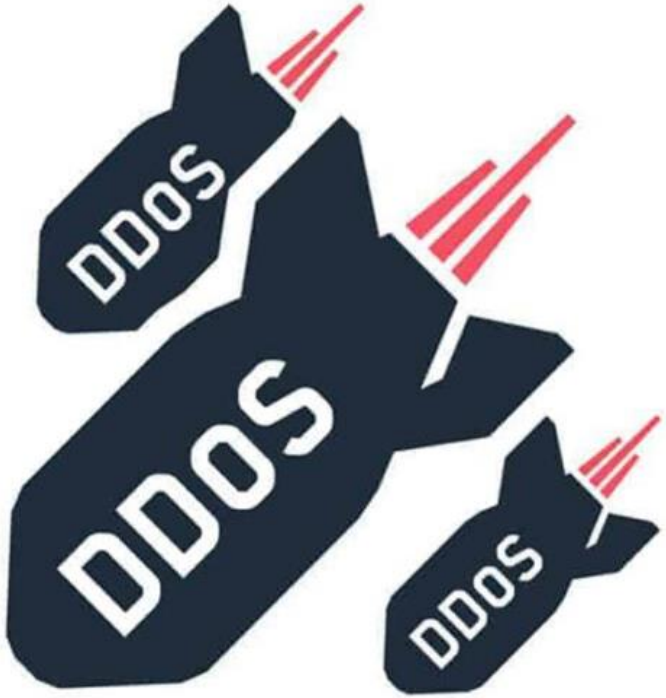
The Worldwide DDoS Landscape: Implications for Greek Digital Resilience

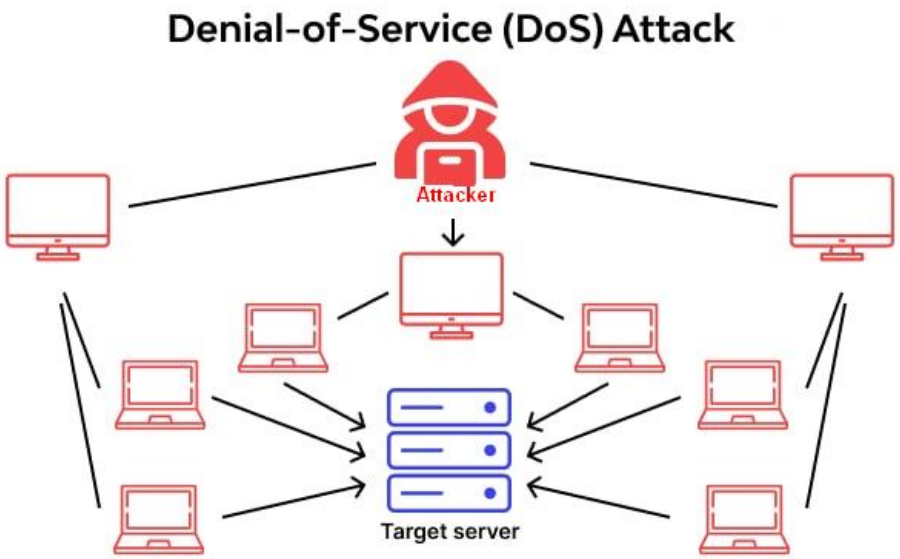
Το παγκόσμιο τοπίο των επιθέσεων DDoS: Επιπτώσεις στην ψηφιακή ανθεκτικότητα της Ελλάδας

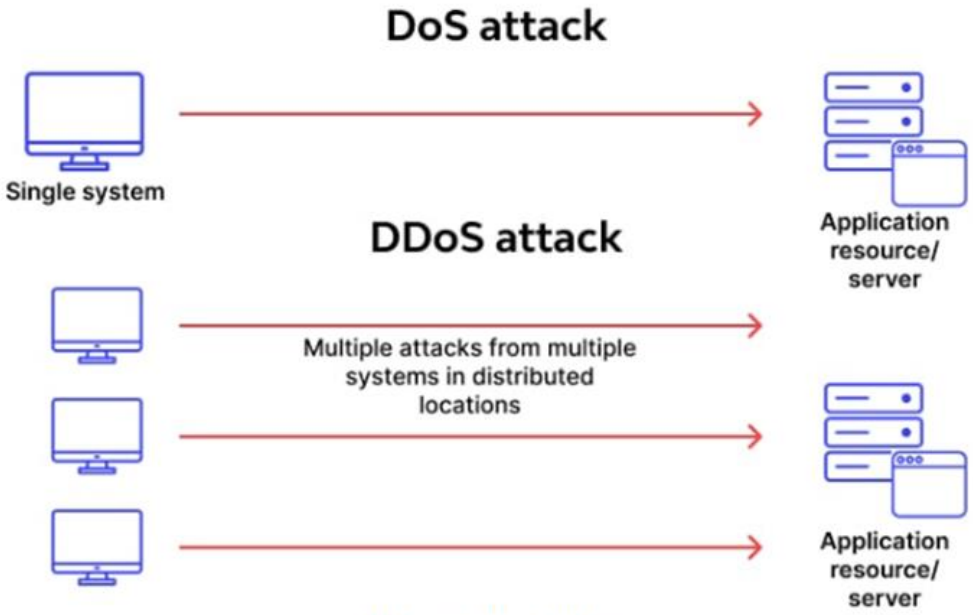
Konstantinos.Chatzithomaoglou@nova.gr
Nova S.A



- DDoS : What, Where, How, Why...Why me ?
- Global and local findings : Statistics and Trends !
- The Greek DDoS fortress : RUReady?
- European NIS2 directive and DORA Regulation
- Solution : There is no one solution
- What's next : The war is AI driven

DDoS : What, Where, How, Why...Why me ?





DDoS vs Dos attack

3+1 main types of attack :

1. **Volumetric**: Very large volume of data to the client (the favorite habit of attackers, often using UDP)
2. **Protocol Layer**: Usually TCP, exploits characteristics-weaknesses of the protocol and exhausts the server's resources.
3. **Application layer**: Smaller volume targeting public services (http/https etc)
4. **Bonus attack!** All of the above combined.

DDoS : What, Where, How, Why...Why me ?

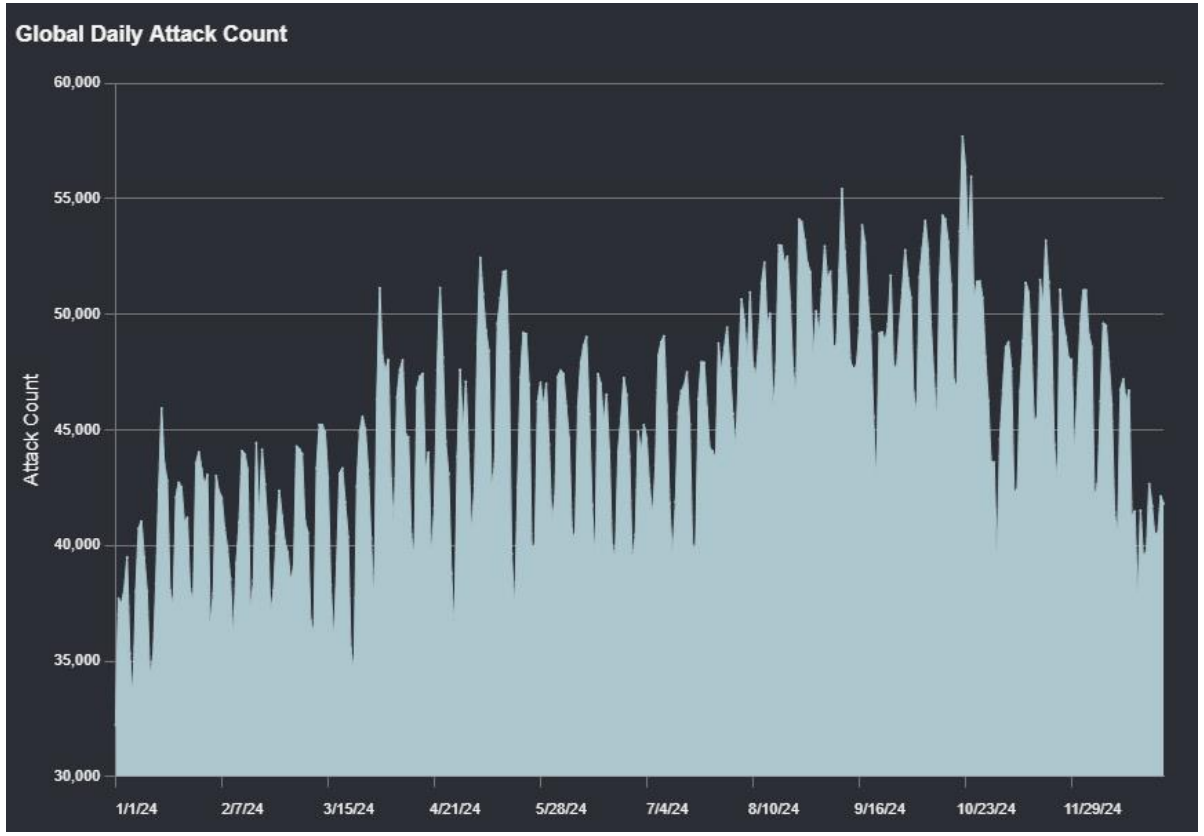
The Worldwide DDoS Landscape: Implications for Greek Digital Resilience

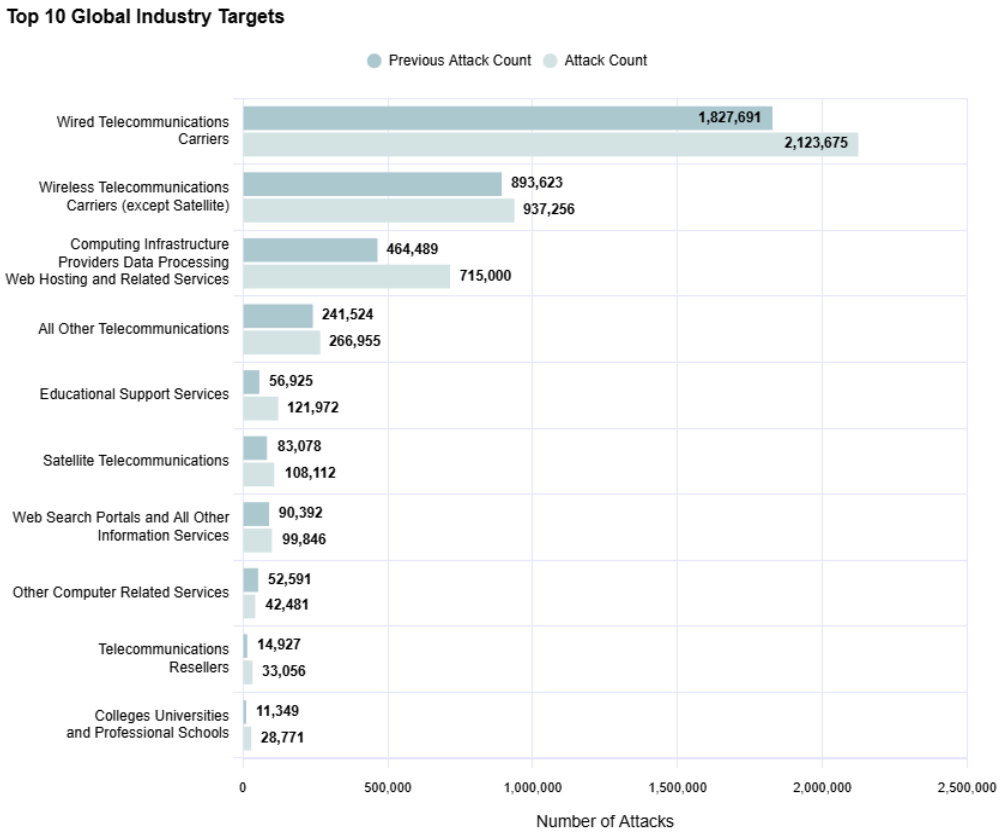
Global and local findings : Statistics

Global Highlights

Attack Count 8,911,312

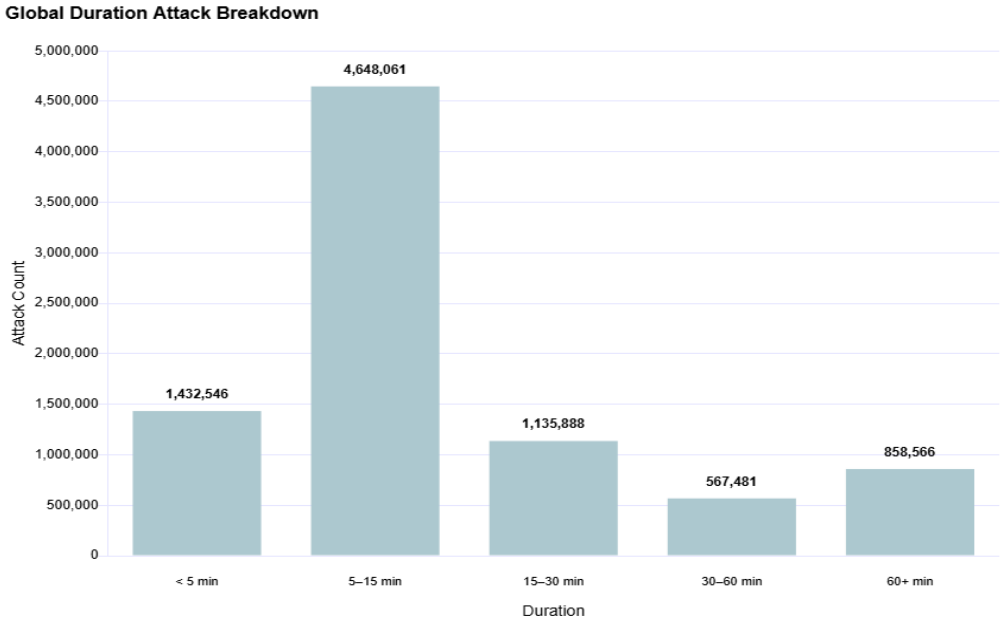
+12.75% change over 7,903,369 in 1H 2024





The Worldwide DDoS Landscape: Implications for Greek Digital Resilience

Global and local findings : Statistics - Current Trend

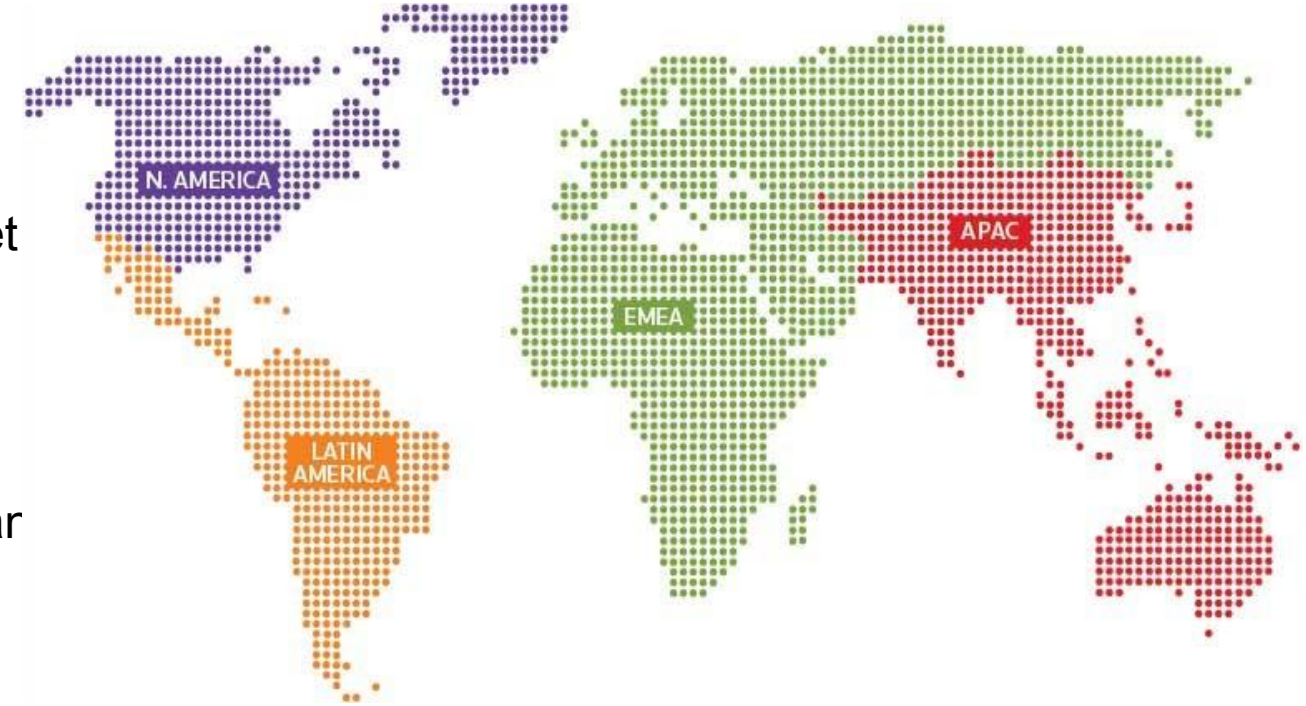


DURATION BY PERCENTAGE	
< 5 min	16.58%
5-15 min	53.78%
15-30 min	13.14%
30-60 min	6.57%
60+ min	9.93%

BANDWIDTH BY PERCENTAGE	
<10Mbps	19.94%
10-100Mbps	19.32%
100Mbps-1Gbps	35.57%
1-10Gbps	20.81%
10-100Gbps	4.15%
>100Gbps	0.21%

Global and local findings : Statistics NAMER + EMEA

NAMER
Largest Attack by Throughput Date 12/25/2024
Max Throughput **540.43Mpps** (Average Packet Size 217 Bytes)
Largest Attack by Bandwidth Date 12/25/2024
Max Bandwidth **941.22Gbps**
Vectors TCP ACK, TCP RST, TCP SYN, TCP SYN/ACK Amplification, Total Traffic (Target



EMEA
Largest Attack by Throughput Date 08/07/2024
Max Throughput **650.84Mpps**
Average Packet Size 132 Bytes (Target Azerbaijar
Largest Attack by Bandwidth Date 12/09/2024
Max Bandwidth **994.36Gbps**
Average Packet Size 1,499 Bytes
Vectors TCP ACK, Total Traffic (Target Germany)

The Worldwide DDoS Landscape: Implications for Greek Digital Resilience

Global and local findings : **Greece 2H 2024**

LARGEST DDoS ATTACK STATISTICS

Max Bandwidth	301.28 Gbps
Max Throughput	28.89 Mpps
Average Duration	40.73 Minutes
Attack Frequency	10,261 Attacks

SUM PEAK THROUGHPUT

Date	2024-08-15
Sum Peak Throughput	50 Mpps

** peak aggregate throughput in one minute*

SUM PEAK BANDWIDTH

Date	2024-08-15
Sum Peak Bandwidth	519 Gbps

** peak aggregate bandwidth in one minute*

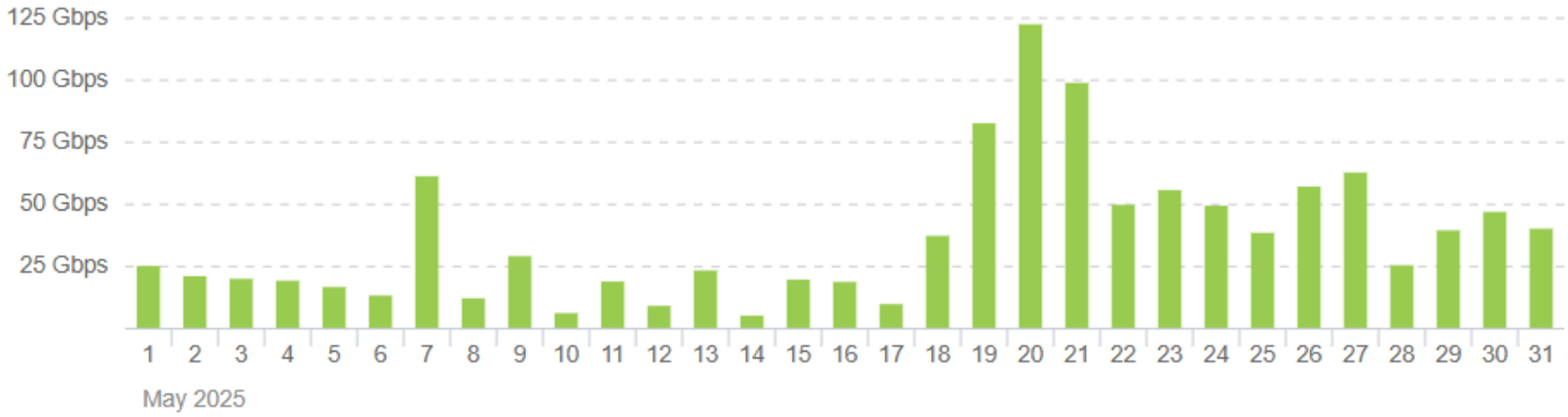
RANK	VERTICAL	FREQUENCY	MAX ATTACK	MAX IMPACT	AVERAGE DURATION
1	**Wired Telecommunications Carriers**	5,421	301.28 Gbps	28.89 Mpps	13 Minutes
2	**Wireless Telecommunications Carriers (except Satellite)**	546	5.75 Gbps	0.6 Mpps	301 Minutes
3	**All Other Professional Scientific and Technical Services**	531	37.69 Gbps	3.8 Mpps	6 Minutes

The Worldwide DDoS Landscape: Implications for Greek Digital Resilience

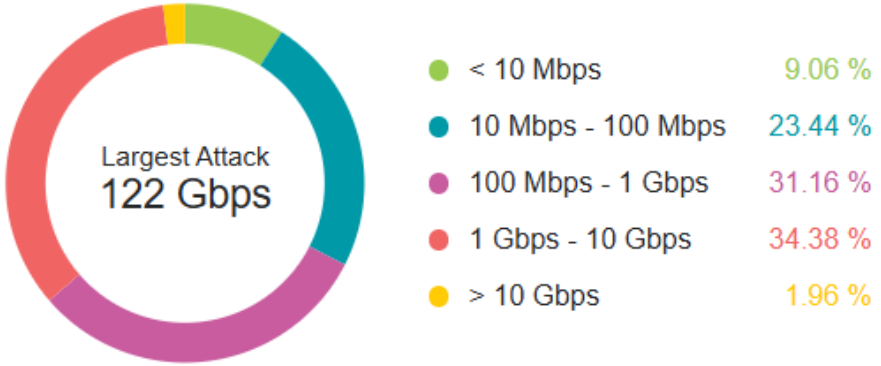
Global and local findings : Greece May

MAY 2025

Peak Attack **Volume:**



Breakout by **Volume:**

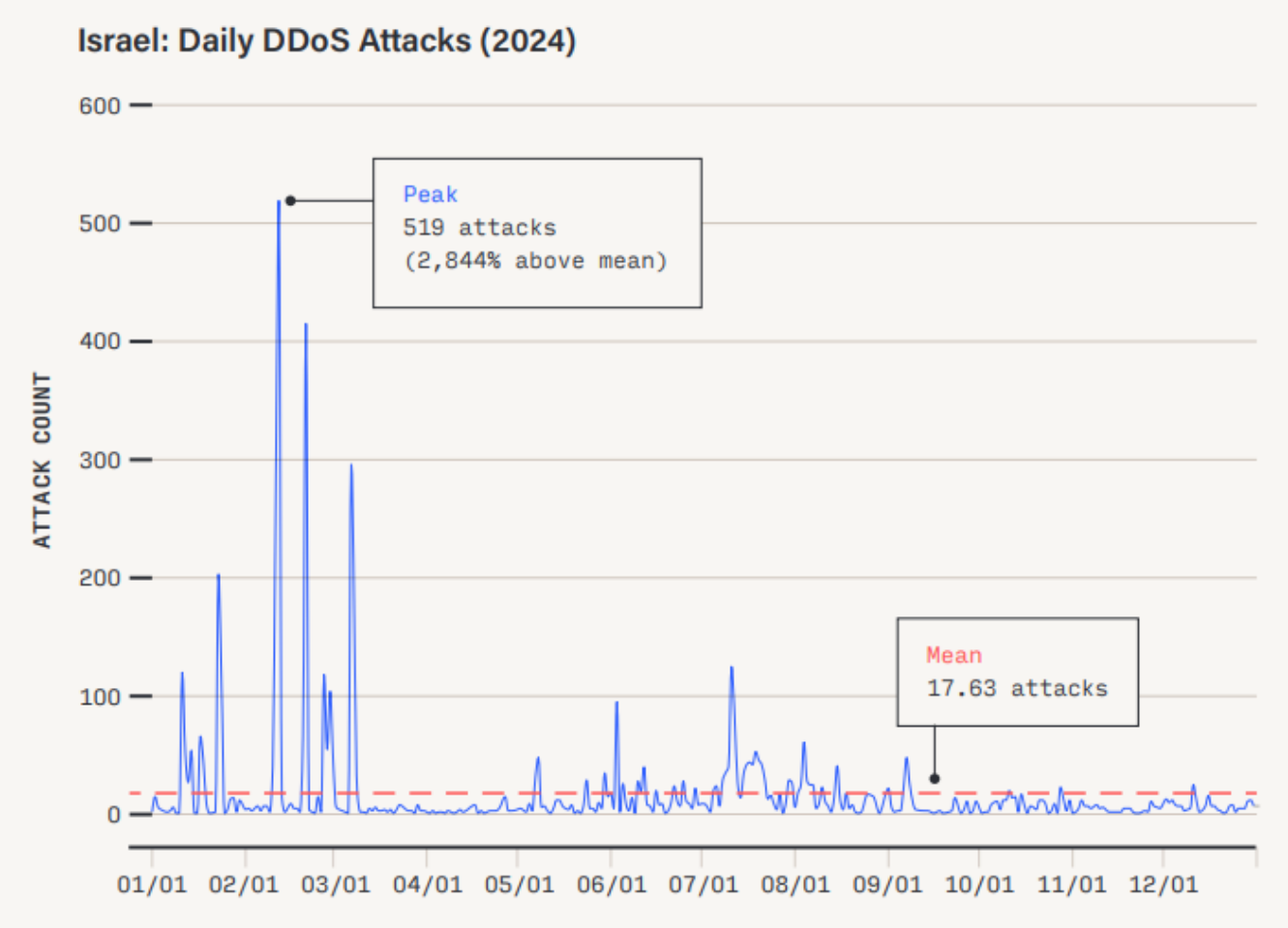


Highlights:

Attacks:4.19 k
Peak Volume:122 Gbps
Peak Speed:81 Mpps
Peak Duration:18 days
Top Attack Types:
Total Traffic
UDP
IP Fragmentation

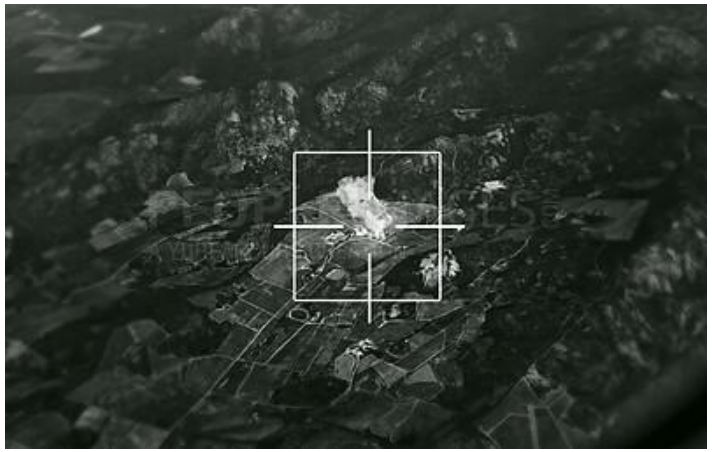
Global and local findings : Current Trend

Global DDoS Trends reflects Geopolitical stress



Iranian-aligned group Dark Storm Team seem behind the majority of these attacks

Global and local findings : A major geopolitical weapon

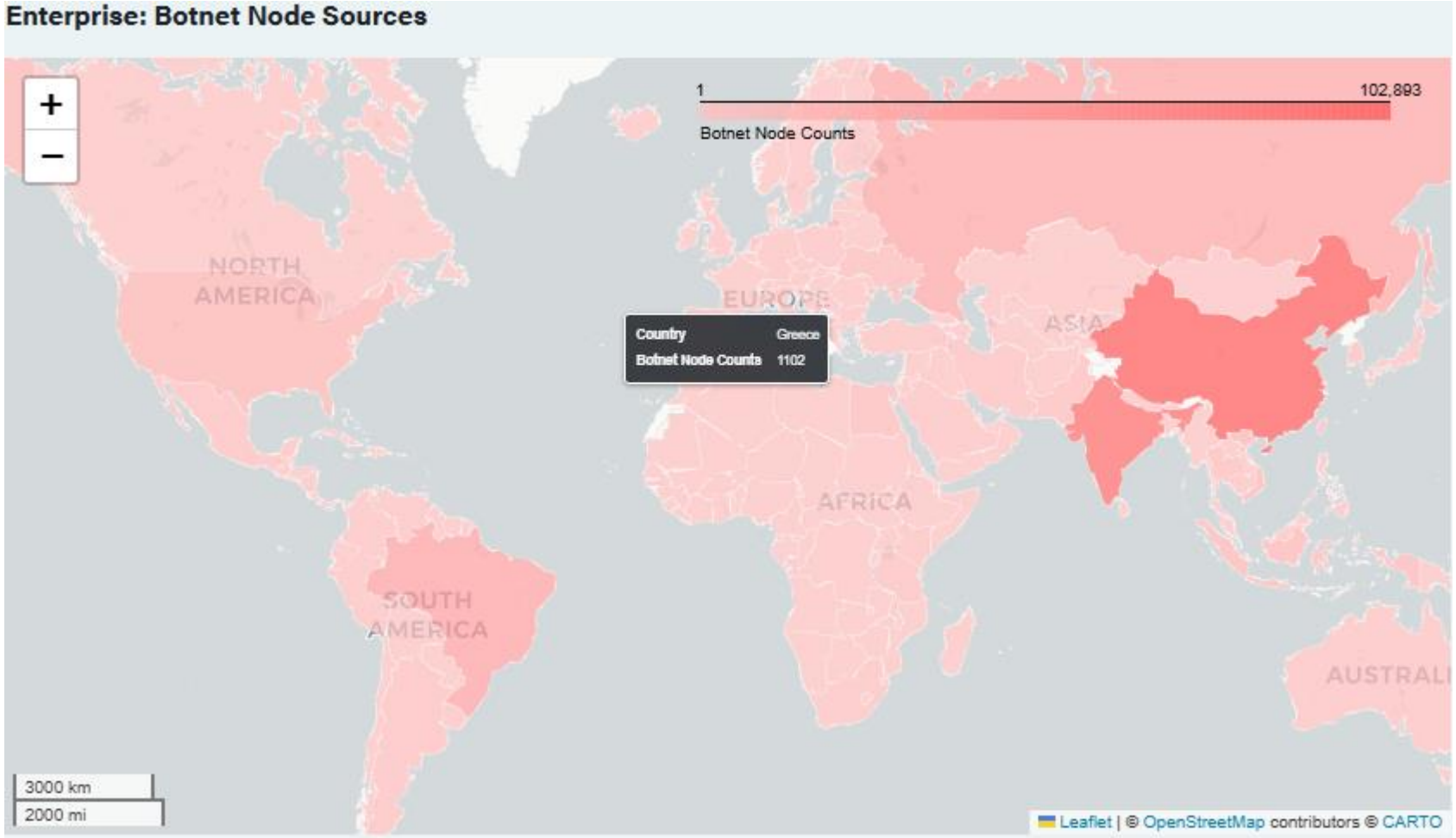


DDoS attacks are now sophisticated digital weapons, precisely aimed to disrupt vital infrastructure when it matters most.

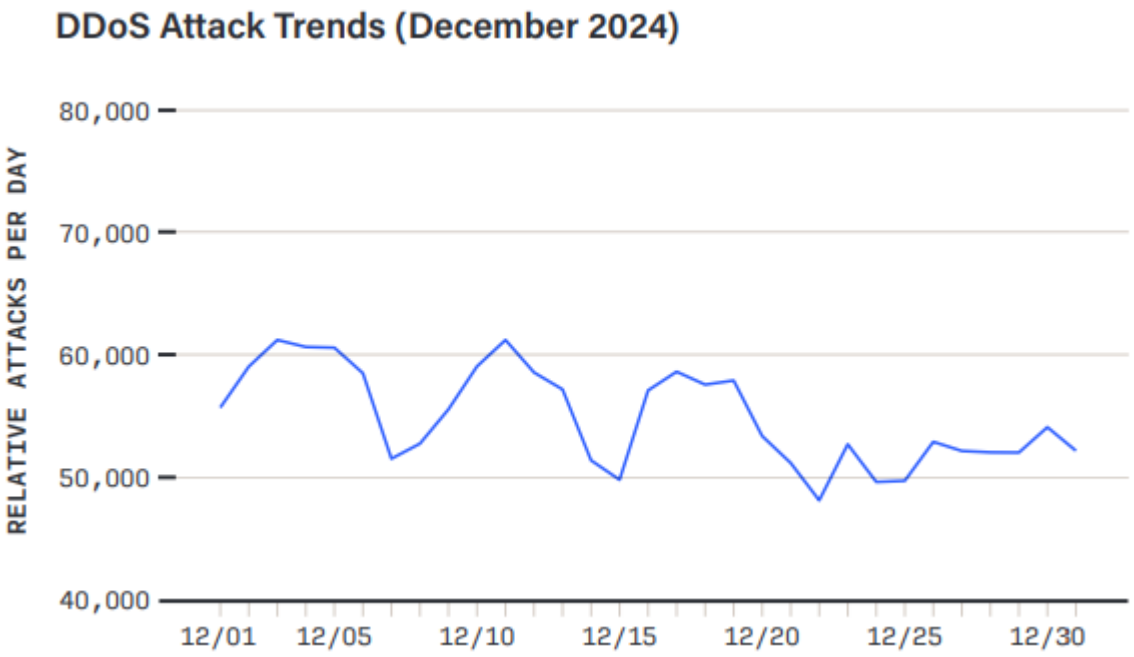
- The dramatic escalation of Mirai-driven attacks against service providers (up 360%) and the impressive rise in politically motivated attacks in countries like Israel (over 2,844% spike) and Georgia (1,478% increase) serve as compelling proof.
- This trend signifies that DDoS has transcended its origins as a cybercriminal's method to become a major geopolitical weapon.
- Greece has seen similar developments.

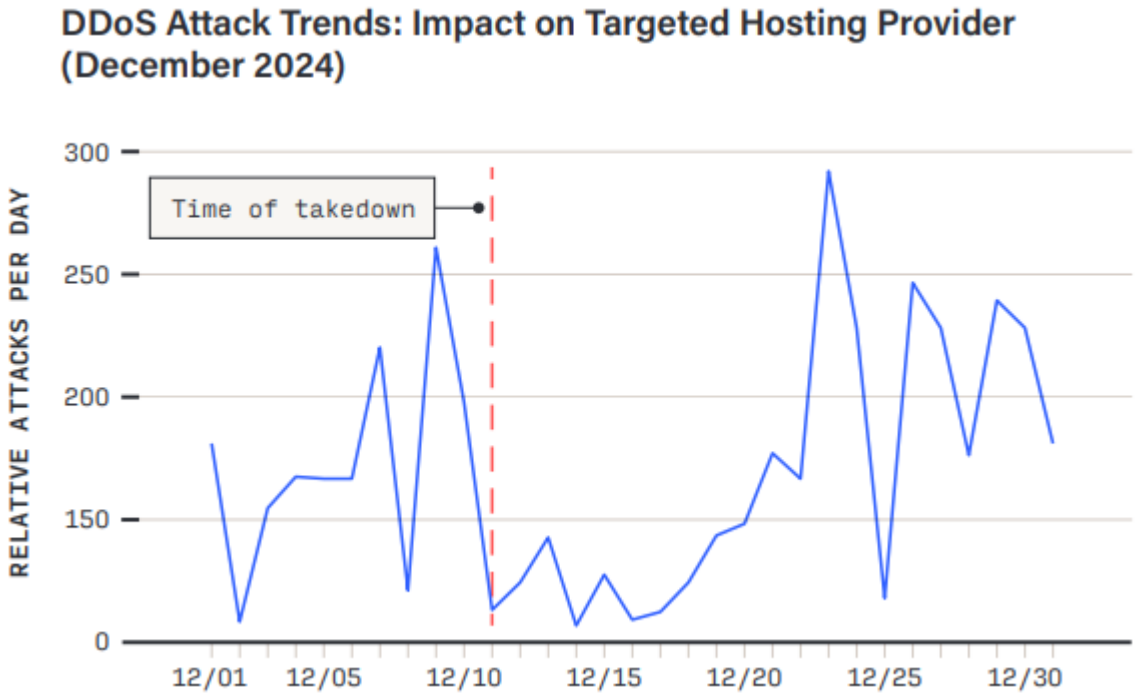
Global and local findings : Current Trend

- Usage of IoT, Bots (The Backbone of DDoS-for-Hire Services), Artificial intelligence (AI)-driven automation, proxy-based application-layer floods, and evolving DDoS-for-hire services.
  Law enforcement takedowns on DDoS-for-hire services, such as Operation PowerOFF was just a few days relief



DDoS-for-Hire Platform Takedowns
December 2024's Operation PowerOFF





Global and local findings : Current Trend

Targeted Political Attacks : NoName057(16) dominant actor behind geopolitical DDoS campaigns, focusing on government websites in the United Kingdom, Belgium, and Spain to name a few. Greece also

Next-Gen DDoS-for-Hire : AI-Driven Precision Attack , AI-powered bypassing CAPTCHA , and real-time attack adaptation. Scalability Through Automation APIs. Advanced techniques such as carpet-bombing, ISP masking, and geo-spoofing expand attack reach and bypass defenses.

Enterprise-Grade Botnets : Attackers now exploit high-power enterprise servers and routers, hiding their self

Carpet-Bombing : Attackers focused on smaller CIDR blocks, primarily targeting /24 CIDR blocks. Massive Network Disruption Despite low per-host impact, these attacks generate up to 500Gbps of traffic. While individual IPs see minimal impact, the combined traffic can cripple entire networks

Hiding Behind the Proxy (and DNS): HTTPS high-volume application-layer floods

DDoS-for-Hire : Tools

Hacking Tools

Use our tools to extract information and attack your target more efficiently.

18 Tools | +2000 Researches

Subdomain Finder
Browse all registered subdomains of your target

WAF Detector
Detect the type of Firewall used by the website

Port Checker
Do a port check on your target, make sure it's active

Port Scanner
Do an advanced port scan on your target

Ping
Do an ICMP traffic test, showing UP/DOWN results

AnyCast DNS Scanner
Do an advanced scan for your DNS target

WHOIS
Check domain/ip owner and complete information

WEBSITE CHECK
Check if your target is online accurately

GEO IP
Locate an IP address and extract all information

TOR Checker
Checks whether an IP is from a TOR network or not.

Proxy Checker
Check if your target is a Proxy or VPN

URL Reputation
Check a URL for malware/phishing

Minecraft Resolver
Resolve Minecraft servers IP address

CFX Resolver
Solve FiveM servers, getting the IP address

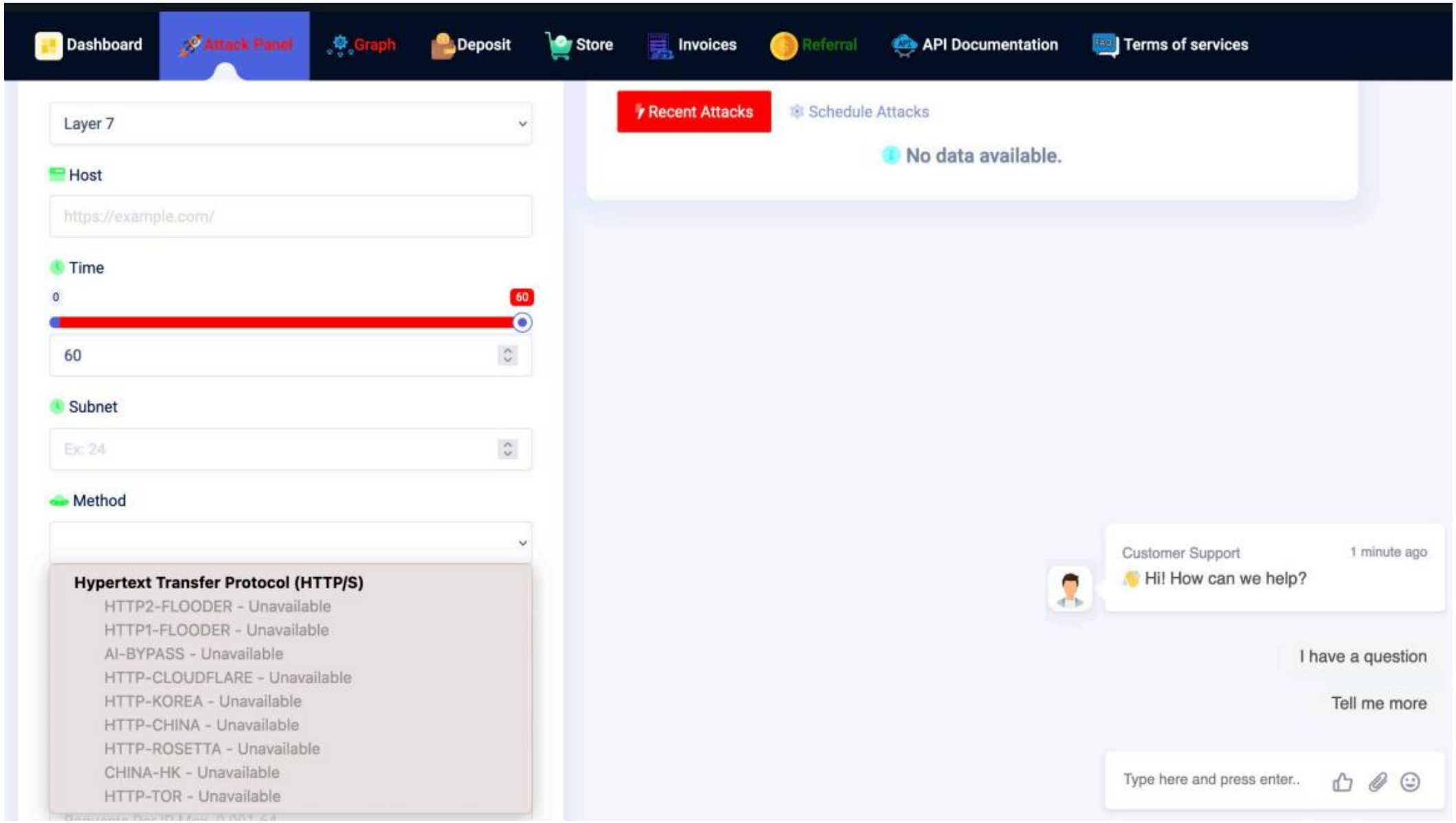
Website Header
Get the desired website header accurately

GEO PHONE
Receive information from a mobile number.

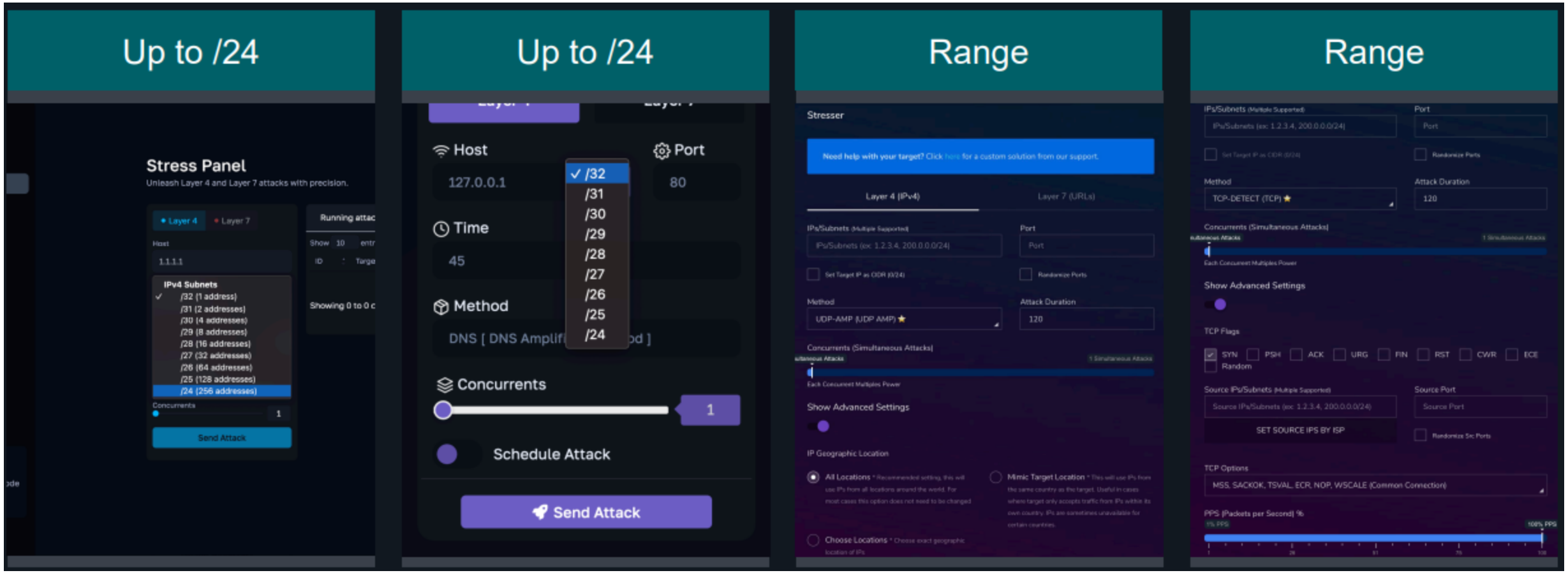
DISPOSABLE MAIL
Check if the email you received is a temporary email.

MAIL Check
Do a full check if the sent email is an existing email

DDoS-for-Hire : App + API



DDoS fof Hire : Carpet-Bombing



DDoS fof Hire : Carpet-Bombing

Schedule Layer 4 Attack

Enter your attack settings in the attack hub, and then come back to this window by clicking on the Attack Schedule button.
Once scheduled, attacks will immediately start executing using the settings below.
If auto-renew is enabled then it will not stop until you **delete** the scheduled attack completely.

Attack Settings Review

Attack Type: Layer 4
Destination IPs/Subnets: None : 0
Method: TCP-REFLECT (TCP AMP)
Attack Duration: 120 Seconds
PPS (Packets per Second): 100%
Simultaneous Attacks: 1
Source IPs/Subnets: Default : Default
Origin Country Codes (AMP Only): ALL
TCP Flags: syn
TCP Options: None
Payload: Default

Schedule Settings

Initial Execution Delay (Seconds)

0

The initial attack will not be executed until the amount of seconds entered here are reached (use 0 for no delay).

☑ Re-Execute Attack

Re-Execution Delay (Seconds)

3600

If enabled the attack will be Re-Executed every amount of seconds you enter here.

Schedule Attack | Dismiss

The Greek DDoS fortress : RUReady?

The Worldwide DDoS Landscape: Implications for G Digital Resilience

The Greek DDoS fortress : RUReady for Europ
DORA Regulation ?

Επίσημη Εφημερίδα
της Ευρωπαϊκής Ένωσης

Συμπεράσματα Η απάντηση

Υπηρεσίες του Gov.gr και του TAXISnet της Ελλάδας – Μία από τις

συνέβη τον Νοέμβριο του 2022, όταν οι

• Κυβερνοε

Το Συ μεγαλύτερ

κυβε εγκληματί

εγκριθ υπηρεσιώ

κατάλλ συνταγον

αποφεί και να ε

συντον

από την

ΤΕΧΝΟΛΟΓΙΑ 17 Φεβρουαρίου 2025 | 14:54

Η Ιταλία καταγγέλ
κυβερνοεπίθ
αερο

ιλώσεις του ιταλού προέδρου

Πρόστιμα έως 10 εκατ. για «τρύπες» στην κυβερνοασφάλεια

ομό όσο και σε πολυπλοκότητα. Η τάση αυτή αναμένεται να

ερεαιτέρω στο μέλλον, καθώς ο αριθμός των συνδεδεμένων συσκευών

παγκοσμίως αναμένεται να διπλασιαστεί σχεδόν, από 15,9 δισεκατομμύρια το 2023

σε πάνω από 32,1 δισεκατομμύρια το 2030, σύμφωνα με τη Statista.

ο υργοί επ

πολιτική προκειμένου να

στον κατάλογο φυσικών και νομικών προσώπων,
ατίθεται στο παράρτημα της απόφασης (ΚΕΠΠΑ)
κές επιπτώσεις ή εμπλέκονται σε κυβερνοεπιθέσεις
ρική απειλή για την Ένωση ή τα κράτη μέλη της.

The Greek DDoS fortress : RUReady for European NIS2 directive and DORA Regulation ?

NIS2 (Directive (EU) 2022/2555) is the EU's overarching cybersecurity framework. Its primary goal is to achieve a high common level of cybersecurity across the Union by enhancing the resilience and incident response capabilities of both public and private sectors.

- **Essential entities**
- **Important entities**
- **Key Requirements:** Entities covered by NIS2 must implement comprehensive cybersecurity risk management measures (e.g., risk analysis, incident handling, supply chain security, multi-factor authentication, cybersecurity training for management). They also have strict incident reporting obligations, with specific timelines for notifying authorities of significant incidents.
- **Enforcement:** National authorities in each EU Member State are responsible for supervising compliance and enforcing the directive, with significant fines possible for non-compliance (up to €10 million or 2% of annual global turnover, whichever is higher).

The Greek DDoS fortress : RUReady for European NIS2 directive and DORA Regulation ?

DORA Regulation (Digital Operational Resilience Act)

- **Objective:** DORA (Regulation (EU) 2022/2554) is specifically designed to strengthen the digital operational resilience of the **financial sector** within the EU. It aims to ensure that financial entities can withstand, respond to, and recover from all types of ICT-related disruptions and threats, including cyberattacks and system failures.
  Scope: DORA applies exclusively to a wide range of financial entities and their critical ICT third-party service providers.
  Key Requirements: DORA establishes a comprehensive framework built around five key pillars:
  - **ICT Risk Management:** Financial entities must have a robust framework to identify, protect, detect, respond to, and recover from ICT-related risks.
  - **ICT-related Incident Management, Classification, and Reporting:** to relevant authorities.
  - **Digital Operational Resilience Testing:**
  - **Managing ICT Third-Party Risks:**
  - **Information and Intelligence Sharing:**
  - **Enforcement:** DORA is supervised by national financial authorities and European Supervisory Authorities (ESAs), with potential fines for non-compliance.

Solution : There is no one solution

If you fail to plan, you plan to fail

Before:

Preparation: The most important step. Tools, people, processes, best practices. Not only in the client's infrastructure, but also in the direct and critical partners. Communication must be ensured at all costs.

During :

Detection: What tools does the organization have? How will they know what is happening? How does the incident communicate?
Categorization: What type of attack, what is it targeting and what size is it in order to take targeted actions and analysis.
Monitoring: Utilizing all the elements of the categorization to plan response actions.
Response: Implementing all the measures that have been designed for the specific attack.

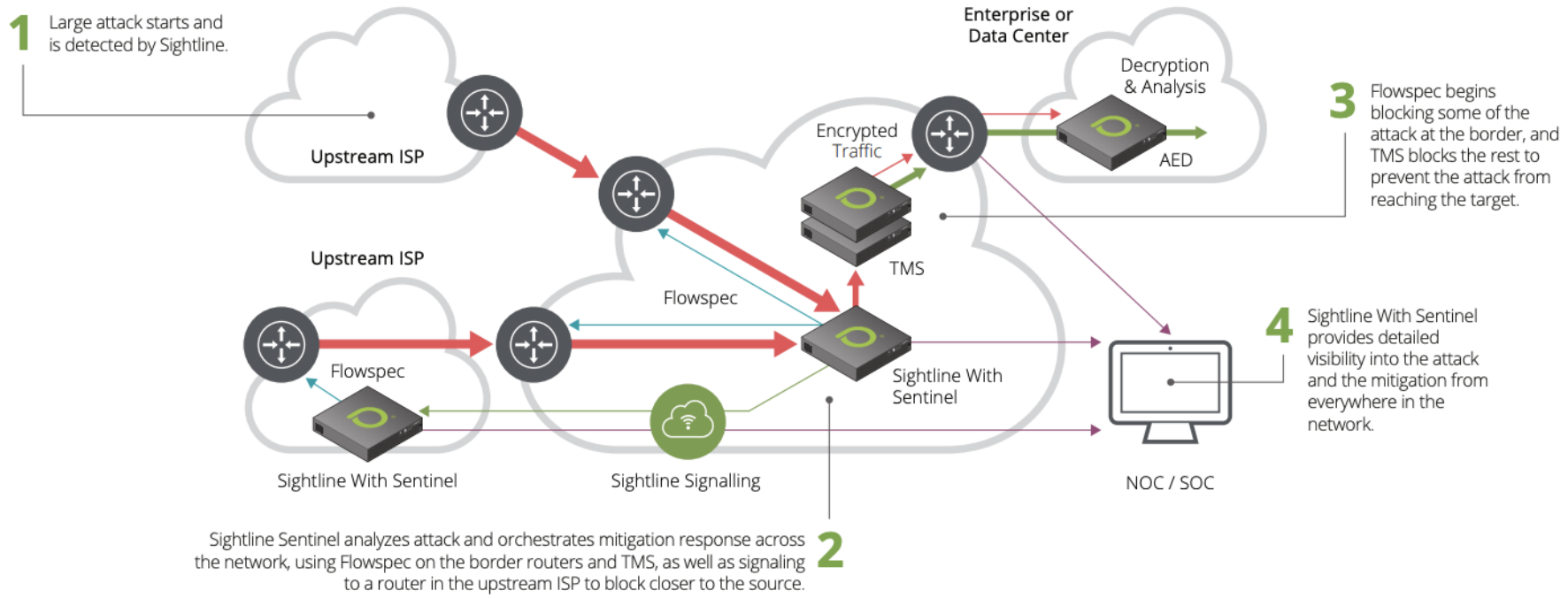
Mitigation, rules, filters are all means of response.

After:

Analysis (meta): Did the steps run correctly, did we have the right reaction?
Impact analysis: What can we improve?

Solution : There is no one solution – keyboard action

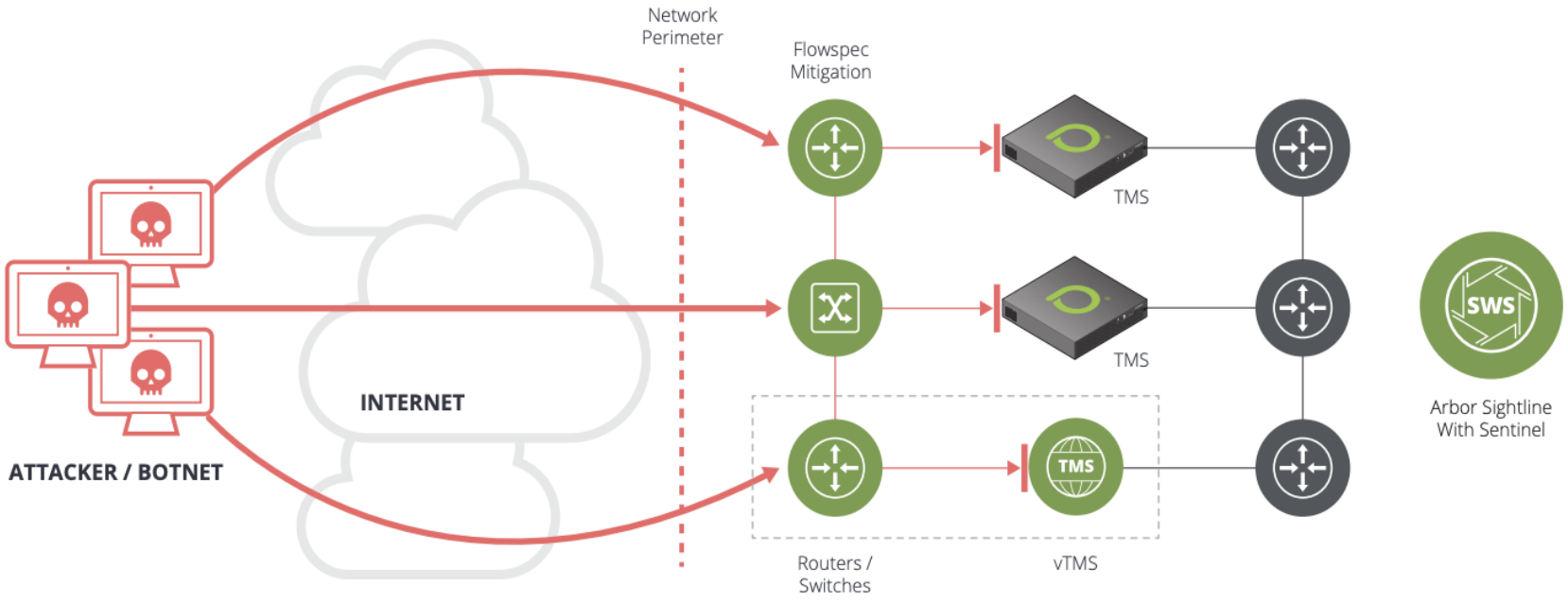
Strategic scrubbing centrally located



Netscout's Arbor Solution

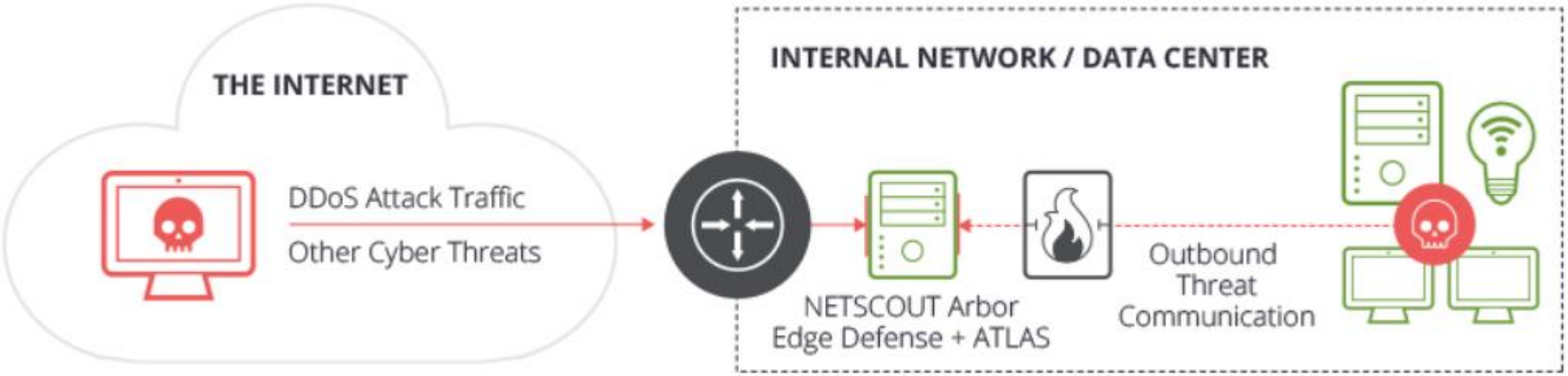
Solution : There is no one solution – keyboard action

Flowspec enabled network



Solution : There is no one solution – keyboard action

Strategic scrubbing at the edge



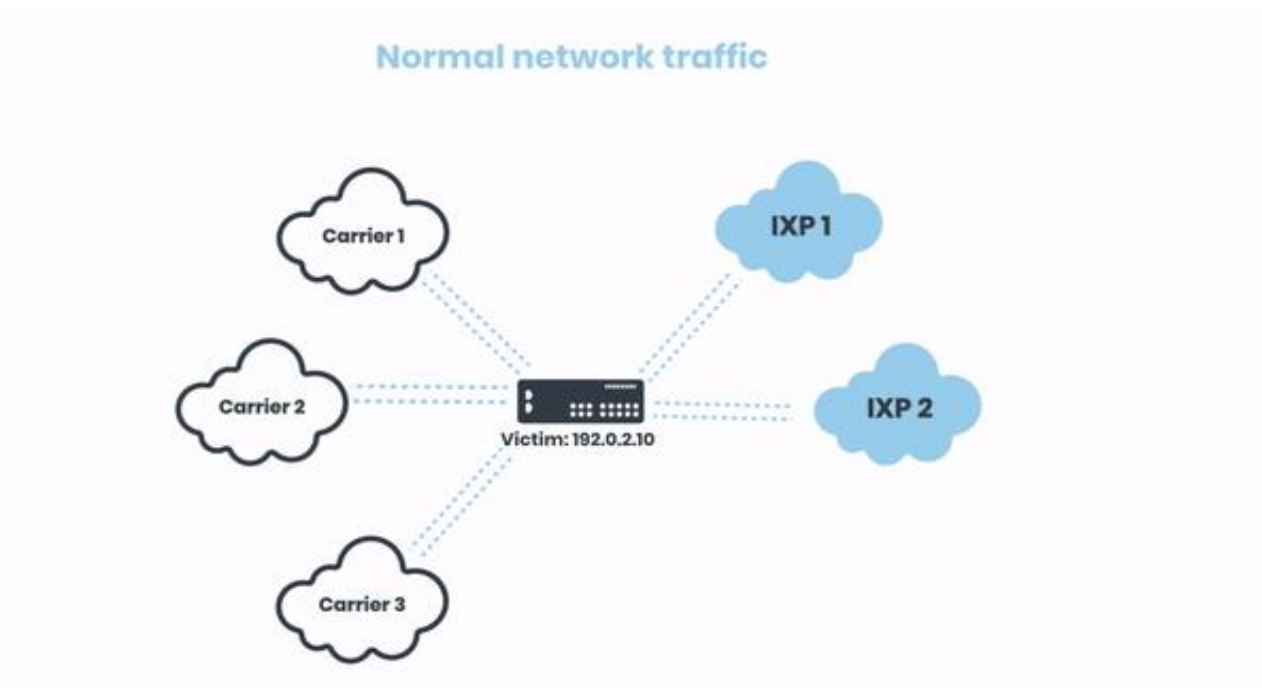
Netscout's Arbor Solution

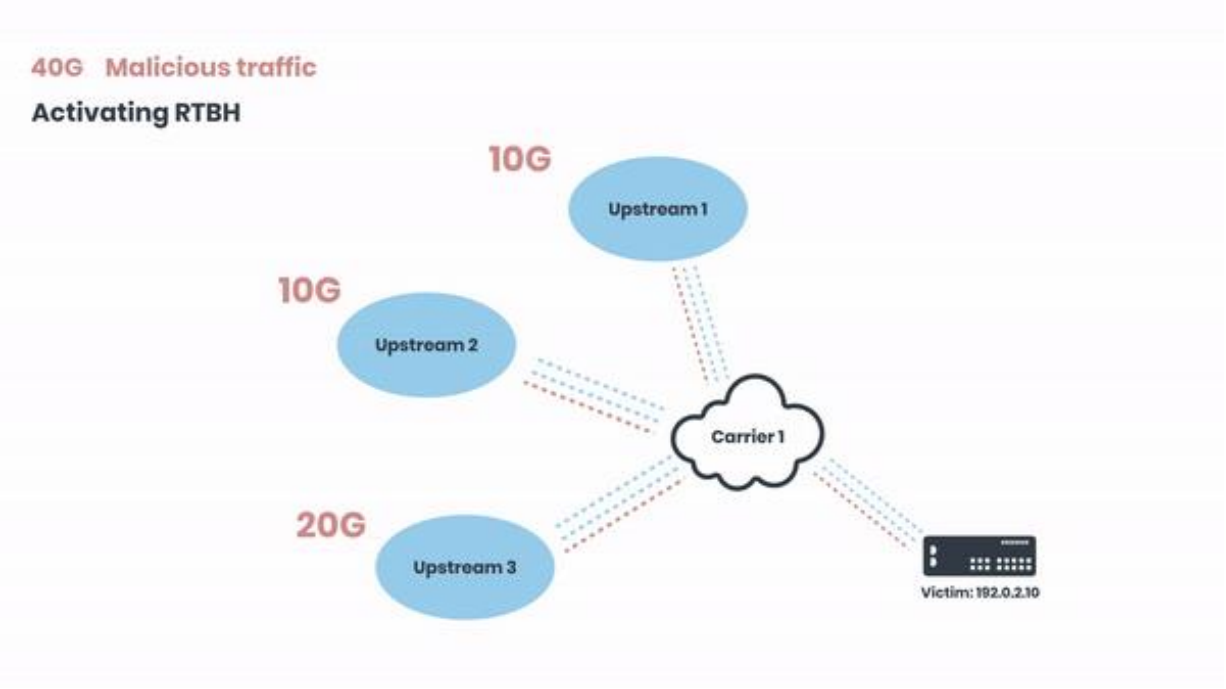
Solution : There is no one solution – keyboard action

Class of Service when needed

&

The old school – RTBH





The Worldwide DDoS Landscape: Implications for Greek Digital Resilience

What's next : The war is AI driven

AI Applications in DDoS Mitigation

- **Anomaly Detection:**
  - AI analyzes real-time network traffic to detect deviations from normal patterns.
  - Uses machine learning (e.g., supervised learning) trained on historical data to identify attack signs.
  - Triggers countermeasures upon detecting unusual traffic spikes.
- **Behavioral Analysis:**
  - Profiles normal user behavior to distinguish malicious activities.
  - Establishes a baseline of regular traffic and flags anomalies.
- **Automated Response:**
  - AI systems automatically mitigate attacks by adjusting firewall rules, redistributing traffic, or activating security protocols.
- **Predictive Analysis:**
  - Uses trends and predictive modeling to anticipate potential DDoS attacks before they occur.
- **Traffic Filtering:**
  - Enhances traditional filtering with AI-driven algorithms to better separate legitimate from malicious traffic.

Challenges & Considerations

- **Data Dependency:** Effectiveness relies on high-quality, large-volume training data.
- **False Positives:** Risk of blocking legitimate traffic, necessitating a balance between sensitivity and specificity.
- **Evolving Threats:** Attackers constantly adapt, requiring continuous AI model updates.

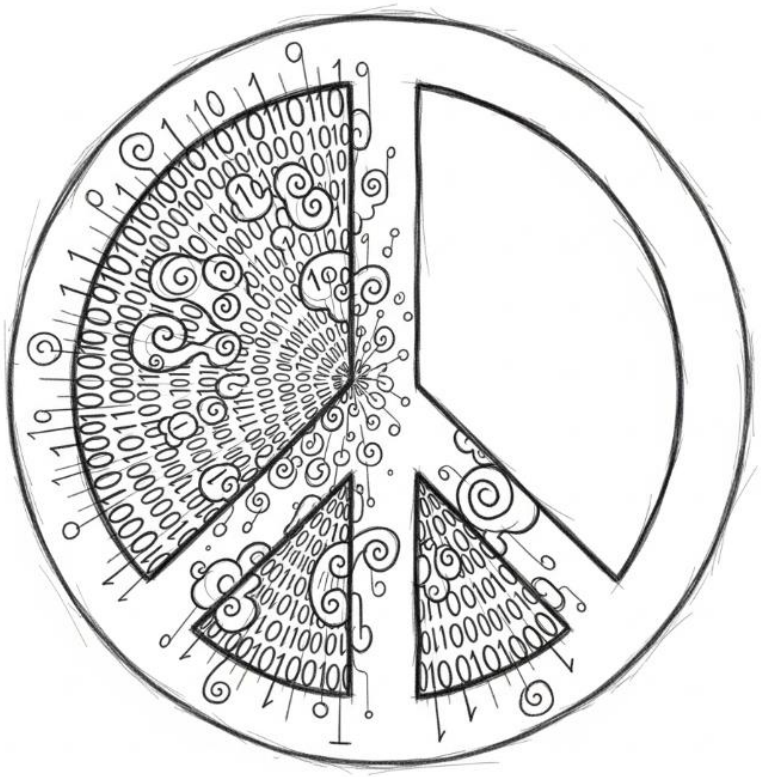
AI significantly improves DDoS defense but requires ongoing refinement to stay ahead of threats.

What's next : The war is AI driven

Guess what...Attackers use AI too.

The Worldwide DDoS Landscape: Implications for Greek Digital Resilience

Konstantinos Chatzithomaoglou
Nova S.A



Thank you