MAZEBOLT

November 2022

DDoS Attack Round Up

The Major Attack Trends of November

As we learned in the past year, financial and governmental institutions continue to be the most sought-after targets for DDoS attacks, with these attacks spanning and reaching every major country. November saw a rise in political targets, as the US held their midterm elections on the one hand, and on the other, CISA and the FBI recognized DDoS attacks as a serious threat and published an official report about the growing danger of DDoS attacks.

The DDoS attacks in November continue the trend of political groups like Killnet and other pro-Russian groups, that perform their acts with a political agenda.

Attack Duration on the Rise?

Of the twelve major reported attacks performed in November, five attacks lasted for several hours, and in the worst cases, several days. These attacks resulted in major financial and governmental sites shutting down for over three hours, and in the specific case of “BikePortland”, an Ecommerce organization, a major shut down of one whole week.

“Loopring”, an American trading platform, was shut down for four hours, and the FBI’s site was down for three whole hours on November 14th. A few days before, a Russian hacktivist group, “The People’s Cyberarmy”, called on its members to target the American Democratic party website. This resulted in the site going down for five hours, right after the midterm elections.

Major Attacks on Financial and Governmental Sites Worldwide

In Greece, the government's site was down for 72 whole hours, with more than 800 services of Greece's Gov.gr being frozen by an unprecedented DDoS attack. The cyber-attack reportedly came from the Netherlands and damaged many government institutions, including medical services. In Switzerland, a major trading platform, "Swissqoute", was down for about ten hours, and in North Korea, a major internet provider was shut down for five hours, resulting in disrupting regular activity for the national airline and major internal email servers.

These hazardous attacks may indicate an escalation in complexity and hacker groups expanding their attack layers. With many global organizations lacking visibility into their critical vulnerabilities, we find this data to be alarming, and we will continue monitoring for trends and new attack vectors as 2022 comes to an end.

Date of attack	Country	Vertical	Duration of Attack	Downtime	Companies affected	Comments	Press
Nov 4	USA	Finance	4 Hours	4 Hours	Loopring (Etherum Trading Platform)	Loopring (LRC) has stated that it's being targeted in a DDOS attack on the same day that its value is rising.	Link
Nov 5	USA	Media	1 Week	1 Week	BikePortland		Link
Nov 7	Estonia, Poland, Romania, Bulgaria, and Moldova	Government	3 Hours	0.5-3 Hours	State intelligence agencies of Estonia, Poland, Romania, Bulgaria, and Moldova	The hacking group Killnet from Russia took responsibility for the attacks as a part of a long campaign against Ukraine's allies	Link
Nov 8	USA	Multipule	1.5 Hours	0.5-1.5 Hours	Election administrator sites of Mississippi, Illinois	The Department of Homeland Security said it's working with local elections officials to mitigate several low-level cyberattacks that affected websites in a handful of states on Election Day.	Link
Nov 8	USA	Government/ Media	5 Hours	0.5-3 Hours	The Democratic Party Website, https://democrats.org/	A Russian hacktivist group calling itself "The People's Cyberarmy" called on its members to target the American Democratic party website	Link

Date of attack	Country	Vertical	Duration of Attack	Downtime	Companies affected	Comments	Press
Nov 9	Switzerland	Finance	48 Hours	5-10 Hours	Swissquote	Swissquote, an online trading platform, confirmed that its servers were the target of "a massive DDoS attack"	Link
Nov 11	Greece	Government	72 Hours	72 Hours	Greece's Gov.gr	More than 800 services of Greece's Gov.gr and TAXISnet, as well as medical prescriptions, were frozen by an unprecedented DDoS attack. The cyber attack reportedly came from the Netherlands.	Link
Nov 14	USA	Government	3 Hours	1.5-3 Hours	FBI Website (Federal Bureau of Investigation)	A pro-Russian hacking group took responsibility for an alleged attack on a section of the FBI's website	Link
Nov 16	USA/Canada	Media	2.5 Hours	1 Hour	Rumble	An hour after Ruble reported a DDoS attack on their servers, the attack was mitigated.	Link
Nov 17	North Korea	Telecom	2.5 Hours	5 Hours	Star Joint (Internet service provider)	Other major websites affected included the Air Koryo national airline and major internal email servers.	Link
Nov 23	Belgium	Government	3 Hours	2 Hours	The European Parliament Website	the European Parliament on Wednesday in a DDoS attack that came just hours after the legislative body declared Russia a terrorist state	Link
Nov 30	Vatican City	Government	5 Days	48 Hours	The Vatican City website	The cyberattack comes days after the Pope was criticized by the Russian government for comments, he made about its soldiers fighting in the war in Ukraine.	Link