MAZEBOLT

DDoS Attack Round-up

JUNE 2023 REPORT

Does Microsoft Need a Reboot?

No organization is safe from a DDoS attack, as long as DDoS protection remains misconfigured. That is a hard lesson to learn, and Microsoft joined the infamous club of organizations that fell victim to relatively simple DDoS attacks, that caused severe damages – downtime, losses, and reputational damages. Also in this club is Blizzard, which suffered yet another devastating DDoS attack this month that crippled their version launch of Diablo VI for over 10 hours.

In early June, Microsoft users reported outages in Microsoft 365, Azure, and OneDrive services, in three separate, but highly publicized incidents. Despite the fact that Anonymous Sudan claimed responsibility for the attacks, and despite the fact that it seemed very clear that these outages were indeed DDoS attacks, it took Microsoft several days to release an official blog post confirming that they had suffered layer 7 DDoS attacks.

So, an independent attack group that seemingly came out of nowhere a few months ago managed to shut down services for one of the most prominent enterprises in the world by exploiting DDoS vulnerabilities. Anonymous Sudan established itself at the beginning of 2023 as a major DDoS threat actor. It carried out a series of DDoS attacks against Swedish, Dutch, Australian, and German organizations, retaliating against what they claim to be anti-Muslim activity.

Microsoft identified a specific threat actor responsible for the attack from Anonymous Sudan's ranks, "Storm-1359", revealing the attacker launched layer 7 DDoS attacks, including HTTP(S) flood attack, Cache bypass, and the infamous yet reliable Slowloris DDoS attack. These attack vectors slow traffic and disrupt online services, and in some cases, cause shutdowns. Microsoft assessed that the attacks relied on DDoS-for-hire services and tools to launch the attacks, which caused many disruptions for customers. Twitter was burning with comments and complaints from customers, and the immediate financial damage to Microsoft may be greater than imagined.

Swiss DDoS Protection is Full of Holes

In Mid-June, the Swiss Parliament's website was hit with a DDoS attack. While initial reports claimed the issue was resolved and that no internal systems or data were compromised, the website couldn't be reached for several days.

The group behind these DDoS attacks is Noname057(16), a pro-Russian hacker group that operates several Telegram channels, with over 50,000 followers, in several languages.

NoName057 offers participation in DDoS attack campaigns as part of their "DDoSia Project", which was launched in 2022. DDoSia quickly enlisted over 10,000 followers on Telegram, paying volunteers in cryptocurrency, based on their contribution to DDoS attacks. Before launching the attack, the new members receive a .zip archive containing the toolkit.

NoName057 didn't stop with the Swiss Parliament, though. In addition to the Swiss Parliament's website, other organizations' online services were attacked as well, some of them suffering severe downtime: The Swiss Federal Railways, Armed Forces of Switzerland, Geneva International Airport, airline companies Zimex Aviation and Heliswiss, the Geneva tourism website, and more.

This was a large-scale, full-blown, and highly publicized DDoS attack, but just like the Microsoft attack – it was relatively simple, using "Low and Slow" attack vectors. Bottom line, it's not the size of the attack that counts, in terms of RPM and using multiple sophisticated attack vectors. DDoS protection misconfigurations create, vulnerabilities in DDoS security, so even the simplest DDoS attack vector can shut down business operations.

Date of attack	Country	Vertical	Duration of Attack	Downtime	Companies affected	Estimated Damage	Press
June 1	India	Cybersecurity	24 Hours	Ongoing	CloudSEK	35K USD	Link
June 4	India	Education	24 Hours	Ongoing	The Institute For Teacher Education, The Bengal College of Teacher Education, P.G. institute of medical sciences, Gopsai Avinandan Sangha Primary Teachers' Training Institute, Institute of Science & Technology, Anindita College for Teacher Education	NA	Link
June 5	USA	Communications	24 Hours	10 Hours	Microsoft Outlook, SharePoint Online, OneDrive for Business	4.2MM USD	Link
June 6	Netherlands	Ports	12 Hours	6 Hours	The websites of the port authorities in Rotterdam, Amsterdam, and Den Helder + Groningen Seaport website	NA	Link

Date of attack	Country	Vertical	Duration of Attack	Downtime	Companies affected	Estimated Damage	Press
June 8	USA	Communications	8 Hours	4 Hours	Microsoft OneDrive	1.7MM USD	Link
June 8	India	Education	24 Hours	Ongoing	Bharatpedia - India's local Wikipedia	NA	Link
June 8	Russia	Banks	72 Hours	24 Hours	Several Leading Banks & Credit Unions	NA	Link
June 9	USA	Communications	4 Hours	2 Hours	Microsoft Azure	7MM USD	Link

Date of attack	Country	Vertical	Duration of Attack	Downtime	Companies affected	Estimated Damage	Press
June 12	Switzerland	Gov, Military, Aviation	72 Hours	Ongoing	Swiss Parliament's website (parlament.ch), Swiss Federal Railways, Armed Forces of Switzerland, Bern regional airport, Geneva International Airport, St. Grenchen, Gallen-Altenrhein, and Samedan airports, airline companies Zimex Aviation and Heliswiss, Geneva tourism website	NA	Link
June 13	Poland	Gov	72 Hours	Ongoing	Electronic Platform of Public Administration Services – ePUAP	NA	Link
June 14	USA	Shipping	4 Hours	1.5 Hours	UPS	4MM USD	Link
June 19	Luxembourg	Banks	12 Hours	3 Hours	EIB - European Investment Bank	260K USD	Link
June 20	New Zealand	Ports	8 Hours	6 Hours	North Sea Port website, the company that operates the ports of Vlissingen and Terneuzen in Zeeland, and the Gent port in Belgium - Attacked by NoName05716	NA	Link

Date of attack	Country	Vertical	Duration of Attack	Downtime	Companies affected	Estimated Damage	Press
June 23	Czechia	Gov	6 Hours	1 Hour	website of the Ministry of Foreign Affairs of the Czech Republic	NA	Link
June 25	USA	Gaming	24 Hours	12 Hours	Blizzard's Battle.net - Diablo 4, world of Warcraft, and other titles	8MM USD	Link
June 26	USA	Gaming	36 Hours	3 Hours	BattleBit	NA	Link