imperva
a Thales company

2024

Imperva DDoS Threat Landscape Report

imperva
a Thales company

2024

Imperva DDoS Threat Landscape Report

Table of Contents

The 2024 Imperva DDoS Threat Landscape Report reviews Distributed Denial of Service (DDoS) attack activity during the first half of 2024, provides insights into the year's most noteworthy DDoS events, and offers recommendations for the year ahead.

DDoS attacks have existed for a long time and show no sign of disappearing. Cybercriminals intent on causing general disruption, either for political reasons or simply in the name of general hacktivism, often use them as their first attack choice.

Notably, the volume of these attacks is increasing, driven by the easier availability of DDoS tools that allow even individuals with limited technical expertise to launch significant attacks. The shift towards automation in these tools has further lowered the barrier to entry, enabling a broader range of cybercriminals to participate in DDoS activities.

Political tensions also contribute to the prevalence of DDoS attacks, as state actors and activists use these methods to make political statements or signal potential future actions. As such, understanding the motivations and methods behind DDoS attacks is crucial for developing effective defense strategies.

The report leverages intelligence provided by Imperva Threat Research based on data from the application and network-level DDoS attacks we have mitigated. It also provides additional observations based on broader global DDoS activity throughout the year.

The insights and recommendations provided in this report are essential for organizations aiming to enhance their cybersecurity posture against the evolving DDoS threat landscape.

What is a DDoS Attack?

04

Distributed Denial of Service (DDoS) attacks are categorized into three main types: volume-based, protocol attacks, and application layer attacks.

Since their inception in the early 1990s, the motivations behind DDoS attacks have evolved from cyberbullying and revenge to hacktivism, cyber warfare, and extortion/Ransom DDoS (RDoS). Concurrently, the methods employed in DDoS attacks have become more advanced.

DDoS attacks are launched from multiple connected devices spread across the Internet, making them difficult to mitigate due to the number of devices involved. These large-scale DDoS attacks often involve botnets, which are networks of compromised devices remotely controlled from a Command & Control Center (C&C).

A detailed list of DDoS attack types and their mitigation methods can be found HERE.

Attackers use DDoS attacks for various purposes, including political hacktivism and other malicious intents.

Executive Summary

05

Report Highlights

111%

Increase in DDoS attacks mitigated by Imperva. In the first half of 2024, Imperva has successfully mitigated 111% more DDoS attacks compared to the same period the previous year, highlighting the need for robust security measures.

4.7 Million RPS

Application Layer DDoS attack of 4.7 Million RPS. The most notable attack in the first half of 2024 was an Application Layer DDoS attack in February, reaching 4.7 Million Requests Per Second (RPS).

215%

DNS attacks surge by 215%: DNS attacks increased in number by 215% when comparing H1 2024 with the same period in 2023.

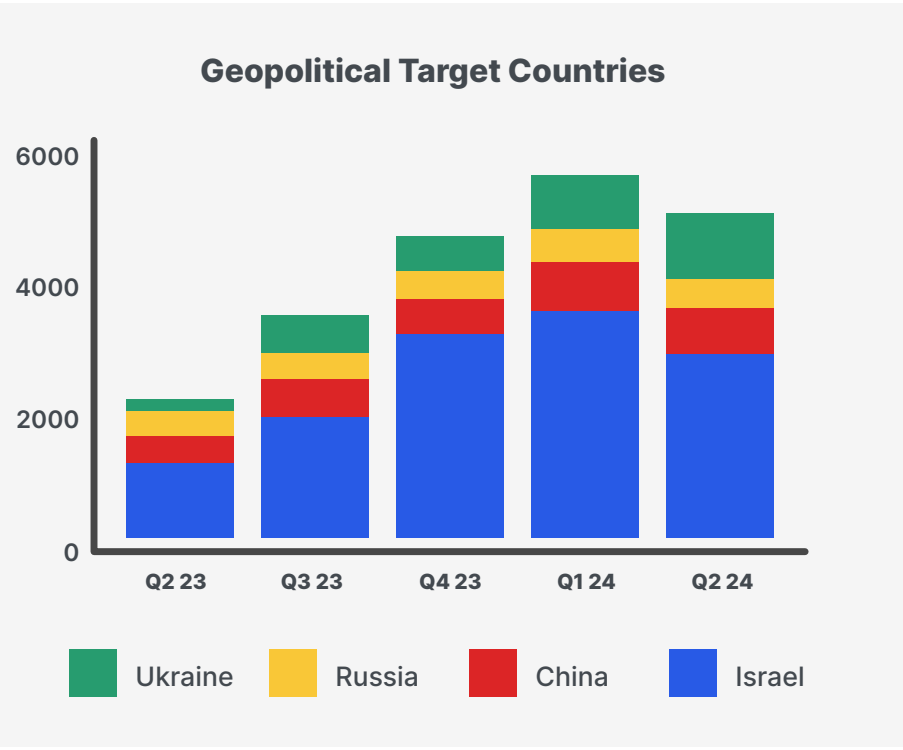
483%

increase in Size of DNS Amplification attacks. In H2 2023, the average size of a DNS Amplification attack increased by 483% compared to the first half of the year.

Geopolitical tensions driving DDoS attack Numbers

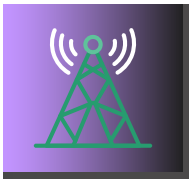
Geopolitical tensions have significantly increased DDoS attacks over the past year. Key areas of impact include:

Middle East Unrest	**118%** Increased attacks on Israel	+118%
Russia-Ukraine Conflict	**519%** Surge in attacks on Ukraine	+519%
Cybersecurity Competition	**84%** Rise in attacks on China	+84%



89%

Increase in DDoS attacks around sporting events.
DDoS attacks targeting industries associated with major sporting events have surged by 89%, demonstrating how high-profile events attract cybercriminals seeking to disrupt operations and gain publicity.



548%

Increase in attacks on Telecommunications and ISPs.
The telecommunications and ISP sectors have experienced a staggering 548% rise in DDoS attacks, reflecting their crucial role in maintaining internet connectivity and the high stakes in disrupting their services.

236%

Increase in attacks on Healthcare targets.
Attacks on healthcare organizations have increased by 236%, underlining the vulnerability of this sector and the potentially devastating impact on critical healthcare services and patient data.

208%

Increase in attacks on the Gaming industry. Attacks on the gaming sector, including online gambling platforms, have risen by 208%, reflecting the high-value targets and the sector's susceptibility to disruptions that can affect gaming experiences and financial transactions.

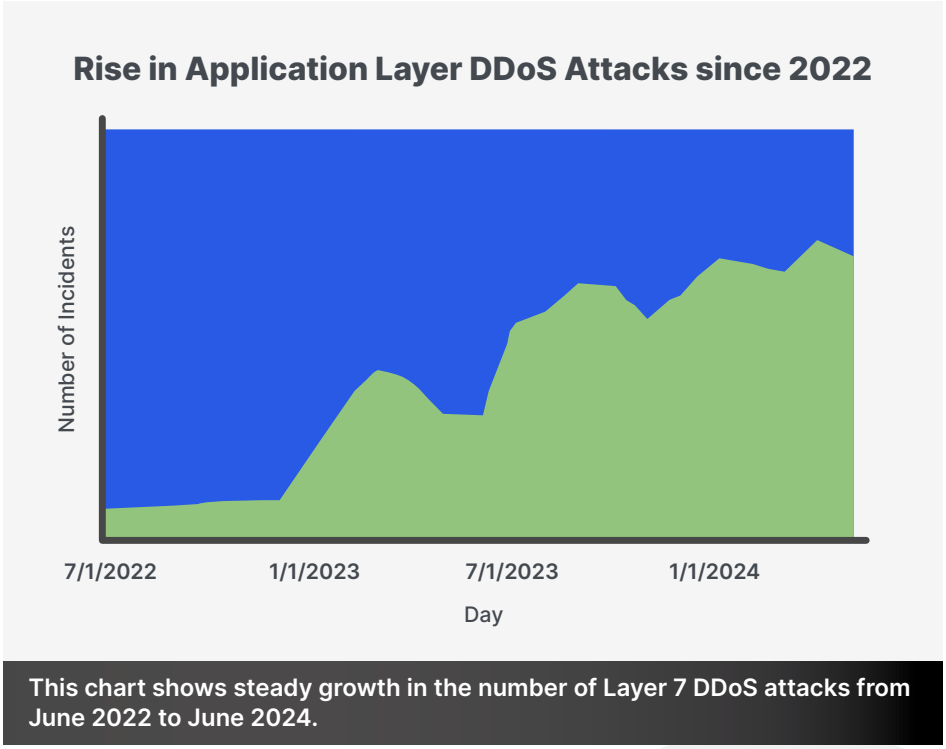
DDoS Attacks Growing in Number and Size

07

DDoS Attacks Growing in Number

The total number of recorded DDoS attacks surged 111% compared to the previous year. This notable rise underscores the escalating threat landscape and the growing importance of robust DDoS mitigation strategies.

Application Layer attacks increased by 110% year-over-year, with the largest mitigation reaching 4.7M RPS on February 24.



This chart shows steady growth in the number of Layer 7 DDoS attacks from June 2022 to June 2024.

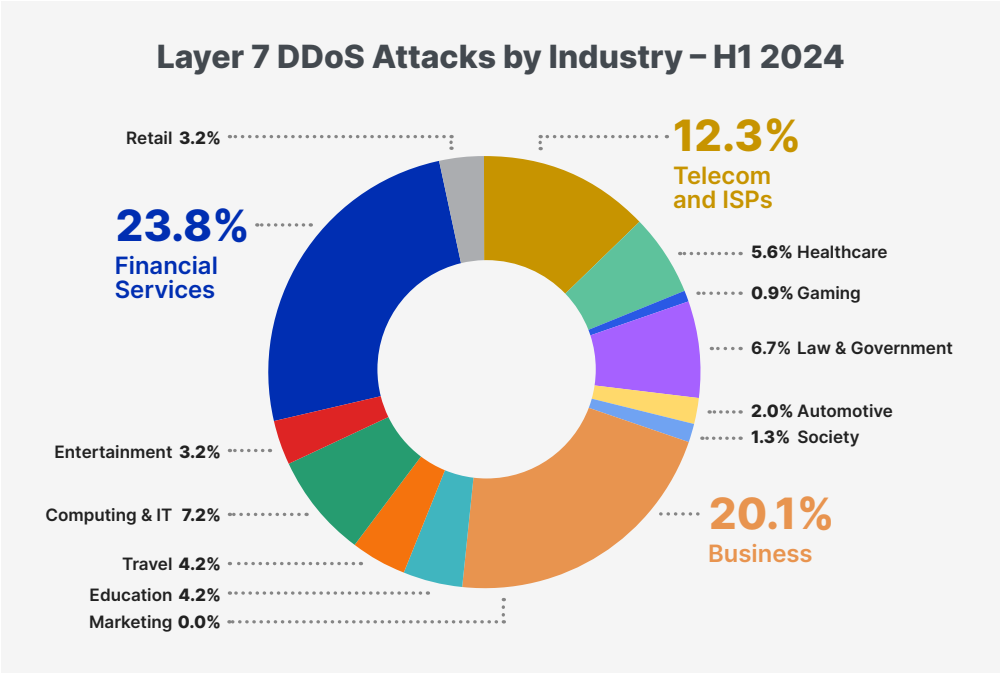
DDoS Attacks Growing in Scale

DDoS attacks have significantly escalated in scale. Notable incidents include:

- **February 2024:** The most significant Layer 7 DDoS attack targeted an Indonesian gaming site with 4.7 million RPS from 1,700 IPs in Canada, India, and the United States.
- **In March 2024,** we mitigated an unusually large attack against an online retail site in Romania measuring 4M RPS, a 2000% increase on the previous record for an attack in that country.
- **April 2024:** A Chinese entertainment site was hit with 4.2 million RPS from 2,600 IPs in China and the United States, lasting nearly five hours.

Top Targeted Industries

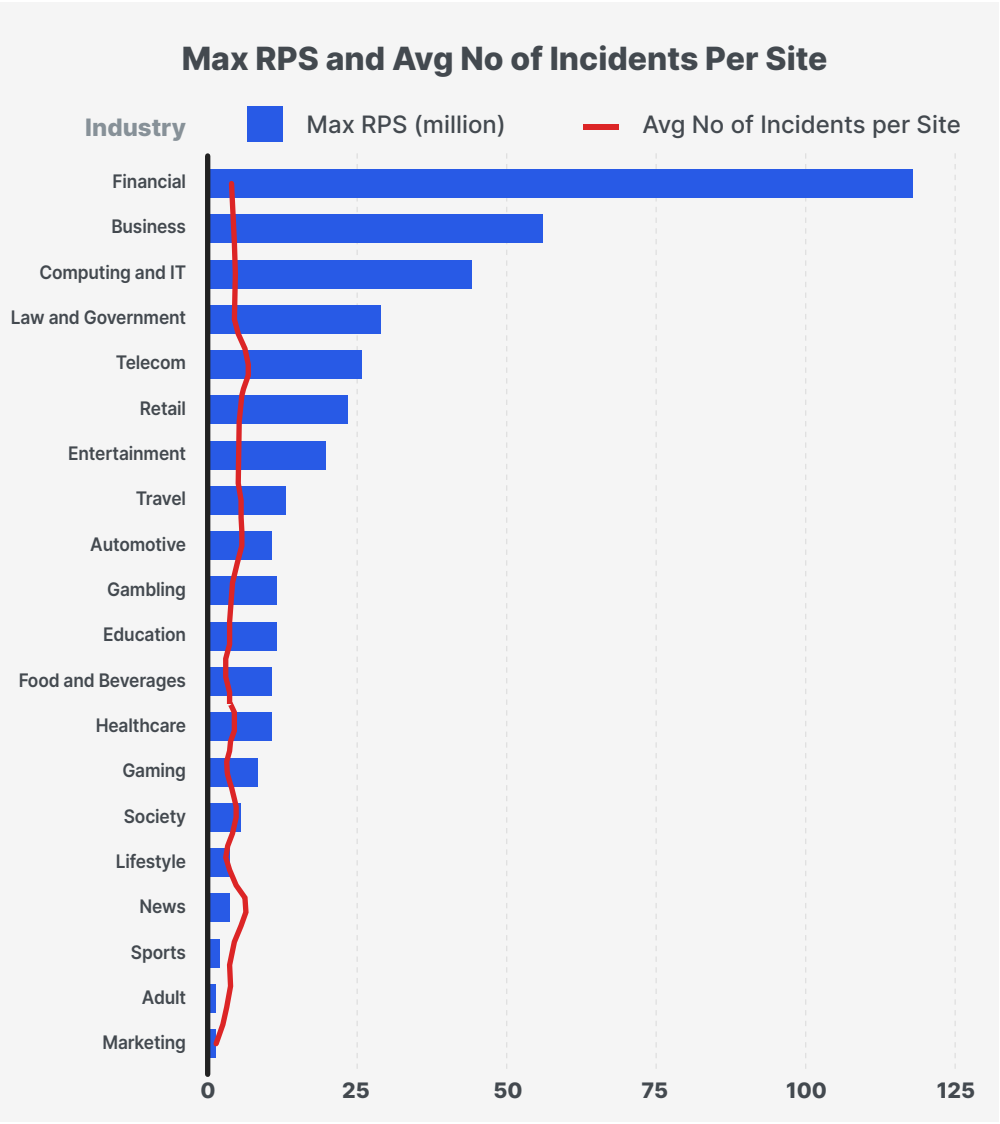
In the first half of 2024, Financial Services (23.8%), Business (20.1%), and Telecoms and ISPs (12.3%) were the top targeted industries, accounting for nearly 60% of all Layer 7 DDoS attacks.



Industries Targeted by the Most Forceful DDoS Attacks

Not only is the financial sector the number one target for DDoS attackers, but it is also the target of the most powerful DDoS attacks in terms of Requests per Second (RPS). When it comes to DDoS attacks, cyber assailants will use more force in an attempt to succeed where the potential gain is largest.

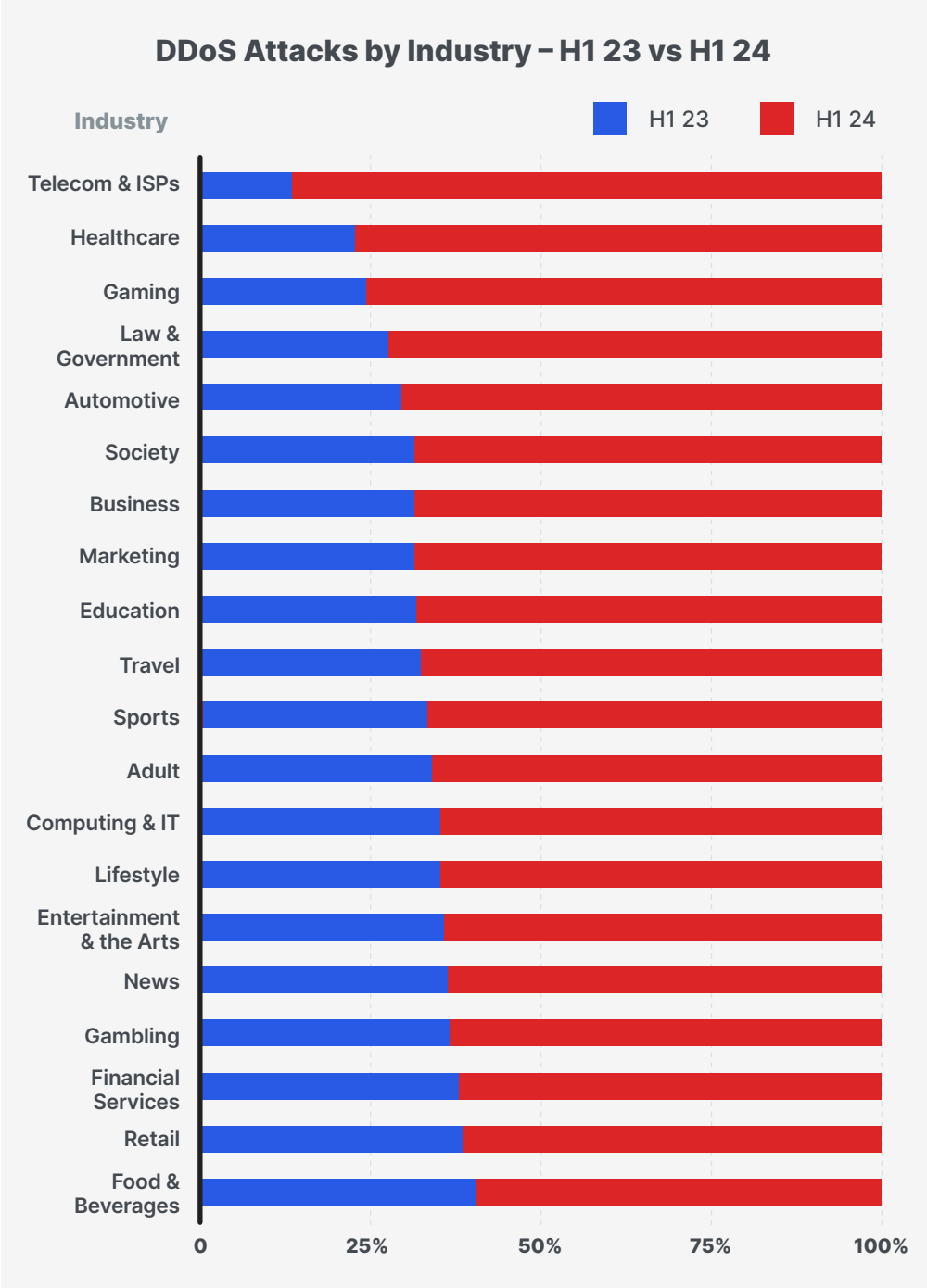
Not surprisingly, attacks on the financial services sector reached a combined RPS of 118 Million in H1 24, with the Business and IT sectors taking second and third place respectively.



Industries with Highest Increase in DDoS Attacks

Comparing the first half of 2024 with the same period last year, there has been a significant increase in DDoS attacks across several industries. The Telecom and ISP industry experienced the highest year-over-year growth, with a 548% increase in Application Layer DDoS attacks. Healthcare saw a 236% increase, and the Gaming industry witnessed a rise in attacks of 208%.

Cyber attacks against Internet Service Providers (ISPs) pose a serious and persistent threat to organizations and public authorities. ISPs are considered national critical infrastructure, providing internet services to businesses and individuals to keep services online and the economy functioning. For these reasons, ISPs are a top target for cybercriminals intent on causing maximum disruption.

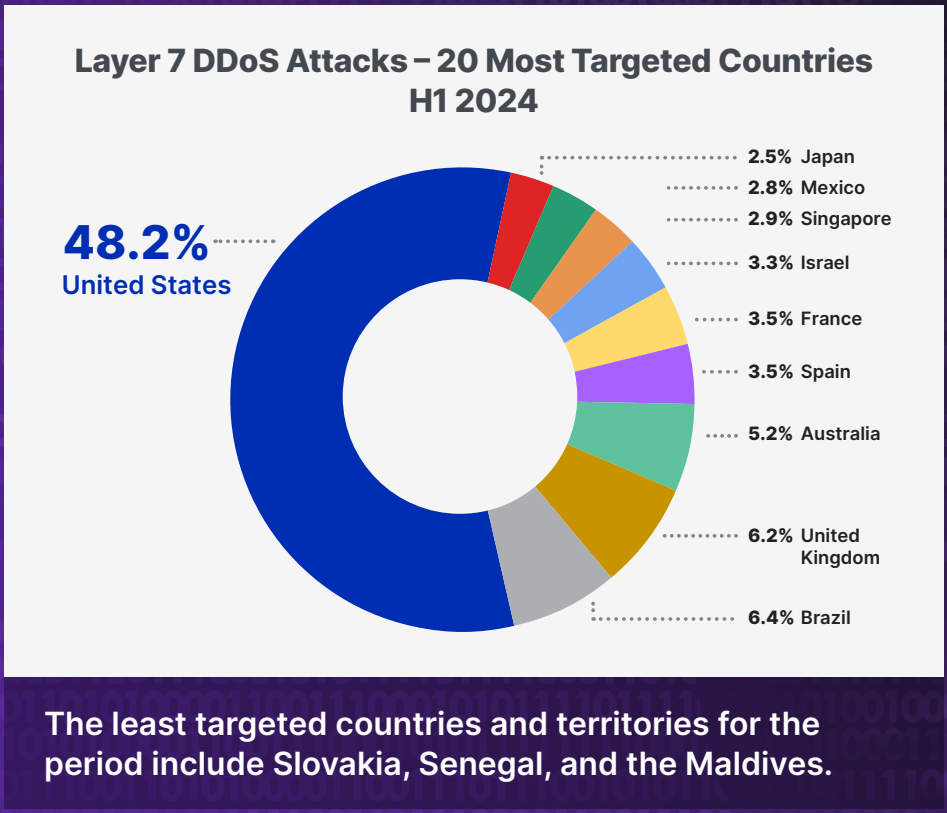


DDoS Attacks on Retail up 61%

Although not in the top 10, DDoS attacks on the retail sector have risen by nearly 61% since last year, reflecting a steady increase in cybercrime targeting e-commerce platforms and online retail operations. This trend highlights the sector's growing vulnerability as cybercriminals aim to disrupt sales and compromise customer data.

Top Targeted Countries

The United States remains the primary target for DDoS attacks, with nearly half of all Application Layer attacks in the first half of 2024 directed at the country. Brazil, the UK, and Australia also experienced significant attacks, but to a lesser extent.



The least targeted countries and territories for the period include Slovakia, Senegal, and the Maldives.

New Attack Vectors Mitigated

New attack vectors are always significant for cybercriminals as they allow them to add to their armory and enable the creation of more complex and sophisticated attacks.

This year we have observed two new major Application Layer DDoS attack vectors:

HTTP/2 Rapid Reset Attacks

HTTP/2 Rapid Reset is a relatively new type of attack, first seen in 2023. It is a denial of service vulnerability categorized as CVE-2024-44487 impacting the HTTP2 protocol, allowing http clients to open a stream and cancel it immediately afterward. This repeated open/cancel activity can, when done in large numbers, overload the server.

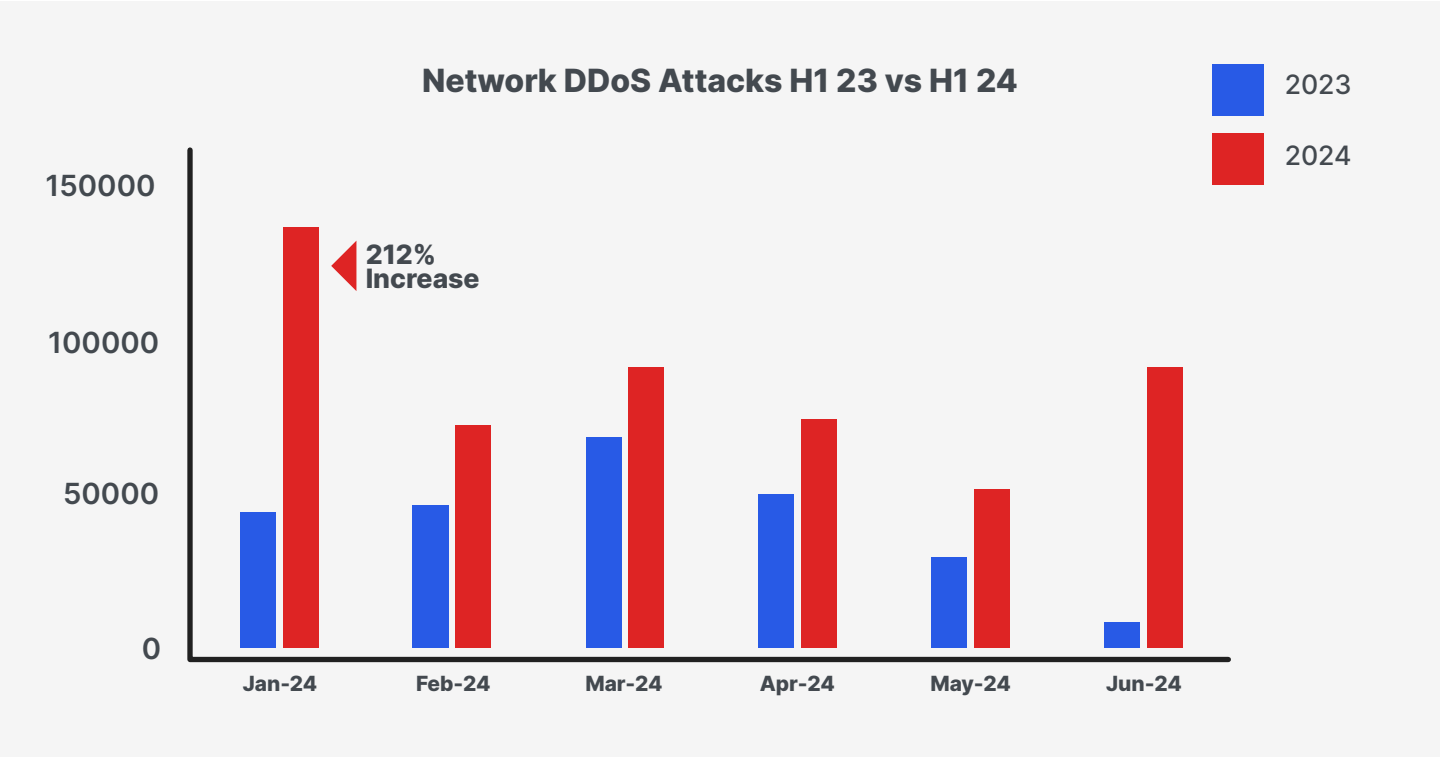
HTTP/2 Continuation Frame Attacks

Recently, there has been a surge in **HTTP/2 Continuation Frame Attacks**, a new type of Layer 7 DDoS attack. These attacks exploit vulnerabilities in the HTTP/2 protocol by sending continuous streams of small, fragmented requests to overwhelm servers. This method allows attackers to bypass traditional defenses and cause significant disruption with relatively low traffic volumes. The increase in these sophisticated attacks highlights the evolving threat landscape and the need for enhanced security measures to protect critical infrastructure.

Network Layer DDoS Attacks Increased Year-Over-Year

DDoS attacks on Layers 3 and 4 increased by 111% in H1 2024 compared to last year, with the most notable attack lasting over four hours, reaching 731 Gbps in March 2024.

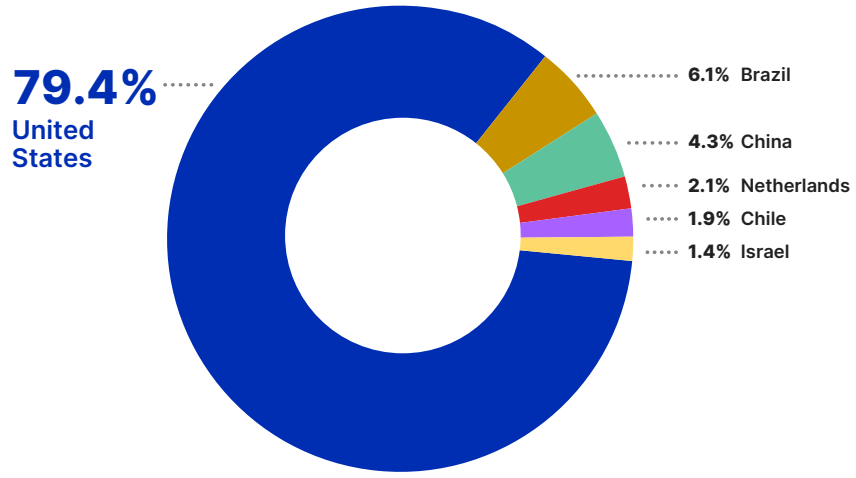
The most significant increase in the number of Layer 3 and 4 DDoS attacks was noted in January 2024, when attacks increased by 212% vs the same month the previous year.



Top Targeted Countries for Network Layer DDoS Attacks

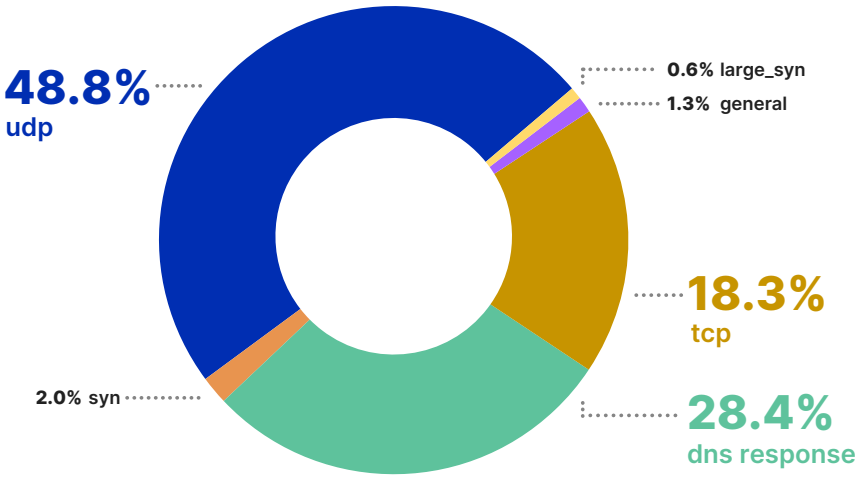
In H1 2024, almost 80% of all attacks targeted networks in the United States, with Brazil, China, and the Netherlands being the next most targeted countries.

Layers 3 and 4 DDoS Attacks – Top Targeted Countries



The least targeted countries include South Africa, Venezuela, and Bahrain.

Network Layer Attack Volume (Gbps) by Vector

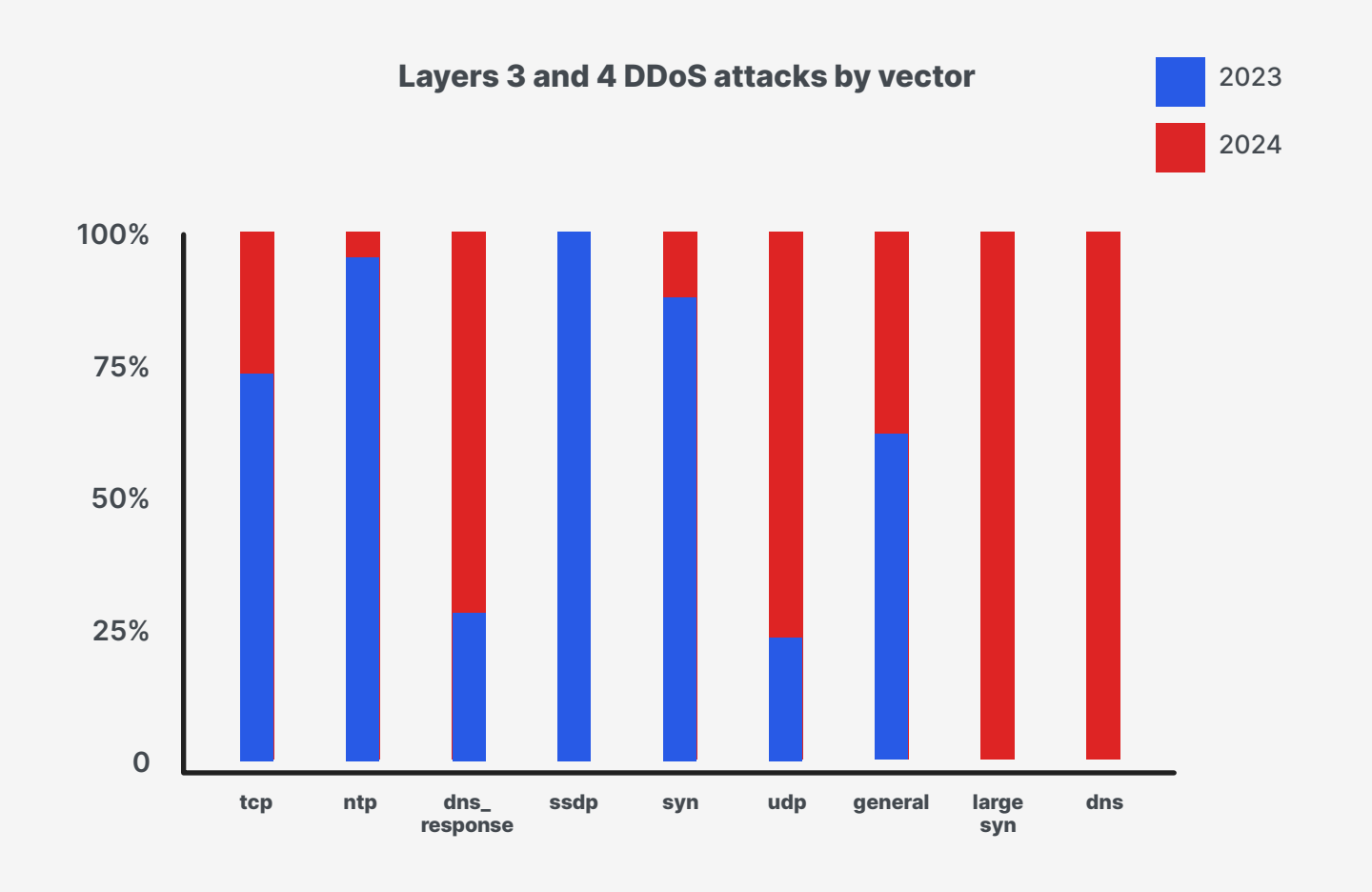


The chart above from May 2024 shows that DNS response attacks and UDP attacks account for the majority of Network Layer attacks. Both vectors experienced significant growth year over year.[3]

New Layer 3 and 4 Attack Vectors

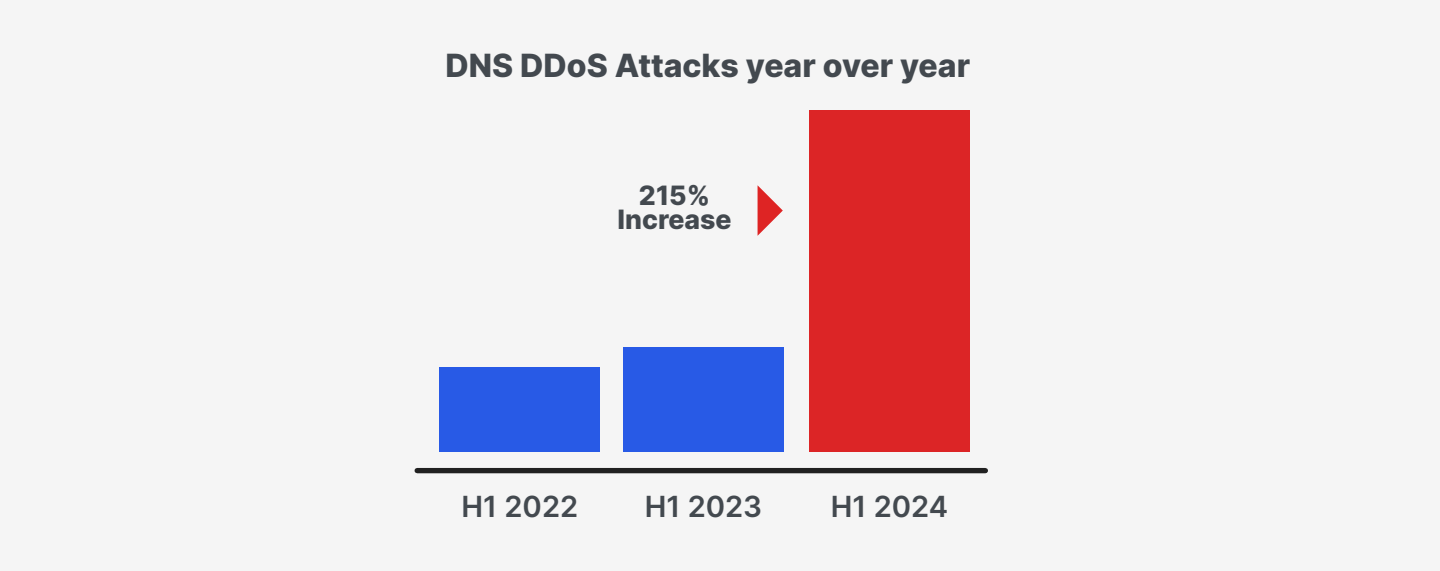
Application Layer Loop DoS Attacks

According to **The Hacker News**, this newly identified attack vector targets UDP-based protocols, both legacy (e.g., QOTD, Chargen, Echo) and contemporary (e.g., DNS, NTP, TFTP), causing servers to communicate indefinitely. Discovered by CISPA Helmholtz-Center researchers, it could affect around 300,000 internet hosts. Despite new DDoS vectors identified this year, Imperva observed no Layer 3/4 DDoS loop attacks in H1 2024.



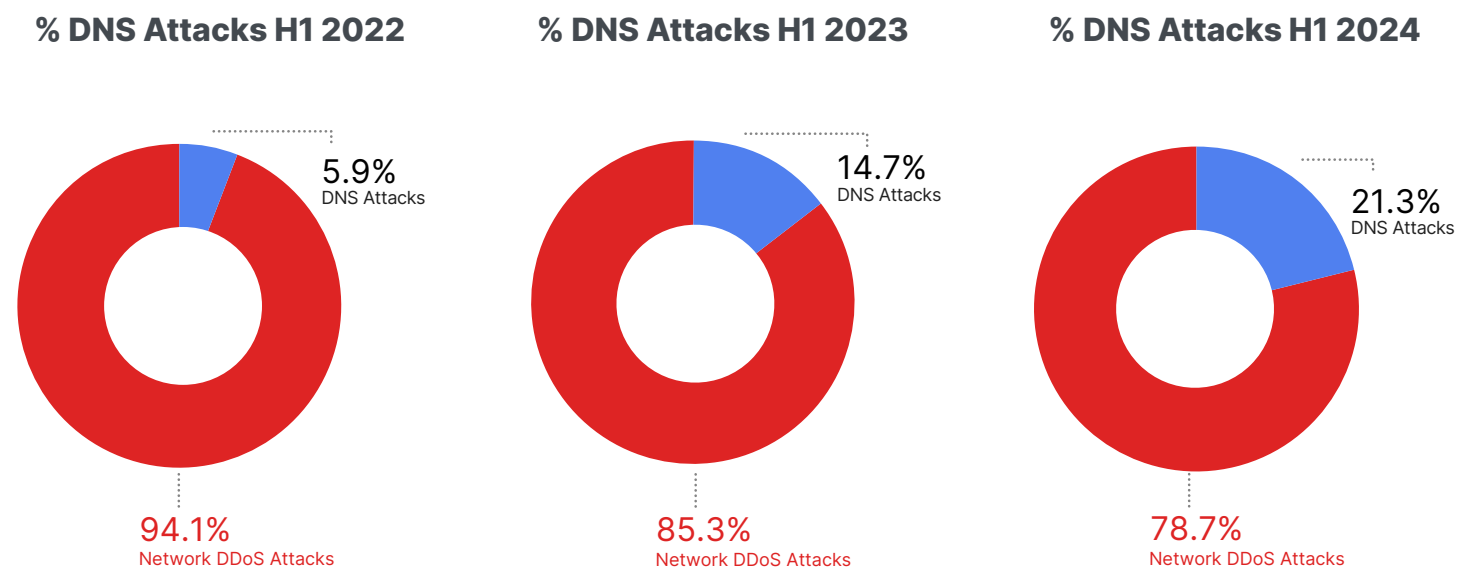
DNS Attacks Surge by 215%

DNS DDoS attacks are experiencing significant growth. Comparing H1 2024 with the same period the previous year, DNS DDoS attacks have increased by 215%.

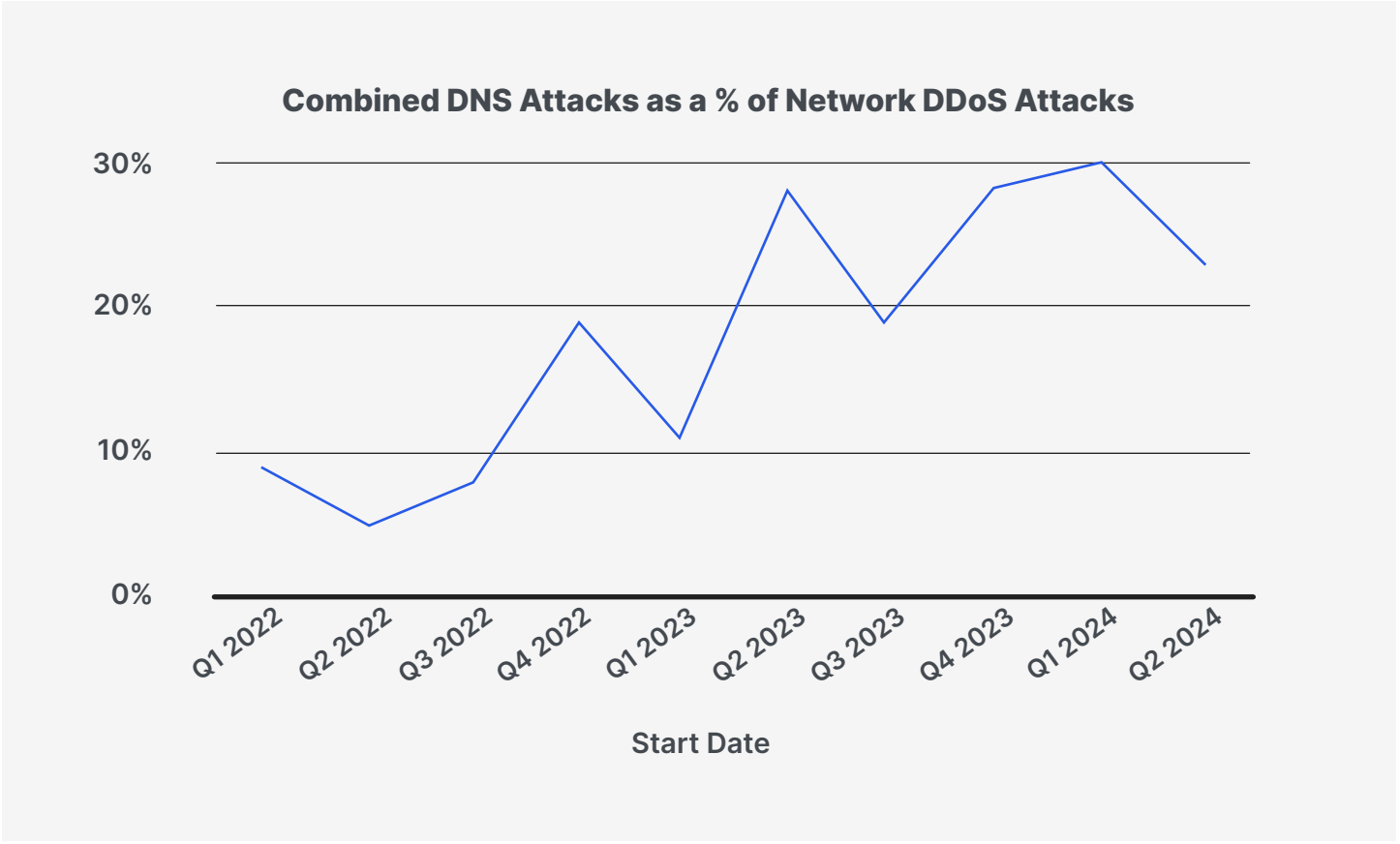


DNS Growing Its Share of the Network DDoS Attack Landscape

DNS attacks as a vector are increasing their percentage share of the overall Network DDoS attack landscape year-over-year. Accounting for only 6% of all Network DDoS attacks in H1 2022, DNS DDoS attacks accounted for more than 21% of Network DDoS attacks in H1 2024.



Both DNS Request and DNS Response vectors are experiencing growth as a percentage of the overall combined number of Network DDoS attacks as the chart below shows.

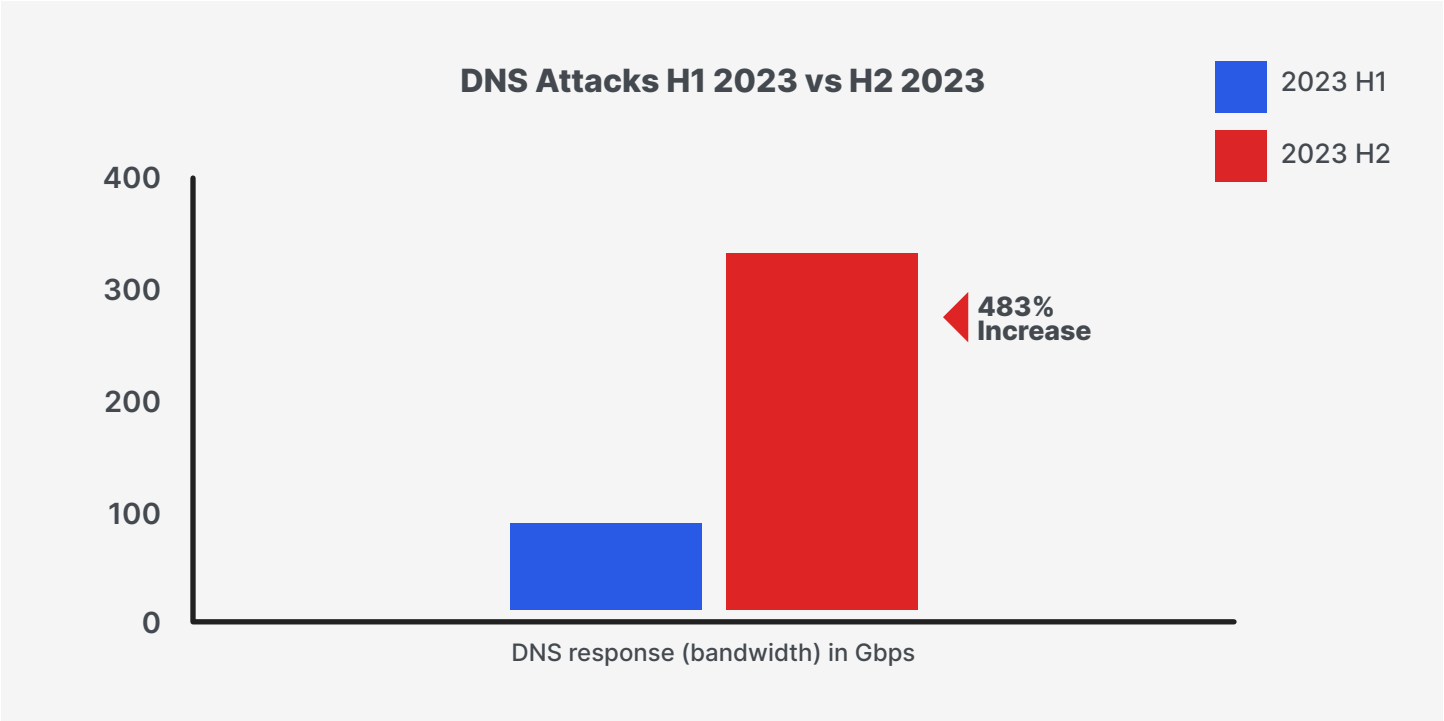


Both DNS Request and **DNS Response vectors**
are experiencing growth as a percentage of
the overall combined number of **Network DDoS attacks.**

DNS DDoS Attacks Increasing in Size

DNS amplification attacks can overwhelm servers by flooding them with queries, often from a botnet, causing a denial of service that translates into service degradation or outage of the attacked server or network.

In 2023, DNS Amplification attacks increased in terms of maximum bandwidth mitigated starting at 59 Gbps in H1 2023, as compared to reaching 344 Gbps in H2 2023.



The maximum bandwidth reached 59 Gbps in H1 2023, compared to 344 Gbps in H2 2023.

The rise in the number and the ferocity of attacks on DNS servers can be attributed to a number of factors, including their critical role in internet functionality, the proliferation of botnets, evolving attack techniques, and weak security practices. Financial, political motives, and the surge in insecure IoT devices also drive these attacks making DNS security a significant concern.

The average DNS Amplification attack bandwidth in H1 2023 was 59 Gbps, compared to **344 Gbps** in H2 2023, an increase of **483%**.

Hacktivism and Targeted DDoS Attacks

Hacktivist groups frequently employ DDoS attacks to disrupt critical infrastructure. Recently, NoName57(16), a Russian hacktivist group linked to geopolitical tensions, threatened European internet infrastructure during EU elections, as reported by **The Register**. Emerging post-Ukraine invasion, their preferred tactic, DDoS, remains a potent tool for causing disruption.

These groups, such as Anonymous Sudan and NoName57(16), underscore the persistent and evolving threat in cyber landscapes. In early 2024, Imperva responded to numerous DDoS attacks on national critical infrastructure. Notably, in March 2024, Imperva thwarted an attack on a major European airport, nearly reaching 1 million requests per second (RPS). Airports are prime targets due to their role as critical national hubs, where disruption can create logistical chaos.

Imperva also mitigated repeated DDoS assaults on communication agencies in Asia. One attack peaked at 2.5 million RPS, while another targeted agency faced a 1.5 million RPS onslaught. In February, a government office in Japan was also defended against a substantial 780,000 RPS attack.

National Critical Infrastructure Frequently Targeted by DDOS Attacks

- National Communications Agencies
- Broadcast Media
- Airports
- Hospitals
- Internet Service Providers
- Government Offices

DDoS Attacks on Major Sporting Events

In February 2024, Imperva thwarted its largest DDoS attack of the year, peaking at 4.7 million RPS. One possible motivation for the attack targeting an Indonesian gaming site could be the AFC Cup Soccer Tournament, which was taking place at the time. Hacktivists often exploit major events to maximize the impact of their attacks, and with France and Germany hosting the Olympic Games, and the UEFA Europe 2024, respectively this year, associated industries are at increased risk. One example of this is the **Polish Sports channel hit by a DDoS attack** during their national team's Euro 2024 game against the Netherlands.

Our threat research indicates that Layer 7 DDoS attacks on European travel, sports, entertainment, and gambling sites surged 89% compared to last year, with peak attack intensity reaching 1.5 million RPS.

For more insights into the impact of DDoS attacks on critical infrastructure during major sporting events, read our blog: **A European Summer of Sports is Upon Us - What Does it Mean for Security?**

Anticipated DDoS Trends and Future Outlook for 2024

Election-Related DDoS Attacks: With 2024 being a significant election year globally, nearly half of the world's population will head to the polls. Elections are often accompanied by spikes in DDoS attacks driven by hacktivist activities and political unrest. For instance, the pro-Russia hacktivist group NoName57(16) emerged post-Ukraine invasion and targeted European internet infrastructure during EU elections. Such incidents exemplify how geopolitical tensions can drive increases in DDoS attacks.

Mirai Botnet Variants: In early 2024, our research observed the delivery of Mirai botnet malware to over 1,200 sites through web vulnerabilities. While the ultimate goal remains unclear, Mirai's history of executing large-scale DDoS attacks is well-documented, signaling potential future threats. Read the full blog here.

AI Lowering Attack Barriers: AI makes it easier for less-skilled attackers to exploit new vulnerabilities quickly. For instance, AI tools can automate the creation and deployment of sophisticated DDoS attacks, allowing even novice hackers to launch powerful attacks. This trend increases the likelihood of significant DDoS attacks powered by AI-enhanced botnets, such as potential new variants of Mirai.

Changes in DDoS Hacking Groups: The cyber threat landscape has evolved, particularly with the disappearance of the prominent DDoS hacking group Anonymous Sudan. Known for aggressive attacks, especially on Israeli sites, their sudden silence has left a notable gap. In February 2024, they claimed responsibility for DDoS attacks on OpenAI's ChatGPT, demanding changes to the chatbot's behavior amid geopolitical tensions. Since then, their activity has ceased, possibly linked to these high-profile incidents.

DDoS Best Practices When Under Attack

- Be proactive
- If you don't have access to always-on DDoS Protection, ensure you at least have on-demand protection in place
- Do your investigations now and get protected with a DDoS solution
- If you find yourself under attack, choose a provider with quick and easy onboarding. You can also bookmark the page to reach us directly should this happen to you.
- Keep the dialogue open between the security and networking teams
- Choose a reputable DDoS provider with a global presence and the capacity to mitigate high-volume and sophisticated attacks
- Choose a low-latency solution with fast and accurate mitigation

About Imperva

18

Imperva is the cybersecurity leader whose mission is to help organizations protect their data and all paths to it.

Customers around the world trust Imperva to protect their applications, data, and websites from cyber attacks. With an integrated approach combining edge, application security, and data security, Imperva protects companies through all stages of their digital journey. The Imperva Threat Research team and our global intelligence community enable Imperva to stay ahead of the threat landscape and seamlessly integrate the latest security, privacy, and compliance expertise into our solutions.

To find out more about Imperva DDoS Protection, visit our website.