

# Security Best Practices for an Evolving Threat Landscape

May 25, 2023

# Agenda

- Escalation of the Threat Landscape
- DNS 'Watertorture' DDoS Attacks
- Conclusion / Q&A

# Today's Presenters



**Ron Meyran,**  
Senior Director, Cyber Threat Intelligence,  
Radware



**Dennis Uslé,**  
Director, Security Solutions Architecture, Radware



**Jim Hodges,**  
Research Director, Cloud and Security, Heavy Reading



# Escalation of the Threat Landscape

**Ron Meyran**

Senior Director, Cyber Threat Intelligence

May 2023

# Attacks Reaching New Heights

Radware Global Threat Analysis Report 2022

## DDoS ATTACK TRENDS



**150%**

Growth in number of attacks compared to 2021

**29.3**

Average number of attacks per day per customer at the end of 2022

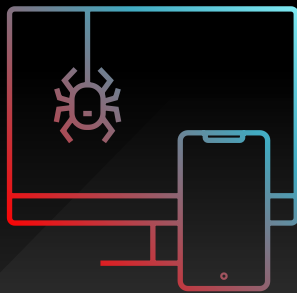
**18HRS**

Average duration of attacks above 500Gbps

**38**

Max number of dissimilar attack vectors in a single attack

## WEB APP ATTACK TRENDS



**128%**

Growth in web application transactions blocked

**75%**

Percent of attacks due to predictable resource location or injection attacks

**60%**

Share of activity directed at retail & wholesale trade, high tech, and carriers industries

# Threat Actors



Organized  
Crime



Angry  
People



Hacktivists



Competitors



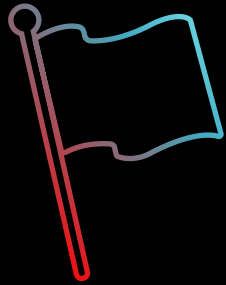
Skids



Nation  
States



# Catalysators For Increased Attack Surface



Patriotic  
Hacktivism



State-sponsored  
Attacks &  
Espionage



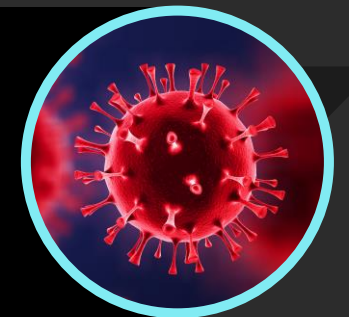
Digitalization

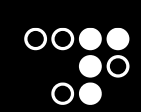


Range of  
Vulnerabilities

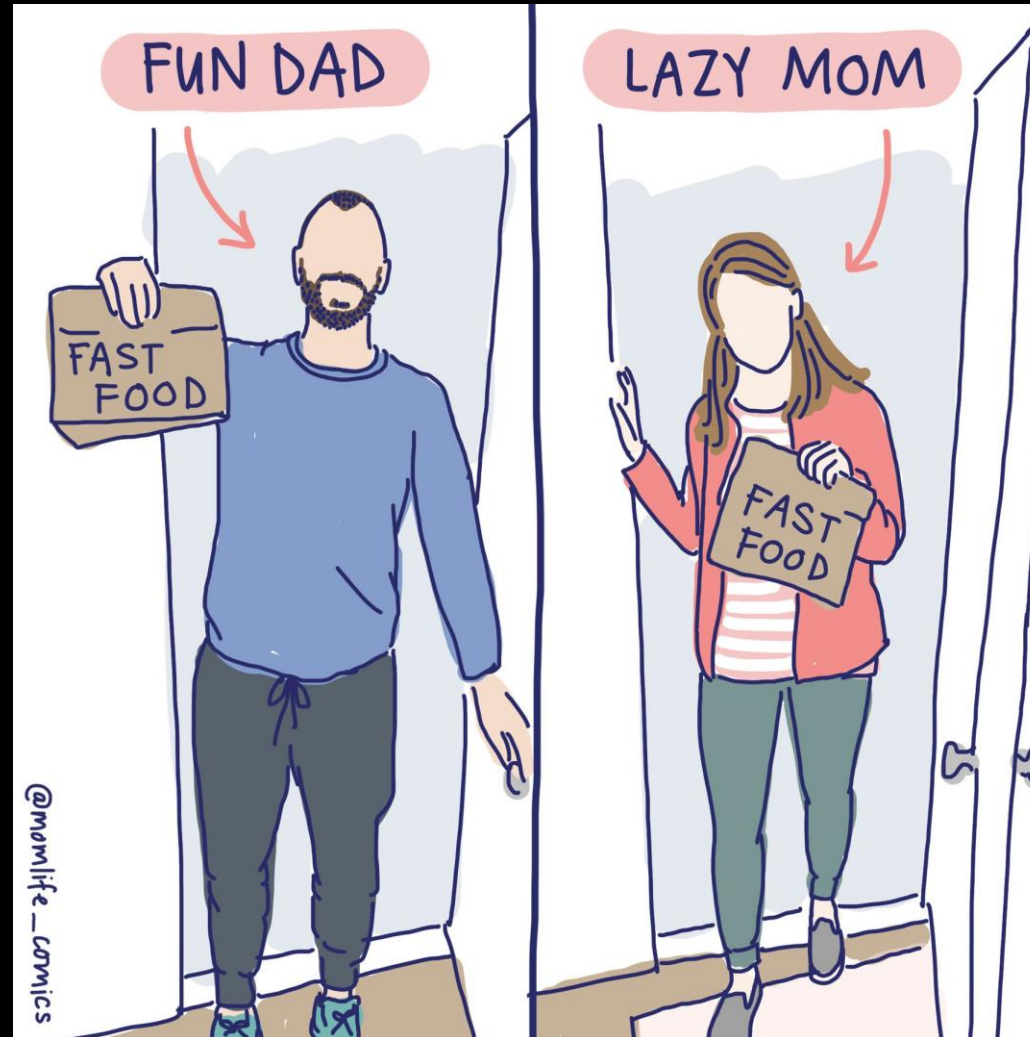


Catalysts of change  
Pivot point: Feb 24, 2022





# Double Standards





# New Actors, Tools and Tactics



**DISBALANCER UA**

### FATALITY FOR RUSSIAN PROPAGANDA

Launch *Liberator* to finish him [Putin and his false machine].

Russian media contributes to putin's aggression, with fake news constructing false reality and legitimizing violence against Ukrainians. *Liberator* is just one app that attacks their propaganda resources. Join the army, fight the aggressor!

[Download the App](#)



# Attack Campaign on Airports October 2022



**BLEEPINGCOMPUTER**

NEWS ▾ DOWNLOADS ▾ VIRUS REMOVAL GUIDES ▾ TUTORIALS ▾

## US airports' sites taken down in DDoS attacks by pro-Russian hackers

By Bill Toulas October 10, 2022 10:15 AM 3



*Update: Title of story modified to indicate it was the sites taken down.*

The pro-Russian hacktivist group 'KillNet' is claiming large-scale distributed denial-of-service (DDoS) attacks against websites of several major airports in the U.S., making them inaccessible.




Notable examples of airport websites that are currently unavailable include the Hartsfield-Jackson Atlanta International Airport (ATL), one of the country's larger air traffic hubs, and the Los Angeles International Airport (LAX), which is intermittently offline or very slow to respond.

www.atl.com | 522: Connection | x

Added security | https://www.atl.com

### Connection timed out Error code 522

Visit [cloudflare.com](https://cloudflare.com) for more information.  
2022-10-10 13:03:14 UTC

 You Browser Working	 Newark Cloudflare Working	 www.atl.com Host Error
--	--	---

**WE ARE KILLNET**

Ваш выход хакеры 🇺🇸  
Список ниже для Вас!

Аэропорты :

- Атланта - <https://www.atl.com>
- Алабама - <https://www.flybirmingham.com>  
<http://www.gadsdenairport.com>  
<https://flymgm.com>
- Аризона - <https://deervalleyairport.com>  
<https://www.gatewayairport.com>  
<https://www.skyharbor.com>
- Арсанзас - <https://www.flyxna.com>  
<https://flyield.com>
- Калифорния - <https://www.flylax.com/>  
<https://www.flyontario.com>  
<https://www.longbeach.gov/lgb/>
- Колорадо - <https://www.flydenver.com>  
<https://coloradosprings.gov/flycos>  
<https://www.flydurango.com>
- Коннектикут - <https://bradleyairport.com>
- Делавэр - <http://www.newcastleairportilg.com>  
<https://delawarecoastalairport.com>
- Флорида - <https://www.mlhair.com>  
<https://flylcpa.com>  
<https://orlandoairports.net>
- Джорджия - <https://www.atl.com>  
<http://www.cityofdouglas.com/index.aspx?NID=95>
- Гавайи - <https://airports.hawaii.gov/hnl/>
- Айдахо - <https://www.flyboise.com>  
<https://iflysun.com>  
<https://www.idahofallsidahogov/181/Airport>
- Иллинойс - <https://cira.com>  
<https://www.flychicago.com/ohare/home/pages/default.aspx>  
<https://flycu.com>
- Индиана - <https://www.indianapolisairport.com>
- Айова - <http://www.dsmaairport.com>  
<https://flycid.com> <http://www.flyalo.com>
- Канзас - <https://www.flykci.com>
- Кентукки - <http://cca.ky.gov> <https://www.flylouisville.com>  
<https://www.cvgairport.com>
- Луизиана - <https://flymsy.com>  
<https://www.flyaex.org>
- Мэриленд - <https://www.bwiairport.com>
- Массачусетс - <https://aeromanagementilc.com>
- Мичиган - <https://westmichiganregionalairport.com>
- Миннесота -  
<https://www.msairport.com>
- Миссисипи - <https://jmaa.com>  
<http://www.flygpt.com>  
<https://www.meridianairport.com>
- Миссури - <https://www.flystl.com>  
<https://nwregionalair.com>

👍 1179 🔥 453 👍 150 🎉 28 ❤️ 17 🍷 12 🧑 7 ⚡ 7 🌪️ 5 🍌 4 🍌 2

👁️ 25.1K 1:50 PM

163 comments



# Attach Campaign On Health Care February 2023


SC MEDIA TOPICS INDUSTRY EVENTS PODCASTS RESEARCH RECOGNITION

Threat intelligence, Application security, Vulnerability management

f t e 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

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>

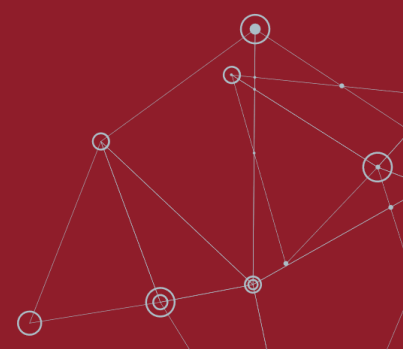
Florida  
<https://www.leehealth.org>  
<https://check-host.net/check-report/e77fbeck78c>

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



# Russian/Ukraine Conflict Ignites New Cyber War Era

Conflict extended beyond the two countries



## Pro-Russian Hacktivist Groups

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

Attacking targets in countries that are  
supporting Ukraine



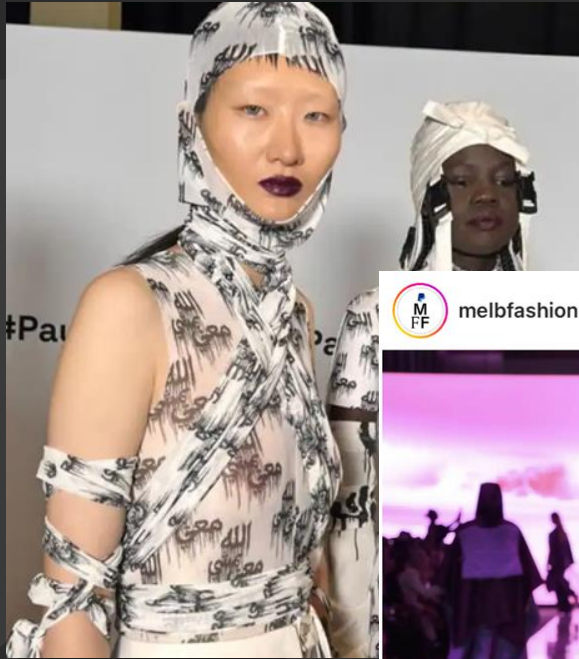
## Religious Groups

Anonymous Sudan, Mysterious Team  
Bangladesh, DragonForce Malaysia, etc

Cyber attacks against targets who  
supposedly insulted Muslims

# NOT A MAN'S DREAM

SYDNEY, NSW, AUSTRALIA

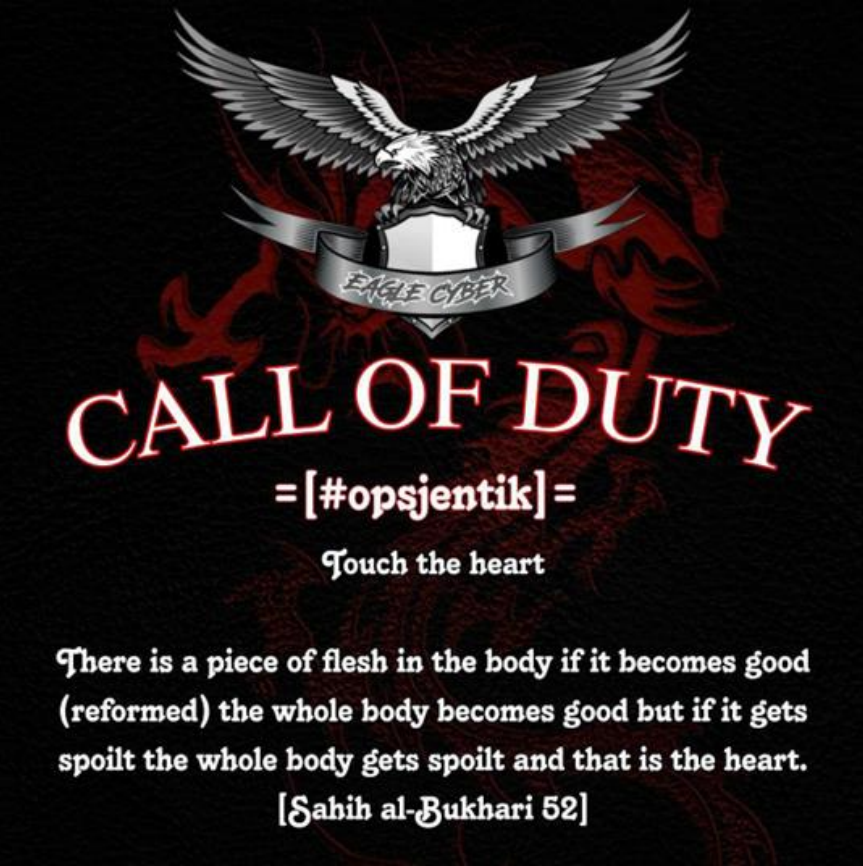


During the final show of the Melbourne Fashion Festival, Not A Man's Dream caused a shock wave across the Muslim community by featuring models wearing designs with “Allah walks with me” (الله يمشي معي)

March 11,  
Melbourne Fashion Festival



# Several Muslim hacktivist groups join hacktivist crews Team insane pk, Eagle Cyber, and Mysterious Team in #OpAustralia and #opsjentik



March 11,  
Melbourne Fashion Festival

#OpAustralia, #opsjentik



As of Friday, March 17, Not A Man's Dream became a prominent target for Muslim hacktivists

Large scale denial-of-service and website defacement campaign targeting Australia started on Saturday, March 18

Over 70 Australian sites—including the public websites of governments, ports, banks, and private businesses—have been the target of denial-of-service attacks

March 11,  
Melbourne Fashion Festival

#OpAustralia  
#opsjentik

March 17  
First DDoS attacks

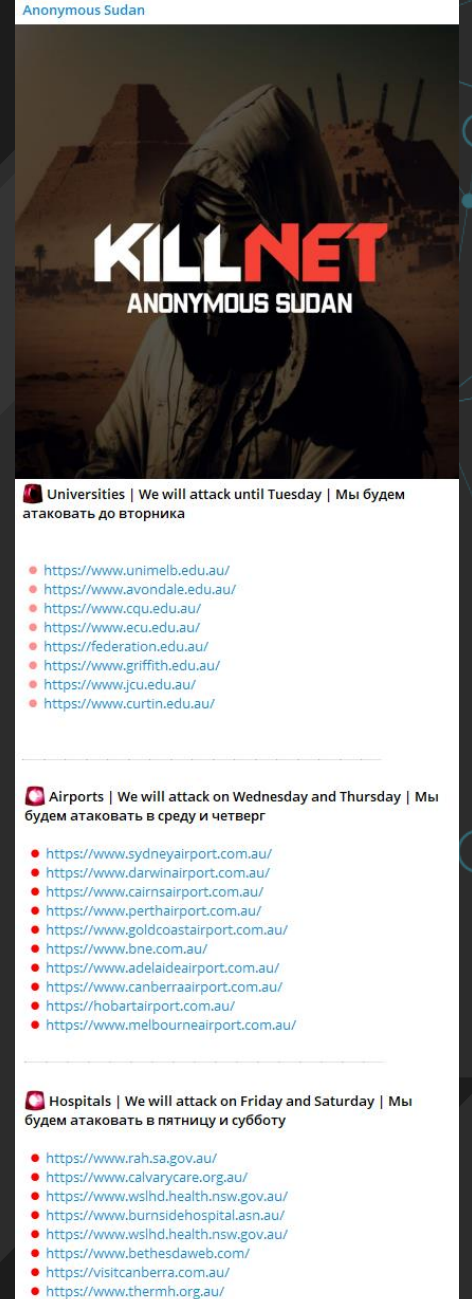
# On Friday, March 24, Anonymous Sudan joins his Muslim hacktivist brothers' campaign

After assaulting Sweden, Denmark and France, announces attacks on Australia

- Universities until Tuesday
- Airports on Wednesday and Thursday
- Hospitals on Friday and Saturday

Called in the help from the Killnet cluster, which it became member of after its attacks on Sweden and Denmark

To date, Killnet and Anonymous Russia ignored the call



March 11,  
Melbourne Fashion Festival

#OpAustralia  
#opsjentik

March 17  
First DDoS attacks

March 24  
Anonymous Sudan

# #OpIsrael

- Yearly escalation of attacks till April 7





# #OpIsrael 2023 – Take II

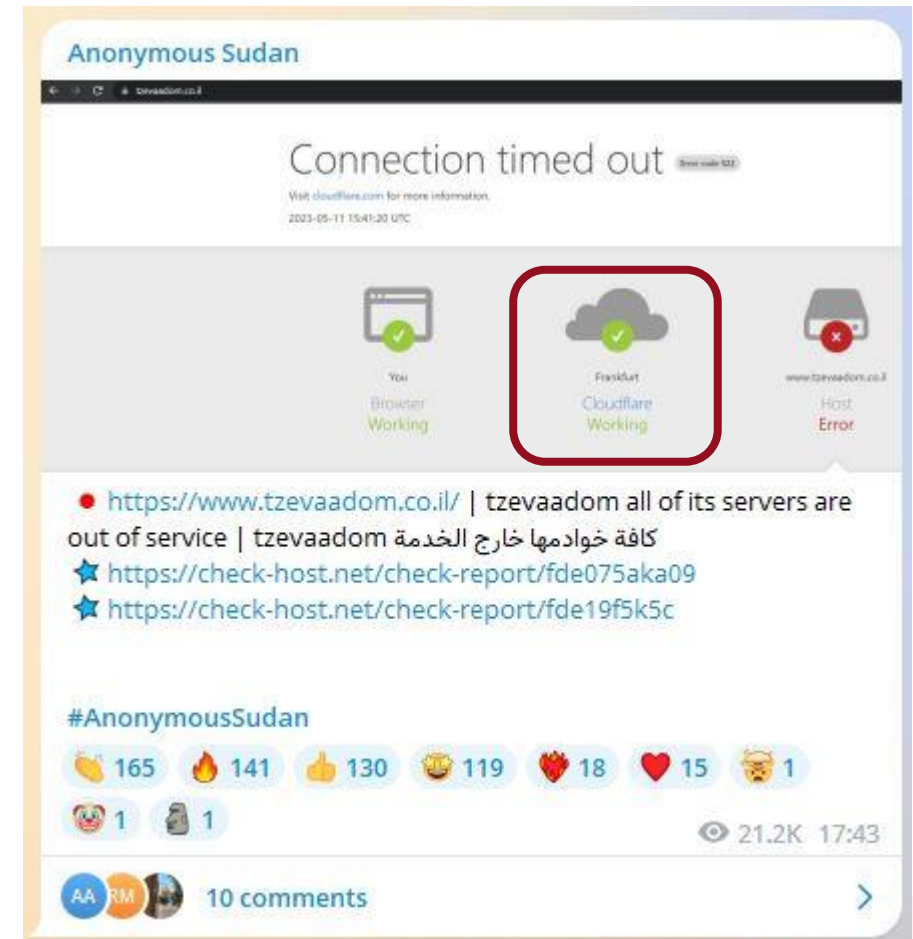
May 9-13, 2023

- Anonymous Sudan joins the Islamic Jihad starting a cyber war against Israel
- Attacks against Israeli sites:
  - Government Agencies
  - Utilities
  - Energy
  - Civil defense
- We followed two sites:
  - Red Colour
  - Rotter



# #OpIsrael 2023 – Red Colour

- Red Colour (in Hebrew: Tzevaadom - צבע אדום)
  - An early-warning radar system that warns civilians of imminent attack by rockets
  - On May 11, 6:17PM, Israel time, **Red Colour system is down for more than 3 hours**
  - Cyber security solution is... Cloudflare

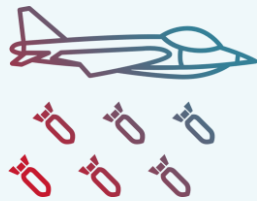


# Recent Campaigns Introduce Disruptive L7 DDoS Attacks

Existing protection solutions fail to protect!



Higher in volume –  
**Ultra high RPS**



**Encrypted floods** that  
appear as **legitimate  
user traffic**



Multiple, **sophisticated  
evasion** techniques  
(randomized headers,  
behind proxies, etc.)





# Escalation of the Threat Landscape

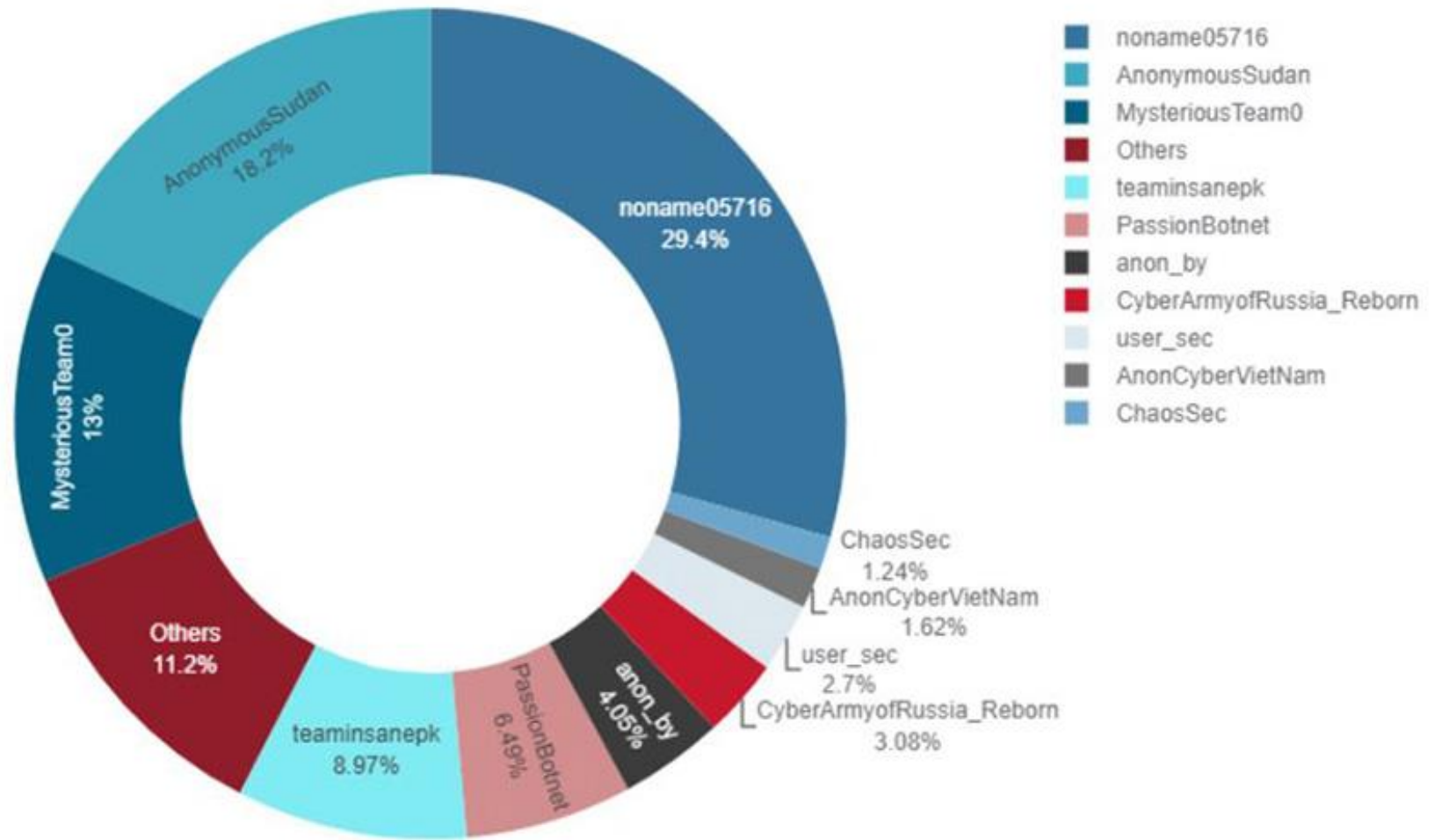


Apr 12 10:30:26	noname05716eng	<a href="#">1121</a>	<p>▼ Canada has expanded sanctions against Russia - 14 individuals and 34 legal entities were subject to restrictions 🇺🇸 The site of the Canadian bank Laurentian Bank was slammed: ❌ <a href="https://check-host.net/check-report/f8732e2kbb">https://check-host.net/check-report/f8732e2kbb</a> 📌 **Subscribe to** [NoName057(16)](<a href="https://t.me/noname05716">https://t.me/noname05716</a>) 🐾 **Join our** [DDoS-project](<a href="https://t.me/+fiTz615tQ6BhZWFj">https://t.me/+fiTz615tQ6BhZWFj</a>)** ⚠️ Subscribe to** [reserve channel](<a href="https://t.me/noname05716_reserve">https://t.me/noname05716_reserve</a>)ru**Victory will be ours!**</p>	
Apr 12 10:58	Apr 12 14:06:16	MysteriousTeam0	<a href="#">3251</a>	<p>[Repeat](<a href="https://t.me/noname05716/2767">https://t.me/noname05716/2767</a>) we put the official website of Canadian Prime Minister Justin Trudeau, who most recently [retweeted](<a href="https://t.me/noname05716/2775">https://t.me/noname05716/2775</a>) that "is not afraid Russian hackers" 🤖: ❌ <a href="https://check-host.net/check-report/f87d22bka5">https://check-host.net/check-report/f87d22bka5</a> Expect Us 🐾</p>
Apr 12 11:46	Apr 12 14:42:20	MysteriousTeam0	<a href="#">3254</a>	<p>#OpIsrael #Opspetir #FreePalestine Israeli 3 University website dropped.. <a href="https://www.openu.ac.il/">https://www.openu.ac.il/</a> Open University Of Israel <a href="https://check-host.net/check-report/f87e378k46e">https://check-host.net/check-report/f87e378k46e</a> <a href="https://in.bgu.ac.il/en/pages/default.aspx">https://in.bgu.ac.il/en/pages/default.aspx</a> Ben Gurion University <a href="https://check-host.net/check-report/f87e715k745">https://check-host.net/check-report/f87e715k745</a> <a href="https://huji.ac.il/en">https://huji.ac.il/en</a> Hebrew University Jerusalem <a href="https://check-host.net/check-report/f87e4f8ke93">https://check-host.net/check-report/f87e4f8ke93</a> Fck Israel.. Expect Us 🐾</p>
Apr 12 17:28:38		MysteriousTeam0	<a href="#">3264</a>	<p>&gt;&gt;&gt; Message forwarded by 'Mysterious Silent Force' &lt;&lt;&lt; Hello Denmark CERT!!! We just launched a testing attack now.. Get Ready for 16th April. Denmark CERT official website shut down for burning Quran.. <a href="https://www.cert.dk/">https://www.cert.dk/</a> <a href="https://check-host.net/check-report/f884d58k8">https://check-host.net/check-report/f884d58k8</a> Expect Us 🐾 --&gt; Mysterious Silent Force.</p>
Apr 12 18:32:49		MysteriousTeam0	<a href="#">3265</a>	<p>&gt;&gt;&gt; Message forwarded by 'Mysterious Silent Force' &lt;&lt;&lt; Greetings Danish National Bank!! A test attack launched on your cyberspace... Get Ready..16th April.. Danish National Bank website shut down for burning Quran... <a href="https://www.nationalbanken.dk/en/Pages/Default.aspx">https://www.nationalbanken.dk/en/Pages/Default.aspx</a> <a href="https://check-host.net/check-report/f886e4dk909">https://check-host.net/check-report/f886e4dk909</a> Expect Us 🐾 --&gt; Mysterious Silent Force.</p>

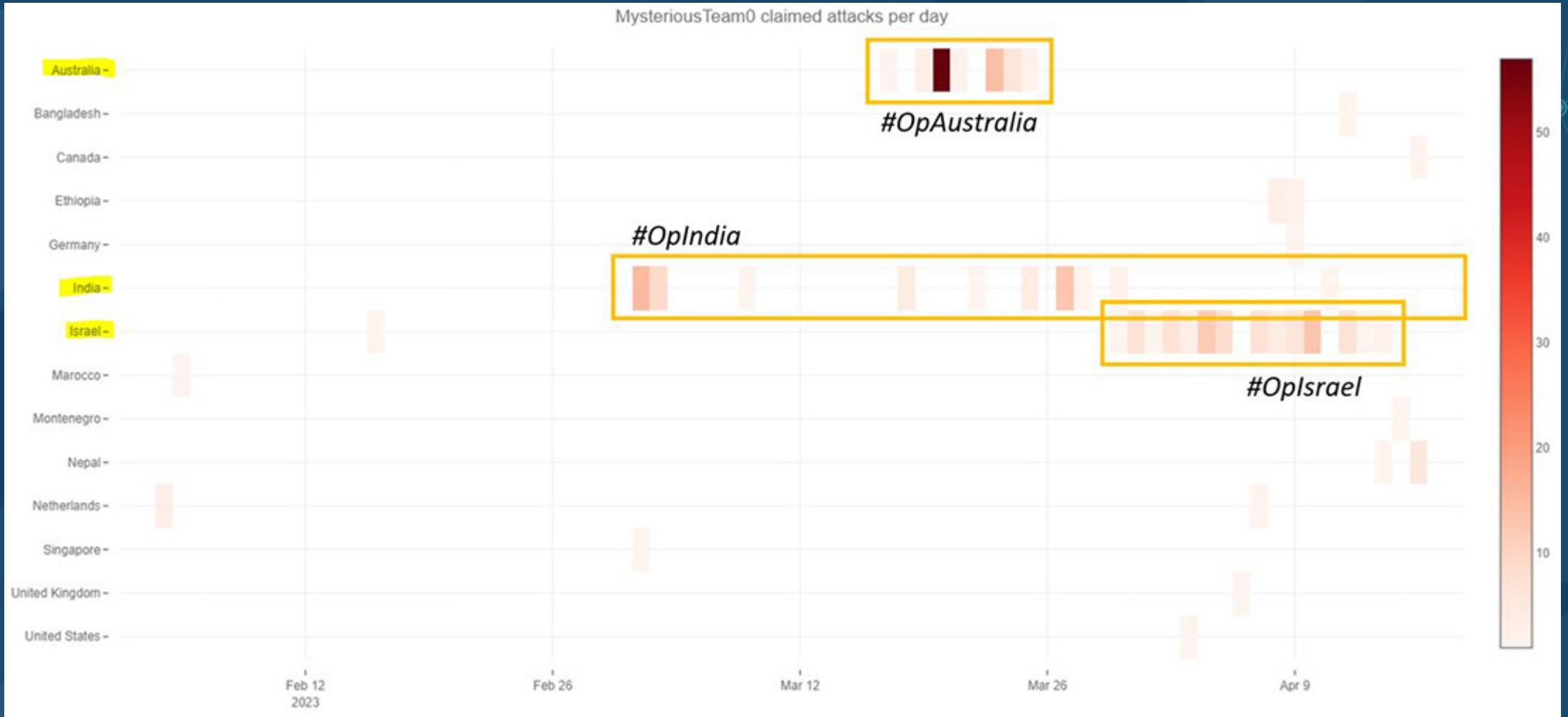
# Top Claiming Actors

NoName057(16) claimed almost 30% of the attacks, followed by Anonymous Sudan (18%) and Mysterious Team (13%)

Top Claiming Actors



# Mysterious Team claimed attacks by country

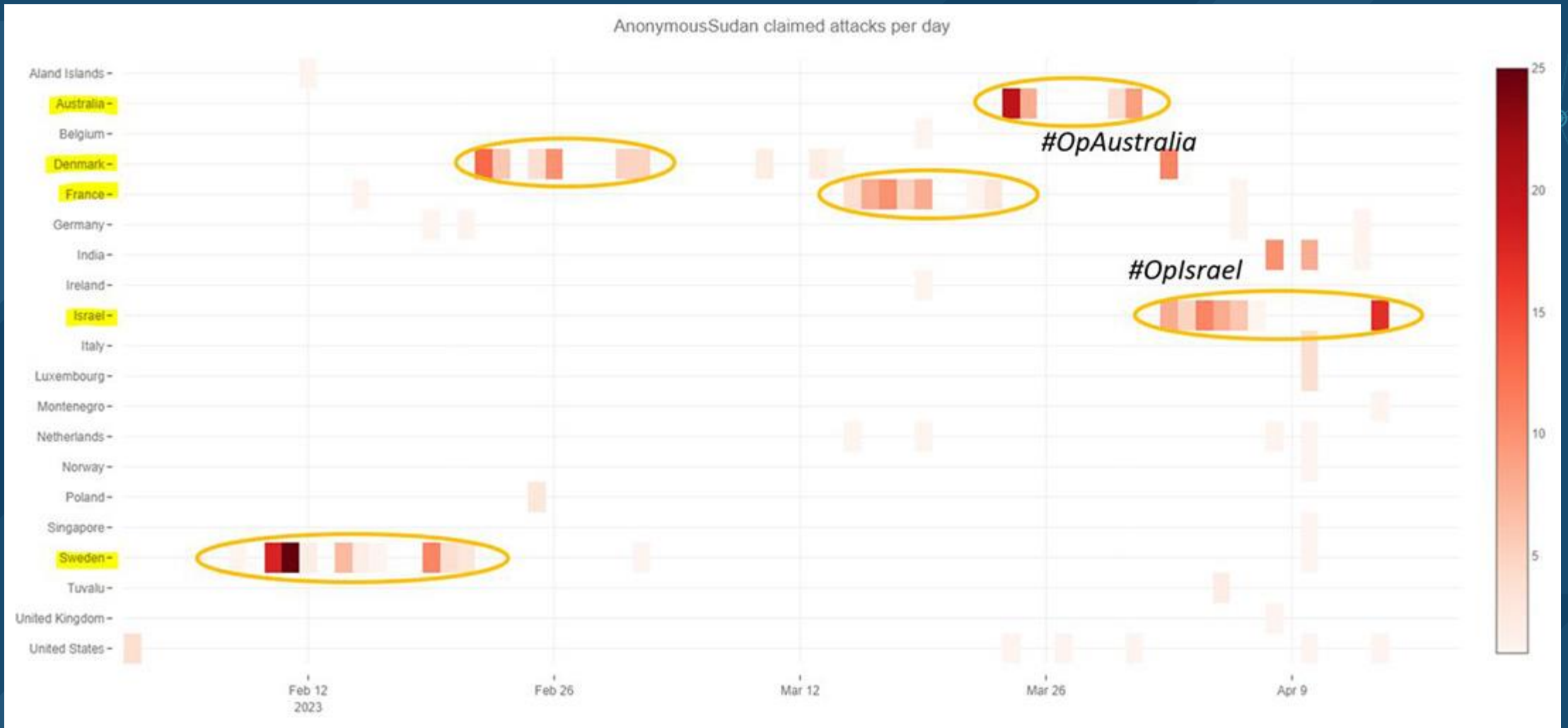


# Team Insane PK claimed attacks by country

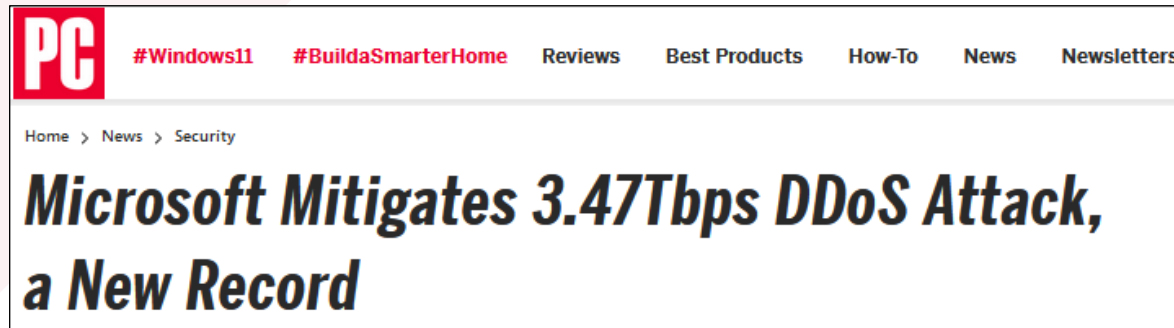




# Anonymous Sudan claimed attacks by country



# Service Providers Under Attack



PCMag #Windows11 #BuildASmarterHome Reviews Best Products How-To News Newsletters

Home > News > Security

## Microsoft Mitigates 3.47Tbps DDoS Attack, a New Record



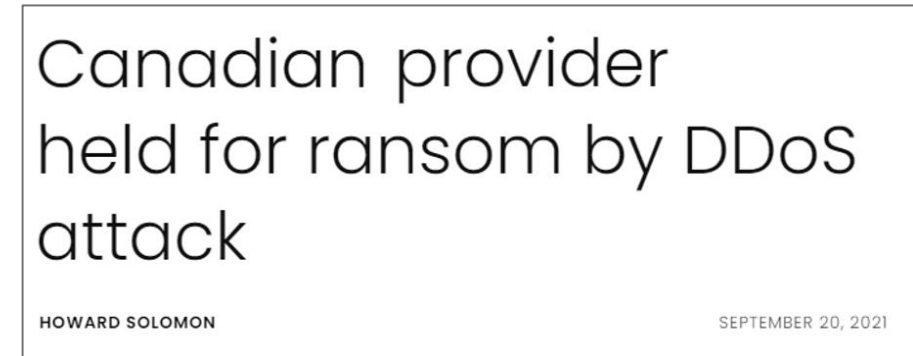
techradar.pro IT INSIGHTS FOR BUSINESS US Edition

## Ransomware actors target VoIP service with another wave of DDoS attacks



The Record.  
BY RECORDED FUTURE

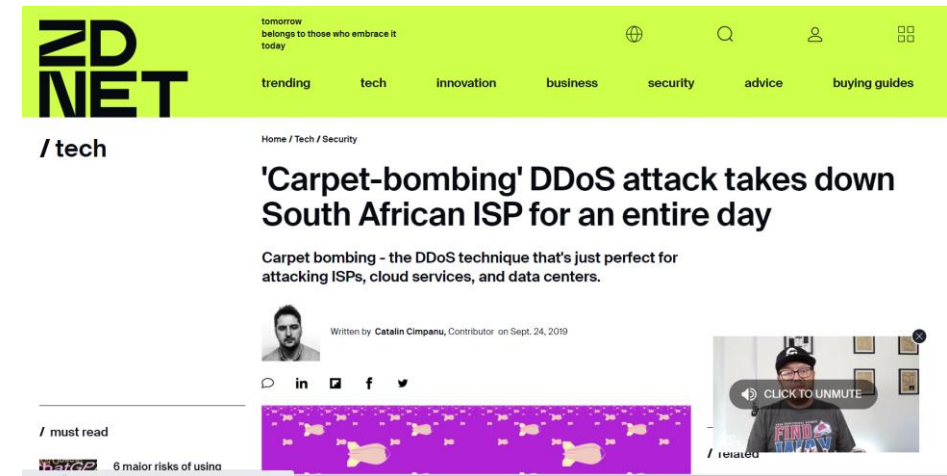
## DDoS attacks hit multiple email providers



## Canadian provider held for ransom by DDoS attack

HOWARD SOLOMON

SEPTEMBER 20, 2021



ZDNET

tomorrow belongs to those who embrace it today

trending tech innovation business security advice buying guides

Home / Tech / Security

## 'Carpet-bombing' DDoS attack takes down South African ISP for an entire day

Carpet bombing - the DDoS technique that's just perfect for attacking ISPs, cloud services, and data centers.

Written by Catalin Cimpanu, Contributor on Sept. 24, 2019

in f

must read

6 major risks of using

related

# MIRAI, KAYE aka "BESTBUY" MTS vs CELLCOM



"THERE IS NO SUGGESTION THAT CELLCOM KNEW WHAT THE EMPLOYEE WAS DOING - BUT THE INDIVIDUAL OFFERED KAYE UP TO \$10,000 (£7,800) A MONTH TO USE HIS SKILLS TO DO AS MUCH AS POSSIBLE TO DESTROY LONESTAR'S SERVICE AND REPUTATION."

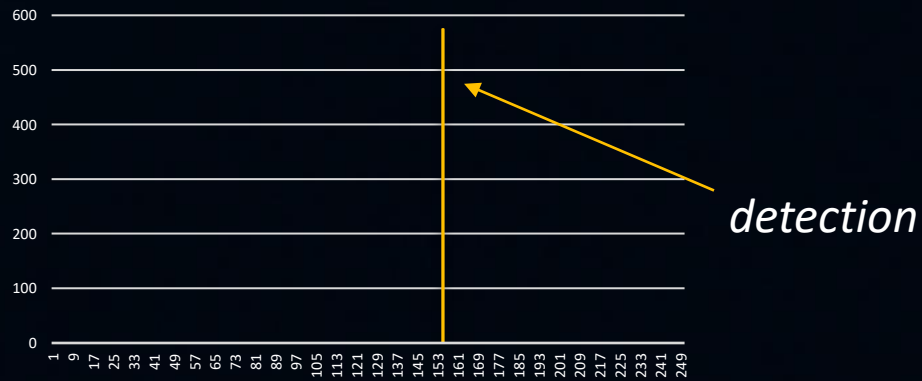


# Carpet Bombing

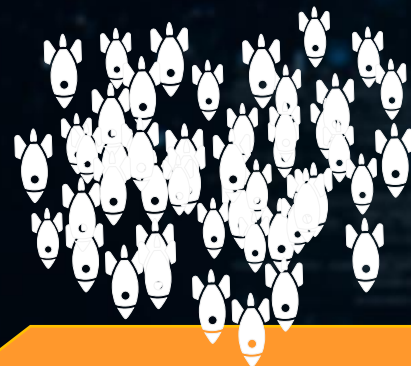
## Targeted DDoS



Victim IP

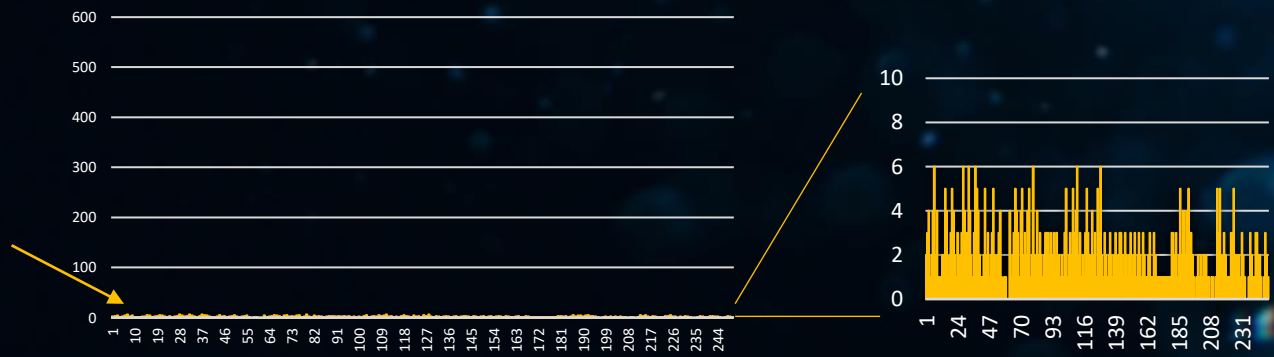


## Carpet Bombing DDoS



Victim ASN

*Spread attack traffic randomly across all IP in victim AS*

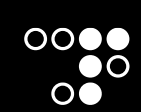


# Attacks on DNS Infrastructure



➔ The DNS infrastructure is A single-point-of-failure for all web traffic, setting an ideal opportunity for attackers





# Where do I go from here?

- Keep an open and critical mind
- Be prepared – where is your incident response plan?
- Red teaming – the attacker mindset
- Act as you were at war: “Shields Up!”



A background image of Earth from space, showing the curvature of the planet and city lights at night. The image is overlaid with several semi-transparent, dark blue geometric shapes (triangles and rectangles) that create a layered, abstract effect.

# Thank You



# DNS 'Watertorture' DDoS Attacks

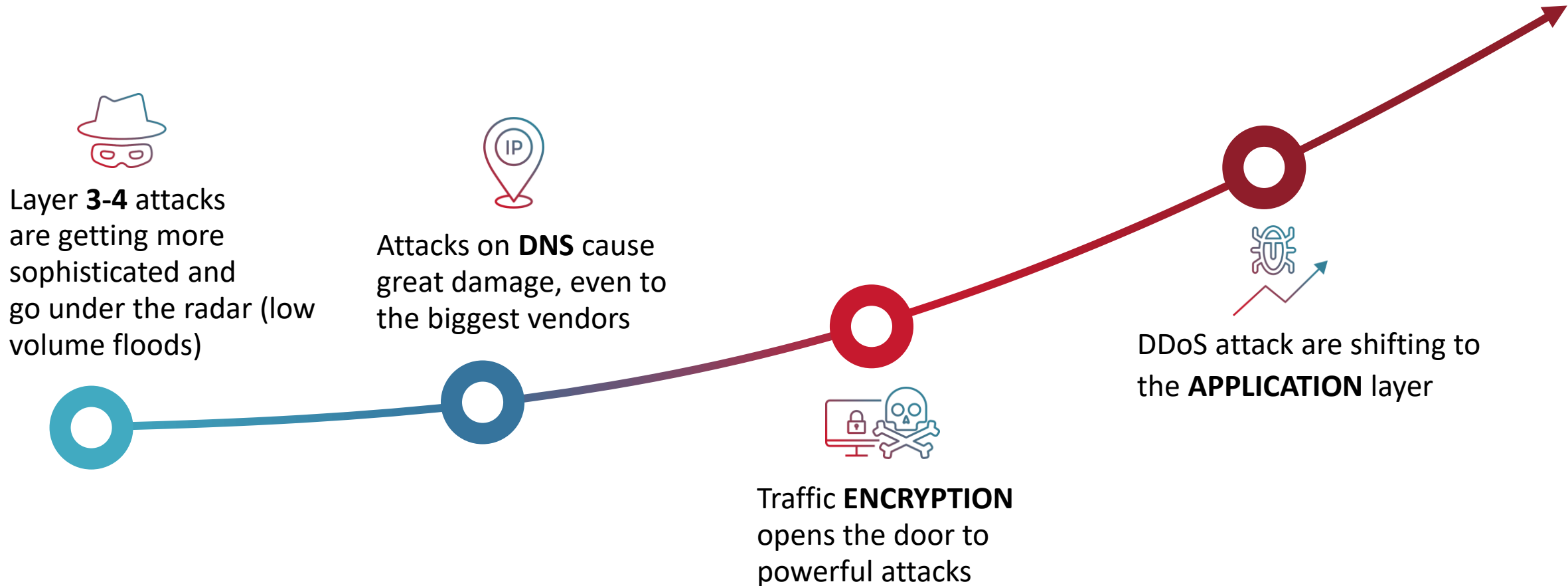
**Dennis Usle**

Director, Security Solutions Architecture

May 2023

# Anatomy of Advanced Cyber Attacks

Are organizations evolving as dynamically as the threats are?



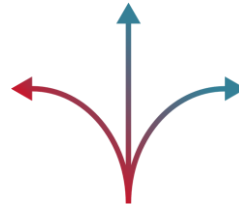


# Challenges with DNS Protection



## Attack Coverage

New sophisticated attackers take advantage of the DNS-protocol behavior to generate more powerful attacks



## Deployment Flexibility

Bi-directional deployment only with detection based on DNS error responses which is often too late for the DNS server



## Protection Accuracy

Failure to distinguish between legitimate & attack DNS queries results in false positives and requires manual protection

**Knocking-out the DNS infrastructure of an organizations means cutting-off access to all web-based assets**

# DNS Attack: History



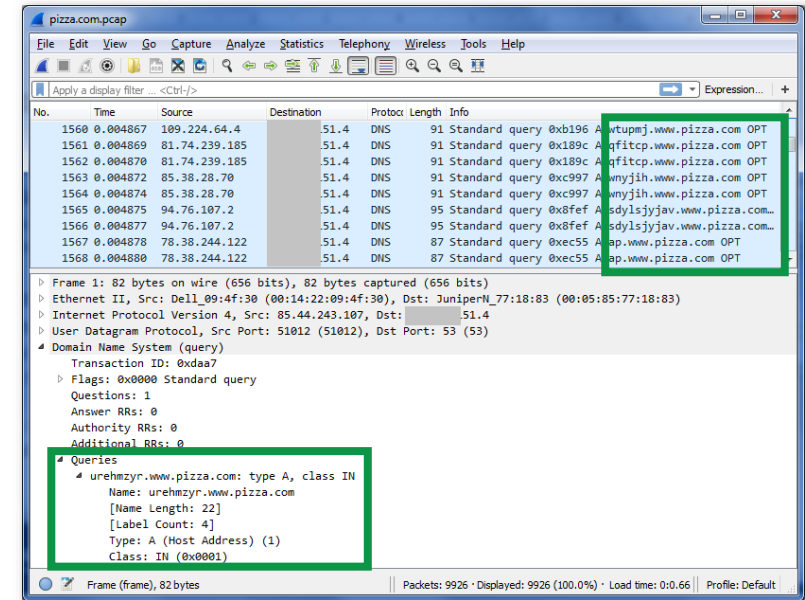
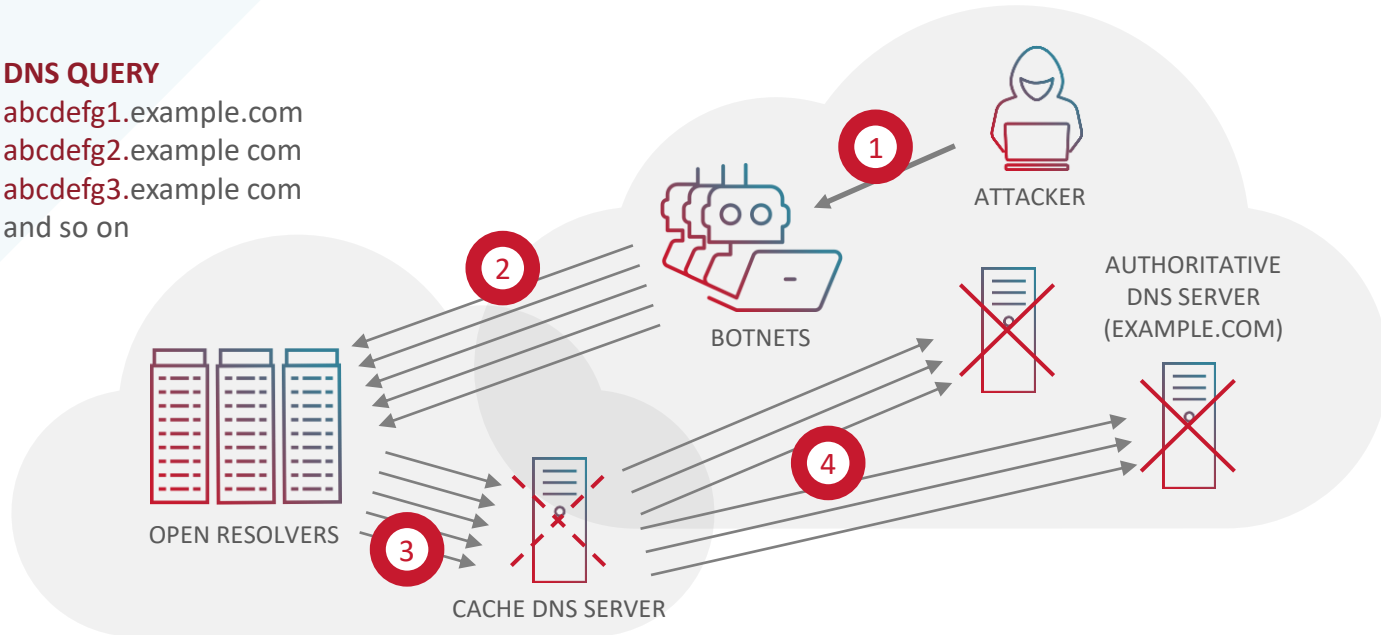
➔ The DNS infrastructure is a single-point-of-failure for all web traffic, setting an ideal opportunity for attackers



# DNS Attack: Anatomy of 'Water Torture'

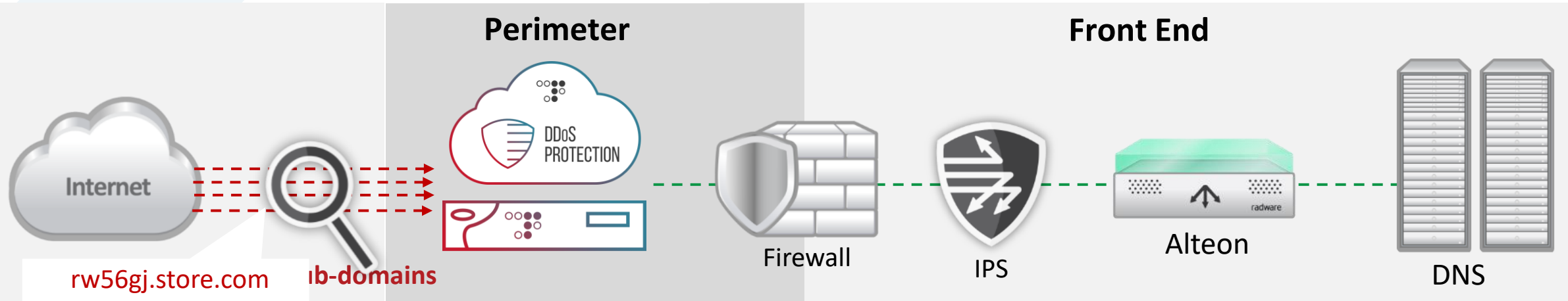
## DNS QUERY

abcdefg1.example.com  
abcdefg2.example.com  
abcdefg3.example.com  
and so on



- 1 The Attacker commands his botnets
- 2 Many bots start to send a small number of random queries to open resolvers
- 3 Open resolvers send random queries to Cache DNS Servers
- 4 Cache DNS Servers send random queries to Authoritative DNS Servers

# Random Subdomains Flood – Non Radware



rw56gj.store.com  
www.store.com  
www.store.com  
gjk78j.store.com  
kl9pvb.store.com  
9486hggj.store.com  
history.store.com  
h7n6mi.store.com  
checkout.store.com  
www.store.com  
www.store.com

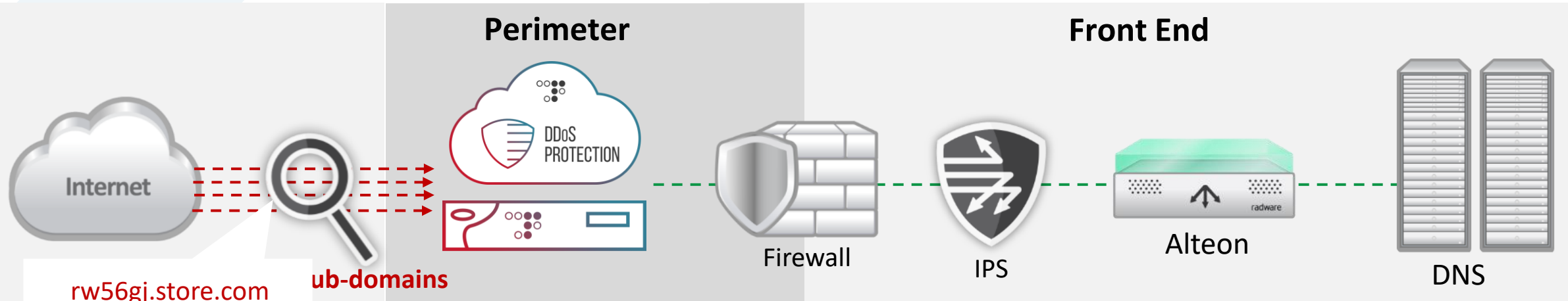
ib-domains



**QPS Rate-Limit**  
Prone to False Positive



# Random Subdomains Flood – Radware



rw56gj.store.com  
www.store.com  
www.store.com  
gjk78j.store.com  
kl9pvb.store.com  
9486hggj.store.com  
history.store.com  
h7n6mi.store.com  
checkout.store.com  
www.store.com  
www.store.com

ub-domains



**Block:** \*.store.com

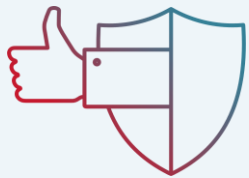


**Allow:** www.store.com, history.store.com, checkout.store.com

# DNS Attack: Protection

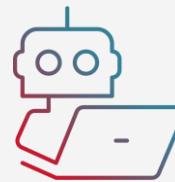


## Allowlist



- Allowlist enforcement
- 24x7 or under attack
- FQDN to prevent dictionary

## DNS Anti-Spoofing



- Improved DNS C/R
- NS-record challenge
- Reduce risks of false positives

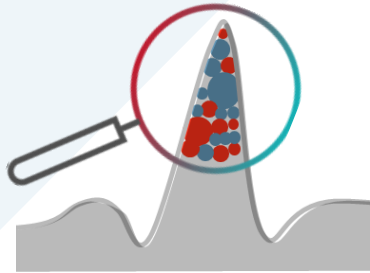
## Carrier/SP Focus



- New DNS tunneling threats
- DNS over HTTPS
- Enriched visibility

**Eliminate randomization attacks – the only automated behavioral solution for this type of DNS threat!**

# Radware High-Level Attack Mitigation Technology



## BEHAVIORAL-BASED DETECTION

Patented algorithm with  
limited false positives



## REAL TIME SIGNATURE CREATION

Block 0-day attacks in seconds



## BEYOND SOURCE IP BLOCKING

Blocking Dynamic IP  
& behind-the-CDN attacks



## DEDICATED ATTACK HARDWARE

With no impact on  
legitimate traffic

# Thank You!