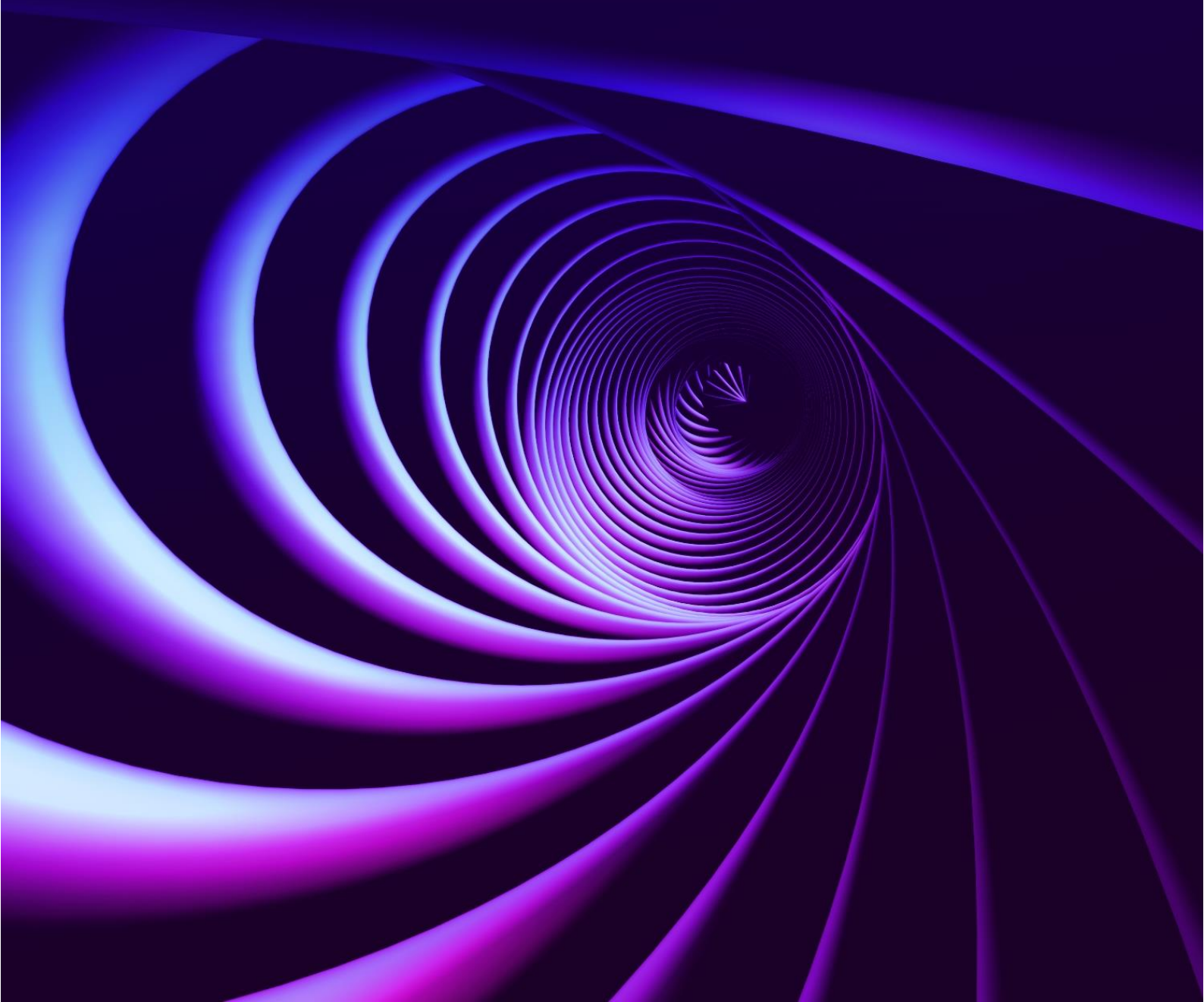
MAZEBOLT

DDoS Attack Round-up

MAY 2023 REPORT



Airlines Are Going Down

Following several successful DDoS attacks on airlines earlier in the year, it seems like DDoS attackers got greedy. SAS, the Scandinavian airline, was hit with a DDoS attack on May 24th, with the attackers demanding ransom. But in contrast to previous attacks on airlines, this one turned out to be much more malicious and costly. Failing to mitigate the attack, SAS received a higher ransom demand of $175K, and after 5 straight days of being under attack, SAS received a new ransom demand of $3 million.

Anonymous Sudan launched the attack, and for 5 days, most of SAS' online services were down. Many customers turned to social media to express their frustrations, and we cannot even begin to estimate the actual damage inflicted on SAS following this attack. The financial loss is enormous, before considering the ransom (it is unclear if SAS eventually paid it). The operational damage is enormous as well, as we can only assume many of SAS' staff were probably allocated to deal with the situation. And the reputational damage may be tremendous – but time will tell.

At one point, the SAS tried to handle the situation and suggested on Twitter that customers could still log in to the Danish version of the SAS website, which led Anonymous Sudan to take that website offline as well. If you want a personal view on the SAS attack – check out our VP, Orly Mager, and her experience with this attack. It is unclear if and how many flights were canceled due to the attack, but assuming that many tickets could not be purchased through SAS' website, as well as other online services that were unavailable, we can assume the financial damage is severe.

What is clear is that once again, organizations are reminded, in the hardest way possible, that even the best DDoS protection leaves them vulnerable to DDoS attacks. Anonymous Sudan, which usually attacks with political motivations, chose to attack SAS this time for ransom, and just as we predicted in our 2023 predictions, DDoS attackers now realize that they can turn in a profit, in addition to fulfilling their desire to disrupt and cause mayhem. Organizations simply cannot afford to continue operating with hidden vulnerabilities in DDoS security, as DDoS threat actors will take advantage of said vulnerabilities, and the price, of ransoms and damages - will continue to rise.

Mid-Month Pause – Quiet Before the Storm

Going through our monthly report, you'll notice that several major attacks were reported at the beginning of the month, and major ones were reported towards the end – but in the middle of May, it seemed all was quiet on the DDoS front. We can only assume that this break from attacks followed the FBI's operation to seize 13 domain names connected to services that allowed paying customers to launch DDoS attacks. i.e. – DDoS for hire.

Following a successful campaign in December of 2022, in which the FBI charged six U.S. men with providing DDoS for hire services, the FBI launched another step of their wide-spared coordinated international campaign, known as "Operation PowerOFF", aimed at disrupting online platforms allowing anyone to launch massive DDoS attacks against any target for the right amount of money. It's likely that following the arrests, several DDoS attackers kept a low profile, still as we now know – this was just a pause, as the end of May saw widespread and disruptive attacks: not only on SAS, but also on the Greek education system, the Senegalese and South-African governments, and the Polish media industry.

The FBI's efforts are noble, but far from being enough. Organizations must not rely on external developments to protect themselves. As we see time and time again, even the best DDoS protection organizations are still vulnerable, and the only way to have complete DDoS resilience is to perform continuous and non-disruptive DDoS testing and remediation.

Date of attack	Country	Vertical	Duration of Attack	Downtime	Companies affected	Estimated Damage	Press
May 1	Zimbabwe	Internet Service Provider	24 Hours	Ongoing 13 Hours	Liquid (Zimbabwe's biggest ISP)	**350K USD**	Link
May 2	Sweden	Government	48 Hours	5 Hours	Sweden's parliament website	**NA**	Link
May 4	Netherlands	Goverment	6 Hours	4 Hours	The Dutch court system's website and the website of the Dutch Senate	**NA**	Link
May 5	France	Goverment	18 Hours	3 Hours	The French Senate website, France's National Centre for Space Studies and Naval Group, and a French industrial group for naval defense manufacturing	**NA**	Link

Date of attack	Country	Vertical	Duration of Attack	Downtime	Companies affected	Estimated Damage	Press
May 16	India	Police	12 Hours	3 Hours	23 State Police websites	NA	Link
May 16	Iceland	Government	4 Hours	2 Hours	The website of the Government Office, the Court of Justice, the Communications Office and the Environment Agency	NA	Link
May 18	Pakistan	Government	4 Hours	4 Hours	10 Pakistani embassy websites from around the world	NA	Link
May 18	Poland	Media	72 Hours	Ongoing	Daily Newspapers Gazeta Wyborcza,wPolityce.pl., Rzeczpospolita and Super Express.	3MM USD	Link

Date of attack	Country	Vertical	Duration of Attack	Downtime	Companies affected	Estimated Damage	Press
May 20	Japan	Muncipalty	5 Hours	2.5 Hours	Hiroshima City website	NA	Link
May 23	South Africa	Government	18 Hours	4 Hours	Western Cape Provincial Parliament (WCPP)	NA	Link
May 24	Sweden	Airline	5 Days	5 Days	SAS Airline	NA	Link
May 26	Senegal	Government	48 Hours	24 Hours	Several Senegalese government websites	NA	Link
May 28	Greece	Government/ Education	48 Hours	40 Hours	Subject Bank Online Exam Platform	NA	Link