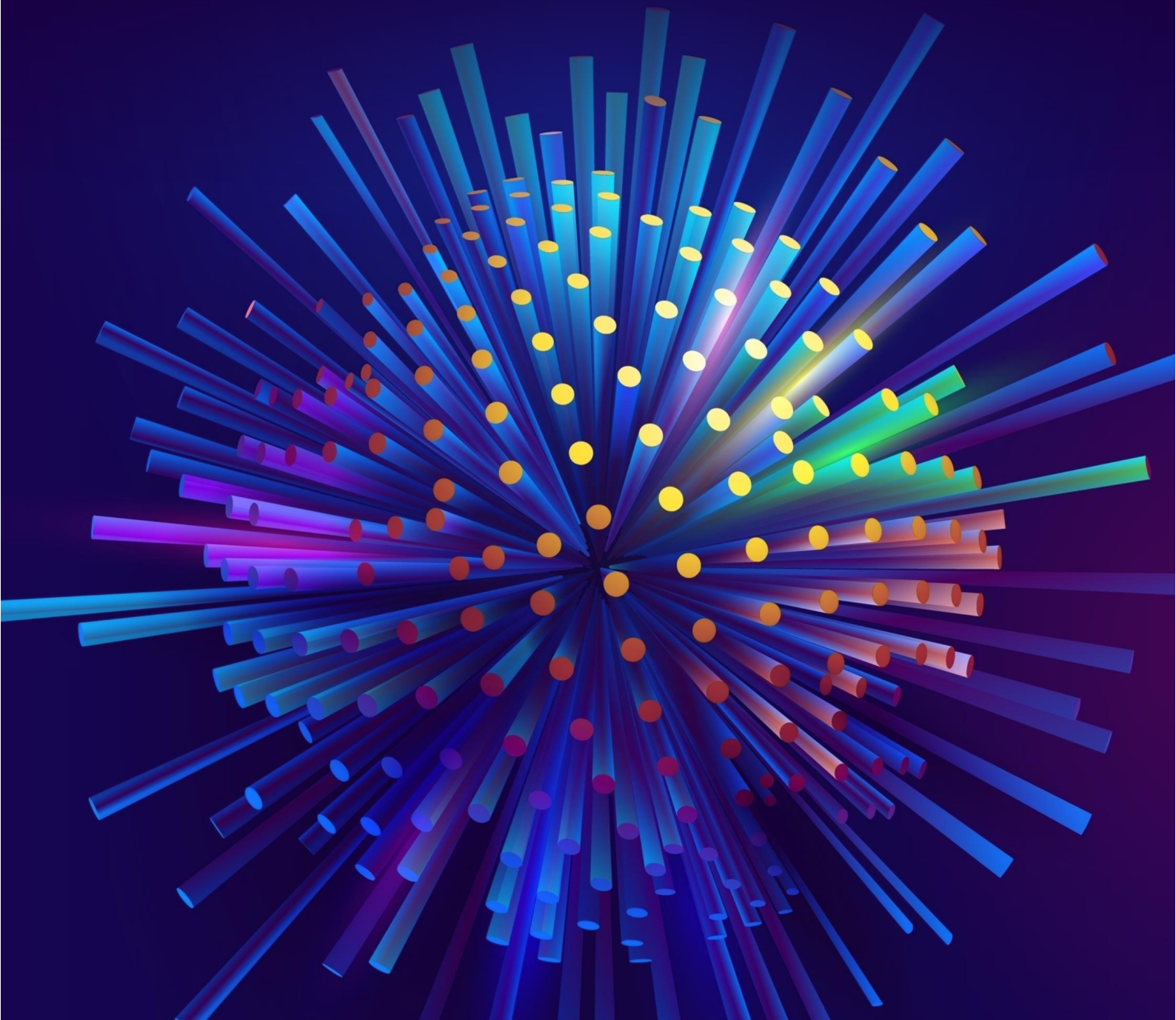
MAZEBOLT

DDoS Attack Round-up

MARCH 2023 REPORT



DDoS Travels Down Under

March of 2023 saw several major DDoS attacks that continued ongoing trends on the one hand, but marked new territories that raise a red flag, on the other. Germany suffered two severe DDoS attacks, one on the Mastodon Social Media platform and the other on Rheinmetall, a leading weapons manufacturer. The latter attack caused a three-hour shutdown of operations, and it's attributed to the Russian hacker group NoName, which is notorious for targeting government institutions and companies with a pro-Ukrainian stance. This attack follows the ongoing trend of malicious, politically motivated DDoS attacks that originate in the Russian-Ukrainian conflict.

Governments Continue to be Targeted

DDoS perpetrators continued to target governmental institutions and sites for ideological reasons. In March, Estonia and France were the selected targets, with 2 major attacks. The Estonian governmental site suffered several hours of downtime during the elections, causing problems with ballot counting. This was the first time Estonia used an internet voting system, and it seems the attack was launched with the sole purpose of disrupting the process. In France, the National Assembly website was down for several hours because the attackers wanted to make a stand against President Macron's highly unpopular pension reform. These attacks are yet another reminder that politically and ideologically based DDoS attacks are one of the major threats today.

DDoS Hits the Outback

If there is one major trend to be noticed during March, it's that there's a clear rise in DDoS targeting businesses and organizations across Australia. Four major attacks hit the land down under, targeting all types of organizations: banking, social channels and events, education, health care, airports, and even weapon manufacturing. These attacks were severe and complex, multi-vectored, and lasted long periods. several hacker groups claimed responsibility for the attacks, including the Killnet and AnonymousSudan attacking education organizations, Team Insane PK, Eagle Cyber, and Mysterious Team launching 70 DDoS attacks against banks and governmental sites because of Australia's fashion week, and more. The attack on the Indonesian branch of the Australian bank PT Commonwealth, that took place on March 8th, cost an estimated damage of 1 million USD in downtime alone.

These attacks tend to be more politically and ideologically motivated, with motives ranging from Australia's support of Ukraine and organizations suspected of taking anti-Islamic positions. Given the fact that many attacks were in response to a fashion show, but included many targets such as government services, schools, banks, and other smaller businesses, one might assume that the fashion week was just an excuse. It seems like Australia, as a whole, could be a new battle ground for the DDoS war. DDoS attacks against Australia have inclined in recent years, with some reports claiming that every few minutes, a new DDoS attack is launched against an Australian target. And even with this information in hand, to witness so many successful attacks in one month is a dramatic shift in the status quo.

Organizations, both in Australia and worldwide, must take proactive measures to gain critical insight into their DDoS attack surface, continuously uncover blind spots and remediate their most relevant DDoS risks, and prioritize remediation of DDoS vulnerabilities. No vulnerabilities mean no successful DDoS attacks.

Date of attack	Country	Vertical	Duration of Attack	Downtime	Companies affected		Press
March 5	Estonia	Gov	3 Hours	Unreported	Estonia Digital Voting System	$360,000.00	Link
March 7	Germany	Social Media	4-5 Hours	Ongoing	Mastodon Social Platform	$13,000.00	Link
March 8	Indonesia/ Australia	Banking	8 Hours	Unreported	PT Bank Commonwealth (PTBC)	$1,000,000.00	Link
March 11	USA	IT	96 Hours	48 Hours ongoing	Wallet Guard Twitter Account	NA	Link

Date of attack	Country	Vertical	Duration of Attack	Downtime	Companies affected		Press
March 13	Canada	Entertainment	96 Hours	16 hours ongoing	Behaviour Interactive- Dead by Daylight - Online game	$1,000,000.00	Link
March 15	USA	Gaming	72 Hours	10 Hours	Star Vault Studios Game - Mortal Online 2	$25,000.00	Link
March 23	Australia	Several	72 hours	Ongoing	Australia Fashion Week, Government websites, Banks and Ports.	NA	Link
March 27	France	Gov	24 Hours	Ongoing	France's National Assembly website	$1,500,000.00	Link

Date of attack	Country	Vertical	Duration of Attack	Downtime	Companies affected		Press
March 28	Australia	Several	48 hours	Ongoing	Several Australian Higher Education Institutions	NA	Link
March 28	Germany	Weapon Manufacturer	4 Hours	3 Hours	Rheinmetall	$3,500,000.00	Link
March 29	France	Gov	18 Hours	6 Hours	The websites of the French National Assembly, the French Senate and the Children's Parliament	$420,000.00	Link