MAZEBOLT

DDoS Threat Report

Q4 2023

Winter is coming

A review of Q4 2023 DDoS attacks

DDoS attacks currently stand out as a prominent cyber threat due to their relative simplicity in execution. Numerous articles have highlighted a significant surge in DDoS attacks during Q4, projecting a record-breaking total of over 15 million incidents for 2023. The accessibility of DDoS-as-a-service, priced as low as $500, facilitates the execution of malicious and intricately varied attacks, posing a threat to online services across multiple industries.

The economic impact of DDoS attacks is evident, with 5% of affected organizations incurring losses exceeding $1 million, encompassing direct financial losses, downtime expenses, and reputational damage. The vulnerability gap in DDoS protection and security postures remains substantial, contributing to the escalating frequency of automated sequences and sophisticated multi-vectored attacks.

The primary factor enabling the frequency of DDoS attacks remains the vulnerabilities that remain in the deployed, yet undetected, DDoS protection layers, resulting from misconfigurations. Regardless of the simplicity of the attack, damaging downtime persistently affects victims, underscoring the impact of misconfigurations in DDoS defense mechanisms.

Following a challenging summer, Q4 also turned out to be highly dramatic in the DDoS landscape. Several high-profile DDoS attacks severely damaged operations across many sectors, including:

- Law enforcement in India
- Transportation in Germany, the Netherlands, New Zealand, and Finland
- Aviation in France and Russia
- The British Royal Family website
- Governmental services in Australia, Spain, Belgium, and the Czech Republic

The gaming industry has not been immune to the impact of DDoS attacks in Q4, experiencing notable downtime from damaging incidents. High-profile attacks have underscored the gaming sector's status as a preferred target for DDoS attacks, driven by motives ranging from ransom demands to pure disruption and chaos. However, Q4 shows that politically motivated DDoS attacks continue to be at the forefront, particularly in the context of two major global events such as the ongoing conflicts in Russia/Ukraine and Israel/Gaza.

Following the October 7 attacks, Israel faced an onslaught of DDoS attacks orchestrated by more than 10 distinct threat actors. Evidently forming a coalition, groups such as Cyber Av3ngers, Killnet, YourAnon T13x, Mysterious Team Bangladesh, Anonymous Sudan, Insane Pakistan, Garnesia Team, Moroccan Black Cyber Army, and others engaged in coordinated DDoS attack efforts. In response, pro-Israel hacktivists initiated similar counter-actions, targeting Palestinian-related outlets. As the Israel-Gaza conflict persists, DDoS attacks continue although many remain unreported or unconfirmed.

The Russia/Ukraine conflict witnessed substantial DDoS attacks targeting critical business and governmental sectors. This included a nationwide attack on Canada, assaults on Russia's civil aviation agency (Rosaviatsia), and major Russian airline carriers like Aeroflot, Pobeda, Azur Air, and Rossiya. Ukraine experienced a significant blow with a DDoS attack on Kyivstar, its largest mobile telecom operator, resulting in residents being without cell reception for over three days. Even Lithuania faced a DDoS attack, possibly in response to its involvement in Ukrainian tank repairs, targeting defense, roads, logistics, mobile operators, telecommunications, internet providers, and authorization services.

This report emphasizes that organizations impacted by state-sponsored DDoS attacks are unable to seek compensation for damages. Lloyd's, the global London-based insurance company, has explicitly excluded liability for losses arising from any state-sponsored cyberattack. The following data in this report highlights that state-sponsored DDoS attacks result in unrecoverable damages, including financial losses, reputational damage, and potentially life-threatening situations, as evidenced by highly publicized attacks on systems such as ChatGPT and various healthcare systems worldwide.

Date of attack	Country	Vertical	Downtime	Companies Affected	Estimated Damage	Press	Threat Actor + Affiliation
October 1	UK	Government	3 hours attack, 1 hour downtime	The Royal Family's official website	**NA**	Link	KillNet, Russian Hacktivist group
October 5	Australia	Government	8 Hours attack, 5 hours downtime	the Department of Home Affairs and Administrative Appeals Tribunal websites in response to a decision to provide the Slinger "drone killer system" to Kyiv.	**NA**	Link	NoName057(16) - State Sponsored by Russia
October 6	Spain	Government	3 hours attack, 1 hour downtime	several public and private websites, including in the city of Granada where an EU summit is taking place, The Granada Bus service	**NA**	Link	NoName057(16) - State Sponsored by Russia
October 6	US	Social Media/ Financial	12 Hours attack, 6 hours downtime	Stars Arena, a social platform backed by Avalanche's Contract Chain - The DDoS attack was a cover for a financial hack	**$4Mil USD**	Link	Unknown

Date of attack	Country	Vertical	Downtime	Companies Affected	Estimated Damage	Press	Threat Actor + Affiliation
October 7	Israel	Government, Infrastructure - "OpIsrael2"	Unconfirmed	Unconfirmed	**NA**	Link	Mysterious Team Bangladesh, Anonymous Sudan, Insane Pakistan, Garnesia Team, Moroccan Black Cyber Army and others
October 8	Israel	Press - "OpIsrael2"	48 Hours attack, 16 hours intermittent downtime	The Jerusalem Post	**$50K USD**	Link	Mysterious Team Bangladesh, Anonymous Sudan, Insane Pakistan, Garnesia Team, Moroccan Black Cyber Army and others
October 8	Israel	Government	1 Hour attack, 1 hour downtime	Shin Bet, the Israeli Homeland Security	**NA**	Link	KillNet, Russian Hacktivist group
October 8	South Korea	Gaming	48 Hour attack, 24 hours intermittent downtime	Ironmace – "Dark and Darker"	**NA**	Link	Unknown

Date of attack	Country	Vertical	Downtime	Companies Affected	Estimated Damage	Press	Threat Actor + Affiliation
October 8	The Palestinian Authority	Government	24 hour attack, 12 hours downtime	The Palestinian government websites, the websites of Hamas and the Islamic University of Gaza.	**NA**	Link	The Indian Cyber Force, and also TeamHDP
October 9	The Palestinian Authority	Government	24 hours attack, 12 hours downtime	Palestinian telecommunications company, the National Bank's website, a government webmail service, and the official Hamas website.	**NA**	Link	The Indian Cyber Force
October 12	Israel	NPO	12 hours attack, 6 hours downtime	United Hatzalah - Jerusalem-based nonprofit which provides emergency medical services	**NA**	Link	Mysterious Team Bangladesh, Anonymous Sudan, Insane Pakistan, Garnesia Team, Moroccan Black Cyber Army and others
October 12	The Palestinian Authority	NPO	12 hours attack, 6 hours downtime	Medical Aid for Palestinians (MAP), a British charity helping with emergency relief	**NA**	Link	Unknown
October 12	Belgium	Government	24 hours attack, 6 intermittent hours downtime	Websites of the Royal Palace, the Prime Minister and the Parliament of Brussels: presumably in response to Volodymyr Zelenskyy's visit to Belgium and its decision to deliver F-16 fighter jets to Ukraine.	**NA**	Link	Unknown but pro-Russian

Date of attack	Country	Vertical	Downtime	Companies Affected	Estimated Damage	Press	Threat Actor + Affiliation
October 13	Iran	Government	24 hours attack, 12 hours downtime	Mojahedin.org website	**NA**	Link	Ministry of Intelligence and the IRGC, under the command of Khamenei
October 14	Guatemala	Government	24 hours attack, 12 hours intermittent downtime	Webpages for Guatemala's judicial branch, Department of Agriculture and the General Secretary of the president, and more – in support of Indigenous organizations in the country	**NA**	Link	Anonymous
October 14	USA	Healthcare	12 hours attack, Unkn own hours downtime	Major U.S. healthcare solutions provider Henry Schein	**$3.3Mil USD**	Link	Unknown
October 22	USA	Entertainment	4 hours attack, 2 hours downtime	Deezer	**$150K USD**	Link	Unknown
October 22	Australia	Sports	2 hours attack, 1 hour downtime	West Australian Optus Stadium	**NA**	Link	Team Insane Pakistan

Date of attack	Country	Vertical	Downtime	Companies Affected	Estimated Damage	Press	Threat Actor + Affiliation
October 24	Czech Republic	Government	4 hours attack, 2 hours downtime	The websites of the Czech Ministry of the Interior and police force, website of the Crimea Platform international summit	**NA**	Link	Unknown – but presumed from Russia
October 27	Russia	Telecoms	8 hours attack, 4 hours downtime	Three Russian internet providers — Miranda-media, Krimtelekom, and MirTelekom	**NA**	Link	Ukrainian IT Army
October 31	USA	Press	3 hours attack, 3 hours downtime	AP - Associated Press, one of the world's best-known news organizations	**NA**	Link	Anonymous Sudan

Date of attack	Country	Vertical	Downtime	Companies Affected	Estimated Damage	Press	Threat Actor + Affiliation
November 1	Singapore	Healthcare	96 hours attack, 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, 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, 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, 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, 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, 16 hours downtime	OpenAI's ChatGPT	**$2Mil USD**	Link	Anonymous Sudan
November 8	Greece	Real Estate	12 hours Attack, 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, 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, 6 hours downtime	Video streaming site Rumble	**80K USD**	Link	Unknown
November 20	USA, Germany	Gaming	12 hours attack, 8 hours downtime	Ravensburger AG, the German games and toys company, launching a new Disney game, "Lorcana : Rise of the Floodborn". The launch was canceled.	**NA**	Link	Unknown
November 22	Russia	Aviation	12 hours attack, 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, 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

Date of attack	Country	Vertical	Downtime	Companies Affected	Estimated Damage	Press	Threat Actor + Affiliation
December 11	UK	Media	72 hours attack, 48 hours intermittent downtime	Newsquest, is the second-largest publisher of regional and local newspapers in the UK. Newsquest is owned by US media giant Gannett and has over 250 local news brands and magazines under its umbrella.	**1.5Mil USD**	Link	Unknown
December 12	Ukraine	Communications / Web Services	96 hours attack, 72 hours downtime	Kyivstar, Ukraine's biggest mobile telecom operator	**8Mil USD**	Link	Killnet, State-sponsored by Russia
December 14	USA	Communications / Web Services	3 hours attack, 1 hour downtime	OpenAI's ChatGPT	**NA**	Link	Anonymous Sudan
December 14	USA	Financial	3 hours attack, 2 hours downtime	The Arbitrum (ARB) Blockchain network	**NA**	Link	Unknown

Date of attack	Country	Vertical	Downtime	Companies Affected	Estimated Damage	Press	Threat Actor + Affiliation
December 16	USA	Communications / Web Services / Retail	24 hours attack, 12 hours downtime	Cox Internet	**NA**	Link	Unknown
December 17	Pakistan	Communications / Web Services	36 hours attack, 12 hours downtime	Pakistan Internet services	**NA**	Link	Unknown
December 18	Iran	Infrastructure	24 hours attack, 12 hours downtime	70% of Iran's petrol stations have seen their services disrupted, in response to the aggression of the Islamic Republic and its proxies in the Middle East	**NA**	Link	Gonjeshke Darande. AKA Predatory Sparrow
December 19	USA	Press	24 hours attack, 10 hours downtime	LancasterOnline, the flagship news website published by LNP Media Group, a subsidiary of WITF Inc. and publisher of the daily newspaper LNP.	**40K USD**	Link	Unknown
December 20	Russia	Communications / Web Services	48 hours attack, 24 hours downtime	Bitrix24, a Russian provider of customer relationship management (CRM) services.	**600K USD**	Link	IT Army of Ukraine

Date of attack	Country	Vertical	Downtime	Companies Affected	Estimated Damage	Press	Threat Actor + Affiliation
December 22	Serbia	Press	72 hours attack, 48 hours downtime	The Balkan Investigative Reporting Network's website **Balkan Insight**. The attacks happened after BIRN on December 19 published a news item, "BIRN Texts on Turkish Fraudster Falsely Reported over Copyright," which concerned two false copyright infringement complaints it received concerning two of its earlier articles.	**70K USD**	Link	Unknown
December 26	Japan	Gaming	24 hours attack, 8 hours downtime	Square Enixm developer and owner of Final Fantasy: the European Light and Chaos Data Centers	**750K USD**	Link	Unknown
December 27	USA	Financial	48 hours attack, 36 hours downtime	Bitcoin Ordinals	**NA**	Link	Unknown
December 27	USA	Transportation	24 hours attack, 10 hours downtime	The Washington State Department of Transportation (WSDOT) website	**NA**	Link	Unknown

Date of attack	Country	Vertical	Downtime	Companies Affected	Estimated Damage	Press	Threat Actor + Affiliation
December 27	Lithuania	Various	36 hours attack, 6 hours intermittent downtime	The targeted sectors included defense, roads, logistics, mobile operators, telecommunications, internet providers, and authorization services. The attacks on Lithuanian Websites Links to Ukrainian Tank Repairs	**NA**	Link	NoName057, State-sponsored by Russia
December 28	UK	Social Media	8 hours attack, 4 hours downtime	Pinterest	**NA**	Link	Anonymous Sudan
December 29	USA	Gaming	6 hours attack, 3 hours downtime	Fortnite	**400K USD**	Link	Unknown

Summary:

How can you avoid a damaging DDoS attack?

Every organization with critical online services is at a high risk of damaging DDoS downtime. As networks become more sophisticated, so do DDoS attackers, becoming more aggressive, succeeding in shutting down online services for organizations - from banks to critical infrastructure. In every case of a successful DDoS attack, the reason for the damage has always remained the same: vulnerabilities in deployed DDoS protection implementations.

Since traditional DDoS testing is reactive and any fixes require extensive maintenance windows, many organizations run them once or twice a year. Thus, organizations are left in the dark regarding the visibility of their security postures, vulnerabilities, and the effectiveness of their deployed DDoS protection. Organizations assume they are well protected against DDoS attacks, when in fact, they are not - suffering up to 75% exposure to DDoS threats, with misconfigurations that lead to vulnerabilities in layers 3,4, and 7.

DDoS protection will only automatically block attacks specifically configured per production environments deployed; all other attacks will result in damaging SLA's time-to-mitigation and emergency response time. Only through identifying vulnerabilities and prioritized remediation can organizations avoid damaging DDoS attacks, and ensure that all protection systems are up-to-date on all DDoS vulnerabilities, with full visibility into their automated DDoS protection.

Want a deeper dive into your DDoS protection or get help with your DDoS challenges? Contact us and a MazeBolt expert will be in touch with you.