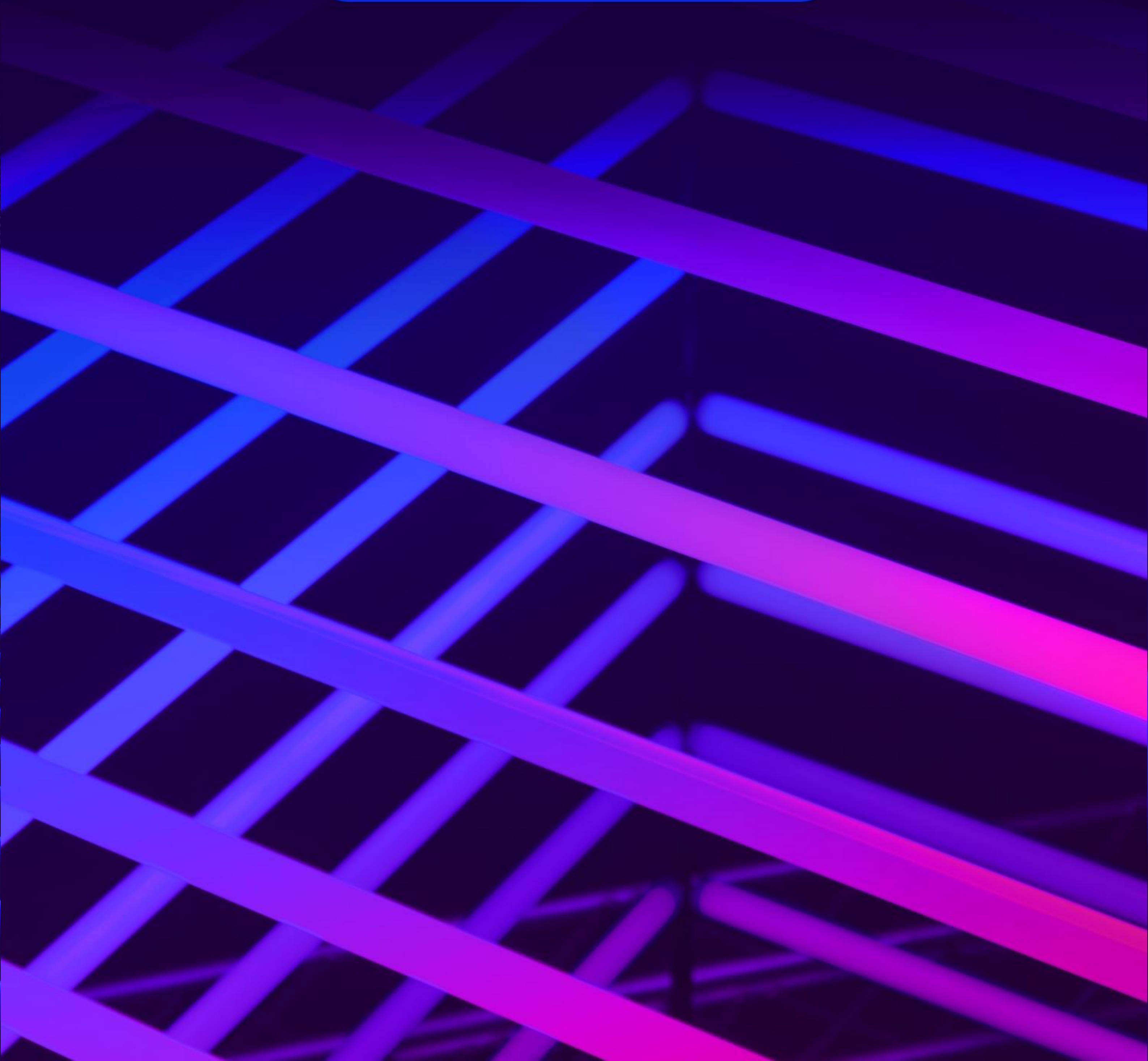
MAZEBOLT

# DDoS Attack Round-up

NOVEMBER 2023 REPORT



## European Infrastructure at Stake

In November 2023, it seems that hacktivist groups with pro-Russian affiliations decided to significantly cripple the mobility of European residents for malicious purposes. Numerous high-profile and sophisticated DDoS attacks targeted major European infrastructure and transportation companies, resulting in a state of helplessness and confusion among many citizens.

During the early days of November, Germany and the Netherlands became prime targets facing severe disruptions orchestrated by NoName057(16), a Russia-state-sponsored DDoS attacker known for causing chaos across Europe in recent months. On this occasion, NoName057(16) directed its efforts towards Deutsche Bahn's DB Navigator, the application for searching transport connections and purchasing tickets, among other critical elements of German infrastructure. The multi-vectored attack led to more than 10 hours of cumulative downtime, causing considerable frustration for residents reliant on essential services accessed through portals like Berlin’s official services website and transportation services provided by Deutsche Bahn.

Merely three days later, NoName057(16) launched an assault on the Dutch transportation company Translink, resulting in the shutdown of their website for public transport chip cards (OV chip cards) for over 9 hours.

This attack not only inflicted substantial financial losses but also severely disrupted the workday, leaving numerous Dutch citizens stranded. Once again, these incidents underscore the vulnerability of organizations, particularly those of a governmental or infrastructure nature, to damaging DDoS attacks and downtime. This emphasizes the critical importance of reinforcing DDoS resilience for maintaining the functionality of critical services.

## AI Couldn't Predict ***That***…

On November 8th, one of the most widely reported DDoS attacks in recent times occurred, resulting in the shutdown of ChatGPT for more than 16 hours. The attack was orchestrated by the Anonymous Sudan hacker group against OpenAI ChatGPT, a leading AI tool that has gained global prominence. OpenAI was compelled to acknowledge that the DDoS attack had a significant impact on both ChatGPT and its application programming interface (API). Remarkably, this marked the second successful DDoS attack that brought down one of Microsoft's services in the same year. The first notable incident took place in June when Anonymous Sudan executed a DDoS attack, causing the shutdown of Microsoft Azure and Microsoft 365.

When trying to use ChatGPT, users encountered error messages saying that ChatGPT was unable to generate responses and that “something seems to have gone wrong”.

Attempts to access ChatGPT, at the time of posting, still result in the AI chatbot not properly working. The attack lasted longer than originally reported, and as a result of the periodic outages, ChatGPT users received various error messages throughout the day of high demand and bad gateways - and some errors prevented logged-out users from logging in.

The incident unfolded over several days, sending shockwaves through the ChatBot industry. Faced with the prolonged unavailability of ChatGPT, numerous users turned to alternative AI chatbots such as Google Bard, only to encounter similar issues. Whether Bard and ClaudeAI experienced DDoS attacks or merely grappled with an overwhelming surge in traffic triggered by ChatGPT's problems remains unclear. What is clear is that all major chatbots, including the popular ones, suffered downtime in the aftermath of this particular extensive DDoS attack.

These attacks, along with the massive DDoS incidents involving gaming companies and the nationwide Healthcare system attack on Singapore, all indicate that organizations need to adopt a new approach to DDoS security. The only way to prevent a damaging DDoS attack and the downtime that follows it is to continuously test for DDoS vulnerabilities and uncover DDoS protection misconfigurations. DDoS protection can only block known attacks, but it is the unknown and unchecked DDoS attack vector that could (and will) shut down online services.

| Date of attack | Country | Vertical | Downtime | Companies Affected | Estimated Damage | Press | Threat Actor + Affiliation |
|---|---|---|---|---|---|---|---|
| November 1 | Singapore | Healthcare | 96 hours attack<br>10 hours intermittent downtime | The websites of Singapore's public healthcare institutions: The websites of Singapore General Hospital, National University Hospital, and Tan Tock Seng Hospital were among those affected, as was that of the Agency for Integrated Care (AIC). Also, Synapxe, who supports the operations of 46 public healthcare institutions. These include acute hospitals and polyclinics, as well as around 1,400 community partners such as nursing homes and general practitioners. | **NA** | Link | Unknown |
| November 1 | Germany | Transportation | 12 hours attack<br>6 hours intermittent downtime | Deutsche Bahn's DB Navigator (the app for searching for transport connections and buying tickets) | **NA** | Link | NoName057(16) - State Sponsored by Russia |
| November 3 | Germany | Government, Infrastructure, Transportation | 24 hours attack<br>4 hours intermittent downtime | The administration of the city of Bielefeld, the official web portal of the city of Berlin, the Federal Office of Foreign Affairs and a railway operator in Germany – Deutsche Bahn | **NA** | Link | NoName057(16) – State Sponsored by Russia |

| Date of attack | Country | Vertical | Downtime | Companies Affected | Estimated Damage | Press | Threat Actor + Affiliation |
|---|---|---|---|---|---|---|---|
| November 4 | Netherlands | Transportation | 24 hours attack<br>10 hours downtime | The website of public transport chip card (OV chip card) company Translink. | **300K USD** | Link | NoName057(16) - State Sponsored by Russia |
| November 7 | Qatar | Government | 12 hours attack<br>4 hours downtime | Various Governmental services, in response to the death sentence handed to eight former Indian Navy officers by a Qatari court in Espionage case. | **NA** | Link | Indian Cyber Force |
| November 8 | USA | Communications / Web Services | 48 hours attack<br>16 hours downtime | OpenAI's ChatGPT | **2Mil USD** | Link | Anonymous Sudan |
| November 8 | Greece | Real Estate | 12 hours attack<br>8 hours downtime | Hellenic Public Properties Co, HPPC, the company managing the real estate assets of the Greek state. | **NA** | Link | Unknown |

| Date of attack | Country | Vertical | Downtime | Companies Affected | Estimated Damage | Press | Threat Actor + Affiliation |
|---|---|---|---|---|---|---|---|
| November 9 | USA | DDoS Mitigation | 2 hours attack 0.5 hours downtime | Cloudflare | **NA** | Link | Anonymous Sudan |
| November 11 | Israel | Communications / Press | 6 hours attack 1 hour downtime | Walla, one of Israel's leading news and content portals (website and app were down) | **35K USD** | Link | CyberArmyPalestine |
| November 12 | USA | Gaming | 8 hours attack 3 hours downtime | Riot Games - EU League of Legends: players are having issues logging into the game: The issue is happening on Windows, macOS, Android, and iOS platforms. | **250K USD** | Link | Anonymous Sudan |
| November 18 | USA | Healthcare | 48 hours attack 24 hours downtime | PruittHealth – leading health care provider in Georgia, Florida, North Carolina, and South Carolina, including senior living, in-home health care, hospice, and skilled nursing. The attack is part of a complex cyber attack that includes ransomware and extortion | **NA** | Link | the NoEscape ransomware gang |

| Date of attack | Country | Vertical | Downtime | Companies Affected | Estimated Damage | Press | Threat Actor + Affiliation |
|---|---|---|---|---|---|---|---|
| November 18 | USA | Gaming and Animation | 96 hours attack<br>72 hours downtime | Blender, the company behind the popular eponymous 3D modeling design software | **NA** | Link | Unknown |
| November 20 | USA | Social Media | 12 hours attack<br>6 hours downtime | Video streaming site Rumble | **80K USD** | Link | Unknown |
| November 20 | USA, Germany | Gaming | 12 hours attack<br>8 hours downtime | Ravensburger AG, the German games and toys company, launching a new Disney game, "Lorcana : Rise of the Floodborn".<br>The launch was canceled. | **NA** | Link | Unknown |
| November 22 | Russia | Aviation | 12 hours attack<br>8 hours downtime | Russian government's civil aviation agency, also known as Rosaviatsia | **NA** | Link | Ukraine's security services, collaborating with pro-Ukrainian hacker groups |
| November 29 | USA | Financial | 8 hours attack<br>3 hours downtime | Auction-as-a-service provider Bounce Finance. The attack happened during the public sale of BitStable's BSSB token. | **NA** | Link | Unknown |

Would you like to discover how to identify and mitigate vulnerabilities in your DDoS protection? **Contact us today!**

MAZEBOLT

MazeBolt is pioneering a new standard in DDoS security. RADAR™ enables organizations to leave behind unexpected manual mitigation and SLAs, and move forward to transformative, reliable, and automated DDoS protection that does not require damaging downtime and response scenarios.

RADAR is an industry-first patented solution that identifies how attackers succeed in bypassing existing protection systems through vulnerabilities, through continuous non-disruptive DDoS attack simulations. RADAR's autonomous risk detection allows cybersecurity teams to go beyond traditional DDoS testing and identify and remediate vulnerabilities in every layer of DDoS protection.

Global enterprises, including financial services, insurance, gaming, and high-security government environments rely on MazeBolt to avoid damaging DDoS attacks.

LEARN MORE