MAZEBOLT

October 2022

DDoS Attack Round Up

The Major Attack Trends of October

As experts reported more than 6 million DDoS attacks in H1 this year, the gaming and governments continue to be targeted, reaching as far as Britain and the United States.

The attacks in both industries continue the current trend of politically motivated attacks from Killnet and other pro-Russian groups.

SYN Flood Attacks US Airports

Attacks hit 14 US airport websites this month, including Los Angeles International, Hartsfield-Jackson International Airport, Chicago O'Hare International Airport, and other smaller airports in Mississippi, Hawaii, Kentucky, Florida, and Arizona. Pro-Russian group Killnet claimed responsibility for the attacks later that day, reporting all airport domains hit on Telegram. The group has gained increased attention after repeated attacks on countries supporting NATO since the Russian invasion of Ukraine.

This is the second attack on US airports by Killnet, after attacks on Bradley International Airport in July. Experts believe the attack is a SYN flood attack – where requests are sent faster than can be processed and force the website offline.

Websites of Government and Defense Shut Down Around the World

United States

Killnet has also claimed responsibility for attacks on state government websites in the United States, making them inaccessible to users. While the attacks took out the websites of Connecticut, Kentucky, and Mississippi for only a few hours, the Colorado state government website was still unavailable a day after the attack. The Kentucky Board of Elections website was also shut down briefly.

Britain

Not to be outdone, pro-Russian group Anonymous led a successful attack on Britain's domestic spy service, the MI5. Also known as the Security Service, it is a counter-intelligence and security agency responsible for defending Britain's citizens against terrorists or other violent threats.

Bulgaria

Bulgaria's Ministry of Justice, Internal Affairs, and Justice Department websites were hit by a DDoS attack found to have originated from the Russian city of Magnitogorsk. It is not known whether the attack is by a malicious threat actor or a politically-motivated group such as Killnet.

Finland

Online newspaper Yle Arrena had to restrict its availability only to users in Finland and Sweden after a DDoS attack. It was able to restore its website quickly later that afternoon. Investigation of the attack is ongoing.

Israel

The website of the Israeli parliament was targeted. Although the attack was mitigated and the website was restored quickly, experts warn of additional attacks or a sign of possible interference in the elections on November 1st.

Blizzard Entertainment Suffers its Third and Fourth DDoS Attack This Year

Blizzard Entertainment once again made headlines for its second DDoS attack this month. The entertainment company that hosts Overwatch 2, World of Warcraft, Call of Duty, Battle.net, and Diablo II on its servers was also hit by DDoS attacks in both May and September.

Date of attack	Country	Vertical	Duration of Attack	Downtime	Companies affected	Comments	Press
Oct 1	UK	Government		2 Hours	Britain's MI5 domestic spy service		Link
Oct 4	USA	Gaming		6 Hours	Blizzard Entertainment		Link
Oct 5	USA	Gaming		1-2 Hours	Blizzard Entertainment	We're steadily making progress on server issues and stability, as well as working through a second DDoS attack. We're all hands on deck and will continue to work throughout the night. Thank you for your patience - we'll share more info as it becomes available	Link
Oct 6	USA	Government	72 Hours	0.5-3 Hours	US State Government Websites : Colorado, Connecticut, Kentucky and Mississippi		Link
Oct 10	USA	Aviation		1-4 Hours	Los Angeles International Airport (LAX) and Hartsfield-Jackson Atlanta International Airport (ATL). Phoenix Sky Harbor International Airport (PHX), Orlando International Airport (MCO), Denver International Airport (DIA)		Link

Date of attack	Country	Vertical	Duration of Attack	Downtime	Companies affected	Comments	Press
Oct 15	Bulgaria	Government	48 Hours	1-4 Hours	Websites of the Bulgarian President, the National Revenue Agency, and the ministries of internal affairs, defense, and justice		Link
Oct 21	Finland	Media	48 Hours	2-4 Hours	Yle Areena, the daily Kauppalehti , the online newspaper Uusi Suomi		Link
Oct 23	Israel	Government			Knesset (Parliament)		Link
Oct 24	Indonesia	Media	2 Hours	2 Hours	Konde.co (Independent media outlet)	This is the second attack experienced by Konde.co after publishing an article on sexual violence.	Link
Oct 27	Poland	Government	3 Hours	0.5 - 1 Hour	Polish Senate website	A distributed denial-of-service attack with connections to Russia briefly disabled the Polish Senate website	Link
Oct 27	Slovakia	Government	3 Hours	0.5 - 1 Hour	Slovakian Parliament IT Systems	the speaker of Slovakia's Parliament postponed voting after announcing that internal IT systems were not working	Link