MAZEBOLT

2025 DDoS Trends Report

Predictions Based on MazeBolt Research into DDoS Attacks

Table of Contents

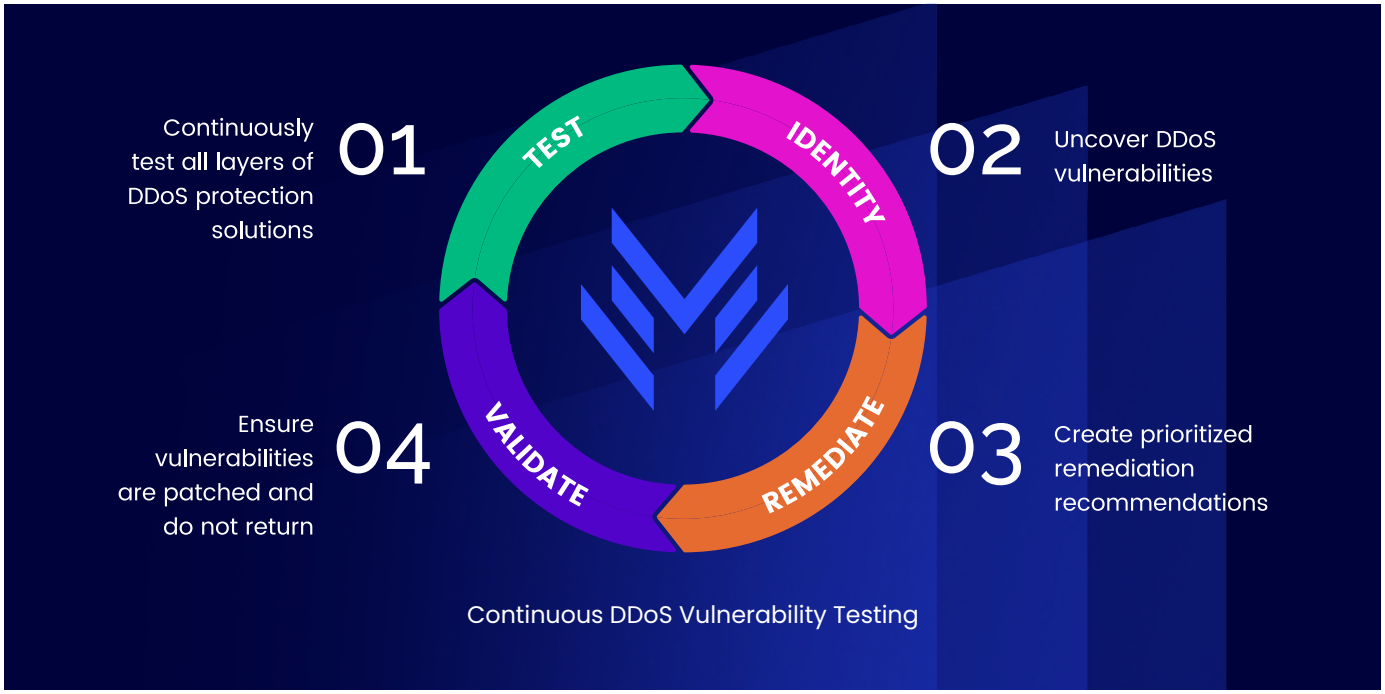
Executive Summary

Why does the risk of Distributed Denial-of-Service (DDoS) attacks continue to rise?

DDoS attacks surged almost a third (30%) in the first half of 2024 compared to the same period in the previous year. Moreover, DDoS attacks on critical infrastructure increased by 55% in the last four years.

Hacktivist groups motivated by political and ideological agendas are driving the current growth in DDoS attacks. Moreover, today's DDoS attacks may utilize advanced botnets to implement sophisticated attack methods that ensure they are harder to detect and neutralize.

Security leaders need to promote an understanding that the main reason DDoS attacks still succeed is due to the existence of vulnerabilities in the DDoS protection being relied on.



This type of ongoing, proactive approach is crucial to maintaining DDoS resilience and supporting the business continuity of online services.

This report provides insight into MazeBolt's DDoS predictions for 2025, based on our own research and reports in the media during 2024.

DDoS Attack Trends for 2025

Based on MazeBolt's internal and market research, we can expect to see the following DDoS attack trends continuing throughout 2025:

Threat to Democratic Elections

Politically motivated hackers can be expected to continue targeting countries undergoing election cycles. The attacks are likely to be both in the months leading up to elections as well as after the polls have opened. These types of attacks may be successful in causing downtime of electoral websites and infrastructure, and they can undermine the public confidence in election results.

Greater Regulatory Enforcement

Companies will continue to invest in adapting their cybersecurity processes to meet the more stringent regulations that came into effect recently, and avoid stiff fines.

In-Depth Reporting

Companies will need to provide in-depth, timely DDoS resilience and attack reports to meet the regulations, and this will create a greater need for the ongoing visibility and attack prevention capabilities provided by continuous DDoS vulnerability testing.

Industries at Greater Risk

Companies in the industries of banking and financial services, insurance, healthcare, and transportation are expected to continue being targeted more than other industries, throughout 2025.

DDoS-for-Hire Services

DDoS-for-Hire gives less technically proficient threat actors an easy way into the hacking industry, by making it easier to launch DDoS attacks. The increase in DDoS-for-Hire tools is particularly notable in Asia and is connected to the rising risk of DDoS attack across multiple sectors. DDoS-for-Hire gives users the ability to carry out an unwarranted performance, on a network.

Lost Business	Downtime of Services or Websites	Damage to Professional Reputation	Increased Churn as Customers Lose Trust
Legal Costs	Time Invested in Response & Recovery	Compliance & Regulatory Fines	Reputation Management (PR/Media)

The Cost of DDoS Attacks to Businesses

2024 DDoS Attack Analysis

A closer look at recently reported DDoS attacks shows that new DDoS attack techniques and emerging vulnerabilities are creating significant challenges for organizations that are trying to protect their digital services. Here are the most significant attack trends that emerged based on the data from recent DDoS attacks.

The Threat to Democratic Elections

2024 was a landmark year in electoral politics, with 50 countries plus the European Union - representing a total of over 2 billion voters – holding elections. Politically motivated DDoS attacks took place in countries in the months leading up to elections as well as after the polls opened.

In some cases, the DDoS attacks were successful in disrupting critical election infrastructure, causing downtime, and undermining the confidence of the public in the reliability of election results. DDoS attacks peaked around critical dates, indicating a coordinated effort to disrupt electoral processes. Funding for the work of the threat actors, including both criminal groups and hacktivists, allegedly was provided by nation-states. Examples of DDoS attacks during election cycles include:

US

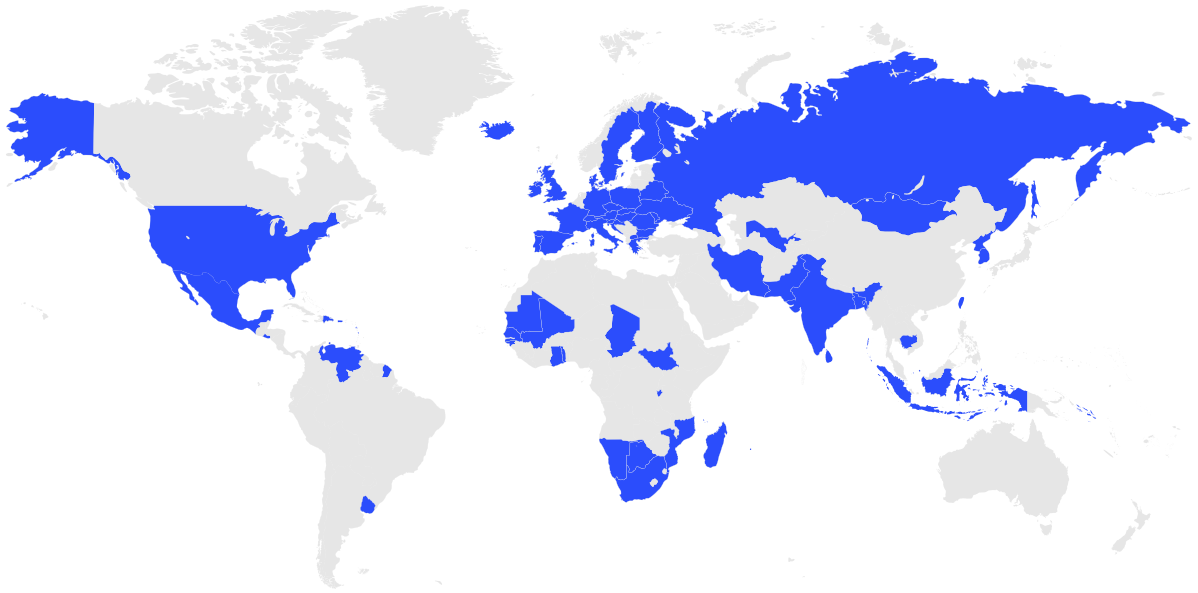
What is a DDoS Attack? Elon Musk Claims Cyberattack Delayed Trump Interview - link

France

First Round of French Election: Party Attacks and a Modest Traffic Dip - link

Venezuela

Venezuela's Election as seen in Cyberspace - link



"Super Election Year" - 54 Elections throughout 2024 (Credit: Time)

More Stringent Compliance Regulations

With the DORA and NIS2 Directive regulations in the EU, and new SEC regulations in the US, 2024 has seen a significant shift in the stringency of DDoS testing. One of the key aspects of the regulations involves more in-depth, transparent, and timely reporting requirements – and continuous DDoS testing is essential to complying with these requirements.

Regulatory Framework	Date for Compliance	Where It Applies
New SEC regulations	December 18, 2023	US
NIS 2 Directive	October 17, 2024	EU
DORA	January 17, 2025	EU

Enterprises doing business in Europe and the US must enhance their cybersecurity processes to meet the new regulations and avoid hefty fines. The DORA regulations, for example, are based on the following five pillars:

The 5 Pillars of DORA Regulation

High-Profile Arrests of Perpetrators of DDoS Attacks

Law enforcement officials are also making the headlines – with a number of instances in which the authorities have taken steps to detain groups responsible for high-profile DDoS attacks. In some cases, the arrest led to a new rash of DDoS attacks in response. For example, after the arrest of Telegram's CEO Pavel Durov, several hacking groups launched a #FreeDurov DDoS campaign against online services in France. Here are some of the stories covered in the media:

US
Two Sudanese Nationals Indicted for Alleged Role in Anonymous Sudan Cyberattacks on Hospitals, Government Facilities, and Other Critical Infrastructure in Los Angeles and Around the World - link

France
Telegram's CEO & Founder Durov Under Arrest: Cybercriminals React - link

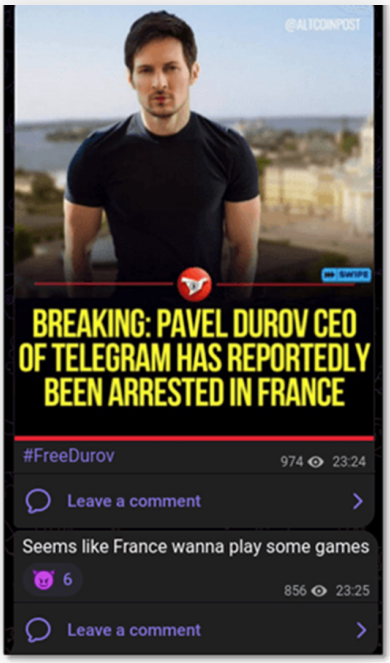
UK
17-Year-Old Linked to Scattered Spider Cybercrime Syndicate Arrested in UK - link

Spain
Spanish Police Arrest Three Suspects Linked to Pro-Moscow NoName057(16) Hackers - link

Japan
International Investigation of DDoS Leads to Oita Man's Arrest - link

Cambodia
Anti-government Hackers Arrested After Attacks on Cambodian Official Websites - link

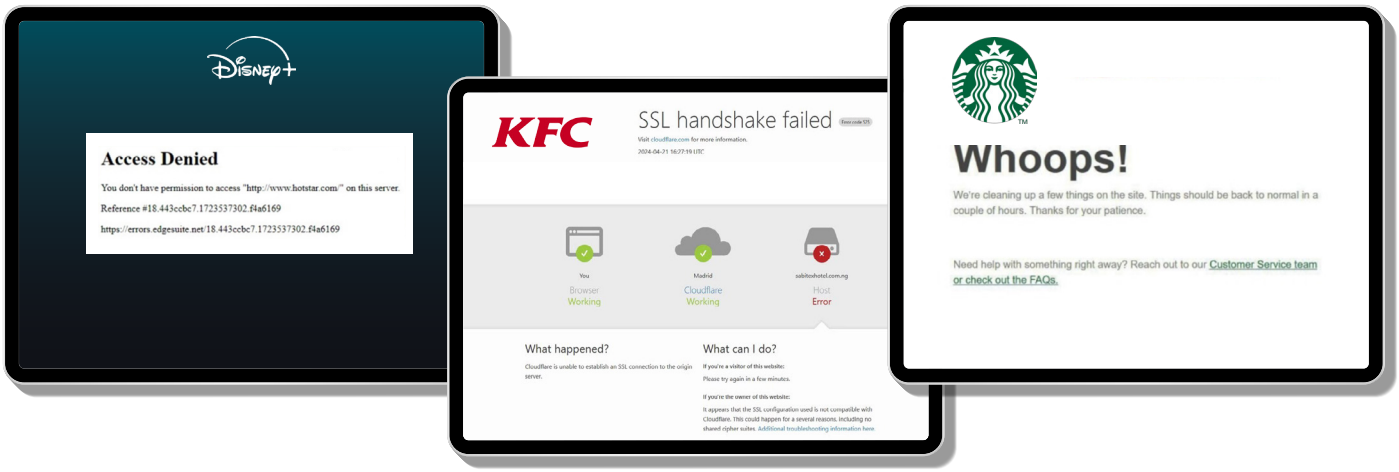
Musk Announced a DDoS Attack on X During Trump Election Interview



#FreeDurov DDoS Campaign (Credit: Check Point)

A Shift in DDoS Public Awareness?

DDoS attacks on big name brands such as Disney+ in France, KFC in Italy, and Starbucks in the US were discussed in online forums and on social media. While these attacks were not confirmed publicly as DDoS attacks, the headlines associating them with DDoS are indicative of an increase in public awareness of DDoS dangers.



Alleged DDoS Attacks on Disney+ in France, Kentucky Fried Chicken in Italy, and Starbucks in the US

Top DDoS Targets: Breakdown by Industry

The following industries were the worst hit by DDoS attacks:

Finance
Disrupted online services and availability, causing financial and reputational damages

Healthcare
Targeted the patient management systems and telemedicine platforms used by healthcare providers

Government
Often coincided with political events; aimed to erode public trust and disrupt administrative functions

Transportation
Disrupted airlines and railway booking systems; exposed or blocked access to sensitive data; and impacted supply chains

While many organizations try to hide cyber breaches, the information that did become public made it clear that the most frequently attacked organizations provide financial services. These include banks, payment processors, and other financial organizations. After financial services, the industries most targeted include healthcare, government organizations, and transportation.

The Most Prevalent Types of DDoS Attacks

The impact of a DDoS attack depends on several factors, including the scale of an attack, the nature of the attack, and the ability of the target system to handle the attack. While the frequency of DDoS attacks continues to rise, the attacks are also evolving in complexity and scale. For example, sophisticated DDoS attack methods are being implemented by advanced botnets such as the botnet malware family Gorilla.

In recent months, a marked increase has been seen specifically in the following types of DDoS attack:

	What Is It	How It Works	Examples
Volumetric Attacks	A botnet attack floods the network with traffic that appears to be legitimate but soon overwhelms the network.	Stifles legitimate traffic, exhausts bandwidth, and results in bringing down an entire website.	Smurf Attacks, ICMP Floods, IP/ICMP Fragmentation.
Targeted Application Layer Attacks	Requires fewer resources, and targets vulnerabilities within applications by mimicking legitimate user behavior.	Overwhelms specific applications or services with malicious requests, depleting server resources and disrupting legitimate user access.	HTTP-encrypted floods, attacks on DNS services.
Multi-Vector Assaults	Sophisticated attack that combines multiple attack techniques or vectors.	Distracts the defense team with a noisy DDoS attack while employing additional attack techniques on other systems.	A trojan is activated while a DDoS attack disables all services.

A Growing Threat: DDoS-for-Hire Services

Typically, DDoS attacks were carried out by highly skilled hackers with access to large networks of compromised devices, often referred to as botnets. With the rise of the commercialization of cybercrime, a new and concerning trend has emerged: DDoS as a Service (DDoSaaS). This trend significantly lowers the barrier to entry for launching powerful DDoS attacks. It is a model that allows individuals with limited technical skills to utilize botnet infrastructure and launch attacks against targets of their choice.

Greater Accessibility

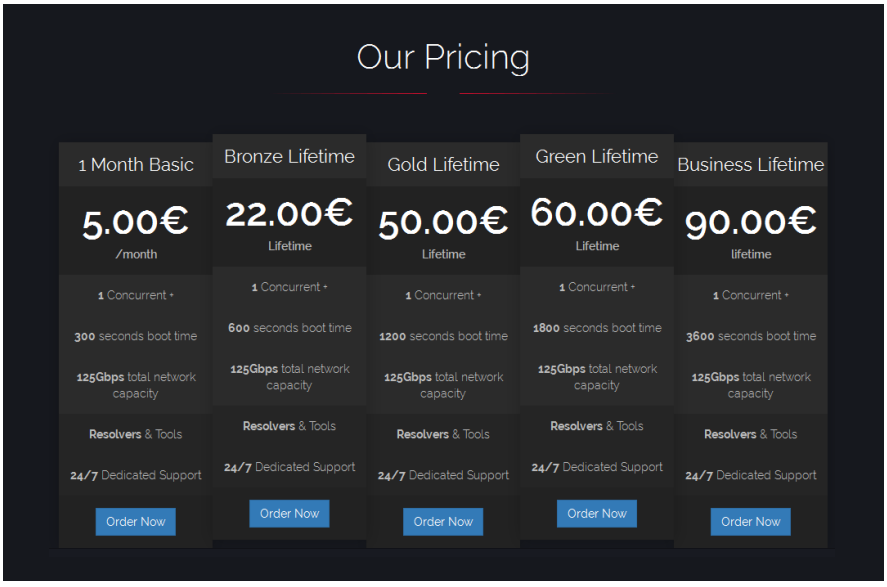
DDoSaaS platforms are available on the dark web – as well as through "legitimate" channels on the open internet, where they are marketed as "stress testing" services. (By masquerading as legitimate services, they can be sold on the open internet.) "Legitimate" channels include Telegram Channels, DDoS-for-Hire Forums and API-based DDoS Platforms.

These services provide simple, web-based dashboards and interfaces, allowing users to easily configure and launch attacks without requiring in-depth technical knowledge. Users can usually select from various DDoS attack types, including volumetric floods, protocol attacks, and application layer attacks.

Greater Affordability

Services are typically offered through tiered subscription plans, with prices ranging from as low as $10 (on sale!) to $500 per month. Pricing often depends on factors like attack duration, volume, frequency, and the number of concurrent targets.

Most platforms accept easy-to-use payment methods such as cryptocurrency payments – particularly Bitcoin, for anonymity. Some services even accept PayPal and other payment methods.



Example of Advertised Prices and Capacities of a DDoS-for-Hire Service

More Effective

DDoSaaS providers maintain networks of compromised devices (frequently called botnets) to carry out attacks. These botnets can sometimes generate very high traffic volumes.

Many of these services utilize reflection and amplification methods to increase attack power and effectiveness.

Most platforms offer features to hide users' identities, like not tracking IP addresses and encouraging VPN/Tor network usage.

Providers Operate Like Legitimate Businesses

Many DDoSaaS providers offer customer support, tiered service packages, and performance guarantees. Some even offer Service Level Agreements (SLAs) and refunds if an attack doesn't achieve the desired outcome.

Beyond DDoS, some platforms offer other malicious tools like IP trackers or credential stuffing services.

DDoSaaS is Contributing to a Notable Surge in DDoS Attacks

The proliferation of DDoSaaS has democratized cyberattacks, making them accessible to anyone with malicious intent and a modest budget. As a result, organizations must be more vigilant than ever, adopting proactive cybersecurity measures. Businesses can reduce the risk of downtime, protect their reputation, and ensure the continuity of their operations by:

- Understanding the mechanics of DDoSaaS
- Implementing robust defenses
- Continuously testing for DDoS vulnerabilities

DDoSaaS is not just a passing fad. It's a growing business that has solidified its place in the cybercrime ecosystem. The best defense is to be proactive, continuously test for vulnerabilities, and adapt to the changing threat landscape.

Drill-Down: Top Attacks

The tables below provide insight into DDoS attacks published in the media during the third quarter of 2024. See also MazeBolt's attack reports for Q1 and Q2.

July

Date	Location	Vertical	Companies Affected	Attacker	Headline
July 3 & 7	France	Politics	French political party websites	Unknown	Link
July 23	Spain	Government	Spain's Ministry of the Interior	NoName057	Link
July 23	Brazil	Education	Federal University of Amapá	Unknown	Link
July 25	UAE	Financial Services	Financial institution in the Middle East	BLACKMETA	Link
July 28	Venezuela	Government	Venezuela's CNE (National Electoral Council) systems	Unknown	Link
July 30	Russia	Government	Banks, government websites, telecommunications and social networks	Hackers from the Main Intelligence Directorate of Ukraine	Link
July 30	United States	Information Technology	Microsoft	Unknown	Link

August

Date	Location	Vertical	Companies Affected	Attacker	Headline
August 6	United Kingdom	Transportation	The Port of Tyne	Unknown	Link
August 7	Venezuela	News	TalCual newspaper	Unknown	Link
August 8	Russia	Government	Government and business websites, and critical infrastructure services, in the Kursk region	Unnamed hackers	Link
August 13	United States	Social media	X (formerly Twitter)	Unknown	Link
August 16	Ukraine	Banking	Monobank	Unknown	Link
August 21	Russia; also impacted Kazakhstan, Uzbekistan, Serbia, and other countries		Telegram, WhatsApp, and websites such as Wikipedia, Skype, and Discord	Unknown	Link
August 23 & 25	International	Gaming	Final Fantasy	Unknown	Link
August 25	International	Gaming	Minecraft	Unknown; the botnet was concentrated in Russia	Link

September

Date	Location	Vertical	Companies Affected	Attacker	Headline
Sep 3	United States	Web services	Internet Corporation for Assigned Names and Numbers (ICANN)	Unknown	Link
Sep 4	France	Government agencies, healthcare, airports, educational institutions, and private companies	Over 50 French organizations	Pro-Russian and pro-Islamic groups including Cyber Army of Russia Reborn (CARR), RipperSec, EvilWeb, CyberDragon, UserSec, and STUCX Team	Link
Sep 10	Taiwan	Government	Hsinchu Local Tax Bureau and other Taiwanese government and financial units	NoName057	Link
Sep 21	United States	Gaming	Rockstar	Unknown	Link
Sep 23	Ukraine	Investigative journalism	Slidstvo.Info	Unknown	Link
Sep 25	Austria	Financial service entities, airports, and the stock exchange	More than 40 Austrian organizations	NoName057 and OverFlame	Link

Key Takeaways

Even with the best DDoS protections in place, the MazeBolt research team has found that, on average, 37% of an organization's DDoS attack surface still remains vulnerable to DDoS attacks. This is because, over time, changes in IT systems and online services lead to security policy drift that results in DDoS vulnerabilities and misconfigurations, which leave organizations unprotected.

Shifts in the DDoS attack landscape that were particularly noteworthy this year included:

- The growing number of attacks disrupting elections
- New and more stringent compliance regulations that went into effect (NIS2, DORA)
- Greater public awareness of DDoS – in response to both the headlines around high-profile arrests of perpetrators of DDoS attacks, and several alleged DDoS attacks on big name brands
- Increased adoption of the business model known as DDoS-for-Hire services

Protecting organizations from damaging DDoS attacks – and thereby strengthening the business continuity of online services – requires:

- Continuous DDoS Testing
- Sharpening of Operational Resilience
- Transparency and Reporting
- Regulatory Compliance

About MazeBolt

MazeBolt RADAR™ is a patented DDoS Vulnerability Management solution. Using thousands of non-disruptive DDoS attack simulations and without affecting online services, it can identify and enable the remediation of vulnerabilities in deployed DDoS defenses. RADAR enables organizations and governments to maintain the uninterrupted business continuity of online services. Using RADAR's patented vulnerability simulation technology, enterprises have unparalleled visibility into their DDoS protection solutions so they can be confident that damaging DDoS attacks can be prevented - before they happen.

Read more at: www.mazebolt.com

MAZEBOLT