MAZEBOLT

DDoS Attack Round-up

JANUARY 2023 REPORT

Opening 2023 With an Escalation

As we've witnessed in the past year, DDoS has become the leading global cyber threat, with malicious and sophisticated attacks hitting across the globe, in all industries. And yet, it was evident that the threat actors' main focus was on several key industries. Governments were hit with DDoS attacks for two main reasons: a government's involvement or position towards the Russia/Ukraine conflict, and a government's overall internal policy. Financial institutions were hit for ideological and criminal reasons, as were the gaming and IT industries. But it seemed that the Healthcare industry was off limits, in most cases. Sometimes it was hit as part of an overall attack on governments, like in the case of the DDoS attack on the Greek government, but throughout 2022, it seemed that threat actors prefer to keep the healthcare industry off limits. Up until now.

January saw two major attacks on the healthcare industry: the Netherlands and the US. Both attacks were launched by the Russian hacktivist group "Killnet", for the same reason, probably due to the country's involvement in the Russia/Ukraine conflict. The attack in the Netherlands was severe and lasted for three days, indicating the hospital's lack of mitigation, while the US attack was larger in scale but lasted three hours. That may seem like a short period, but given that lives were at stake, three hours are three hours too many.

Spreading the Disease

Another worrying trend we've noticed in January of 2023 is the expansion to new territories of attack. If 2022 saw a growth in the number of countries attacked, then 2023 opened with new players in the DDoS game, and this is a dangerous game to play. Serbia, the Czech Republic, and Nepal were not targeted that much in 2022, but all three countries suffered complex DDoS attacks, with Nepal suffering a continuous, 36-hour attack. This, in addition to the severe attacks on Banks in Germany and Denmark.

South Korea suffered a major attack that turned out to be even more severe than it initially seemed. LGU+, Korea's biggest mobile operator and service provider,was attacked by a malicious DDoS attack on January 30th. Services including LGU+ internet and credit cards are unavailable due to the attack. A week later, the JoongAng Daily reported that following a second serious DDoS attack that happened a few days later, the Korean government issued "a strong warning" to the telecommunications provider and promised a strict investigation of the company's cyber security systems. This is yet another reminder of how damaging DDoS attacks can be, and the fact that organizations cannot afford to keep flying blind when it comes to protecting their environment from DDoS threats.

Date of attack	Country	Vertical	Duration of Attack	Downtime	Companies affected	Comments	Press
January 3	Japan	Goverment	3 Days	3 Days	Tokyo's Shibuya Ward	Shibuya ward spokespamn said that the DDoS attach came apparently in retaliation for the eviction of homeless people from a closed park.	Link
January 5	Iran	Finance	2 Days	Unreported	Central Bank of Iran	Iran's infrastructure has come under numerous cyber-attacks recently, particularly since the outbreak of foreign-backed riots across the country in September last year.	Link
January 8	Serbia	Government	3 Hours	0.5 Hours	Website and IT infrastructure of its Ministry of Internal Affairs	The DDoS attacks come amid a spate of similar incidents claimed by Russian-supporting groups in the context of the invasion of Ukraine, although no group has claimed to be behind the attempts.	Link
January 10	Denmark	Finance	3 Hours	1 Hours	Bankdata, Denmark Central Bank, Jyske Bank, Sydbank and 5 other private banks	The attack also affected the IT financial industry solutions developer Bankdata	Link

Date of attack	Country	Vertical	Duration of Attack	Downtime	Companies affected	Comments	Press
January 15	France	Entertainment	3 Hours	1.5 Hours	Virtual 24 Le Mans Race	A number of teams suffered random disconnects throughout the competition due to DDoS attacks	Link
January 25	Germany	Various	5 Hours	1.5 Hours	Multipole Government, Airports, and Banking websites	The DDoS attacks came in response to Berlin's decision to deploy tanks to Ukraine to support its war efforts.	Link
January 28	Netherlands	Healthcare	3 Days	Ongoing	University Medical Center Groningen (UMCG)	The pro-Russian hacker group Killnet is behind the DDoS attacks	Link
January 29	Nepal	Various	36 Hours	Ongoing	Nepal Central Bank, Multipule Government Websites, and Airports	The DDoS attacks had also hit international travel due to the shutdown of the immigration server.	Link

Date of attack	Country	Vertical	Duration of Attack	Downtime	Companies affected	Comments	Press
January 30	South Korea	Telecom	1 Hour	0.5 Hour	LG Uplus	The DDoS attacks paralyzed credit card transaction systems in some superstores and a number of small businesses. There were also reports of disruptions in wired internet use with computers and smart TVs	Link
January 30	USA	Healthcare	3 Hours	1.5 Hours	14 Hospitals including Stanford Healthcare, Duke University Hospital and Cedars-Sinai	Russian hackers (Killnet) are claiming responsibility for a cyberattack that brought down the websites	Link