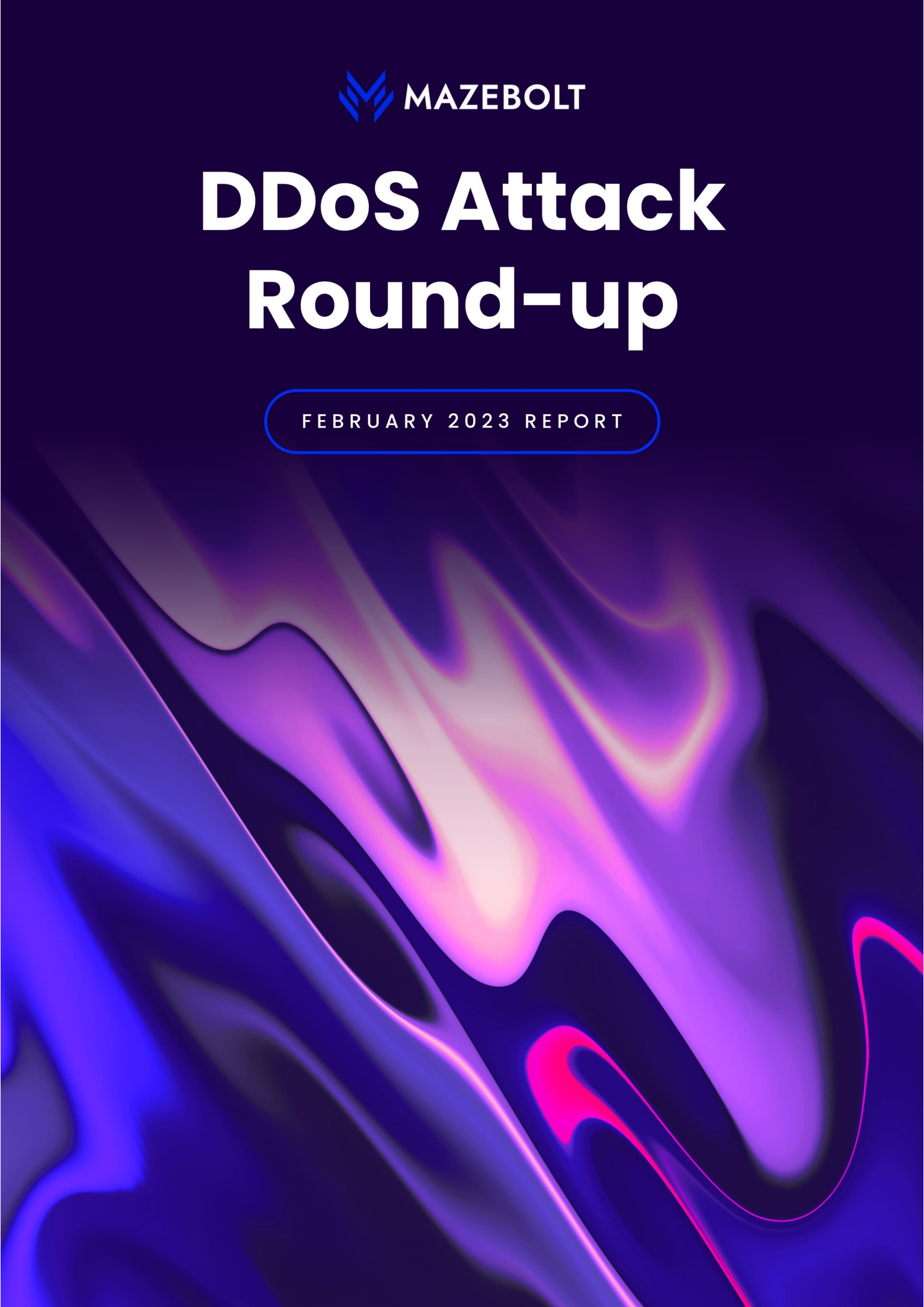
MAZEBOLT

DDoS Attack Round-up

FEBRUARY 2023 REPORT



Short Month, But the DDoS Attackers Used Every Minute of it

February will be recorded in history as the month in which DDoS attackers decided to escalate their efforts to disrupt and cause mayhem all over the world, with a blatant disregard for their fellow man. While major attacks on governments, telecom providers, and media outlets took place, which is the sad norm for DDoS attacks, February saw four major attacks that could mark a pivotal point in the DDoS battlefield.

Germany and Sweden suffered Major DDoS attacks on airports and airlines on the one hand, and on the other, Denmark and the US suffered sophisticated attacks on several hospital and medical organizations. These attacks are a new low for DDoS threat actors. These attacks may evolve into more complex and sophisticated attacks that can put lives at stake. It is also clear that the Nordic region is a major target nowadays, following several religion-oriented incidents, as the attackers who took responsibility for the Sweden and Denmark attacks claimed to have performed said attacks due to these countries' disregard for these religious incidents.

Medical Facilities are No Longer a Safe Haven

The US attack that occurred on February 1st was a major attack that lasted three days. During this attack, 14 hospitals' sites were down, with crucial services rendered unavailable for patients and customers. This includes the site for Cedars-Sinai, one of the busiest hospitals in the US. The pro-Russian hacktivist group Killnet claimed responsibility for these attacks, as part of their ongoing campaign against the US, for its support of Ukraine. The Denmark medical facilities attacks lasted 6 hours, with a shutdown period of over 2 hours, in which nine hospitals' sites were down, with critical services unavailable for patients. This attack was launched because of a religious incident in front of the Turkish embassy in Stockholm.

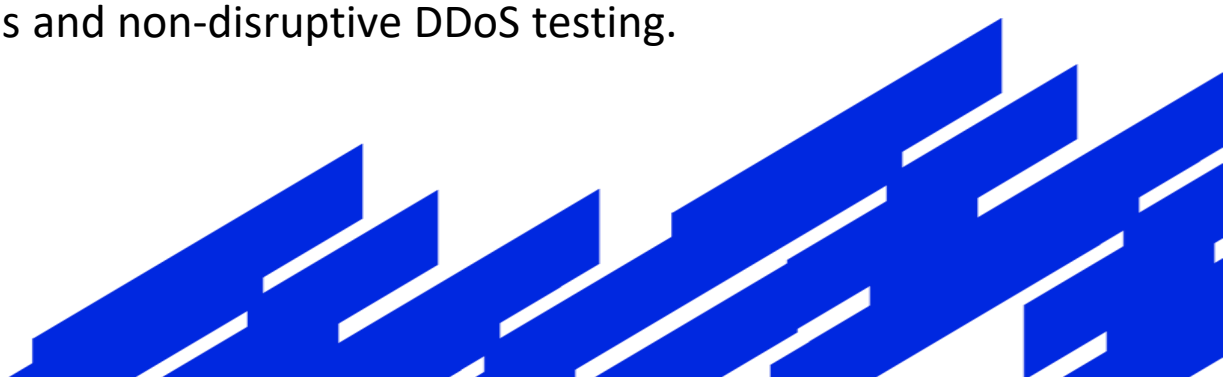
These horrendous attacks on medical facilities prove that DDoS threat actors are no longer considering the medical industry off-limits. No matter what their causes are, whether political, ideological, or simple crime, DDoS attackers have crossed the line and moved into life-threatening territories.

The Cost is Getting Too high - the Germany Airlines Attack

The coordinated attack on German Airlines took place for 4 hours and brought an hour-long shutdown of services in 7 airports across Germany. Seven airports' sites were down due to this attack, including Dortmund, Nuremberg, and Dusseldorf. Overall, around 250 flights were canceled during this attack. Considering the damages inflicted by an hour of a service shutdown in seven airports, this attack turns into a major incident. An hour of shutdown may not seem like a lot at first glance, but when trying to calculate the overall cost of this attack, the numbers become serious.

In a conservative and rough calculation, an average flight will cost an airline around 40,000 USD. This includes the costs of staff (both ground and in-air), fuel, landing permissions, taxes, etc. This amount is the average of Cross-Atlantic and In-Continent flights, with an average duration of 5 hours. When multiplying 250 flights by 40,000 per flight, the conservative estimation of monetary damage for the airlines inflicted alone is 10 million USD. If we add the monetary damages to the airports themselves and the passengers, we might end up with 20 million USD in damages. As mentioned, this attack lasted for 4 hours with an hour-long shutdown. Imagine what would happen next time, when the DDoS attack will be more complex, with longer downtime and perhaps even life-threatening implications.

It's clear that organizations, no matter the field they're in, must take a proactive approach to their DDoS resilience, as DDoS attackers are getting more aggressive with their attacks. A successful DDoS attack is one that penetrates mitigation layers, exploiting unknown vulnerabilities, and the average DDoS vulnerability for organizations is between 30-75%. 2023 will most likely see a rise from the average 23,000 DDoS attacks per day, and a solution like RADAR is critical for organizations who wish to strengthen their DDoS resilience, no matter who is their mitigation vendor. RADAR is the only solution that uncovers blind spots present in existing mitigation layers, through continuous and non-disruptive DDoS testing.



Date of attack	Country	Vertical	Duration of Attack	Downtime	Companies affected	Comments	Press
February 1	USA	Medical	72 Hours	Ongoing	14 Hospitals and medical websites including Stanford Healthcare, Duke University Hospital and Cedars-Sinai.	The Pro-Russian hacktivist group Killnet claimed responsibility for the attacks	Link
February 4	South Korea	Telecom	72 Hours	30 Minutes	LG UPLUS	LG Uplus' internet service suffered connection failures due to DDoS attacks about three times during the past week, including the latest one. It was also attacked at around 3:00 a.m. and 6:00 p.m. on Jan. 29. They caused a connection failure for about 20 minutes each time.	Link
February 12	Belgium	NATO	24 Hours	Ongoing	Several NATO websites	The DDoS attack may also have affected networks used by NATO's Strategic Airlift Capability (SAC), a program within NATO that provides military airlift capabilities to 12 member states using Boeing C-17 Globemaster III aircraft.	Link

Date of attack	Country	Vertical	Duration of Attack	Downtime	Companies affected	Comments	Press
February 15	Sweden	Airline	2 Hours	30 Minutes	SAS - Scandinavian airline	Scandinavian airline SAS was hit by a cyber-attack yesterday that reportedly downed its website and app, and may have leaked customer information	Link
February 16	Germany	Airline	4 Hours	1-1.5 Hours	7 Airports website including Dortmund, Nuremburg and Dusseldorf	The websites of airports including Dortmund, Nuremburg and Dusseldorf taken offline. Larger German airports, including Munich, Berlin and Frankfurt were not targeted in the attack.	Link
February 16	Morroco	Media	6 Hours	Ongoing	Rabat - Moroccan news agency Maghreb Arab Press (MAP)	A number of the agency's sites were down following the attack on Thursday night.	Link

Date of attack	Country	Vertical	Duration of Attack	Downtime	Companies affected	Comments	Press
February 22	Italy	Governme nt, Energy	12 Hours	Ongoing	Foreign Affairs and the Carabinieri websites	Ministry of Foreign Affairs and Defence, Carabinieri, Bper bank, A2A (energy), interior site for the identity card, site of agricultural policies, and of the Tim group, which hosts all the attacked sites	Link
February 22	Russia	Media	1 Hour	30 Minutes	All-Russia State Television and Radio Broadcasting Company (VGTRK), Smotrim live-streaming platform	The DDoS attacks downed several websites broadcasting President Putin's state of the nation address	Link
February 26	Denmark	Medical	6 Hours	2.5 Hours	9 Danish Hospitals Websites	Anonymous Sudan claimed on Telegram the attacks were "due to Quran burnings," a reference to an incident in Stockholm in which the holy book was set alight in front of the Turkish embassy	Link