radware

Report

2025 Global Threat Analysis Report

Analysis of the Global Network and Application Attack Trends of 2024

Table of Contents

Executive Summary

A sharp escalation in both the frequency and sophistication of cyberattacks marked the 2024 cybersecurity landscape with distributed denial of service (DDoS) incidents leading the charge. Major geopolitical events—ranging from the Russia-Ukraine conflict to elections in India and the European Union (EU)—served as catalysts for a growing wave of targeted attacks. Simultaneously, hacktivist alliances leveraged emerging communication platforms like Telegram to coordinate large-scale campaigns, even as these channels came under heightened scrutiny and partial shutdowns. Beyond DDoS, web application and API threats grew significantly, fueled by advanced methods of vulnerability exploitation, widespread use of shadow and zombie APIs and increasingly automated and artificial intelligence-driven hacking techniques. The integration of AI itself into cyber operations has introduced both opportunities and challenges. Threat actors have leveraged AI to enhance the sophistication of attacks, including the use of generative AI models to craft convincing phishing lures and develop malware. This evolution has lowered the barrier to entry for aspiring threat actors, made social engineering attacks more effective and helped seasoned threat actors more accurately identify system vulnerabilities.

The DDoS Threat Landscape

Escalation of Web DDoS Attacks

Web DDoS attacks escalated significantly, increasing almost 550% year-over-year compared to 2023. The intensity of these attacks grew exponentially during the first half of the year and plateaued at high levels during the second half, reflecting a sustained and aggressive threat environment. Use of advanced Layer 7 (L7) DDoS attacks became a prominent tactic, leveraging vulnerabilities such as the HTTP/2 Rapid Reset and Continuation Flood to target online applications with increasing sophistication. Notable incidents included a six-day attack on a financial institution in the Middle East, which peaked at 14.7 million requests per second (RPS), and another attack on a major institution that reached 16 million RPS.

Europe, the Middle East, and Africa (EMEA) remained the primary target for Web DDoS attacks, accounting for 78% of global incidents. Political tensions such as the Russia-Ukraine conflict, combined with EU elections and various international sporting events, provided ample impetus for threat actors to strike at high-value targets. Elsewhere, Asia-Pacific (APAC) saw DDoS activity climb to 8% of the global total.

Network DDoS Evolution

Network DDoS attacks in 2024 witnessed significant upticks in intensity and duration. The average mitigated attack volume per customer doubled compared to 2023, contributing to an overall 120% rise in total volume. The average duration continued to grow considerably in 2024 with a 37% increase over 2023. The average attack frequency, volume and duration have all more than doubled since 2022.

"Low and slow" attack strategies, designed to evade detection, increased by 38% and lasted an average duration of 9.7 hours in 2024, more than doubling the average duration of 4.6 hours in 2023.

The year 2024 witnessed an unprecedented amount of DNS query flood denial of service attacks, which surpassed the previous year by 87%. This marked 2024 as another pivotal year in the evolution of cyberthreats and, more specifically, L7 DNS DoS attacks. The financial sector bore the brunt of this continued evolution, accounting for 44% of the total L7 DNS attack activity. Other significantly affected sectors included healthcare (13%) and telecom (10%).

UDP and DNS amplification attacks continued to dominate volumetric DDoS methods with DNS amplification alone accounting for 65% of all amplification-based attacks.

Organizations in Europe faced the highest proportion of network DDoS activity, accounting for 44.5% of the global attack volume and 32.5% of the total malicious packets. North American organizations were the second most targeted by volume, experiencing 21% of global attack traffic. The Middle East ranked as the second most targeted by packets, intercepting 24% of global malicious packets. Organizations in Oceania faced the highest average network DDoS volume and packet counts per customer.

Telecommunications faced 43% of global network DDoS volume. Finance followed at 30%, experiencing the steepest growth in attack volume per customer at 393% year-over-year—more than twice the global average growth of 120%. Technology absorbed 11% of the global network DDoS attack volume, while transportation, e-commerce and government services also observed notable surges.

The United States emerged as both the leading attacker and target of network-layer traffic, reflecting a potentially significant DDoS resource presence and the attractiveness of U.S. assets to global adversaries. For both top attacking and most targeted countries, United States and Israel, the majority of the attack volume originated from infrastructure and bots inside the country. While the threat from inside the country is significant, still 12% of all malicious network DDoS packets were mitigated by geo-blocking.

DDoS-for-hire Services

The rise of DDoS-for-hire platforms has further democratized access to potent offensive capabilities, lowering the technical threshold required to launch large-scale attacks. These services have contributed to an increase in application-layer DDoS assaults, which are generally more challenging to detect and mitigate than network-layer attacks.

Hacktivism and Alliances

Hacktivist Motivations and Targets

Throughout 2024, hacktivism remained a leading driver of cyberattacks, propelled by political and ideological tensions. The total number of claimed DDoS attacks on Telegram increased by 20% compared to 2023. Ukraine topped the list of targeted nations, with 2,052 claimed attacks, predominantly orchestrated by pro-Russian groups such as NoName057(16), which boasted 4,767 claims. High-profile events like India's national elections in June sparked further activity, as cyber vigilantes on both sides used DDoS and data exfiltration attacks to advance political agendas.

Government institutions remained the primary target of attacks since January 2023, representing 20% of hacktivist activity in 2024. E-commerce platforms and organizational websites were also heavily targeted (9%), as well as the financial sector (8.9%) and other industries including transportation (7%), media and internet (7%), and manufacturing (6.9%). NoName057(16) consistently emerged as the primary threat actor across all the most targeted sectors.

Alliances and Collaboration

Despite historically operating as "lone wolves," even groups like NoName057(16) have begun forming strategic alliances. Notably, pro-Russian and pro-Palestinian hacktivists joined forces in coordinated campaigns to strike common perceived adversaries. These alliances boosted operational capabilities, often resulting in multi-vector attacks that fused techniques and resources from multiple collectives.

The Role of Telegram

In 2024, Telegram acted as a primary coordination and communication hub for hacktivist groups, largely due to its anonymity features and lenient moderation. Following the arrest of its founder and CEO, Pavel Durov, in August 2024, Telegram increased its cooperation with law enforcement and stepped up moderation efforts, as evidenced by a surge in data-sharing with authorities. For instance, it fulfilled 900 U.S. government requests in the latter half of 2024. Concurrently, the European Union restricted certain Telegram channels deemed to violate EU laws, including Russian state-owned news and hacktivist channels like the Pro-Palestinian Hacker Movement (PPHM).

Despite the heightened scrutiny, Telegram remains vital for hacktivist operations. Some prominent channels—such as those of NoName057(16) and CARR (Cyber Army of Russia Reborn)—were banned, not through official moderation but seemingly via ban-spamming attacks from rival groups.

Meanwhile, Telegram's bot automation and cryptocurrency services have encouraged the rise of DDoS-as-a-service offerings, letting individuals hire attacks through Telegram bots that handle real-time commands, scheduling and payments. This ecosystem has made it alarmingly easy for users with minimal technical skills to launch or commission DDoS attacks, further cementing Telegram's role in the global hacktivist and cybercriminal landscape.

Web Application and API Threats

Rapid Expansion of Attacks

In 2024, the rise of Web application and API attacks continued, increasing 41% over 2023. Vulnerability exploitation remained the most prominent attack type, comprising one-third of all malicious requests. North America experienced 66% of these attacks, followed by EMEA at 26%, highlighting a strong concentration of targeted applications in developed markets.

Surge in API Exploitation

Because of their broad adoption, APIs now represent a substantial portion of online web application traffic and have become prime targets. Their inherently automated nature—which requires no human intervention—makes them especially vulnerable to automated assaults. Threat actors increasingly exploit this vulnerability to compromise the business logic or core functionality of APIs. By emulating legitimate automated API requests, these attacks often go unnoticed, allowing malicious actors to operate without disruption.

Shadow and Zombie APIs

The rapid pace of development and innovation in online applications has given rise to numerous APIs that either lack proper documentation (shadow APIs) or are outdated and no longer actively maintained (zombie APIs). These unmanaged and often overlooked endpoints serve as enticing entry points for unauthorized access, significantly increasing the risk of data breaches. For security teams, these neglected APIs create critical blind spots, undermining their ability to maintain a comprehensive defense. Cybercriminals are increasingly exploiting these vulnerabilities, using shadow and zombie APIs to establish an initial foothold in systems or to stealthily exfiltrate sensitive information, often remaining undetected for extended periods. As a result, these hidden gateways have become high-priority targets in the evolving threat landscape.

Advanced Attack Techniques

Business logic vulnerabilities have already found their place among the OWASP Top Ten API Security Risks and they are among the HackerOne Top Ten Vulnerability Types, which is based on bug bounty reports. Cybercriminals continually advance their tactics while researchers demonstrate practical use cases for emerging attack methodologies such as web timing attacks.

The Bad Bot Threat

Growing Proportions and Sophistication

Bad bot activity grew significantly in 2024, with a 35% increase in malicious transactions compared to 2023, following a 26% rise in 2023 relative to 2022. Bad bot activity is consistently higher in the second half of the year, an observation that aligns with high-traffic periods such as Black Friday, Cyber Monday and the winter holiday season when promotional campaigns and increased online activity make platforms more susceptible to such transactions.

Bad bots, responsible for activities such as account takeover, fraud and web scraping, made up 71% of all bot traffic in 2024. North America emerged as the most targeted region, accounting for half of all bad bot transactions, while EMEA, APAC and CALA regions experienced lower but still notable levels of activity.

AI-Driven and "Grey" Bots

The surge in AI technologies gave rise to sophisticated "grey" bots, which aggressively scrape data to train AI models—often without explicit permission. AI is also rapidly becoming the next major focus for search engine optimization (SEO) strategies. With the rise of AI-driven tools like generative AI models, conversational AI and AI-powered search engines, the SEO landscape is evolving to prioritize content that aligns with AI processing and user behavior in AI-assisted searches. This adds a layer of ethical and operational complexity, as data owners grapple with how to protect their assets without hindering legitimate AI scrapers used for research and for SEO.

AI in Cybercrime

Advanced Phishing and Deepfakes

Cybercriminals utilized AI to generate highly persuasive phishing emails, text messages and even deepfake videos. This level of realism severely impedes an organization's ability to distinguish authentic communications from fraudulent ones. As the World Economic Forum warned, the prevalence of AI-driven social engineering demands robust awareness training and multi-layered defenses.

AI-Enhanced Attacks

Studies in 2024 showcased the potential for adaptive and self-learning capabilities in AI agents, enabling them to select the most promising exploits. By integrating AI, attackers can continuously test defenses, identify weaknesses, and generate and deploy customized payloads at unprecedented speed.

Offline AI Models: The New Frontier in Cyberattacks

The advent of downloadable, pre-trained AI models has transformed the cybersecurity landscape, enabling broader adoption and innovation in both defense and offense. Unlike traditional neural networks requiring significant resources, offline models are accessible and modifiable, presenting new security risks. While cloud-based AI systems maintain ethical safeguards, offline models can be exploited for malicious purposes. Tools like WormGPT and FraudGPT can be used to enhance malware or automate phishing campaigns. This underscores the ongoing technological race between cyber defenders and threat actors, as the potential for fully automated attack campaigns looms on the horizon.

Lowering the Barrier to Entry for New Cybercriminals

AI-based hacking resources became more accessible in 2024, lowering the barrier to entry for potential cybercriminals. A Bugcrowd study revealed that 71% of hackers felt AI boosted the "value" of hacking, up from 21% in 2023, while 77% reported using generative AI tools—up from 64% the previous year.

Direct Attacks on AI Systems

AI platforms themselves are high-value targets. By manipulating training data or forcing AI systems into unexpected behaviors, attackers can degrade service reliability or generate flawed outputs, raising concerns about data integrity and brand reputation.

Web DDoS Attack Activity

The prevalence of Web DDoS attacks has surged in the first half of 2024, driven by several evolving trends in the threat landscape. A significant portion of these attacks, particularly in Europe and the Middle East, can be linked to hacktivist groups fueled by political tensions in the regions. These groups have increasingly adopted sophisticated Layer 7 (L7) attack techniques to target online applications and their backend infrastructure. Since the onset of the conflict in Ukraine, hacktivists have grown more experienced and technically adept. Some have shifted their focus to financial gain, monetizing their non-volunteer-based botnets by renting them out to well-funded third parties.

The impact of this evolution is evident in the metrics recorded by Radware's Cloud Protection Services. From 2023 up to the first half of 2024, the volume of blocked Web DDoS attacks rose exponentially. In the second half of 2024, the increase stagnated but the number of Web DDoS attacks sustained. The rapid escalation in the first half and the continued high number of attacks in the second half highlight the growing intensity of Web DDoS threats in today's cyber landscape.

The number of Web DDoS attacks observed in the first half of 2024 surged by 246.46% compared to the latter half of 2023. In the final two quarters of 2024, the frequency of Web DDoS attacks stabilized at the elevated levels recorded in Q2 2024, resulting in a 33.42% increase in attack activity in the second half compared to the first half of the year. On a year-over-year basis, the total rise in Web DDoS attacks for 2024 was an astonishing 548.79% compared to 2023.

Since 2023, DDoS-for-hire platforms have started to shift their primary focus from traditional Layer 3/4 attack vectors to offer more potent L7 vectors. They were quick to exploit vulnerabilities like the HTTP/2 Rapid Reset flaw disclosed in October 2023 and the HTTP/2 Continuation Flood vector disclosed in April 2024. This shift has resulted in a dramatic increase in Web DDoS attack rates targeting online applications.

Figure 1: Number of Web DDoS attacks mitigated per quarter (source: Radware)

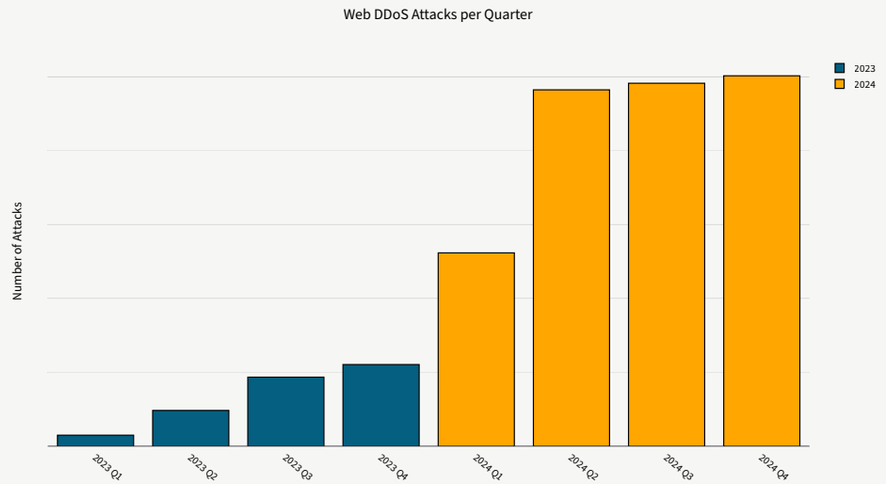
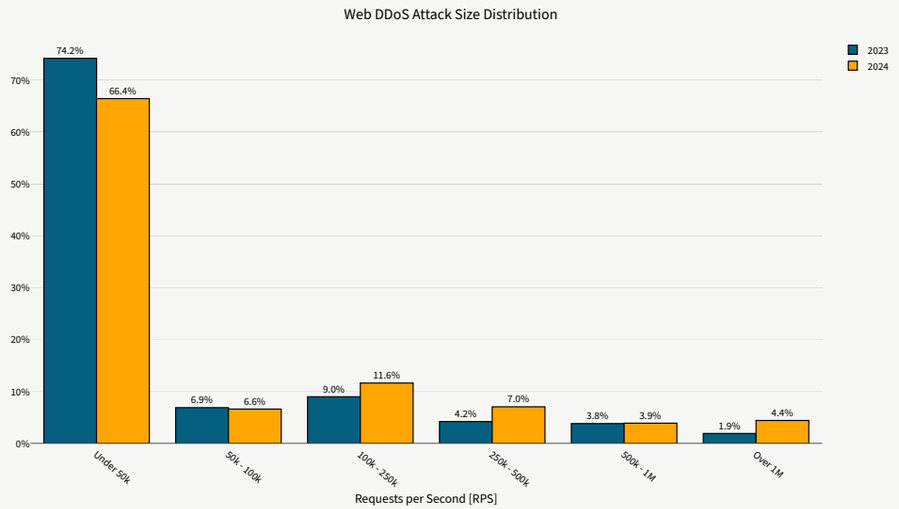


Figure 2: Web DDoS attack size (RPS) distribution per year (source: Radware)



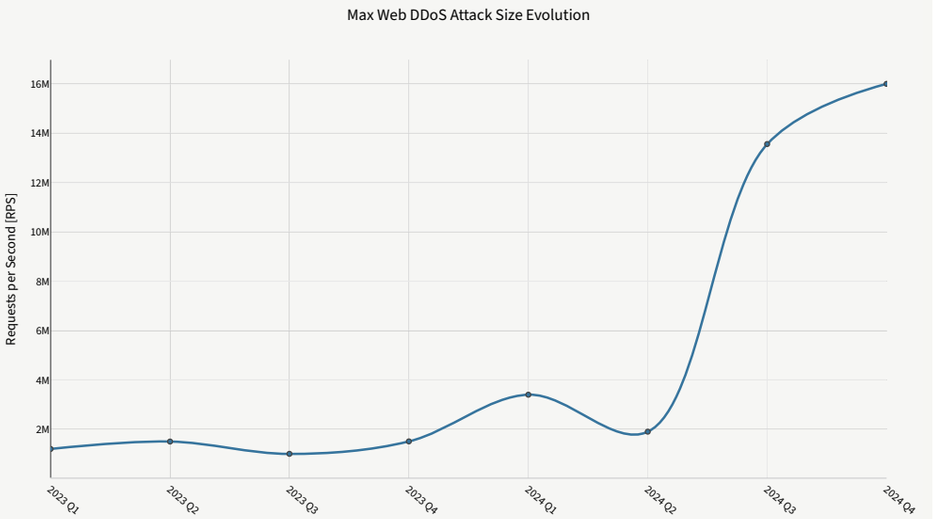
In 2024, Web DDoS attacks exceeding one million requests per second (RPS) accounted for 4.4% of all observed incidents, a significant increase from less than 2% in 2023. Meanwhile, the proportion of Web DDoS attacks with rates under 50,000 RPS dropped from 74% in 2023 to 66% in 2024, highlighting a shift toward higher-intensity attacks. This trend is further evident in the category of attacks ranging from 100,000 to 500,000 RPS, which made up nearly 19% of the total in 2024, up from 13% in the previous year.

Radware successfully mitigated two significant Web DDoS attacks targeting financial institutions in 2024, demonstrating the increasing scale and sophistication of such threats. In July 2024, a financial institution in the Middle East endured a relentless six-day Web DDoS attack campaign, characterized by ten waves lasting between four to 20 hours each, totaling 100 hours of attack time. The assault sustained an average of 4.5 million RPS, peaking at 14.7 million RPS. During the attack, the ratio of legitimate to malicious web requests was as low as 0.002%, averaging 0.12%. Radware's Web DDoS Protection Services effectively blocked over 1.25 trillion malicious requests while allowing 1.5 billion legitimate requests to pass through, ensuring uninterrupted service for the institution. The attack was attributed to SN_BLACKMETA, a pro-Palestinian hacktivist group with potential ties to Sudan.

In October 2024, a major financial institution faced a multi-million RPS Layer 7 DDoS attack during its morning business hours. The attack targeted a critical application used by the institution to shield its main systems from external traffic. This application acts as a gateway, ensuring that malicious requests from outside their core operational region are not impacting internal services. The attack peaked at 16 million RPS and encompassed over 6.5 billion total requests during its 16-minute duration. Attackers employed sophisticated techniques, including HTTP GET requests designed to appear legitimate, along with randomized headers, path parameters and user-agent strings to evade detection. Radware's advanced Web DDoS Protection automatically generated custom signatures tailored to the attack's unique patterns, enabling real-time adaptation without human intervention.

This proactive defense ensured that all malicious requests were blocked, legitimate traffic remained unaffected the institution experienced no downtime or service disruption.

Figure 3: Evolution of peak Web DDoS attack sizes over time (source: Radware)



On a year-over-year basis, the total rise in Web DDoS attacks for 2024 was an astonishing 548.79% compared to 2023.

Geographical Activity

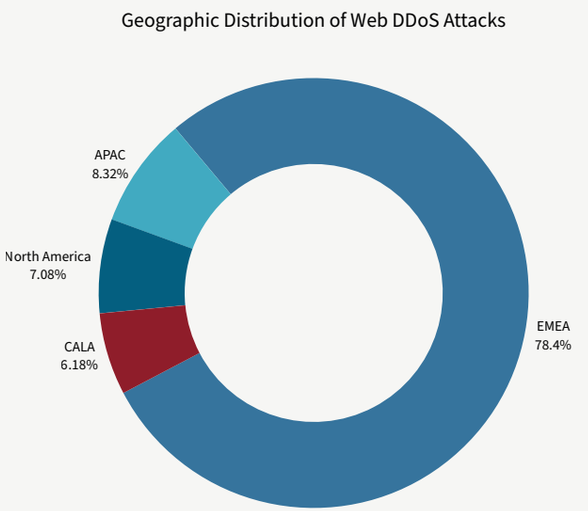
As significant geopolitical tensions continue in Europe, the Middle East and Africa, these regions have increasingly become focal points for political cyber activism as well. In Europe, hacktivist activities have been observed in response to the Russia-Ukraine conflict, instantiating numerous cyber operations targeting governmental and private sector entities, aiming to disrupt services and disseminate propaganda. Also, Europe held a significant number of elections in 2024, including the EU parliament elections, which took place in June across member countries. Furthermore, Sweden hosted the 2024 Eurovision Song Contest in May, Germany hosted Euro 2024 from June to July and Paris hosted the Olympic Games in August.

The Middle East has also witnessed a surge in DDoS attacks linked to regional conflicts. Ongoing conflicts, such as the Israeli-Palestinian situation, have fueled hacktivist activities, leading to an increase in politically motivated cyberattacks targeting public, private and critical infrastructure.

In Africa, the expansion of digital infrastructure has been accompanied by a rise in cyberattacks. Countries such as Algeria, Morocco, Tunisia and Egypt have experienced significant increases in DDoS attacks, often linked to political activism and regional disputes. In recent years, Africa has witnessed a notable increase in hacktivist-driven Web DDoS attacks, reflecting the continent's expanding digital footprint and the growing use of cyber tactics for political activism. One prominent example is the hacktivist group Anonymous Sudan, which has orchestrated several DDoS attacks across Africa. In February 2024, Anonymous Sudan targeted major telecommunications companies in Uganda, including Airtel, MTN and Uganda Telecom, disrupting core services. The group claimed the attacks were in protest against companies supporting the Sudanese government amid civil conflict. Back in July 2023, the group launched cyberattacks on Kenyan government websites, allegedly in retaliation for the country's support of the Rapid Support Forces (RSF) in Sudan. In early 2024, Anonymous Sudan claimed responsibility for disabling internet services in Chad and Djibouti, protesting their relations with the RSF.

In 2024, the Asia-Pacific (APAC) region experienced a significant surge in Web DDoS attacks, with notable increases in both frequency and sophistication. Political events, particularly elections in South Korea and Taiwan, played a significant role in the distribution of attacks. According to the National Security Bureau of Taiwan, cyberattacks targeting Taiwan's government departments averaged 2.4 million per day, doubling from the previous year's 1.2 million daily attacks. The National Security Bureau attributes the majority of these incidents to Chinese cyber forces, with key sectors such as telecommunications, transportation and defense being primary targets. These actions are perceived as part of Beijing's strategy to exert military and political pressure, aiming to compel the democratically governed island to accept its sovereignty claims.

Figure 4: Geographic distribution of Web DDoS attack activity (source: Radware)



This leads to a geographic distribution in 2024 where organizations and institutions in EMEA are still the most often targeted (78% of the global Web DDoS attack activity) and where the APAC region represented 8% of the global activity, up from below 6% in 2023.

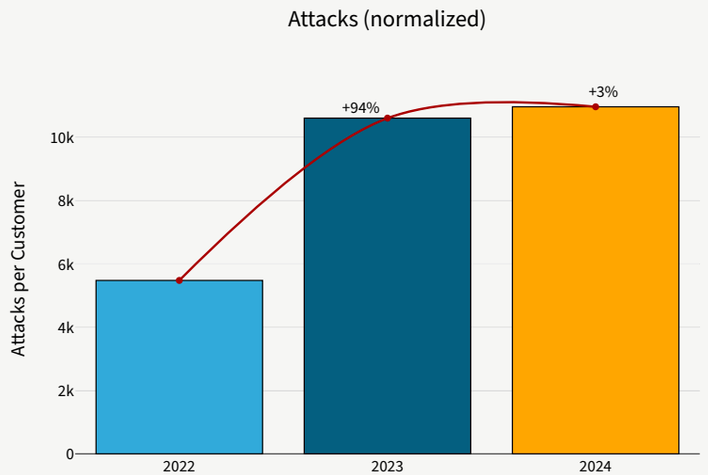
Network DDoS Attack Activity

While the surge in encrypted L7 web application attacks has garnered significant attention over the past two years, it's important not to overlook developments in network DDoS attacks. Although L3/L4 attacks haven't experienced the same explosive growth in 2024, there has been a notable increase in their frequency compared to 2022. Additionally, these attacks have evolved in 2024 to become larger and more prolonged, indicating a shift towards more persistent and resource-intensive attack vectors.

Concurrently, there has been a significant rise in "low and slow" attacks, both in their frequency and duration. These attacks are particularly insidious as they involve a small stream of very slow traffic targeting application and server resources, making them difficult to detect and mitigate.

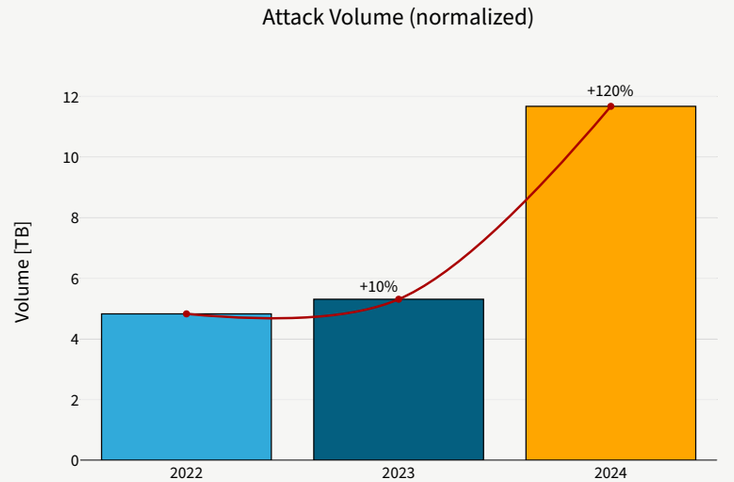
In 2024, the average number of network DDoS attacks per customer increased by 3% compared to 2023. This follows a substantial rise in 2023, where there was a 94% increase in attacks per customer compared to 2022.

Figure 5: Evolution of network DDoS attacks normalized per customer (source: Radware)



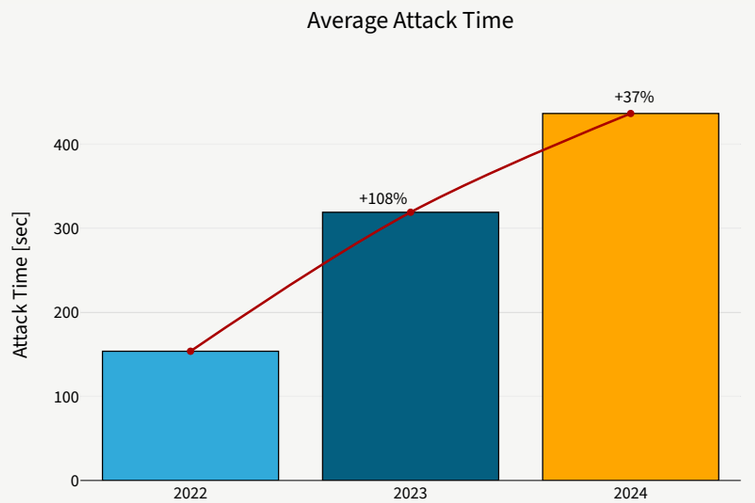
Despite the modest growth in attack frequency in 2024, the average total attack volume that customers had to mitigate more than doubled, demonstrating a 120% increase from the previous year. In 2023, there was a 10% increase in average mitigated attack volume per customer compared to 2022.

Figure 6: Evolution of attack volumes normalized per customer (source: Radware)



Additionally, the average duration of attacks more than doubled in 2023 compared to 2022 and continued to grow considerably in 2024, increasing 37% over 2023.

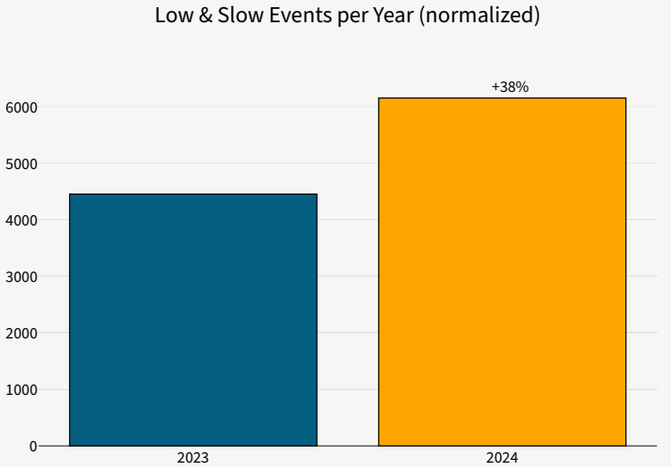
Figure 7: Evolution of average attack time (source: Radware)



Positioned at the opposite end of the DDoS spectrum from high packet rate and large volume network DDoS attacks, low and slow attacks are characterized by minimal data volumes and deliberate intervals between successive packets. These attacks deplete server and application resources, making them challenging to detect and mitigate, yet they can significantly disrupt applications and services.

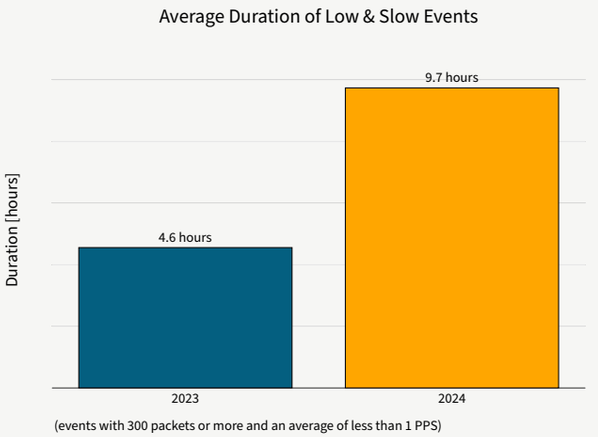
In 2024, the number of mitigated low and slow attack vectors increased by 38% compared to 2023, considering attack vectors with an average packet rate of less than one packet per second (PPS) and a minimum of 300 packets.

Figure 8: Evolution of "low and slow" attacks per customer (source: Radware)



Due to their nature, low and slow attacks tend to have a longer average duration compared to volumetric and high packet rate attacks. While the average network DDoS attack lasted approximately 437 seconds (just over seven minutes), low and slow attack vectors in 2024 averaged 9.7 hours in duration, more than doubling from an average of 4.6 hours in 2023.

Figure 9: Evolution of average duration of "low and slow" events (source: Radware)



The average Radware customer in 2024 mitigated a total volume of 11.7TB and 10,963 attacks lasting an average of just over seven minutes each and representing an average of 72,696 mitigated attack vectors, of which 6,150 were low and slow attack vectors that lasted an average of 9.7 hours each.

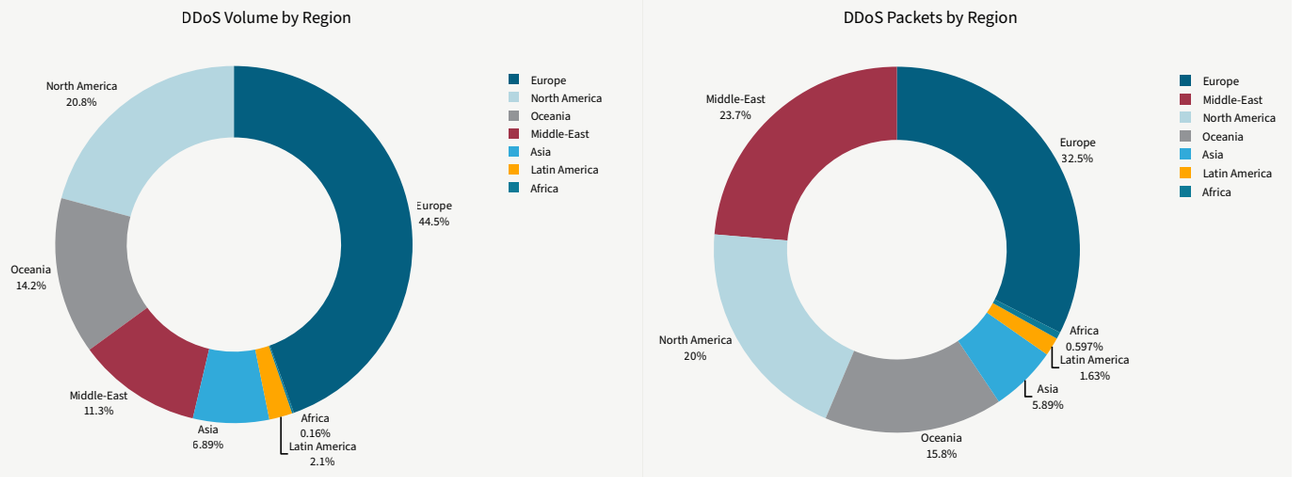
In 2023, the same average Radware customer mitigated a total volume of 5.3TB and 10,602 attacks lasting an average of just over five minutes each and representing an average of 29,122 mitigated attack vectors, of which 4,452 were low and slow attack vectors that lasted an average of 4.6 hours each.

Geographical Activity

In 2024, organizations in Europe faced the highest proportion of network DDoS activity of any region, accounting for 44.5% of the global attack volume and 32.5% of the total malicious packets. North American organizations were the second most targeted by volume, experiencing roughly 21% of global attack traffic, followed by those in Oceania (14%), the Middle East (12%), Asia, Latin America and Africa.

When considering the number of malicious packets blocked, the Middle East ranked second, intercepting nearly 24% of global malicious packets. North American entities accounted for 20% of blocked packets, Oceania had 16%, and Asia, Latin America, and Africa followed.

Figure 10: Network DDoS volume and packet distribution by regions (source: Radware)



Organizations in Oceania faced the highest average network DDoS volumes and packet counts per customer. European organizations experienced the second-largest volume per customer, while those in the Middle East encountered the second-highest number of malicious packets.

Figure 11: Average DDoS Volume mitigated per customer by region (source: Radware)

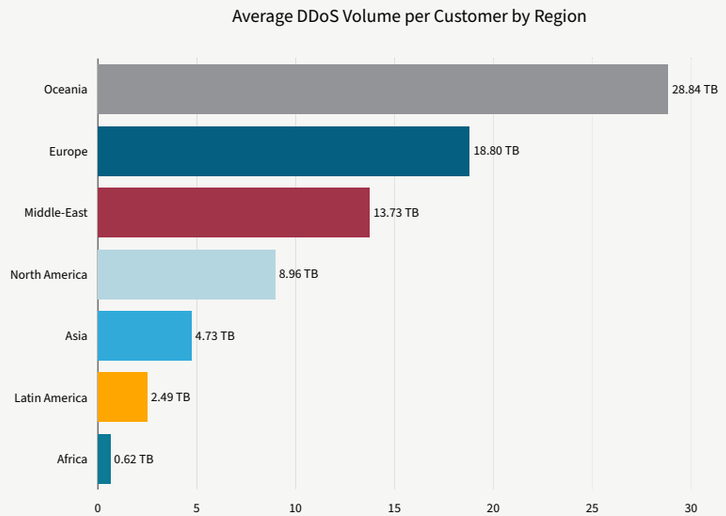
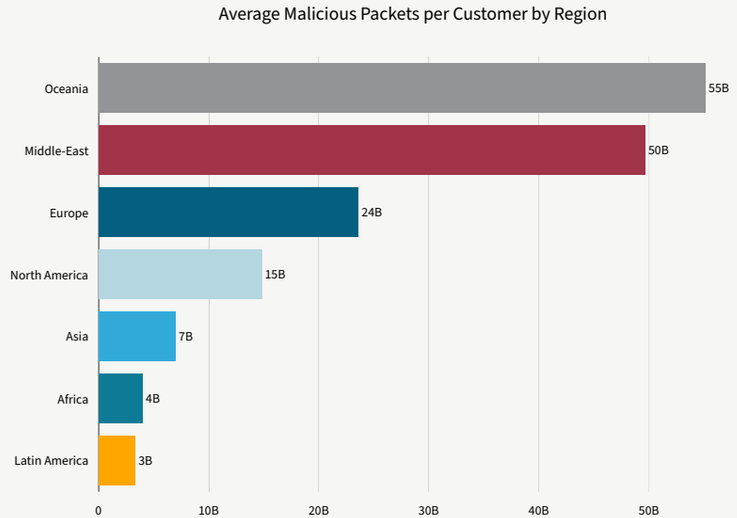
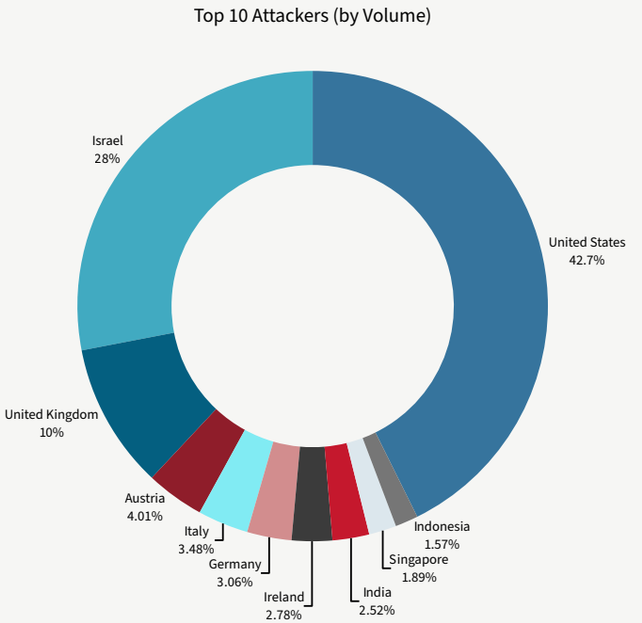


Figure 12: Average number of malicious packets blocked per customer by region (source: Radware)



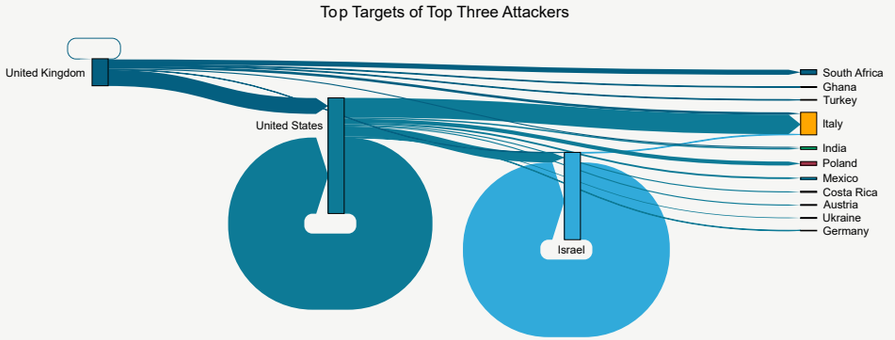
Analyzing the sources of network DDoS attack traffic by volume, the United States emerged as the leading originator, accounting for a substantial portion of global attack traffic. Israel followed, contributing approximately one-third of the volume generated by the top ten attacking countries. The United Kingdom was also a notable source, producing about one-tenth of the attack volume attributed to the ten leading nations.

Figure 13: Top ten attackers by network DDoS volume (source: Radware)



An analysis of network DDoS attack volumes emerging from the top three attackers (Figure 14) reveals that the United States was both a significant source and target. Domestically, the largest attack volumes were directed against itself, while also directing substantial volumes toward Italy, Israel and Poland. Israel also was predominantly both the origin and target of its own attack traffic with most of the volume directed internally. The United Kingdom exhibited a diverse attack pattern, targeting the United States, South Africa and Italy. These patterns underscore the complex and often domestic nature of the sources of network DDoS attack traffic.

Figure 14: Top targeted countries by the top three attackers by network DDoS volume (source: Radware)



In 2024, the United States not only led as the primary originator of network DDoS attack traffic by volume but also emerged as the most targeted nation, nearly matching the level of attack volume directed at Israel, the second most targeted country. Italy also faced a substantial share of these attacks, enduring over one-fifth of the total volume aimed at the top ten most targeted nations.

Figure 15: Top ten targeted countries by network DDoS volume (source: Radware)

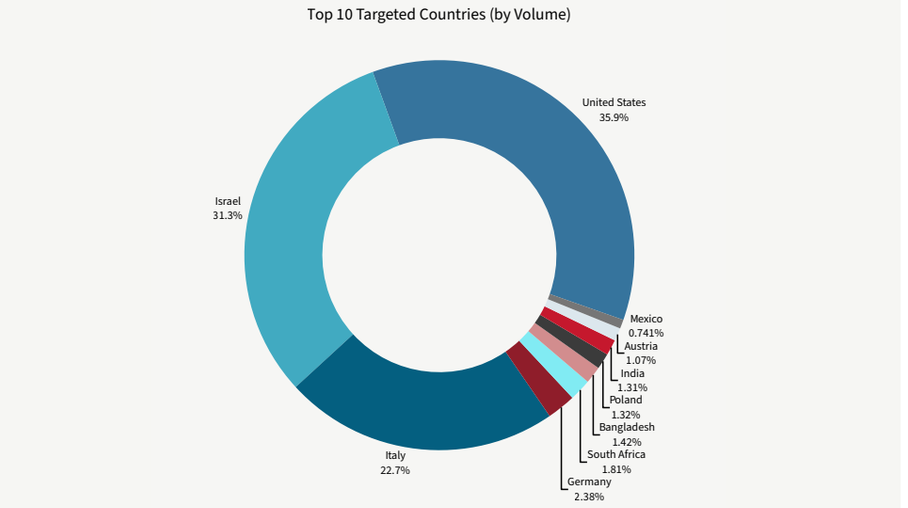
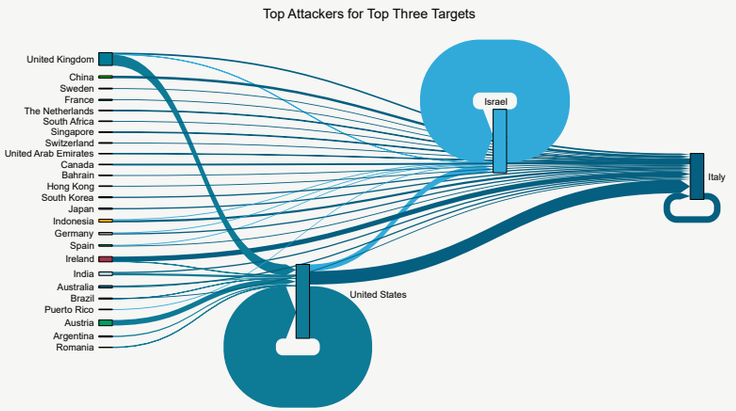


Figure 16: Top attackers targeting the top three countries targeted by network DDoS volume (source: Radware)



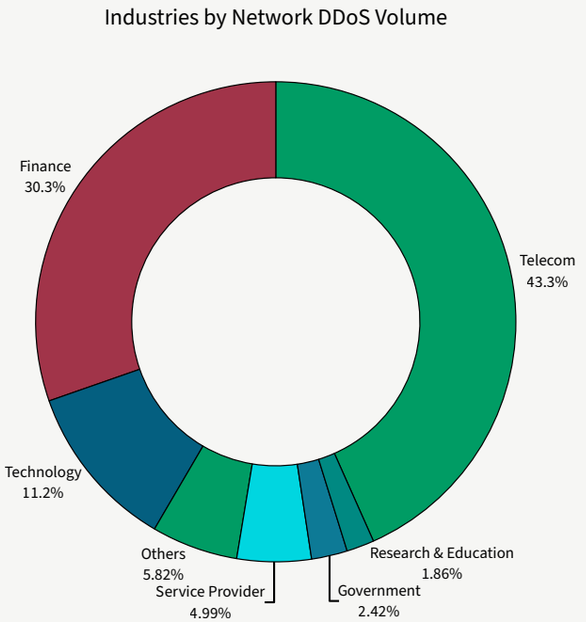
An analysis of network DDoS attack volumes targeting the United States, Israel and Italy (Figure 16) reveals that both the United States and Israel experienced the majority of attack traffic originating domestically. Significant volumes targeting the United States also stemmed from the United Kingdom, Austria and India. Notable sources of network DDoS traffic targeting Israel included the United States, Indonesia and Germany. For Italy, the United States was the predominant source of attack traffic, followed by Ireland, Italy itself and China.

The observation of substantial domestic DDoS attack volumes supports the notion that threat actors often utilize in-country service providers and compromised devices, such as IoT devices, to generate malicious traffic. This strategy involves leveraging botnets to flood target systems with traffic. Additionally, attackers may route their malicious packets through forwarders and their sessions through proxies, which also could include IoT devices, located near their targets to enhance the efficiency and impact of their attacks.

Industries

In 2024, the telecommunications sector bore the brunt of network DDoS volume, enduring over 43% of the global malicious traffic. The finance industry followed, facing roughly 30% of the global attack volume, while the technology sector contended with 11%. Service providers and government entities were also significantly impacted, with 5% and 2.4% of the global attack traffic, respectively. The research and education sector experienced 1.9% of the global attack volume, and the other industries collectively accounted for 5.8%.

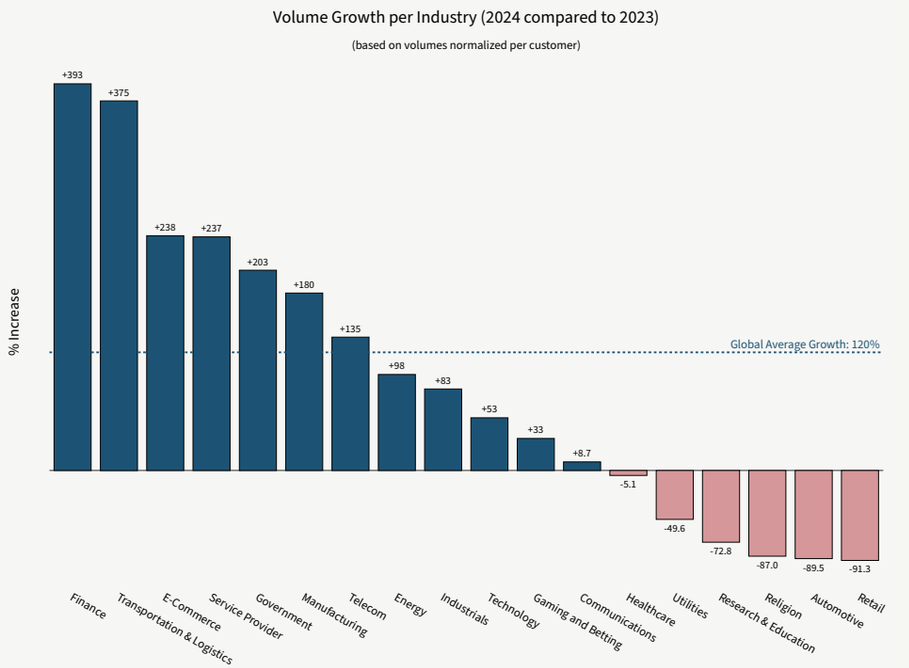
Figure 17: Industries that mitigated the most network DDoS attack volume (source Radware)



Between 2023 and 2024, several industries experienced significant changes in their average network DDoS attack volume per customer. The finance sector saw the most substantial increase with a surge of 393%. Transportation and logistics followed closely, experiencing a rise of 375%.

E-commerce and service providers also faced notable increases, with the average volume per customer growing by 238% and 237%, respectively. Government entities, the manufacturing and the telecommunications sector also grew faster than the global average of 120%, increasing by 203%, 180% and 135%, respectively. The energy industry observed a rise of 98%, below the global average growth, while the industrials and technology sectors' network DDoS volume grew by 83% and 53%, respectively. Conversely, some industries saw reductions in average network DDoS attack volumes. Healthcare experienced a slight decrease of 5%, while utilities faced a more significant drop of 50%. The research and education sector saw a substantial decline of 73%, and the religion sector experienced a decrease of 87%. The automotive industry faced the most pronounced reduction with a decline of 90%, and the retail sector's volume decreased by 91%.

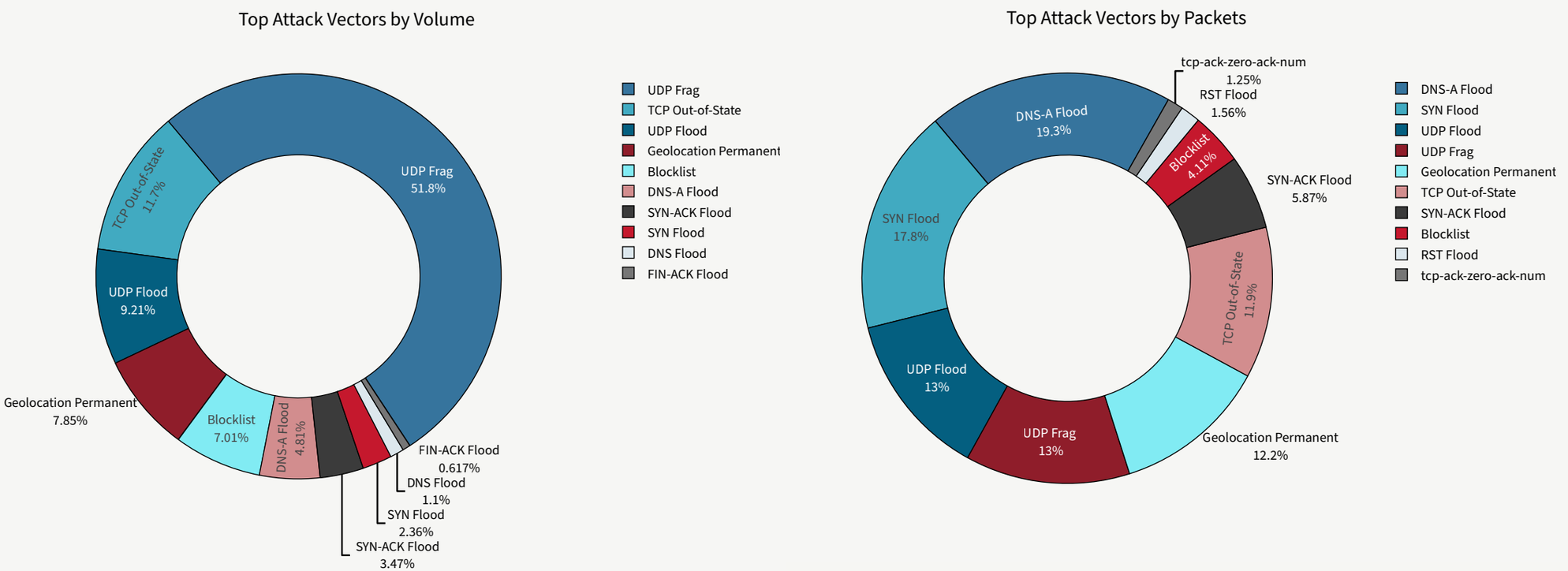
Figure 18: Change in volume per customer by industry from 2023 to 2024 (source: Radware)



Attack Vectors and Targeted Applications

In 2024, the User Datagram Protocol (UDP) remained the predominant vector for volumetric DDoS attacks. Its stateless nature makes UDP particularly susceptible to exploitation in reflection and amplification attacks, where legitimate services are misused to inundate targets with excessive traffic. Among the various attack methods, UDP fragment floods accounted for nearly 52% of the total volumetric attacks, underscoring their prevalence. Other significant attack vectors included TCP out-of-state floods at 12%, UDP floods at 9%, and DNS-A query floods at 5%. Notably, the Layer 7 DNS-A query floods were responsible for nearly 20% of the malicious packet volume, highlighting their efficiency in resource exhaustion attacks. Similarly, SYN floods continued to be an effective method for depleting target resources. The significant portions of UDP and UDP fragment flood packets are related to their use in volumetric attacks.

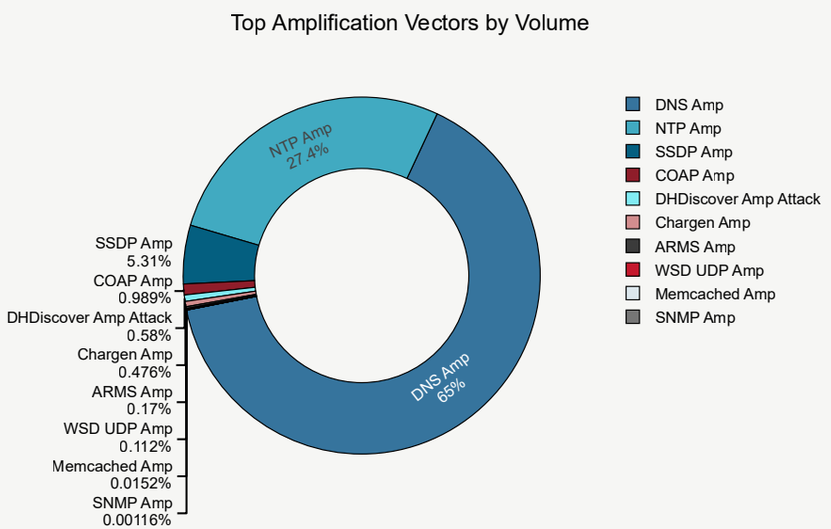
Figure 19: Top network DDoS attack vectors (source: Radware)



While geo-blocking alone cannot fully prevent network DDoS attacks, it serves as an effective initial defense by offloading a significant portion of malicious traffic. This approach conserves resources for more advanced detection and mitigation strategies, particularly against attacks utilizing globally distributed botnets. In practice, approximately 8% of global network DDoS attack volume and 12% of malicious packets have been mitigated through geo-blocking, with an additional 7% of the global volume addressed via IP intelligence feeds.

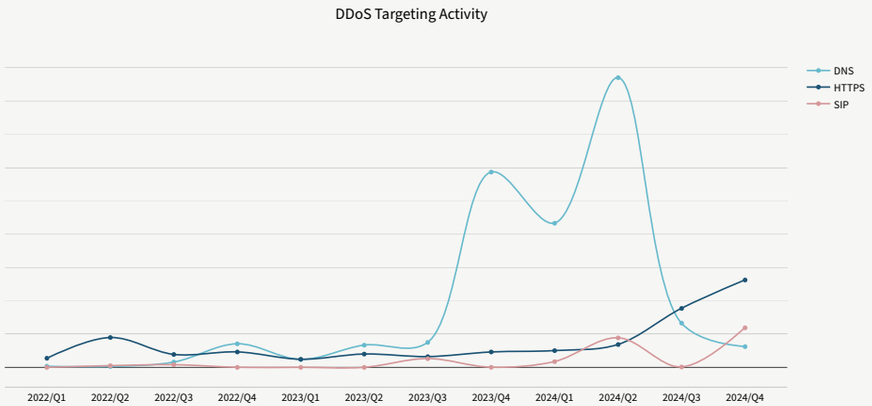
DNS and NTP amplification generated the most volume in 2024, representing 92.4% of the total network DDoS attack volume. DNS amplification was the most leveraged amplification attack vector and represented 65% of all the amplification attack volume observed in 2024. SSDP amplification represented over 5% of the amplification attack volume.

Figure 20: Network DDoS amplification attack vectors (source: Radware)



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. 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. 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 service becomes unavailable.

Figure 21: Evolution of DNS, HTTPS and SIP network DDoS attack activity (source: Radware)



Application-layer DNS DDoS Attack Activity

In the first half of 2024, organizations experienced a significant surge in L7 DNS DDoS attacks, with the volume of such attacks quadrupling compared to the same period in 2023. This escalation posed substantial challenges to businesses, particularly those in the finance sector, which accounted for 52% of the total DNS query flood attack activity. However, as the year progressed into the second half, the intensity of these DNS attacks began to diminish, gradually returning to levels observed in previous years.

Figure 22: Evolution of the ratio of DNS flood attack vectors (source: Radware)

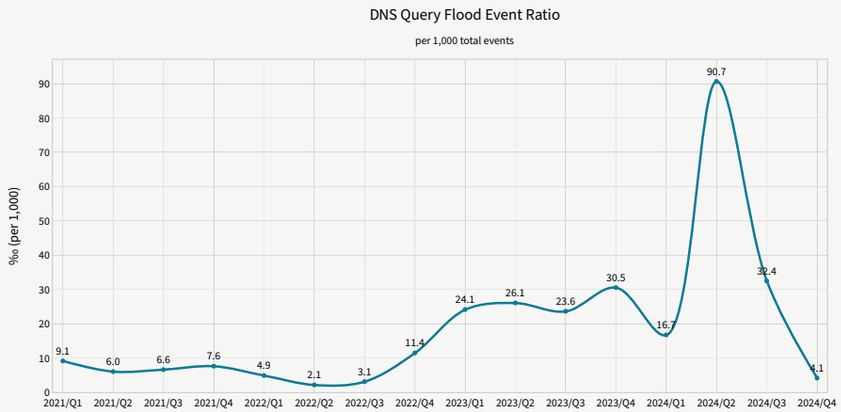
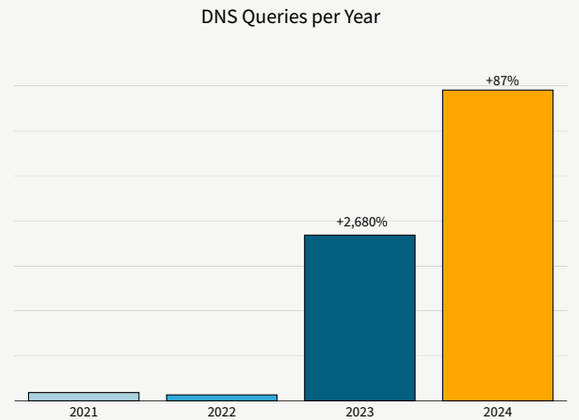


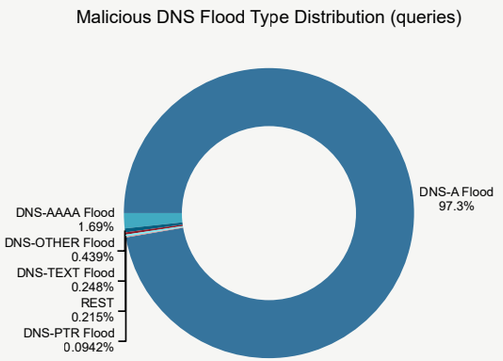
Figure 22 shows that throughout 2021 and most of 2022, fewer than nine out of every 1,000 attack vectors were DNS flood vectors. However, from Q4 of 2022, there was a marked increase in the proportion of attacks featuring a DNS flood vector. By the end of 2023, the ratio of DNS flood attack vectors more than tripled, and by the end of Q2 2024 the ratio surged to 90.7 vectors per 1,000 attack vectors. In the last two quarters of 2024, however, the ratio gradually reduced and normalized to its pre-2023 ratio. Overall, the year 2024 witnessed an unprecedented amount of DNS query flood denial of service attacks, up 87% from 2023, marking it as another pivotal year in the evolution of cyberthreats and, more specifically, L7 DNS DoS.

Figure 23: Blocked malicious DNS queries per year (source: Radware)



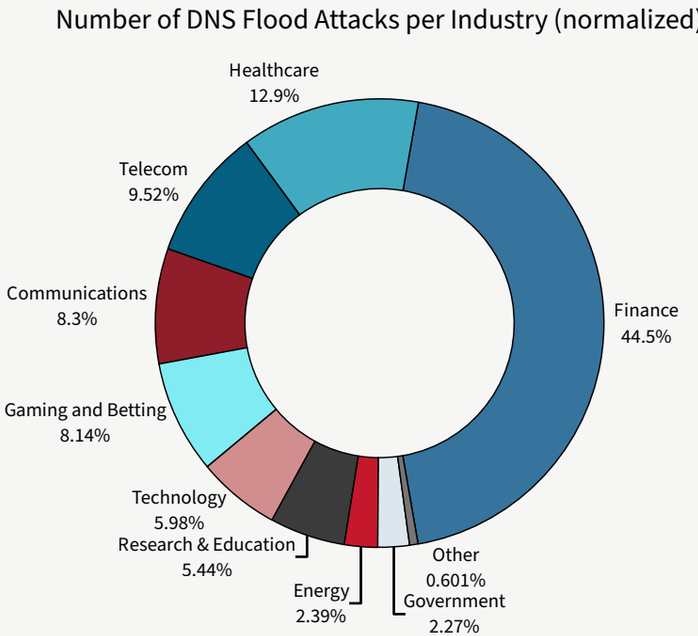
It is clear from Figure 24 that the DNS query type of most malicious DNS queries in 2024 was DNS-A (roughly 97%), followed by DNS-AAAA (1.7%) by a significant margin. DNS-A queries request the address mapping record, also known as DNS host record, that stores the hostname and its corresponding IPv4 address. DNS-AAAA queries are similar to DNS-A but for IPv6 addresses.

Figure 24: L7 DNS flood query type distribution (source: Radware)



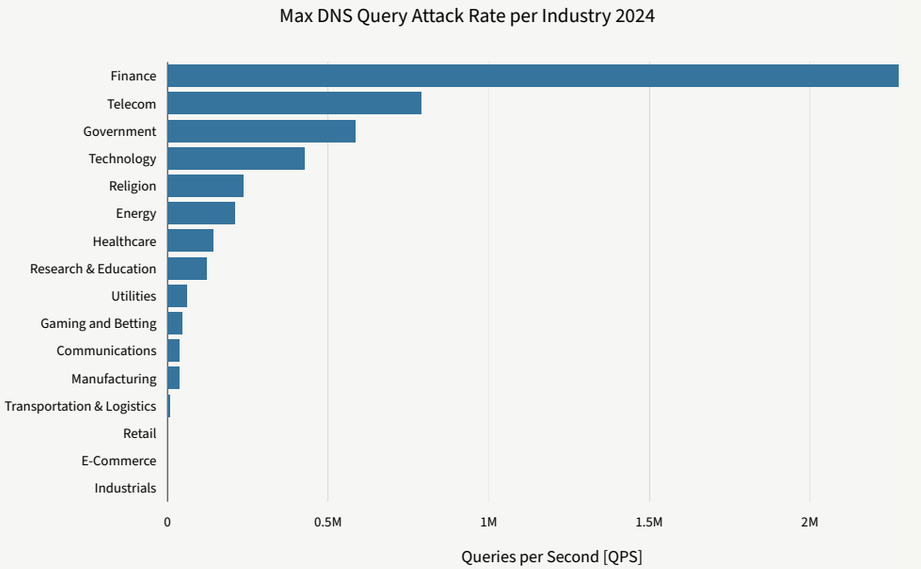
In 2024, L7 DNS flood attacks impacted a wide range of industries, with the financial sector bearing the brunt, accounting for roughly 44% of the total attack activity. Other significantly affected sectors included healthcare (13%), telecom (10%), communications (8%), gaming and betting (8%), technology (6%), and research and education (5.5%).

Figure 25: DNS Flood attacks per industry (source: Radware)



Finance was targeted by the most significant DNS query flood attack, which peaked at 2.3 million QPS. Finance was also targeted by the largest DNS query flood attack in 2023, which then peaked at 2.15 million QPS. The largest attack targeting telecom organizations peaked at 789,000 QPS. One government organization was targeted by an attack that peaked at 584,000 QPS.

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



Hacktivist DDoS Activity

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.

The State of Telegram in 2024

Shortly after the start of the invasion of Ukraine in 2022, the then 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. From that moment, Telegram took a pivotal role in the ongoing conflict between Russia and Ukraine, inspiring many other groups, hacktivists and others alike, to move to the platform.

Two years later, in 2024, Telegram became the central platform for hacktivist activities, offering features like anonymity and minimal content moderation that facilitate coordination and dissemination of cyber operations. Hacktivist groups, such as NoName057(16) and RipperSec, have utilized Telegram to orchestrate and claim DDoS attacks, particularly in the context of geopolitical conflicts like the Russia-Ukraine and the Israel-Hamas wars.

In August 2024, Telegram's founder and CEO, Pavel Durov, was arrested by the French authorities on charges of inadequate content moderation, which allegedly allowed the proliferation of criminal activities on the platform. This arrest prompted significant reactions within the hacktivist community. Several pro-Russian groups launched cyberattacks against French entities under the campaign hashtag #FreeDurov, targeting websites such as the National Court of France and the Paris Tribunal.

The arrest also led to concerns among cybercriminals and hacktivists about potential changes in Telegram's policies and the platform's future. Some feared increased scrutiny and possible shifts in content moderation practices, which could impact their operations. Despite the apprehensions that led some groups to explore alternative platforms like Signal and Discord, many groups continued their activities on Telegram.

Since Durov's arrest, the platform has significantly increased its moderation efforts and cooperation with authorities. Telegram's transparency reports indicate a substantial rise in data sharing with law enforcement agencies, particularly in the latter half of 2024. In 2024, the platform fulfilled 900 U.S. government requests, sharing the phone number or IP address information of 2,253 users with law enforcement. Prior to September 30 of that year, Telegram only shared users' IP addresses and phone numbers in cases of terrorism and had only fulfilled 14 requests affecting 108 users.

In parallel, the European Union (EU) has taken measures to restrict access to certain Telegram channels deemed violating EU laws. Notably, Telegram restricted access to Russian state-owned news channels and hacktivist channels such as the Pro-Palestinian Hacker Movement (PPHM) in EU countries.

The hacktivist landscape on Telegram was not without its disruptions. Prominent groups such as NoName057(16) and the Cyber Army of Russia Reborn (CARR) have had their channels banned. Interestingly, these bans do not appear to result from official regulations or moderation efforts but are instead believed to be the work of rival hacktivist groups targeting them through ban-spamming campaigns.

Overall, while Durov's arrest has introduced uncertainties regarding Telegram's stance on content moderation and its implications for hacktivist operations, the platform remains a significant hub for such activities.

Telegram's platform also offers bot automation and cryptocurrency payment services, enabling users to create bots that perform a wide range of functions. These bot channels, operated by software rather than individuals, can handle tasks from simple chat interactions to complex integrations with external services, including custom AI agents and botnet attack panels. Notably, some DDoS-for-hire services have adopted Telegram as their user interface. They direct clients to Telegram bots that facilitate real-time command execution and scheduling of DDoS attacks, providing status updates through the same channel. This trend has led to the proliferation of DDoS-as-a-service offerings on Telegram, making it alarmingly easy for individuals with minimal technical expertise to perform DDoS attacks. Vendors openly advertise a range of DDoS attack services at different price points, often accepting payments via cryptocurrency integrated into the platform, which adds another layer of convenience to these illegal activities.

Hacktivist DDoS Claims

Hacktivist groups frequently post claims of their DDoS attacks on Telegram, often providing evidence by sharing snapshots of website availability through check-host links. These links enable verification of the claimed target as well as the date and time of the attack. By focusing on messages containing valid check-host links, it is possible to monitor claimed attacks on Telegram with greater reliability. However, check-host links are not infallible. For instance, some reports have included links where the host was specified as "radware.com:666." Since there is no service running on port 666 of radware.com, the check-host report incorrectly returns as unavailable. In such cases, the report does not confirm that the targeted website was affected by the alleged DDoS attack.

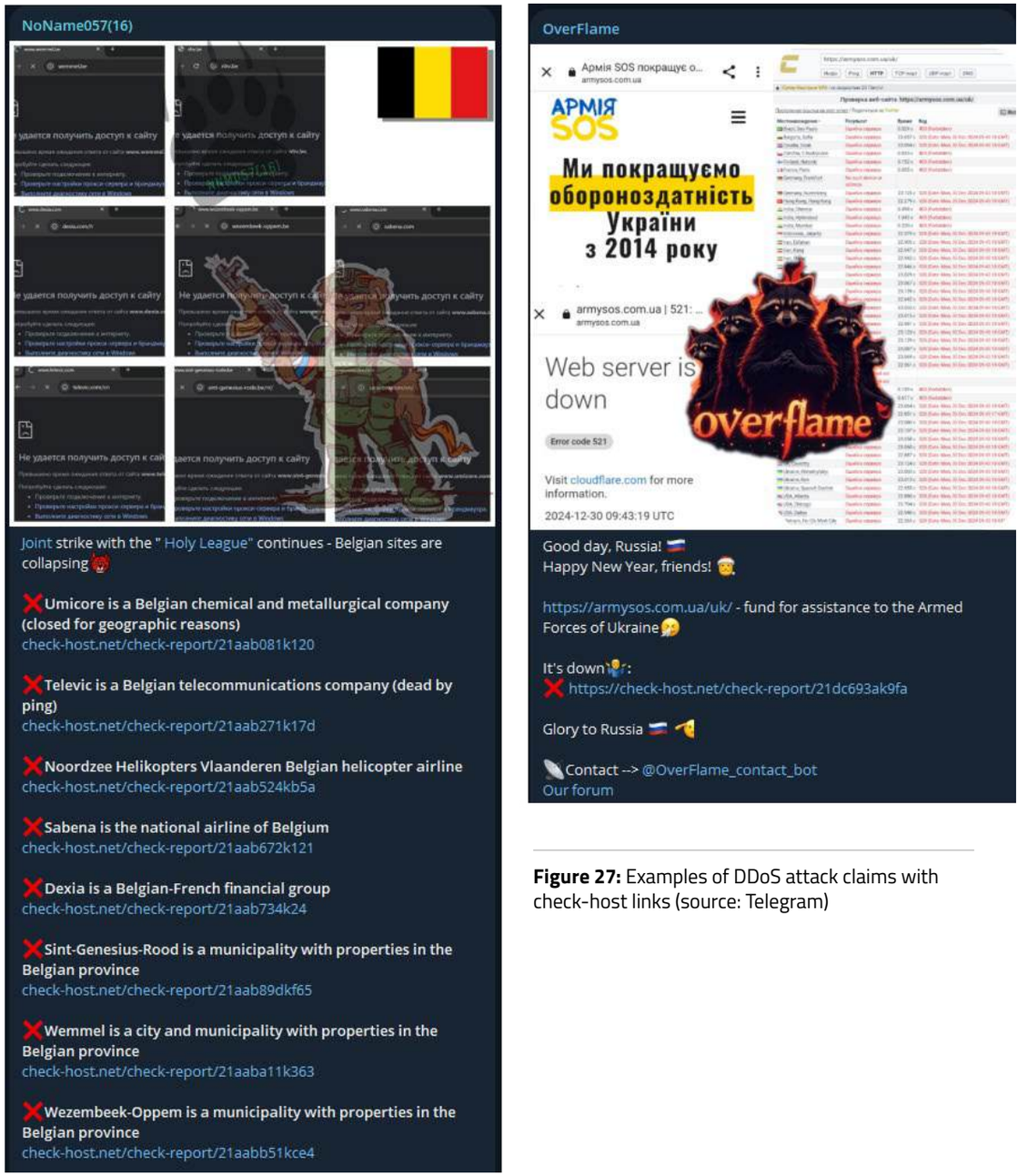


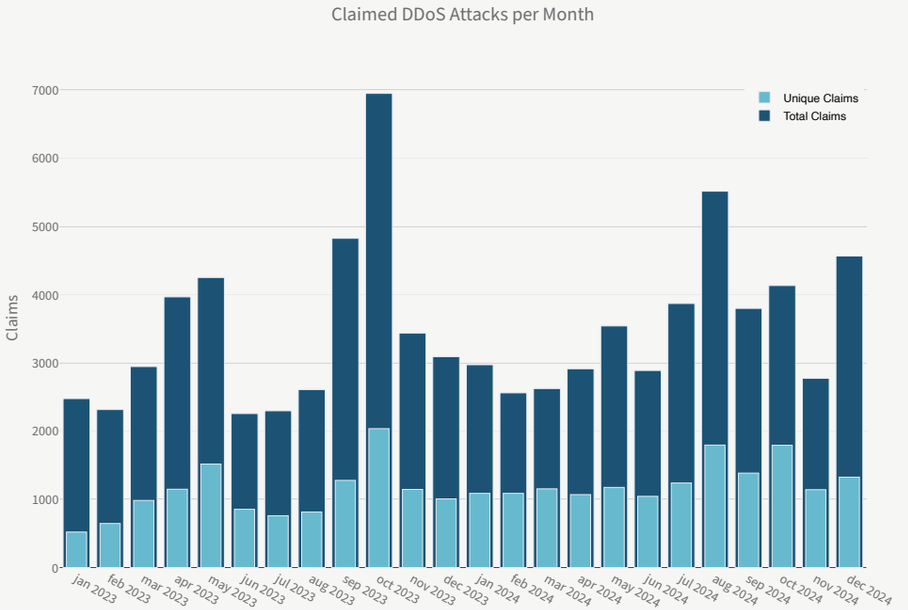
Figure 27: Examples of DDoS attack claims with check-host links (source: Telegram)

Attack claims posted on Telegram also frequently get forwarded to other channels. Radware only counts the message of the original post in hacktivist reports. This ensures that only unique attack claims—not the number of reposts or forwards—are counted. Figure 28 provides the number of unique DDoS attack claims per month as well as the total claims across more than 400 Telegram channels. The total claims include reposts of unique claims. The ratio of reposts of unique claims provides a measure of cooperation between hacktivists who share exploits. In 2023, threat actors claimed 12,709 DDoS attacks on Telegram; in 2024, this number increased by 20% to 15,295 unique claims. The hacktivist landscape is a dynamic one: many actors come and just as many leave. Some remove one channel only to create a new channel to clean out historical data and limit potential tracking of the channel by authorities and researchers. The overall trend of hacktivist-driven DDoS activity, however, remained mostly constant throughout 2024, hovering between 1,000 and 2,000 claimed DDoS attacks per month.

In 2023, two events generated a surge in activity across the hacktivist landscape. First was the yearly #OpIsrael campaign (OpIsrael 2023, OpIsrael 2024) led by several south-Asian hacktivists. The second and largest spike in hacktivist activity was in the period following the start of the conflict between Israel and Hamas, which made Israel the most targeted country in 2023 by pro-Palestinian hacktivists and their supporters.

> *In 2023, threat actors claimed 12,709 DDoS attacks on Telegram; in 2024, this number increased by 20% to 15,295 unique claims.*

Figure 28: DDoS attacks claimed per month on Telegram (source: Radware)



In 2024, increases were observed in August and October. The increase in August coincided with Venezuela's contested presidential elections that were held on July 28, 2024. Driven by accusations of election fraud by Nicolás Maduro's administration, hacktivist groups including Anonymous Venezuela and Cyber Hunters launched the #OpVenezuela campaign against Venezuelan government entities. The arrest of Telegram CEO Pavel Durov by French authorities on August 24, 2024, also sparked a wave of cyberattacks against French websites.

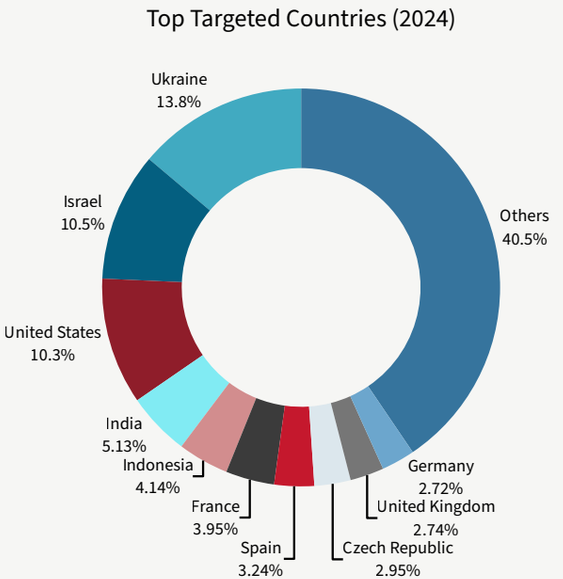
Throughout October, pro-Russian hacktivist groups intensified their cyber campaigns. Notably, groups such as NoName057(16) targeted various European entities, including governmental organizations and ports in Belgium and the United Kingdom. These actions were often in retaliation against nations perceived as supporting Ukraine in the ongoing conflict. In mid-October, Japanese organizations faced DDoS attacks from pro-Russian hacktivist groups, including NoName057 and the Cyber Army of Russia Reborn. These attacks, aiming to disrupt Japanese infrastructure and services, reportedly were a response to Japan's military collaborations with the United States.

Most Targeted Countries and Regions

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 and 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.

In 2024, a significant portion of hacktivist activity was once again driven by geopolitical events. For instance, the Russia-Ukraine conflict has spurred numerous cyber activities targeting entities aligned with either side. Countries like Israel and India have been targeted due to religious and ideological reasons, with hacktivist groups aiming to make political statements or protest against perceived injustices. Europe has always been a major focus for certain hacktivist groups, particularly pro-Russian entities, reflecting the complex political landscape and historical contexts of the region.

Figure 29: Hacktivist DDoS attack claims per country (source: Radware)



Ukraine leads the list of top targeted countries in 2024 with over 2,000 claimed attacks. It has been a focal point for hacktivist activities, especially in the context of geopolitical tensions with Russia. Pro-Russian hacktivist groups have frequently targeted Ukrainian infrastructure to disrupt services and propagate political messages. 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 in 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 in 2024 with 2,052 claimed attacks.

With 1,550 claimed attacks, Israel has faced significant cyberthreats, often from groups opposing its policies in the Middle East. Campaigns like #OpIsrael have been orchestrated by various hacktivist collectives aiming to protest Israeli governmental actions. The top attacker collectives targeting Israel in 2024 included RipperSec, NoName057(16), Anonymous Guys, Anonymous Muslims, Moroccan Black Cyber Army, Ketapang Grey Hat Team, 1915 Team and Al Ahad. The most targeted industries were government, education and finance.

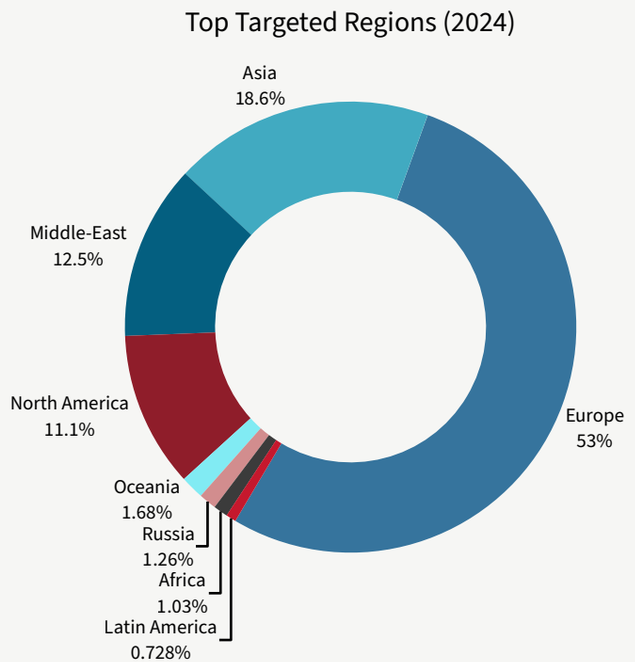
The United States has become a prime target for DDoS-as-a-service providers, who often exploit high-profile organizations to showcase their capabilities in proof-of-concept demonstrations. Among the most active DDoS-as-a-service providers in 2024 were Executor DDoS, Krypton Networks, ZeusAPI Services and XcDDoS. Simultaneously, prominent hacktivist groups, including RipperSec, NoName057(16), Cyber Army of Russia Reborn and LulzSec by the Anonymous Group, most frequently claimed responsibility for attacks on U.S. entities.

In South Asia, India was the subject of 761 claimed attacks in 2024. These attacks originated from various hacktivist groups, both regional—hailing from Malaysia, Indonesia and Bangladesh—and international. Prominent attackers included RipperSec, Executor DDoS, Anonymous Susukan, Sylhet Gang, Ketpang Grey Hat Team, Anonymous KSA, Al Ahad, Anonymous Guys, Garuda From Cyber and Sulawesi Cyber Team Indonesia.

France, Spain, the Czech Republic, the United Kingdom and Germany reported between 404 and 586 claimed attacks in 2024. NoName057(16) predominantly targeted each of these countries and accounted for at least one-third of their attacks. The reasons for attack include their positions on international conflicts, domestic policies and election-related activities. European nations, in particular, have been a focal point for pro-Russian hacktivist groups, making Europe the most targeted region globally, accounting for over half of all hacktivist activity.

The "Others" category, encompassing 6,013 attacks, indicates that hacktivist activities are widespread, affecting numerous countries across different continents.

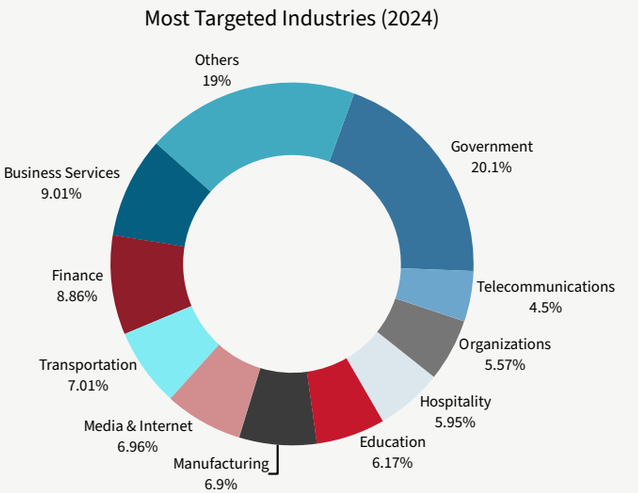
Figure 30: Hacktivist DDoS attack claims per region (source: Radware)



Top Targeted Industries

The distribution of the most targeted industries in 2024 closely mirrored the trends observed in 2023. Governments remained the primary focus of attacks since January 2023, with notable targets located in Ukraine, India, Israel, the United States, the Czech Republic, France, Poland, Spain and the United Kingdom. The leading threat actor targeting government institutions was NoName057(16), responsible for 2,072 claimed attacks targeting government institutions in 2024. Following them were Team Insane Pakistan with 277, Mysterious Team Bangladesh with 232, and Cyber Army of Russia Reborn with 215 claimed attacks targeting government entities.

Figure 31: Attacks claimed by industry (source: Radware)

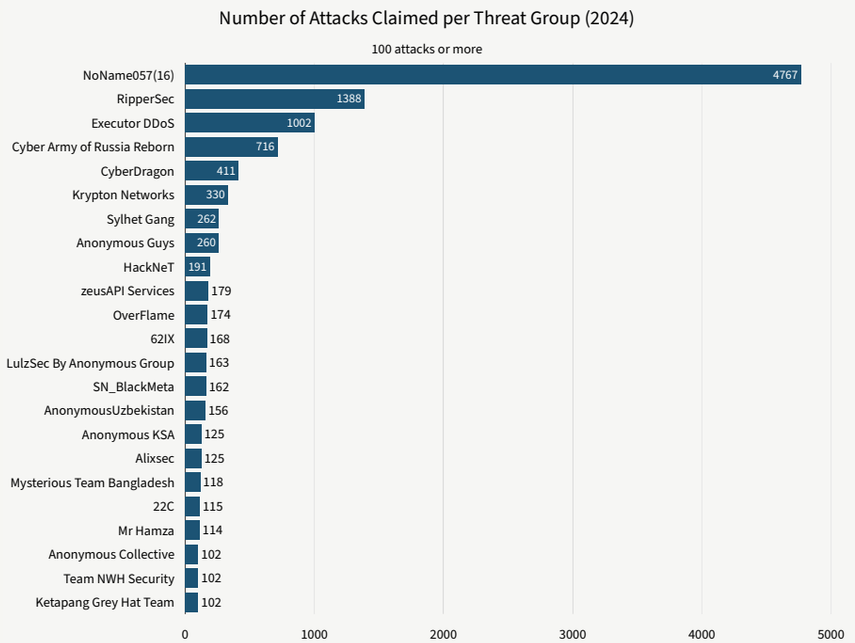


Business services, encompassing e-commerce platforms and organizational websites, were also heavily targeted by NoName057(16). In the financial sector, which includes online banking and payment services, NoName057(16) claimed 949 attacks, solidifying their dominance. Other highly targeted industries, such as transportation, media and internet, and manufacturing, also faced significant attack volumes, with NoName057(16) consistently emerging as the primary actor across these sectors.

Top Claiming Actors

It comes as no surprise that NoName057(16) once again led as the most prolific claiming threat actor in 2024. With over 8,150 DDoS attack claims since January 2023, including 4,767 claims in 2024 alone, NoName057(16) outpaced other actors by a wide margin. RipperSec ranked as the second most active hacktivist group in 2024 with 1,388 DDoS attack claims, followed by Executor DDoS, the Cyber Army of Russia Reborn, CyberDragon and Krypton Networks.

Figure 32: Attacks claimed per threat actor in 2024 (source: Radware)



Evolving Hacktivist Tactics

In 2024, the hacktivist group NoName057(16), previously known for its solitary operations, underwent a significant transformation by forming well over a dozen strategic alliances with various pro-Russian and pro-Palestinian hacktivist groups. This shift from isolation to collaboration enabled the group to enhance its operational capabilities and broaden its impact.

Key Alliances Formed by NoName057(16) in 2024:

- Cyber Army of Russia Reborn (CARR) and Z-Pentest (September 26, 2024): This partnership positioned NoName057(16) as a central figure in the pro-Russian hacktivist ecosystem, amplifying its reach and influence.
- Cyber Team Indonesia (October 8, 2024): Collaboration with this Southeast Asian group extended NoName057(16)'s influence into new regions, reflecting a strategic move to globalize its operations.
- VoltActivist (October 10, 2024): Partnering with this entity further diversified NoName057(16)'s network, enabling coordinated cyber campaigns against shared adversaries.

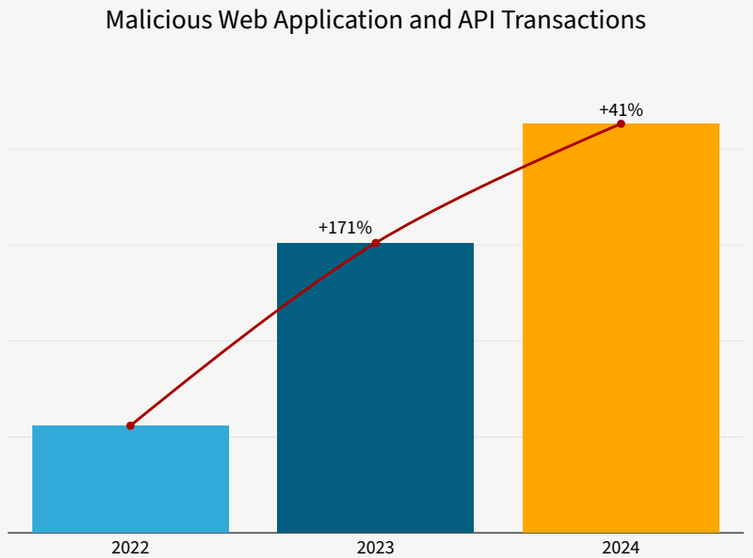
These alliances signify a broader trend within the hacktivist community, where groups with common perceived enemies are increasingly collaborating to enhance their operational effectiveness. Another notable example of this trend is the formation of the Holy League in July 2024, a coalition resulting from the union of the High Society and 7 October Union alliances. This collective unified pro-Russian and pro-Palestinian hacktivists who launched coordinated attacks against shared adversaries, primarily Western nations, NATO, India, and countries supporting Ukraine and Israel.

The rise of such alliances indicates a shift towards more organized and potent hacktivist operations. By pooling resources and expertise, these groups can execute more sophisticated and large-scale attacks thereby amplifying the impact, reach and visibility of their cyber campaigns.

Web Application and API Attack Activity

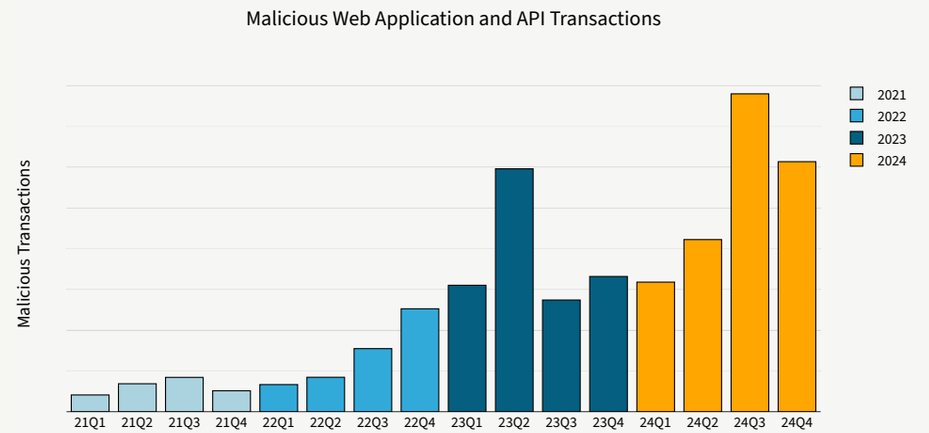
In 2023, attackers put more focus on online applications, transitioning from the network layer to the application layer. This led to a substantial 171% increase in the number of web application and API attacks detected by Radware's Cloud WAF Service. This trend continued into 2024, solidifying the shift as the new norm, with the volume of mitigated web application and API attacks rising by an additional 41% compared to 2023.

Figure 33: Malicious web application and API transactions per year (source: Radware)



As shown in Figure 34, a drop and an interruption of the growth trend was observed in malicious web application transactions in Q3 of 2023. This drop 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 its Web DDoS automated detection and mitigation solution to efficiently block large-scale Web DDoS attacks. This new layer of protection sits between the network DDoS protection and the Web Application and API protection layer. The new protection layer is significantly more efficient in detecting and processing large-scale, sophisticated Web DDoS attacks. As more Web DDoS attacks were mitigated by the new service, fewer malicious transactions made it through to the web application and API protection layer. This resulted in a significant drop in the number of recorded malicious web application transactions, which now comprise only exploits, leaks and anomalies (before Q3 2023, tracking of malicious transactions also included Web DDoS transactions).

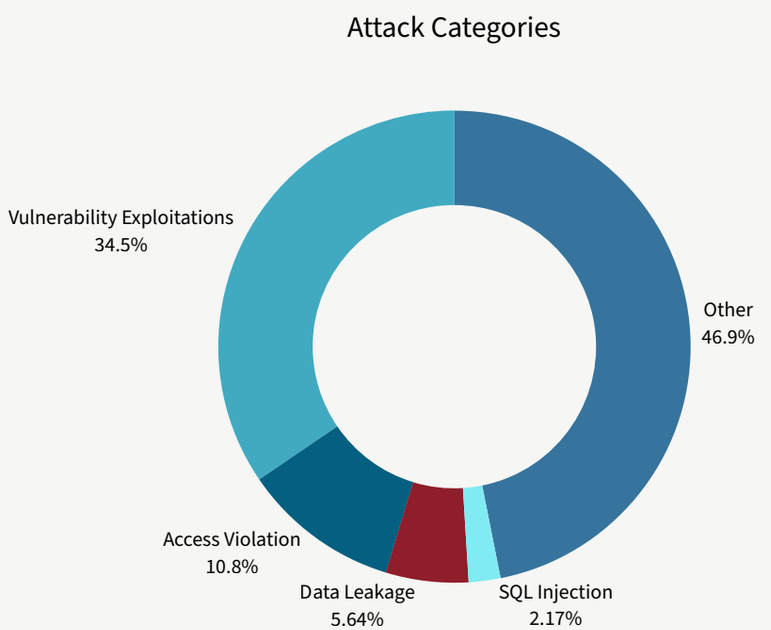
Figure 34: Malicious web application and API transactions per quarter (source: Radware)



[1] This trend can also be explained by more organizations moving published applications from on-premises to the cloud. Before, attackers could target the organization's uplink to impact the application. Now that an application is hosted in the cloud, the attackers either need to bring down the cloud or find a way to target only the specific application they aim to impact.

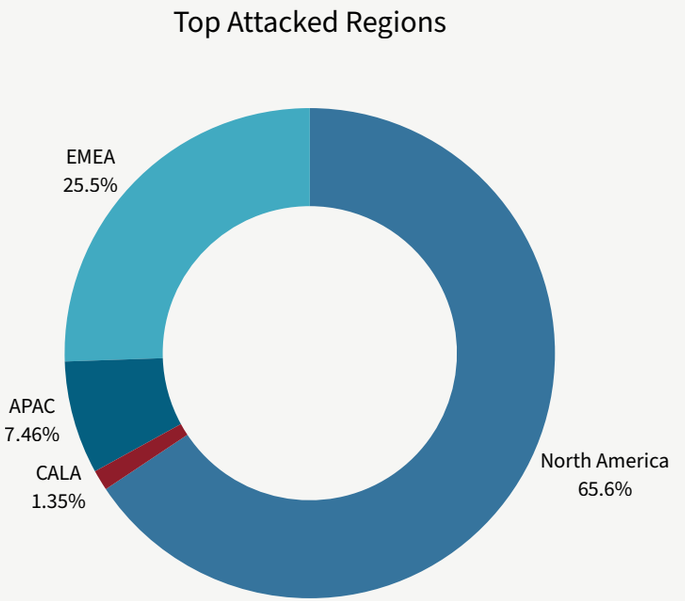
The most important attack category for 2024 (Figure 35) was vulnerability exploitation, representing more than a third of all malicious web requests. Access violations account for a tenth of all malicious web requests and include predictable resource location attacks that target hidden content and functionality 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 5.6% and 2.2% of the malicious activity, respectively.

Figure 35: Web application and API attacks by category (source: Radware)



The majority of web attacks (66%) targeted applications and APIs located in North America. Applications in EMEA accounted for 26% of the attack activity in 2024.

Figure 36: Web application and API attacks by region (source: Radware)



> *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.*

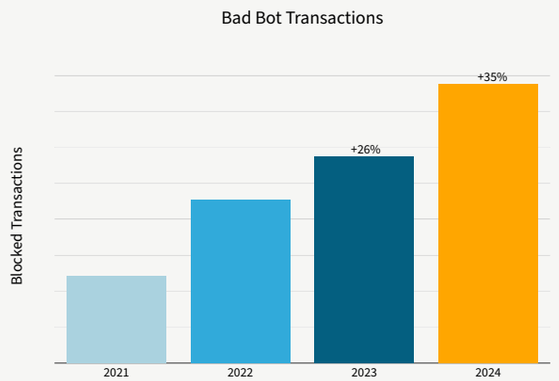
Bad Bot Activity

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

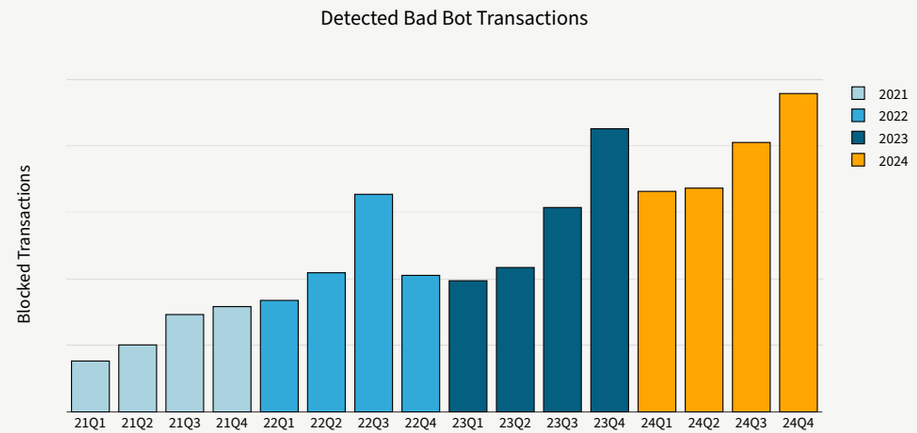
In contrast to bad bots, good bots are programs that run automated tasks that are beneficial for their target. Good bots can help improve the functionality and performance of websites and APIs. They also provide useful services and information to users. Examples of good bots include search engine bots, which crawl through web content and index the information for search engines; AI-driven bots, which aggressively scrape data to train AI models, often without permission and by consequence are also referred to as "grey bots"; 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.

Figure 37: Bad bot transactions per year (source: Radware)



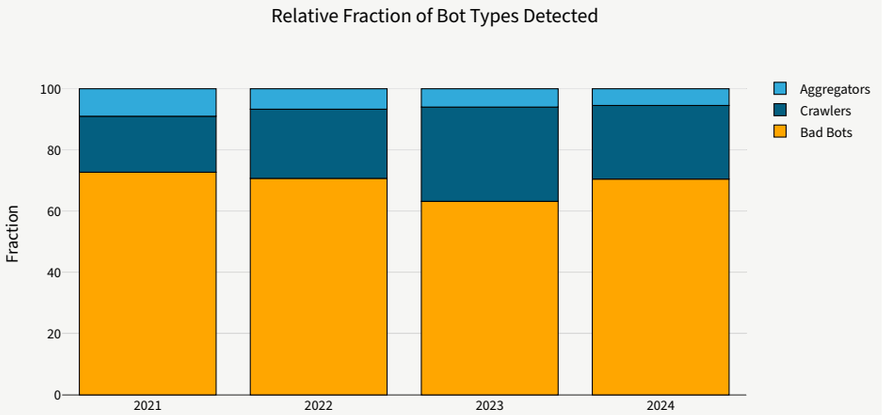
The volume of bad bot transactions saw a 35% increase in 2024 compared to 2023, following a 26% rise in 2023 relative to 2022. As illustrated in Figure 38, the latter half of each year consistently records significantly higher bad bot activity compared to the first half. This observation aligns with high-traffic periods such as Black Friday, Cyber Monday, and the winter holiday season when promotional campaigns and increased online activity make platforms more susceptible to such transactions.

Figure 38: Bad bot transactions per quarter (source: Radware)



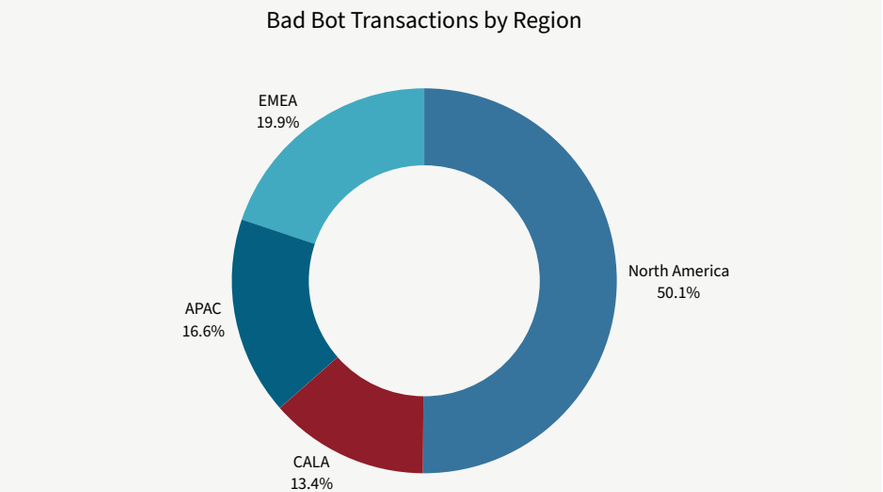
Aggregator bots accounted for the smallest share of detected bot transactions, comprising 5% in 2024, down from 6% in 2023. Crawlers constituted a more significant portion, representing 31% of bot transactions in 2023 and decreasing to 24% in 2024. However, bad bots dominated bot traffic, making up 63% of all bot transactions in 2023 and increasing to nearly 71% in 2024, underscoring their growing prevalence and impact.

Figure 39: Yearly evolution of relative fractions of detected bot types (source: Radware)



In 2024, North America emerged as the most targeted region, accounting for 50% of all bad bot transactions. The EMEA region followed with 20%, while APAC accounted for 16.6%, and CALA represented 13.4% of the total bad bot activity.

Figure 40: Bad bot transactions per region (source: Radware)



The Dual Impact of AI on Data Scraping and SEO Evolution

The rapid advancement of AI technologies has led to the emergence of sophisticated "grey bots" that aggressively scrape data to train AI models, often doing so without explicit authorization. At the same time, AI is quickly becoming a central focus for search engine optimization (SEO) strategies. With the proliferation of generative AI models, conversational AI and AI-powered search engines, the SEO landscape is shifting to emphasize content optimized for AI processing and user behavior in AI-driven searches. This evolution introduces ethical and operational challenges, as data owners strive to safeguard their assets while balancing the needs of legitimate AI-driven data collection for research and for SEO.

The rapid advancement of AI technologies has led to the emergence of sophisticated "grey bots" that aggressively scrape data to train AI models, often doing so without explicit authorization.

Conclusion

The year 2024 underscored a clear trajectory: cyberthreats are not only proliferating but becoming more adept at circumventing traditional defenses. From massive volumetric DDoS campaigns to Layer 7 attacks that exploit newly discovered vulnerabilities, the scope of DDoS alone has expanded far beyond the capability of older, static protections. Concurrently, hacktivist collectives showcased unprecedented levels of coordination, while web application and API threats continued to multiply under the weight of complex infrastructures and widespread reliance on third-party components. Bad bots and AI-powered cybercrime have redefined what is possible in terms of evasion, automation and destructive potential.

With these developments come significant implications for every sector: finance, telecommunications, government, e-commerce and beyond. The confluence of political motivations, advanced technology and criminal innovation creates a dynamic threat environment that demands equally dynamic defense strategies. Organizations must not only adopt layered protection strategies but also invest in ongoing risk assessments, cyberthreat intelligence and employee education to stay one step ahead of adversaries. By recognizing and preparing for the realities of 2024's threat landscape, stakeholders can better safeguard their operations, assets and reputations in the years to come.

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 from the same attack corresponds 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 is able to assess the global DDoS activity conducted by hacktivists.

Author

Pascal Geenens | Director of Cyber Threat Intelligence

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.

RWI 426 | 02.20.2025