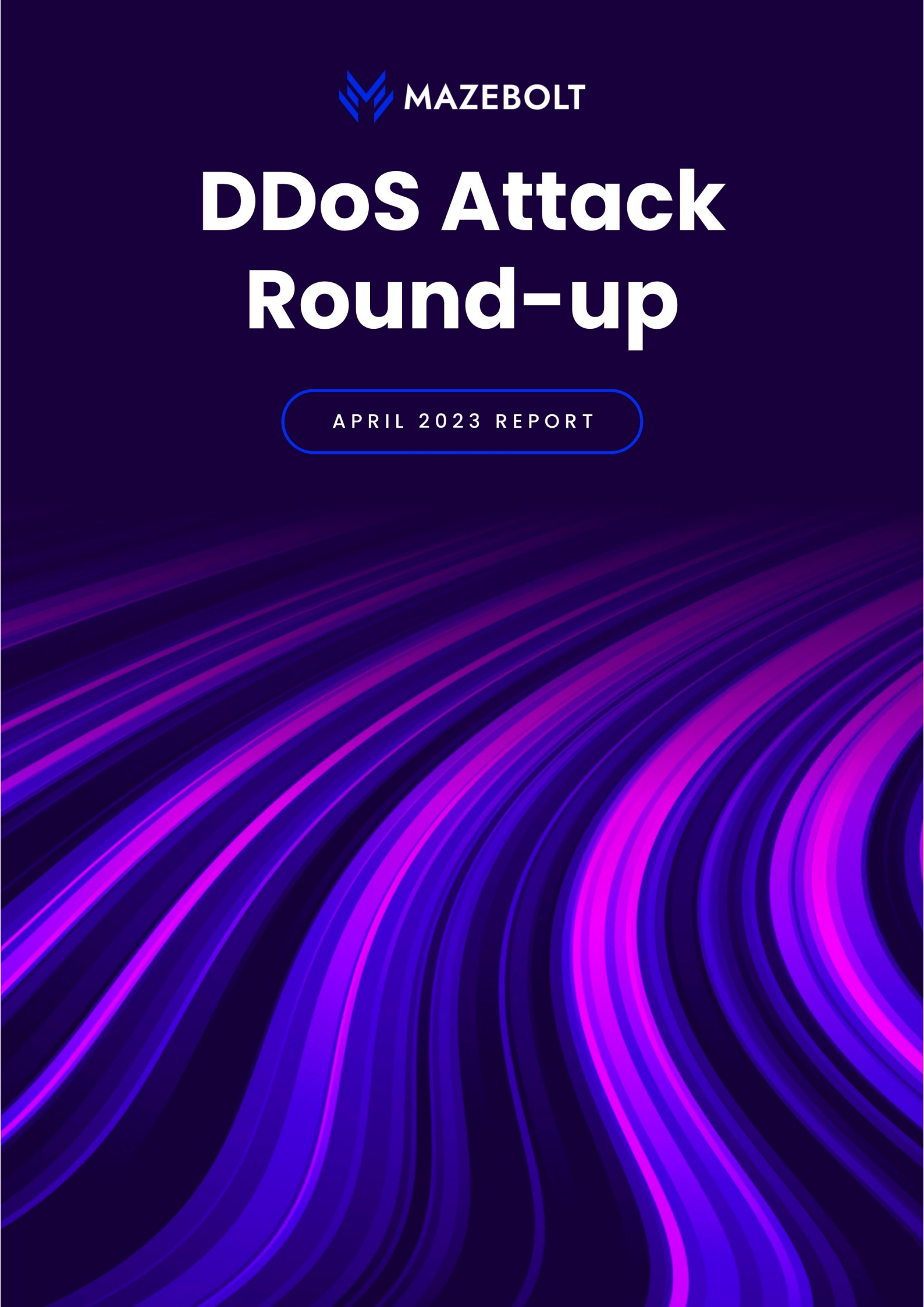
MAZEBOLT

DDoS Attack Round-up

APRIL 2023 REPORT



Israel is Under Fire

Every April, several DDoS attacker groups launch #OpIsrael, usually around April 7th. But this year, there we saw a surge of aggressive DDoS attack campaigns, mainly by threat actor group Anonymous Sudan. Following the malicious success of #OpIsrasel, some of the DDoS attackers sought to wreak havoc on other countries as well. The bottom line – the enormous monetary damages and disruption of crucial online services could have been avoided by fine-tuning DDoS protection configurations and continuously testing for vulnerabilities with zero downtime.

The Most Damaging #OpIsrael in Years

Leading up to April 7th, the official date of #OpIsrael, most leading universities in Israel were attacked, with many of them suffering downtime. The same universities were attacked again, later in the month, proving that their DDoS protection is far from effective. Many DDoS attacks were launched on April 7th, and most of them were mitigated, but later in the month, the campaign resumed, with Anonymous Sudan leading the charge against Israel’s leading infrastructure organizations. Israel's Electric Company's services were disrupted several times, the National Insurance Institute’s site crashed during an 18-hour attack, and some of Israel’s leading media outlets were hit as well, including i24News, Kan 11, and CellcomTV. Another major attack was targeting several leading Israeli banks, which were attacked in a combined, 18-hour-long attack that caused severe downtime and disruption to client’s online services. We estimate the initial damages of this combined bank attack to be around 3 million USD, but we can predict that the actual costs will be higher in the long run.

DDoS Protection isn't Protected

One of the most shocking DDoS attacks in April took place on the 27th when The Israeli Mossad's site crashed as well as Checkpoint's services shut down for almost an hour. Both organizations are known for their top-notch security and protection, however, Checkpoint is a company that provides enterprises with end-to-end security. So, while they were down, their clients' networks, cloud, data, and more were unprotected. If companies offering security solutions are vulnerable to DDoS attacks, so too are their customers. The only way to discover vulnerabilities is to continuously test for them and make sure their DDoS security is updated with all attack vectors and known threats.

Damage Cost is on the Rise

At the end of the month, it was officially published that LG Uplus, the leading South Korean communications provider, will pay almost $30 million to more than 4 million retail customers and small business owners following major DDoS attacks that took place in February of 2023. This astonishing amount is added to the real-time monetary damage of the attack, which is estimated to be around $4 million.

So, one successful DDoS attack caused almost $35 million in damages, and disrupted services for millions of clients, in addition to severe reputational implications. In comparison, the attack on Virgin Media UK that took place on April 4th was no less severe. With an estimated $2 million in immediate damages and millions of clients experiencing severe disruption to services, from internet connectivity to zero connectivity to IPTV and mobile phones. This attack took a major toll on Virgin Media. During the 8-hour-long attack, at least 3 hours were considered official downtime, leaving millions, literally, in the dark.

Organizations must take proactive measures to gain important insight into their online services' protection layers. It's hard to imagine that organizations take the risk of falling victim to a successful DDoS attack when the cost of avoiding such an attack is so low in comparison. It only takes one successful DDoS attack to bring an organization's online services down. In order to avoid that attack, it is vital to continuously test for DDoS vulnerabilities and remediate the relevant DDoS risks. This can be done without disruption to production, and it only takes one step – to be proactive. At the end of the day, no vulnerabilities mean no successful DDoS attacks.

Date of attack	Country	Vertical	Duration of Attack	Downtime	Companies affected	Estimated Damage	Press
April 3	Israel	Education	4 Hours	1 Hour	the Open University, Ben-Gurion University, the Technion and the University of Haifa, and other academy institutions	NA	Link
April 4	Finland	Government	4 Hours	2.5 Hours ongoing	The Finnish parliament's website	NA	Link
April 4	UK	Telecom	8 Hours	3 Hours	Virgin Media Broadband ISP	**2 Mil USD**	Link
April 5	Finland	Media	3 Hours	0.5 Hours	The Finnish Broadcasting Company's (Yle) website	NA	Link

Date of attack	Country	Vertical	Duration of Attack	Downtime	Companies affected	Estimated Damage	Press
April 6	Germany	Government	4 Hours	2 Hours ongoing	The citizen services portal and the police websites, state authorities and several ministries	NA	Link
April 8	India	Aviation	9 Hours	9 Hours ongoing	6 Major airports including Delhi, Mumbai, Hyderabad, Goa and Cochin airports	**4Mil USD**	Link
April 11	Canada	Government	4 Hours	2 Hours	Prime Minister Justin Trudeau's official website	NA	Link
April 12	USA	Gaming	2 Hours	1.5 Hours	Blizzard - Battle.net (World of Warcraft, Overwatch 2, and more)	**1.2Mil USD**	Link

Date of attack	Country	Vertical	Duration of Attack	Downtime	Companies affected	Estimated Damage	Press
April 12	Canada	Ports	12 Hours	2 Hours ongoing	The Port of Halifax, Port authorities in Montreal and Quebec	NA	Link
April 13	Canada	Critial Infrastructure	12 Hours	6 Hours Ongoing	Hydro-Québec	**4Mil USD**	Link
April 14	Israel	Banking + Government	18 Hours	Ongoing	Postal service and banks such as Bank Leumi, Bank Benleumi, Discount Bank, Mizrahi-Tefahot, Bank Mercantile, and Bank Benleumi subsidiaries Bank Otzar Ha-hayal and Bank Massad.	**3Mil USD**	Link
April 14	Israel	Government	18 Hours	1 Hour	National Insurance Institute's website	NA	Link

Date of attack	Country	Vertical	Duration of Attack	Downtime	Companies affected	Estimated Damage	Press
April 14	Israel	Education + Media	8 Hours	0.5 Hour	the Open University, Ben-Gurion University, the Technion and the University of Haifa, as well as media outlets such as The Jerusalem Post, Kan 11 and i24News.	NA	Link
April 17	South Korea	Gaming	6 Hours	Ongoing	Ironmace - Dark And Darker (playtest)	NA	Link
April 19	USA	Gaming	3 Hours	1 Hour	Blizzard - Battle.net (Call of Duty, World of Warcraft, Overwatch 2, and more)	**750K USD**	Link
April 20	Belgium	Aviation	72 Hours	Ongoing	Eurocontrol	**6Mil USD**	Link

Date of attack	Country	Vertical	Duration of Attack	Downtime	Companies affected	Estimated Damage	Press
April 26	Israel	Ports	9 Hours	Ongoing	Website of Haifa port and Israel Ports Development & Assets Company	NA	Link
April 27	Israel	Government /Technology	3 Hours	0.5Hours	The Mossad website, Checkpoint webiste	NA	Link
April 28	Czech Republic	Government	6 Hours	2 Hours	Prague City Hall Website	NA	Link
April 28	USA	Airport/ shipping	3 Hours	0.5 Hours	UPS Website, and the Hartsfield-Jackson Atlanta International Airport website	**6Mil USD**	Link