MAZEBOLT

DDoS Attack Round-up

AUGUST 2023 REPORT

End of Summer Wave

August has seen less publicized DDoS attacks, and for a while there, it seemed as if DDoS threat actors took some time off - a “summer vacation” if you will. The most vocal threat actors seemed dormant for at least two weeks in the middle of the month, but of course that was not really the case. With many unpublicized attacks, and a lot of unconfirmed attacks that the DDoS perpetrators bragged about, August was actually a very hectic month for DDoS protection vendors. Some of them have had their hands full, as DDoS threat actors continued their malicious efforts throughout the month.

Russia Punishes Eastern Europe’s Banking System

NoName057(16), the infamous Russia state-sponsored DDoS threat actors, managed to shut down the banking systems of two countries, in the span of just a few days. Two widespread attacks were launched against Poland and the Czech Republic’s banking systems, with devastating consequences.

On August 28th, The Warsaw Stock Exchange along with the Polish government's website for public services, and several banks in the country were all targeted and successfully brought down for more than 24 hours of ongoing downtime. While some of the above-mentioned organizations managed to bring their online services back to full capacity within a few hours, others had their online services shut down for almost 36 hours, with on-and-off breaks of availability.

Imagine the frustration across the country, with millions of customers unable to perform any financial action, and in some cases, unable to use ATM machines. A very similar situation occurred in the Czech Republic just two days later, with five banks getting hit with a DDoS attack launched by NoName057(16) - Česká spořitelna, ČSOB, Air Bank, Fio Banka and Komerční banka. This time, the overall downtime lasted for 48 hours, with similar results - financial losses, operational chaos, and severe reputational damages.

These attacks were successful only because of **misconfigurations in the DDoS protections deployed**, which led to **DDoS vulnerabilities**. Only through continuously identifying vulnerabilities and prioritized remediation can organizations avoid a damaging DDoS attack - otherwise, SLAs with guaranteed damaging downtime will be required during an actual attack.

DDoS is Used as an Anti-Democracy Weapon in Hungary

An official report was published lately by the International Press Institute (IPI), stating that we are witnessing an unprecedented wave of DDoS attacks targeting independent media outlets in Hungary in recent months. This attack wave poses a serious and growing threat to the free flow of information in the European Union's worst country for press freedom. As many official reports indicate, Hungary is considered a "Fragile and Backsliding Democracy". Hacktivists see political interference by the legislative and executive branches of government as threatening the institutional independence of the judiciary - and in this case, the free press.

The report indicates that since April 2023, at least 40 different media websites in Hungary have suffered severe DDoS attacks, with the majority of portals targeted including many of the country's leading independent media, including Telex, HVG, 444.hu, Magyar Hang, Forbes Hungary, and Népszava. These portals are officially opposing Prime Minister Viktor Orbán's government. To date, no media outlet supporting the ruling Fidesz party has been targeted in the current wave of attacks, according to IPI assessments, indicating a political or ideological motive.

The DDoS attacks appear to follow a pattern of targeting critical and independent media websites and were, in some cases, aimed at disrupting access to news reporting that criticizes the government. In some cases, the damaging DDoS attacks began less than half an hour after the publication of reports critical of the government or entities connected to it. This may indicate a new type of politically motivated DDoS threat - the internal threat kind, meaning potential political adversaries within the same country using DDoS as a weapon.

So far, we've witnessed many politically motivated DDoS attacks sponsored or launched by countries against other countries due to their international policies. But this new wave of Hungarian DDoS attacks may be the start of a new trend - democratic countries in political turmoil using DDoS as a means to control and manipulate their inbound media, to control the flow of information.

The only DDoS attack in Hungary that was officially published this month was the eight-hour-long attack on the Mex Internet Radio Network, but as the report mentions, over 40 DDoS attacks have been successful since April, with little to no international echoing. It is alarming, and we will keep our eyes open to report if this trend indeed goes global.

Date of attack	Country	Vertical	Downtime	Companies Affected	Estimated Damage	Press	Threat Actor + Affiliation
August 8	France	Government, Finance	6 Hours	The national customs service, French financial regulator's website	**NA**	Link	NoName057(16) - State Sponsored by Russia
August 8	Netherlands	Government, Finance	6 Hours	Dutch public transport website, local bank SNS, the Groningen seaport, and the website of the municipality of Vlardingen	**SNS Bank: est. 700K**	Link	NoName057(16) - State Sponsored by Russia
August 12	UAE	Infrastructure	36 Hours	International oil corporation - the website of **Levare** International Ltd. (Levare)	**NA**	Link	Medusa ransomware group
August 12	Japan	Infrastructure	24 Hours: Ongoing	Several leading nuclear websites in Japan: the Japan Atomic Energy Agency, Japan Atomic Power Corporation, and the Atomic Energy Society of Japan	**NA**	Link	Anonymous

Date of attack	Country	Vertical	Downtime	Companies Affected	Estimated Damage	Press	Threat Actor + Affiliation
August 22	South Africa	Media	1 Hour	The Daily Maverick	**NA**	Link	Unknown attacker from India
August 28	Poland	Financial	36 Hours: Ongoing	The Warsaw Stock Exchange, the Polish government's website for public services, Raiffeisen Bank, Plus Bank, Credit Agricole Bank	**30Mil USD**	Link	NoName057 (16) - State Sponsored by Russia
August 29	USA	Social Media	2 Hours	X (formerly Twitter) was offline in more than a dozen countries in an attempt to pressure Elon Musk into launching his Starlink service in their country.	**NA**	Link	Anonymous Sudan

Date of attack	Country	Vertical	Downtime	Companies Affected	Estimated Damage	Press	Threat Actor + Affiliation
August 30	Czech Republic	Financial	48 Hours: Ongoing	Leading Banks: Česká spořitelna, ČSOB, Air Bank, Fio Banka and Komerční banka - Services restored on August 31st	**8Mil USD**	Link	NoName057(16) - State Sponsored by Russia
August 30	France	Government, Infrastructure	9 Hours	La Poste - the postal service company in France	**NA**	Link	#OpFrance - Anonymous Sudan
August 30	Hungary	Media	8 Hours	Mex Rádió Network Kft. - Internet Radio	**NA**	Link	Probably HANO, A local threat actor
August 31	USA	Media	2 Hours: Ongoing	Archive of Our Own (Ao3)	**NA**	Link	Anonymous Sudan