# radware

# 2024 Global Threat Analysis Report

Analysis of the most significant
cybersecurity events and trends of 2023
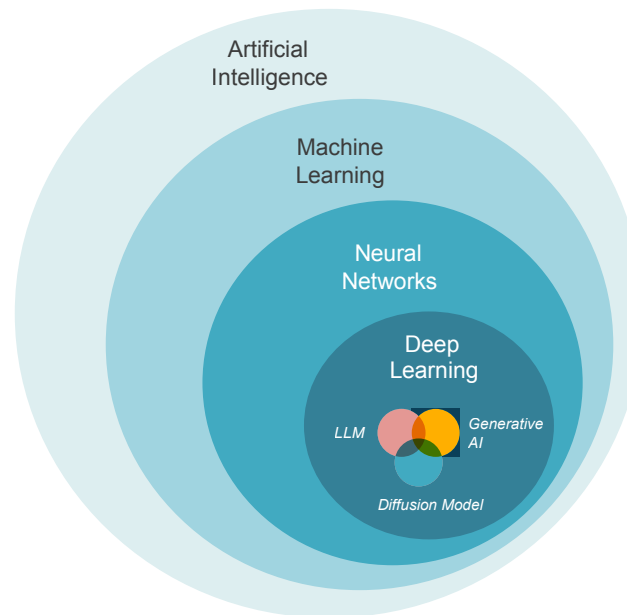
# Contents

# Major Trends in the Threat Landscape

## The Impact of AI (GPT)

In 2023, something remarkable happened in the world of technology: artificial intelligence (AI) became mainstream. Actually, it is large language models (LLMs) and, more specifically, generative pre-trained transformers (GPT) that took center stage in 2023.

LLM is a broader term that encompasses various language models, including but not limited to transformer-based models like GPT. AI is an even broader domain of which LLMs are but a subset. Generative AI, on the other hand, is an umbrella term including a spectrum of content-creation technologies for text, images, videos and music. LLMs are a subset of generative AI focusing on text. That said, GPT has taken the world by storm and, considering the innovations presented at CES 2024, generative AI will be a part of every aspect of our lives very soon. As AI made its way into the spotlight, it did not escape the attention of malicious threat actors. Generative AI applications started gaining significant traction, but with their rise came new challenges in safeguarding against misuse.

Providers of generative AI services recognized the importance of putting guardrails in place



**Figure 1:** AI and ML vs generative AI

to prevent their models from being abused for nefarious purposes. As AI prompt hacking emerged as a new threat, it forced providers to continuously improve their guardrails. AI prompt hacking allows both well-intentioned users and malicious actors to manipulate AI models into performing tasks they were never meant to do.

On another front, open source private GPTs started to emerge on GitHub, leveraging pre-trained LLMs for the creation of applications tailored for specific purposes. These private models often lack the guardrails implemented by commercial providers, which led to paid-for underground AI services that started offering GPT-like capabilities—without guardrails and optimized for more nefarious use-cases—to threat actors engaged in various malicious activities.

At the heart of this AI revolution lies a crucial understanding: LLMs are not truly intelligent. They are massive statistical language processors, trained on vast amounts of internet data. They excel at providing information based on their training, but they lack the ability to think critically or generate entirely new ideas. Instead, they interpolate and seek the closest match based on their enormous dataset.

Nevertheless, LLMs offer a powerful tool for education and productivity. When used judiciously, LLMs can help individuals achieve their objectives more efficiently. They also open the door for malicious threat actors looking to cast a wider net and scale their attack campaigns.

Generative adversarial networks (GANs) and diffusion models are a class of machine learning frameworks for approaching content other than text. While LLMs are like parrots, faithfully echoing what they've learned, GANs and diffusion models are akin to artists. They have the capability to generate images, videos, audio or other content. GANs employ a generator and discriminator network to create and assess outputs, allowing them to "invent" new content, albeit through a process of trial and error.

While LLMs can enhance productivity and sophistication to some extent, they are ultimately bound by their training data. LLMs are not limited to natural languages, but also excel at reproducing and generating programming languages. Lower-skilled threat actors may leverage LLMs to create more complex attack scripts or malware, but these attacks and malware pieces are still limited by the knowledge embedded in the LLM model. Thus, the increase in sophistication lies more in the quantity of attacks with a higher average sophistication rather than their inherent complexity and sophistication.

Threat actors, like everyone in the industry, learn and adapt. The acceleration in learning and research facilitated by current generative AI systems allows them to become more proficient and create sophisticated attacks much faster compared to the years of learning and experience it took current sophisticated threat actors. Even for advanced threat actors, the current generative AI tools provide ample opportunity to increase their productivity and could, for instance, be employed to discover vulnerabilities in open-source software, potentially resulting in a rapid increase of zero-day exploits appearing in the wild.

The landscape is evolving, and generative AI is evolving at head-spinning speeds. Recently, Google introduced Gemini, their most capable AI model to

**Figure 2:** Impact of GPT on attacker sophistication



Impact of AI (GPT) on attack sophistication

*(More sophisticated attacks, but no increase in the sophistication of attacks)*
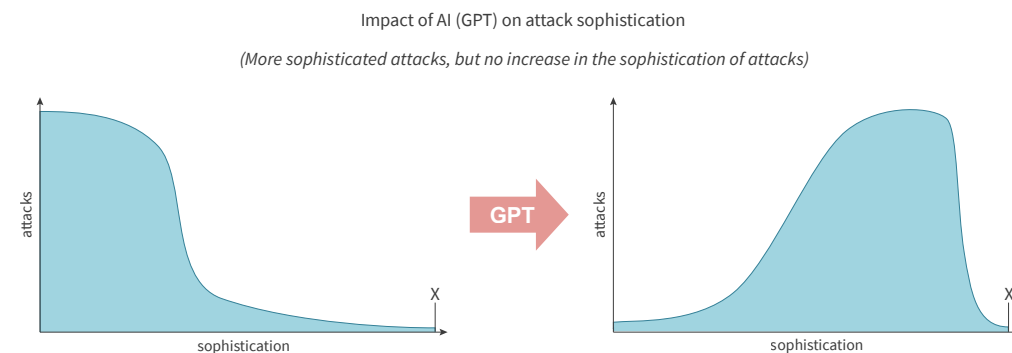
date. Gemini is a multi-modal generative AI system capable of interpreting and generating text, audio/voice, images, video and code through a single prompt. These tools will enable highly credible scams and deepfakes to be generated with just a few keystrokes. Ethical providers will ensure guardrails are put in place to limit abuse, but it is only a matter of time before similar systems make their way into the public domain and malicious actors transform them into real productivity engines. This will allow criminals to run fully automated large-scale spear-phishing and misinformation campaigns.

LLMs and GANs are transforming the technological landscape. LLMs boost productivity and automate tasks at an unprecedented scale, both for legitimate users and malicious actors. GANs, on the other hand, possess the potential to create novel content, including new attack payloads.

While the AI journey has seen its share of winters and springs, one thing remains certain: the AI landscape continues to evolve, offering both promise and challenge. Much like the security scene has been for many years, it's a technological race between the good and bad actors. AI might force us to adapt and change the way we approach threats and threat actors, but it will not be fundamentally different in the future than it was in past.

# The Shift to Application-level Attacks

The cybersecurity landscape evolved rapidly in 2023. In the first half, we observed a significant shift in denial-of-service (DoS) attack patterns. Increasingly, DoS attacks were progressing to L7, targeting not just the online applications and their APIs but also essential infrastructure such as the Domain Name System (DNS). We noted a considerable surge in DNS query floods during the first half and this trend only worsened in the second half of 2023.

Web distributed denial-of-service (Web DDoS) attacks have become more sophisticated, and a previously unknown HTTP/2 Rapid Reset attack technique was disclosed by Google in October of 2023. Leveraging a vulnerability in the HTTP/2 specification allowed attackers to significantly increase the rate of their application-layer Web DDoS attacks without having to invest more resources. Google observed a series of DDoS attacks leveraging this new HTTP/2 Rapid Reset technique reaching peaks of up to 398 million requests per second (RPS), a 7.5x increase in attack rates compared to the previous record recorded by Google last year.

Hacktivists continued to constitute a major part of the L7 DDoS problem. The effectiveness of their attacks has been significantly amplified by using patriotic volunteers in crowdsourced botnets or by providing custom attack tools and detailed tutorials on how to execute attacks.

Network-layer attacks are better understood, and arguably easier to detect and mitigate compared to the new generation of HTTPS floods organizations are facing in 2023. Since HTTPS floods have been around for a few years, they are sometimes considered old news. However, the volume and intensity of the new generation of HTTPS floods has increased dramatically while the sophistication and viciousness of attackers continued to grow.

# Attackers Migrating to the Cloud

There's a discernible trend among malicious actors transitioning to cloud-based operations. By switching from compromised IoT devices to much more scalable and cost-effective cloud services providing high-speed internet connectivity, they can now orchestrate a limited number of very powerful nodes within their control. The advantages are considerable: they maintain control over their servers, suffer no loss from device reboots and run a lower risk of detection by security researchers. Utilizing bulletproof hosting and proxy services that provide frequently rotating residential IP addresses creates the perfect platform to launch high-frequency, sophisticated attacks, including and not limited to Web DDoS attacks.

# Hitting Where it Hurts the Most

DNS query floods continued their growth through 2023, reaching new heights in the last months of the year. DNS query floods are application-level attacks, aiming at impacting the resources of the DNS server. Attackers benefit from an aging IoT installed base and persistent default and weak passwords of publicly exposed devices and servers. Consumer IoT devices provide the ideal basis for performing devastating pseudo random subdomain (PRSD) attacks, aka DNS Water Torture attacks. Through consumer devices, PRSD attacks leverage local provider's forwarding DNS resolvers as allies to create a distributed random query flood that will be directed at the authoritative DNS server. The authoritative server can challenge the forwarders, but since they are legitimate servers, they will not be flagged as malicious devices.

Voice-over-IP infrastructures continue to be an important target for denial-of-service attacks. Since the global pandemic, SIP services have become the more common target of DDoS attacks. Typically performed against branches and headquarters of businesses, attackers try to cripple the communications of their victims.

# The New Hacktivists

2023 was a year where we saw a lot of new hacktivists appearing on the threat scene. After a year of patriotic pro-Russian and pro-Ukrainian hacktivist activity, more hacktivists appeared following religious incidents while new conflicts resulted in increasingly more hacktivity.

Hacktivists became more visible through Telegram, the new favorite social media platform for many modern threat actors. Towards the end of 2023, hacktivists started gathering in temporary, campaign-based alliances. Some of these alliances later reconvened to gather in new campaigns and resulted in a more concentrated circle of activity that hit harder on targets of the campaign.

Hacktivism has reached new heights in 2023, following a trend set by the IT Army of Ukraine and pro-Russian hacktivists such as Killnet and NoName057(16) in 2022. We expect 2024 to confirm this new hacktivity level, if not to see it increase. Activists are movements of every era and in the era of digitalization it had to be expected that hacktivism would reach new heights. We have yet to see model citizens reaching for DDoS attacks to express their unsettlement or make their message heard, but plenty of groundwork has been done by proficient hacktivists in the last two years. It is only a matter of time before we see grandma and grandpa gathering around the tablet that shows a booter control center and bringing down the website of the tax authorities that increased taxes on pensions.

**Figure 3:** Grandma and grandpa performing DDoS attacks against the government[1]



1.  Image generated by Bing Microsoft Image Creator. Prompt: "Create a cyberpunk picture with grandma and grandpa disguised as Anonymous performing hacking attacks on the government."

# Network-level Attacks in 2023

## Denial-of-Service Attack Activity

As seen in Figure 4, the average number of DDoS attacks[2] blocked by a customer in 2023 grew by 94% compared to 2022, adding to the 99% growth observed in 2022.

The average number of DDoS attacks each customer had to mitigate per quarter reached a new record of 4,392 attacks in Q1 of 2023. This represents an average of 49[3] attacks per day per organization in the first quarter of 2023. The average number of DDoS attacks per customer has been growing at a rate of 106[4] attacks per month or 3.48[5] attacks per day since Q1 2021.

The average attack volume per customer increased by 48% in 2023 compared to 2022.

Compared to 2022, there were 63% more small attacks with traffic peaks below 1Gbps in 2023. Attacks peaking between 100Gbps and 250Gbps increased with 177% while large attacks peaking above 500Gbps increased with 150%.

**Figure 4:**

DDoS attacks per customer, per year


Attacks per Year (normalized per customer)

**Figure 5:**

Evolution of time of average number of DDoS attacks mitigated per customer


DDoS Attack Evolution (normalized per customer)
slope = +317.97
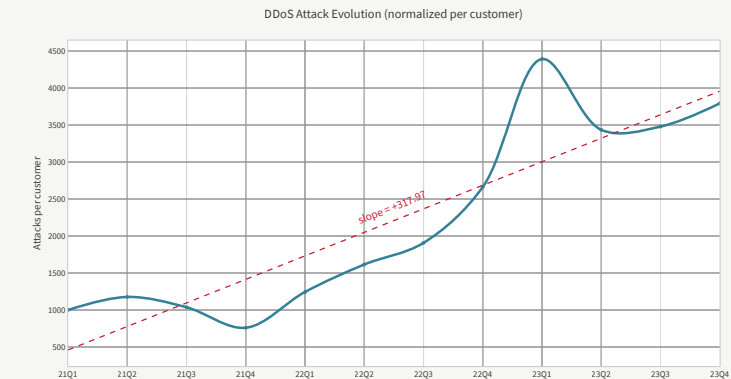
**Figure 6:** Attack volume per customer by year


Attack Volume per Year (normalized per Customer)
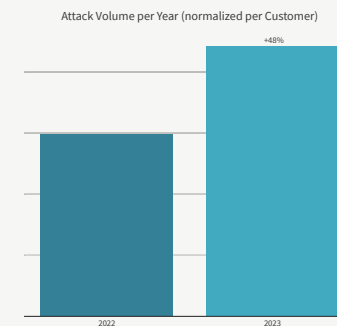
**Figure 7:** Number of attacks by attack size


Number of attacks by attack size

---

2. To eliminate bias caused by an increase in the number of customers subscribing to our services, the year-over-year comparison is normalized by taking the metrics per customer and not the total metric.

3. 4,392 / (31+28+31) = 48.8 attacks per day.

4. The slope of the trendline in Figure 5 represents the average increase in number of attacks per quarter. The slope is 317.97 attacks per quarter, corresponding to an average increase of 106 attacks per month.

5. 106 attacks per month divided by 30.436875, the mean month length in the Gregorian calendar.
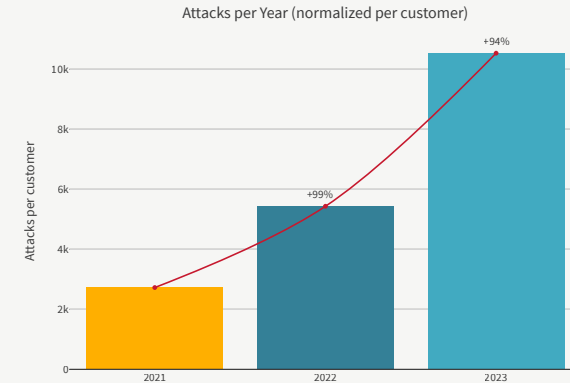
# Regions

The Americas were targeted by almost half of the global DDoS attacks and over 30% of the global volume. The EMEA region, while accounting for 39% of the DDoS attacks, had to mitigate 65% of the global DDoS attack volume. The APAC region accounted for almost 12% of global DDoS attacks and 5% of the global volume.

Addressing DDoS attacks effectively necessitates a worldwide, decentralized strategy. The best method to mitigate distributed threats is by eliminating them as close to their source as possible, significantly reducing the strain of malicious traffic on the wider internet infrastructure.

A scrubbing center is a data cleansing facility designed to help organizations protect their data and infrastructure from DDoS attacks. When incoming network traffic is directed through a scrubbing center, the role of the center is to "scrub" the data, that is to filter out malicious traffic and allow only legitimate traffic to be routed through the Cloud DDoS Protection Service backbone to its intended destination. This process involves the separation of "clean" data, which is allowed to reach the target server, from the "dirty" or harmful data, which is dropped.

Scrubbing centers should be distributed across the world to provide global DDoS protection and ensure uninterrupted service, even when an attack is underway. The quantity of attack volume intercepted by a scrubbing center offers a reliable indication of the origin of the hostile traffic.

London (United Kingdom) handled almost 27% of the total global attack volume. Ashburn (United States) handled nearly 25% of the attack volume while Frankfurt (Germany) accounted for 22.5%.

Overall, scrubbing centers located in EMEA blocked 60% of the total attack volume, scrubbing centers in the Americas blocked 34% and scrubbing centers in APAC blocked almost 6%.

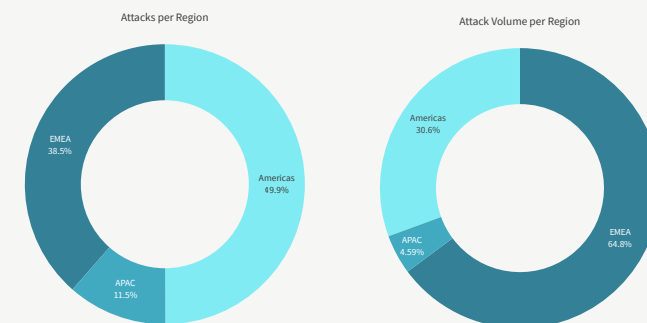**Figure 8:**

DDoS attacks and volume per region


Attacks per Region

Attack Volume per Region

**Figure 9:** Mitigated attack volume per scrubbing center location


Attack Volume per Scrubbing Center

London: 26.59%
Ashburn: 24.61%
Frankfurt: 22.47%
Amsterdam: 10.88%
Dallas: 5.71%
San Jose: 3.87%
Hong Kong: 2.13%
Chennai: 1.18%
Sydney: 1.01%
Tokyo: < 1%
Tel Aviv: < 1%
Seoul: < 1%
Auckland: < 1%
Johannesburg: < 1%
Taipei City: < 1%
Melbourne: < 1%
Sao Paulo: < 1%
Dubai: < 1%

**Figure 10:**

Scrubbing center blocked attack volume per region
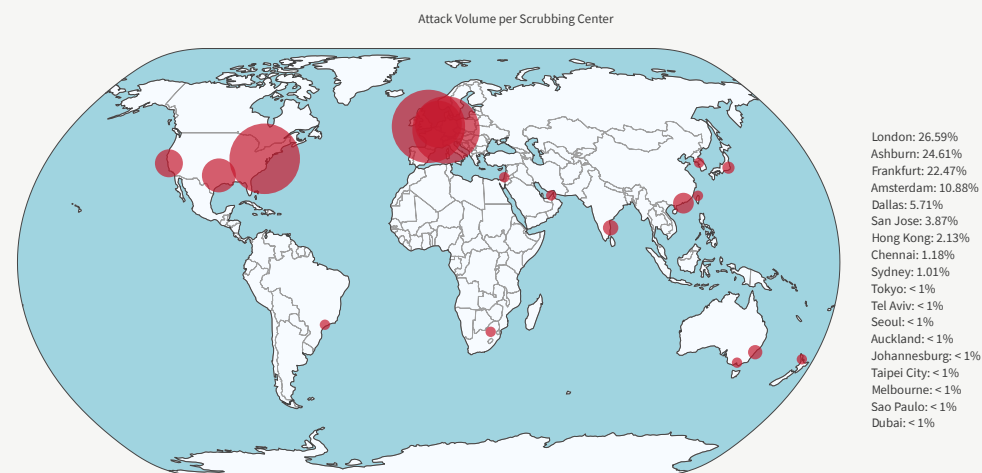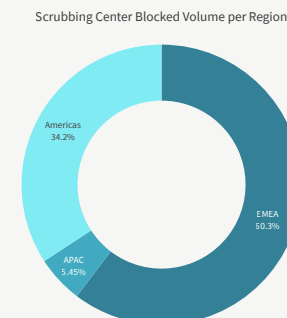

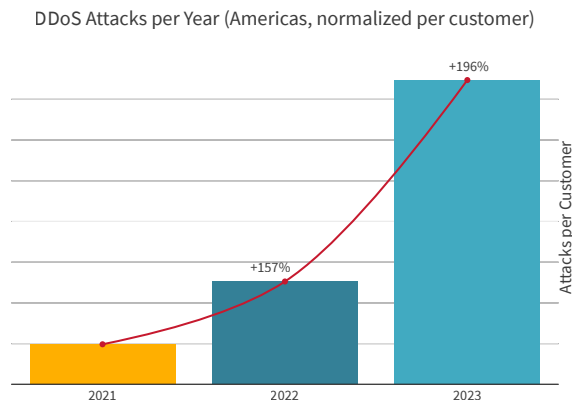Scrubbing Center Blocked Volume per Region

## North, Central and South America

As seen in Figure 11, the average number of DDoS attacks targeting customers in the Americas grew significantly by 196% in 2023 compared to 2022. In 2022, the number of attacks per customer had already grown by 157% compared to 2021.

The number of attacks per customer peaked significantly in Q1 of 2023. Attacks targeting the Americas are trending with an average increase of 522 attacks per quarter, equal to 174 attacks per month or 5.72[6] attacks per day. This is faster than the global average of 3.48 attacks per day.

**Figure 11:** DDoS attacks per year per customer targeting organizations located in the Americas

DDoS Attacks per Year (Americas, normalized per customer)



## Europe, Middle East and Africa

The number of DDoS attacks targeting customers in the EMEA region in 2023 slowed to a double-digit growth of 43% in 2023 compared to the triple-digit growth of 107% in 2022.

The number of attacks per customer in the EMEA region reached record levels in Q1 and Q2 of 2023. In the EMEA region, attacks are trending with an average increase of 314 attacks per quarter, 105 attacks per month or 3.44[7] attacks per day. This is almost on par with the global average of 3.48 attacks per day.

**Figure 13:** DDoS attacks per year targeting organizations located in the EMEA region

DDoS Attacks per Year (EMEA, normalized per customer)



---

6.  522 attacks per month divided by 3 * 30.436875, the mean month length in the Gregorian calendar.
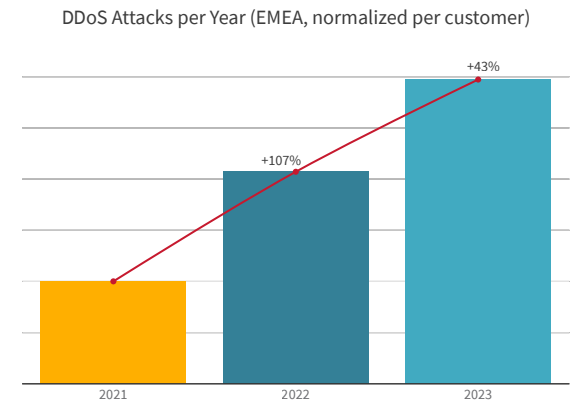
7.  314 attacks per quarter divided by 3 * 30.436875, the mean month length in the Gregorian calendar.
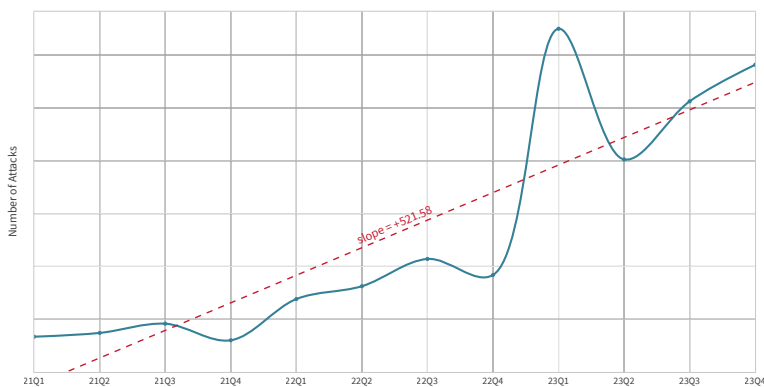
DDoS Attacks per Customer - Americas



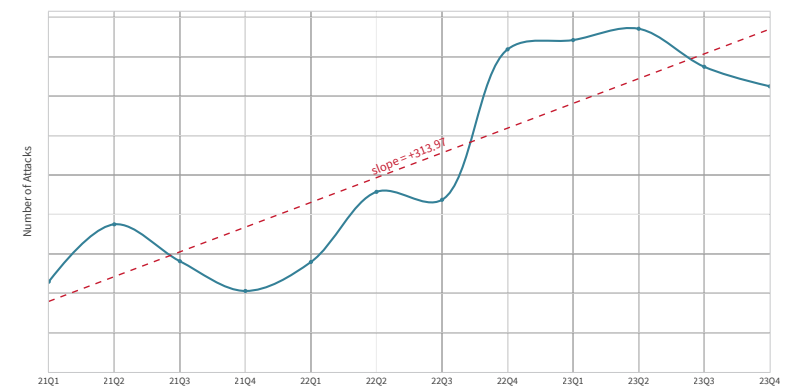**Figure 12:**

Evolution of DDoS attacks targeting organizations located in the Americas

**Figure 14:**

Evolution of DDoS attacks targeting organizations located in the EMEA region

DDoS Attacks per Customer - EMEA

## Asia Pacific

The number of DDoS attacks targeting customers in the APAC region increased by a staggering 260% in 2023 compared to 2022. In 2022, the number of attacks per customer was on par with 2021.

The number of attacks per customer in the APAC region reached an all-time high in Q4 of 2023.

The number of attacks per customer in the APAC region is trending with an average increase of 182 attacks per quarter, 61 attacks per month, or 2.0[8] attacks per day. This is slower than the global average of 3.48 attacks per day.

**Figure 16:**

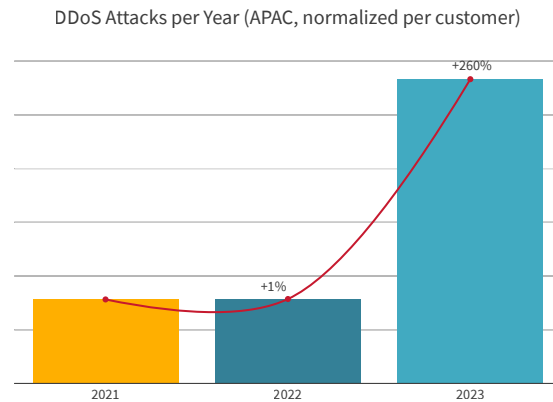Evolution of DDoS attacks targeting organizations located in the APAC region

DDoS Attacks per Customer - APAC



**Figure 15:**

DDoS Attacks per year targeting organizations located in the APAC Region

DDoS Attacks per Year (APAC, normalized per customer)



---
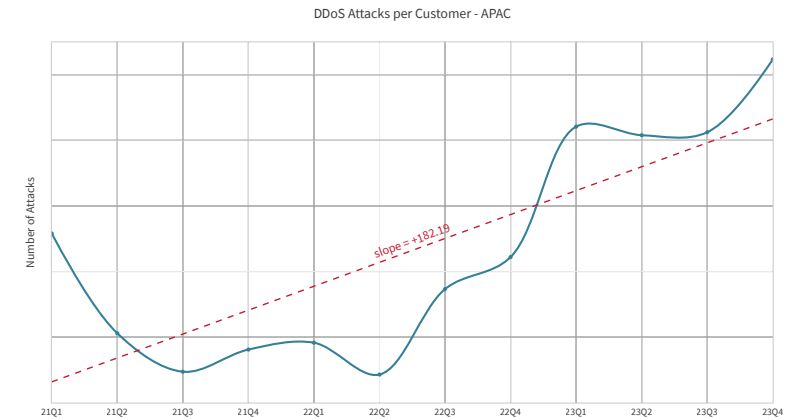
8.   182 attacks per quarter divided by 3 * 30.436875, the mean month length in the Gregorian calendar.

# Industries

In 2023, certain industries faced a disproportionate share of DDoS attacks (see Figure 17). Notably, organizations within finance experienced almost 30% of the global attack activity. Organizations in the technology industry faced a considerable number of attacks and were targeted by 22.2% of all DDoS attacks.

Other notable industries that were frequent targets of DDoS attacks were healthcare (14.2%), government (11.5%), transportation and logistics (8.64%), and gaming (3.09%). All other organizations combined suffered 11% of the global attack activity.

Compared to 2022, organizations in transportation and logistics faced 36% more attacks in 2023. Organizations in the utilities industry faced 23% more attacks in 2023. Energy (10%), gaming (8.9%), government (5.5%) and manufacturing (5.2%) were the other notable industries with considerable growths in number of attacks in 2023.

Only a limited number of industries had a decrease in attack activity compared to last year. Organizations in the communications industry had a reduction of 0.5% in attack activity in 2023. Service providers saw a reduction of 0.6% and e-commerce a reduction of 0.8%, all less than 1% reduction based on the average number of attacks per customer per industry.

Considering the number of attacks over time (Figure 19), finance institutions and technology organizations were targeted throughout the

**Figure 17:** Most attacked industries
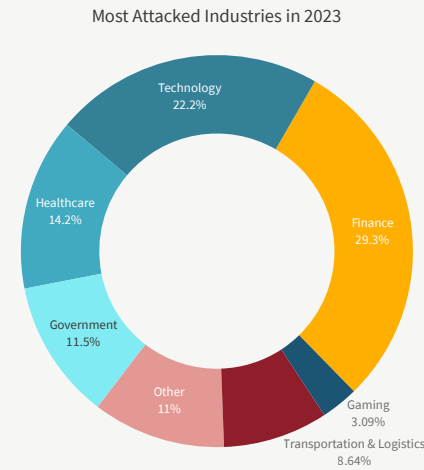


Most Attacked Industries in 2023

Compared to 2022, organizations in **transportation and logistics faced 36% more attacks** in 2023. Organizations in the utilities industry faced 23% more attacks

**Figure 18:** Increase in DDoS attacks per industry from 2022 to 2023



Attack Growth per Industry (2023 compared to 2022)
(based on number of attacks normalized per customer)
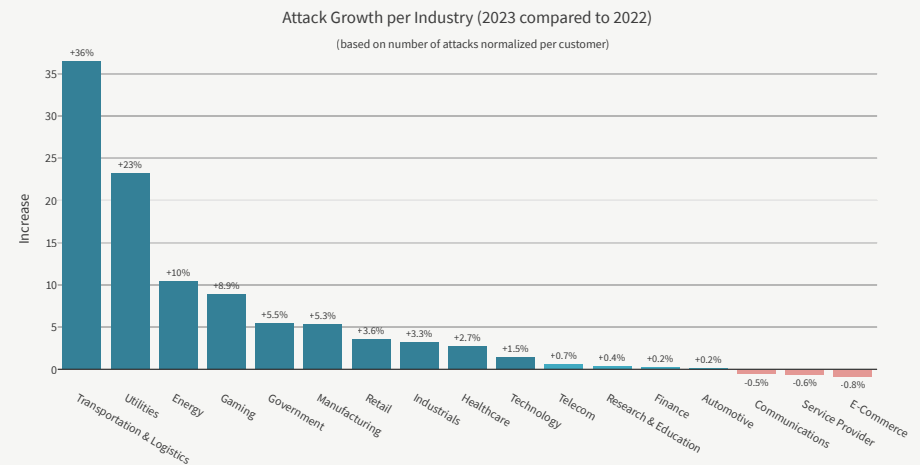
whole year. Organizations in the transportation and logistics industry and government institutions were assaulted more heavily in the first quarter of the year with still a significant number of attacks in the other quarters. Healthcare was most attacked in the third quarter of 2023, but a small increase compared to the activity in Q1, Q2 and Q4.

Technology organizations and institutions in research and education shared the largest volumes of attack traffic in all quarters but Q3 (Figure 20). In Q3, telecom organizations bore the brunt of the global attack volume. Finance institutions faced more considerable volumes in Q2 and Q4 of 2023.
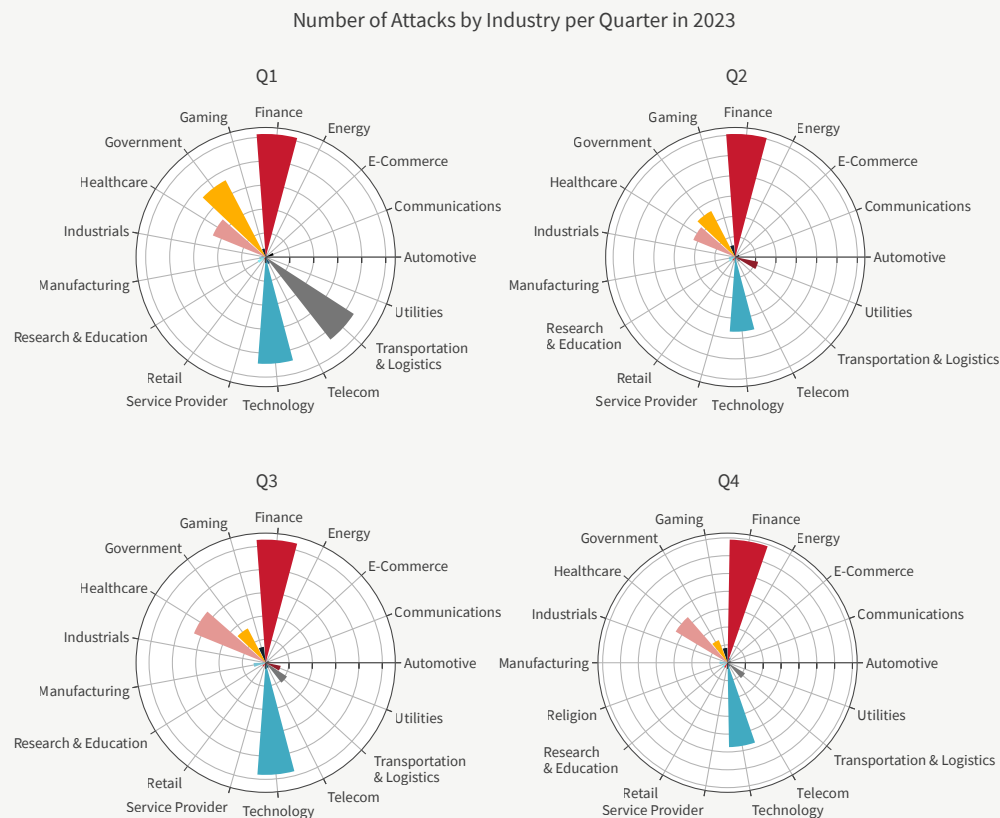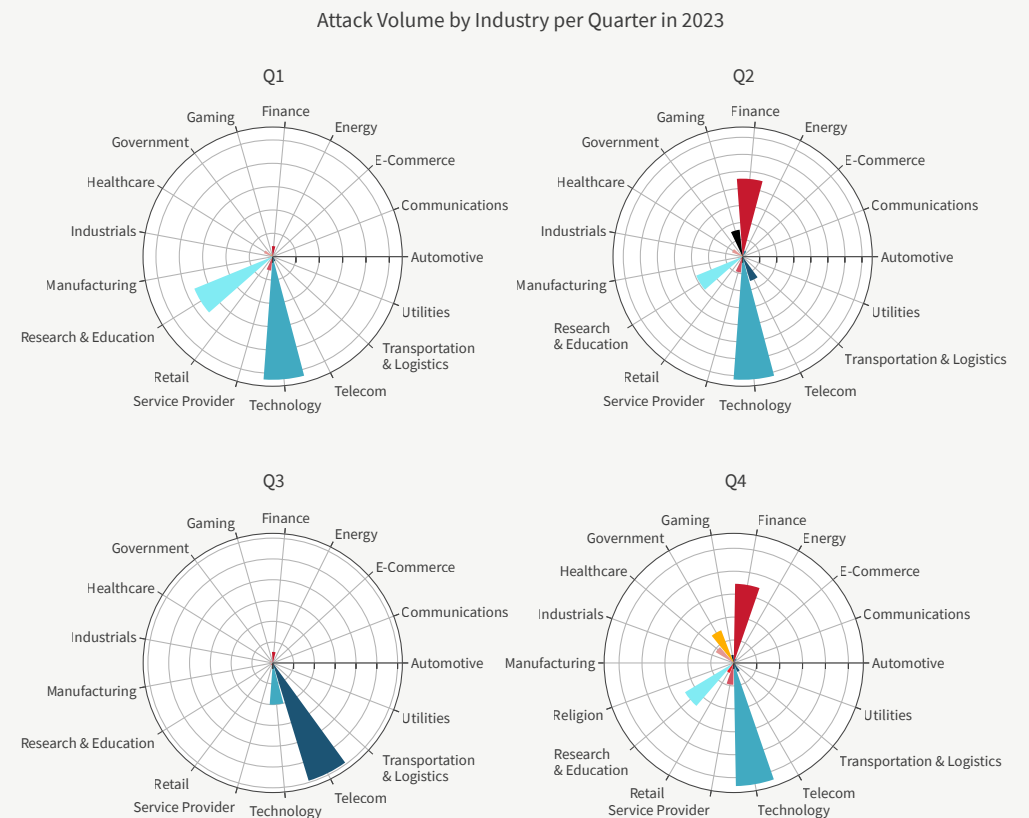
**Figure 19:** Attack activity per industry per quarter



Number of Attacks by Industry per Quarter in 2023

**Figure 20:** Attack volume per industry per quarter



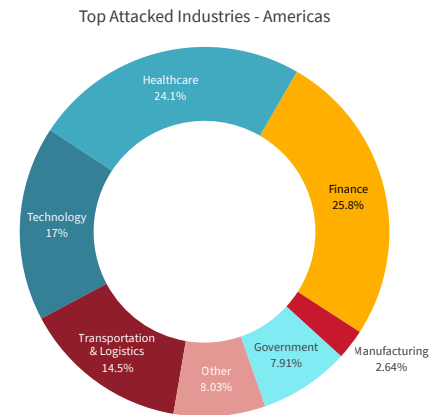Attack Volume by Industry per Quarter in 2023

## North, Central and South American Industries

Finance (25.8%) and healthcare (24.1%) institutions accounted for almost half of the attack activity in the Americas region. Organizations in technology and the transportation and logistics industry mitigated 17% and 14.5% of the attacks, respectively, in the region. Government institutions were attacked by almost 8% of the total attack activity of the region.

Except for communication and service providers, all industries in the Americas region suffered more attacks in 2023 compared to 2022. Transportation and logistics grew the most significantly, with 69% more attacks in 2023 compared to 2022. Energy (12%) and government (10%) were the second and third most notable industries that had a double-digit increase in attack activity in the region in 2023.

**Figure 21:**

Most attacked industries in the Americas region
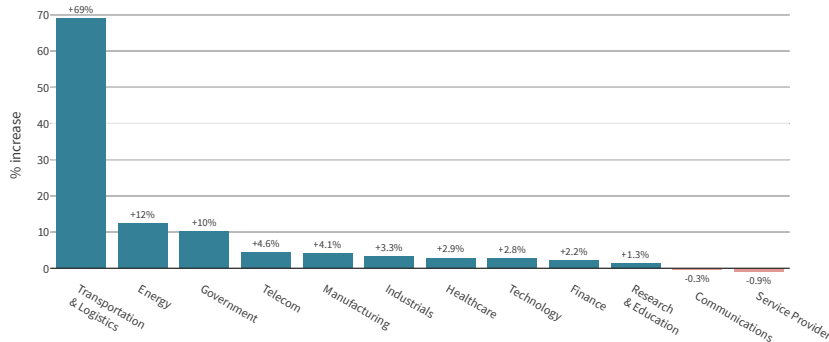
Top Attacked Industries - Americas



**Figure 22:**

Increase in DDoS attacks per industry for the Americas region

Attack Growth per Industry - Americas



## Europe, Middle East and African Industries

Finance was the most attacked industry in the EMEA region in 2023, accounting for 41.4% of all the attacks in the region. Technology organizations and government institutions mitigated 18.2% and 14.6% of the attack activity, respectively, in the region. Utilities (6.27%), healthcare (4.86%), and gaming (4.75%) were also notable industries, while the other industries combined had to fend off 9.9% of the attack activity in the region.

Organizations in the transportation and logistics and the utilities industry in the EMEA region were attacked 48% and 35% more frequently, respectively, in 2023 compared to 2022. The energy (16%), gaming (14%) and manufacturing (13%) industries in the region all had a considerable growth in attack activity in 2023. Only e-commerce and research and education had a very mild reduction of 0.2% and 0.9% of the number of attacks, respectively, in 2023 compared to 2022.

**Figure 23:**

Most attacked industries in the EMEA region
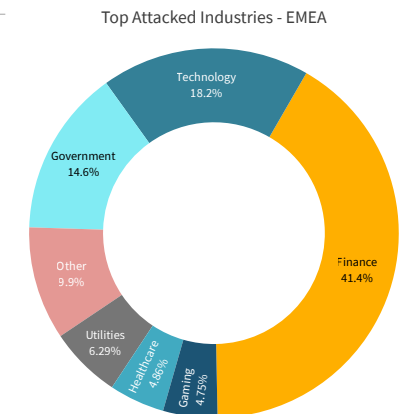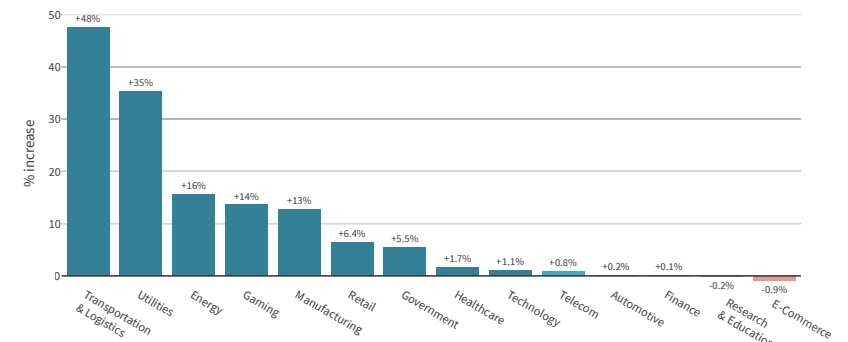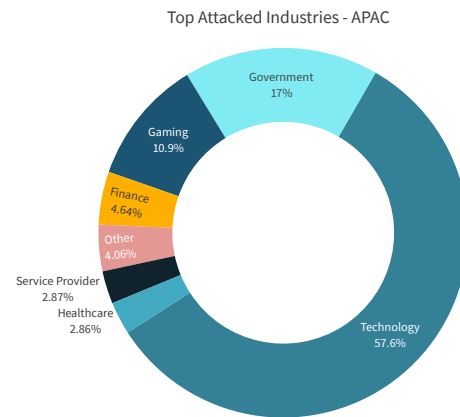
Top Attacked Industries - EMEA



**Figure 24:**

Increase in DDoS attacks per industry for the EMEA region

Attack Growth per Industry - EMEA
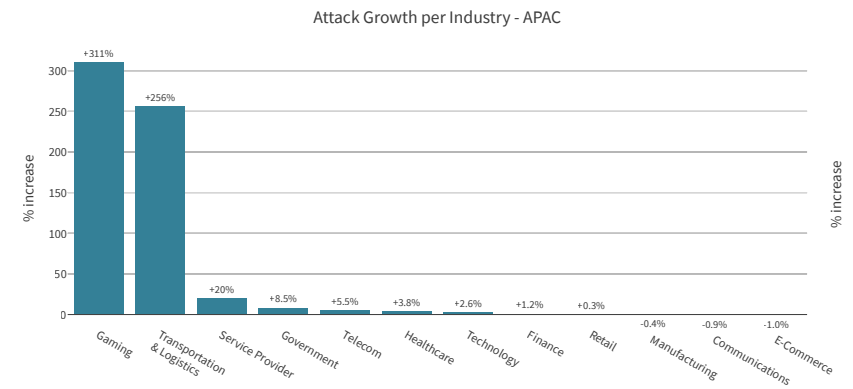
## Asia Pacific Industries

In the APAC region, technology organizations were targeted by more than half (57.6%) of the overall attack activity in the region. Government institutions (17%) and gaming organizations (10.9%) had to endure a significant amount of the attacks. Finance (4.64%), service providers (2.87%) and healthcare (2.68%) were other notable industries that accounted for a fair amount of attack activity in the region. All other industries combined represented 4.06% of the attacks in the APAC region.

Also in the APAC region, the gaming industry fended off 3.11 times more attacks in 2023 compared to 2022. The transportation and logistics industry also had an important growth of 2.6 times the number of attacks in 2023 compared to 2022. Service providers in the region saw 20% more attacks in 2023. Only manufacturing, communications and e-commerce industries had a slight reduction in the number of attacks in 2023 compared to 2022, which was 0.4%, 0.9%, and 1.0%, respectively.

**Figure 25:**

Most attacked industries in the APAC region

Top Attacked Industries - APAC

Government 17%
Gaming 10.9%
Finance 4.64%
Other 4.06%
Service Provider 2.87%
Healthcare 2.86%
Technology 57.6%

**Figure 26:**

Increase in DDoS attacks per industry for the APAC region

Attack Growth per Industry - APAC

Gaming +311%
Transportation & Logistics +256%
Service Provider +20%
Government +8.5%
Telecom +5.5%
Healthcare +3.8%
Technology +2.6%
Finance +1.2%
Retail +0.3%
Manufacturing -0.4%
Communications -0.9%
E-Commerce -1.0%

# Attack Vector Characterization

A DDoS attack consists of one or more attack vectors running simultaneously or sequentially over the time of the attack. In this section, individual attack vectors are analyzed to understand and characterize the nature of the DDoS attack threat landscape in 2023.

To compare the size evolution, attack vectors are divided into three categories based on their attack size, expressed in gigabits per second (Gbps). Small attacks are those below 1Gbps, while large attacks are those above 100Gbps. By normalizing the number of vectors in each size category against the number of vectors in 2020, the relative vector size evolution over time can be compared.

Compared to earlier years, the relative number of mid-sized attacks grew very slowly with a 1.76-time increase in 2023 compared to 2020. In contrast, the medium attack vectors demonstrate a steady, almost exponential growth over the last four years. The large vectors, however, grew very steeply compared to a stagnant trend in previous years. The medium attack vectors were 13.4 times more present during attacks in 2023 compared to 2020 and more than two times compared to 2022. Large attack vectors grew from a two-time increase between 2020 and 2022 to a staggering 15.5-time increase.

In conclusion, the 2023 DDoS threat landscape can be characterized by the rapid growth of attack sizes.

The attack bandwidth is governed by the packet rate and the size of the packets. Average packet size is an important metric to maximize the impact of an attack depending on the resources available to the attackers or the victims. Attackers will typically favor larger packets to increase the bandwidth of the attack when packet rates are constrained by the available processing resources. When attempting to exhaust the processing resources of network components and servers, the packet rate will be the most effective tactic. Consequently, bandwidth can be reduced by leveraging smaller packets without impacting the effectiveness of the attack.

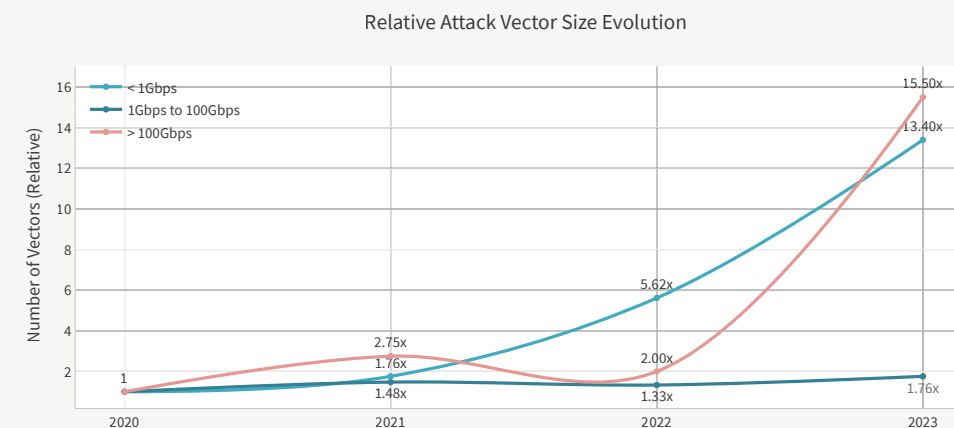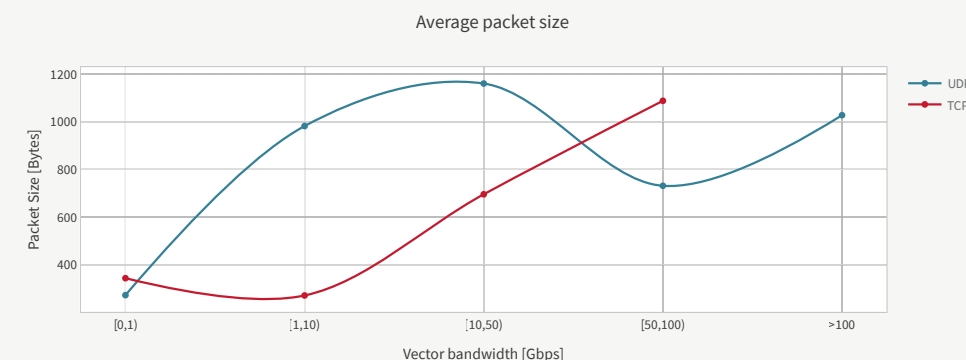**Figure 27:** Relative DDoS attack vector size evolution



**Figure 28:** Average attack vector packet size for TCP and UDP as function of the vector's bandwidth

## Attack Protocols

User Datagram Protocol (UDP) is by far the most leveraged protocol in volumetric DDoS attacks. Because of its stateless character, UDP allows legitimate services to be abused to send large volumes of unsolicited traffic to victims through reflection and amplification attacks. TCP SYN and out-of-state packets are also leveraged for volumetric attacks, but the TCP protocol is typically most used in attacks aiming to exhaust resources on devices and servers.

By significant margin, the top attack vector leveraged during volumetric attacks was UDP fragment flood (43%), followed by UDP flood (19.2%) and TCP flood (14.4%).

Attacks aiming to exhaust resources will typically be characterized by higher packet rates. DNS-A query floods accounted for most (21.8%) of the malicious packets in 2023.

For volumetric attacks, attackers leverage amplification services that are publicly exposed on the internet. If it's UDP and it is exposed to the internet, it can be weaponized for DDoS amplification attacks. The motivation to weaponize a specific protocol depends on the amplification factor (AF)— the ratio between the size of the request and the reply— and the number of available or exposed services on the internet. A higher AF means a more efficient attack. More exposed services represent a larger total aggregate bandwidth and a higher diversity in source IPs in the attack traffic, making detection slightly more difficult.

Some of the most important and top amplification vectors and their associated maximum amplification factor are listed in Table 1.

NTP amplification generated the most volume in 2023, representing almost half of the total attack volume for the year. DNS amplification was the most leveraged amplification attack vector and represented over 65% of all the amplification attack vectors observed in 2023.
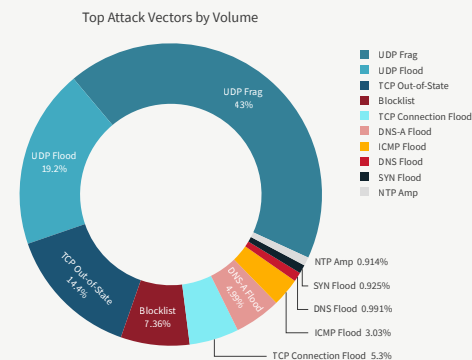


**Figure 29:** Attack vectors by volume
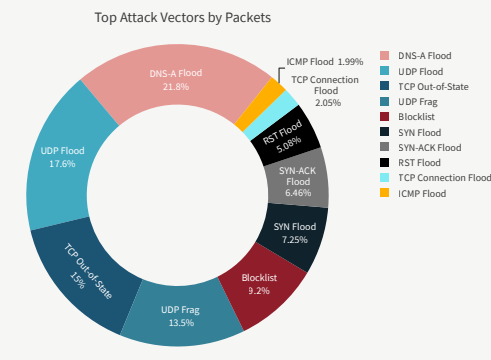


**Figure 30:** Attack vectors by packets

**Table 1:** DDoS amplification attack vectors

| Amplification Vector | Amplification Factor | Port |
|---|---|---|
| NTP | 500x | UDP/123 |
| DNS | 160x | UDP/53 |
| SSDP | 30x | UDP/1900 |
| Memcached | 50,000x | UDP/11211 |
| Chargen | 1,000x | UDP/19 |
| ARMS | 30x | UDP/3283 |
| CLDAP | 50x | UDP/398 |
| DHCPDiscover | 25x | UDP/37810 |
| SNMP | 880x | UDP/161 |

DNS, HTTPS and HTTP were the most targeted applications, both in terms of volume and in terms of packets. DNS and HTTPS form the cornerstone of online applications and APIs. Attackers had a clear mission in 2023: hit where it hurts the most. DNS, by far, was the most targeted application protocol, followed by HTTPS.

The Session Initiation Protocol (SIP), a signaling protocol used for initiating, maintaining and terminating communication sessions that include voice, video and messaging applications, was the fifth most targeted application protocol in 2023. SIP is used in internet telephony, private IP telephone systems and mobile phone calling over LTE (voice over LTE or VoLTE). SIP is a key protocol and most communications in businesses will grind to a halt when the protocol becomes unavailable through a denial of service attack.

The top network-level attack vectors targeting HTTPS services were SYN flood, TCP Out-of-State, and UDP and TCP RST floods, jointly representing over 75% of all malicious packets directed at encrypted web applications.

Almost 95% of the attacks targeting DNS services leveraged DNS-A query floods, followed at a fair distance by DNS-AAAA floods, leveraged only by a fraction of the attacks. DNS-A and DNS-AAAA queries are the most common DNS queries on the internet. Query record type A allows a client to request the IPv4 address for a specified hostname. Record type AAAA is very similar, but requests the IPv6 address. Application layer DNS attacks leveraging pseudo random subdomain (PRSD) attacks, also known as DNS water torture, have been one of the most common attacks in 2023.

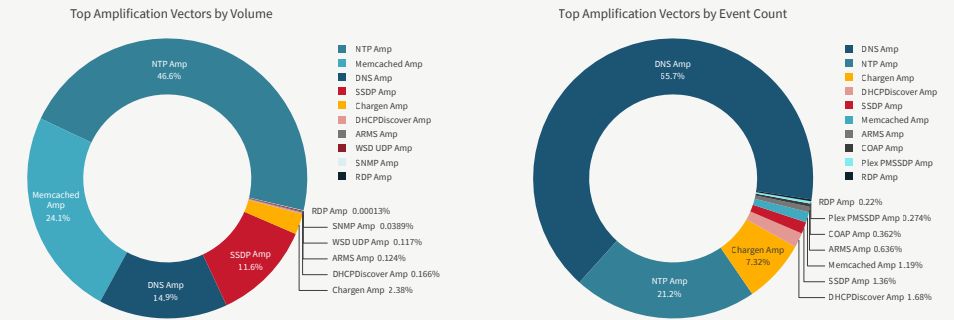**Figure 31:** Top amplification vectors by volume and by event count

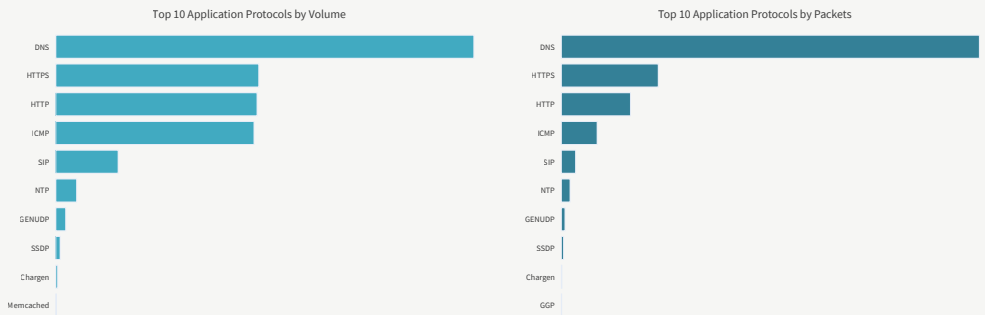

**Figure 32:** Top application protocols by volume and by packets



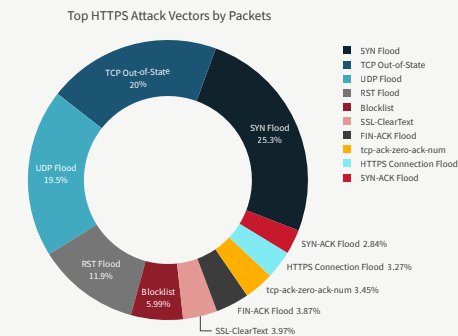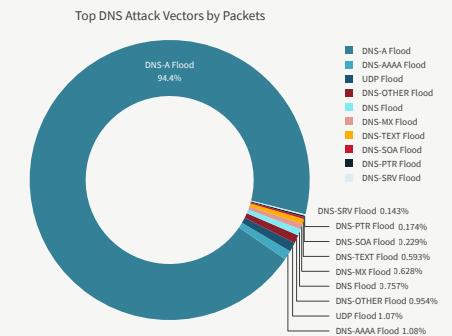**Figure 33:** Top attack vectors targeting HTTPS services

**Figure 34:** Top attack vectors targeting DNS services

# Industry Attack Characterization

## Finance Attack Activity

Most of the attack volume that targeted finance organizations in 2023 was comprised of UDP Frag, TCP Out-of-State and UDP floods. DNS-A query floods represented just over 5% of the finance attack volume.

**Figure 35:** Top attack vectors targeting finance institutions



*Finance Top Attack Vectors by Volume*

*Finance Top Attack Vectors by Packets*
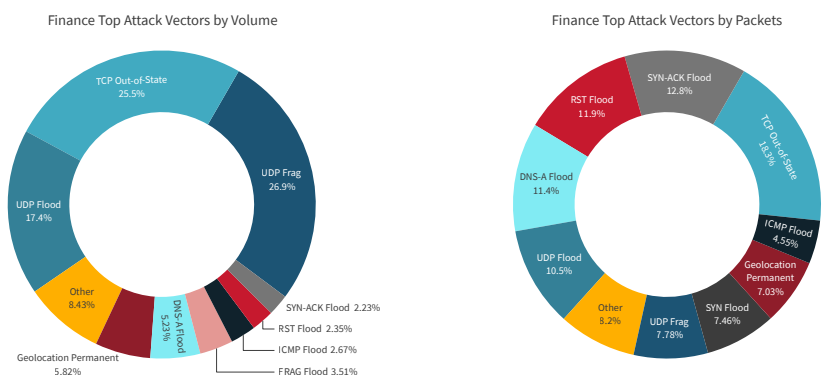
Almost 20% of all attack packets targeting finance were TCP out-of-state packets. SYN-ACK and RST floods each representing about 12% of all packets targeting finance organizations. DNS-A query floods and UDP floods each represented about 11% of all malicious packets.

Almost half of the attack vectors targeting finance applications were encrypted web attacks. Nearly 30% of the attack vectors were random destination port floods while IPSec NAT-T[9] was the target of 16% of the attack vectors.

**Figure 36:** Top targeted services in finance institutions



*Finance Top Targeted Ports by Event Count*

---
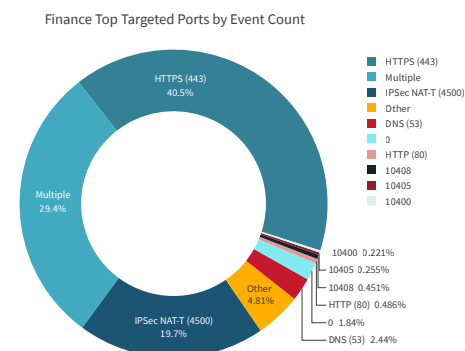
9.  IPSec is a network protocol suite that authenticates and encrypts communications between two remote networks over the internet. IPSec NAT-T is used to allow remote devices and networks to communicate across a Network Address Translation device. A typical use case would be a road warrior or home office worker connecting to the main office or branch through IPSec.

## Technology Attack Activity

The attack volume targeting technology organizations was mostly generated by UDP fragmentation and UDP as well as TCP connection floods. DNS-A floods generated 43.3% of all packets targeting technology organizations.

More than half of the attack vectors were targeting online web applications using encrypted web attacks. IPSec NAT-T and DNS were other notable technology organization services targeted by DDoS attacks.

## Healthcare Attack Activity

Most of the network-level attack activity targeting healthcare organizations consisted of TCP attack vectors targeting network devices through random destination ports and network ranges by leveraging Carpet Bombing attacks. Also notable are attacks targeting DNS services in those organizations.

**Figure 37:** Top attack vectors targeting technology organizations



Technology Top Attack Vectors by Volume

Technology Top Attack Vectors by Packets

**Figure 39:** Top attack vectors targeting healthcare



Healthcare Top Attack Vectors by Volume

Healthcare Top Attack Vectors by Packets

**Figure 38:**

Top targeted services of technology organizations



Technology Top Targeted Ports by Event Count
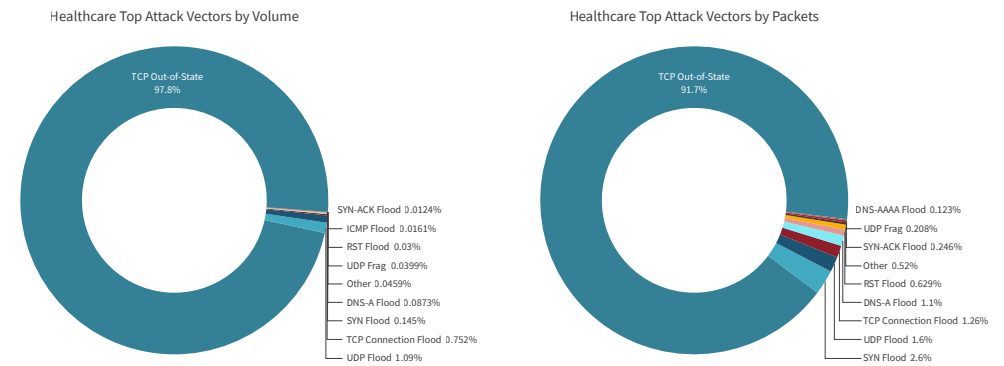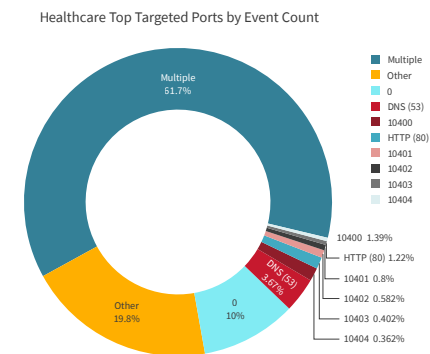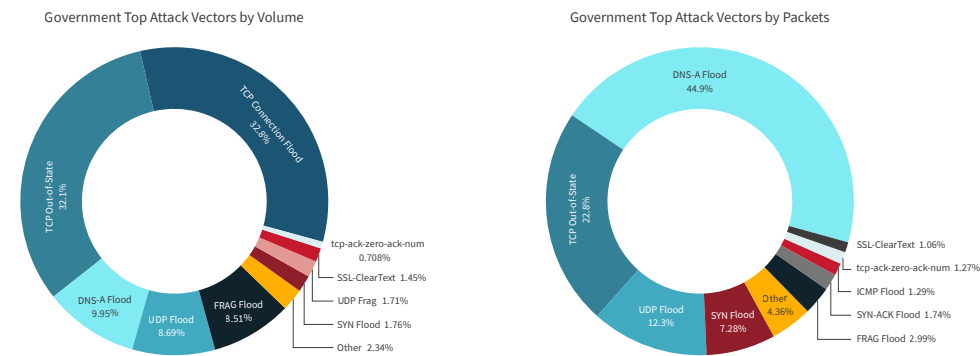
**Figure 40:**

Top targeted healthcare services



Healthcare Top Targeted Ports by Event Count

## Government Attack Activity

The network-level attack volume targeting government services consisted of TCP connection (32.5%), TCP out-of-state (32.1%) and DNS-A query floods (9.85%). Jointly, those resource exhaustion attack vectors represented almost 75% of the attack volume. The remainder of the attack volume mostly consisted of volumetric attack vectors. DNS-A query floods were the most aggressive attacks the industry had to fend off, representing 44.6% of all malicious packets targeting government organizations.

## Transportation & Logistics Attack Activity

In the transportation and logistics industry, 58.7% of the network-level attack volume consisted of TCP out-of-state attack floods while NTP amplification and UDP floods jointly represented 30.65%. DNS-A query floods generated 44.6% and TCP out-of-state floods generated 22.8% of all malicious packets targeting the industry.

**Figure 41:** Top attack vectors targeting government



Government Top Attack Vectors by Volume

Government Top Attack Vectors by Packets

**Figure 42:** Top attack vectors targeting transportation and logistics



Transportation & Logistics Top Attack Vectors by Volume

Transportation & Logistics Top Attack Vectors by Packets
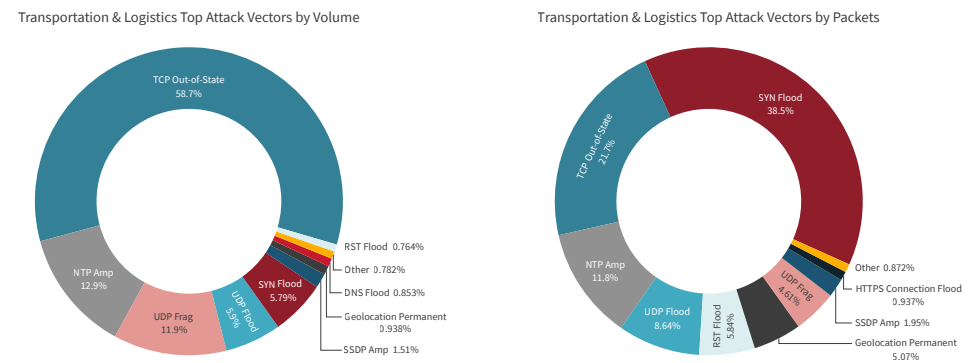
# Application-level Attacks in 2023

## DNS Floods

The digital era has catalyzed rapid growth in online commercial activities, making e-commerce and online platforms a vital component of the global economy. However, this technological advancement is not without its vulnerabilities. A crucial and ubiquitous part of this digital ecosystem is DNS, which acts as the internet's phonebook, translating human-readable domain names into their underlying IP addresses. When a DNS service is subjected to a cyberattack, such as denial-of-service or distributed denial-of-service, the disruption caused can be catastrophic for businesses.

DNS denial-of-service attacks come in various forms, each with unique techniques and impacts. Here are the most common attack types:

**DNS Amplification Attack:** This is a type of network-level, reflection-based, volumetric DDoS attack where the attacker crafts a DNS query packet with a forged source IP address (the victim's). It sends it to a legitimate open DNS resolver which subsequently replies to the victim with a large amount of data. The goal is to overwhelm the victim's network with traffic.

**DNS Flood Attack:** A DNS flood is a type of application-layer DDoS attack that seeks to overload a DNS server with a high volume of requests until it becomes unresponsive. The requests appear legitimate, making it difficult to filter out malicious traffic.

**DNS NXDOMAIN Attack**: In this type of DNS flood attack the attacker sends a high volume of requests for non-existent or invalid domains, resulting in DNS recursion and NXDOMAIN (nonexistent domain) responses. The server must work hard to try and resolve these spurious requests, thereby consuming valuable resources instead of processing legitimate requests. When a DNS server is under NXDOMAIN attack, the cache of the DNS server will be flooded with NXDOMAIN results, forcing the server to resolve legitimate requests repeatedly instead of fetching the answer from its cache.

**Phantom Domain Attack:** This attack involves the attacker setting up one or more phantom domains that do not respond to DNS queries and sending requests to the victim's DNS server to resolve the phantom domains. The victim's DNS server gets overwhelmed when it tries to resolve the phantom domains through nonresponsive servers. This causes the recursive server to spend valuable resources waiting for responses that will never come.

**Pseudo Random Subdomain (PRSD) Attack:** Also known as water torture attacks, this attack is similar to the DNS NXDOMAIN attack. The attacker sends a massive number of requests for nonexistent subdomains of a valid and existing domain through different recursive resolvers. This causes the authoritative server to consume resources trying to resolve these non-existent subdomains, eventually leading to a denial of service.

In each case, the attacker's objective is to disrupt the DNS service and make the websites and online services that rely on it inaccessible. These attacks exploit different aspects of the DNS protocol, making them challenging to defend against and highlighting the importance of implementing robust DNS security measures.

DNS amplification attacks are discussed in the Network-level Attack section under [Attack Protocols](#) on page 16. This section considers application-level attacks and only considers DNS flood attacks or Layer 7 DNS query flood attacks that aim to overwhelm a DNS server with a high volume of illegitimate requests.

By determining the proportion of DNS flood attack events or vectors directed specifically at DNS services in relation to the overall event count, we can gauge the progression of DNS floods over time, irrespective of the total activity or number of customers protected by the Cloud DDoS Protection service.

Throughout 2021 and most of 2022, fewer than nine out of every 1,000 attack vectors was a DNS flood vector. However, from Q4 of 2022, we noted a marked increase in the proportion of attacks featuring a DNS flood vector. Throughout 2023, the ratio experienced a significant increase quarter after quarter and rose to more than 28 attacks per 1,000 in Q4 of 2023.

The area chart depicted in Figure 44 traces the development of the count of DNS flood attack vectors according to each query type. A description of the key DNS record types can be found in Appendix A: Common DNS Record Types. The total number of DNS floods mitigated each month corroborates the escalating trend discerned in the previous DNS flood attack ratio graph. From September 2022 onward, the monthly number of DNS floods grew significantly and accelerated even more during the last four months of 2023.

Considering the number of queries per DNS type in Figure 45, DNS type A queries have been the dominant DNS flood attacks since September 2020, and its number per month kept relatively constant until November 2022. In the last three months of 2023, we observed new levels of DNS-A queries reaching well above 200 billion queries per month in December of 2023.

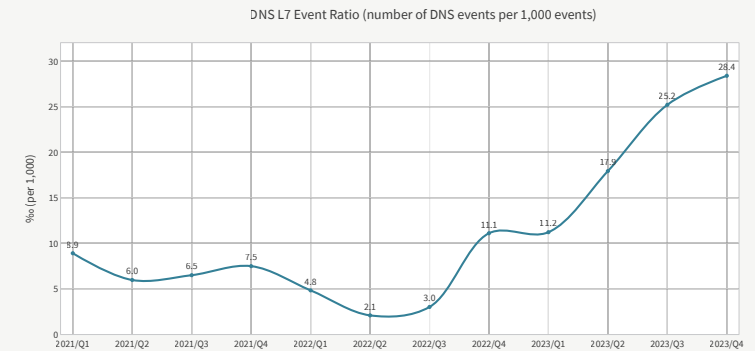**Figure 43:**

DNS flood attack vector ratio evolution over time
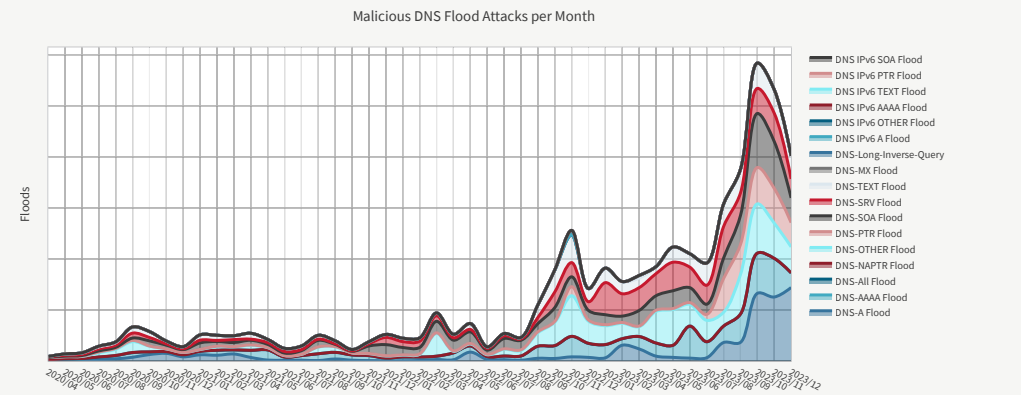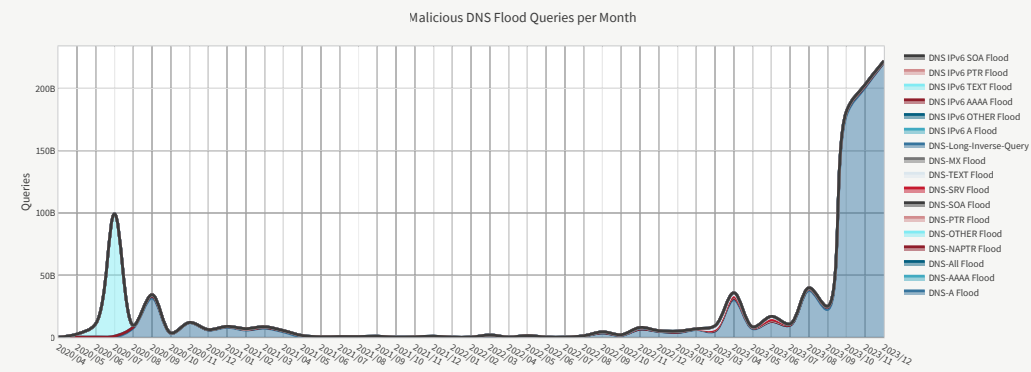


**Figure 44:** Number of DNS floods per month



**Figure 45:** DNS flood queries per month

DNS floods are application-layer assaults with the objective of compromising the server's capability to respond to valid DNS requests. The pace of these requests determines the total effect on the server. The blue trajectory in Figure 46's chart illustrates the highest DNS query rate detected each quarter, denoted in queries per second (QPS). Note that the QPS rates increased significantly since Q4 2022 and kept increasing for most of 2023, peaking at 2.15 million DNS queries per second in Q3 of 2023.

The red trajectory in Figure 46's chart demonstrates the peak traffic of the most significant DNS flood each quarter. The traffic rate shows a consistent pattern aligning with the maximum query rate. It is important to note that DNS Query floods do not generate large traffic volumes. The most substantial flood of 2.15 million QPS generated a traffic volume that peaked at 1.52 Gbps.

Organizations in research and education (31.5%), telecom (24.9%), technology (18.7%), finance (9.53%) and healthcare (6.02%) were most targeted by DNS flood attacks. Technology organizations observed 73.2% of all malicious DNS queries while finance and government had to manage 10.8% and 5.45% of all malicious DNS queries, respectively.

Finance had to manage the most significant DNS Query flood attack, which peaked at 2.15 million QPS. A telecom customer managed the second most significant attack, which peaked at 1.29 million QPS, while a government customer managed an attack that peaked at 830,000 QPS.

**Figure 46:**

Queries per second and bandwidth consumption by DNS floods


DNS Queries per Second and Bandwidth Consumption
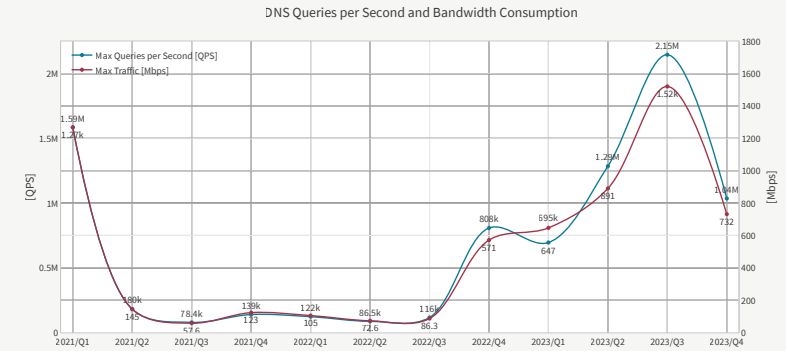
**Figure 47:** Number of DNS floods and queries per industry


Number of DNS Flood Attacks per Industry


Total Number of DNS Flood Queries per Industry

**Figure 48:**

Maximum DNS attack query rate per industry
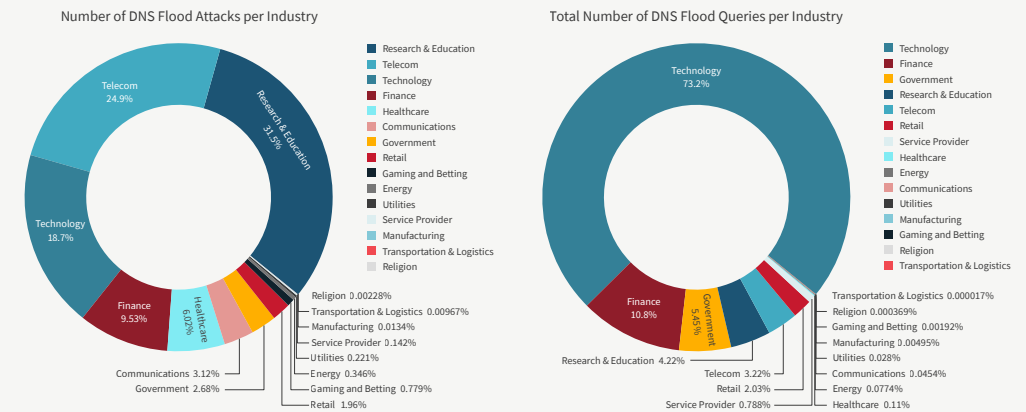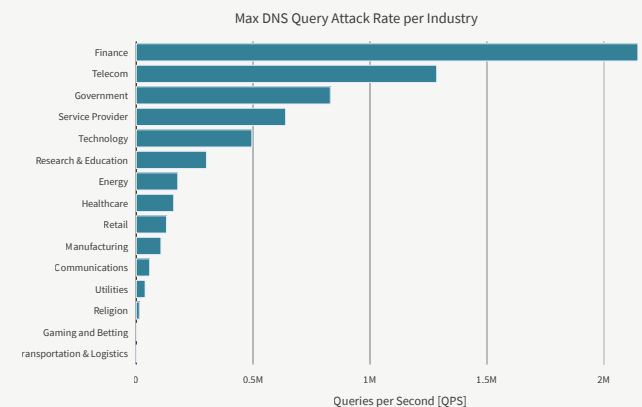

Max DNS Query Attack Rate per Industry

# Web Application and API Attacks

The total number of malicious web application and API transactions increased by 171% in 2023 compared to 2022. This is a significant increase compared to the 128% increase in 2022 compared to 2021. As noted in the H1 2023 report, a significant part of this increase in attack activity is caused by L7 encrypted web application attacks or Web DDoS attacks. During the first half of 2023, we noticed a large increase in web application DDoS attacks. This trend continued, if not accelerated, towards the end of the year.

As shown in Figure 50, the drop in observed malicious web application transactions in Q3 and Q4 is attributed to a new layer of defense introduced in Radware's Cloud Protection Services. Following the large increase in the number and sophistication of Web DDoS attacks at the beginning of the year, Radware released a new automated detection and mitigation solution for Web DDoS attacks. This new layer of protection sits between the network layer DDoS protection and the web application and API protection layer. The new protection layer is significantly more efficient in detecting and processing large scale Web DDoS attacks. As customers subscribed to the new service, fewer malicious transactions made it through to the Web application and API protection layer. This resulted in a decrease in the number of recorded malicious web application transactions.

Based on a sample period of one week in December 2023, the new Web DDoS protection service mitigated 927 million malicious web transactions with an average request rate of 6,809 RPS. The largest attack observed during that week was 1.5 million RPS. The shortest observed attack had a duration of 20 seconds, and the longest lasted 24 hours.

Starting in Q3, Web DDoS attack transactions are mostly eliminated from the reporting, but there is still a significant increase in targeted web application attacks in Q3 and Q4 compared to earlier years. Considering

**Figure 49:**

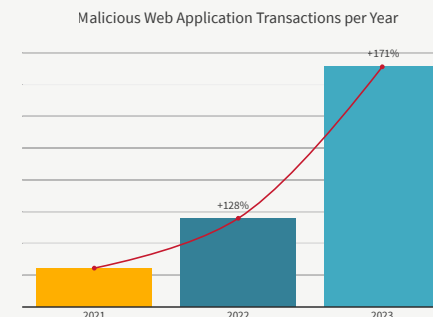Malicious web application and API transactions per year

Malicious Web Application Transactions per Year

**Figure 50:**

Malicious web application and API transactions per quarter

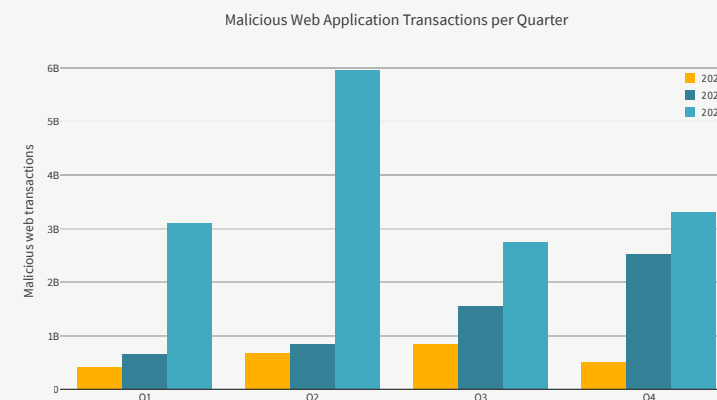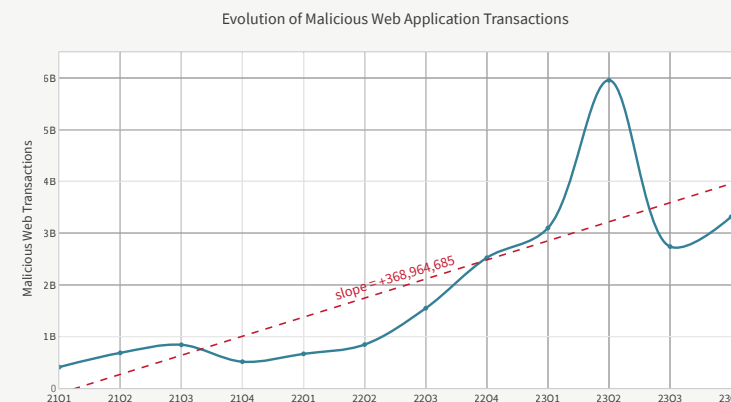Malicious Web Application Transactions per Quarter

**Figure 51:**

Evolution and trend over time of malicious web application and API transactions

Evolution of Malicious Web Application Transactions

slope = +368,964,685

the Web DDoS activity, it is assumed[10] that web application transactions kept rising in the second half of 2023. This effect was caused by several trends in the threat landscape. It was driven by hacktivists reaching for more sophisticated L7 attacks targeting online applications and many DDoS-for-hire services that started creating more offerings of L7 web application and API attack vectors, continuously improving them and adding features. DDoS-for-hire services moved their focus from L3/L4 to L7 attack vectors. The HTTP/2 Rapid Reset vulnerability disclosed in October was quickly picked up by many DDoS-for-hire service providers and resulted in a significant increase in the application-level attack rates.

Targeted malicious web application attacks can be blocked by application-specific and custom rules—learned by inspecting the application and tuned by the security operations center (SOC)—or by generic signature detection and known and zero-day attack detection modules. The chart in Figure 52 shows that the share of targeted malicious transactions blocked by generic signature and attack detection modules remained mostly unchanged for the first three quarters of the year before increasing in last quarter.

The remainder of this section considers attacks detected and blocked by signatures and attack detection modules based on malicious behavior, vulnerabilities and exploits.

**Figure 52:** Web application and API transactions—total vs blocked by signature

Total Blocked Web Application Transactions Vs Blocked By Signature



---
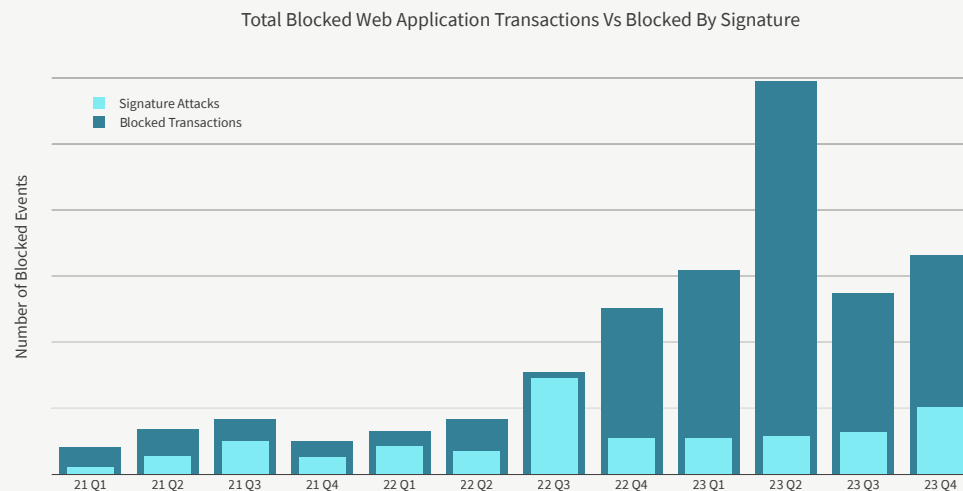
10. Web DDoS attack statics are based on a sample collected in December 2023. The new Web DDoS service event logging infrastructure was not integrated into the global infrastructure to provide full coverage in stats of the second half of 2023. Stats are expected to be available starting the H1 2024 report.

# Security Violations

The most important security violation for 2023 (Figure 53), predictable resource location attacks, has always accounted for a significant part of the total attack count (Figure 54). Predictable resource location attacks target hidden content and functionality of web applications. By guessing common names for directories or files, an attack may be able to access resources that were not intended to be exposed. Examples of resources that might be uncovered through brute force techniques include old backup and configuration files and yet-to-be-published web application resources.

Code and SQL injection were in second and third position, respectively. Combined with predictable resource location attacks, these three web application attacks were responsible for 62% of the total attack activity on web applications and APIs. Compared to 2022, predictable resource location is less prominent, but the top four violations remain predictable resource locations, code injection, SQL injection and server information leakage.

**Figure 53:**

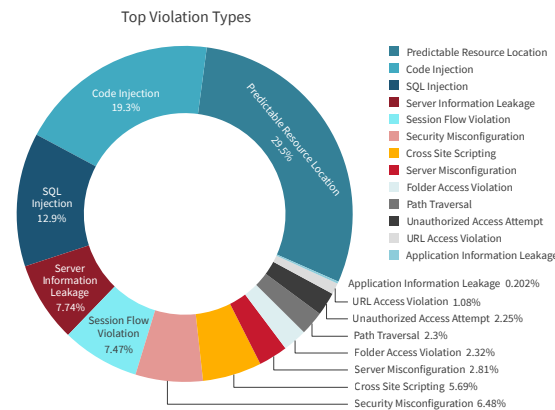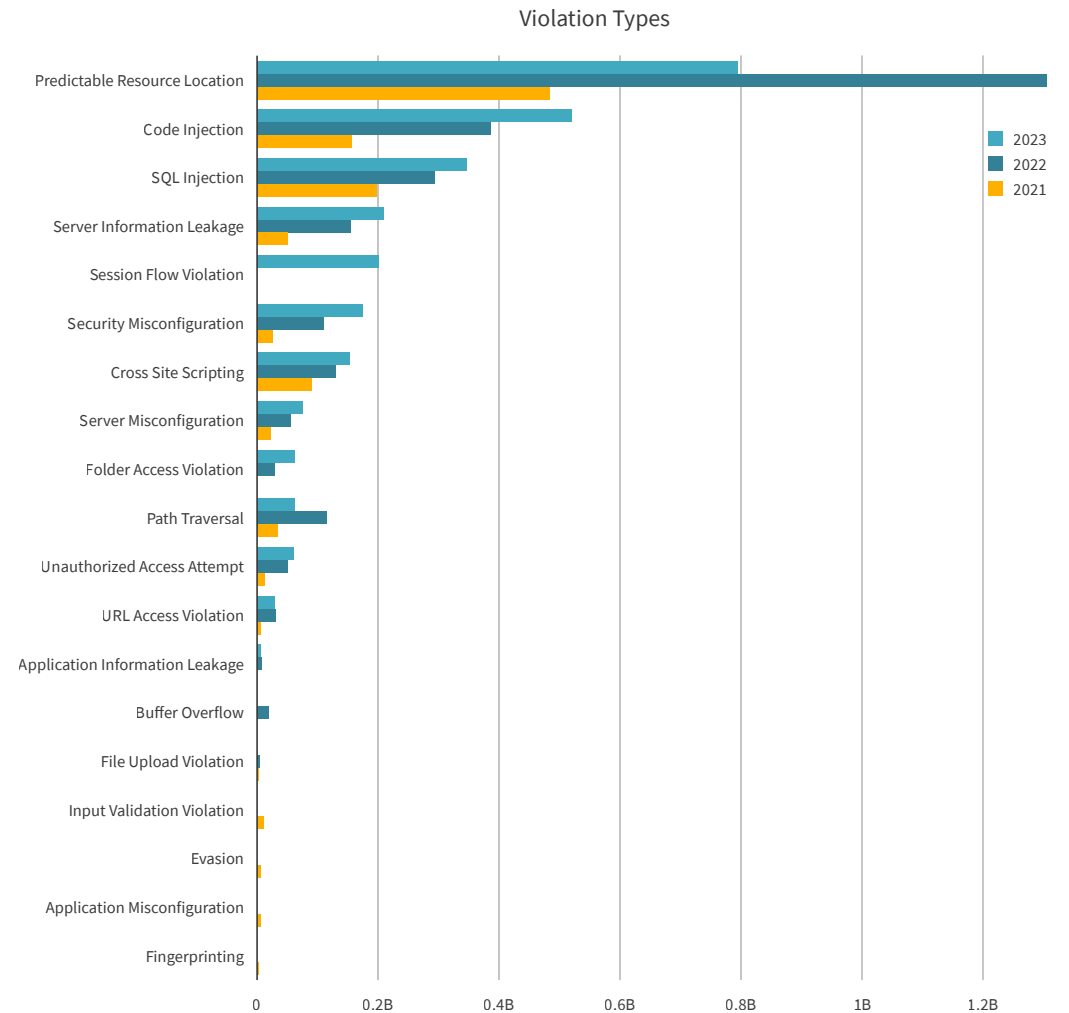Top web application security violations per type



Top Violation Types

**Figure 54:** Top web application security violations per type since 2021



Violation Types

## Attacked Industries

The most attacked industries in 2023, retail (36.7%) and transportation (18.6%), together account for more than half of all web application and API attacks. Software as a service (8.4%), carrier (8.1%), utility (4.4%), healthcare (4.2%), education (4%), ISP (3.5%), insurance (3.4%) and government (3%) represent the top 10 most attacked industries of 2023 in terms of web application and API attacks.

**Figure 55:**

Top industries attacked by web application and API attacks

Top Attacked Industries (normalized)
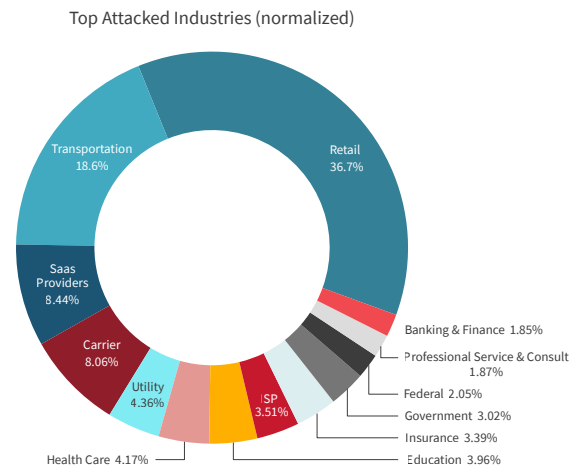
## Attacking Countries

Most blocked web security events originated from the United States (55.9%). The U.S. is—and historically has always been—the top country where most targeted and unsolicited attacks originate. Philippines, Germany, the United Kingdom and Italy completed the top five in 2023, not far ahead of Canada, France, Russia, India, the Netherlands and Australia.

It is important to note that the country where an attack originates does not necessarily correspond to the nationality of the threat actor or the origins of the threat. Often, the country where the attack originates will be the country that was targeted. Threat actors leverage anonymizing VPNs, dark net routers and compromised systems as jump hosts to perform attacks. The originating country of an attack will often be chosen based on the location of the target or the nation the threat actor wants to see attributed during false flag operations.

**Figure 56:**

Top countries from which web application and API attacks originated

Top Attacking Countries
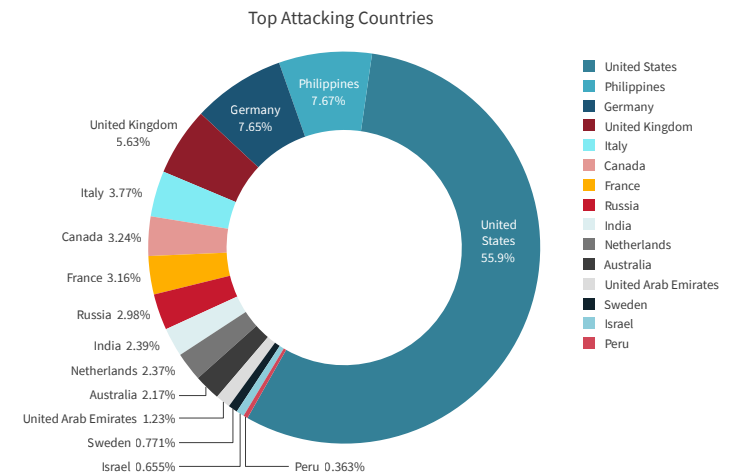
# Bad Bots

Bad bots are malicious programs that run automated tasks with malicious intent, including criminal activities such as fraud and theft. Fraudsters, unethical competitors and bad actors from various backgrounds and with differing motivations carry out a wide range of malicious activities and attacks by deploying malicious bots against websites, mobile apps and APIs.

Examples of bad bots are account takeover bots, which use stolen credentials to access users' online accounts; web content scraping bots, which copy and reuse website content without permission; social media bots, which spread fake news and propaganda on social media platforms; and scalping bots, which purchase services and products in bulk.

In contrast to bad bots, good bots are programs that run automated tasks which are beneficial for their target. Good bots can help improve the functionality and performance of websites, mobile apps and APIs. They also provide useful services and information to users. Examples of good bots are search engine bots, which crawl through web content and index the information for search engines; travel aggregator bots, which check and gather flight details and hotel room availabilities and pricing; and business intelligence bots, which analyze product reviews and social media comments to provide insights on brand perception.

Having a comprehensive bot management strategy is crucial for businesses to protect themselves from automated threats. A good bot management strategy can help detect and mitigate bad bots, protecting critical applications and APIs while ensuring a positive user experience for customers while allowing good bots to optimize the efficiency of the online business. An effective bot management product must have a strong detection layer that features several detection methods to analyze web traffic from different angles, differentiate legitimate from malicious traffic and detect potential threats like credential stuffing and inventory hoarding.
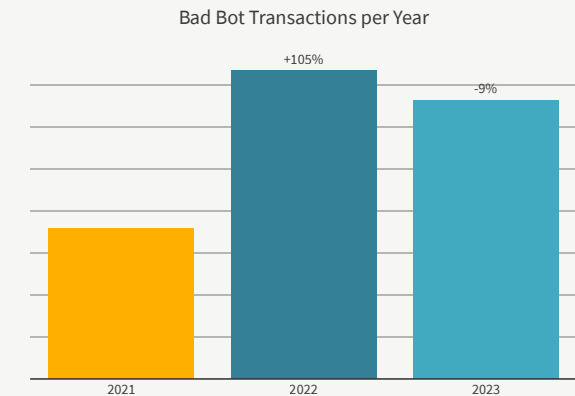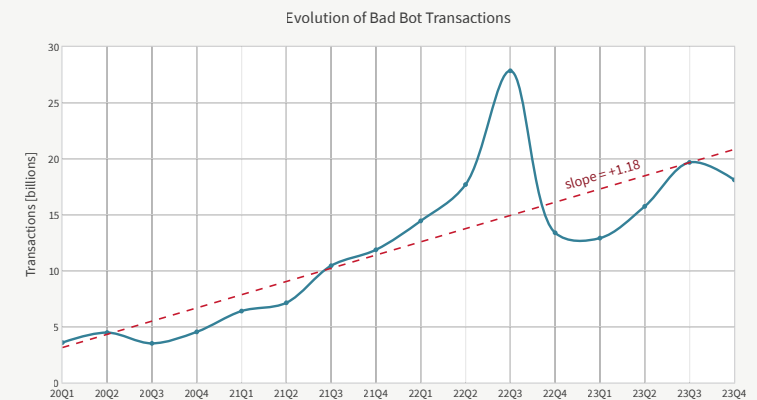
**Figure 57:**

Bad bot transactions per year


Bad Bot Transactions per Year

**Figure 58:**

Evolution over time of detected bad bot transactions


Evolution of Bad Bot Transactions

After a year of staggering growth in 2022, the number of bad bot transactions detected per year slightly regressed with a 9% drop in 2023 compared to 2022.

The number of detected bad bot transactions per quarter demonstrates a growing trend on a quarterly basis. Bad bots grow on average with 1.18 billion transactions per quarter, equivalent to an average of 393 million transactions per month or 12.9[11] million transactions per day.

The most targeted region in 2023 was North America, which observed a growing trend across the year starting at 54.8 million transactions per day and reaching almost 110 million transactions on average per day during the last quarter. The number of bad bot transactions in the EMEA region peaked at 37.2 million transactions per day in Q3. The CALA region started the year with almost 46 million transactions per day and observed a downward trend toward the end of the year, ending the last quarter of the year with an average of 27 million transactions per day. The APAC region started with 27.4 million transactions per day and peaked in Q3 with almost 50 million transactions per day.

The retail and entertainment industry saw their online applications increasingly assaulted by bad bots across the year. Media observed a reduction in the second quarter and then remained stable for the rest of the year. Banking applications were most attacked during Q2 while travel applications had the worst period of the year in Q3.

**Figure 59:** Evolution of bad bot transactions over time by region



Bad Bot Transactions by Region Over Time
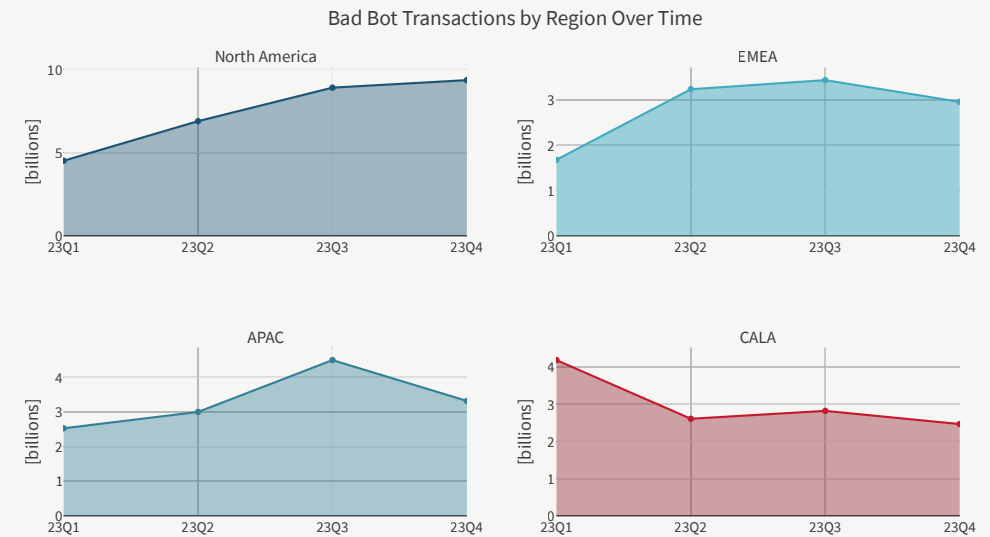
**Figure 60:** Evolution of bad bot transactions over time by vertical



Bad Bot Transactions by Vertical Over Time (normalized per vertical)

---

11.  The mean month-length in the Gregorian calendar is 30.436875
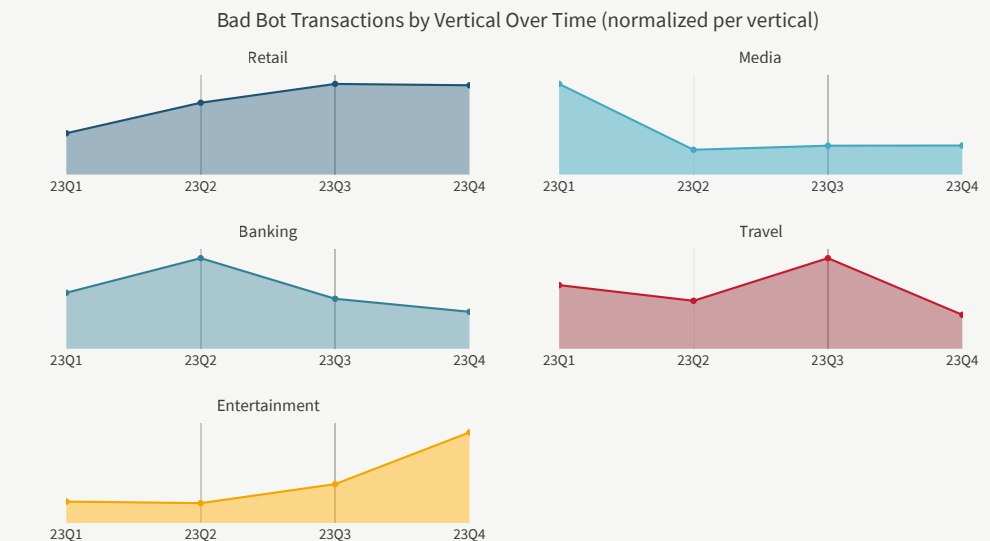
# Network Scanning and Exploit Activity in 2023

Not all network-level attacks that target internet-exposed assets are denial-of-service attacks. Network intrusion attacks consist of easy-to-execute exploits based on known vulnerabilities. These range from scanning using open source or commercial tools, information disclosure attempts for reconnaissance, and path traversal and buffer overflow exploitation attempts designed to render a system inoperable or provide access to sensitive information.

In 2023, 26.8% of the blocked events were denial-of-service attacks and 13.2% were network intrusion attempts. 60% of all blocked attacks were identified as known culprits in the Radware active attackers threat intelligence feed.

The ERT Active Attackers Feed (EAAF) includes devices caught in the Radware Global Deception Network (GDN) that were found to be actively scanning or randomly exploiting the internet. See Unsolicited Network Activity section (page 33) for more information on the GDN and the type of activity caught in our global honeypots.

Since intrusions and scans from active attackers do not generate large volumes, it will not be surprising that 99.9% of the total attack volume originated from DoS events.

The largest increase in the number of intrusions detected per year happened between 2021 and 2022. In 2023, we observed a moderate 16% increase in intrusion activity. The threat landscape has been very active since 2023, and this comes with high levels of widescale scanning and exploit attempts. We do not expect 2024 to be any different. We do anticipate the scanning and exploit activity to remain mostly stable,
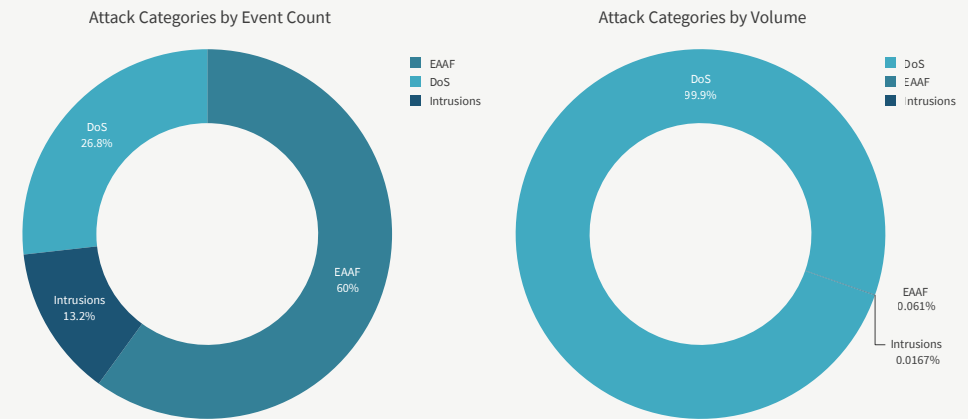
**Figure 61:** Network-level attack categories

Attack Categories by Event Count

- EAAF
- DoS
- Intrusions

DoS 26.8%
EAAF 60%
Intrusions 13.2%

Attack Categories by Volume

- DoS
- EAAF
- Intrusions

DoS 99.9%
EAAF 0.061%
Intrusions 0.0167%

**Figure 62:** Intrusions per Year

Intrusions per Year

2021, 2022 (+285%), 2023 (+16%)
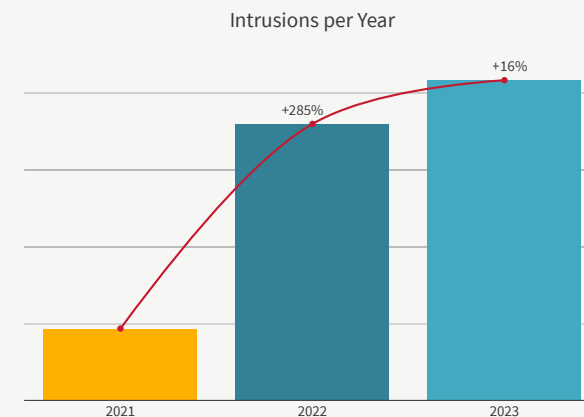
unless attackers find new ways of leveraging generative AI to further automate their scanning and exploiting, in which case the activity could see another significant increase.

DNS-named-version-attempt, an information disclosure exploit used by malicious actors to identify the version of the Bind named[12] DNS service, is leading the intrusion charts in 2023 by a huge margin. In 2022, the DNS server information disclosure merely took seventh place, down from fifth place in 2021 and second place in 2020. Referring back to Figure 45: DNS flood queries per month, one notices a relatively small but increased level of DNS flood attack activity in 2020 that slowed to barely noticeable levels from mid-2021 until the end of 2022. In the last months of 2022, the DNS flood activity started to become more noticeable and reached new heights in 2023.

Six of the top ten network intrusions in 2023 were known Log4j exploits. The December 2021 publicly disclosed Log4j vulnerability, dubbed Log4Shell, still attracts a large amount of attention across the attacker community. Log4Shell is a vulnerability in a commonly used Java logging library allowing an unauthenticated attacker to leverage publicly available exploit tools for remote command execution (RCE). Log4shell was the most critical vulnerability of 2021,

and by some considered to be the worst vulnerability of the decade. This past year demonstrates the long tail of the vulnerability and shows that threat actors are successful in leveraging more than zero-day attacks.

The second spot in the top 10 network intrusions is taken up by the ZMAP scanning tool. ZMap is a free and open-source security scanner that was developed as a faster alternative to Nmap. ZMap was designed for information security research and can be used for both white hat and black hat purposes. The tool is able to discover vulnerabilities and their impact and detect affected IoT devices.

SIP, the voice-over-IP (VoIP) Session Initiation Protocol, another fan favorite among services targeted by network-level DDoS attacks, took two spots in the network intrusion top 10. The sixth spot is taken by SIPSAK. Also known as the SIP Swiss Army Knife, SIPSAK is a SIP stress and diagnostics utility that is used by developers and administrators to run simple tests on SIP applications and devices. SIPVicious, on the other hand, is a set of open-source security tools used to audit SIP-based Voice-over-IP (VoIP) systems. It allows discovery of SIP servers, enumeration of SIP extensions, password brute-forcing and scanning for known vulnerabilities in SIP services. SIPVicious was the fourth most detected intrusion in 2020 and 2021 and started its decline in favor of other, more noisy exploits, with a sixth place in 2022 and a tenth spot in 2023.
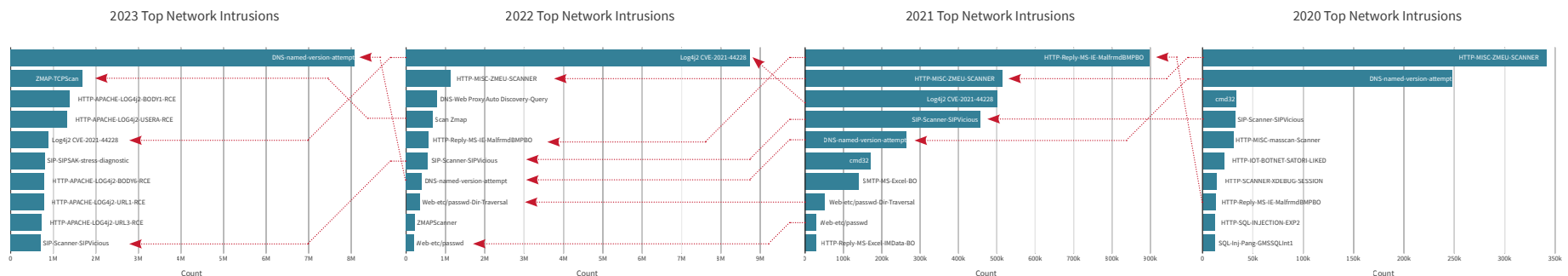
---

12. BIND is a suite of software for interacting with the Domain Name System. Its most prominent component, named, performs both of the main DNS server roles, acting as an authoritative name server for DNS zones and as a recursive resolver in the network (source: Wikipedia).

**Figure 63:**

Top network intrusions from 2020 until 2023

# Log4Shell: the Long Tail of a CVSS Score 10 Vulnerability

The December 9, 2021, the publicly disclosed Log4j vulnerability attracted plenty of attention across the security community. It occurred when a vulnerability in a commonly used Java logging library allowed unauthenticated attackers to leverage publicly available exploits for remote command execution (RCE).

Scanning and exploit activity was detected and blocked by the Radware Cloud WAF Service as early as December 9 at 6pm UTC, only hours after disclosure of the vulnerability. By December 10, scanning and exploit activity already reached several thousands of events per day.

Since its public disclosure, the exploit was detected and blocked more than 30 million times in the Radware Cloud. Looking at the activity over time, it appears that exploits became more frequent in the second half of 2023, albeit slightly. The Log4Shell vulnerability is a good reminder that threat actors are not only leveraging the most recent vulnerabilities but have also found success leveraging exploits for vulnerabilities that are several years old.

**Figure 64:** Daily blocked Log4Shell activity in Radware Cloud WAF and Cloud DDoS Services



Blocked Log4shell Exploits per Day (a total of 30,491,286 exploits blocked since dec 2021)
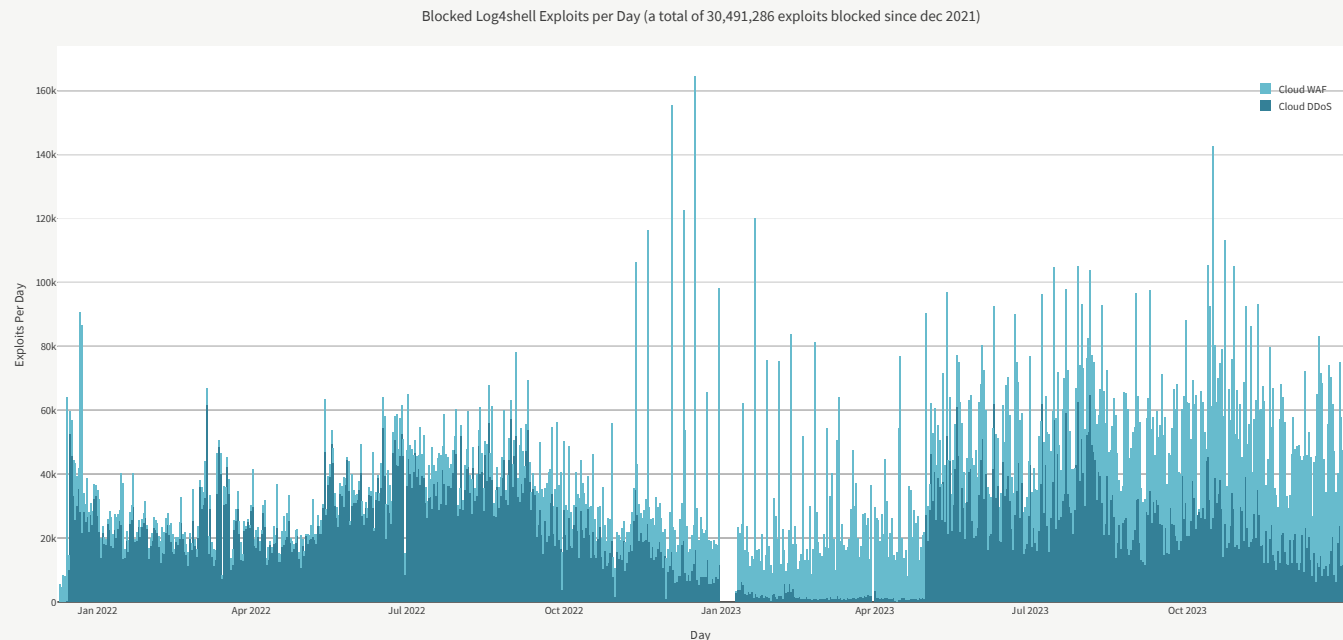
# Unsolicited Network Activity in 2023

The Radware Global Deception Network (GDN) consists of a network of globally distributed sensors that collect data on unsolicited traffic and attack attempts. Unsolicited events include DDoS backscatter and spoofed and non-spoofed scans and exploits.

The major difference between the GDN events discussed in this section and the web application and DDoS attack events in previous sections, is the unsolicited nature of the events. Web application and DDoS attack events were collected from real-world services accessible via the internet. In the latter case, attackers were targeting a particular organization or a specific application or service. By contrast, the unsolicited events recorded by the GDN are random acts. The scans or attacks were not targeting known services or a particular organization. The IP addresses of the sensors in the GDN are not published in DNS and do not provide accessible applications or services. No client, agent or device has a legitimate reason to reach a Radware GDN sensor.

The GDN collected a total of 4.4 billion unsolicited events in 2023. This represents a 65% increase compared to the 2.6 billion events collected in 2022.

The network collected an average of 12.1 million events per day in 2023, compared to 7.1 million events per day in 2022.

IP addresses provide a measure for the evolution of the number of malicious hosts and devices randomly scanning the internet and exploiting known vulnerabilities. In 2023, the deception network registered an average of 580,054 unique IPs per month, a slight increase compared to 2022 but less than in 2021.

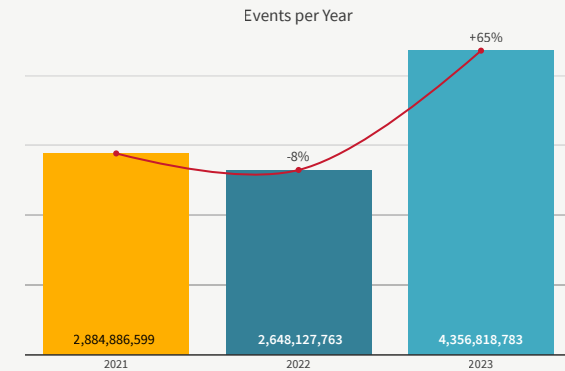**Figure 65:** Number of events per year recorded by the GDN


Events per Year

**Figure 66:** Number of events per month recorded by the GDN


Number of Events
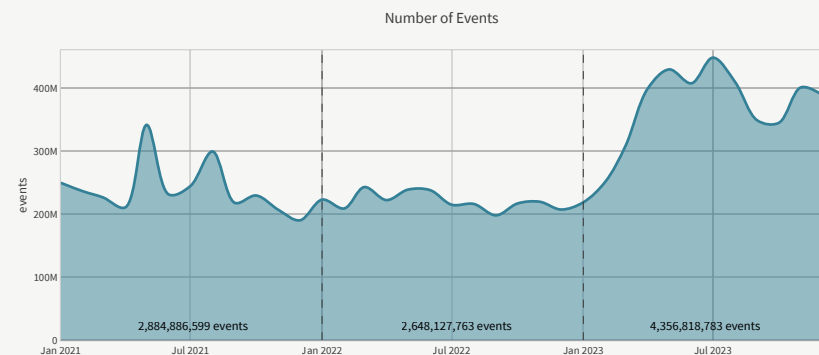
**Figure 67:** Number of unique IP addresses per month trying to exploit the GDN


Number of Unique IPs
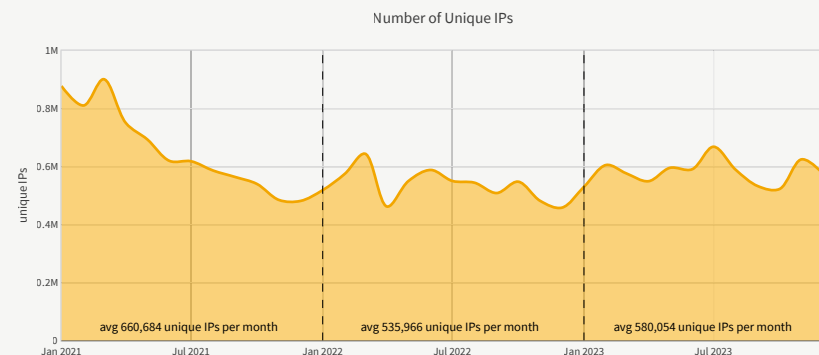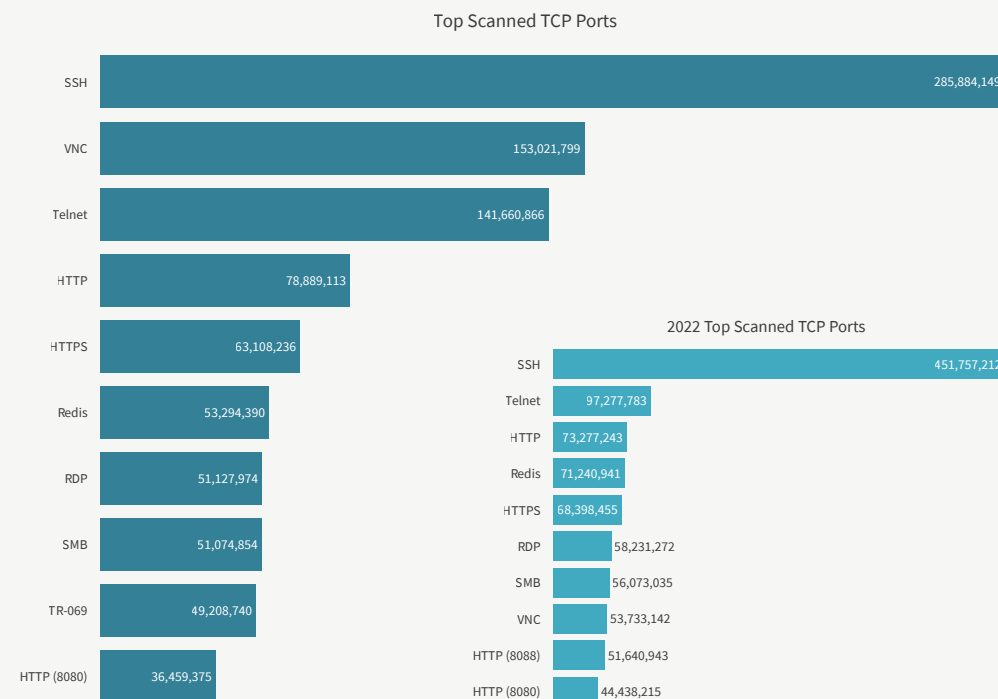
# Most Scanned and Attacked TCP Ports

The most attacked TCP service in 2023 was SSH on port 22, followed by VNC and Telnet. The top 10 was completed by HTTP, HTTPS, Redis, RDP, SMB, TR-069 (port 7547) and HTTP port 8080, a popular IP camera web UI port. TR-069 was a new entry in the top 10 for 2023 compared to 2022. Leaving the top 10 in 2023 was HTTP port 8088, another popular IP camera web UI port.

Virtual Network Computing (VNC) is a graphical desktop sharing system that uses the Remote Frame Buffer (RFB) protocol to remotely control another computer. It transmits the keyboard and mouse input from one computer to another, relaying the graphical screen updates over a network. In 2022, VNC took the eighth spot on the top 10 most scanned ports. This year VNC scans were even more prominent, moving VNC up to the second most scanned TCP port in 2023.

While Telnet was a favorite of the Mirai botnet for a long time, the number of access attempts on SSH surpassed Telnet by a good margin. SSH attacks are leveraged in account takeover and brute force attempts. Leveraging default or leaked credentials, attackers try to gain unauthorized access to devices and systems to move laterally across organizations' networks. This is used for abuse of cloud instances such as cryptomining. It can also be used as a jump host to anonymize targeted attacks, to plant cryptolocking malware during ransomware campaigns or to hijack a device's connectivity to perform DDoS attacks.

Redis (TCP port 6379) is an open source (BSD licensed) in-memory data structure store used as a database, cache and message broker. In March 2022, the Muhstik malware gang started actively targeting and exploiting a Lua sandbox escape vulnerability in Redis (CVE-2022-0543) after the release of a proof-of-concept exploit. In December 2022, a previously undocumented Golang-based malware, dubbed Redigo, targeted Redis servers to take control of systems with this vulnerability, most likely to

**Figure 68:** Top scanned and exploited TCP ports

Top Scanned TCP Ports

| Port | Value |
|---|---|
| SSH | 285,884,149 |
| VNC | 153,021,799 |
| Telnet | 141,660,866 |
| HTTP | 78,889,113 |
| HTTPS | 63,108,236 |
| Redis | 53,294,390 |
| RDP | 51,127,974 |
| SMB | 51,074,854 |
| TR-069 | 49,208,740 |
| HTTP (8080) | 36,459,375 |

2022 Top Scanned TCP Ports

| Port | Value |
|---|---|
| SSH | 451,757,212 |
| Telnet | 97,277,783 |
| HTTP | 73,277,243 |
| Redis | 71,240,941 |
| HTTPS | 68,398,455 |
| RDP | 58,231,272 |
| SMB | 56,073,035 |
| VNC | 53,733,142 |
| HTTP (8088) | 51,640,943 |
| HTTP (8080) | 44,438,215 |

build a botnet. The malware mimicked the Redis protocol to communicate with its command and control (C2) infrastructure. In 2022, Redis took fourth place, between HTTP and HTTPS. In 2023, both HTTP and HTTPS surpassed Redis, dropping it down to sixth place.

Remote Desktop Protocol (RDP) was eclipsed by VNC in the top 10 and moved down from sixth place in 2022 to seventh place in 2023. RDP is a proprietary protocol developed by Microsoft which provides users with a graphical interface to connect to other computers over a network connection. RDP is still a regularly exposed remote access protocol in remote locations used by industrial control systems (ICS) and became more exposed as people worked from home during the pandemic. RDP is one of the favorite initial attack vectors leveraged by initial access brokers (IAB), who purchase and exploit leaked accounts from underground forums to install cryptolocking ransom malware.

Server Message Block (SMB) is a popular file and printer sharing protocol leveraged by Microsoft in Windows and many Linux implementations through Samba or the more recent ksmbd kernel service. In December 2022, a critical vulnerability with a Common Vulnerability Scoring System (CVSS) score of 10 was disclosed that could enable remote attackers to execute arbitrary code on Linux servers exposing the SMB protocol on Linux servers with ksmbd enabled. SMB dropped from seventh place in 2022 to eighth place in the top ten for 2023.

Technical Report 069 (TR-069) is a technical specification of the Broadband Forum that defines an application-layer protocol for the remote management and provisioning of customer premises equipment (CPE) connected to an IP network. TR-069 uses the CPE WAN Management Protocol (CWMP), which provides support functions for auto-configuration, software or firmware image management, software module management, status and performance management and diagnostics. The CPE WAN Management Protocol is a bidirectional SOAP- and HTTP-based protocol, which provides communication between a CPE and Automatic Configuration Servers (ACS). The protocol addresses the growing number of different internet access devices such as modems, routers and gateways as well as end user devices such as set-top boxes and VoIP phones. TR-069 was one of the most targeted IoT protocols back in 2016 when Daniel Kaye, also known as "BestBuy" and "Spiderman", adapted Mirai to exploit vulnerabilities in routers exposing TR-069 on their WAN interfaces.

# Most Scanned and Attacked UDP Ports

Most of the scanned and exploited UDP ports during 2023 were similar to the top scanned UDP ports in 2022 (see Figure 69). The exceptions were LDAP, NetBIOS and CoAP which left the top 10 in favor of UDP port 80, IPSec (IKE) and Bittorrent P2P.
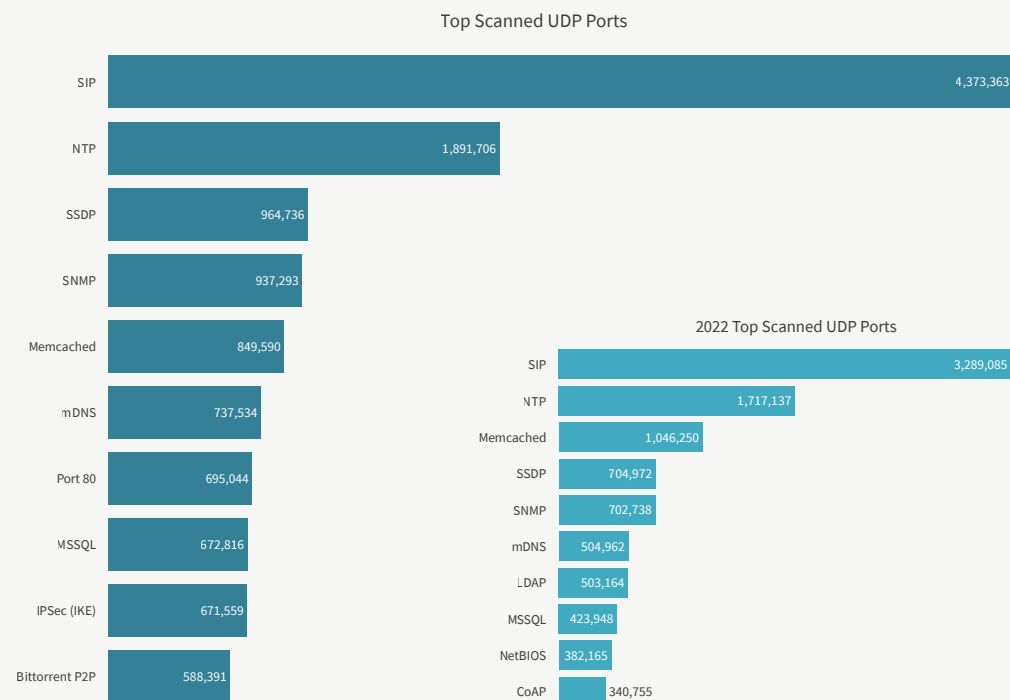
SIP (UDP port 5060) was again the most targeted UDP-based service in 2023. Port 5060 is used by many SIP-based VoIP phones and providers. VoIP remains critical to organizations and for this reason it also made the charts as one of the most targeted services for DDoS attacks in 2021. Vulnerabilities and weak or default passwords in VoIP services allow attackers to abuse them for initial access, spying and moving laterally inside organizations' networks.

NTP (UDP port 123), SNMP (UDP port 161), SSDP/UPnP (UDP port 1900), Memcached (UDP port 11211) and mDNS (UDP port 5353), are among the most abused protocols for DDoS amplification attacks. Many black hat and white hat actors are continuously scanning and cataloging the internet's addressable range to abuse for DDoS attacks (black hat) or assess the risk in the DDoS threat landscape (white hat).

MSSQL (UDP port 1434) is used by the Microsoft SQL Server database management system monitor. It is abused through remote code execution vulnerabilities and is known for the W32.Spybot.Worm that spread through MSSQL Server 2000 and MSDE 2000 from the early 2000s onwards. It remained a very solicited port in 2021, 2022 and 2023.

IKE (UDP port 500) is the protocol used to set up a security association (SA) in the IPsec VPN protocol suite. In the first half of 2023, OpenVPN (UDP port 1194) was in the top 10 top scanned UDP ports and is now replaced by the similar but competing VPN protocol IPSec.

**Figure 69:** Top scanned and exploited UDP ports



Top Scanned UDP Ports

| Port | Count |
|---|---|
| SIP | 4,373,363 |
| NTP | 1,891,706 |
| SSDP | 964,736 |
| SNMP | 937,293 |
| Memcached | 849,590 |
| mDNS | 737,534 |
| Port 80 | 695,044 |
| MSSQL | 672,816 |
| IPSec (IKE) | 671,559 |
| Bittorrent P2P | 588,391 |

2022 Top Scanned UDP Ports

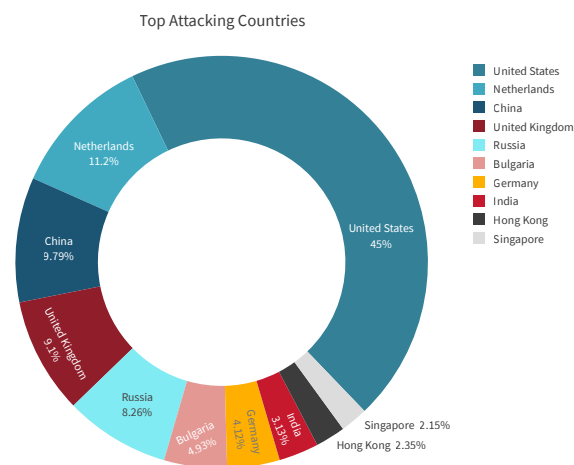| Port | Count |
|---|---|
| SIP | 3,289,085 |
| NTP | 1,717,137 |
| Memcached | 1,046,250 |
| SSDP | 704,972 |
| SNMP | 702,738 |
| mDNS | 504,962 |
| LDAP | 503,164 |
| MSSQL | 423,948 |
| NetBIOS | 382,165 |
| CoAP | 340,755 |

# Attacking Countries

The United States was the country from which the most unsolicited network activity originated during 2023. The United States was also the number one in 2022 with 42.5% of all activity and remained so with 45% of the activity in 2023. The Netherlands moved from fourth spot in 2022 to second place in 2023 with 11.2%. China remained in the third spot in 2023 while the United Kingdom traded places with Russia. That said, as discussed earlier, the origin of an attack often does not align with the home country of the attacker and can be spoofed to impersonate a different country. If there is one thing to learn about the attacking country, it is that it is most often not the origin country of the threat actor.

The origin of an attack often does not align with the home country of the attacker and can be spoofed to impersonate a different country. **If there is one thing to learn about the attacking country, it is that it is most often not the origin country of the threat actor**

**Figure 70:** Top attacking countries



Top Attacking Countries

- United States 45%
- Netherlands 11.2%
- China 9.79%
- United Kingdom 9.1%
- Russia 8.26%
- Bulgaria 4.93%
- Germany 4.12%
- India 3.13%
- Hong Kong 2.35%
- Singapore 2.15%

# Web Service Exploits

The top attacked HTTP Uniform Resource Identifiers (URI) were led by "/", the universal URI for testing the presence of a web service and collecting information from header fields in server responses. There is a significant difference in the top targeted URIs for unsolicited events compared to the top targets in web application attacks where services are supporting real applications. This section covers unsolicited events, meaning there is no real application or service running on the targeted server and the IP address of the targeted server is not published in DNS or referred by any services on the internet. The top URIs should be interpreted as the top services and applications targeted by actors that are randomly scanning and exploiting the full internet range of IP addresses. Typically, a URI will conform with a known and disclosed vulnerability.

The following table lists the most important and known vulnerabilities based on the most scanned URIs:

### /.env

A predictable resource location access exploit attempting to find configuration information of the service in the hidden file ".env". Moved from a fourth spot in 2022 to second place in 2023.

### /ctrlt/DeviceUpgrade_1

Huawei HG532 routers Remote Code Execution vulnerability, CVE-2017-17215. Moved from tenth place in 2022 to third place in 2023.

### /ws/v1/cluster/app/new-application

A known vulnerability used to exploit Hadoop YARN services and schedule arbitrary workloads on Hadoop clusters. An exploit abused by many cryptojacking campaigns that try to illegitimately leverage the cloud instances of enterprises and research institutions since 2018. This was the second most exploited URI in 2022 and moved to third place in 2023.

### /v1.16/version

Used by threat actors to identify the available Docker API version by invoking a command for an old version. Used by cryptocurrency miners for abusing containers through the Docker API. This was in seventh place in 2022 but moved to fifth place in 2023.

### /nice%20ports%2C/Tri%6Eity.txt%2ebak

Request for "/nice ports,/Trinity.txt.bak" is used by Nmap's service detection routine to test how a server handles escape characters within a URI. This was in ninth place in 2022 and moved to sixth place in 2023.

**Figure 71:** Top Scanned URIs

Top URI

```
/
                                                          42,483,885
/.env
        2,340,583
/ctrlt/DeviceUpgrade_1
      1,285,118
/ws/v1/cluster/apps/new-application
     1,104,519
/v1.16/version
    858,991
/nice%20ports%2C/Tri%6Eity.txt%2ebak
   840,934
google.com:443
  710,192
/?q=ultrasurf
  695,917
*
  694,183
/Core/Skin/Login.aspx
  659,606
```
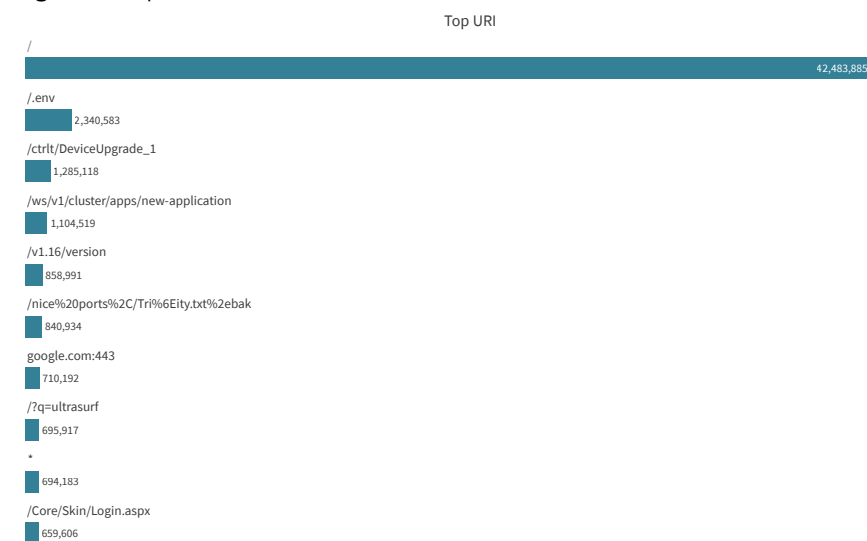
### /?q=ultrasurf

UltraSurf is a freeware internet censorship circumvention product created by UltraReach Internet Corporation. The software bypasses internet censorship and firewalls using an HTTP proxy server, employing encryption to ensure privacy. The software works by creating an encrypted HTTP tunnel between the user's computer and a central pool of proxy servers, enabling users to bypass firewalls and censorship. UltraReach hosts all of its own servers. The software makes use of sophisticated proprietary anti-blocking technology to overcome filtering and censorship online. The tool was originally designed for internet users in mainland China, where the internet is heavily censored and internet activities are monitored. With the advent of Ultrasurf and other circumvention tools, these internet users are provided a lifeline to access and share information freely. After nearly two decades of development, the technology has proven extremely resilient and adaptable in the face of increasingly advanced censorship techniques and aggressive blocking. Its success in helping internet users in China to surf the web in freedom has attracted the attention of internet users beyond China's borders. Today, Ultrareach has millions of users from over 180 countries. We assume that "/q=ultrasurf" is leveraged in attempts to identify the locations and addresses of Ultrareach proxies. Ultrasurf is a new entry in the top scanned URI list.

### /Core/Skin/Login.aspx

We are unsure about the application that is being targeted by this URI. The "/core" and "Login.aspx" makes us assume applications that are running on top of the Microsoft ASP.Net Core framework, a cross-platform, open-source framework for building web apps and services with .NET and C#. A new entry in the top scanned URI list.
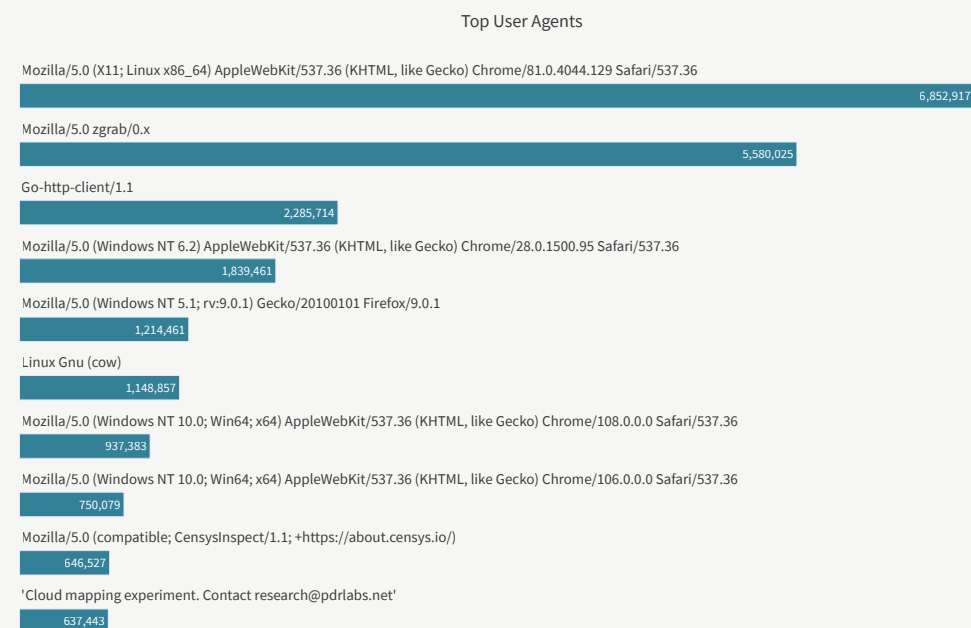
# Top User Agents

In the HTTP protocol, the user-agent string is used for content negotiation, where the origin server selects suitable content or operating parameters for the response. For example, the user-agent string might be used by a web server to choose variants of its response based on the known capabilities of a particular version of client software, and to differentiate its interface for smartphones or desktop browsers. The concept of content tailoring is built into the HTTP standard in RFC1945.

As such, the user-agent field in a web request can be used to identify the client agent that makes the request. Some malicious actors are aware of this identifying feature being used to score the legitimacy of a web request by web security modules. This causes them to mask their malicious nature by randomly generating and changing the user-agent to known legitimate values.

Commercial and open-source web service vulnerability scanning tools and programming language implementations can be identified through their user agent. For example, zgrab is the application-layer network scanning component of the Zmap open-source scanning tool and "Go-http-client" is the default user agent header when using the Golang net/http package.

Security researchers may also leverage the user agent to identify themselves through white hat scanning and some bug bounty hunters leverage it to leave a fingerprint and claim their discovery based on their ethical scans.

**Figure 72:** Top user agents

Top User Agents

Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.129 Safari/537.36
6,852,917

Mozilla/5.0 zgrab/0.x
5,580,025

Go-http-client/1.1
2,285,714

Mozilla/5.0 (Windows NT 6.2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1500.95 Safari/537.36
1,839,461

Mozilla/5.0 (Windows NT 5.1; rv:9.0.1) Gecko/20100101 Firefox/9.0.1
1,214,461

Linux Gnu (cow)
1,148,857

Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
937,383

Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 Safari/537.36
750,079

Mozilla/5.0 (compatible; CensysInspect/1.1; +https://about.censys.io/)
646,527

'Cloud mapping experiment. Contact research@pdrlabs.net'
637,443

# Top Account Takeover Credentials

Not all web service vulnerabilities can be exploited without authentication. Some web services embed widely used defaults and some even have hardcoded secrets to protect access from unauthorized users or devices. Typically, weak passwords are combined in credential pairs such as "admin:admin," "admin:password," "admin:1234567890" or just no password "admin:." These weak password permutations make up nine of the top 10 credentials. The exact same nine that were in the top 10 in 2022, only in a slightly different order. These are, and for good reason, universally agreed to be the worst credentials and are abused the most because they provide access to devices that have not had their default credentials changed during deployment.

The credential "report:8Jg0SR8K50" is a hard coded user and password in digital video recorders (DVRs) from vendor LILIN and was publicly disclosed in March 2020, together with the credential "root:icatch99." These flaws were found to be abused widely and spread at least three botnets, namely Chalubo, FBot, and Moobot. DVRs are ubiquitous in the IoT landscape and are still a favorite target for IoT botnets, as are the security cameras that feed them.

The top usernames used during SSH authentication give an indication of the services most vulnerable to brute forcing. Amongst the top 10 are "postgres," "oracle," "ftpuser," "git" and "pi" (Raspberry Pi default username). "ubnt," the Ubuntu Linux default username in tenth place in 2022, was replaced by "guest."

**Figure 73:** Top HTTP ATO credentials
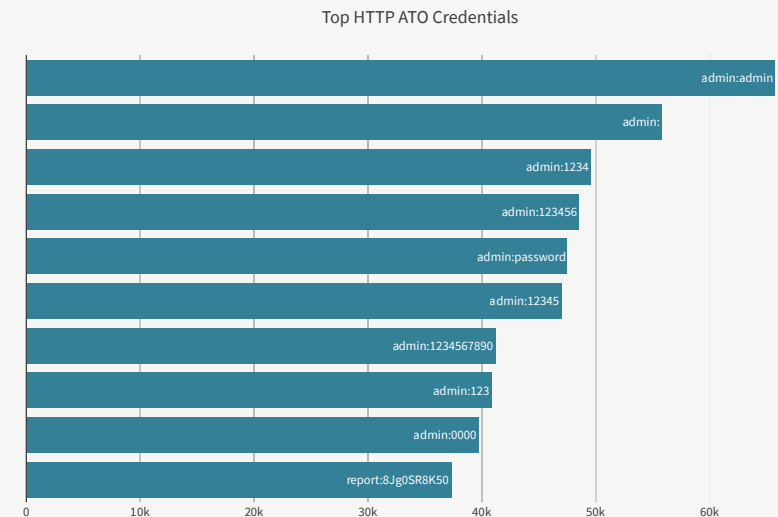


**Figure 74:** Top SSH ATO usernames
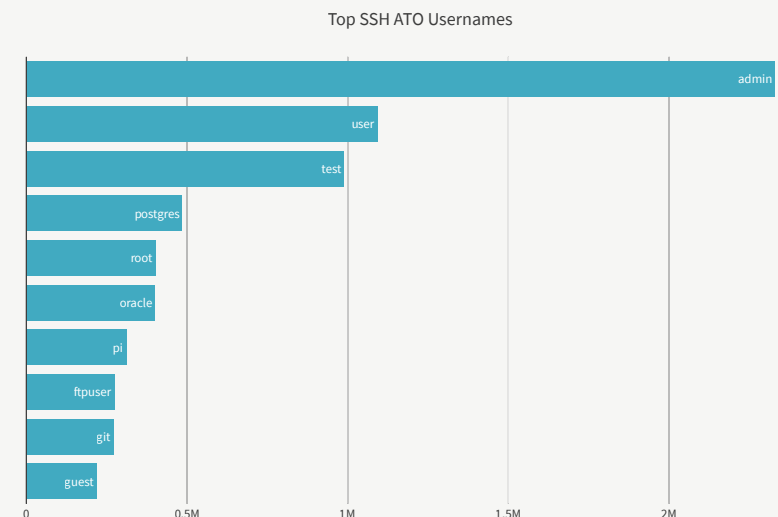
# Hacktivist Attack Activity in 2023

Hacktivism is a complex phenomenon that can be motivated by various factors, including religious and political beliefs. While hacktivists may have different motivations and methods, they all share a desire to use technology to advance their cause and to challenge those they believe are acting against it.

Hacktivists use a variety of tactics to achieve their goals, and the specific tactics they use depend on their motivations and the resources they have at their disposal. Their methods are constantly evolving as new technologies and platforms emerge. While some tactics may be illegal or unethical, hacktivists argue that they use their skills to promote social or political change and hold powerful organizations and governments accountable for their actions.

Some common tactics used by hacktivists include DoS attacks, website defacements, data breaches and media publicity campaigns.

## Telegram

Shortly after the start of the invasion of Ukraine, the vice prime minister of Ukraine, Mykhailo Fedorov, announced the creation of a volunteer cyber army to fight Russian propaganda and protect the interests of Ukraine in cyberspace. The IT Army of Ukraine mainly coordinates its efforts via Telegram and Twitter. The IT Army of Ukraine Telegram channel gathered over 175 thousand members in a little over a year. It became one of Telegram's largest active hacker channels.

Telegram has taken a pivotal role in the ongoing conflict between Russia and Ukraine and inspired many other groups, hacktivist and other, to make a move for the platform. Telegram provides private and public channels and a standardized platform that allows forwarding and sharing of messages between channels. Telegram provides an easy means to create large follower groups and keep up to date with the latest security and hacking news.

Following these early adopters, more established groups followed the example of the freshly established hacker groups. DragonForce Malaysia, one of the most active hacktivist groups that has been around for many years, moved part of their activity from their private member forum to a Telegram channel. By the end

While some tactics may be illegal or unethical, hacktivists argue that they use their skills to **promote social or political change and hold powerful organizations and governments accountable for their actions**

of 2023, DragonForce Malaysia surpassed all hacktivist channels to become the largest hacktivist channel we are following in terms of member count.

Telegram also provides an open bot API that allows anyone to create bots hosted in the telegram platform. Bots are Telegram accounts operated by software, not people, and can do anything, from chat bots to integration with other services outside of the telegram platform.

Some DDoS-for-hire services leverage Telegram as the new end-user UI, guiding subscribers to a Telegram bot that allows them to perform real-time commands and schedule DDoS attacks while getting status information through the same Telegram channel.

Telegram, with all its freedom and openness, is quickly becoming the new "underground," though it is above ground and public compared to the underground forums deeply buried in the dark web.

**Figure 75:** Top Telegram channels by member count



Top 20 Telegram Channels by Member Count

| Channel | Members |
|---|---|
| Mash | 2,153k |
| DragonForce Malaysia | 254k |
| Joker DPR | 242k |
| IT ARMY of Ukraine | 154k |
| Beregini | 104k |
| We are Killnet | 94k |
| NoName057(16) | 58k |
| stand4muslim | 53k |
| Anonymous OpIran | 44k |
| Anonymous Sudan | 40k |
| ANONYMOUS - SCHWEIZ | 38k |
| XakNet Team (ru) | 30k |
| Killnet mirror | 29k |
| Peoples Cyber Army | 27k |
| Termux Israel | 26k |
| ZulikGroup | 25k |
| KillMilk | 22k |
| DDosia Project | 16k |
| HackYourMom | 16k |
| UserSec | 15k |

# Telegram DDoS Attack Claims

Hacktivist groups post their DDoS attack claims on Telegram and include some sort of proof of the legitimacy of the attack by providing a snapshot of the availability of the website through a check-host link. Check-host links allow us to verify the claimed target and the date and time of the attack. By gathering only the messages with check-host links, we are able to monitor claimed attacks on Telegram with a higher degree of certitude. That said, check-host links are not foolproof. For example, we have observed a few instances where the checked host was "radware. com:666." Because there is no service listening on port 666 of radware. com, the check-host report will return unavailable. The report, in this case, does not indicate a successful DDoS attack.

Attack claims posted on Telegram also frequently get forwarded to other channels. To ensure we count unique attack claims and not the number of reposts or forwards, we only count the message of the original post in our hacktivist reports. Figure 77 provides the total number of DDoS attack claims and also the number of unique claims per month across all monitored Telegram channels. The total claims include not only the original claim but also all forwarded and reposted claims. The unique claims number in the chart only takes into account original claims.

In the first half of 2023, threat actors claimed 5,606 attacks on Telegram. During the second half, this number increased by 24% to 6,971 claimed DDoS attacks. Some of the more noticeable actors became less prominent in the second half, but the overall trend of hacktivist-driven DDoS activity increased in the second half and reached a record level of 2,034 original claims in October 2023, a record that can be attributed to the global hacktivist activity following the conflict between Israel and Hamas.

**Figure 76:**

Example DDoS attack claims on Telegram
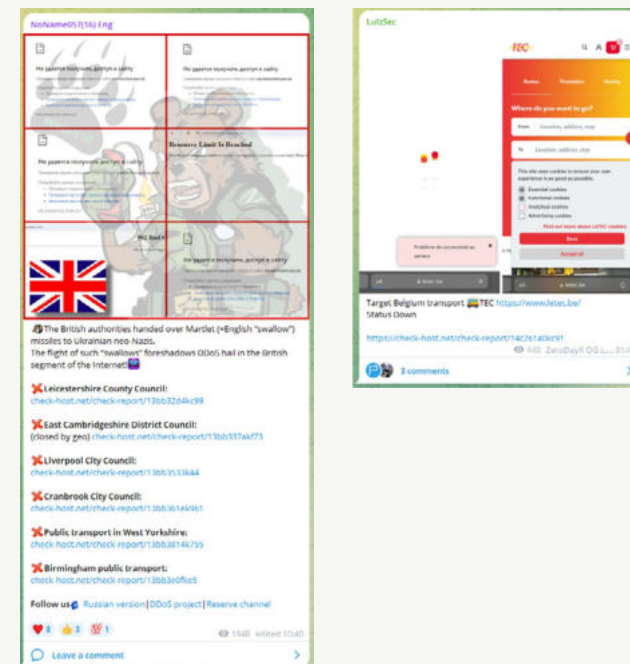


**Figure 77:** DDoS attacks claimed per month on Telegram



Claimed DDoS Attacks per Month
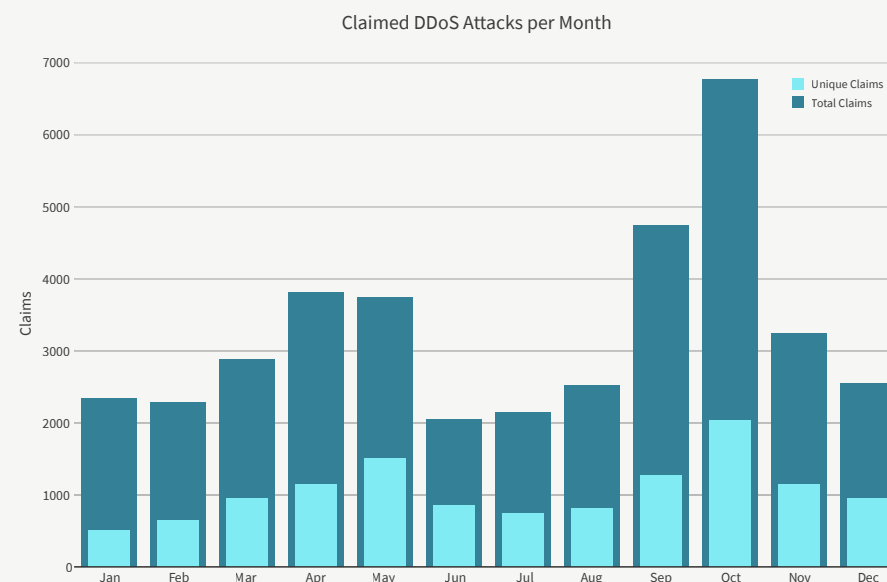
# Most Targeted Countries

While most of the claimed DDoS attacks targeted India in the first half of 2023, Israel gained more attention from the hacktivist community after the ongoing conflict with Hamas started on October 7, 2023. By consequence, in 2023, Israel was the most targeted country for hacktivist activity in the world with 1,480 claimed DDoS attacks, followed closely by India and the United States. Further down the list, Ukraine and Poland close out the top five with 731 and 580 claimed attacks, respectively, targeting the countries.

**Figure 78:** Countries with most DDoS attacks claimed on Telegram

Number of Attacks Claimed Per Country (100 attacks or more)

| Country | Attacks |
| --- | --- |
| Israel | 1480 |
| India | 1242 |
| United States | 1164 |
| Ukraine | 731 |
| Poland | 580 |
| Germany | 492 |
| Indonesia | 448 |
| Czech Republic | 429 |
| Sweden | 405 |
| Italy | 320 |
| France | 317 |
| Lithuania | 295 |
| Pakistan | 285 |
| Netherlands | 283 |
| United Kingdom | 261 |
| Russia | 240 |
| Spain | 203 |
| Finland | 191 |
| Denmark | 175 |
| Australia | 167 |
| Canada | 163 |
| Estonia | 163 |
| Senegal | 157 |
| Latvia | 151 |
| United Arab Emirates | 120 |
| Belgium | 102 |

# Top Claiming Actors

With 3,391 claimed DDoS attacks, NoName057(16) was by far the most active hacker group on Telegram in 2023. Executor DDoS v2, a DDoS-for-hire that performs DDoS attacks for a living (literally), was in second place with less than one fourth of the claimed DDoS attacks by NoName057(16). Hacktivist groups Mysterious Team, Anonymous Sudan, Team Insane Pakistan and the Cyber Army of Russia completed the top five most active hacktivists on Telegram in 2023. Just behind the top five hacktivists comes the second most active DDoS-for-hire service, SPYEYE BOTNET.

Throughout 2023, we observed a significant growth in DDoS-for-hire services on Telegram. A good portion of these new services are Russian speaking. One of the potential explanations behind this growth are hacktivists getting more experienced while also getting tired of supporting their community when they could leverage their new skills for more lucrative activities, such as renting access to their DDoS tools and botnets.

The most targeted web category, globally, was government with 2,694 claimed attacks. Business and economy and travel websites were second and third, respectively, with notably less attacks. Financial services, educational institutions and news and media websites close the top six web categories with 500 claimed attacks or more in 2023.

**Figure 79:** DDoS attacks claimed per actor



Number of Attacks Claimed per Actor (100 attacks or more)
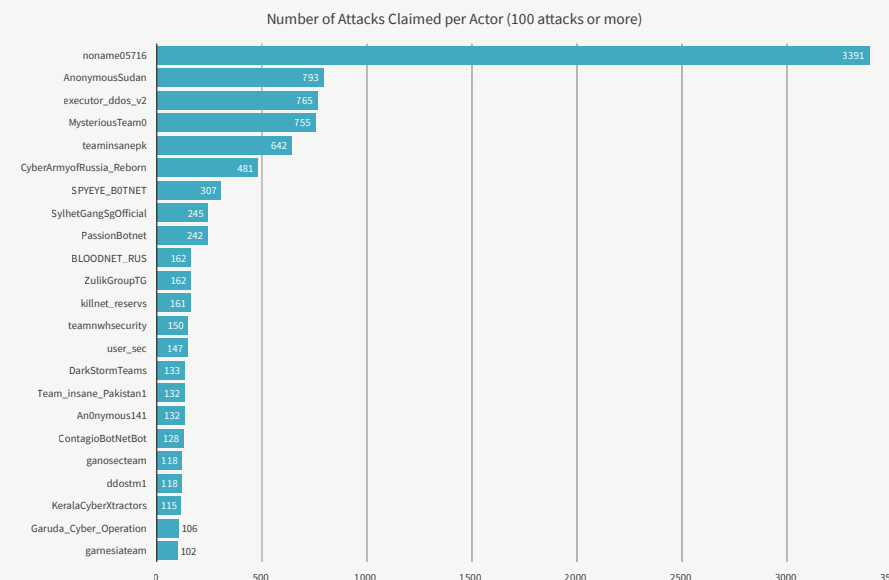
**Figure 80:** DDoS attacks claimed per web category



Number of Attacks Claimed per Web Category (50 attacks or more)
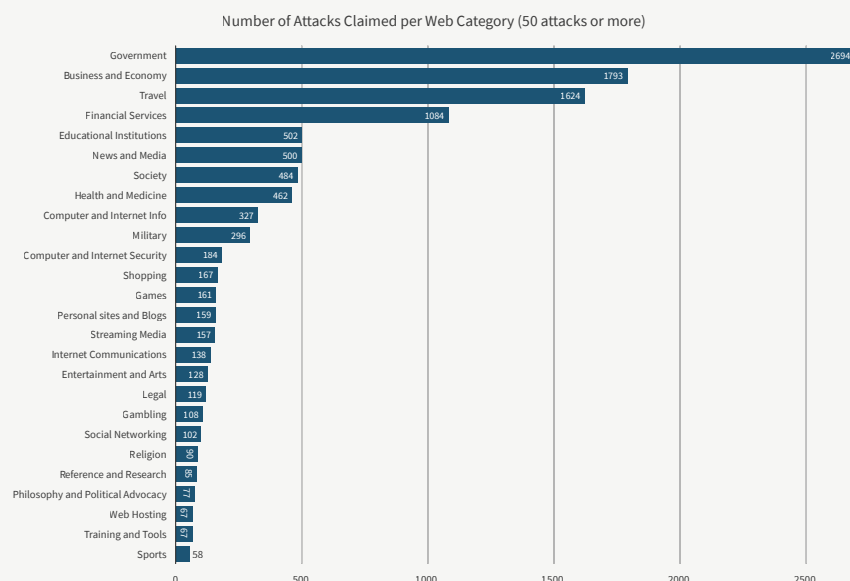
# Notable Hacktivists

We tracked over 230 channels in 2023, and while all deserve our attention, we can only cover a few of the most iconic or most active hacktivists in this report. We do provide a link where you can consult all interactive versions of the charts for every channel and every country that we are tracking. Please see the sidebar entitled "Radware Link" for more information and the link to access the report.

## Radware Link

Interactive versions of the hacktivist reports are regularly published in the Radware Link Community..

Subscribe to get notifications whenever an update becomes available. View the publicly available 2023 interactive report.

## NoName057(16): Pro-Russian Patriotic Hacktivist

NoName057(16) is probably the most organized and disciplined pro-Russian hacktivist group on the global threat scene. NoName057(16) was observed attacking multiple targets and sometimes multiple countries every day of 2023. They posted proof and claimed attacks without faulting any day of the year, providing background and motivation for their attacks. Attack campaigns by NoName057(16) are driven by geopolitical events that threaten or negatively impact the reputation of their home country.

NoName057(16) provides a custom-developed DDosia bot that enables their channel subscribers to become a part of the crowdsourced botnet. Members of Project DDosia only have to run the bot on their Windows, Unix, Mac or Android devices to support the cause of NoName057(16). To incentivize their members, NoName057(16) rewards their top DDosia attackers with crypto payouts.

The number of subscribers to NoName's Telegram channel has been steadily growing since May 2023 with an average of 80.3 new subscribers per day.

**Figure 81:** NoName057(16) Telegram subscriber count evolution



Telegram Subscribers: NoName057(16)
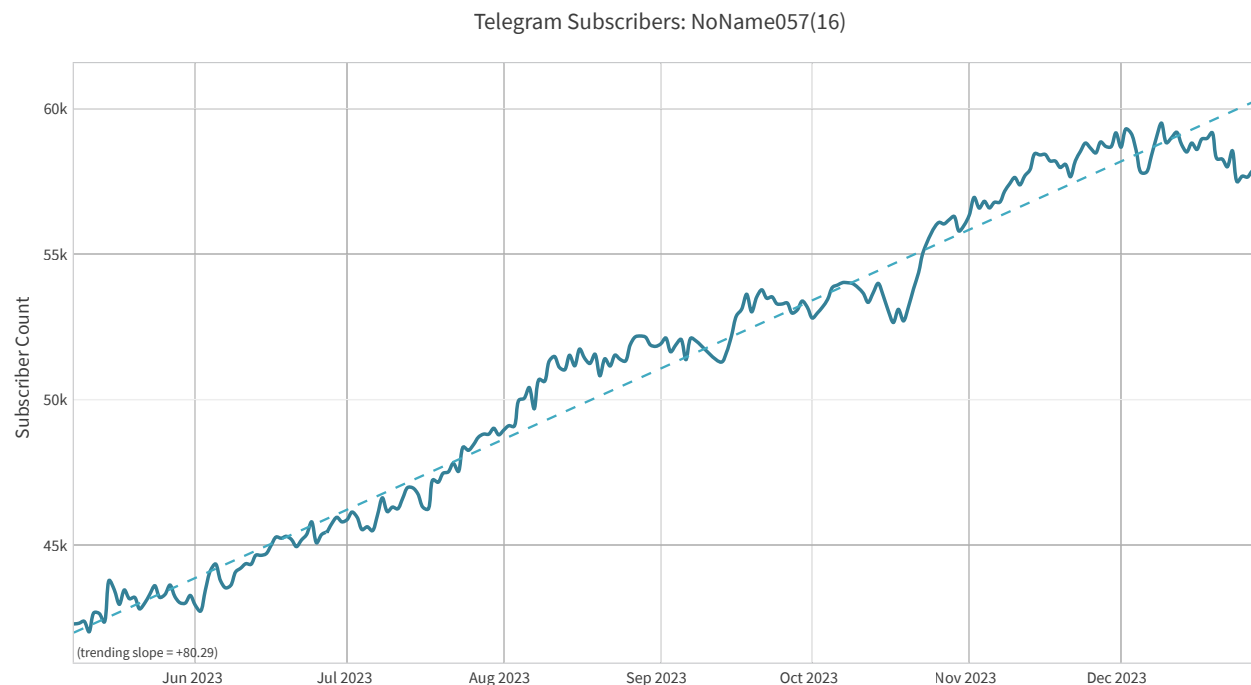
The Czech Republic was targeted the most by NoName057(16), accounting for 395 attacks in 2023. Czech Republic is closely followed by Poland with 353 attacks by NoName057(16). Lithuania, Germany and Italy completed the top five most targeted countries by NoName057(16).

NoName057(16) primarily targeted government websites (25.3%), travel websites (23.8%), business websites (19.2%) and websites providing financial services (12.5%).

**Figure 82:** NoName057(16)-claimed DDoS attacks



NoName05716-claimed Attacks
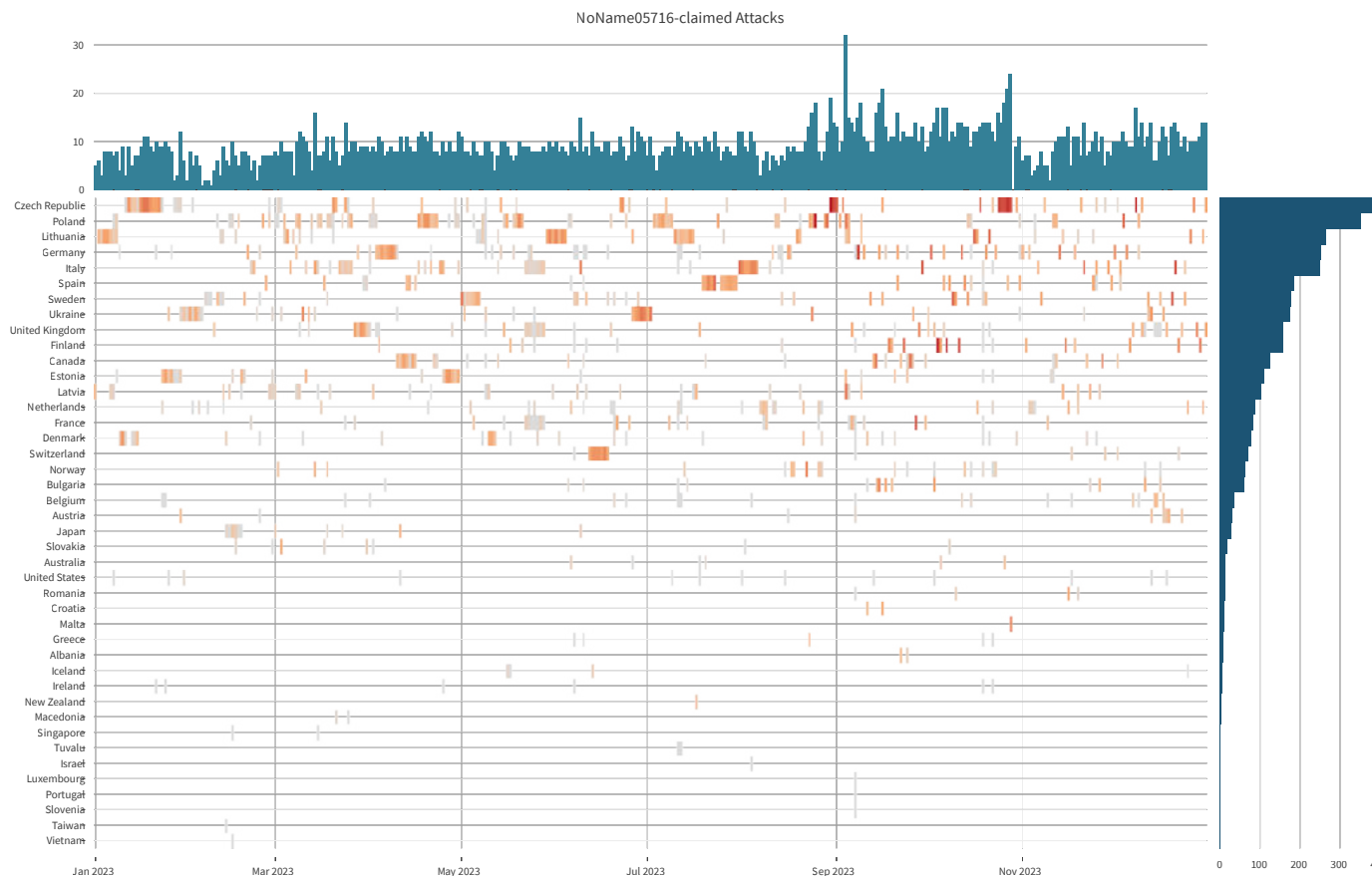
**Figure 83:** Web categories targeted by NoName057(16)



NoName05716-targeted Web Categories
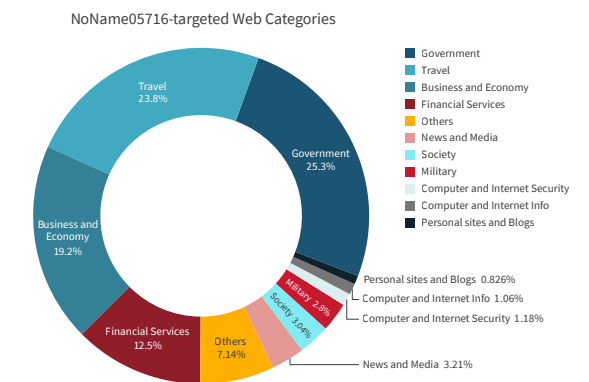
# Cyber Army of Russia:
# Pro-Russian Patriotic Hacktivist

The Cyber Army of Russia Reborn, describing itself as the "People's Cyber Army," caught our attention for its dedicated targeting of Ukraine. While Cyber Army of Russia did claim DDoS attacks on other countries, 341 out of a total of 481 attacks in 2023 (Figure 85) were targeting Ukrainian websites. The runner up, Poland, was targeted only 19 times. While on some days the Cyber Army of Russia would target up to a dozen websites, most days it was focusing on one or two Ukrainian targets.

The activity by Cyber Army of Russia Reborn corroborates the Mandiant statement in its intelligence report published September 23, 2022, and updated August 10, 2023: "We assess with moderate confidence that moderators of the purported hacktivist Telegram channels 'XakNet Team,' 'Infoccentr' and 'CyberArmyofRussia_ Reborn' are coordinating their operations with Russian Main Intelligence Directorate (GRU)- sponsored cyber threat actors."

**Figure 85:**

Cyber Army of Russia- claimed DDoS attacks

**Figure 84:** Cyber Army of Russia Telegram subscriber count evolution
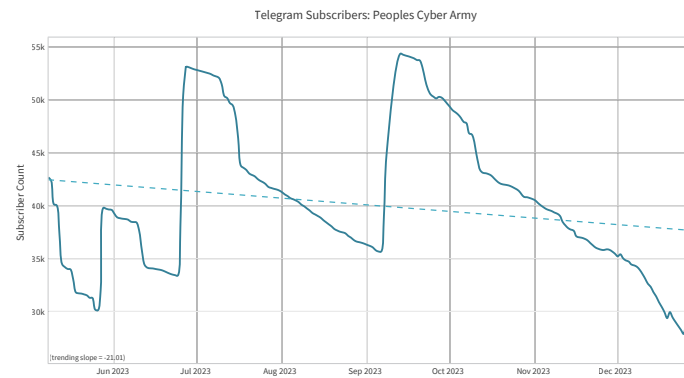


**Figure 86:** Web categories targeted by Cyber Army of Russia
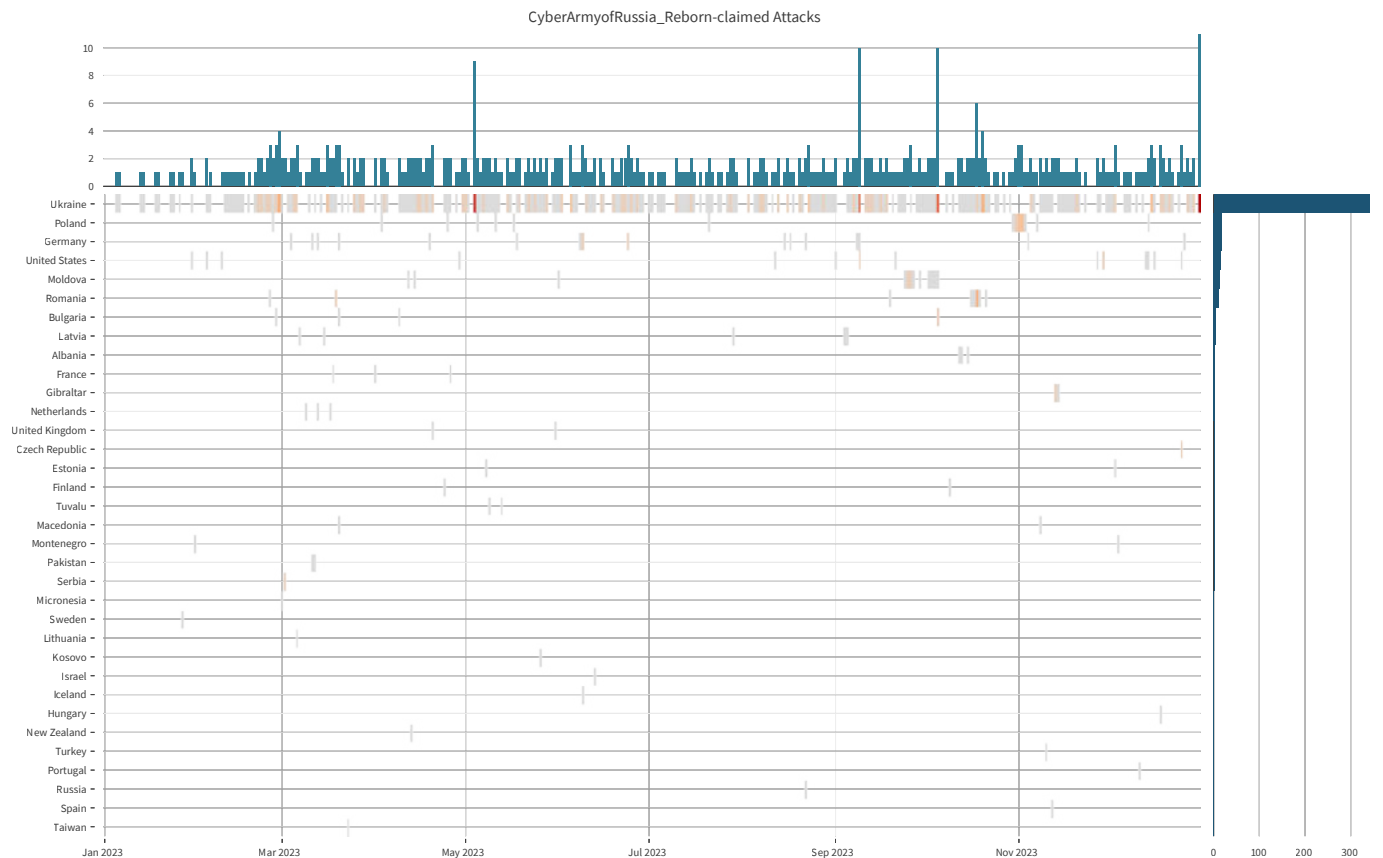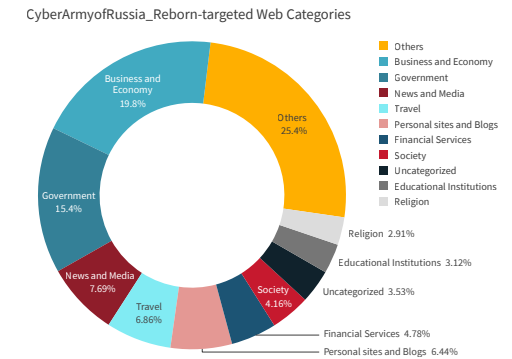
## Anonymous Sudan:
## The Rebel That Lost His Cause

Anonymous Sudan, the hacktivist group that joined the global threat scene in January 2023, has the security community divided on its origins. Some believe Anonymous Sudan to be a black flag operation run by the Russian government, others believe they were originally pro-Islamic hacktivists and operated from Sudan. In earlier reports we referred to Anonymous Sudan as the rebel with too many causes, claiming DDoS attacks driven by religion (pro-Islamic), by politics (pro-Sudanese and pro-Russian) and some by financial gain (ransom DDoS and stresser advertisements). This random behavior became most prominent in the second half of 2023, where the activity of Anonymous Sudan slowed considerably. Anonymous Sudan still regularly made headlines in the second half by targeting and breaking several high-profile websites in the process. Microsoft, X (former Twitter), OpenAI and others have been targeted by Anonymous Sudan and all suffered interruptions to some extent.

When Anonymous Sudan first appeared on the stage, it was an unknown entity until it attacked a common enemy of the enigmatic Russian hacktivist group Killnet and was knighted in the Killnet cluster by the hacker formerly known as KillMilk. Leveraging the Killnet brand to lift itself out of anonymity (pun intended), Anonymous Sudan quickly became a force to reckon with.

**Figure 87:**

Anonymous Sudan Telegram subscriber count evolution



Telegram Subscribers: Anonymous Sudan
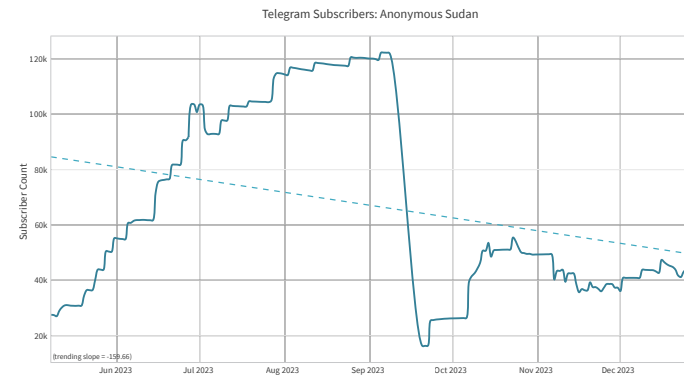
**Figure 88:** Anonymous Sudan-claimed DDoS attacks



AnonymousSudan-claimed Attacks
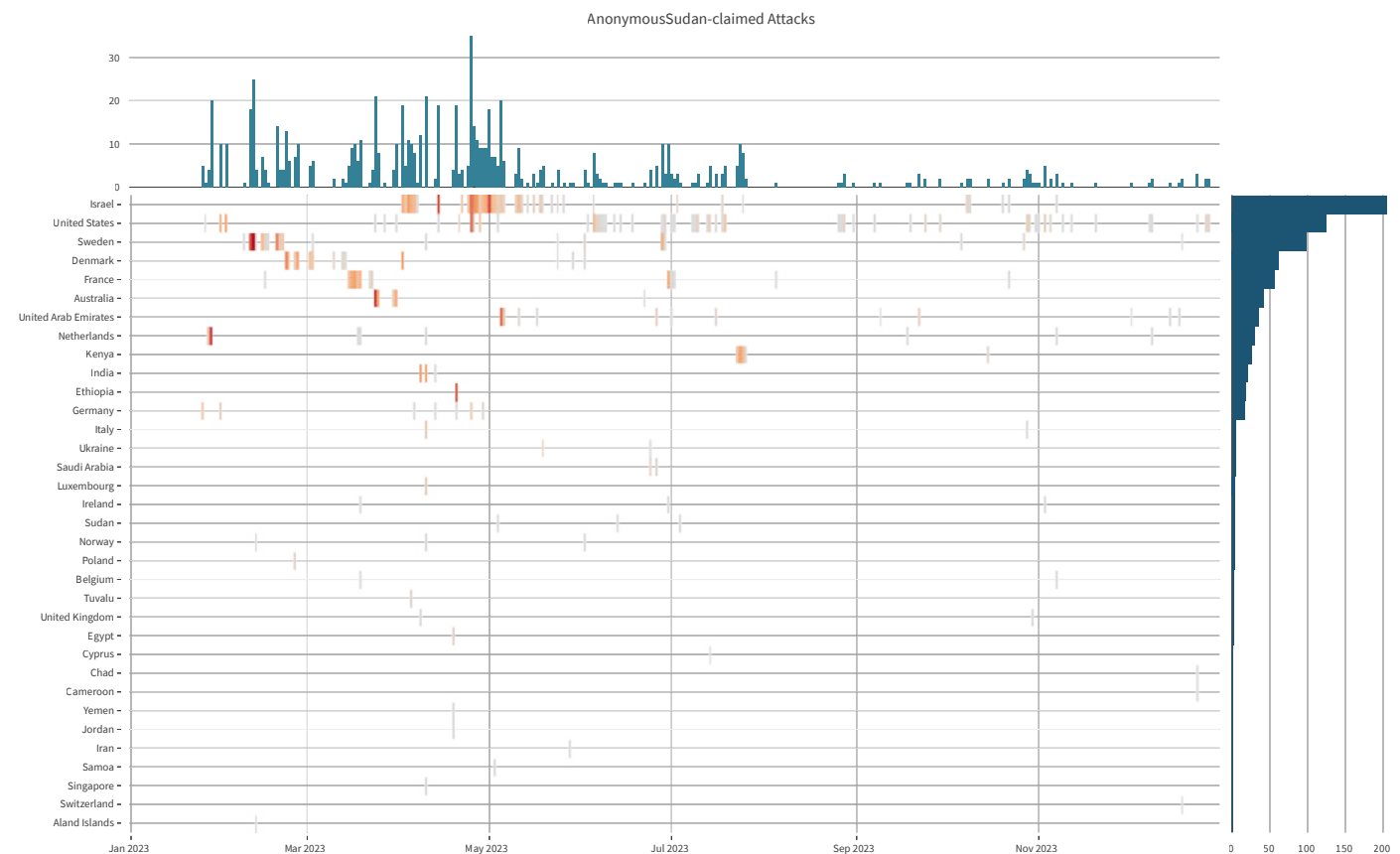
Although originally driven by religious motivations and part of several campaigns of political nature, towards the end of the year Anonymous Sudan mainly performed attacks on highly visible targets with little political or religious drive. Their attacks used the Skynet botnet, which advertised Skynet's capabilities in the process. The hacktivist-turned-Telegram-influencer most likely was paid for advertisements through stunt hacking. Advertisement is one of the main financial sources of income for hacktivist groups that have channels with high subscriber counts.

In September 2023, Telegram banned Anonymous Sudan's main Telegram channel, which at that time gathered over 120,000 subscribers. Anonymous Sudan was not able to recover their original channel, but they came back a few days later with a new Telegram channel, @xAnonymousSudan. The switch to a new maiden channel caused Anonymous Sudan to lose their entire subscriber count in a single day, and it was only able to recover one third (40,000) of the subscribers by year's end.

**Figure 89:** Web categories targeted by Anonymous Sudan



AnonymousSudan-targeted Web Categories

Legend:
- Others
- Travel
- Health and Medicine
- Government
- Educational Institutions
- News and Media
- Business and Economy
- Financial Services
- Society
- Streaming Media
- Social Networking

Travel 17.5%
Others 18.4%
Health and Medicine 15.8%
Government 10.3%
Educational Institutions 8.83%
News and Media 8.32%
Business and Economy 8.2%
Financial Services 5.3%
Social Networking 2.27%
Streaming Media 2.27%
Society 2.77%

## Killnet: Pro-Russian Patriotic Hacktivist That Lost Its Iconic Leader

One could fill books with stories of KillNet and the special projects of its former iconic leader, KillMilk. KillNet was the most prominent pro-Russian patriotic hacktivist that emerged mere days after the conflict in Ukraine started and became the most mediatized and most influential Russian hacktivist. We covered KillNet extensively in past advisories and blogs. In 2023, KillNet became less active in claiming DDoS attacks, while KillMilk focused his attention on other projects such as the Inifinity forum, Black School and the Black Skills "private military cyber company."

The group came under increased scrutiny in November after the Russian news site Gazeta.ru claimed to reveal the identity of KillMilk. On December 7, 2023, KillMilk announced his retirement on his Telegram channel and noted that KillNet will be "moving to a new stage of development under the auspices of a new team."

➡️

**Figure 90:**

KillMilk announcing his retirement
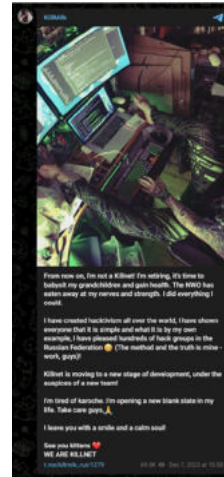


**Figure 91:**

Killnet's main Telegram channel subscriber count evolution



Telegram Subscribers: We are Killnet

**Figure 92:**

KillNet-claimed DDoS attacks



killnet_reservs-claimed Attacks
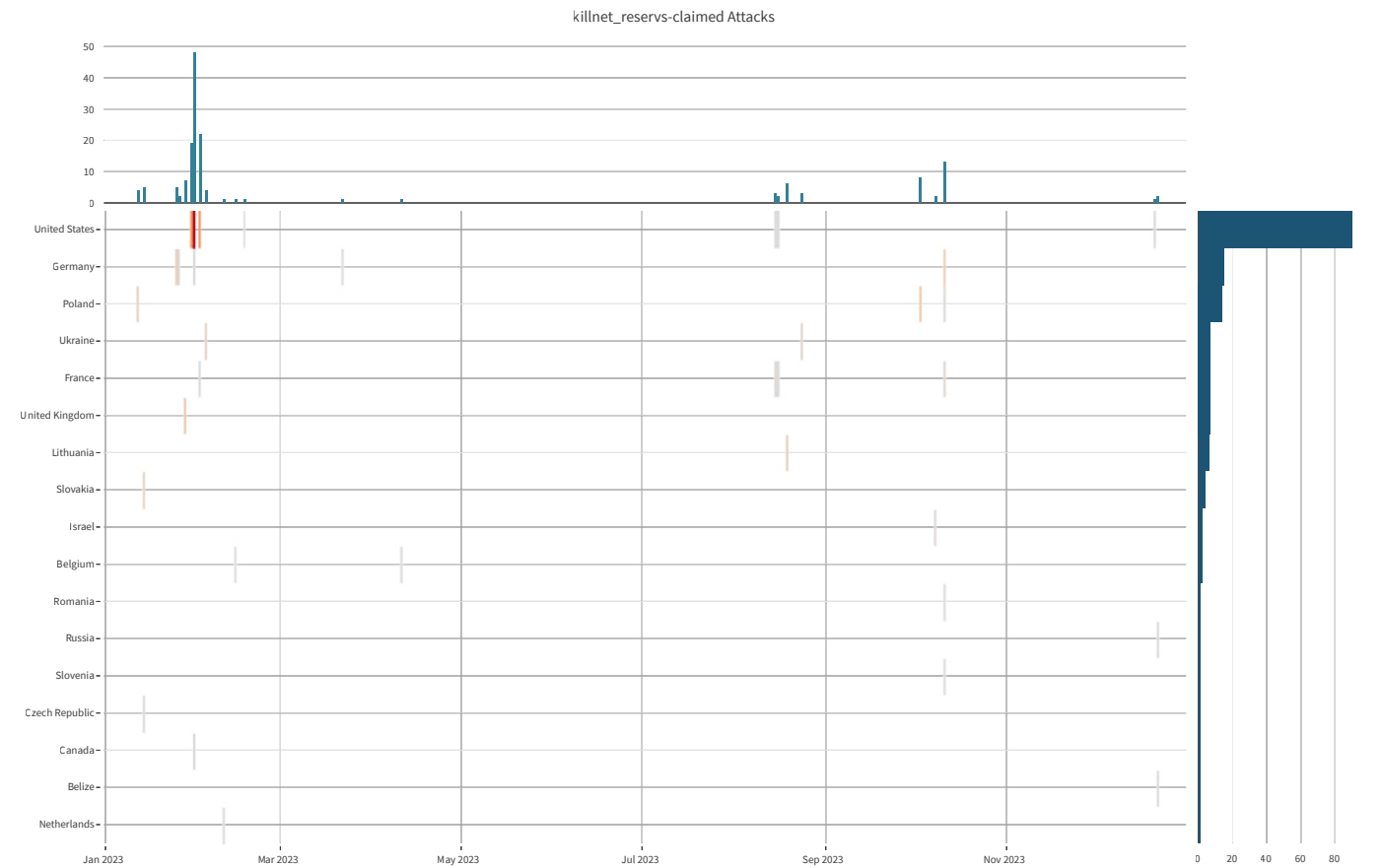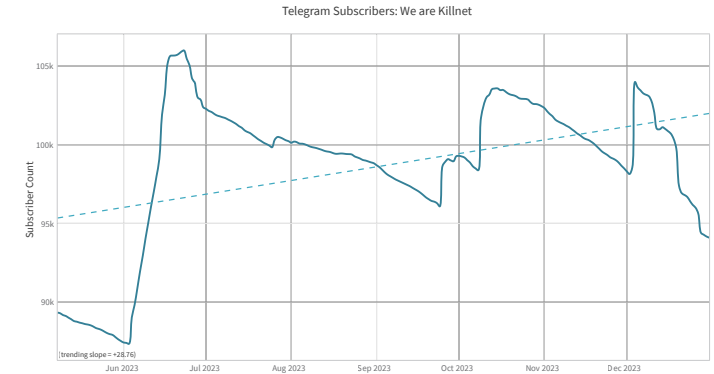
# Israel: The Most Targeted Country

Israel was the most targeted country by hacktivists in 2023. In the first half of 2023, Israel was the target of pro-Islamic hacktivists. These groups, using newly gained motivation from the pro-Russian hacktivists' activity in 2022, targeted Israel in the yearly #OpIsrael campaign that was started by Anonymous over 10 years ago and rebranded to #OpsBedil by DragonForce Malaysia in later years. In the second half, Israel became the target of pro-Palestinian hacktivists after the Israel/Hamas conflict began on October 7, 2023.

**Figure 93:** DDoS attacks targeting Israel
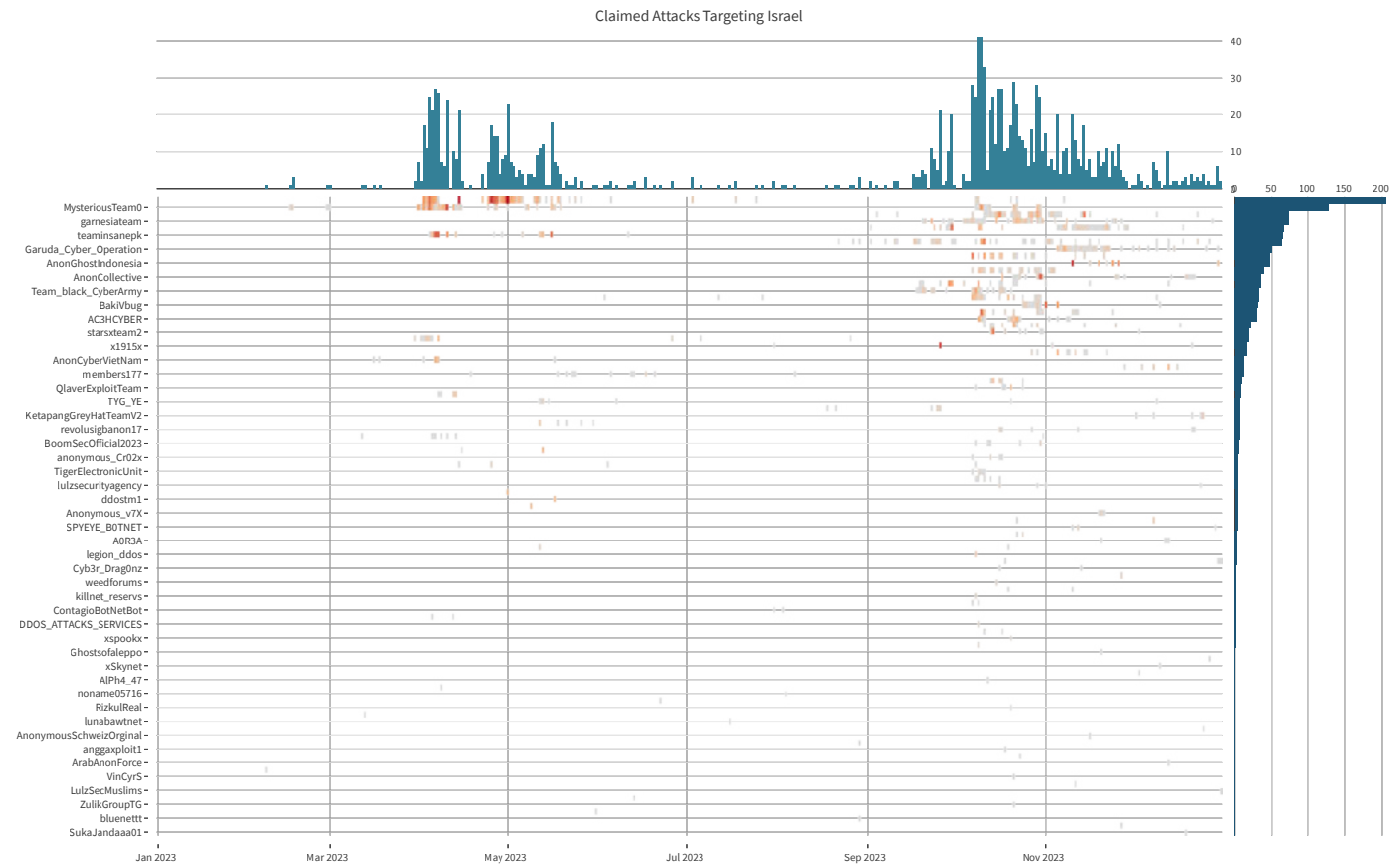
# Hacktivist Operations

Hacktivists have long been naming their operations with hashtags. Most battle tags start with "#Op" and provide a convenient way for groups to promote attack campaigns and create temporary alliances.

#OpIsrael was the most mentioned hashtag in 2023. It was mentioned in 5,918 posts on Telegram. #OpIndia took a considerable second place with 4,308 mentions. Jointly, #OpIsrael and #OpIndia represent more than half of the operation tags in 2023. Other notable countries in operations were France, the United States, Canada, Japan, Ukraine, Italy and the United Kingdom.

Considering the mentions over time for the top operation hashtags, #OpIsrael had a relatively small flareup in April during the yearly Anonymous #OpIsrael campaign. This was followed by a considerably large amount of mentions in October related to the start of the conflict with Hamas.

#OpIndia exhibited two bumps, one in the March-April timeframe and another in September-November timeframe—both closely related to the #OpIsrael campaign increases. There is also a noticeable overlap in hacktivist groups between the two operations.

The months of October and November were much more active for all operation hashtags. This flareup of activity can also be observed in Figure 77.

In the second half of 2023, we observed more hacktivist groups starting to create alliances, under joint attack campaigns and #Op battle tags. Some turned out to be temporary, but others were more lasting.

By relating channels based on their communications and message forwarding between all monitored channels, we found most channels and users are gravitating around a limited number of key channels, creating clusters of activity (see Figure 96).

**Figure 94:**

Most used operation hashtags in 2023



Top #OpX hashtags
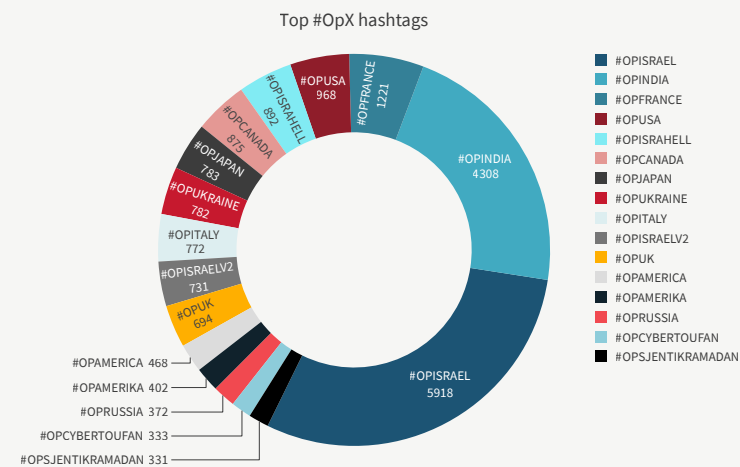
**Figure 95:** Most operation hashtag mentions in 2023



Operation Hashtag Mentions 2023
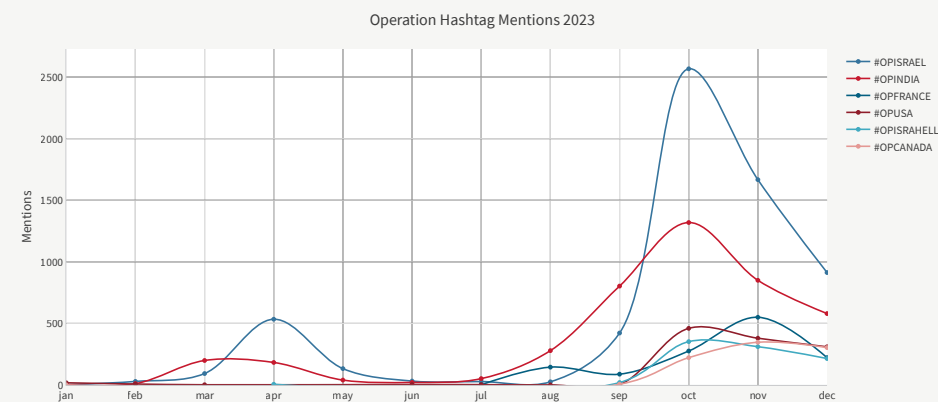
The study of the Telegram clusters and their related activity is a work in progress that we expect to publish on one of the Radware channels in the near future.

**Figure 96:** Telegram channel clusters gravitating around some key channels

# Appendix A: Common DNS Record Types

| | |
|---|---|
| **A** | The address mapping record, also known as a DNS host record, stores a hostname and its corresponding IPv4 address. |
| **AAAA** | The IP Version 6 address record stores a hostname and its corresponding IPv6 address. |
| **CNAME** | The canonical name record is used to alias a hostname to another hostname. When a DNS client requests a record containing a CNAME pointing to another hostname, the DNS resolution process is repeated with the new hostname. |
| **MX** | The mail exchanger record specifies an SMTP email server for the domain. |
| **NS** | The name server record specifies that a DNS Zone, such as 'example.com,' is delegated to a specific authoritative name server and provides the address of that name server. |
| **PTR** | The reverse-lookup pointer record provides the IP address of a hostname (reverse DNS lookup). |
| **SRV** | The service location record is like the MX record but for other services. |
| **TXT** | The text record can contain arbitrary information and typically carries machine-readable data such as opportunistic encryption, sender policy framework (SPF), DKIM, DMARC, etc. |
| **SOA** | The Start of Authority record appears at the beginning of a DNS zone file. It indicates the authoritative name server for the current DNS zone, contact details of the domain administrator, domain file version number, and information on how frequently DNS information for this zone should be refreshed. |
| **NAPTR** | The Naming Authority Pointer records map domain names to URIs (uniform resource identifiers) and other resources. NAPTR records are commonly used for applications in internet telephony. |

# Table of Figures

# Methodology and Sources

The data for DDoS events and volumes was collected from Radware devices deployed in Radware cloud scrubbing centers and on-premises managed devices in Radware hybrid and peak protection services, jointly denoted as **Radware's Cloud DDoS Protection Service**. Note that attack events and blocked events are considered the same for the purpose of this report. All blocked volume is considered attack volume. An attack is a collection of several related attack vectors targeting the same customer and overlapping in time. Events correspond to attack vectors. Attack vectors consist of one or more packets. All packets of an attack vector generate a certain volume expressed in bytes. The volume generated by an attack vector is referred to as the blocked volume for that attack vector, which corresponds to the attack volume for that vector. The attack volume of all attack vectors part of the same attack correspond to that attack's attack volume.

**Radware's Global Deception Network (GDN)** provides detailed events and payload data on a wide range of attacks and serves as a basis for the Unsolicited Network Activity section.

The data for web application attacks was collected from blocked application security events from the **Radware Cloud WAF Service**. Collected events were based solely on automatically detected and known vulnerability exploits and exclude any events that might be blocked or reported by custom rules added to a web application policy by managed services and/or customers.

Web DDoS attack details were collected from the **Web DDoS Protection Service**. For 2023, only a sample of attacks was available.

**Hacktivists** openly publicize their actions on social media and public Telegram channels to gain media attention and raise awareness. They do not operate covertly or evade the media, but instead reveal the names and resources of their targets and attempt to take credit for their attacks. Hacktivists utilize website monitoring tools to demonstrate the impact of their denial-of-service attacks on online resources and frequently share links to reports from online web monitoring tools in their messages. Through tracking and analyzing messages from several active hacktivist groups on Telegram, the Radware Threat Intelligence team assessed the global DDoS activity conducted by hacktivists.

## Editors

**Pascal Geenens** | Director of Threat Intelligence
**Arik Atar** | Senior Threat Intelligence Researcher

## Executive Sponsors

**Shira Sagiv** | VP Portfolio Marketing
**Deborah Myers** | Senior Director of Corporate Marketing
**Ron Meyran** | Senior Director of Corporate Enablement

## Production

**Kimberly Burzynski** | Sr. Marketing Communication Manager
**Jeffrey Komanetsky** | Content Development Manager

# About Radware

Radware® (NASDAQ: RDWR) is a global leader of cybersecurity and application delivery solutions for physical, cloud and software-defined data centers. Its award-winning solutions portfolio secures the digital experience by providing infrastructure, application and corporate IT protection and availability services to enterprises globally. Radware's solutions empower more than 12,500 enterprise and carrier customers worldwide to adapt quickly to market challenges, maintain business continuity and achieve maximum productivity while keeping costs down. For more information, please visit www.radware.com.

Radware encourages you to join our community and follow us on: Radware Blog, LinkedIn, Facebook, "X"/Twitter, SlideShare, YouTube, Radware Connect app for iPhone® and our Security Research Center that provides a comprehensive analysis of DDoS attack tools, trends and threats. This document is provided for information purposes only.

This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law. Radware specifically disclaims any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. The technologies, functionalities, services or processes described herein are subject to change without notice.