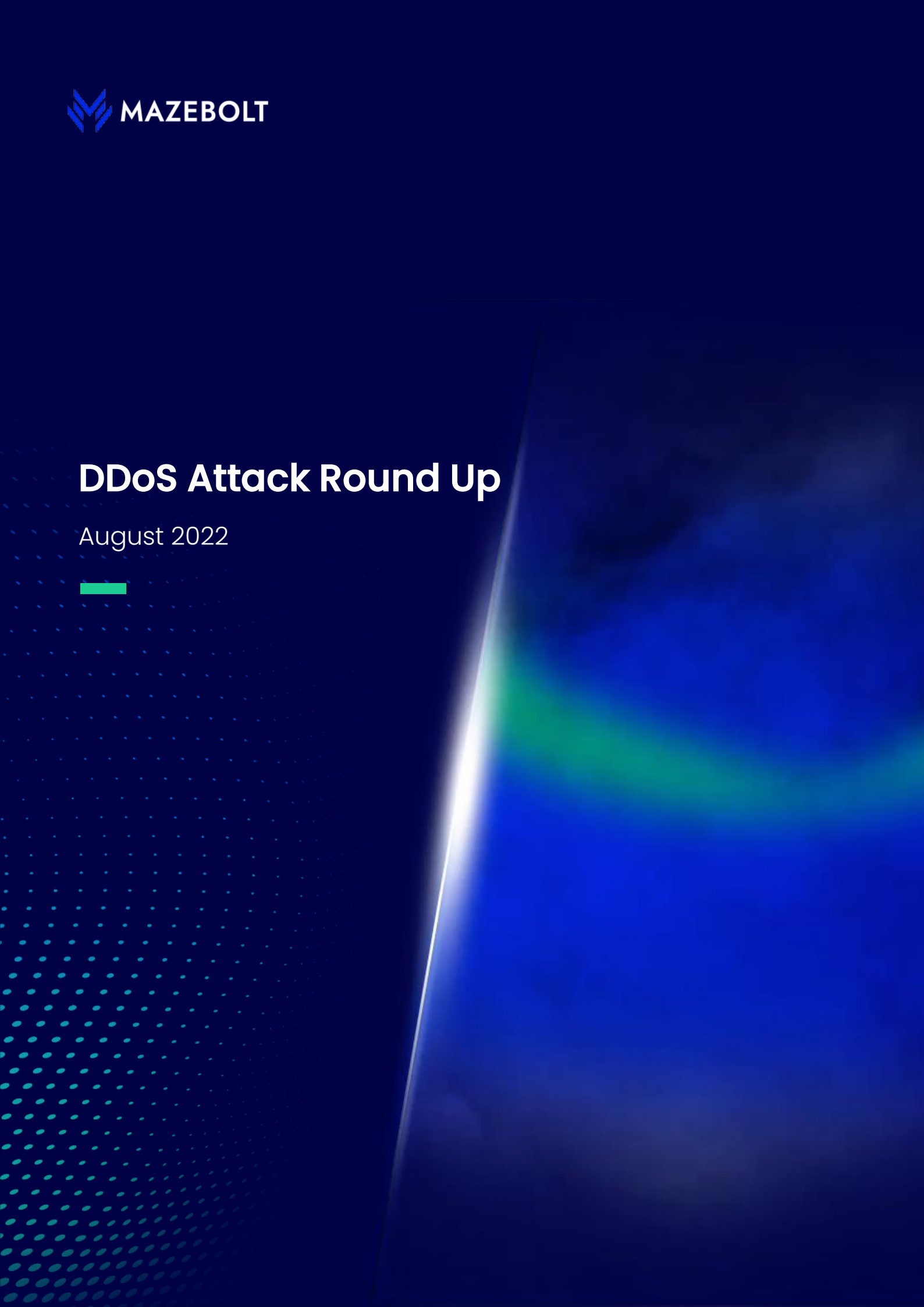
MAZEBOLT

DDoS Attack Round Up

August 2022



The Major DDoS Attack Trends of August

This month we saw the general trend of politically motivated malicious threat actors continuing to target governmental organizations. Many were suspected of having links to pro-Russian groups. This monthly trend follows the annual trend of a spike in patriotic DDoS attacks related to the Russo-Ukrainian conflict as well as an overall increase in DDoS attacks. The number of DDoS attacks in H1 increased by 203% compared to the same period the year before. In the first half of the year, DDoS attacks increased by 60% compared to the entire year in 2021.

Attacks on Countries escalate worldwide as they join NATO

Nordic region

The second most disruptive attack this month was targeted against the Finnish parliament website, resulting in three hours of downtime. While it's difficult – if not impossible – to find concrete evidence of who was responsible for the attacks, it is suspected that they were a result of the country's interest in joining NATO. In Telegram, pro-Russian hacker group NoName057(16) took responsibility for the attack, citing this exact reason as their motivation. In addition, the attack occurred the same day President Biden passed legislation approving Finland's application to join NATO.

This attack follows the general trend of DDoS attacks against the Nordic region as each prepares to join the NATO appliance. In June, the website of the Norwegian Labour Inspection Authority suffered downtime; in July Sweden suffered cyberattacks on its private sector. The ransomware attack affected a Swedish supermarket chain, shutting down half of its 800 stores and another 200 Swedish businesses using the same supplier.

This month a major DDoS attack hit the Swedish public sector, including the Stockholm public transport website. It was one of the biggest attacks in years.

Montenegro

Montenegro's online government, water and transportation services suffered the longest recorded DDoS attack this month – a total of three days. The combination of DDoS and ransomware attacks not only disrupted government services but also forced the country's electrical to switch to manual control. As a member of NATO and a Western ally against Russia, the DDoS attacks are suspected to be originated from pro-Russian cybercriminals.

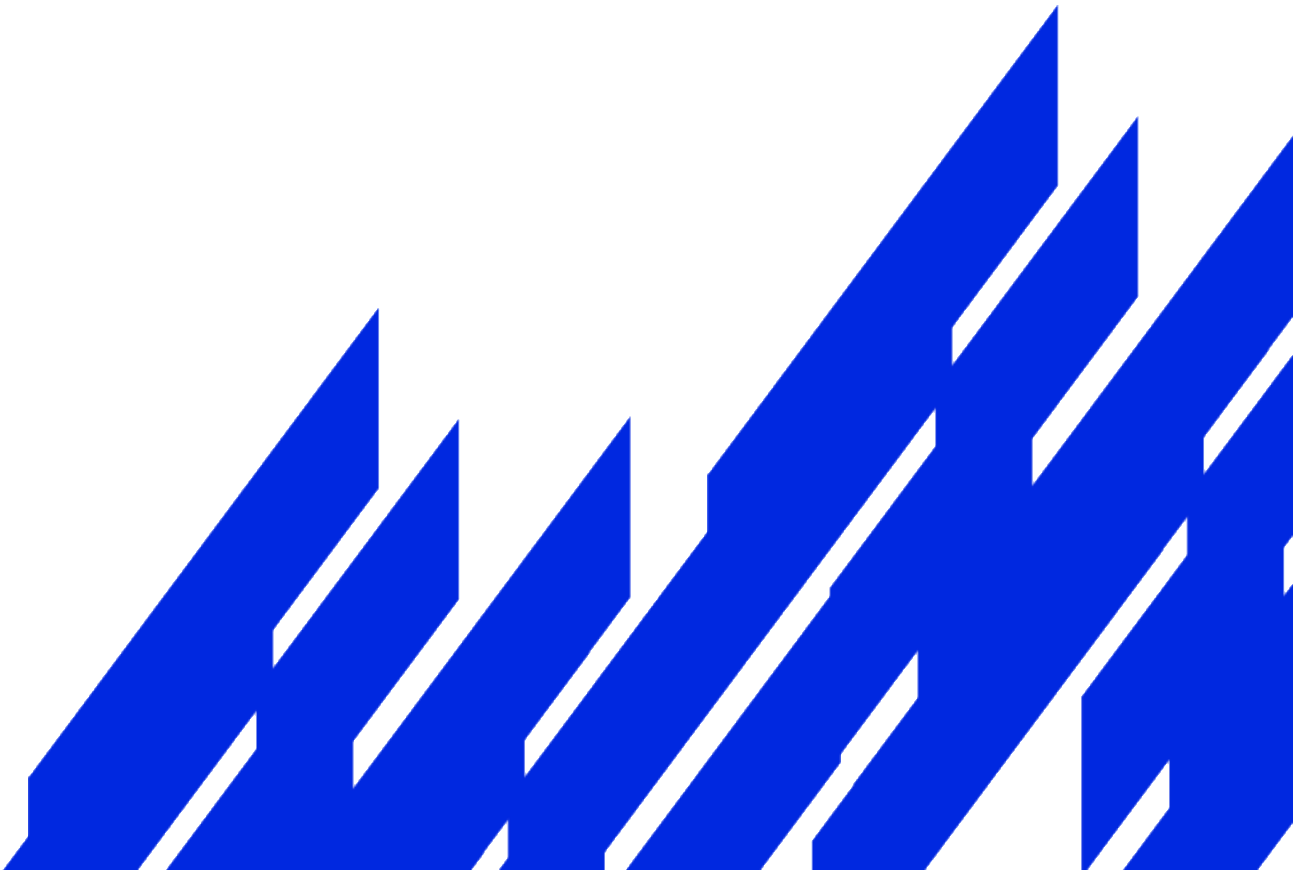
Estonia

Although services weren't disrupted, Estonia also suffered a series of 12 DDoS attacks against various state institutions and services. The attack was deemed the largest attack on the country since 2007.

More Hits to the Gaming and Media Industry

The gaming and media industries didn't escape from DDoS attacks this month either. Final Fantasy 14 Players were thrown offline for the second time in two months as they were disconnected from Square Enix gaming company's data centers in North America. The attack coincided with the company's announcement to expand its data centers to North America and its delay due to the global chip shortage.

Kiwi Farms, an online forum that promotes the harassment and doxing of individuals online, suffered DDoS attacks lasting several days that ultimately led to both their ISP and Cloudflare to halt service entirely to the forum.



Date of attack	Country	Vertical	Duration of Attack	Downtime	Companies affected	Comments	Press headlines
2-Aug	Taiwan	Government			President Tsai Ing-wen, the National Defense Ministry, the Foreign Affairs Ministry and the country's largest airport, Taiwan Taoyuan International	intermittent outages on Tuesday (August 2)	https://www.nbcnews.com/tech/security/taiwanese-websites-hit-ddos-attacks-pelosi-begins-visit-rcna41144
3-Aug	USA	Gaming			Final Fantasy Square Enix.	Second attack in 2 months. It was a lower volume than the attack in June.	https://www.playstationlifestyle.net/2022/08/03/final-fantasy-14-ddos-attacks-august-2022/
9-Aug	Finland	Government	3 Hours		Finnish parliament's website	Pro-Russian hackers took down the website of Finland's parliament, citing Helsinki's NATO application as the reason behind the DDoS attack	https://cybernews.com/cyber-war/russian-hackers-target-finland-parliaments-website/
10-Aug	Latvia	News	4 Hours		LETA - Latvian news agency	The information technology security incident prevention body "Cert.lv" explained that a group of activists supporting Russian ideology was responsible for the attacks, most likely funded by Russia.	https://eng.lsm.lv/article/features/media-literacy/newswire-leta-experienced-big-cyber-attack-over-weekend.a468891/
16-Aug	Ukraine	Energy/Critical Infrastructure	3 Hours		Energoatom - Ukrainian Nuclear Agency	The Russian group 'People's Cyber Army' carried out a cyber attack using 7.25 million bot users	https://nationalinterest.org/blog/techland-when-great-power-competition-meets-digital-world/ukrainian-nuclear-agency-hit-
17-Aug	Estonia	Government/Private			Online Service Portal E-Estonia	12 DDoS attacks made against various state institutions or their websites. There were also four DDoS attacks directed at private sector organizations. Services were not disrupted due to help from the Estonian Information System Authority (RIA) and others who helped fight the attacks	https://news.err.ee/1608688201/estonia-subjected-to-extensive-cyberattacks-after-moving-soviet-monuments
26-Aug	Montenegro	Government	3 Days	Unknown	Government systems, utilities & services	Montenegro's Agency for National Security blamed the attack on Russia, A combination of ransomware and distributed denial-of-service attacks, the onslaught disrupted government services and prompted the country's electrical utility to switch to manual control.	https://apnews.com/article/russia-ukraine-technology-hacking-montenegro-2a8eb2df87f657b6d7b9971b7419bff9?utm_source=hs_email&utm_medium=email&_hsenc=p2ANqtz-80sMPWmcfaAuK1hpm-O8RWEb_D8NdXVYXJLsftmG9E0Vxw8wJNosl88NiFGi9B0qPeY413
26-Aug	USA	Media	3 Days	3 Days	Discussion Forums	Since August 26th, 2022, Kiwi Farms has been offline and displaying a note uploaded by its administrators which explains why the website is down and how they have been suffering DDoS and other forms of cyber attacks.	https://www.hackread.com/kiwi-farms-offline-ddos-attack-hosting-issues/