

# Businesses in the line of Fire Are You Ready for the Next Web DDoS Tsunami?

## Heise Jan-2024

Alexander Krakhofer | Markus Spahn

2024

# Key Takeaways of the Webinar

- Why should you care
  - In view of the recent increase in cyber aggressions against DACH and International targets, every company is at risk
- Get insights into:
  - The threat actors you should care about
  - Their motivation and tactics
  - New tactic: Web DDoS attacks
- Understand
  - Why current security solutions fail to accurately detect the new type of attacks
- Learn
  - How to protect your business against emerging cyber aggressions

# About Radware

Secure Your Apps. Regain Control. Enable Your Business.



## Over 12,500 Customers



## Analysts Praise Us



DDoS MarketScape  
**#1 Leader**



**#2 API & High Security**



DDoS Wave Leader



Bot Management Leader  
WAF Leader  
DDoS Protection Leader

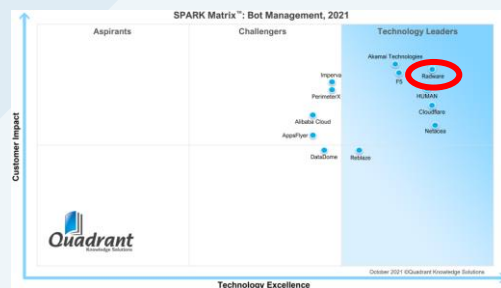
## Our Partners



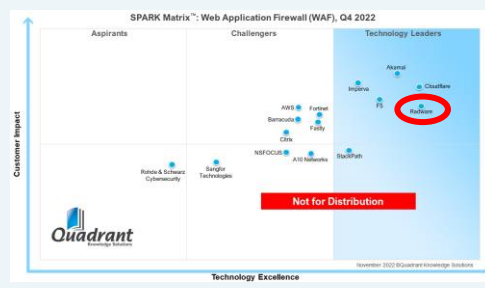


# State-of-the-Art Protection: Winning Industry Recognition in 2022

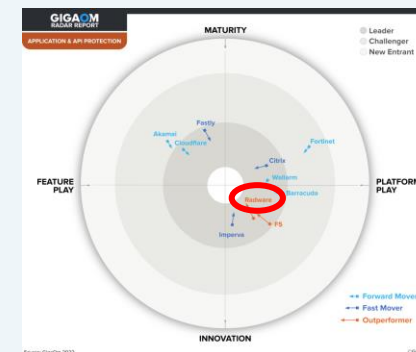
## BOT MANAGEMENT 2022 LEADER



## WAF 2022 LEADER



## GIGAOM APP & API PROTECTION 2022 LEADER & OUTPERFORMER



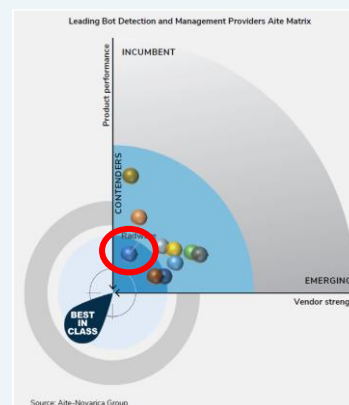
## FORRESTER® DDoS MITIGATION WAVE 2021 LEADER



## AiteNovarica

### BOT DETECTION MATRIX, 2022 BEST IN CLASS

*“The largest global financial institutions, brokerage firms, and financial services companies use Radware’s Bot Manager.”*



## kuppingercoie WAF LEADERSHIP COMPASS 2022 OVERALL LEADER Product, Innovation & Market Leader



# Umfrage

# Evolution of Latest Attack Campaigns





# Russian/Ukraine Conflict Ignites New Cyber War Era

Conflict extended beyond the two countries



## Pro-Russian Hactivist Groups

NoName057, Killnet cluster,  
Anonymous Russia, Passion Group, etc

Attacking targets in countries that are  
supporting Ukraine



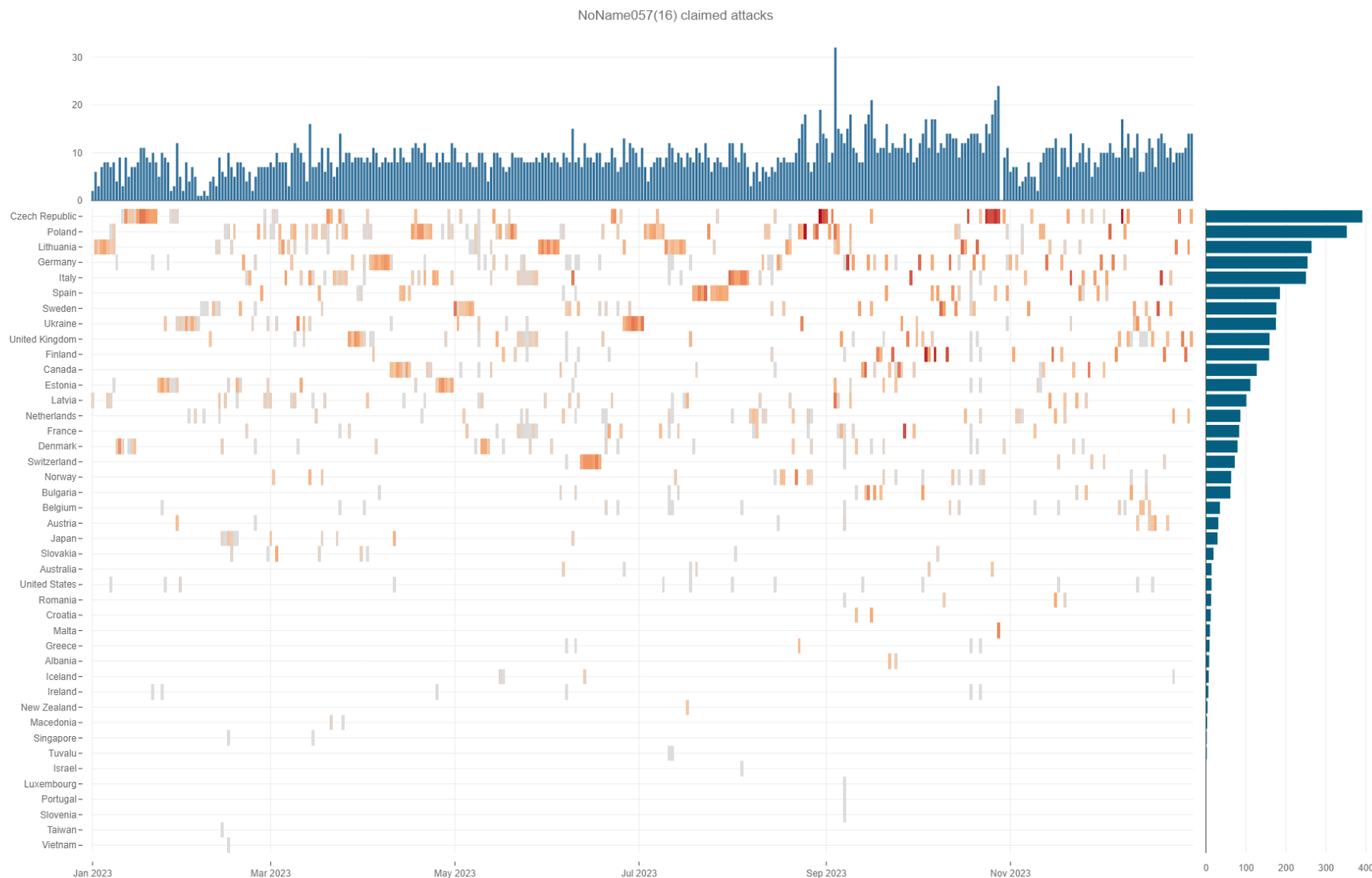
## Religious Groups

Anonymous Sudan, Mysterious Team  
Bangladesh, DragonForce Malaysia, etc

Cyber attacks against targets who  
supposedly insulted Muslims

# NoName057(16)

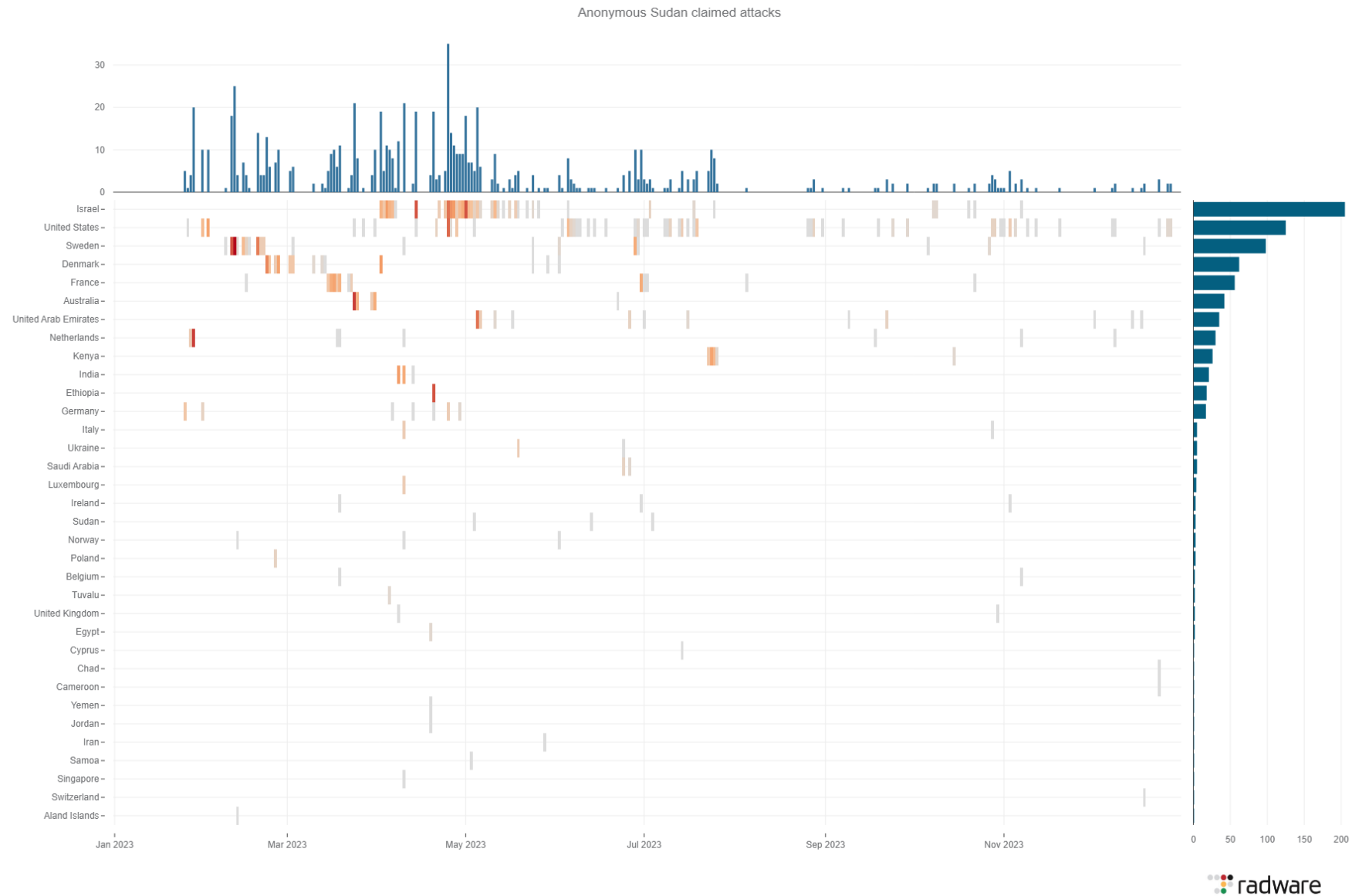
Most active pro-Russian  
Patriotic Hacktivist





# Anonymous Sudan

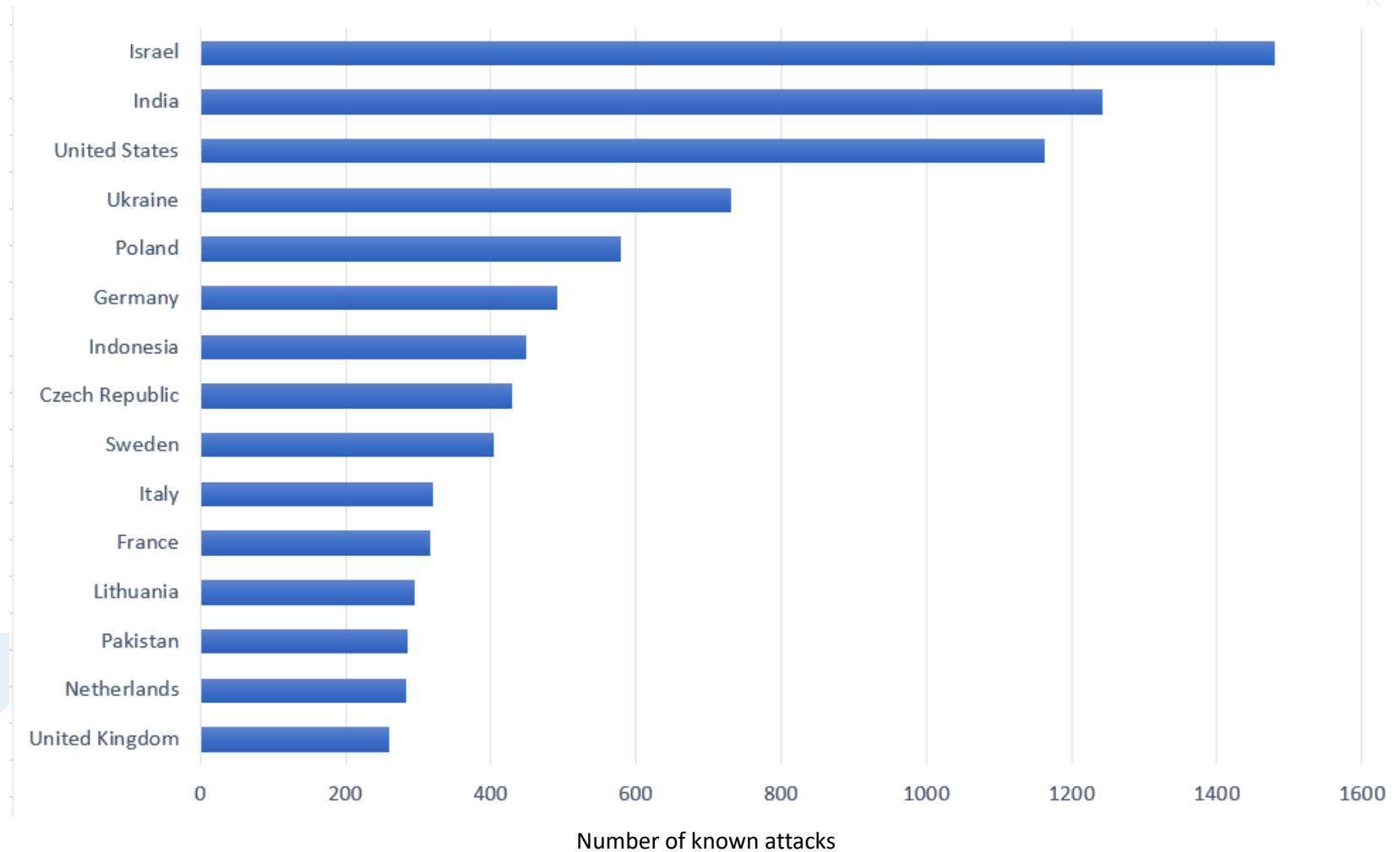
A Rebel with too many causes



# DDoS Attacks by Activist Groups Have Gone Global

While the trend of state-backed and hacktivist groups began with the war between Russia and Ukraine, it is now a global trend

Top Attacked Countries in 2023



**Source:** Based on tracking by Radware's Threat Intelligence Team of over 12,500 DDoS attacks by hacktivist and state-backed groups in 2023.

# Businesses in the Line of Fire: Attack Campaign On Health Care

February 2023


SC MEDIA TOPICS INDUSTRY EVENTS PODCASTS RESEARCH RECOGNITION LE

Threat intelligence, Application security, Vulnerability management

f t x in

## Killnet DDoS attacks inflicting damage on healthcare: 'This is war'

Jessica Davis February 13, 2023




Recent alerts to the health sector warn that the Russia-Ukraine war have spurred hacktivists to leverage more destructive tactics. (iStock via Getty Images)

The Killnet hacktivist group's DDoS attacks against healthcare and the mass data exfiltration in January was reportedly just the first round of targeting. Industry leaders

<https://www.scmagazine.com/news/threat-intelligence/killnet-ddos-attacks-inflicting-damage-on-healthcare-this-is-war>

Malwarebytes LABS Personal Business Pricing Partners R

Search Labs



CYBERCRIME | NEWS

## KillNet hits healthcare sector with DDoS attacks

Posted: February 10, 2023 by Pieter Arntz

At the end of January, the Health Sector Cybersecurity Coordination Center warned that the KillNet group is actively targeting the US healthcare sector with distributed denial-of-service (DDoS) attacks.

The Cybersecurity and Infrastructure Security Agency (CISA) says it helped dozens of hospitals

<https://www.malwarebytes.com/blog/news/2023/02/killnet-group-targets-us-and-european-hospitals-with-ddos-attacks>

Automatic Translation  
Russian → English

ATTENTION TO TEAMS THAT JOIN OUR MISSION!

Everyone hit L7 on 50 hospital targets - 50 states of America!

Alaska  
<https://www.providence.org>  
<https://check-host.net/check-report/e77f515k82d>

Arizona  
<https://www.abrazohealth.com>  
<https://check-host.net/check-report/e77f5a2kcbe>

Arkansas  
<https://arksurgicalhospital.com>  
<https://check-host.net/check-report/e779e33kf96>

California  
<https://www.sclhealth.org>  
<https://check-host.net/check-report/e7821b1kf6>

Colorado  
<https://www.sclhealth.org>  
<https://check-host.net/check-report/e7821b1kf6>

Connecticut  
<https://gfp.griffinhealth.org>  
<https://check-host.net/check-report/e781374kbab>

Delaware  
<https://christianacare.org>  
<https://check-host.net/check-report/e77a063kb3e>

Florida  
<https://www.leehealth.org>  
<https://check-host.net/check-report/e77fbeck78c>

Georgia  
<https://www.northside.com>  
<https://check-host.net/check-report>




# Businesses in the Line of Fire: Attacks on Scandinavian Targets



Combined DDoS, Web, and Bot attack Campaign

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>

# Germany became a Focus-Target as well as Europe

WE ARE KILLNET  
Forwarded from ANONYMOUS | RUSSIA



Нелётная погода в Германии объявлена!

▼ Гамбург (аэропорт)  
<https://www.hamburg-airport.de/de>  
<https://check-host.net/check-report/e61b977k231>

▼ Дортмунд (аэропорт)  
<https://www.dortmund-airport.de/>  
<https://check-host.net/check-report/e61b9a6k551>

CYBERANGRIFF

## Vergeltung: Russische Hacker schießen sich auf deutsche Internet-Seiten ein

DDoS-Angriffe unter anderem auf Regierung und Flughafen Hamburg als Vergeltung für deutsche Panzer-Entscheidung

25. Jänner 2023, 17:10 · 9 Postings

▼ Аэропорт Дортмунд  
<https://www.dus.com/de>  
<https://check-host.net/check-report/e61b9a6k551>

▼ Аэропорт Зинделанд  
<https://www.flughafen-zindelndorf.de/>  
<https://check-host.net/check-report/e61b9a6k551>

▼ Карлсруэ/Баден-Вюртемберг  
<https://www.baden-airport.de/>  
<https://check-host.net/check-report/e61b9a6k551>

▼ Веце (аэропорт)  
<https://airport-weeze.nl/>  
<https://check-host.net/check-report/e61b9a6k551>

▼ Ганновер-Лангхаген  
<https://www.hannover-airport.de/>  
<https://check-host.net/check-report/e61b9a6k551>

1035 🔥 340

Unter der Flughäfen auch aufwartet.

Foto: IMAGO

Viele Angriffe abgewehrt

"Derzeit sind einige Websites nicht erreichbar", teilte die Behörde mit. "Hinweise auf direkte Auswirkungen auf die jeweilige Dienstleistung liegen aktuell nicht vor und sind nach Einschätzung des BSI bei Ergreifen üblicher Schutzmaßnahmen auch nicht zu erwarten." Die Angriffe auf die Seiten der Bundesverwaltung seien größtenteils abgewehrt worden.

DDoS-Attacken gelten als technisch simple Angriffe, die häufig von "Hacktivisten" eingesetzt werden. Dabei nehmen Gruppen einzelne Internet-Seiten aufs Korn, um auf bestimmte Themen aufmerksam zu machen. In der Regel bleiben die internen IT-Systeme eines Unternehmens davon unberührt und es werden auch keine Daten abgezogen.

Vergeltung

Laut mehreren Medienberichten kündigte unter anderem die prorussische Hackergruppe Killnet an, deutsche Ziele anzugreifen. Als Motivation nannte sie die Panzer-Lieferungen aus Deutschland an die Ukraine. In einem Telegram-Kanal ist zu lesen: "Die Apokalypse rückt immer näher", wie das "Handelsblatt" berichtet. Auch andere Hackergruppen werden aufgerufen, sich diesen Angriffen anzuschließen. (APA, red, 25.1.2023)

Anonymous Sudan

502 Bad Gateway

LHR → OSL

Add a new app

ADD

Log in to your account


السودان ، عشان كذا وقتنا الموقع و التطبيق الخاص بشركة طيران

We were bored and we missed Sweden and we dropped the SAS app

• <https://www.sas.se/>  
★ <https://check-host.net/check-report/100598c3>

#AnonymousSudan

WE ARE KILLNET



🔥 72 часа назад, три главы хакерских группировок из России и Судана провели очередное заседание в парламенте DARKNET'a, и пришли к общему решению:

⚡ РЕШЕНИЕ №0191

- Сегодня мы начинаем вводить санкции в отношении европейских банковских трансферных систем SEPA, IBAN, WIRE, SWIFT, WISE.

Перевод\*

× 72 hours ago, three heads of hacker groups from Russia and Sudan held a regular meeting in the DARKNET parliament, and came to a common decision:

× SOLUTION №0191

- Today we are starting to impose sanctions on the European banking transfer systems SEPA, IBAN, WIRE, SWIFT, WISE.

WE ARE KILLNET 🤖

94.7K 👁 edited 12:56

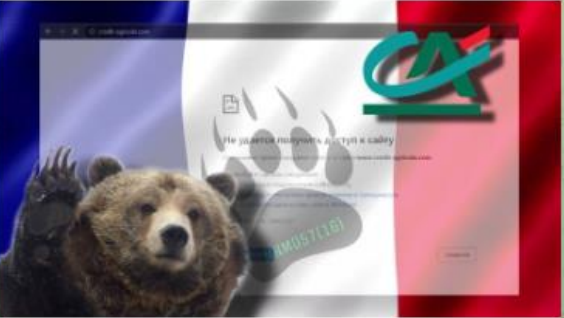
\*Sources Telegram und DerStandard



# Claimed Attack on Telegram: Global

## Attack on Credit Agricole Bank

NoName057(16) Eng



▼ Makron broke into a blissful smile and announced that the SAMP/T anti-aircraft missile system had been delivered to Ukrainian neo-Nazis and was ready for operation.

This is the weapons that France supplies together with Italy, as a result, of course, it will either be captured or destroyed by Russian troops, so the French president rejoices for no reason...🐻

We go to the French segment of the Internet and kill the website of the financial conglomerate "Credit Agricole":

✗ <https://check-host.net/check-report/10576ed8k281>

👉 Subscribe to NoName057(16)  
🐻 Join our DDoS-project  
⚠️ Subscribe to reserve channel

🇷🇺 Victory will be ours!

t.me/noname05716eng/1755 971 Jun 21 at 11:07

## Attack on Canadian PM

NoName057(16)



Узнали, что канадский премьер Джастин БиберТрюдо приперся на Украину подлизывать бандеровцам🐻

Приложили за это его официальный сайт:

✗ <https://check-host.net/check-report/1034a6dckd6c>

Делаем это примерно в 100500-й раз🐻


👉 Подписывайтесь на канал NoName057(16)  
🐻 Вступайте в наш DDoS-проект  
⚠️ Подписывайтесь на резервный канал  
▼ Eng version

🇷🇺 Победа За нами!

t.me/noname05716/3634 5.0K edited Jun 10 at 13:35

## Attack on Zurich Airport

NoName057(16) Eng



The website of the Zurich transport association ZVV was slammed:

✗ <https://check-host.net/check-report/104e9951k38b>

👉 Subscribe to NoName057(16)  
🐻 Join our DDoS-project  
⚠️ Subscribe to reserve channel

🇷🇺 Victory will be ours!

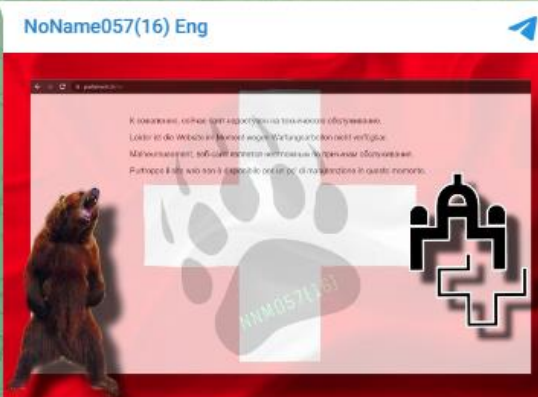
t.me/noname05716eng/1739 1.1K Jun 18 at 19:34



# Claimed Attacks on Telegram: Over 60 Targets in Switzerland

## Swiss Parliament

NoName057(16) Eng



▼ Bandera member Zelensky thanked Switzerland, which this week joined the 10th package of EU anti-Russian sanctions. We also "thanked" the Swiss Russophobes and sent DDoS missiles to the website of the Swiss Parliament, after which the resource administrators closed access for foreign ip 🤔:

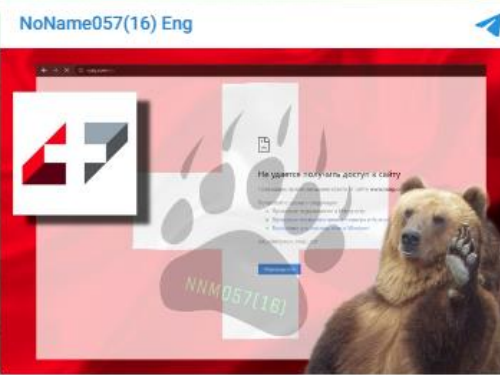
✗ <https://check-host.net/check-report/103a4c6aka29>

👉 Subscribe to [NoName057\(16\)](#)  
🐻 Join our [DDoS-project](#)  
⚠️ Subscribe to [reserve channel](#)

🇺🇦 Victory will be ours!  
[t.me/noname05716eng/1674](https://t.me/noname05716eng/1674) 1.3K 🗨 Jun 12 at 11:03

## Ruag Defense Concern

NoName057(16) Eng



▼ The Swiss defense concern Ruag recently applied to the authorities of its country with a request to give it permission to sell 96 Leopard tanks to the German company Rheinmetall for subsequent deliveries of this equipment to Kyiv.

The Swiss defense concern Ruag - no more turning to your authorities with such stupid requests! Otherwise, we can visit Switzerland and smash the entire Internet infrastructure to hell, as it has [already happened once](#) 🤔

In the meantime, relax, think about our offer... 🐻

✗ <https://check-host.net/check-report/10440518kcd6>

👉 Subscribe to [NoName057\(16\)](#)  
🐻 Join our [DDoS-project](#)  
⚠️ Subscribe to [reserve channel](#)

🇺🇦 Victory will be ours!  
[t.me/noname05716eng/1706](https://t.me/noname05716eng/1706) 1.2K 🗨 Jun 15 at 13:34

## Swiss Private Bankers

NoName057(16) Eng



The website of the association of Swiss bankers SwissBanking did not survive our attack:


✗ <https://check-host.net/check-report/10440b9ak78e>

👉 Subscribe to [NoName057\(16\)](#)  
🐻 Join our [DDoS-project](#)  
⚠️ Subscribe to [reserve channel](#)

🇺🇦 Victory will be ours!  
[t.me/noname05716eng/1710](https://t.me/noname05716eng/1710) 1.3K 🗨 Jun 15 at 17:12

## Julius Bär Group

NoName057(16) Eng



We killed the website of the Swiss bank Julius Bär:

✗ <https://check-host.net/check-report/10440aadk1ad>

👉 Subscribe to [NoName057\(16\)](#)  
🐻 Join our [DDoS-project](#)  
⚠️ Subscribe to [reserve channel](#)

🇺🇦 Victory will be ours!  
[t.me/noname05716eng/1709](https://t.me/noname05716eng/1709) 1.2K 🗨 Jun 15 at 16:15

# Businesses in the Line of Fire: Victims Are Down

## Check-host.net

IP: 192.115.180.11 Country: Israel (Tel Aviv, Tel Aviv) 100% Offshore Server

Hostname or IP address

Info Ping HTTP TCP port UDP port DNS

Check website <https://www.ruag.com/en>

The incredible is real! Profitable VPS 5.7 GHz, 6 locations, and more: [aeza.net](https://aeza.net)

Permanent link to this check report | Share report on Twitter

Checked on **Thu Jun 15 07:10:30 UTC 2023** | Check again

Location	Result	Time	Code	IP address
Australia, Sydney	Connection timed out			
Austria, Vienna	Connection timed out			
Brazil, Sao Paulo	Connection timed out			
Bulgaria, Sofia	Connection timed out			
Czechia, C.Budejovice	Connection timed out			
Finland, Helsinki	Connection timed out			
France, Paris	Connection timed out			
Germany, Frankfurt	Connection timed out			
Germany, Nuremberg	Connection timed out			
Hong Kong, Hong Kong	Connection timed out			
India, Mumbai	Connection timed out			
Japan, Tokyo	Connection timed out			
Poland, Warsaw	Connection timed out			
Portugal, Lisbon	Connection timed out			
Russia, Moscow	Connection timed out			
Russia, Saint Petersburg	Connection timed out			
South Korea, Seoul	Connection timed out			
Spain, Madrid	Connection timed out			
Sweden, Stockholm	Connection timed out			
Switzerland, Zurich	Connection timed out			
Thailand, Bangkok	Connection timed out			
Turkey, Istanbul	Connection timed out			
USA, New York	Connection timed out			

IP: 192.115.180.11 Country: Israel (Tel Aviv, Tel Aviv) 100% Offshore Server

Hostname or IP address

Info Ping HTTP TCP port UDP port DNS

Check website <https://www.ruag.com/en>

The incredible is real! Profitable VPS 5.7 GHz, 6 locations, and more: [aeza.net](https://aeza.net)

Permanent link to this check report | Share report on Twitter

Checked on **Thu Jun 15 07:10:30 UTC 2023** | Check again

Location	Result	Time	Code	IP address
Australia, Sydney	Connection timed out			
Austria, Vienna	Connection timed out			
Brazil, Sao Paulo	Connection timed out			
Bulgaria, Sofia	Connection timed out			
Czechia, C.Budejovice	Connection timed out			
Finland, Helsinki	Connection timed out			
France, Paris	Connection timed out			
Germany, Frankfurt	Connection timed out			
Germany, Nuremberg	Connection timed out			
Hong Kong, Hong Kong	Connection timed out			
India, Mumbai	Connection timed out			



# Attack Tools More Powerful, Easier to Use



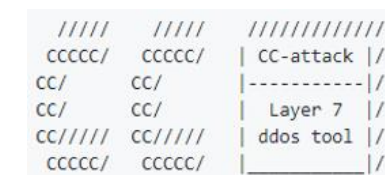
# Tools Are More Accessible Than Ever

The image displays four overlapping screenshots of GitHub repositories for various DDoS attack tools, illustrating the ease of access to such tools.

- KARMA DDoS** (HyuklsBack/KARMA-DDoS): A DDoS Script (DDoS Panel) with Multiple Bypass (Cloudflare UAM, CAPTCHA, BFM, NOSEC / DDoS Guard / Google Shield / V Shield / Amazon / etc...). It has 392 stars and 219 forks.
- CC-attack** (Leon123/CC-attack): A script for using socks4/5 or http proxies to attack http(s) server. It has 3.7.1 version and GPLv2 license. News include: Added Support of HTTP proxies, Added More proxies api to download.
- ZxCDDoS: Release v1.4 - Free** (hoaan1995/ZxCDDoS): Terminal only accepts ANSI color. Username: admin, Password: admin. It has 259 stars and 174 forks. Language options: PYTHON, JAVASCRIPT, PERL, C.
- MHDDoS - DDoS Attack Script With 56 Methods** (MatrixTM/MHDDoS): (Programming Language - Python 3). It has 2.1K forks, 9.4K stars, and 1 open issue. It includes a disclaimer: "Please Don't Attack websites without the owners consent." and a screenshot of a "Layer 7 Dstats" graph showing requests per second.

# New Generation of Attack Tools Uses Randomization

- HTTP method randomization (GET, POST, HEAD, etc.)
- Randomized header values
- Dynamic request arguments
- Use open proxy networks
- IP spoofing
- Cookie harvesting
- Built-in bypass techniques
- Etc.



# Modern Tools Include Built-in Bypass

They know how to deal with common protection tools



## Features And Methods

- Layer7
  - GET | GET Flood
  - POST | POST Flood
  - OVH | Bypass OVH
  - RHEX | Random HEX
  - STOMP | Bypass chk\_captcha
  - STRESS | Send HTTP Packet With High Byte
  - DYN | A New Method With Random SubDomain
  - DOWNLOADER | A New Method of Reading data slowly
  - SLOW | Slowloris Old Method of DDoS
  - HEAD | <https://developer.mozilla.org/en-US/docs/Web/HTTP/Methods/HEAD>
  - NULL | Null UserAgent and ...
  - COOKIE | Random Cookie PHP 'if (isset(\$\_COOKIE))'
  - PPS | Only 'GET / HTTP/1.1\r\n\r\n'
  - EVEN | GET Method with more header
  - GSB | Google Project Shield Bypass
  - DGB | DDoS Guard Bypass
  - AVB | Arvan Cloud Bypass
  - BOT | Like Google bot
  - APACHE | Apache Exploit
  - XMLRPC | WP XMLRPC exploit (add /xmlrpc.php)
  - CFB | CloudFlare Bypass
  - CFBUAM | CloudFlare Under Attack Mode Bypass
  - BYPASS | Bypass Normal AntiDDoS
  - BOMB | Bypass with codesenberg/bombardier
  - KILLER | Run many threads to kill a target
  - TOR | Bypass onion website



# Application Layer Attacks Grow On Top of Network Attacks



+120%

Increase in number of DDoS attacks, 2023 vs. 2022



+60%

Increase in large attack vectors, 2023 vs. 2022



+770%

Increase in #malicious web transactions, 2023 vs 2021



The unit of measurement of DDoS attacks is changing from **volume-based** (Gbps/Tbps) to additional **rate-based** (RPS)

# Characteristics of New Web DDoS Tsunami Attacks

Requires a behavioral-based approach for accurate detection & mitigation

- Higher in volume – Ultra high RPS
- Encrypted floods
- Appear to be legitimate requests
- Multiple, sophisticated evasion techniques (randomized headers, IP spoofing, etc)

# Traditional DDoS Protections are Not Effective

A network diagram in the top right corner showing a series of interconnected nodes and lines, representing a network topology.

Network-Based DDoS protection cannot detect & mitigate L7 DDoS attacks

Standard WAF solutions look for vulnerability exploits

Rate-limiting techniques impact legit traffic

➔ Available mitigation tools ineffective in detecting & mitigating HTTP/S floods **without impacting legitimate web traffic!**

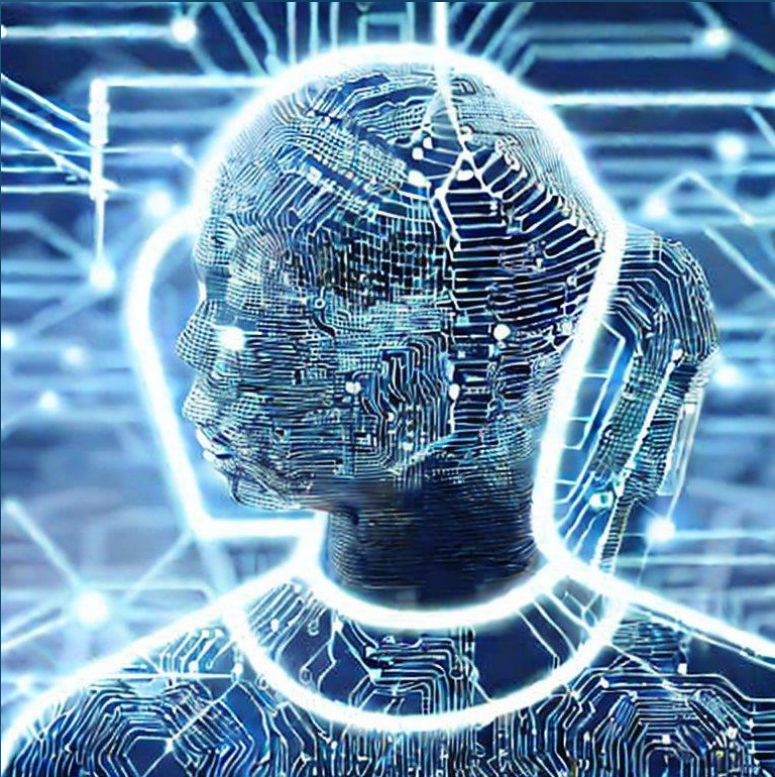


# What is Needed to Stay Protected



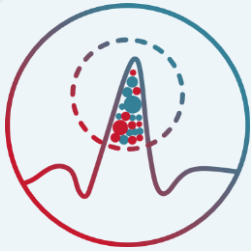
# Businesses in the Line of Fire

We fight Fire with...



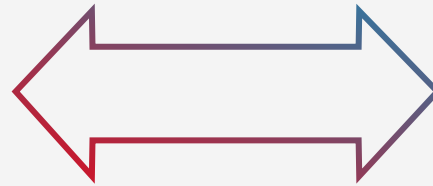
# AI

# New Advanced Protection for Web DDoS Attacks



## Automated, Accurate Detection & Mitigation

Behavioral-based algorithms w/ advanced learning capabilities to accurately distinguish flash crowd vs. flood attack



## Widest L7 DDoS Attack Coverage

Large-scale, sophisticated Web DDoS Tsunami attacks, smaller, sophisticated attacks, new L7 attack tools/ vectors &

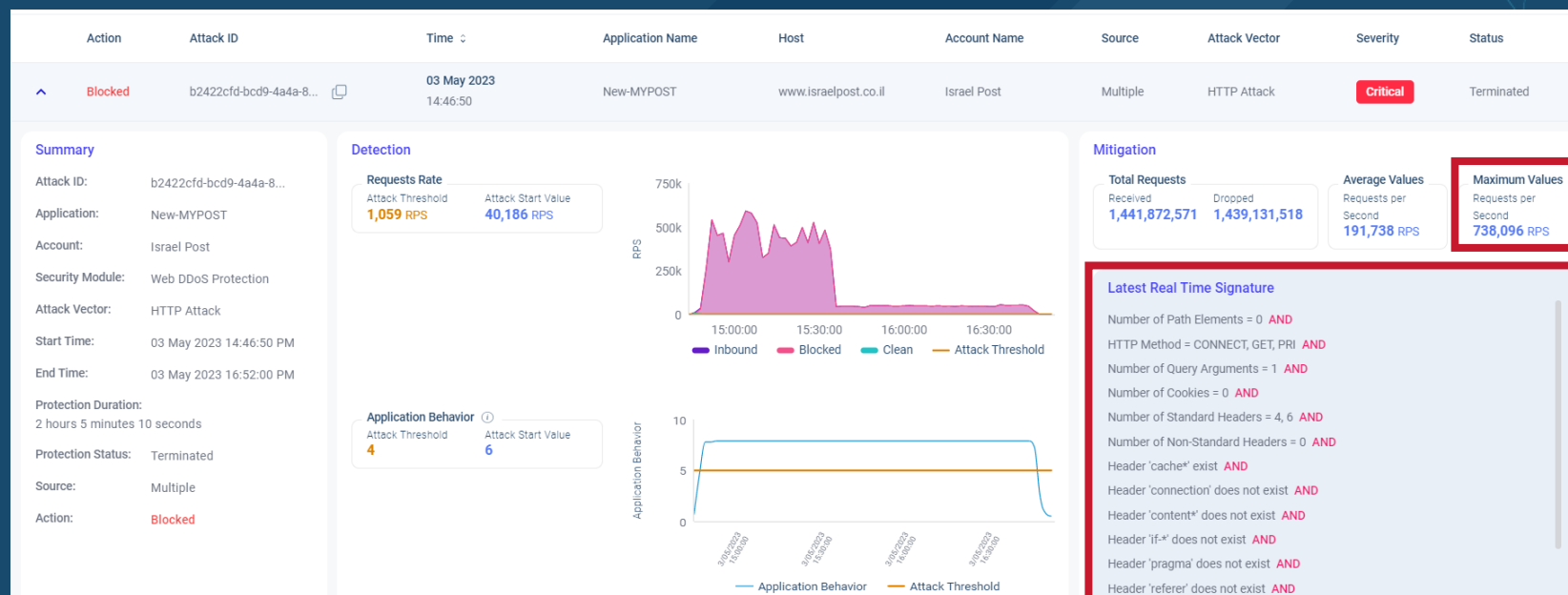


## Best Protection for Web DDoS Tsunami

Combines automated algorithms & high-scale infra to accurately protect against high-RPS, complex L7 DDoS threats



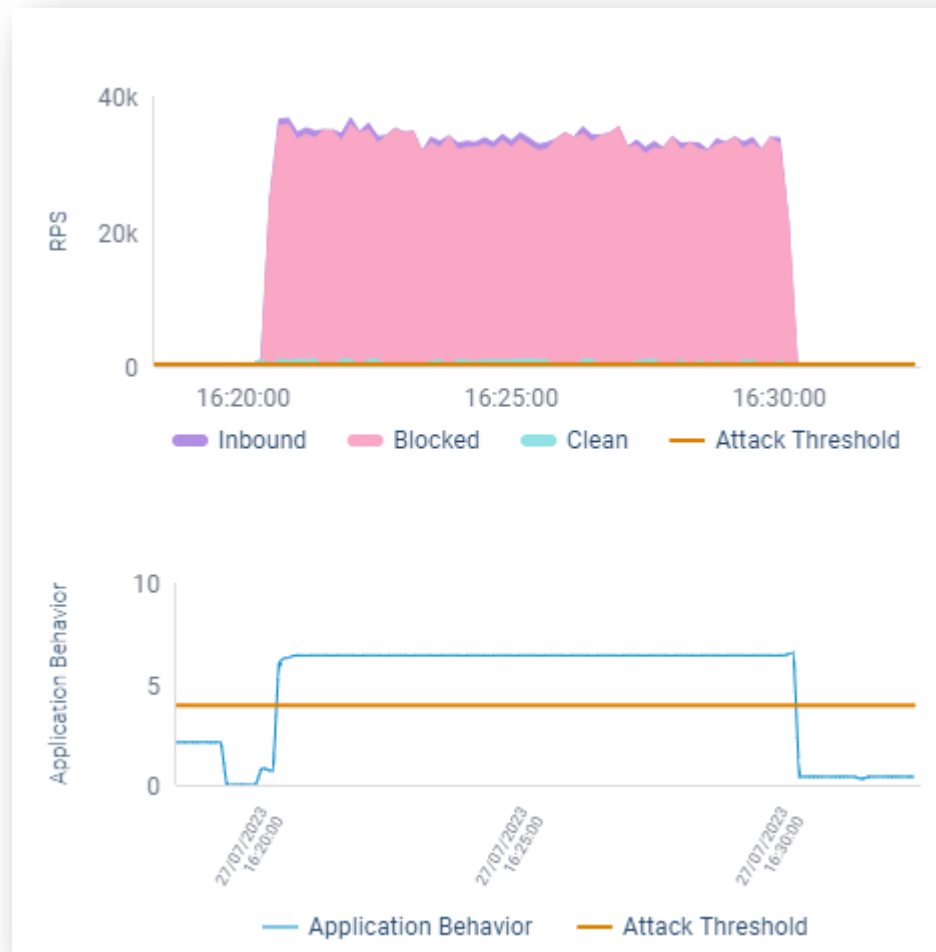
# Radware Protects Gov't Services from Web DDoS Attacks



- **Attacks Peak:** Up to 738K RPS
- **Attacks Length:** Almost 2 hours
- **Attack Layers:** HTTP Flood + Network floods
- **Mitigation Engines:** Web DDoS + L3 mitigation

# Industry-Leading Behavioral L7 DDoS Detection

Full behavioral detection with rate-variant and rate-*invariant* parameters



- Combines both **rate-based** (volume) and **behavioral** (risk) parameters
- **Separate, independent thresholds** for each parameter type
- Identifies attacks **even if they don't cross volume threshold**
- **Distinguishes between attack and legitimate rise in traffic** (e.g., holiday shopping peaks)

# Automatic, Real-Time Adaptive Signatures

Dynamic signatures which automatically adapt to changing attack patterns



## Latest Real Time Signature

HTTP Method = GET, HEAD, ST AND

Number of Query Arguments = 0 AND

Number of Cookies = 0, 4 AND

Number of Standard Headers = 10, 9 AND

Number of Non-Standard Headers = 3, 4 AND

Header 'cache\*' exist AND

Header 'pragma' exist AND

Header 'sec-\*' exist AND

Header 'upgrade-insecure-requests' exist AND

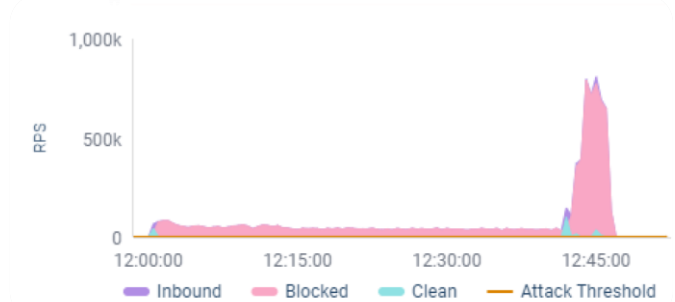
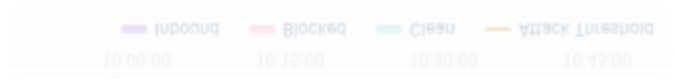
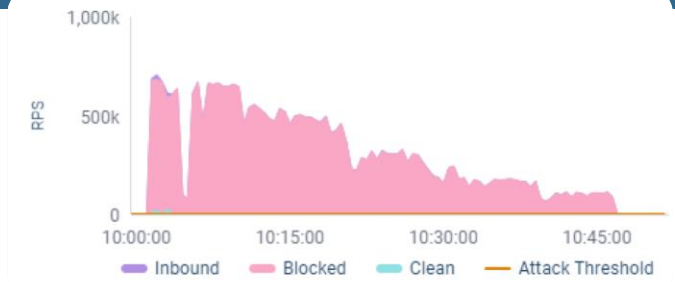
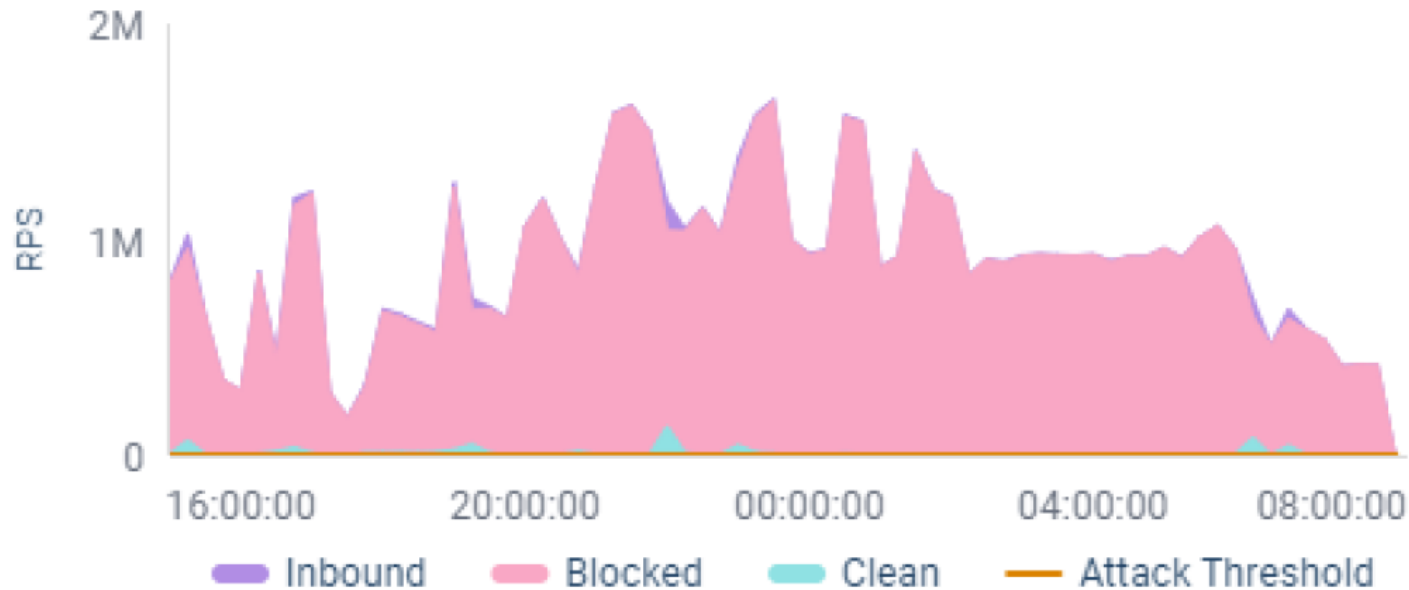
Header 'via' exist

- **Automated, real-time signatures** tailored to attack characteristics
- Applies L7 logic, **with up to 40 separate HTTP/S parameters**
- **Dynamically adapts** to changing traffic patterns
- Automatically deployed and mitigates attacks **with no human intervention required**



# Protecting from an Advanced, Persistent Attack Campaign

7 waves over 48 hours, the longest wave lasted 17 hours straight @ 1 million RPS



Attack Peaks

Up to

1.6M

RPS

Attack Length

More than

17 Hours

Total Packets

39 Billion

Requests

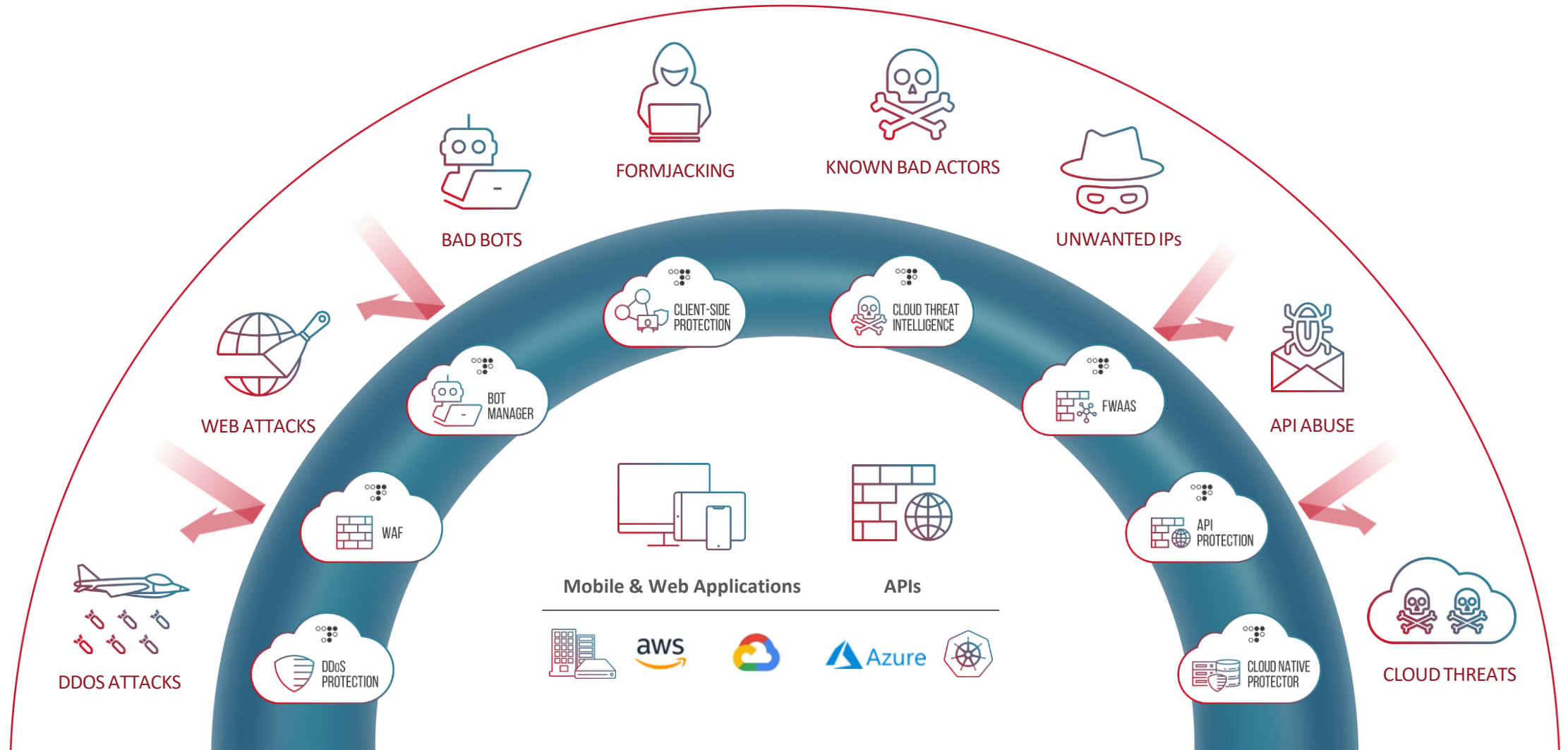
Network Attacks

Up to

200 Gbps

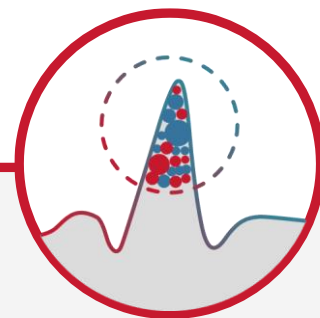
# Radware 360 Application Protection

Comprehensive, Adaptive, Managed Cloud Application Protection Service



# Adaptive, Automated

## No Human Intervention Required



### Network, Application DDoS Protection

Behavioral-based  
detection w/ real-time  
signature creation

Advanced protections for  
L7 DDoS, Burst and  
Encrypted attacks



### Next-Gen Web App Protection

Advanced ML to detect  
0-day & emerging attacks

Crypto-challenge bot  
mitigation

Client-side attack protection



# The Radware Difference



## Intelligent Security

Automated, real-time protections based on AI + ML-based algorithms that evolve as the attacks morph



## Consistent Protections

360-degree, consistent protection across all environments and entry points



## Expert Defense

Access to security experts 24/7 during attack and in peacetime

# Summary & Call to Action

# How to Stay Protected



1

Recent attack campaigns have given rise to **new web DDoS attacks**

2

These **attacks go undetected** by network-based DDoS protection or standard WAF solutions

3

Radware is the only solution that can protect your customer against emerging cyber aggressions

# Action Plan & Considerations



What is needed  
to get  
protected



1

Who can authorize a diversion to Cloud?  
Legal has to be involved

2

Who can issue a short-term certificate?  
DEV-Ops/SEC-Ops or other division

3

Who can change DNS for diversion?  
CNAME must be changed

A background image of a city skyline, likely Dubai, featuring the Burj Khalifa. The image is overlaid with large, semi-transparent geometric shapes in shades of blue and red. The text "Thank You!" is centered in the middle of the image.

# Thank You!