



Report

H1 2024 GLOBAL THREAT ANALYSIS REPORT



Contents

Key Insights	3	Hacktivist DDoS Activity	19
Web DDoS Attack Activity	3	Telegram.....	19
Network-Layer DDoS Attack Activity	3	Hacktivist DDoS Claims.....	20
Application-layer DNS DDoS Attack Activity	3	Most Targeted Countries and Top Claiming Actors.....	22
Hacktivist DDoS Attack Activity	4	Top Targeted Websites and Domains	23
Web Application and API Attack Activity	4	Top Claiming Actors.....	24
Bad Bot Activity	4	Web Application and API Attack Activity	25
Web DDoS Attack Activity	5	Bad Bot Activity	27
A Six-day, 14.7 Million RPS, Web DDoS Attack Campaign	5	Appendix A: Characteristics of Common DDoS Amplification Vectors	29
Web DDoS Attacks in H1 2024	6	DDoS Amplification Attack Vectors	29
Geographical Distribution.....	7	Table of Figures	30
Network-layer DDoS Attack Activity	8	Methodology and Sources	31
Regions	9	Editors.....	31
The Americas.....	10	Executive Sponsors	31
EMEA.....	11	Production	31
APAC.....	12	About Radware	32
Industries	13		
Attack Vectors and Targeted Applications	14		
Application-layer DNS DDoS Attack Activity	16		
DNS Amplification Attack	16		
DNS Flood Attack	16		
DNS NXDOMAIN Attack.....	16		
Pseudo Random Subdomain (PRSD) Attack.....	16		

Key Insights

Web DDoS Attack Activity

In the first half of 2024, web distributed denial of service (DDoS) attacks saw a significant increase in frequency and intensity:

- One notable Web DDoS attack campaign lasted six days, attacking 70% of that time (totaling 100 hours). It comprised 10 waves, each lasting four to 20 hours. This Web DDoS attack campaign averaged 4.5 million requests per second (RPS) with a peak of 14.7 million RPS.
- A surge in Web DDoS attacks was evident, considering a 137% increase in Q1 2024 over Q4 2023, followed by an 85% increase in Q2 2024 over Q1. New vectors such as HTTP/2 Rapid Reset and Continuation floods drove these attacks, resulting in a combined increase of 265% in the first half of 2024 compared to the second half of 2023.
- The majority of Web DDoS attacks targeted organizations in the EMEA region, influenced by geopolitical conflicts and significant events like the EU parliament elections, Euro 2024 in Germany and the 2024 Olympic Games in Paris.

Network-Layer DDoS Attack Activity

Network-layer DDoS attacks, which actually spanned L3 and L4, also exhibited a rising trend in H1 2024:

- There was a 16% increase in blocked network-layer attacks per organization compared to H2 2023 and a 12% increase compared to H1 2023. The average network-layer attack volume per organization grew by 127% between 2023 and 2024, a faster growth than the 17% growth in average network-layer volume blocked per organization per month between 2022 and 2023.
- The Americas faced 58% of global network-layer attacks and 37% of the network-layer volume, while EMEA accounted for 23% of the network-layer

attacks but had to mitigate 56% of the global network-layer volume. The APAC region accounted for almost 19% of network-layer attacks and 7% of the global network-layer volume.

- The number of monthly network-layer DDoS attacks targeting organizations in the Americas increased by 47% in 2024 compared to 2023. The average monthly DDoS volume per organization increased by 128%.
- The number of monthly network-layer DDoS attacks targeting organizations in EMEA decreased by 30% in 2024 compared to 2023. The average monthly DDoS volume per organization increased by 122%.
- The number of monthly network-layer DDoS attacks targeting organizations in APAC increased by 81% in 2024 compared to 2023. The average monthly DDoS volume per organization increased by 86%.
- Finance organizations experienced the highest network-layer attack activity (44%), followed by healthcare (17%), technology (10%), government (7.2%), transportation and logistics (5%), and gaming (5%).
- DNS and NTP were responsible for 87% of the total network-layer amplification attack volume.
- DNS, HTTPS and SIP were the most targeted applications by network-layer DDoS attacks.

Application-layer DNS DDoS Attack Activity

DNS DDoS attack activity tripled between 2022 and 2023 and quadrupled between H1 2023 and H1 2024:

- The number of malicious DNS queries surged by 2,680% in 2023 compared to 2022.
- The number of malicious queries in the first six months of 2024 has already increased by 76% compared to the total number of queries observed during the whole year in 2023.

- Most large application-layer DNS flood attacks in the first half of 2024 leveraged DNS-A requests.
- Finance was the most targeted industry, representing 52% of the total DNS query flood attack activity. Healthcare, telecom, research and education, technology, and communications were other notable industries.
- The largest DNS query flood attack observed in H1 2024 peaked at 811,000 queries per second (QPS) and targeted a financial organization. In 2023, the largest DNS flood was 2.15 million QPS, also targeting a financial organization.

Hactivist DDoS Attack Activity

The hactivist landscape remained dynamic with constant DDoS activity:

- Hactivist-driven DDoS attacks hovered between 1,000 to 1,200 claimed attacks per month in 2024 with Ukraine being the most targeted country.
- Pro-Russia hactivist group NoName057(16) remained the most active threat actor, collaborating with other groups like the Cyber Army of Russia Reborn to target Ukraine and other countries.
- Ukraine was the most targeted country by hactivists during the first half of 2024, followed by the United States, Israel, India and Moldova.
- In South Asia, India observed many claimed attacks from Indonesian and Bangladeshi hactivists with Anonymous Susukan, Ketapang Grey Hat Team and Sylhet Gang claiming the most attacks. Pakistan was also one of the most frequently attacked countries, mostly by Indian hactivists Team NWH, Dark Cyber Warrior, Kingsman, Hactivist Vanguard and Team Network Nine.
- The United States became an important target for DDoS-as-a-service providers that like to leverage big, highly visible organizations as a target for their proof-of-capability advertisements. The Telegram groups Channel DDoS v2, ZeusAPI Services and Krypton Networks claimed the most attacks targeting the United States.
- The top attacker collectives targeting Israel included RipperSec, 1915 Team, Sylhet Gang, Anonymous Muslims, LulzSec Indonesia, Team ARXU, StarsX Team and Dark Storm Team.

- Government websites were the most targeted since January 2023, especially in Ukraine, Israel, India, Moldova, Poland, Senegal and Spain. The top threat actor targeting government websites was, by a good margin, NoName057(16), followed by Mysterious Team, Team Insane Pakistan and Cyber Army of Russia Reborn.
- The Ukrainian domains rada.gov.ua and tax.gov.ua were the most targeted domains since January 2023. Other notable targeted domains were X (former twitter.com), Twitch, Amazon and Spotify. Of the most attacked government sites, Ukrainian and Moldovan domains suffered the most attacks while Italian and German domains were also in the top 20. The Warsaw Metro in Poland and the domain of a bank in Israel were also notable targets.

Web Application and API Attack Activity

Web application and API attacks increased by 22% in H1 2024 compared to H2 2023:

- Vulnerability exploitation was the leading attack category (33% of malicious requests), followed by access violations (10%), data leaks (4.8%) and SQL injection attacks (2.3%).
- North America was the most targeted region with 66% of attacks.

Bad Bot Activity

Bad bot transactions saw a significant rise with notable regional targeting:

- Compared to H1 2023, the number of bad bot transactions increased by 61% in 2024.
- North America experienced the highest bad bot activity, representing half of all transactions, followed by APAC, EMEA (20% each) and CALA (12%).
- The presence of web crawlers detected in the first half of 2024 was 5.8%, an increase from below 4% in 2021 and nearly 7% in 2023.

Web DDoS Attack Activity

Network-layer DDoS attacks are better understood and arguably easier to detect and mitigate than the new generation of HTTPS floods that organizations started facing more often in 2023. Since HTTPS floods have been around for a few years, they are sometimes considered old news. However, the frequency and intensity of the new generation of HTTPS floods have increased dramatically, and the sophistication introduced by attackers is growing quickly and viciously. That is why we like to refer to these new-generation HTTPS floods as Web DDoS attacks.

A Six-day, 14.7 Million RPS, Web DDoS Attack Campaign

The February 2024 Global Threat Analysis Report referenced a 20-hour Web DDoS attack that happened in 2023. The campaign consisted of several waves reaching up to 2.8 million RPS. In contrast, we've already seen a six-day attack campaign in the first half of this year. The attack consisted of several four to 20-hour Web DDoS attack waves totaling 100 hours of Web DDoS and sustaining an average of 4.5 million RPS with a peak of 14.7 million RPS.

The UAE financial institution was under attack 70% of the time during the six-day barrage. While under attack, the ratio of legitimate to malicious web requests was as low as 0.002% and averaged 0.12%. Radware's Web DDoS Protection Services stopped over 1.25 trillion malicious web requests while leaving 1.5 billion legitimate web requests untouched. Throughout the attack campaign, the attacker tried several times to overrun the customer's web applications but failed to impact the services. They ultimately gave up after six days and 100 hours of generating malicious web requests.

Radware's threat research has [attributed the attack campaign](#) to the hacktivist threat group SN_BLACKMETA, based on the motivation, common traits with earlier threat groups and threats announced by the group. We assume that the infrastructure leveraged during the attack could be part of the InfraShutdown premium DDoS-for-hire service. InfraShutdown is a premium service with subscription fees that range from \$500 for a week up to \$2,500 for a month.

Figure 1:
Statistics of each wave of the six-day Web DDoS attack campaign (source: Radware)

	Wed	Thu	Fri	Sat (AM)	Sat (PM)	Sun (AM)	Sun (AM)	Sun (AM)	Mon (AM)	Mon (AM)	6 days
Duration [hours]	12.05	11.60	19.85	7.18	4.16	6.58	10.02	9.82	9.83	10.00	101.09
% time under attack	50.21%	48.33%	82.71%	59.83%	34.67%	54.83%	83.50%	81.83%	81.92%	83.33%	70.20%
Max RPS	5,528,829	14,652,566	13,538,520	13,558,301	3,048,283	5,285,425	10,196,679	5,571,367	9,717,985	7,416,667	14,652,566
Avg RPS	2,339,163	6,935,632	4,488,406	5,379,275	978,664	985,130	3,265,967	1,065,804	2,444,654	3,402,565	4,408,825
Received Req	101,402,734,075	289,978,805,092	321,100,614,286	139,484,602,358	14,719,117,639	23,416,544,333	117,836,106,031	37,708,179,334	86,785,229,407	122,356,266,667	1,254,788,199,222
Dropped Req	101,158,022,259	289,925,578,273	320,582,965,583	139,426,394,363	14,716,282,276	23,379,395,212	117,325,706,311	37,665,669,152	86,751,607,095	122,354,407,670	1,253,286,028,194
Passed Req	244,711,816	53,226,819	517,648,703	58,207,995	2,835,363	37,149,121	510,399,720	42,510,182	33,622,312	1,858,997	1,502,171,028
% legitimate	0.24%	0.02%	0.16%	0.04%	0.02%	0.16%	0.43%	0.11%	0.04%	0.002%	0.12%

Web DDoS Attacks in H1 2024

Web DDoS attacks have continued to rise since the start of 2023 due to several trends in the new threat landscape. A good portion of the activity, especially in Europe, can be attributed to hackers motivated by political tensions in the region. Hacktivists are known to reach for more sophisticated L7 attacks targeting online applications. Since the start of the conflict in Ukraine, hackers have become more experienced and sophisticated. Some hackers turned to financial gain by renting out their non-volunteer-based botnets to third parties with better finances. During 2023, we observed an increase in DDoS-for-hire services that started creating more offerings around L7 web applications and API attack vectors. Hacktivists improve them and leverage artificial intelligence to add features such as CAPTCHA bypass and, more recently, CAPTCHA solving. DDoS-for-hire services moved their focus from L3/L4 attack vectors to L7 vectors, quickly picking up on the [HTTP/2 Rapid Reset](#) vulnerability disclosed in October 2023 as well as the [HTTP/2 Continuation flood](#) attack vector disclosed in April 2024. This resulted in a significant increase in Web DDoS application request rates.

The number of Web DDoS attacks blocked by Radware’s Cloud Protection Services increased almost exponentially in 2024. In Q1 2024, the number of mitigated Web DDoS attacks increased by 137% compared to Q4 2023. In Q2 2024, the number of Web DDoS attacks increased again with 85% compared to Q1 2024.

In the first half of 2024, almost 3% of the attacks were over 1 million RPS. Almost 17% of all Web DDoS attacks so far in 2024 were between 100,000 and 250,000 RPS. The fraction of relatively small Web DDoS attacks (below 50,000 RPS) decreased from 74% in 2023 to 55% in 2024. This demonstrates a shift to larger, more intense and more impactful Web DDoS attacks in 2024. In general, as seen in **Figure 3**, the size of Web DDoS attacks in 2024 has increased compared to last year.

Figure 2: Number of Web DDoS attacks mitigated per quarter (source: Radware)

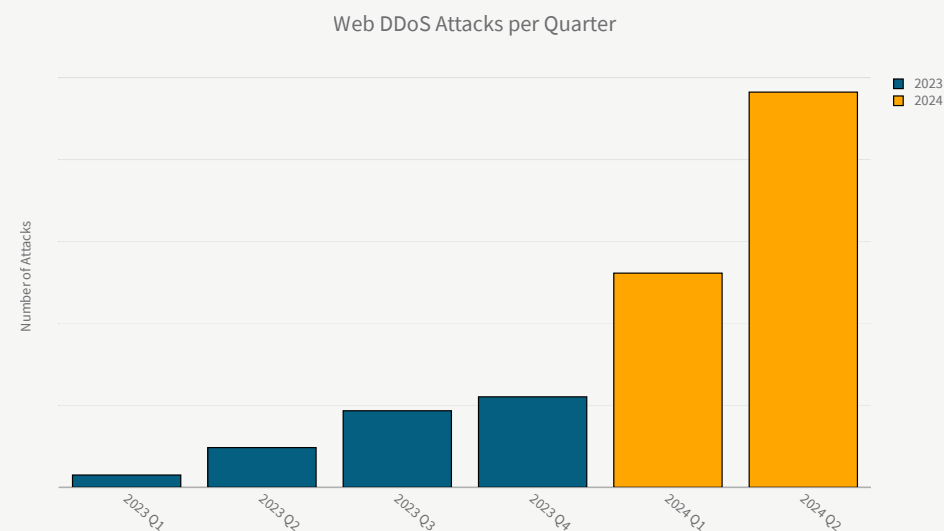
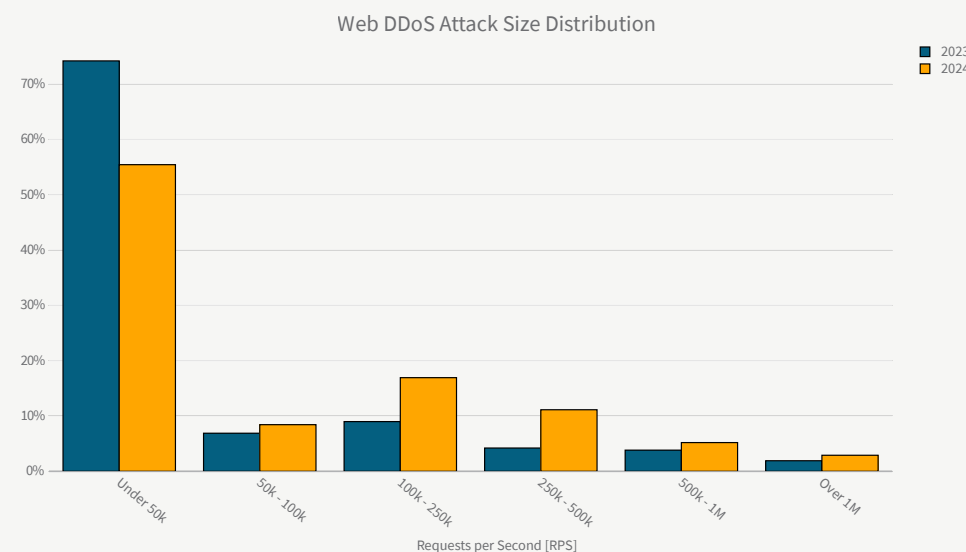


Figure 3: Web DDoS attack size (RPS) distribution per year (source: Radware)

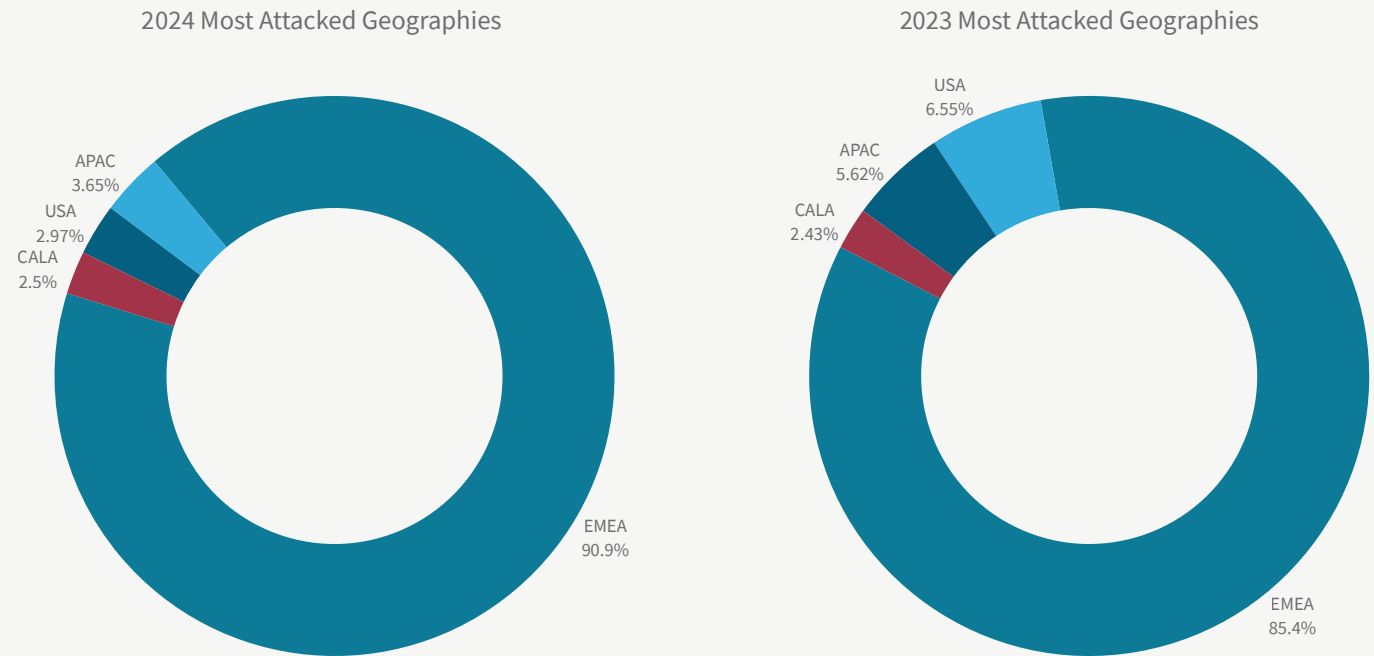


Geographical Distribution

More than 90% of all Web DDoS attacks in 2024 targeted organizations based in EMEA, a rise from the still significant 85% of Web DDoS attacks that targeted EMEA in 2023.

The EMEA region's position at the center of gravity of most Web DDoS attacks can be explained by geopolitical tensions and conflicts in the region, including the war in Ukraine, the conflict between Israel and Hamas, and the war between the Rapid Support Forces and the Sudanese Armed Forces. Also, Europe held a significant number of elections during the first half of 2024. This includes, but is not limited to, the EU Parliament elections, which took place from June 3 to June 9 across the European Union. Furthermore, Germany hosted Euro 2024 from June 14 to July 14, 2024, and Paris hosted the Olympic Games in the second half of 2024.

Figure 4: Geographical distribution of Web DDoS attacks (source: Radware)



Network-layer DDoS Attack Activity

The average number of network-layer DDoS attacks blocked per organization¹ during the first half of 2024 grew by 16% compared to the second half of 2023 and by 12% compared to the first half of 2023. The number of network-layer attacks mitigated per organization in the first six months of 2024 is 16% higher than the total number of network-layer attacks mitigated per organization in 2022. The number of network-layer attacks in H1 2024 represents 57% of the total number of network-layer attacks per organization in 2023.

In H1 2024, Radware’s Cloud DDoS Protection Service mitigated an average of 1,227 network-layer attacks per month per organization, compared to 1,075 network-layer attacks in 2023. In contrast, in 2022, the average number of network-layer attacks per organization was 528 per month.

The average network-layer DDoS volume blocked per organization in H1 2024 grew by 81% compared to H2 2023 and by 205% compared to H1 2023. The network-layer volume blocked per organization in H1 2024 was 14% higher compared to the network-layer volume all of 2023.

In H1 2024, Radware’s Cloud DDoS Protection Services mitigated an average network-layer attack volume of 1.23TB per month per organization compared to 0.54TB in 2023. In 2022, the average network-layer volume per month per organization was 0.46TB. This represents an increase of 127% in the average network-layer DDoS volume blocked per organization per month between 2023 and 2024. In contrast, the increase in average network-layer volume blocked per organization per month between 2022 and 2023 was 17%.

1. 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 rather than the total metric.

Figure 5: Network-layer DDoS attacks mitigated per organization by year (source: Radware)

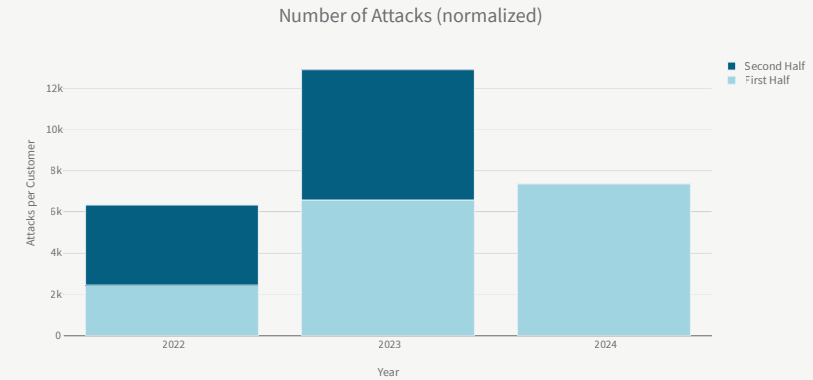


Figure 6: Network-layer DDoS attacks mitigated per organization by the end of H1 2024 (source: Radware)

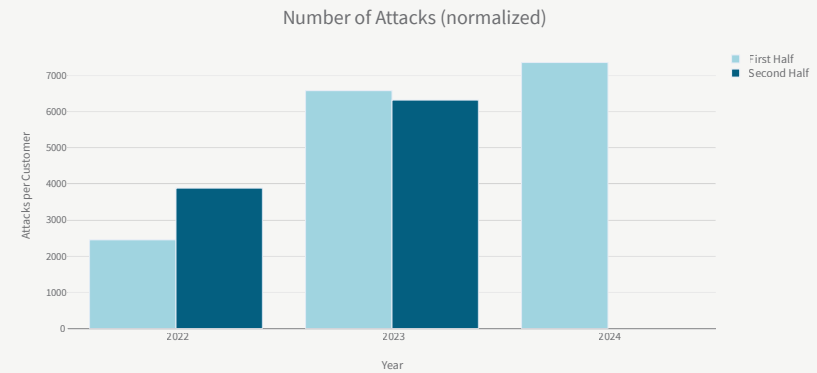
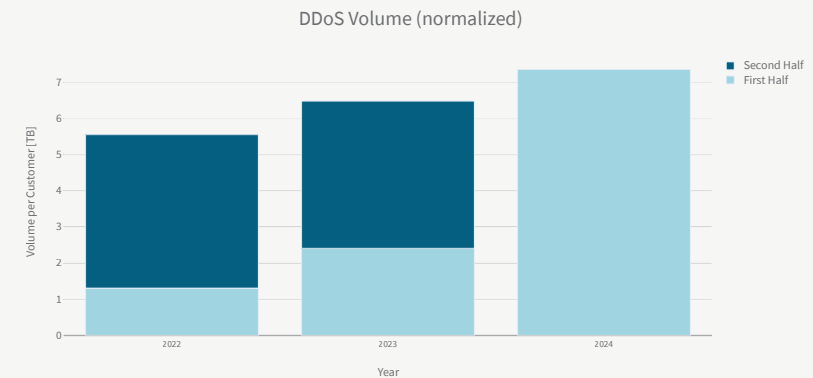


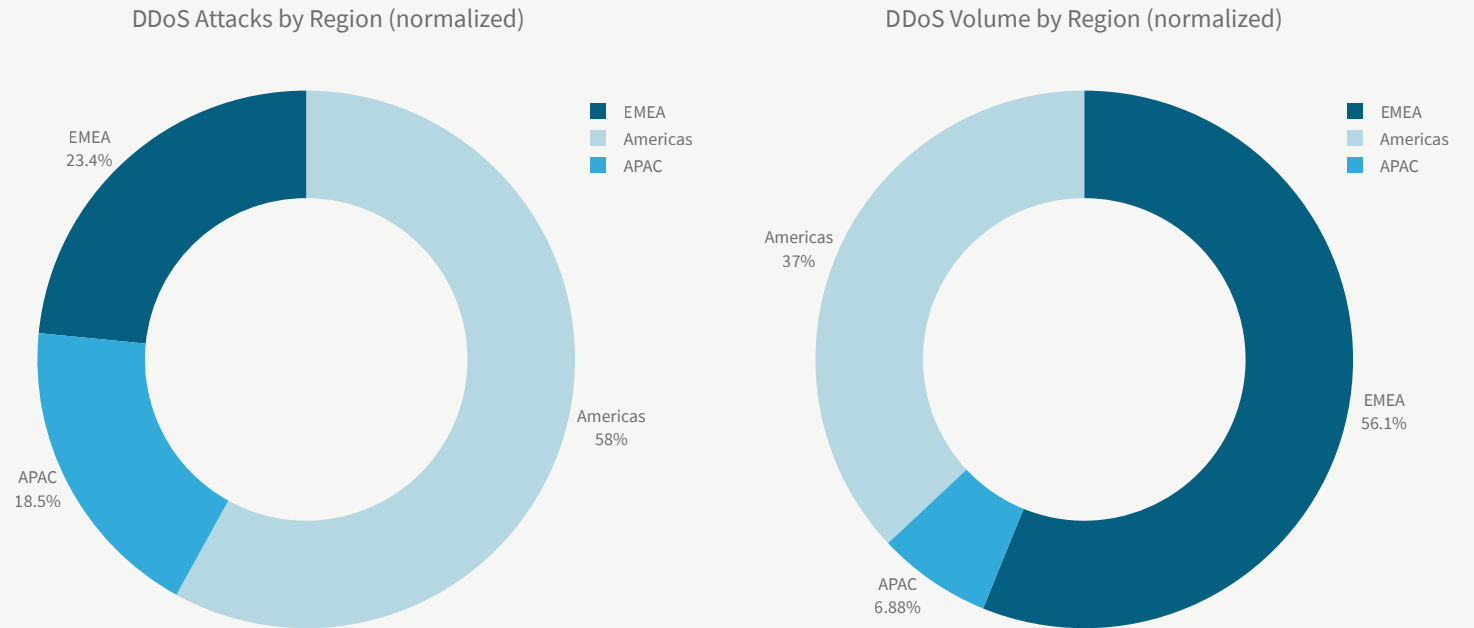
Figure 7: Network-layer DDoS volume blocked per organization by year (source: Radware)



Regions

Organizations located in the Americas were targeted by 58% of the global network-layer DDoS attacks and saw a network-layer attack volume of 37% of the global network-layer attack volume. Organizations in the EMEA region, while accounting for 23% of the network-layer attacks, had to mitigate 56% of the global network-layer attack volume. The APAC region accounted for almost 19% of global network-layer DDoS attacks and 7% of the global network-layer attack volume.

Figure 8: 2024 H1 network-layer DDoS attacks and volume per region (source: Radware)



The Americas

The Americas region saw a steady growth in the number of network-layer attacks targeting the region since 2021. In H1 2024, the number of network-layer DDoS attacks targeting organizations in the Americas grew by 42% compared to H2 2023 and 52% compared to H1 2023.

In H1 2024, a typical organization located in the Americas mitigated an average of 2,053 network-layer attacks per month per organization, compared to 1,400 network-layer attacks in 2023. This represents an increase of 47% in the monthly number of network-layer attacks mitigated by organizations located in the Americas between 2023 and 2024.

The average network-layer DDoS volume blocked per organization located in the Americas grew by 140% in H1 2024 compared to H2 2023 and by 116% compared to H1 2023. The network-layer volume blocked per organization in the Americas in H1 2024 was 14% higher compared to the network-layer volume blocked per organization in all of 2023.

In H1 2024, Radware's Cloud DDoS Protection Services mitigated an average network-layer volume of 1.17TB per month per organization in the Americas compared to 0.51TB in 2023. This represents an average increase of 128% of network-layer DDoS volume blocked per organization per month between 2023 and 2024 in the Americas.

Figure 9: Network-layer DDoS attacks mitigated per organization located in the Americas region (source: Radware)

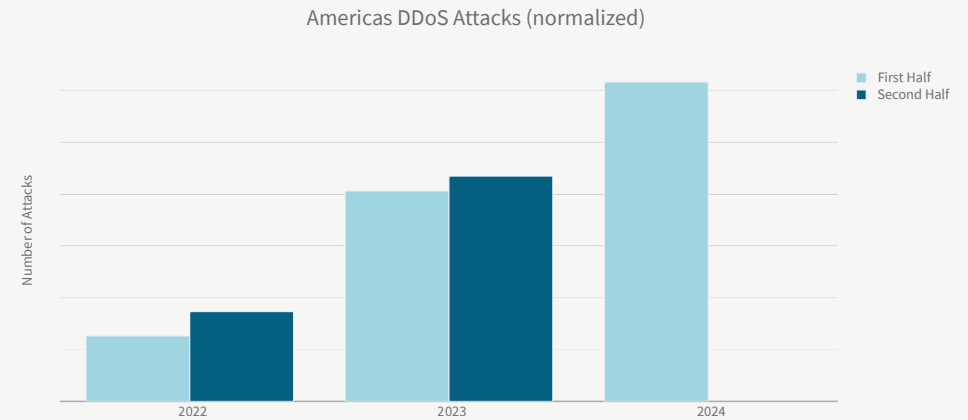
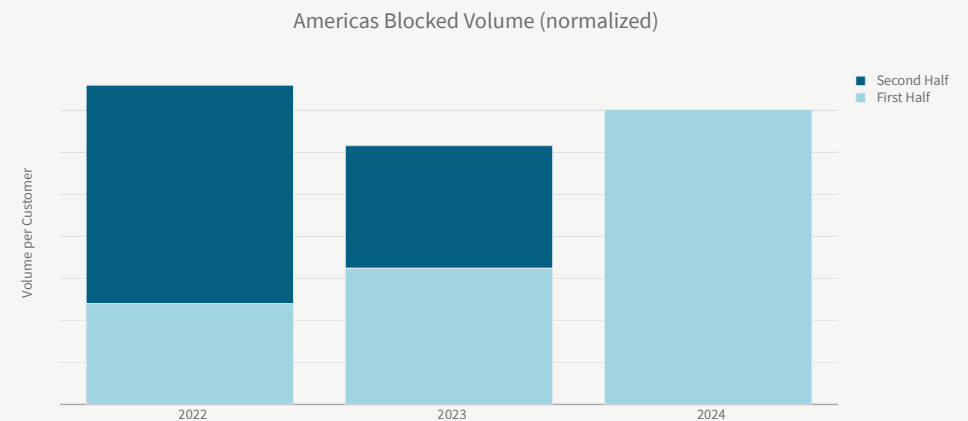


Figure 10: Network-layer DDoS volume blocked per organization located in the Americas region (source: Radware)



EMEA

The EMEA region saw a drop in the number of network-layer DDoS attacks targeting the region since 2023. In H1 2024, the number of network-layer DDoS attacks targeting organizations in the EMEA region shrunk by 26% compared to H2 2023 and 33% compared to H1 2023. Compared to H1 2022, the number of attacks in H1 2024 increased by 44%.

In H1 2024, organizations located in EMEA mitigated an average of 829 attacks per month per organization, compared to 1,181 attacks per month per organization in 2023. This represents a decrease of 30% in the monthly number of attacks mitigated by organizations located in EMEA between 2023 and 2024.

The average network-layer DDoS volume blocked per organization located in EMEA grew by 54% in H1 2024 compared to H2 2023 and by 293% compared to H1 2023. The volume blocked per organization in EMEA in H1 2024 was 10% higher compared to the volume blocked per organization for all of 2023.

In H1 2024, Radware’s Cloud DDoS Protection Services mitigated an average volume of 1.77TB per month per organization in EMEA compared to 0.80TB per month per organization in 2023. This represents an average increase of 122% of network-layer DDoS volume blocked per organization per month between 2023 and 2024 in EMEA.

Figure 11: Network-layer DDoS attacks mitigated per organization located in EMEA (source: Radware)

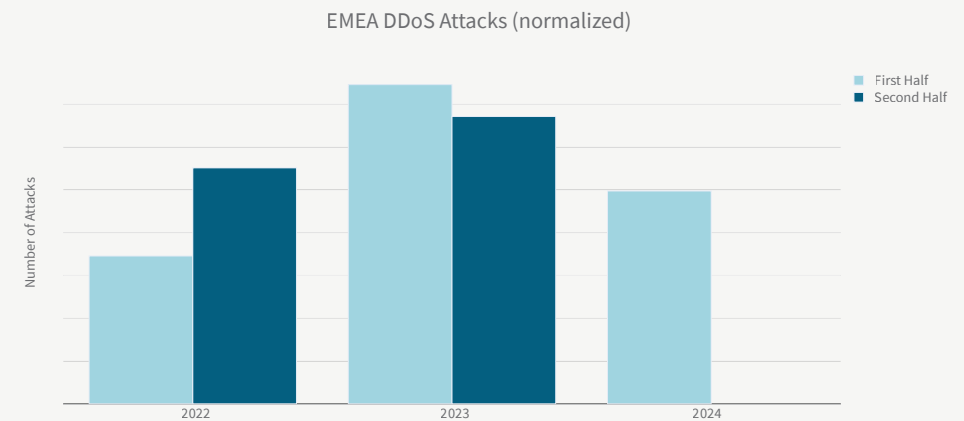
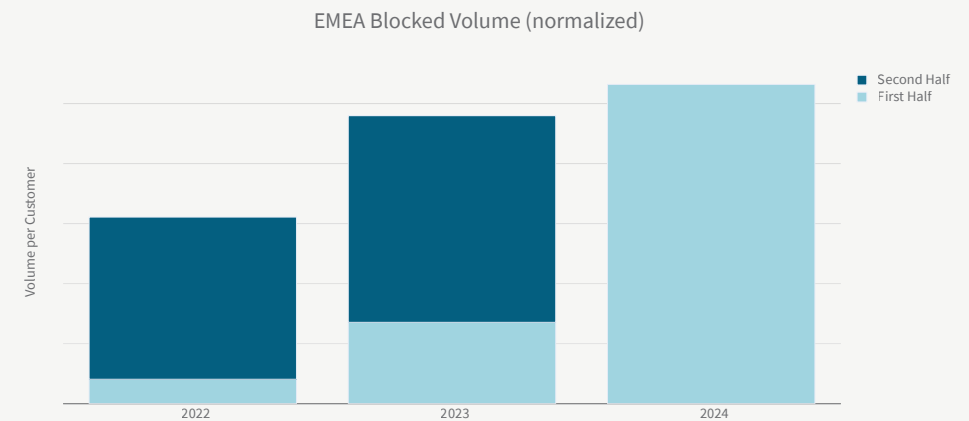


Figure 12: Network-layer DDoS volume blocked per organization located in EMEA (source: Radware)



APAC

The APAC region saw a significant growth in the number of attacks targeting the region in H1 2024. The number of network-layer DDoS attacks targeting organizations in the APAC region grew by 101% compared to H2 2023 and 65% compared to H1 2023.

In H1 2024, an organization located in the APAC region mitigated an average of 656 attacks per month per organization, compared to 362 attacks per month per organization in 2023. This represents an increase of 81% in the monthly number of attacks mitigated by organizations located in APAC between 2023 and 2024.

The average network-layer DDoS volume blocked per organization located in APAC grew by 21% in H1 2024 compared to H2 2023 and by 302% compared to H1 2023. The volume blocked per organization in APAC in H1 2024 was just 7% shy of the total volume blocked per organization in all of 2023.

In H1 2024, Radware’s Cloud DDoS Protection Services mitigated an average volume of 117GB per month per organization in APAC compared to 217GB per month per organization in 2023. This represents an average increase of 86% in APAC network-layer DDoS volume blocked per organization per month between 2023 and 2024.

Figure 13: Network-layer DDoS attacks mitigated per organization located in APAC (source: Radware)

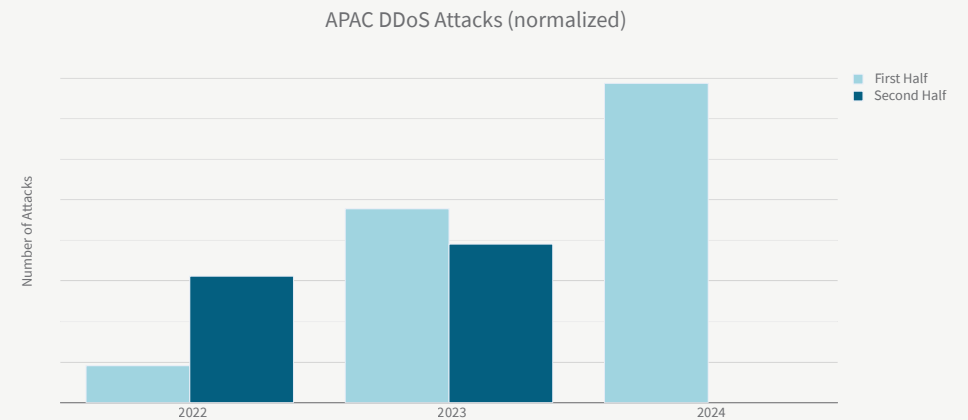
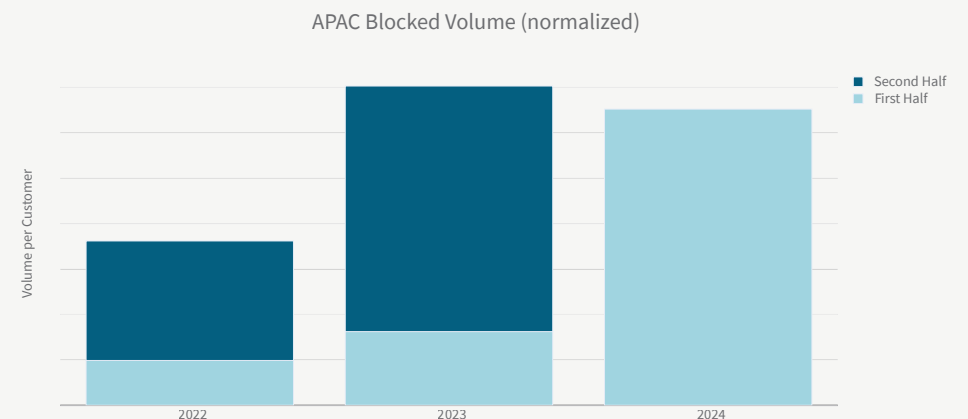


Figure 14: Network-layer DDoS volume blocked per organization located in APAC (source: Radware)



Industries

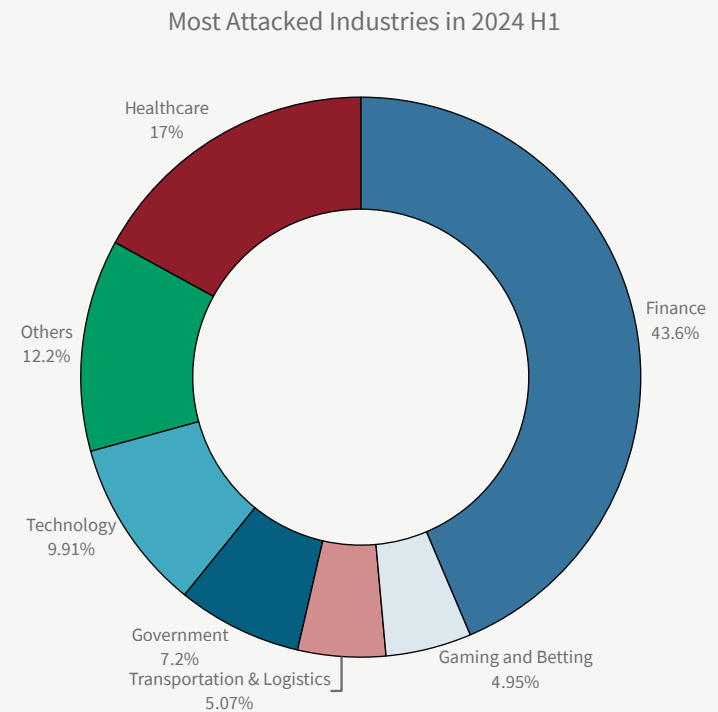
In H1 2024, certain industries faced a disproportionate share of network-layer DDoS attacks. Notably, organizations within finance experienced almost 44% of the global attack activity. Healthcare organizations faced a considerable number of attacks and were targeted by 17% of all attacks.

Other notable industries that were frequent targets of network-layer DDoS attacks were technology (10%), government (7.2%), transportation and logistics (5%), and gaming (5%). All other organizations combined suffered 12% of the global attack activity.

Organizations in the e-commerce, energy and automotive industries faced a significant increase in attack activity in the first half of 2024 compared to 2023. Research and education, telecom, finance and gaming were the other notable industries with considerable growth in the number of attacks in H1 2024.

Organizations in the utilities, service provider, retail and industrials industries were considerably less targeted in H1 2024 compared to last year.

Figure 15: Most attacked industries (source: Radware)



Attack Vectors and Targeted Applications

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 out-of-state and SYN-ACK floods are also often leveraged for volumetric attacks.

By a significant margin shown in **Figure 16**, the top attack vector leveraged during volumetric attacks was UDP fragment flood (64.5%), followed by TCP out-of-state (9.8%), DNS-A query flood (9.8%), UDP flood (6.6%) and SYN-ACK flood (6.3%).

Attacks aiming to exhaust resources will typically be characterized by higher packet rates. DNS-A query floods accounted for half of the malicious packets in H1 2024. This also explains the earlier mentioned significant portion of 9.8% of all malicious volume being taken up by DNS-A query floods.

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. Table 1 in Appendix A lists some of the top amplification vectors and their associated maximum amplification factor.

Figure 16: Top network-layer DDoS attack vectors (source: Radware)

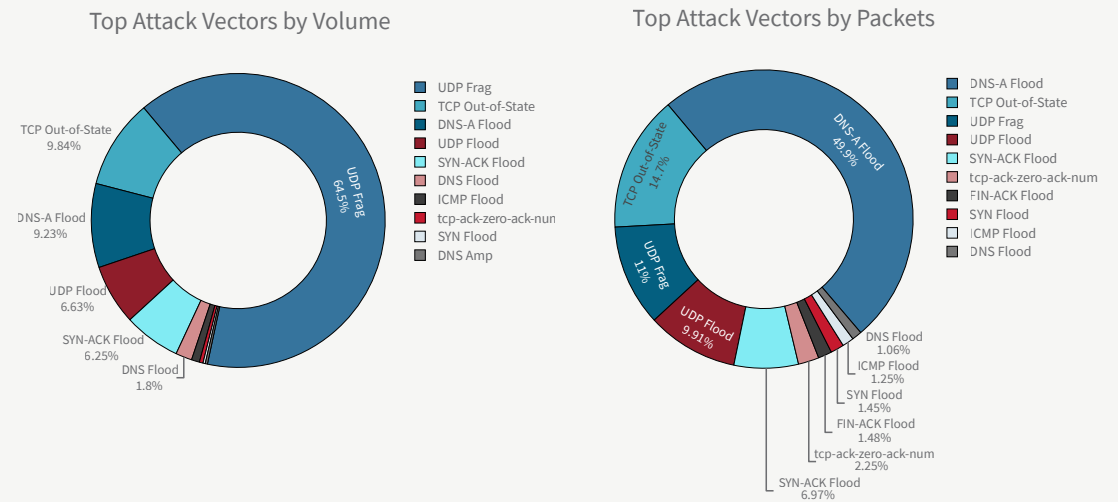
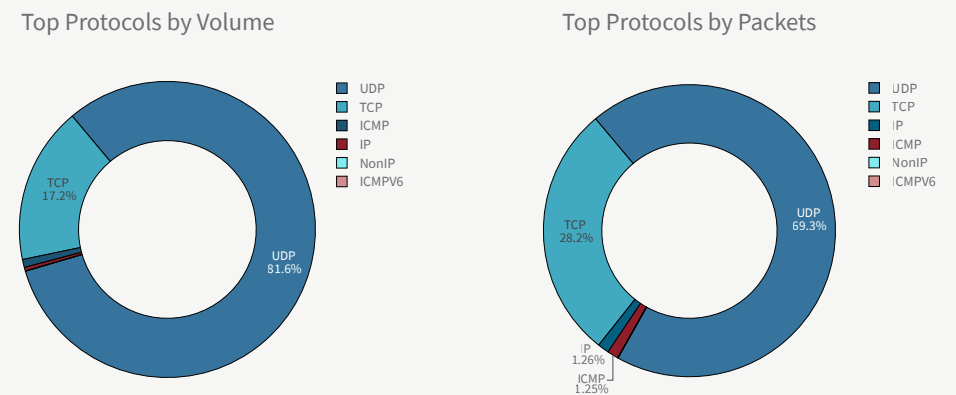


Figure 17: Top network-layer DDoS protocols (source: Radware)



DNS and NTP amplification generated the most volume in the first half of 2024, representing 86.5% of the total attack volume. DNS amplification was the most leveraged amplification attack vector and represented 55% of all the amplification attack volume observed in H1 2024. SSDP amplification represented another significant portion, almost 11% of the amplification attack volume.

DNS, HTTPS and SIP 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. DNS was the most targeted application protocol by far. It was targeted by almost half of all malicious packets blocked in H1 2024.

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 third most targeted application protocol in 2024 so far. 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 (DoS) attack.

Figure 18: Top network-layer DDoS amplification vectors (source: Radware)

Top Amplification Vectors by Volume

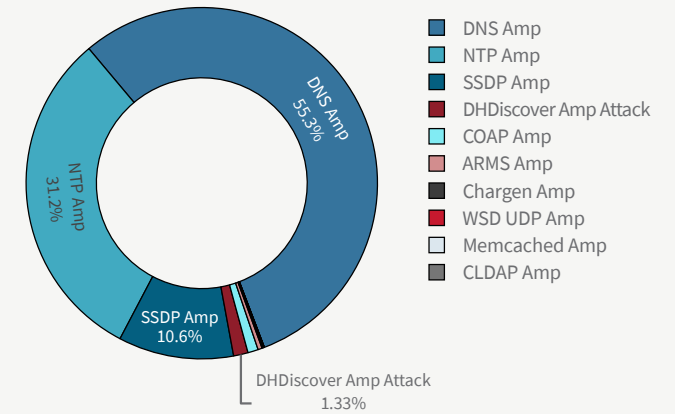
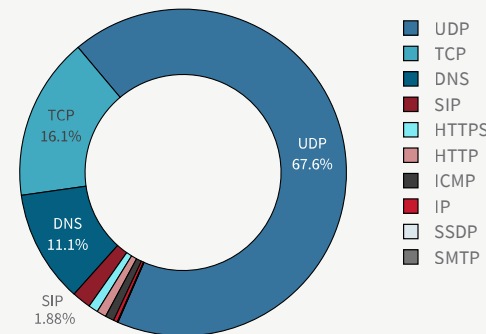
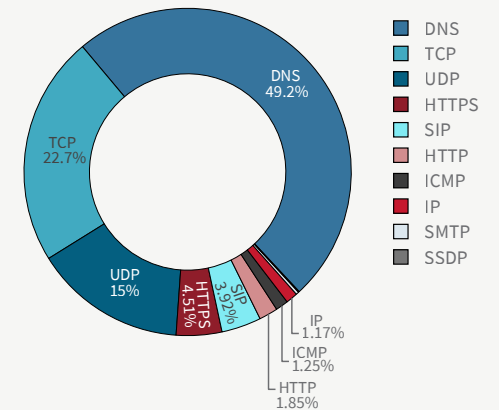


Figure 19: Top targeted application by network-layer DDoS attacks (source: Radware)


Top Targeted Applications by Packets



Top Targeted Applications by Packets



Application-layer DNS DDoS Attack Activity



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 by translating human-readable domain names into their underlying IP addresses. When a DNS service is subjected to a cyberattack, such as DoS or DDoS, 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.

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 aims 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.

This report's "Network-Layer DDoS Attack Activity" section discusses DNS amplification attacks. The section analyzes the DNS query flood attack, a form of application-layer DNS attack that aims 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 Radware’s Cloud DDoS Protection Services.

Figure 20 shows that throughout 2021 and most of 2022, fewer than nine out of every 1,000 attack vectors were DNS flood vectors. However, from Q4 of 2022, there was a marked increase in the proportion of attacks featuring a DNS flood vector. By the end of 2023, the ratio of DNS flood attack vectors more than tripled, and by Q2 2024 the ratio surged to 86.4 vectors per 1,000 attack vectors.

Figure 20: DNS flood attack vector ratio evolution over time (source: Radware)

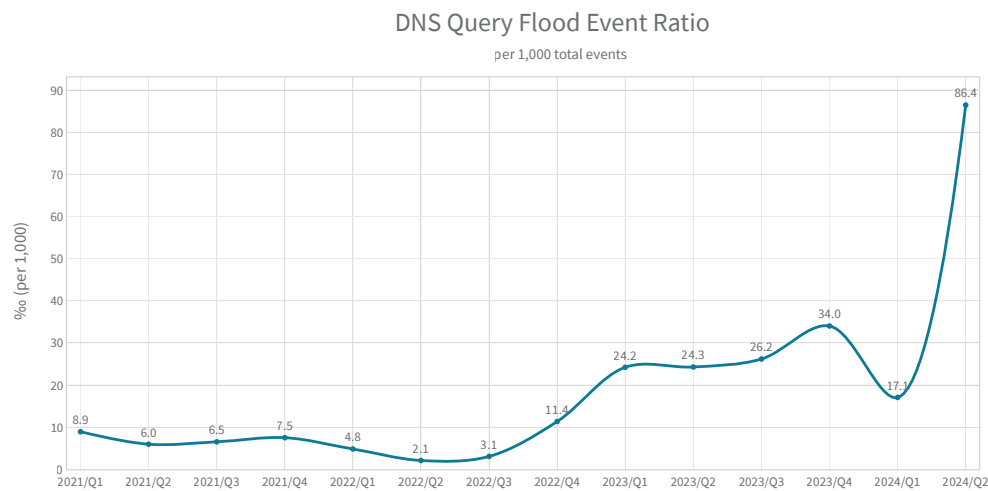


Figure 21 and **Figure 22** trace the evolution of blocked malicious DNS queries over time. The total number of malicious DNS queries surged in 2023, a trend that continued and accelerated during the first half of 2024. Compared to 2022, the number of malicious DNS queries increased by 2.680% in 2023. Subsequently, the total number of malicious DNS queries in the first six months of 2024 was already 76% higher compared to 2023.

Figure 21: Blocked malicious DNS queries per year (source: Radware)

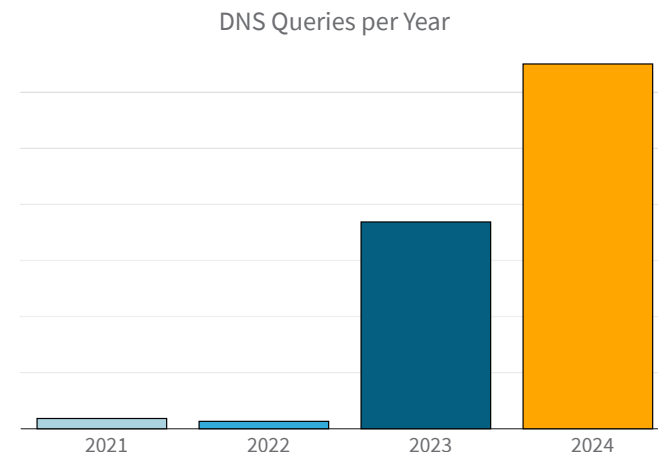
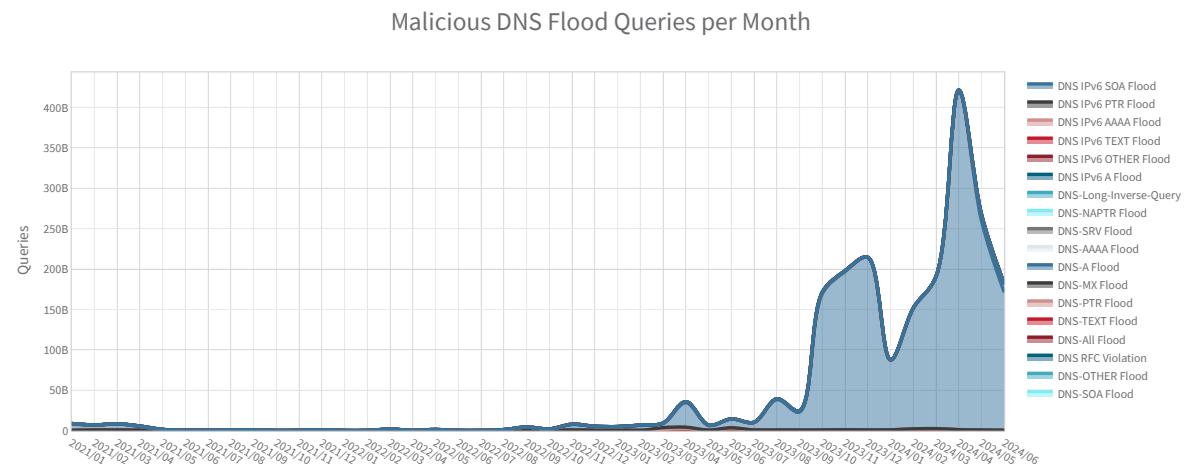
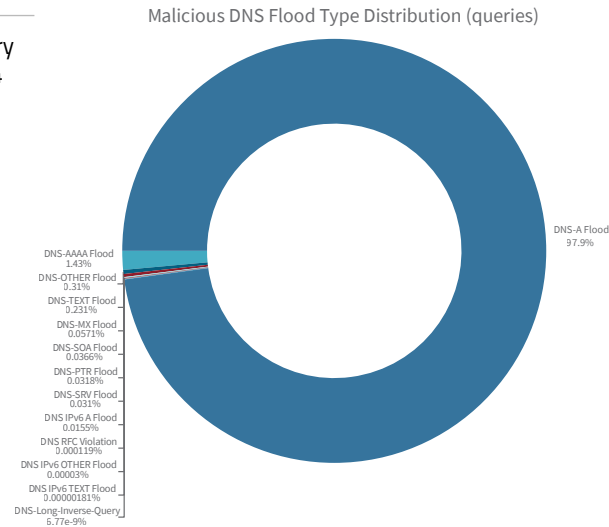


Figure 22: Blocked malicious DNS queries per month (source: Radware)



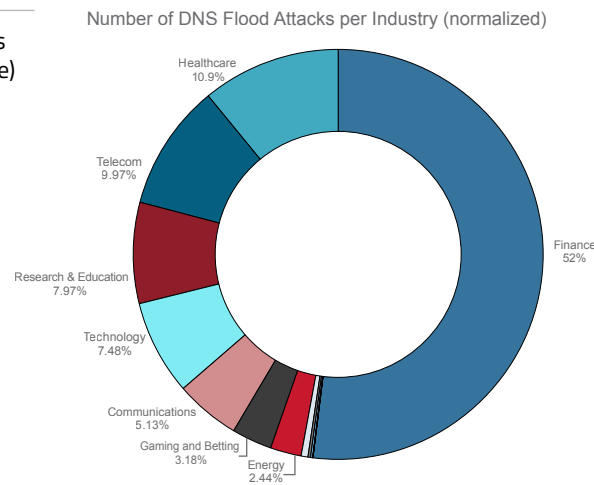
It is clear from **Figure 23** that the most common DNS query type of malicious DNS queries in H1 2024 was DNS-A (96%), followed by DNS-AAA (1.1%) by a significant margin. DNS-A queries request the address mapping record, also known as DNS host record, that stores the hostname and its corresponding IPv4 address. DNS-AAA queries are similar to DNS-A but for IPv6 addresses.

Figure 23: L7 DNS flood query type distribution for H1 2024 (source: Radware)



The most targeted industry by L7 DNS flood attacks in H1 2024 was finance 52%, followed by healthcare 11%, telecom 10%, research and education 8%, technology 7.5%, and communications 5%.

Figure 24: DNS Flood attacks per industry (source: Radware)



In H1 2024, finance was targeted by the most significant DNS query flood attack, which peaked at 811,000 QPS. Finance was also targeted by the largest DNS query flood attack in 2023, which then peaked at 2.15 million QPS.

In H1 2024, the largest attack targeting technology organizations peaked at 426,000 QPS. One government organization was targeted by an attack that peaked at 282,000 QPS.

By comparison, in 2023, the largest attack targeting a technology organization peaked at 495,000 QPS and the largest attack targeting a government organization peaked at 830,000 QPS.

Figure 25: Largest DNS query rate per industry for H1 2024 (source: Radware)

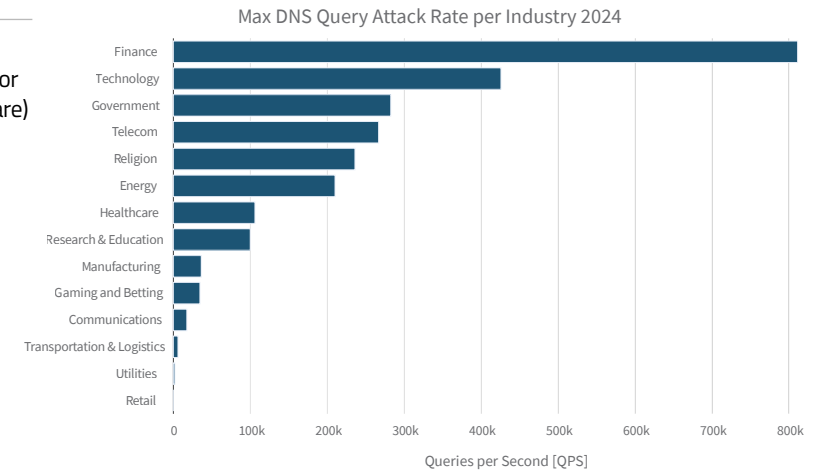
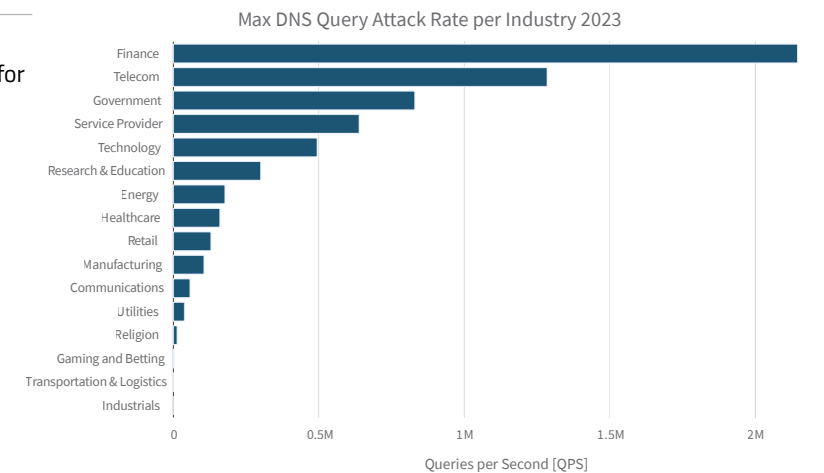


Figure 26: Largest DNS query rate per industry for 2023 (source: Radware)



Hacktivist DDoS Activity

Hacktivism is a phenomenon that can be motivated by various factors, including religious and political beliefs. While hackers 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.

Hackers 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, hackers 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 hackers 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 X. The IT Army of Ukraine Telegram channel has over 140,000 members and has become one of Telegram’s largest active hacker channels.

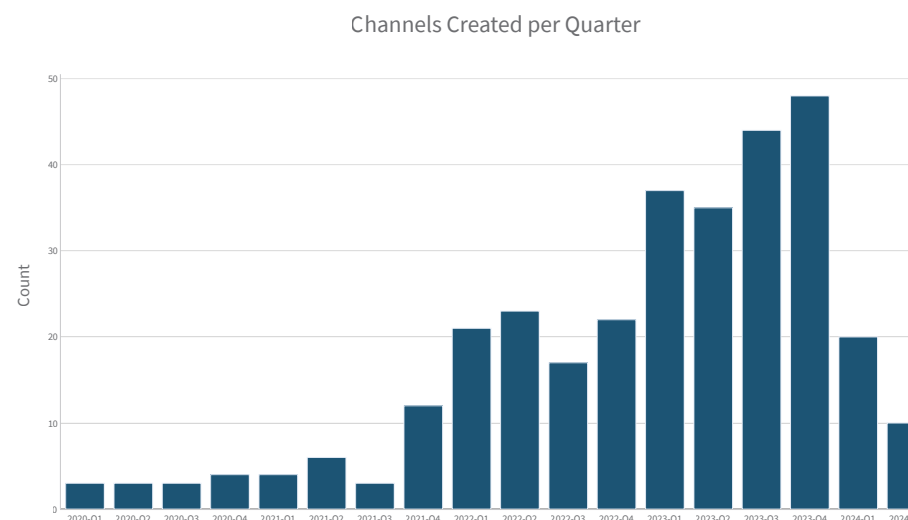
Telegram has taken on a pivotal role in the ongoing conflict between Russia and Ukraine, inspiring many other groups, hackers and others alike, to move to the platform. Telegram provides private and public channels and a standardized platform that allows forwarding and sharing of messages between channels. It also offers an easy means to create large follower groups and keep up to date with the latest security and hacking news.

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. They can do anything from chatbots to integration with other services outside of the Telegram platform, such as OpenAI, custom AI agent platforms, botnet C2 APIs, etc.

Some DDoS-for-hire services leverage Telegram as the new end-user interface, 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.

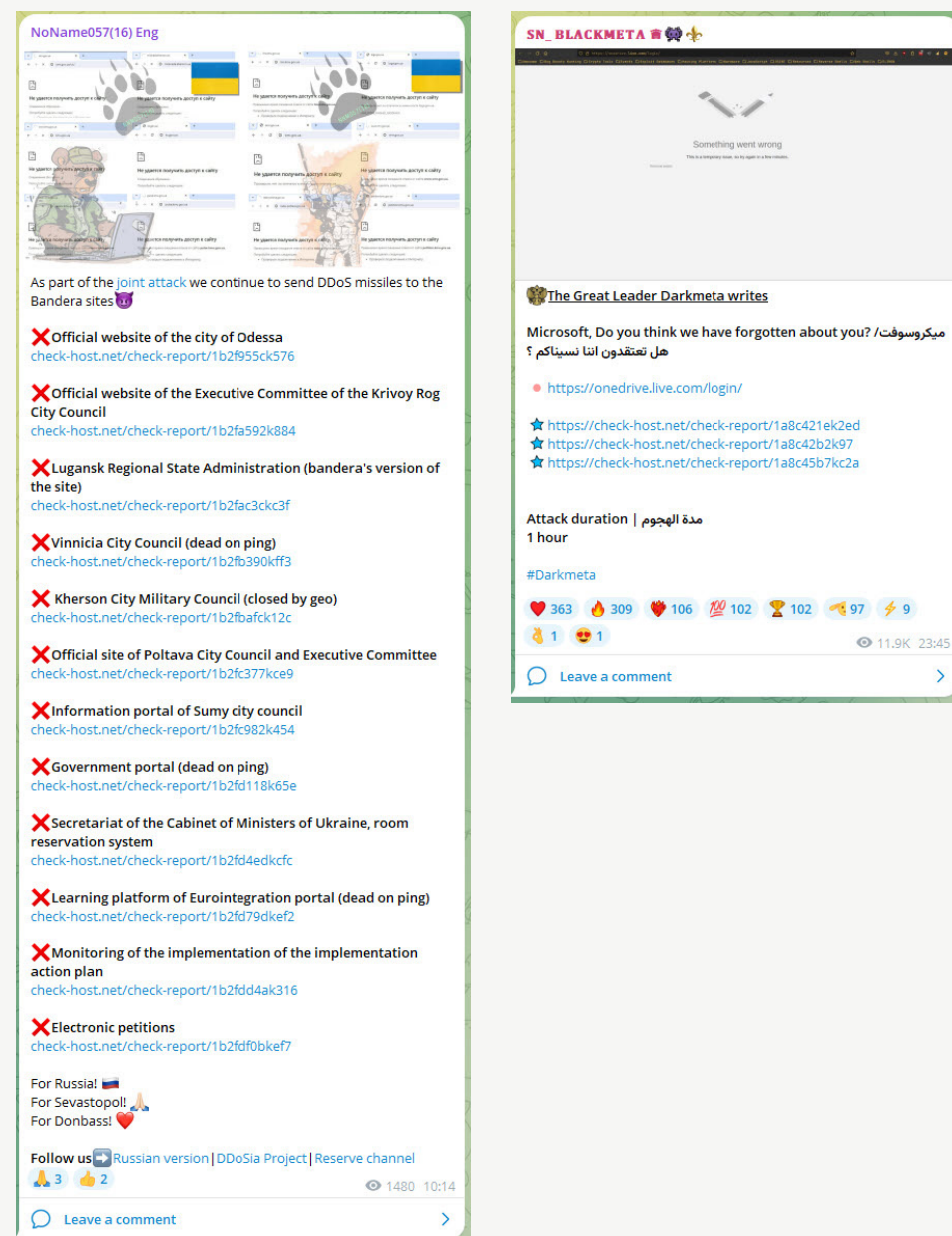
Figure 27: Hacker, botnet and hacktivist channels created on Telegram per quarter (source: Radware)



Hacktivist DDoS 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 messages with valid check-host links, we can monitor claimed attacks on Telegram with a higher degree of confidence. 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 that the targeted website was impacted by the DDoS attack attempt.

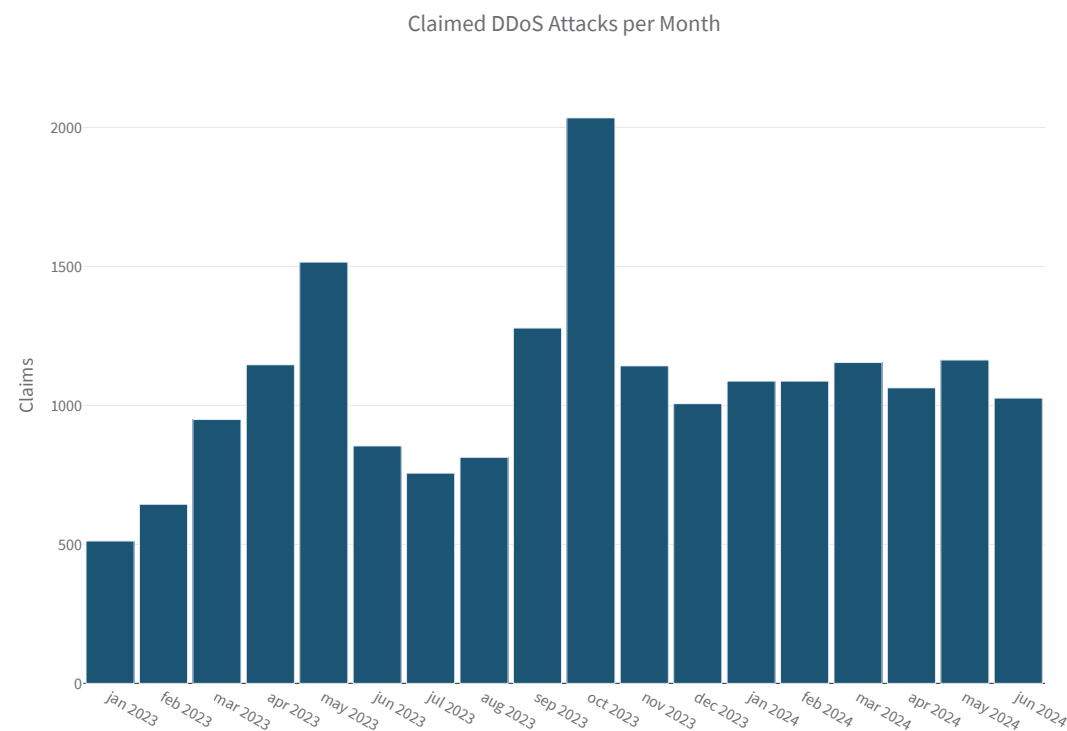
Figure 28: Examples of DDoS attack claims with check-host links (source: Telegram)



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 activist reports. **Figure 29** provides the number of unique DDoS attack claims per month across the 324 Telegram channels that we monitor. **Figure 27** shows the number of channels created per quarter. It clearly shows that most new channels were created in 2023 Q3 and Q4, a total of 92 channels.

In 2023, threat actors claimed 12,649 DDoS attacks on Telegram. During the first half of 2024, this number was 6,580. The activist landscape is a dynamic one: Many actors come, just as many leave, and some remove one channel only to create a new channel to clean out historical data and limit potential tracking of the channel by security researchers. The overall trend of activist-driven DDoS activity, however, remains mostly constant throughout 2024, hovering between 1000 and 1,200 claimed DDoS attacks per month. In 2023, two events generated a surge in activity across the activist landscape. First was the yearly #OplIsrael campaign (OplIsrael 2023, OplIsrael 2024) led by several south-Asian pro-Muslim activists. The second and largest spike in activist activity was in the period following the conflict between Israel and Hamas, which made Israel the most targeted country in 2023 by pro-Palestinian activists and their supporters.

Figure 29: DDoS attacks claimed per month on Telegram (source: Radware)



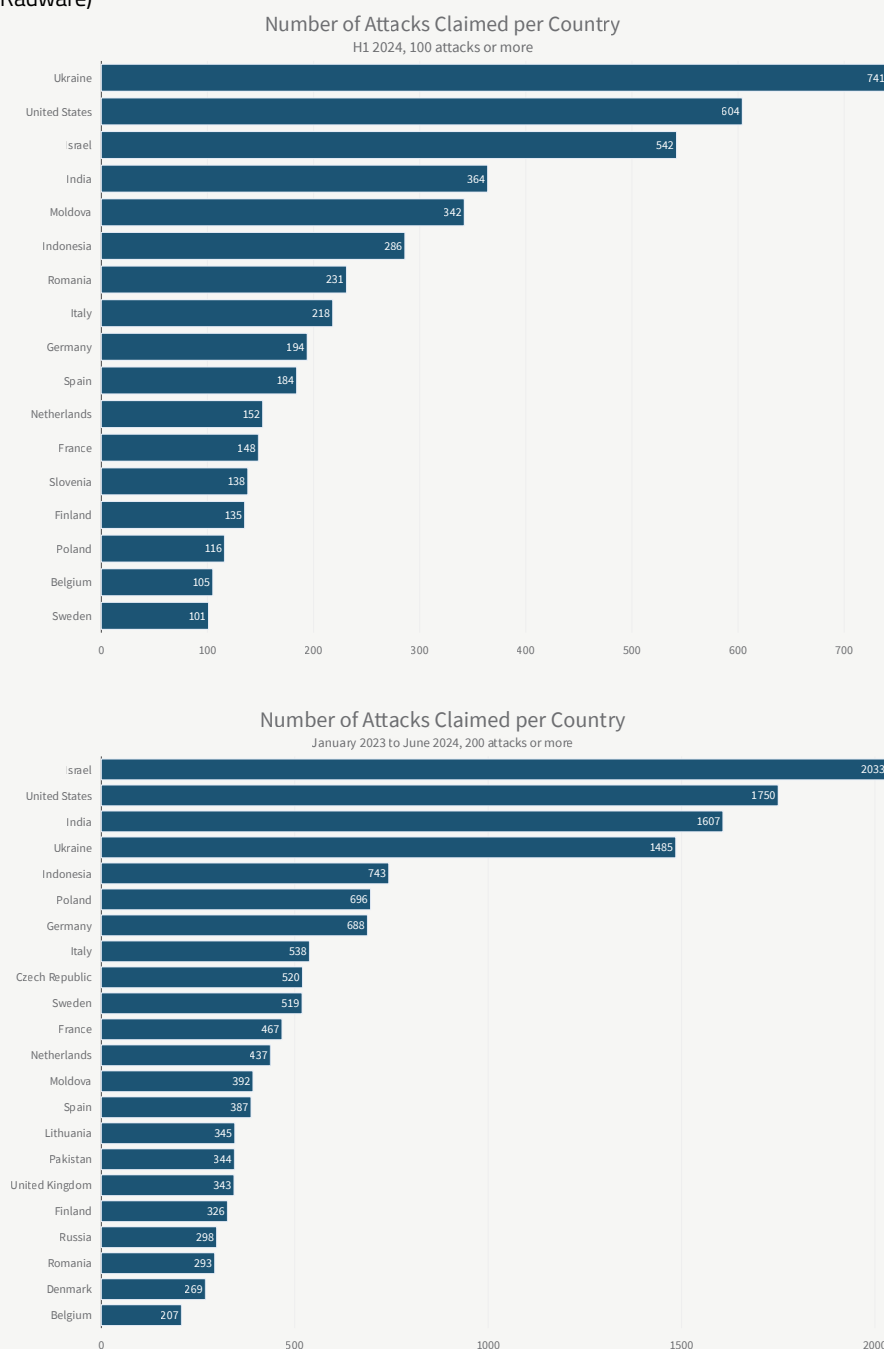
Most Targeted Countries and Top Claiming Actors

During the first half of 2023, India was the most targeted country. After the conflict with Hamas, however, a large number of pro-Palestinian hacktivists targeted Israel, making it the most targeted country of 2023, leaving India in second place. The United States was close behind India while Ukraine and Poland were the fourth and fifth most targeted countries in 2023.

During the first half of 2024, the pro-Russia hacktivist actor group NoName057(16) was observed joining and creating multiple alliances—some temporary, others more permanent. One of their collaborations, with the Cyber Army of Russia Reborn, resulted in a significant amount of attack activity targeting Ukraine, doubling the activity on Ukraine compared to what was observed in 2023 (741 attacks in H1 2024 vs 744 attacks in 2023). While Ukraine was only the fourth most targeted country in 2023 with 744 claimed attacks, it became the most targeted country during the first half of 2024 with 741 claimed attacks. Israel dropped to third place with 542 claimed attacks, followed by India with 364 claimed attacks. The United States was the second most targeted country during the first half of 2024 with 604 claimed attacks. Moldova, in fifth place, became an important target of pro-Russia hacktivists during the first half of 2024 and was targeted 342 times versus 50 times in 2023.

In 2024, in South Asia, India observed many claimed attacks from Indonesian and Bangladeshi hacktivists with Anonymous Susukan, Ketapang Grey Hat Team and Sylhet Gang claiming the most attacks. Pakistan was also one of the most frequently attacked countries and its activity consisted mostly of Indian hacktivists such as Team NWH, Dark Cyber Warrior, Kingsman, Hacktivist Vanguard and Team Network Nine.

Figure 30: Number of attacks claimed per country during H1 2024 and between 01/2023 and 06/2024 (source: Radware)



The United States became an important target for DDoS-as-a-service providers that like to leverage big, highly visible organizations as a target for their proof-of-capability advertisements. The Telegram groups Channel DDoS v2, ZeusAPI Services and Krypton Networks claimed the most attacks targeting the United States.

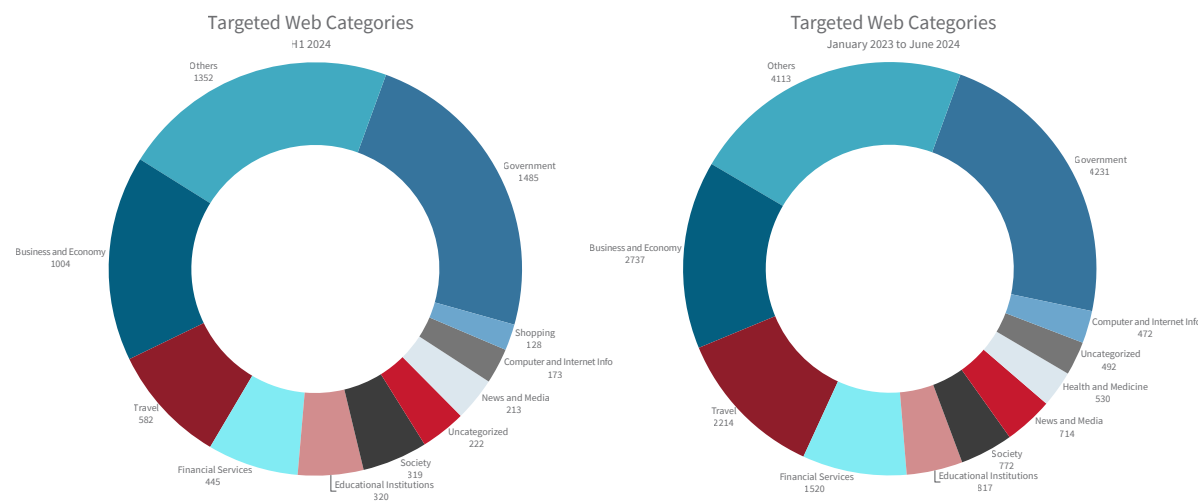
The top attacker collectives targeting Israel during the first half of 2024 included RipperSec, 1915 Team, Sylhet Gang, Anonymous Muslims, LulzSec Indonesia, Team ARXU, StarsX Team and Dark Storm Team.

NoName057(16), joined by the Cyber Army of Russia Reborn, Anonymous Russia and 62IX (346, 135, 63 and 61 claimed attacks, respectively), claimed more than 80% of the DDoS attack activity targeting Ukraine during the first half of 2024.

Top Targeted Websites and Domains

The distribution of the top targeted website categories in H1 2024 remained very consistent with the distribution in 2023. Government websites have been the most targeted since January 2023, especially in India, Ukraine, Israel, Moldova, Poland, Senegal and Spain. The top threat actor targeting government websites was, by a good margin, NoName057(16), which claimed 1,611 attacks on the government since January 2023, followed by Mysterious Team (225), Team Insane Pakistan (216) and Cyber Army of Russia Reborn (206).

Figure 31: Top targeted website categories during H1 2024 and between 01/2023 and 06/2024 (source: Radware)



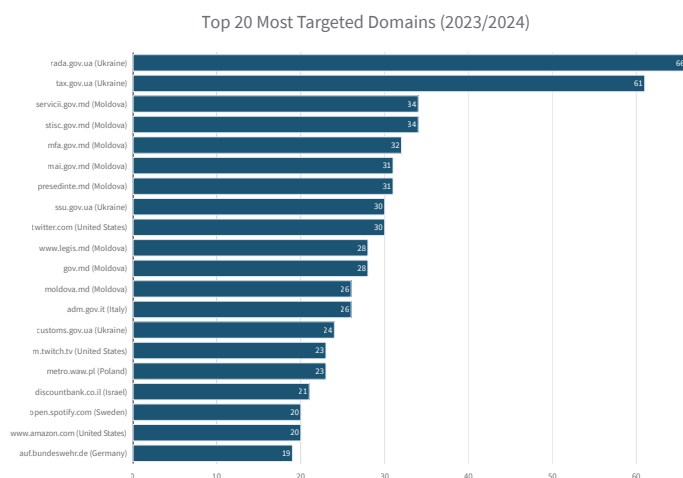
Business and economy websites, including e-commerce and the main websites of organizations, were mostly targeted by NoName057(16).

Travel websites were the third most targeted website category. These include airport and seaport information sites, and public transport sites providing train and bus ticketing and schedules. These are very visible to the citizens of a country and form a prominent target for patriotic hackers. Travel websites were predominantly targeted by pro-Russia hacker group NoName057(16) with 1,052 claimed attacks since January 2023.

Financial services, including online banking and payment services, were once again mostly targeted by NoName057(16) with 604 claimed attacks since January 2023.

Figure 32 lists the domains that were most targeted by hackers since January 2023. Most are government domains in Ukraine and Moldova. Other government domains in the top 20 were located in Italy and Germany. The Warsaw Metro in Poland was another significantly targeted domain, as was the domain of a bank in Israel. Rada.gov.ua and tax.gov.ua in Ukraine were by far the most targeted domains since January 2023 with 66 and 61 claimed attacks, respectively. Other notable top-targeted domains belong to X (former twitter.com), which was targeted 30 times, Twitch (23 times), Amazon (20 times) and Spotify (20 times).

Figure 32: Top 20 most targeted domains (source: Radware)

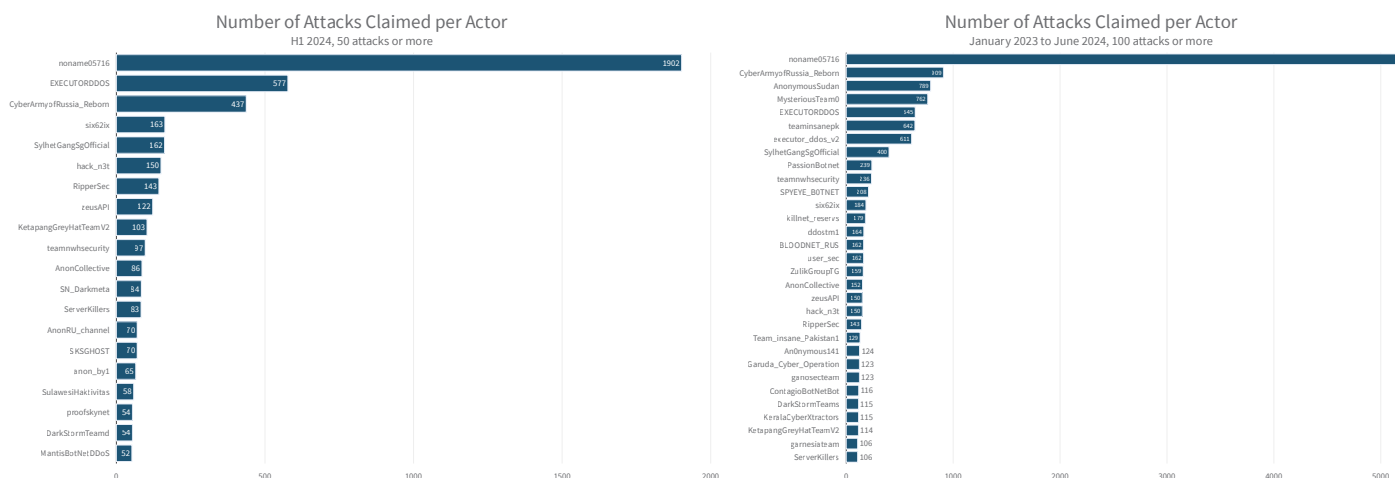


Top Claiming Actors

It should be no surprise by now that NoName057(16) is the top claiming threat actor. With a total of 5,287 DDoS attack claims since January 2023, of which 1,902 claims took place in the first half of 2024, NoName057(16) leaves the other actors behind by a significant margin. The Cyber Army of Russia Reborn, Anonymous Sudan, Mysterious Team0, Executor DDoS and Team Insane PK have been the most active threat actors since January 2023.

62IX, Sylhet Gang, Hacknet and RipperSec were among the most notable hacktivist groups in the first half of 2024 alone.

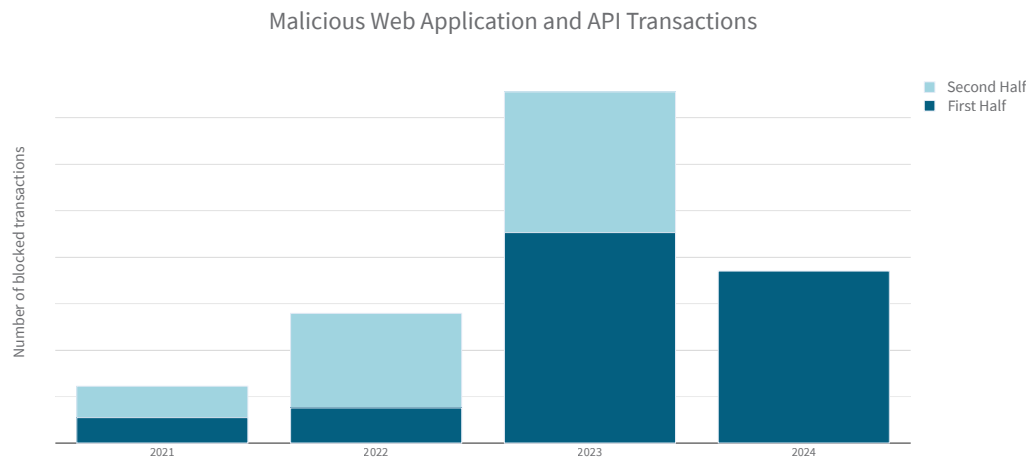
Figure 33: Number of attacks claimed per threat actor during H1 2024 and between 01/2023 and 06/2024 (source: Radware)



Web Application and API Attack Activity

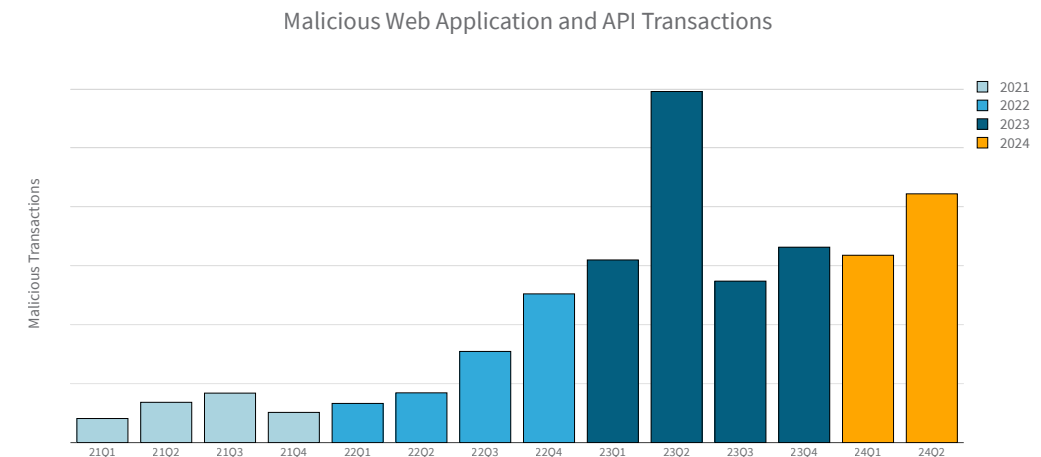
The number of web application and API attacks mitigated in the first half of 2024 increased by 22% compared to the second half of 2023. The total number of malicious transactions in the first six months of 2024 represents 49% of the total number of malicious transactions observed in 2023. Note that the number of malicious web application and API transactions before Q3 2023 included a significant amount of Web DDoS attack activity. Starting Q3 2023, the number of malicious transactions represents only exploits, violations and leaks. This biases any comparisons with the first half of 2023. Starting in 2024, Web DDoS attacks are discussed in a separate, dedicated section of the report (see “Web DDoS Attack Activity”).

Figure 34: Malicious web application and API transactions per year (source: Radware)



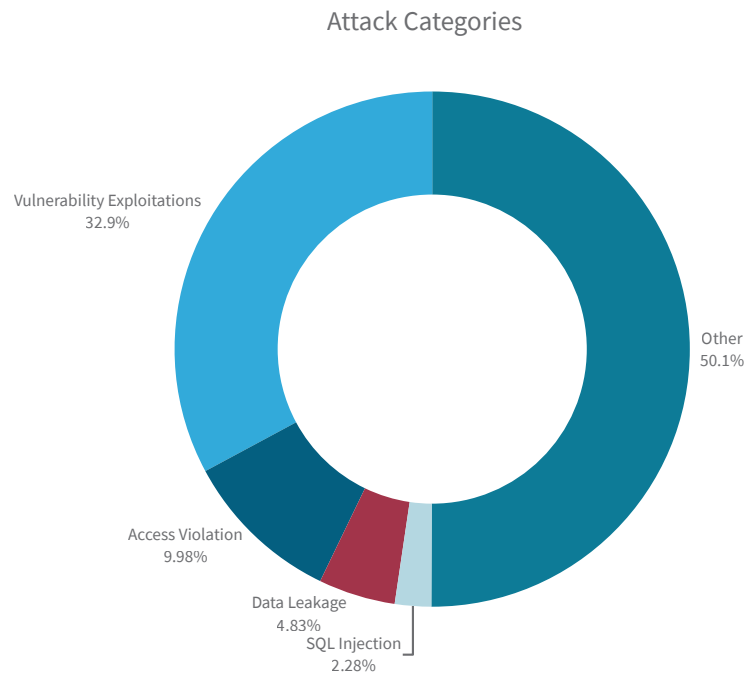
As shown in **Figure 35**, the drop in observed malicious web application transactions in Q3 of 2023, Q4 of 2023 and the first half of 2024 is attributed to a new layer of defense introduced in Radware’s Cloud Protection Services. Following the large increase in the number and sophistication of Web DDoS 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, ultra-sophisticated 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 significant decrease in the number of recorded malicious web application transactions, which now comprise only exploits and leaks. Before Q3 2023 tracking of malicious transactions also included Web DDoS transactions.

Figure 35: Malicious web application and API transactions per quarter (source: Radware)



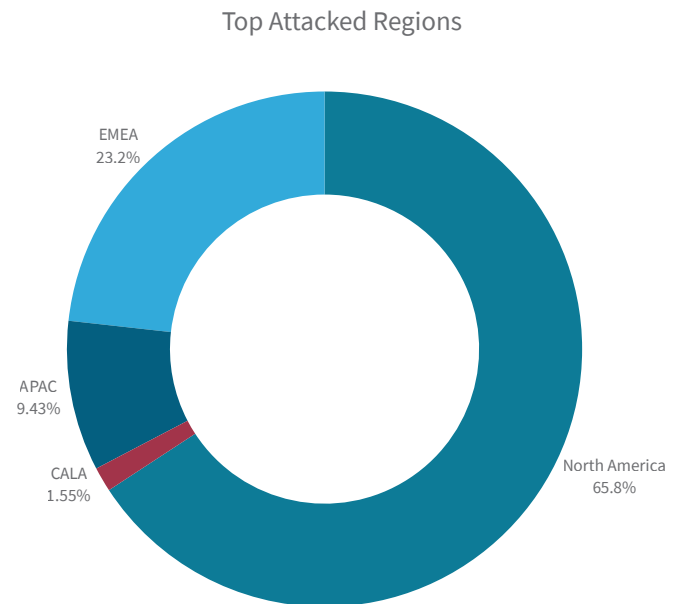
The most important attack category for 2024 (**Figure 36**) was vulnerability exploitation, representing a third of all malicious web requests. Access violations account for a tenth of all malicious web requests and include predictable resource location attacks that target hidden content and functionality 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. Data leaks and SQL injection attacks accounted for 4.8% and 2.3%, respectively, of the malicious activity.

Figure 36: Top web application attack categories (source: Radware)



The majority of web attacks (66%) targeted applications and APIs located in North America. Applications in EMEA accounted for 23% of the attack activity in the first half of 2024.

Figure 37: Top attacked regions (source: Radware)



Bad Bot Activity

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 and leaked 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 that 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.

The number of bad bot transactions increased by 61.25% compared to the first half of 2023. Compared to the second half, the number of bad bots slightly reduced by 8.85%. It is not uncommon to see higher bad bot transactions during periods of promotion, like Black Friday, Cyber Monday and the holidays. Given the large increase in the first half of 2024, expect to see more activity in the second half, especially during these same times.

Figure 38: Bad Bot transactions per year (source: Radware)

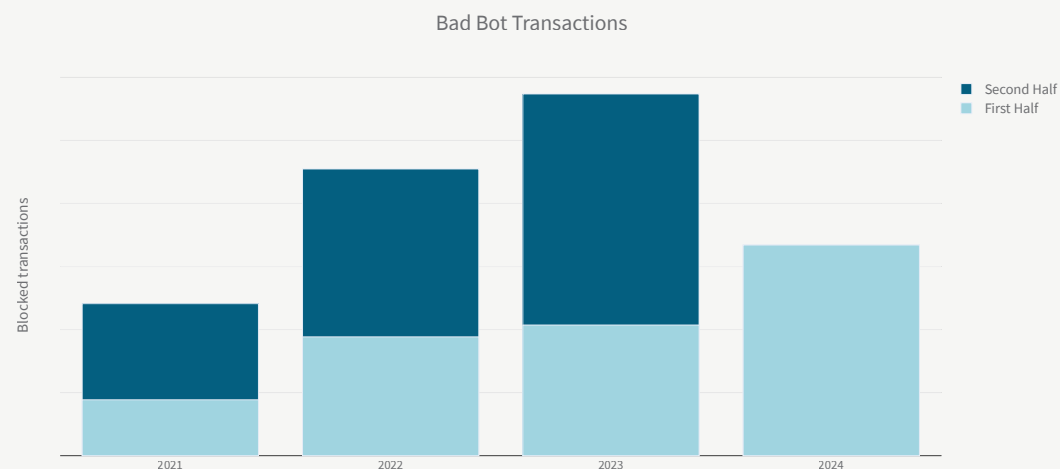
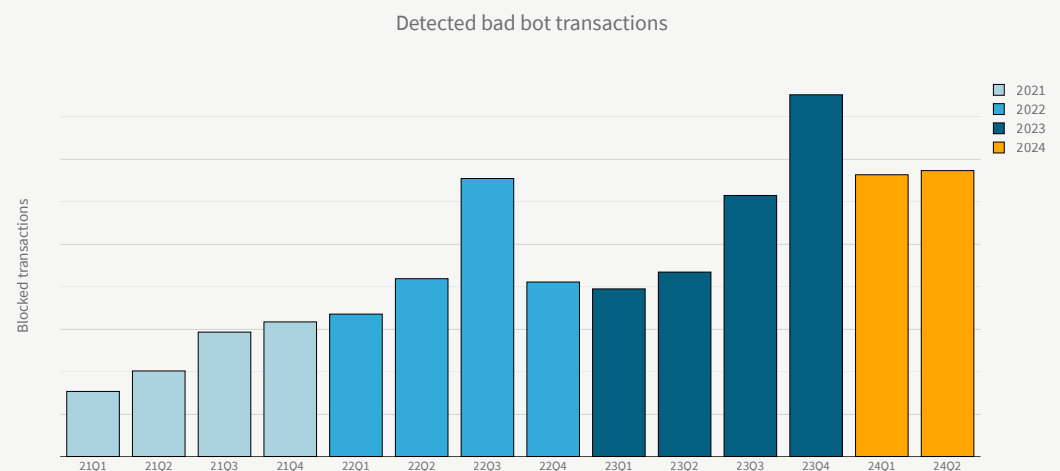


Figure 39: Bad Bot transactions per quarter (source: Radware)



The fraction of crawlers detected in 2021 was below 4% of all inspected web transactions. In 2023, this fraction increased to almost 7% before leveling off to 5.8% in the first half of 2024. The increase of the density of crawlers over the years could mean a relative increase in malicious actors scanning for hidden content and sensitive data such as configuration files, password files and API keys that were left unprotected. It can also indicate an increase in the overall indexing activity from good bots. Lately, there has been a lot of discussion and controversy around the intensity of scanning and scraping internet content by generative AI providers.

North America was the most targeted region in the first half of 2024, representing almost half of all bad bot transactions. APAC and EMEA each represented about 20% of the bad bot transactions, while websites and APIs in CALA accounted for 12% of the bad bot transactions.

Figure 40: Yearly evolution of the fraction of crawlers detected in web traffic (source: Radware)

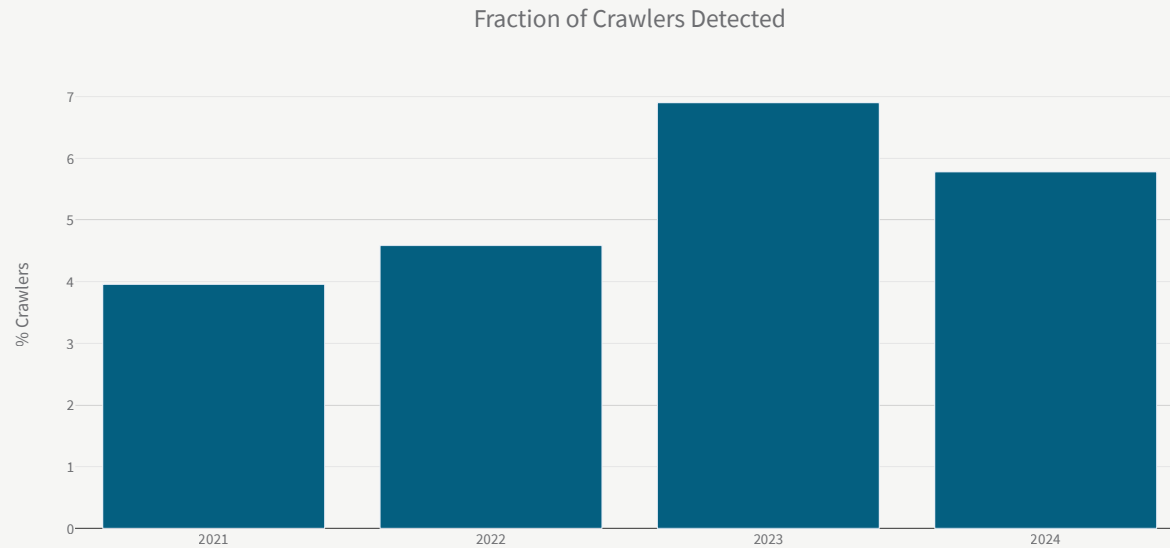
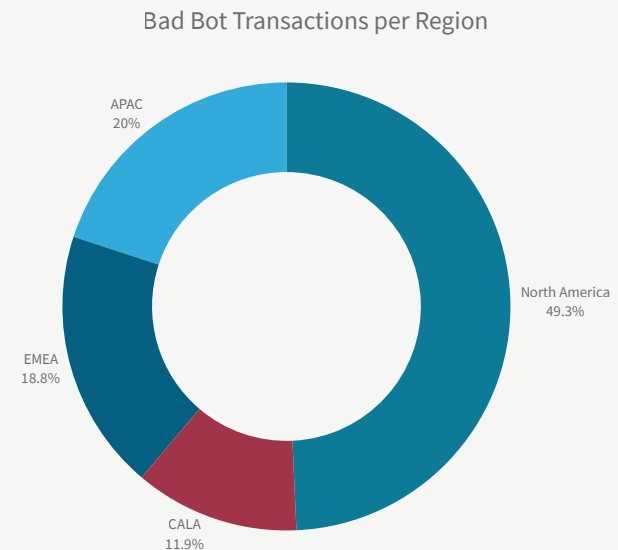


Figure 41: Bad bot transactions per region (source: Radware)



Appendix A: Characteristics of Common DDoS Amplification Vectors

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
RDP	80x	UDP/3389
CoAP	30x	UDP/5683
mDNS	5x	UDP/5353
WSD	500x	UDP/3702, TCP/3702
Plex (PMSSDP)	5x	UDP/32410

Table of Figures

Figure 1: Statistics of each wave of the six-day Web DDoS attack campaign (source: Radware).....	5
Figure 2: Number of Web DDoS attacks mitigated per quarter (source: Radware).....	6
Figure 3: Web DDoS attack size (RPS) distribution per year (source: Radware).....	6
Figure 4: Geographical distribution of Web DDoS attacks (source: Radware).....	7
Figure 5: Network-layer DDoS attacks mitigated per organization by year (source: Radware).....	8
Figure 6: Network-layer DDoS attacks mitigated per organization by the end of H1 2024 (source: Radware).....	8
Figure 7: Network-layer DDoS volume blocked per organization by year (source: Radware).....	8
Figure 8: 2024 H1 network-layer DDoS attacks and volume per region (source: Radware).....	9
Figure 9: Network-layer DDoS attacks mitigated per organization located in the Americas region (source: Radware).....	10
Figure 10: Network-layer DDoS volume blocked per organization located in the Americas region (source: Radware).....	10
Figure 11: Network-layer DDoS attacks mitigated per organization located in EMEA (source: Radware).....	11
Figure 12: Network-layer DDoS volume blocked per organization located in EMEA (source: Radware).....	11
Figure 13: Network-layer DDoS attacks mitigated per organization located in APAC (source: Radware).....	12
Figure 14: Network-layer DDoS volume blocked per organization located in APAC (source: Radware).....	12
Figure 15: Most attacked industries (source: Radware).....	13
Figure 16: Top network-layer DDoS attack vectors (source: Radware).....	14
Figure 17: Top network-layer DDoS protocols (source: Radware).....	14
Figure 18: Top network-layer DDoS amplification vectors (source: Radware).....	15
Figure 19: Top targeted application by network-layer DDoS attacks (source: Radware).....	15
Figure 20: DNS flood attack vector ratio evolution over time (source: Radware).....	17
Figure 21: Blocked malicious DNS queries per year (source: Radware).....	17
Figure 22: Blocked malicious DNS queries per month (source: Radware).....	17
Figure 23: L7 DNS flood query type distribution for H1 2024 (source: Radware).....	18
Figure 24: DNS Flood attacks per industry (source: Radware).....	18
Figure 25: Largest DNS query rate per industry for H1 2024 (source: Radware).....	18
Figure 26: Largest DNS query rate per industry for 2023 (source: Radware).....	18
Figure 27: Hacker, botnet and hacktivist channels created on Telegram per quarter (source: Radware).....	19
Figure 28: Examples of DDoS attack claims with check-host links (source: Telegram).....	20
Figure 29: DDoS attacks claimed per month on Telegram (source: Radware).....	21
Figure 30: Number of attacks claimed per country during H1 2024 and between 01/2023 and 06/2024 (source: Radware).....	22
Figure 31: Top targeted website categories during H1 2024 and between 01/2023 and 06/2024 (source: Radware).....	23
Figure 32: Top 20 most targeted domains (source: Radware).....	24
Figure 33: Number of attacks claimed per threat actor during H1 2024 and between 01/2023 and 06/2024 (source: Radware).....	24
Figure 34: Malicious web application and API transactions per year (source: Radware).....	25
Figure 35: Malicious web application and API transactions per quarter (source: Radware).....	25
Figure 36: Top web application attack categories (source: Radware).....	26
Figure 37: Top attacked regions (source: Radware).....	26
Figure 38: Bad Bot transactions per year (source: Radware).....	27
Figure 39: Bad Bot transactions per quarter (source: Radware).....	27
Figure 40: Yearly evolution of the fraction of crawlers detected in web traffic (source: Radware).....	28
Figure 41: Bad bot transactions per region (source: Radware).....	28

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 from the same attack correspond to that attack's attack volume.

The data for web application attacks and bot activity 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 ERT SOC incidents relating to the **Web DDoS Protection Service**.

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 Cyber Threat Intelligence
Arik Atar | Senior Cyber Threat Intelligence Researcher

Executive Sponsors

Ron Meyran | VP Strategic Alliances Marketing & Cyber Threat Intelligence
Deborah Myers | Senior Director of Corporate Marketing

Production

Jeffrey Komanetsky | Content Development Manager
Kimberly Burzynski | Senior Marketing Communication 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.

THIS REPORT CONTAINS ONLY PUBLICLY AVAILABLE INFORMATION, WHICH IS PROVIDED FOR GENERAL INFORMATION PURPOSES ONLY. ALL INFORMATION IS PROVIDED "AS IS" WITHOUT ANY REPRESENTATION OR WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES THAT THIS REPORT IS ERROR-FREE OR ANY IMPLIED WARRANTIES REGARDING THE ACCURACY, VALIDITY, ADEQUACY, RELIABILITY, AVAILABILITY, COMPLETENESS, FITNESS FOR ANY PARTICULAR PURPOSE OR NON-INFRINGEMENT. USE OF THIS REPORT, IN WHOLE OR IN PART, IS AT USER'S SOLE RISK. RADWARE AND/OR ANYONE ON ITS BEHALF SPECIFICALLY DISCLAIMS ANY LIABILITY IN RELATION TO THIS REPORT, INCLUDING WITHOUT LIMITATION, FOR ANY DIRECT, SPECIAL, INDIRECT, INCIDENTAL, CONSEQUENTIAL, OR EXEMPLARY DAMAGES, LOSSES AND EXPENSES ARISING FROM OR IN ANY WAY RELATED TO THIS REPORT, HOWEVER CAUSED, AND WHETHER BASED ON CONTRACT, TORT (INCLUDING NEGLIGENCE) OR OTHER THEORY OF LIABILITY, EVEN IF IT WAS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, LOSSES OR EXPENSES. CHARTS USED OR REPRODUCED SHOULD BE CREDITED TO RADWARE