

Aktualne trendy w atakach DDoS – perspektywa izraelska

Andrzej Sienkiewicz

Sales Engineer @ Radware

CSO Council, 23.11.23



Web DDoS Tsunami – the new weapon in cyberwarfare



- The flows are **encrypted** *Invisible to anti-DDoS appliances*
- Each flow **looks like legitimate traffic** *Go right through WAF protections*
- Utilize **ultra-high RPS rate** *Overwhelming web servers, backend databases, etc.*
- Generated from **large Botnets** *Rate limiting is ineffective*
- Use multiple **evasion techniques** *e.g., Randomization (of HTTP Method, Headers, Cookies, referrer, UA and more), IP (XFF) Spoofing, open headless browser to harvest application cookies, anonymous proxies, ...*

It all started with the Russians...



- The Russian DDoS attack campaign started as soon as the war begun
- The attacks disrupted critical resources of the Ukrainian Government
- Radware was urgently called to protect Ukraine
- The attack campaign peaked at only 400Gbps, but employed relatively sophisticated attack vectors, including **application layer DDoS attacks**

FORTUNE SEARCH SIGN IN [Subscribe Now](#)

Most Popular

Airbnb's CEO: More than 1 million people have visited our job page since announcing permanent 'work from anywhere' policy

Here's what's open (and closed) on Memorial Day 2022

TECH • UKRAINE INVASION

Russian cyberattacks could soon strike the West, analysts say. 'The risk right now is high and rising'

BY DAVID MEYER
February 24, 2022 7:04 PM GMT-2

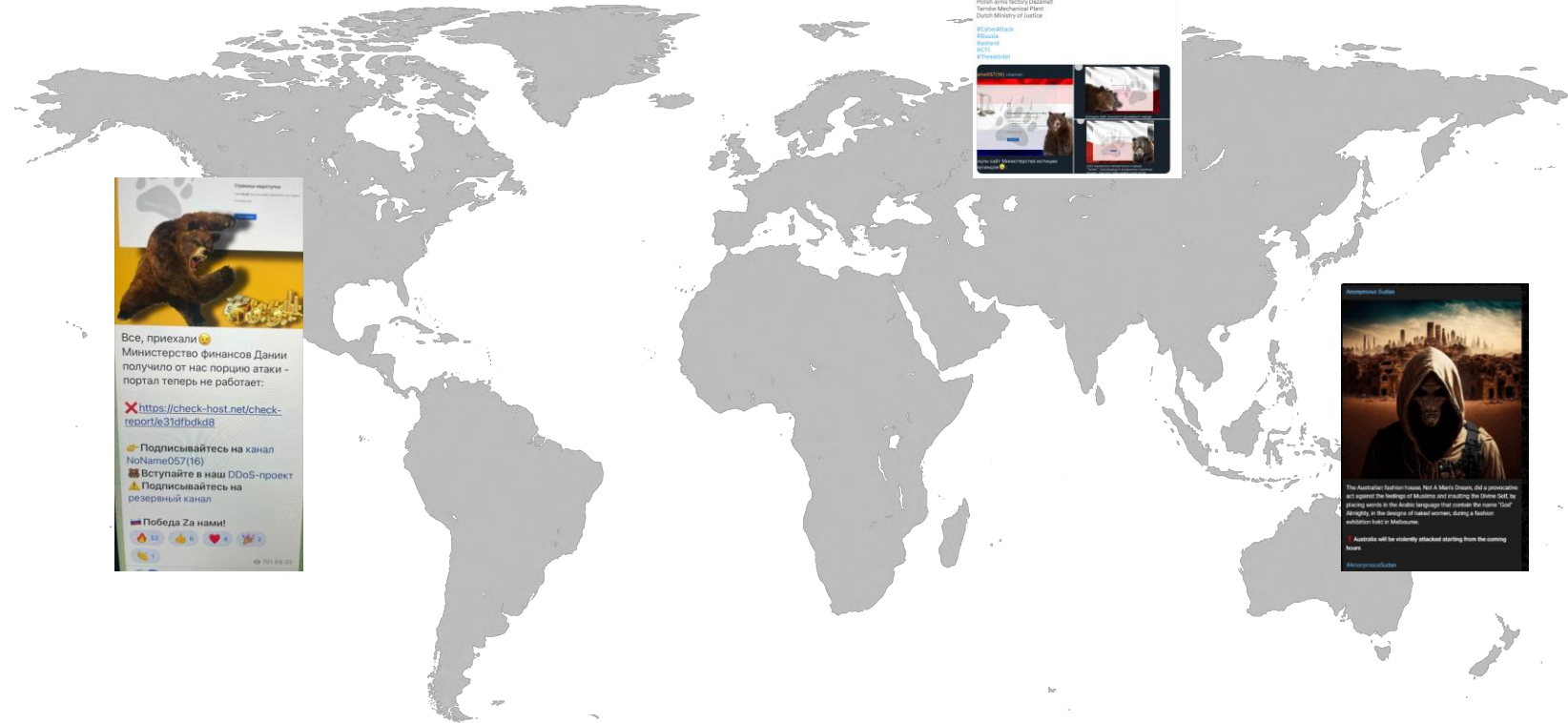
On Wednesday, before Putin [declared war](#) and the bombing began, distributed denial-of-service (DDoS) attacks [pummeled the websites](#) of Ukraine's Defense Ministry and one of its major commercial banks, PrivatBank. Such attacks flood the victim's servers with connection requests, causing them to seize up as they would if millions of genuine people tried to log on at once.

Now they are Everywhere!




HTTP/s Flood attack campaigns in the last months on assets in:

- *The US*
- *Canada*
- *Germany*
- *Poland*
- *The UK*
- *India*
- *Israel*
- *Australia*
- *Scandinavia*
- ...



Attack on SAS: Application-layer DDoS Campaign (HTTP/s Floods)

Anonymous Sudan
Forwarded from Anonymous Sudan



Infrastructure: The Danish education sector was brought down by the burning of the Quran

- <https://www.ku.dk/> | Københavns Universitet
<https://check-host.net/check-report/ec3b718k18e>
- <https://www.dtu.dk/> | Danmarks Tekniske Universitet
<https://check-host.net/check-report/ec3b761k49f>
- <https://ruc.dk/> | Roskilde Universitet
<https://check-host.net/check-report/ec3b5d7k34b>
- <https://www.en.aau.dk/> | Aalborg Universitet (AAU)
<https://check-host.net/check-report/ec3b66akcc3>
- <https://www.sdu.dk/> | Syddansk Universitet
<https://check-host.net/check-report/ec3b70ckf11>
- <https://en.itu.dk/> | IT-Universitetet i København
<https://check-host.net/check-report/ec3b66dk381>


#AnonymousSudan 2379 21:18

February 22

Anonymous Sudan
Good morning, The airports of Denmark will be our first targets. We're going to launch the attack in 30 minutes from now

#AnonymousSudan 7084 edited 07:33

Anonymous Sudan



The infrastructure of Denmark airports has been down because of their burning of the Quran

- <https://www.cph.dk/> | Copenhagen Airport
<https://check-host.net/check-report/ec0c43dk815>
- <https://aal.dk/> | Aalborg Airport
<https://check-host.net/check-report/ec0c3fakcf1>

HTTP/s Flood Attack Tools Available in the Wild



CC

- HTTP method can be random GET\POST\HEAD...
- **Randomized** HTTP headers values : accept*, referer, UA... from pre-defined list
- Custom static cookie
- Single random query args
- **Hundreds-thousands** of distinct requests
- Very few attack vectors
- Support HTTPs, HTTP Pipeline
- Use open Proxy SOCK4,5

```
//////  ////  //////////////
ccccc/  ccccc/  |CC-attack |
cc/      cc/    |-----|
cc/      cc/    |  Layer 7 |
cc/////  cc///// |  ddos tool |
cccccc/  ccccc/  |         |
```

Saphyra

- HTTP method can be random GET\POST\HEAD...
- Random HTTP headers values - accept*, UA ...
- **Randomized cookies (0,1-5)**
- **Query args are random (1-5)**
- **Random referer appearance** and values
- **Millions of distinct** requests
- Very few attack vectors
- Support HTTPs, HTTP Pipeline



MHDDoS

- Randomization... (method, headers, UA, Cookies, empty requests)
- Hundreds-thousand of distinct requests
- **Large number of attack vectors**
- **Approaches to bypass existing mitigation techniques, e.g. impersonate Google Analytics IP (X-FF) spoofing**
- Support HTTPs, HTTP Pipeline
- Use open Proxy SOCK4,5

MHDDoS

Python3, (Cyber / DDos)



Blood

- Large number of attack vectors
- Randomization... (method, headers, UA, Cookies, empty requests)
- Hundreds-thousand of distinct requests
- Approaches to bypass existing mitigation techniques, e.g. **open headless browser to harvest application cookies**, controlled cipher suite
- Support HTTPs, HTTP Pipeline
- Use open Proxy SOCK4,5



Sophistication of attacks and evasion techniques

For each tool we can find number of variants and mutations...

... and it continues with Hamas



- October-November 2023 – Operation “Iron Swords” – DDoS Attacks
- More than 500 DDoS attacks targeting various sectors have been mitigated in the last 30 days
- The volume of attacks has reached up to 1,300,000 requests per second
- The targeted sectors include media, government services, critical infrastructure, and the financial services industry

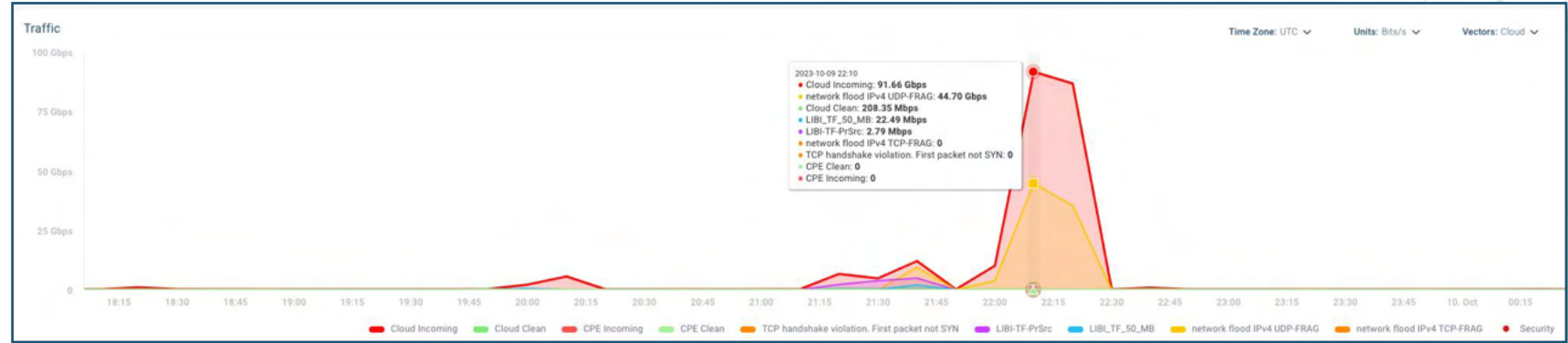
- Anonymized list of selected customers in Israel:
 - Major mass media group
 - Major news outlet
 - Bank A: one of the largest banks
 - Bank B: one of the largest banks
 - Bank C: one of the largest banks
 - Public services company
 - State-owned transport service
 - Government services
 - State-owned critical infrastructure service
 - Major transport authority

TIME

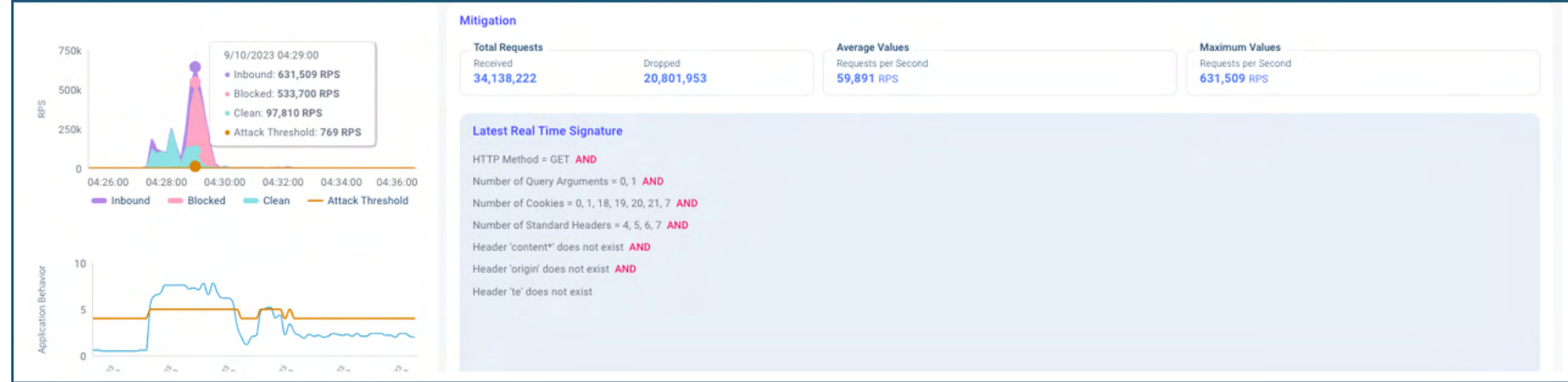
Hacking groups, including some tied to Russia, are attacking Israeli government and media websites, allying themselves with the Palestinian military group Hamas that launched a series of deadly strikes on the country over the weekend.

Source: Radware Attack Detection and Mitigation Data

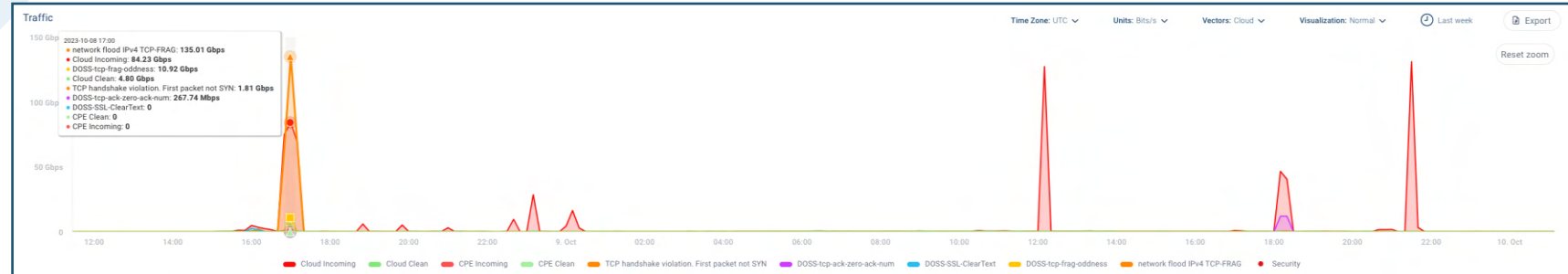
Bank A: Network Flood > 90Gbps



State-owned public service: HTTPS Flood > 650K RPS



Government service: Network Flood > 135Gbps



Source: Radware Attack Detection and Mitigation Data

Most common attack vectors observed:

- HTTPS Flood
- Network Flood IPv4 UDP
- Network Flood IPv4 UDP-FRAG
- Network Flood IPv4 ICMP
- SYN Flood HTTP
- ICMP-BlackNurse-Attack
- BO-Apache-HTTPD-log-Cookie
- DDOS-APPLE-ARMS-AMP
- DDOS-Mirai-GENUDP-flood
- DDoS-UDP-MEMCACHED-AMP
- DOSS-chargegen-reflected
- DOSS-DNS-Ref-L4-Above-3000
- DOSS-UDP-flood-80-Req
- DOSS-UDP-flood-80-Res
- DOSS-UDP-no-data
- TCP Anomalies
- TCP-FIN-ACK Flood
- DOSS-APPLE-ARMS-AMP
- DOSS-Mirai-GENUDP-flood
- DOSS-SSL-ClearText
- DNS Amplification
- DNS Random Sub-Domain

Observed attack size ranges:

- 1.2Gbps - 135Gbps
- 9K RPS – 1.5M RPS
- 4K QPS - 16K QPS

Observed range of single attack duration times:

- 2 min – 1443 min

Gov't Sector – Israel

Full mitigation and no impact



Attack Type:

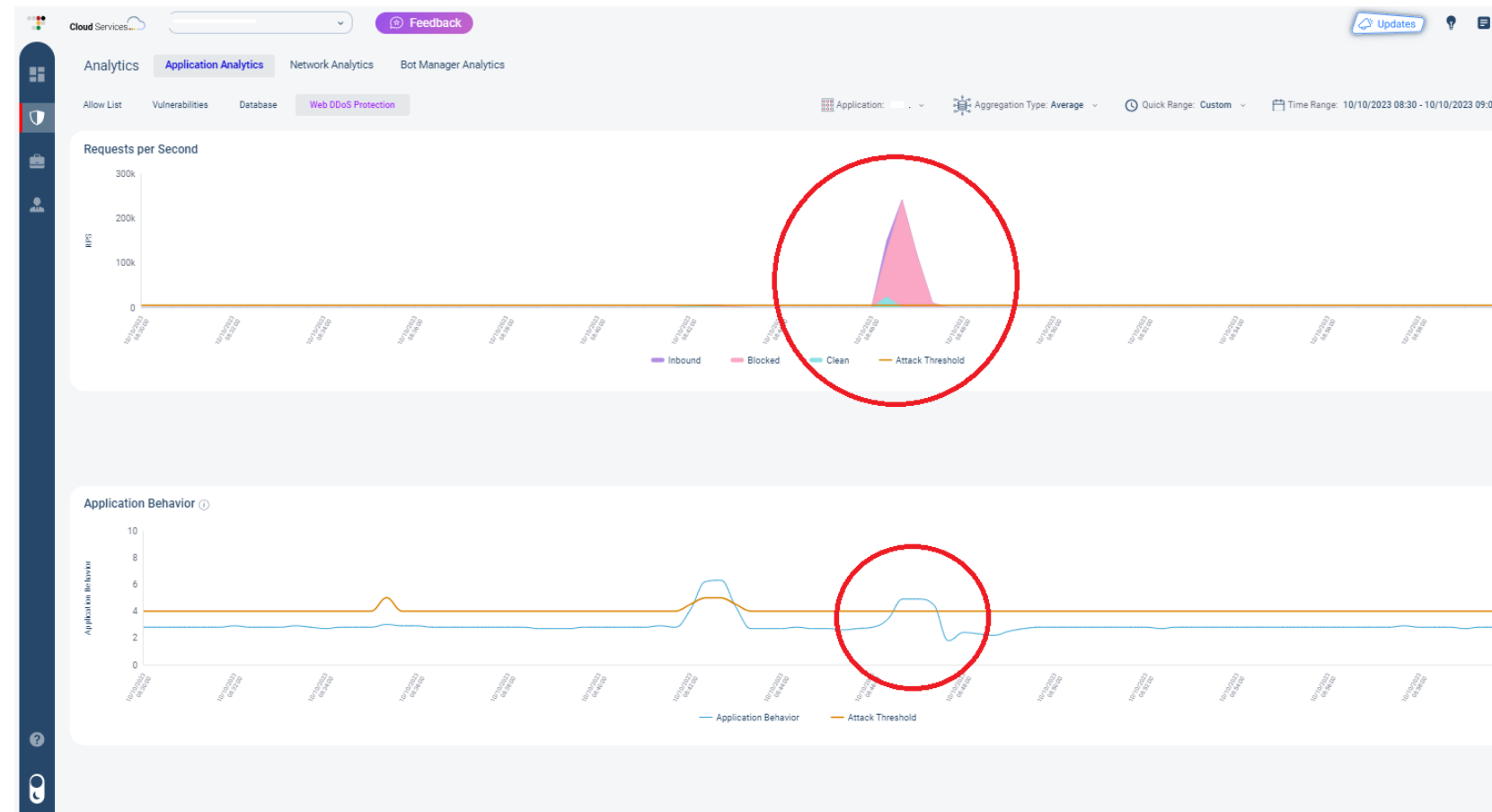
- **WebDDOS**

Trigger:

- **RPS threshold**
- **ML Application behavioral threshold**

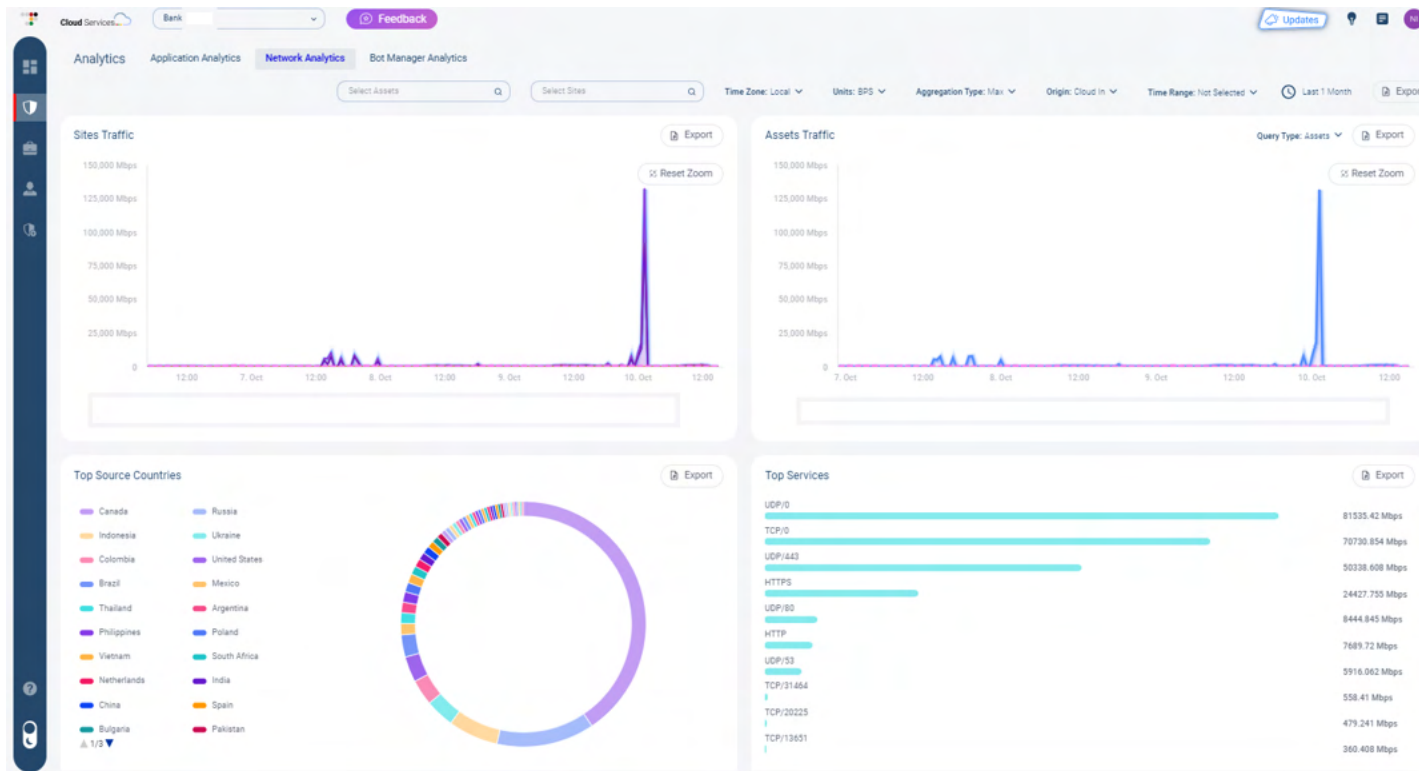
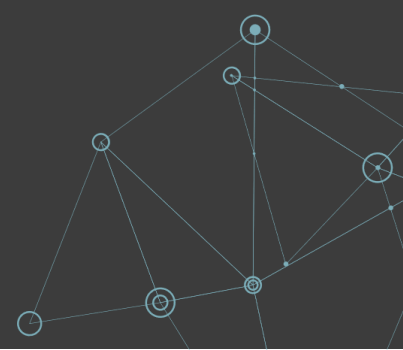
Additional Comments

- **Both triggers are required**
- **Previous attack did not cross RPS threshold**



Banking Sector – Israel

Full mitigation and no impact



Attack Type:

- **DDOS**

Date/time:

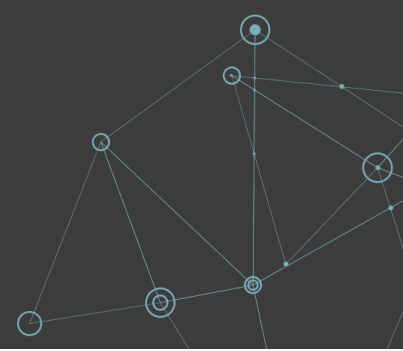
- **October 10th 2023**
- **9:32 PM Local time**

Additional Comments

- **Major Spike in Level 4 traffic**

Banking Sector – Israel

Full mitigation and no impact



Attack Type:

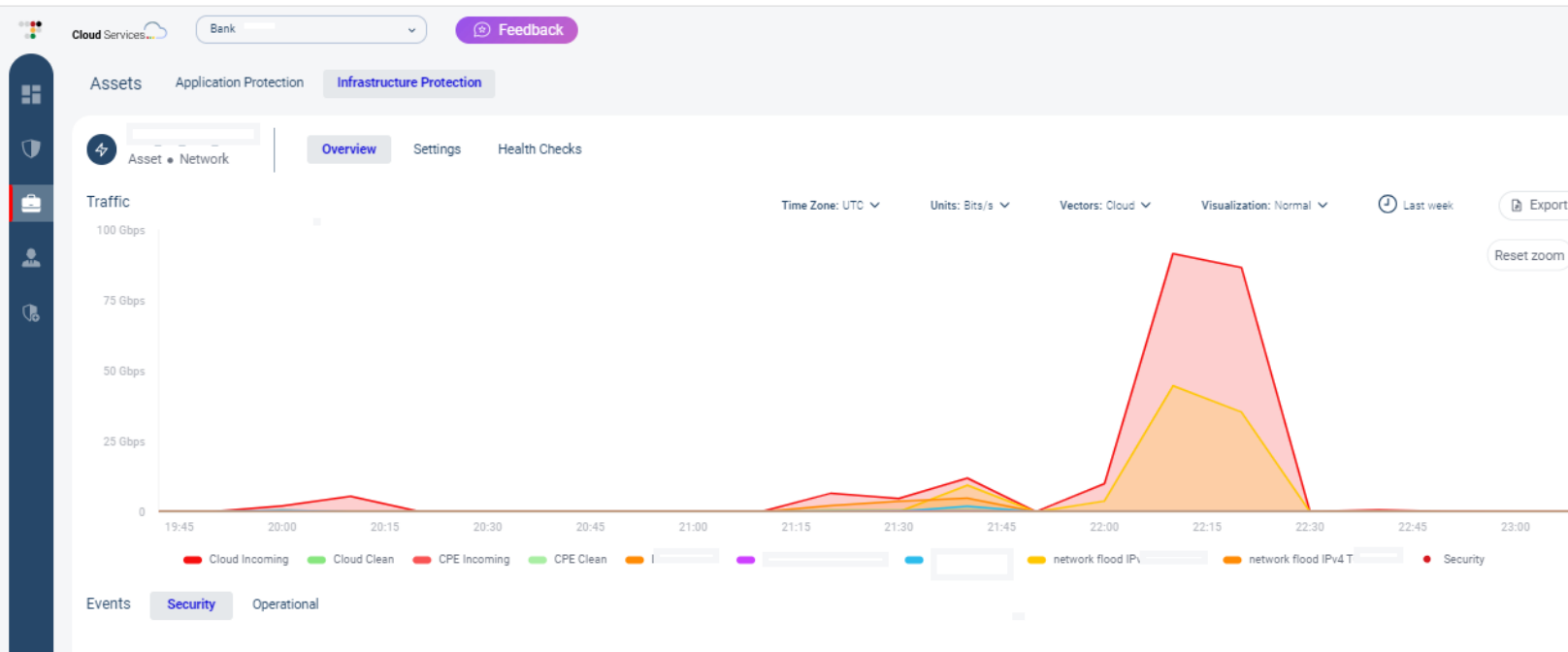
- **DDOS**

Trigger:

- **Traffic Bandwidth**

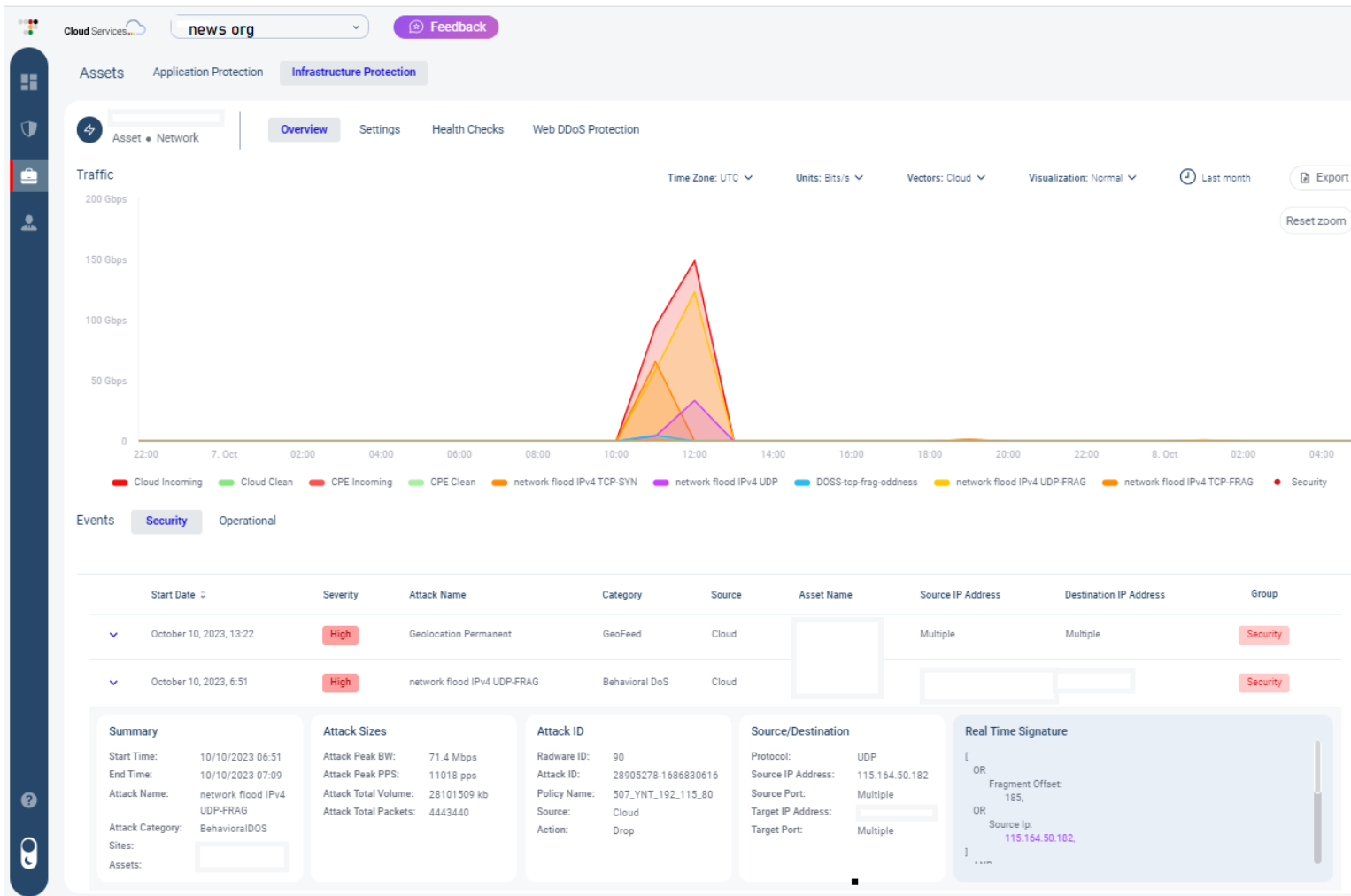
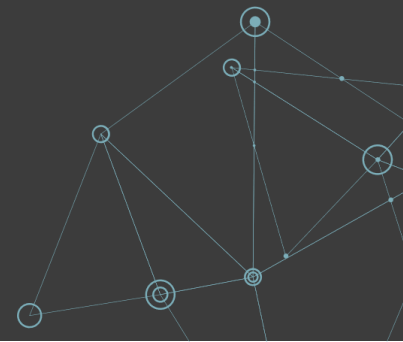
Additional Comments

- **Cloud Clean (green) stays level**
 - **Blocking and removal**
- **No impact on servers**



News Organization Sector – Israel

Full mitigation and no impact



Attack Type:

- **WebDDOS**

Date/time:

- **October 10th 2023**
- **6:51AM Local time**

Additional Comments

- **150Gbit/s**

Service Sector – Israel

Full mitigation and no impact



Attack Type:

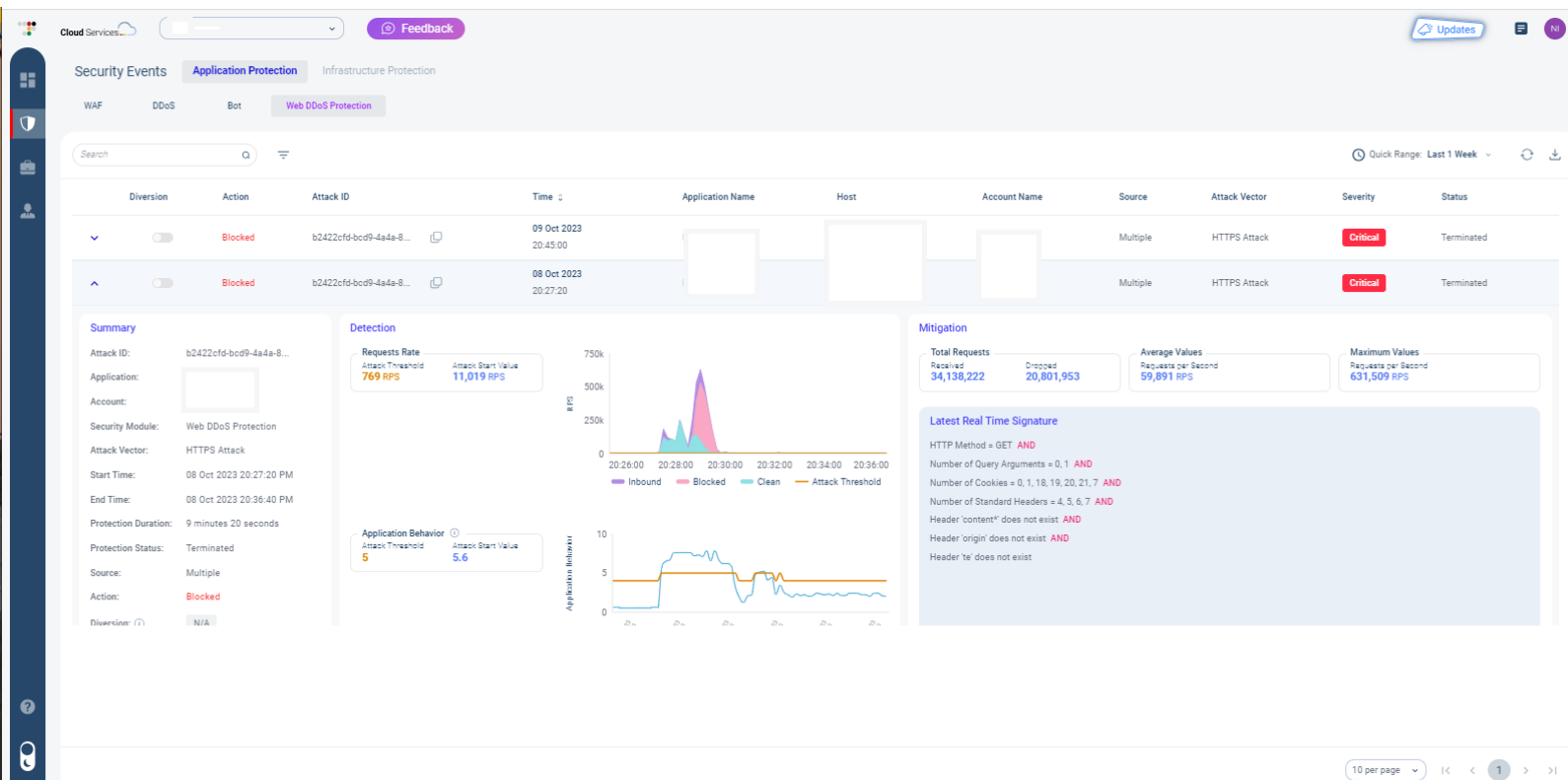
- **WebDDoS**

Date/time:

- **October 8th 2023**
- **8:27 PM Local time**

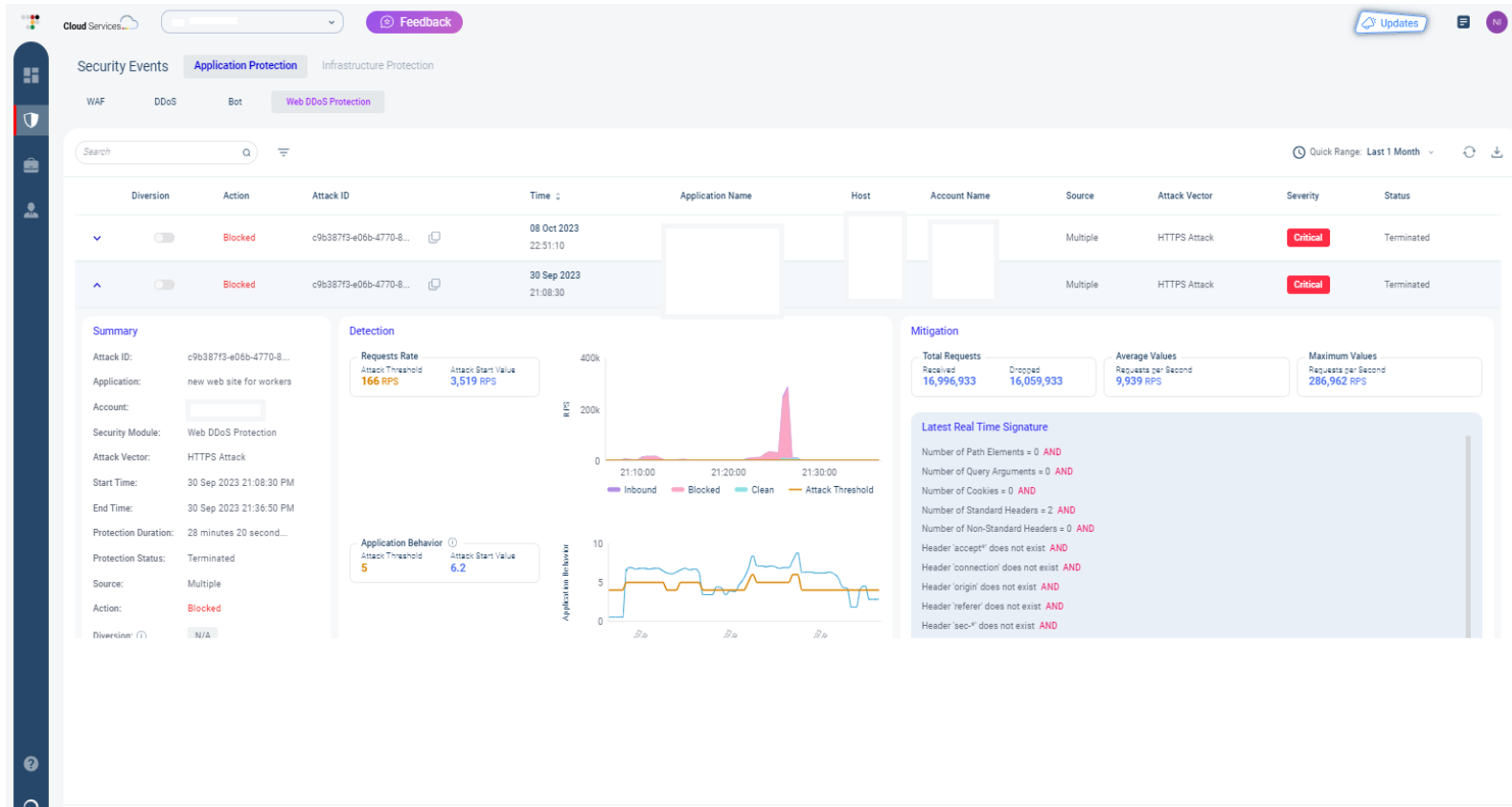
Additional Comments

- **There were two back-to-back attacks.**
- **Both attacks mitigate with some leakage since no baseline**
- **Attack mode WebDDoS**



Transport Sector – Israel

Full mitigation and no impact



Attack Type:

- **WebDDOS**

Date/time:

- **September 30th 2023**
- **9:08 PM Local time**

Additional Comments

- **WebDDOS pkgs were previous, but need RPS and WebDDOS to trigger**
- **300,000 RPS**
- **Almost no leakage**
- **No Impact on customer**

How Radware is protecting Israel?



Behavioral L7 baselining



Cloud Services

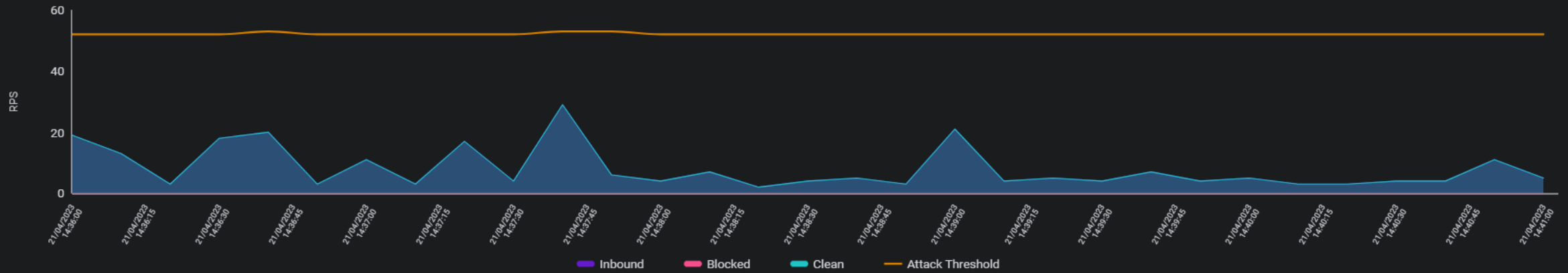
Radware

Feedback

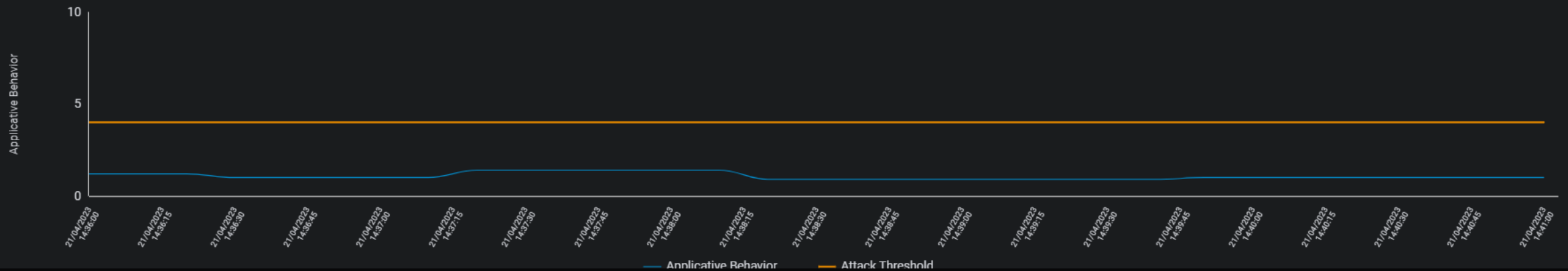
NI

Beta

Requests per Second



Applicative Behavior



Behavioral L7 baselining



Cloud Services... Radware Feedback

Security Events Application Protection Infrastructure Protection

WAF DDoS Bot Web DDoS Protection

Search Quick Range: Last 1 Week

Action	Attack ID	Time	Application Name	Host	Account Name	Source	Attack Vector	Severity	Status
Blocked	0e09bed5-340f-455e-b...	29 Mar 2023 09:14:00	Hackers Almanac	hackersalmanac.radware.com	Radware	Multiple	HTTP Flood Attack	Critical	Terminated

Attack Details

Attack ID: 7919af29-2c78-401e-b...

Application: www.radware.com

Account: Radware

Security Module: Web DDoS Protection

Attack Vector: HTTP Flood Attack

Start Time: 29 Mar 2023 13:11:10 PM

End Time: 29 Mar 2023 13:19:50 PM

Attack Duration: 9 minutes

Attack Status: Terminated

Source: Multiple

Action: Blocked

Detection

Requests Rate

Attack Threshold: 80 RPS | Attack Start Value: 747 RPS

29/23/2023 13:13:40

- Inbound: 875 RPS
- Blocked: 856 RPS
- Clean: 19 RPS
- Attack Threshold: 65 RPS

Applicative Behavior

Attack Threshold: 6 RPS | Attack Start Value: 9 RPS

Applicative Behavior

Attack Threshold

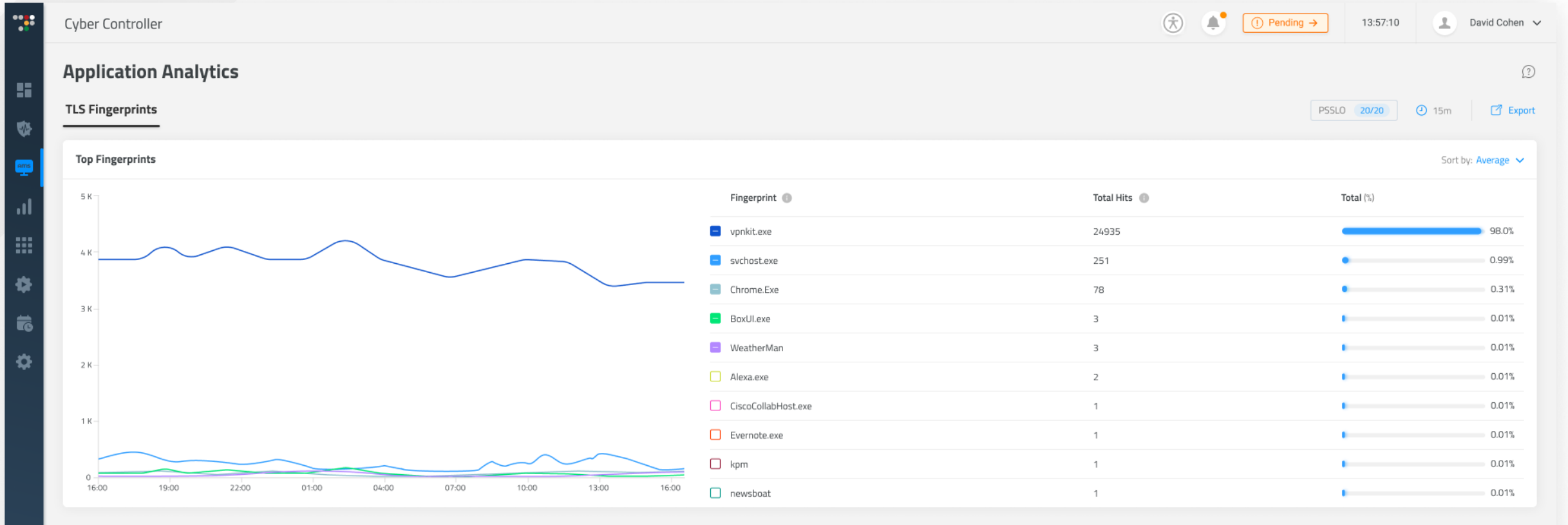
Mitigation

Total Requests		Average Values		Maximum Values	
Received	Dropped	Requests per Second		Requests per Second	
217371	201044	410 RPS		878 RPS	

Real Time Signature

- Number of Path Elements = 7 AND
- HTTP Method = POST AND
- Number of Query Arguments = 1 AND
- Number of Cookies = 2 AND
- Number of Standard Headers = 6 AND
- Number of Non-Standard Headers = 5 AND
- Header 'accept*' exist AND
- Header 'access-*' does not exist AND
- Header 'authorization' does not exist AND
- Header 'cache*' exist AND
- Header 'connection' does not exist AND
- Header 'content*' exist AND

Behavioral TLS Fingerprinting



Thank You!