MAZEBOLT

DDoS Threat Landscape Report

Q1 2025 Review

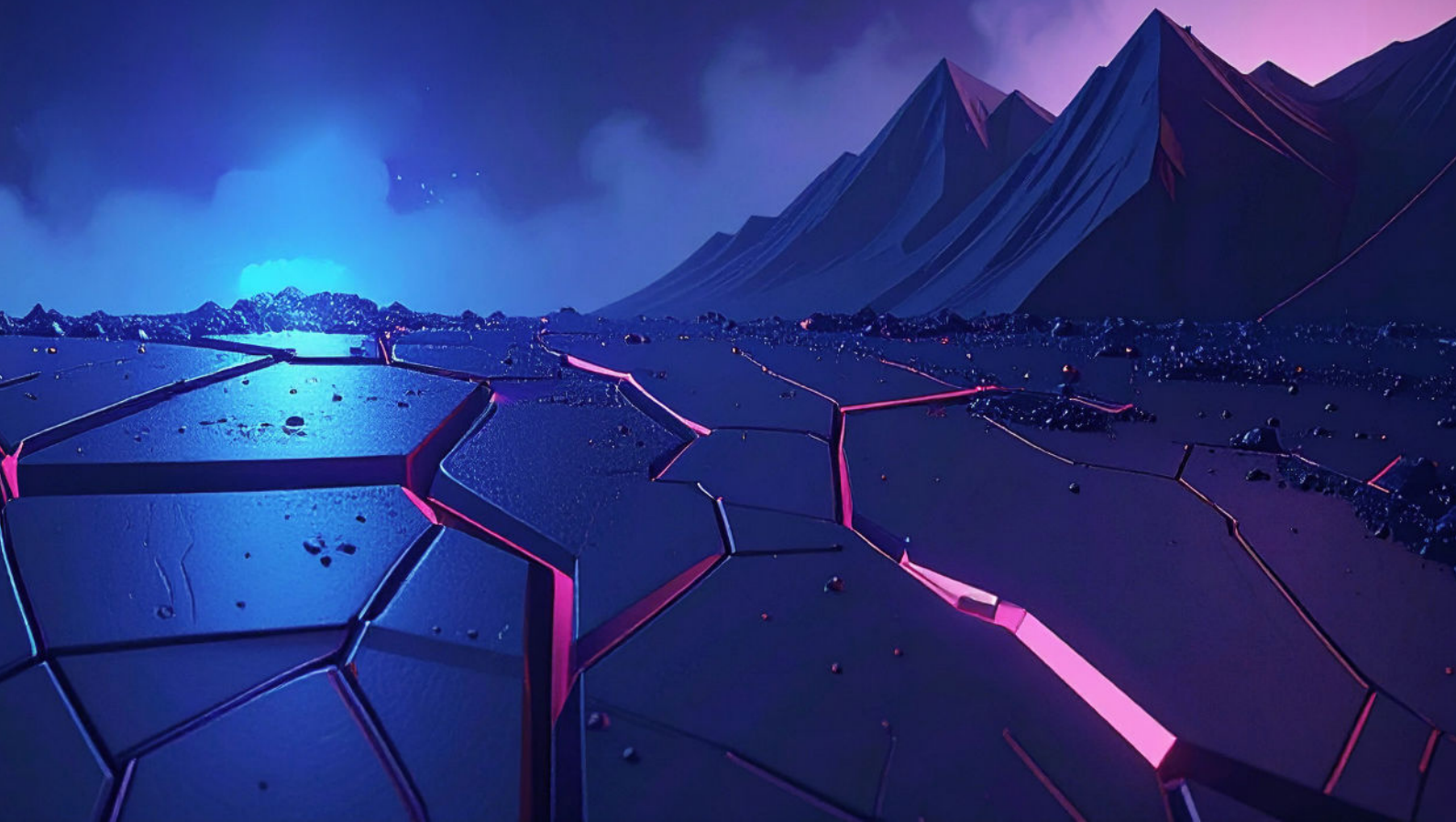


Table of Contents

Executive Summary

The Distributed Denial-of-Service (DDoS) threat landscape is intensifying. In the first quarter of 2025, research shows that the number of DDoS attacks jumped 358 percent compared to the same period as last year. The rise is not just in the volume but also in the size of these attacks, which included some of the largest ever recorded.

As organizations continue to boost their DDoS security investments, many remain exposed to attack. The root cause? Critical gaps in DDoS protection configurations that allow even the most basic DDoS attacks to succeed.

Notable developments from the first quarter of 2025 include:

- **56% of financial sector Scrubbing Centers are highly vulnerable**
  MazeBolt RADAR data shows that over half of scrubbing centers in the BFSI sector are critically exposed due to unseen misconfigurations. Organizations lack visibility into these weaknesses—until a damaging DDoS attack exposes them.

- **X platform downtime traced to DDoS misconfigurations**
  In March 2025, the social platform X suffered multiple DDoS-related outages. Analysts revealed that origin servers were left exposed due to misconfigured protections, enabling attackers to bypass defenses despite premium DDoS mitigation in place.

- **Hacktivist group NoName(057) amplifies attacks with DDoSia Project**
  This pro-Russian group uses a crowdsourced DDoS platform to coordinate daily attacks on government, infrastructure, and banking sectors. With over 20,000 active users and multiple alliances, their reach and impact continue to grow.

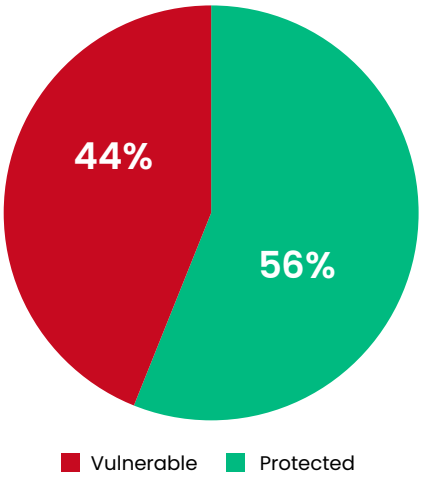
- **DDoS is now a stealth tactic for breaches and ransomware**
  Modern cyberattacks increasingly combine DDoS with ransomware and data breaches. DDoS is used to distract defenders or extort organizations, while attackers infiltrate systems - making real-time visibility and proactive remediation essential for defense.

- **AI is transforming both attack and defense strategies**
  While threat actors explore AI-driven exploits, defenders are also starting to leverage AI tools to block critical vulnerabilities.

56% of Scrubbing Centers in the Financial Sector are Highly Vulnerable

MazeBolt's research, informed by over 100,000 hours of attack simulations annually, found that 56% of financial organizations operate Scrubbing Centers that are highly vulnerable to DDoS attacks.

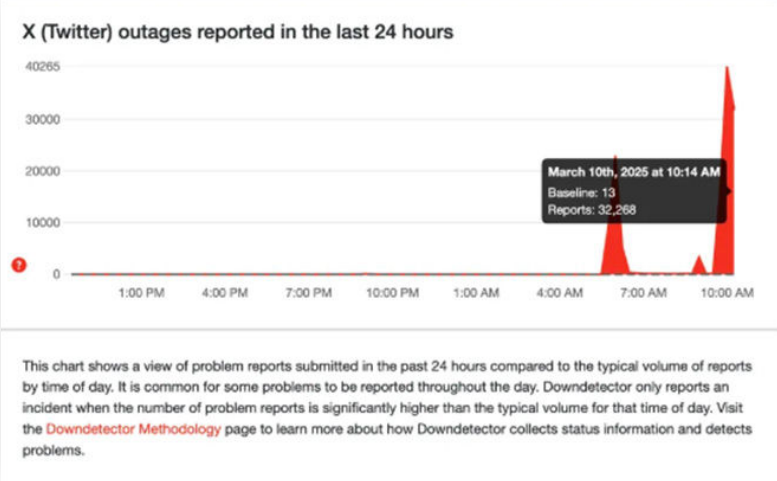
This high-risk situation is due to a complete lack of visibility into how DDoS protection solutions are configured. Most organizations remain unaware of critical DDoS misconfigurations and vulnerabilities until they experience a disruptive attack. Even with the best DDoS protection solutions, it's only after a damaging outage that hidden vulnerabilities come to light.



56% of BFSI Scrubbing Centers are Highly Vulnerable

X Goes Down - Due to DDoS Vulnerabilities and Misconfigurations

The social network X experienced intermittent outages due to a series of apparent DDoS attacks on March 10. Researchers stated they observed 5 distinct attacks of varying length against X's infrastructure.



Downdetector Reports of the March 10 Attack on X

Careful analysis revealed that some of X's origin servers which respond to web requests, such as help.x.com, were not properly secured behind the company's DDoS protection solution, Cloudflare. As a result of DDoS misconfigurations, these servers were publicly visible - allowing attackers to target them directly.

Some of X's origin servers were not secured properly behind X's Cloudflare DDoS protection – and these misconfigurations allowed attackers to target them directly.

X owner Elon Musk attributed the disruptions to a "massive cyberattack" from a "large, coordinated group and/or a country," later suggesting Ukrainian IP addresses as the source. However, security experts emphasized that IP attribution alone is inconclusive, as attackers often use compromised devices and proxy networks to mask their true origins. While responsibility for the attack was claimed by a pro-Palestinian hacktivist group called Dark Storm, its true origin remains uncertain.

Image credit: Elon Musk / X / Cointelegraph

Several weeks after this attack, X faced additional downtime on March 30. Over 57% of users affected were using the app on iOS and Android, while others experienced issues accessing the platform via desktop. However, this incident has not been acknowledged by X's technical team, leaving open the question of whether this was really a DDoS attack or just platform instability.

The attacks during March were not the first time that DDoS was used to take down the X platform. DDoS allegedly took down the platform in August 2009, June 2012, October 2016, and August 2024.

NoName(057) Implements Daily Attacks through "Crowdsourcing"

NoName(057) is a pro-Russian hacking group whose level of activity is one of the highest among DDoS attack groups. NoName(057) developed a DDoS sharing platform called the DDoSia Project; any attacker who goes into the platform can participate in a DDoS attack.

The DDoSia project allows users to volunteer to donate resources and compute to an attack. This allows NoName(057) to implement large-scale DDoS attacks without developing a botnet.

NoName(057) targets private corporations, ministries, and public institutions belonging to countries supporting Ukraine – predominantly, NATO member states. Targets primarily include organizations in government, infrastructure, and banking:

Government	Banking	Infrastructure	Other
54%	14.8%	12.2%	10%

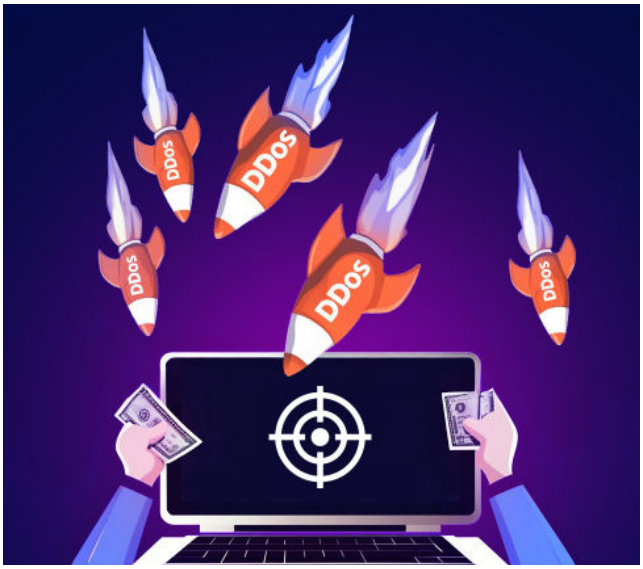
Targets of the DDoSia Project by Industry (Source: Sekoia.io)

NoName057 establishes collaboration agreements with other hacktivist collectives, focusing their combined efforts on targeted objectives. The group has established alliances with the groups SoubearArmy, 22C, CyberDragon, Horus Team, UserSec and PHOENIX, notably against Italian infrastructures. This form of cooperation may possibly reflect a desire to strengthen the presence and influence of NoName(057) in the public arena.

The DDoSia Project has close to 20,000 members on Telegram. The number of total users following NoName057 Telegram channels has passed 60,000.

DDoS as a Dangerous Smoke Screen

While DDoS attacks alone cause major damage, the combination of DDoS that masks the infiltration of ransomware has a disproportionately higher potential for damage. In other words, DDoS can be used as a distraction to keep cyber teams occupied while the attackers conduct a breach, leading to a ransomware attack.



Combination of DDoS that Masks the Infiltration of Ransomware

This cyber threat combination means cybercriminals combine DDoS attacks with ransomware or breach attempts to increase the likelihood of payment or data compromise. DDoS is used as a distraction or to disable defenses so that ransomware or intrusion tactics can succeed unnoticed. In other cases, the DDoS itself serves as an extortion method, demanding payment to stop the attack and signaling the threat of deeper breaches.

This dual-threat approach significantly escalates risk, as organizations must defend against service disruption and potential data loss simultaneously. It underscores the need for proactive DDoS vulnerability management and real-time visibility across attack surfaces.

AI Capabilities Impact Both Attackers and Defenders

87 percent of organizations report that they were hit by an AI-driven cyberattack this year. 91 percent of security experts anticipate a significant surge in AI-driven threats over the next three years.

Currently, criminals are not deploying AI agents to hack at scale. But researchers have demonstrated that AI agents could execute complex attacks, and experts warn that we may start seeing these types of attacks. AI agents theoretically could be used to:

- Identify vulnerable targets
- Hijack their systems
- Steal valuable data from unsuspecting victims

Beyond the threat of AI-based attacks, in-house adoption of AI is inadvertently expanding organizations' attack surfaces, creating risks related to new innovative attacks such as data poisoning and AI hallucinations.

In parallel to their use by cybercriminals, AI is also being leveraged by defenders to stop attacks. For example, MazeBolt's SmartCycle™ feature is an AI-powered DDoS simulation engine that intelligently prioritizes the attack vectors that are most likely to cause damage to a specific environment, during an attack.

Drill-Down: Top DDoS Attacks in Q1 2025

The tables below provide insight into DDoS attacks published in the media during the first quarter of 2025.

Jan 2025

Date	Location	Vertical	Targets	Attacker	Headline
Dec. 31-Jan. 1	France	Government	French municipal and departmental websites	Pro-Russian hackers	Link
Jan. 2	Japan	Telco	NTT Docomo	N/A	Link
Jan. 9–12	Italy	Government, Finance, Transportation	Multiple Italian institutions: government ministries, major banks (e.g. Intesa Sanpaolo, MPS), and transport hubs (ports of Taranto and Trieste)	NoName057	Link
Jan. 11	Crimea	Telco	Major fixed-line and mobile operators in Crimea	N/A	Link
Jan. 24	Russia	Telco	MegaFon	IT Army of Ukraine - a pro-Ukraine hacktivist group	Link
Jan. 26	Germany	Transportation	Websites of regional rail operators Enno, Erixx, and Metronom	N/A	Link
Jan. 27	China	Technology (AI Platform)	DeepSeek (DeepSeek-V3 chat platform)	N/A	Link
Jan. 31-Feb. 6	Czech Republic	Gaming (Online Games)	Bohemia Interactive – known for the DayZ and Arma Reforger series	Styled Squad Reborn	Link

February 2025

Date	Location	Vertical	Targets	Attacker	Headline
Feb. 10–13	Germany	Technology/ Open-Source Development	Codeberg e.V.	N/A	Link
Feb. 17	Italy	Transportation/ Government/ Finance	Airports of Linate and Malpensa, Transport Authority, Ports of Taranto and Trieste	NoName057	Link
Feb. 18	Italy	Government and Law Enforcement	Websites of the Ministry of Enterprises and Made in Italy, Guardia di Finanza, and other institutions	NoName057	Link
Feb. 26	Italy	Government	Websites of the regions of Abruzzo, Basilicata, Marche, Molise, and the Regional Council of Aosta Valley	NoName057	Link
Feb. 26	Russia	Telco	Beeline (PJSC VimpelCom)	Not publicly named – likely pro-Ukraine hacktivists	Link

March 2025

Date	Location	Vertical	Targets	Attacker	Headline
Mar. 03	Russia	Telco	Beeline	N/A	Link
Mar. 05	Spain	Government/ Transportation	Multiple government and transportation portals	NoName057	Link
Mar. 10	United States	Social Media	X	"Dark Storm - pro-Palestinian hacktivist group"	Link
Mar. 15	United States	Gaming	Blizzard Entertainment (World of Warcraft Classic)	N/A	Link
Mar. 21–24	Russia	Telco	Lovit	IT Army of Ukraine	Link
Mar. 26	Global	Various	N/A	N/A	Link
Mar. 31	Russia	Transportation	Moscow Metro	(Unknown hacktivists - sources link it to pro-Ukraine hackers)	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