MAZEBOLT

December 2022

DDoS Attack Round Up

Closing the year with severe DDoS attacks

2022 was full of turmoil when it comes to DDoS attacks. Following the events of 2021 and the war between Russia and Ukraine, 2022 saw a dramatic rise in politically motivated DDoS attacks on the one hand, and malicious ransom DDoS attacks on the other. New threat actors emerged, new and old botnets were used in widespread attacks, and the surface became more dynamic.
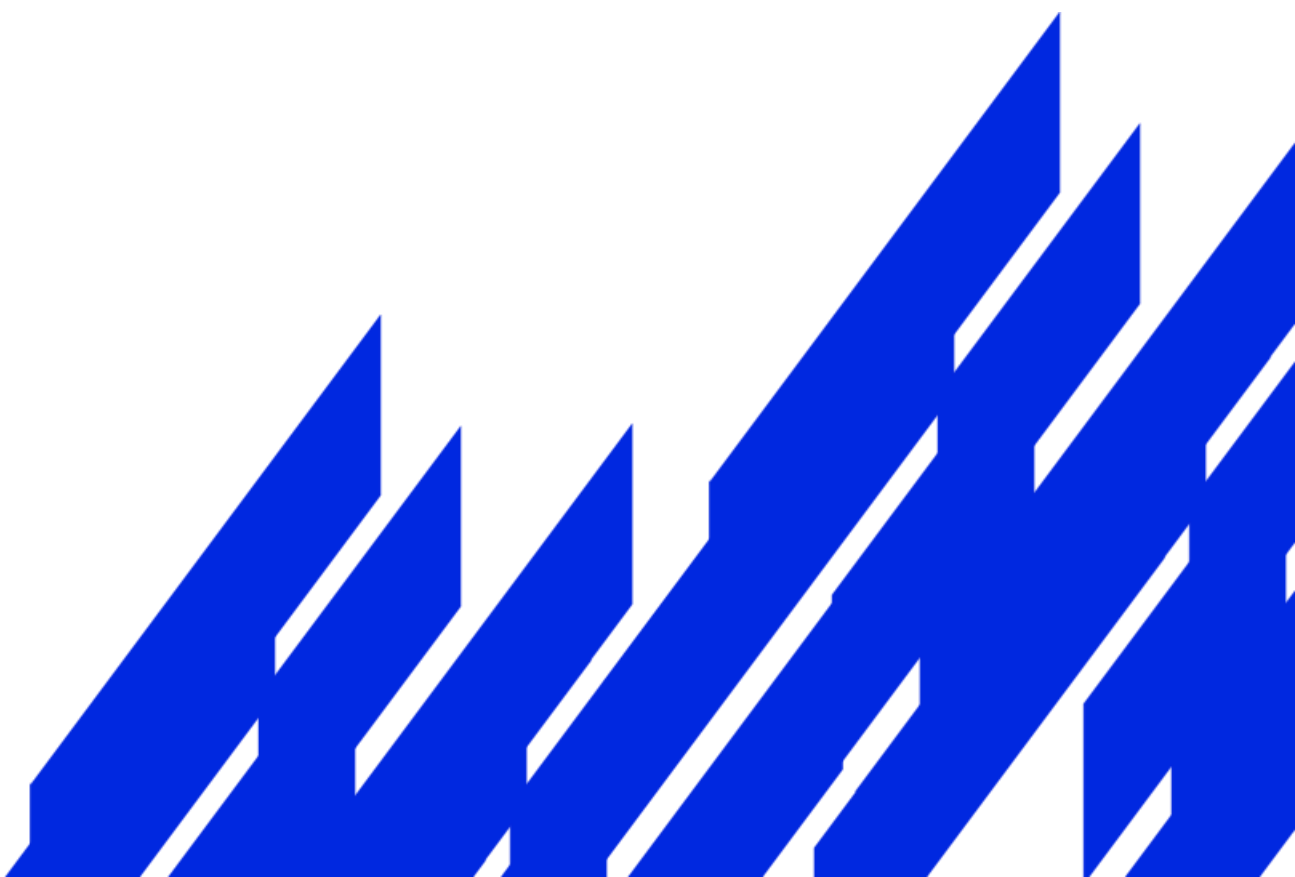
The end of the year continued these trends, and sadly, also the latest trend which is longer and more complicated attacks. Three major DDoS attacks that took place in December lasted over 24 hours. The shortest of the three was an attack on Ukraine's Ministry of Defense and Armed Forces, combined with a DDoS attack and PrivatBank and Oschadbank, both major Ukrainian financial institutions. This widespread attack took place over 24 hours, with several hours of official downtime.

The other two major attacks were even more severe: the Russian bank VTB was under a five-day attack, which caused disruptions throughout the entire period. This led to the bank issuing a statement that claimed that the attack was "The largest, not only this year, but in the whole time the bank has operated". The third major attack targeted The Metropolitan Opera in New York, and it lasted seven whole days, with a total downtime of over 24 hours. Online operations, including commerce, were affected and damaged, and an official statement from then Opera confirmed that internal files were also breached.

These complicated attacks prove, yet again, that the DDoS threat is constantly evolving and causing major disruption and severe damage. The motivations may vary from pure greed to disruption for the sake of it or political ideology, but the results are always significant downtime and total disruption of services, sometimes crucial. Going over this month's roundup, you will notice that the connecting thread between most attacks is political and financial, with no preference for a specific side in a specific conflict. It appears that, as proven throughout 2022, no one is safe and that DDoS attacks can hit anyone, anywhere, anytime.

But we do not want to close out 2022 on a sour note, despite the troubling data. First of all, we'd like to wish you a happy new year, and we hope that 2023 will bring joy and prosperity to you and your family. On the professional side, we're happy to share that DDoS resilience is not a complicated matter, but something that can be achieved with a few simple steps, so there's really no reason for any organization to not get critical insight into their critical DDoS vulnerabilities in the dynamic attack surface. 2023 is going to continue with alarming DDoS attack trends, and organizations should remediate their vulnerabilities to have the best possible mitigation.

Date of attack	Country	Vertical	Duration of Attack	Downtime	Companies affected	Comments	Press
Dec 3	Italy	Government	1 Hour	0.5 Hours	The Italian Ministry of Agriculture	The incident happened after Pope Francis suggested in an interview that some Russian ethnic groups were the "cruelest" against Ukrainians in the ongoing conflict.	Link
Dec 5	Belgium	Government	12 Hours	1.5 Hours	The city of Antwerp	The disruption in services has affected everything from schools, daycare centers, and the police. The DDoS attack was a part of a wide ransdom attack	Link
Dec 6	Russia	Banking	5 Days	Disruptions over 5 days	VTB	VTB said in a statement. "The largest not only this year, but in the whole time the bank has operated."	Link
Dec 7	USA	Entertainment	7 Days	30 Hours	The Metropolitan Opera, New York	The company's website, box office, call center, gift shop and streaming platform were restored after a week of disruption, but an email to company members confirmed that internal files were breached.	Link

Date of attack	Country	Vertical	Duration of Attack	Downtime	Companies affected	Comments	Press
Dec 8	Denmark	Government	2.5 Hours	1.5 Hour	Denmark's Defence Ministry	Denmark's defence ministry was hit by a cyberattack on Thursday that had cut off access to its websites	Link
Dec14	USA	Media	3 Hours	2 Hours	FuboTV	FuboTV reported that it fell victim to a cyberattack last Wednesday that knocked out access to the service during the time of the World Cup semifinal game between France and Morocco	Link
Dec 16	Ukraine	Government / Banking	24 Hours	2 Hours	Ukraine's Ministry of Defence and Armed Forces + PrivatBank and Oschadbank,	This follows a number of attacks reported at the end of January which affected numerous Ukrainian official websites.	Link
Dec 25	Iran	Social Media Platform	6 Hours	6 Hours	Eita	The DDoS attacks launched from the US and Europe, adding that attackers had created more than 140 terabytes of traffic with a maximum rate of 30 gigabits per second.	Link