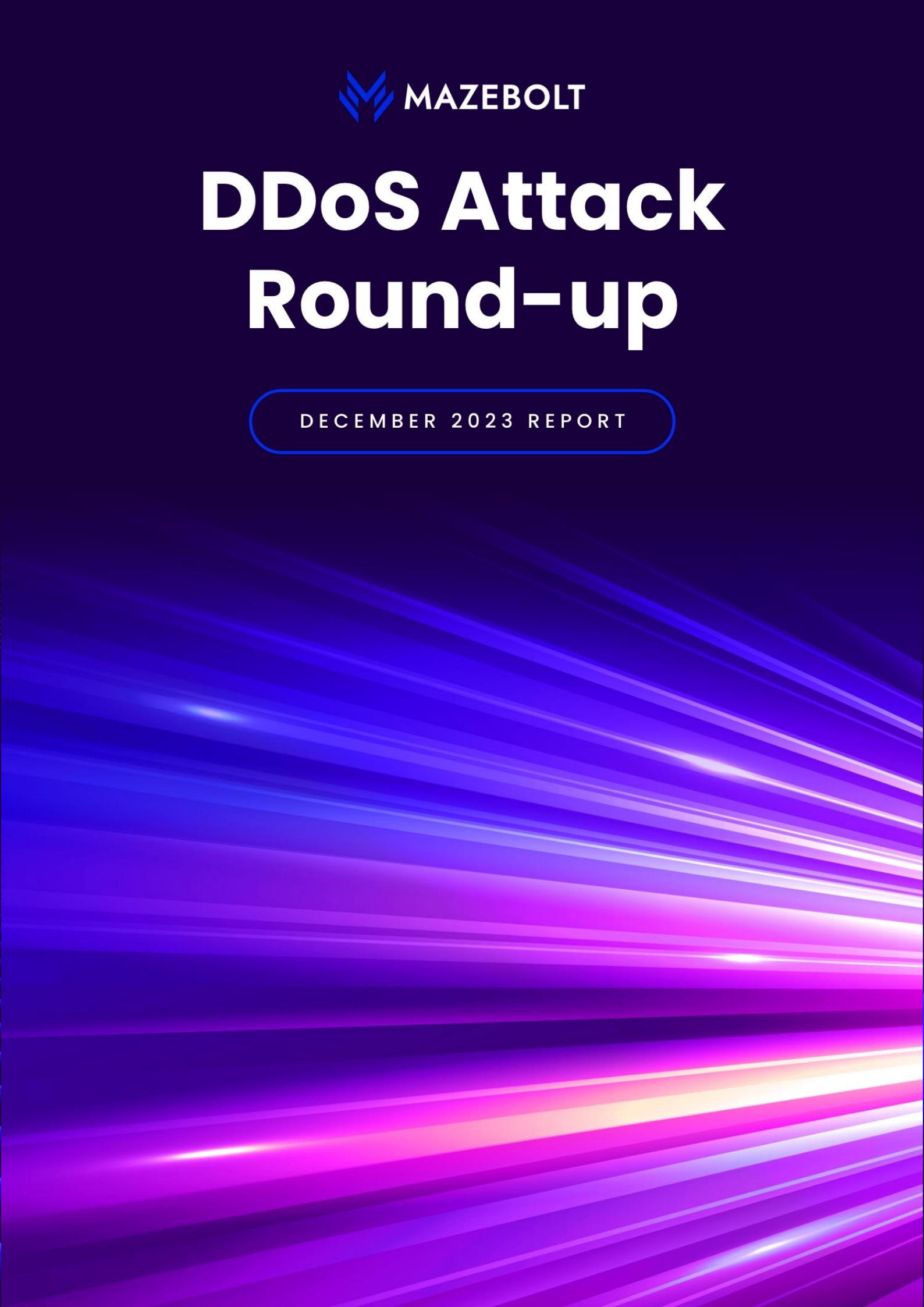
MAZEBOLT

DDoS Attack Round-up

DECEMBER 2023 REPORT



DDoS is Still a Tool for Digital Warfare

Since the beginning of the Russia/Ukraine conflict, many articles analyzed and explained how DDoS attacks are used as a weapon in the digital battleground between the two countries, as using hacktivism as a narrative for recruitment into state hacking groups is a known practice already being implemented by Iran, China, and Russia. The dramatic surge in DDoS attacks in recent years is attributed, among other reasons, to this highly publicized international conflict - but it seems that in recent months, both governments have perhaps found a way to prevent such attacks from being used as a highly effective weapon.

Well, whoever thought that, was wrong. December of 2023 saw two major DDoS attacks that were part of the ongoing conflict in the region. The first, launched by Killnet (the infamous Russia-sponsored DDoS threat actor) on December 12th, shut down Kyivstar, Ukraine's biggest mobile telecom operator for over 72 hours, leaving many Ukrainian residents without online connectivity. The attack on Kyivstar is considered to be one of the most destructive attacks on Ukrainian networks since the start of the conflict, with government resources and emergency services being affected.

It took about a week for the “IT Army of Ukraine” (a government-sponsored DDoS attacker group) to respond, and on December 20th, they retaliated with an attack on Bitrix24, a Russian provider of customer relationship management (CRM) services. Shutting down their services for over 24 hours, the IT army of Ukraine stated that they chose this specific target since “war sponsors like Rosneft (a Bitrix24 user) are facing huge operational issues with their clients, just like over 40% of CRM system users in the aggressor country”. Bitrix24 is one of the most popular CRM systems for Russian businesses, providing services similar to Western brands such as HubSpot and Zoho. With over 24 hours of downtime, the estimated, conservative, calculation of the damage was around $0.5 million USD.

However, the Russia/Ukraine conflict was not the only political battleground in December 2023. As the conflict between Israel and Gaza continues, several cyber incidents were reported. The destructive DDoS attack on Iranian Infrastructure took place on December 18th: 70% of Iran’s petrol stations had their services disrupted, in response to the aggression of the Islamic Republic and its proxies in the Middle East. The DDoS attacker behind this massive attack was Gonjeshke Darande, AKA Predatory Sparrow, a pro-Israel hacktivist group. Iran’s Ministry of Petroleum also told an Iranian television station that the disruption at gas stations would not impact the price of fuel, but the attack left many of the country’s residents stranded for over 12 hours.

These politically-motivated DDoS attacks raise the question again: how can governments provide continuous online services and protection without having full visibility into their security postures? Organizations and governments must prioritize their DDoS security and perform continuous testing of their DDoS protection layers regularly to quickly identify vulnerabilities and avoid damaging DDoS attacks.

This time it was online connectivity and fuel supply that were jeopardized - but the next time, it could be a matter of life and death.

Date of attack	Country	Vertical	Downtime	Companies Affected	Estimated Damage	Press	Threat Actor + Affiliation
December 11	UK	Media	72 hours attack 8 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

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

MazeBolt is pioneering a new approach in DDoS security. MazeBolt RADAR™ is the only solution that identifies and enables the elimination of DDoS vulnerabilities in every layer of DDoS protection, by continuously testing every attack vector across online services, with zero operational downtime. Using RADAR's patented vulnerability testing 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.

Visit www.mazebolt.com to learn more.