference (local Deepfield Defender instance)

Traffic telemetry and feedback

FlowSpec/NETCONF

FP4 FP5 FPcx Nokia routers

7750 Defender Mitigation System

Third-party routers

IP network

< 30 sec

Mitigation Compiler Engine (MCE)

- Inference from Deepfield Secure Genome ML models (trained on 10K+ real-world attack samples)
- Generates optimized mitigation strategies for complex DDoS attacks
- Effective against known DDoS and emerging vectors

Nokia Deepfield GDTA

- **Global DDoS Threat Alliance**
- **Opt-in membership**
- **Sharing information about threats for improved protection against the latest DDoS threats as they emerge**