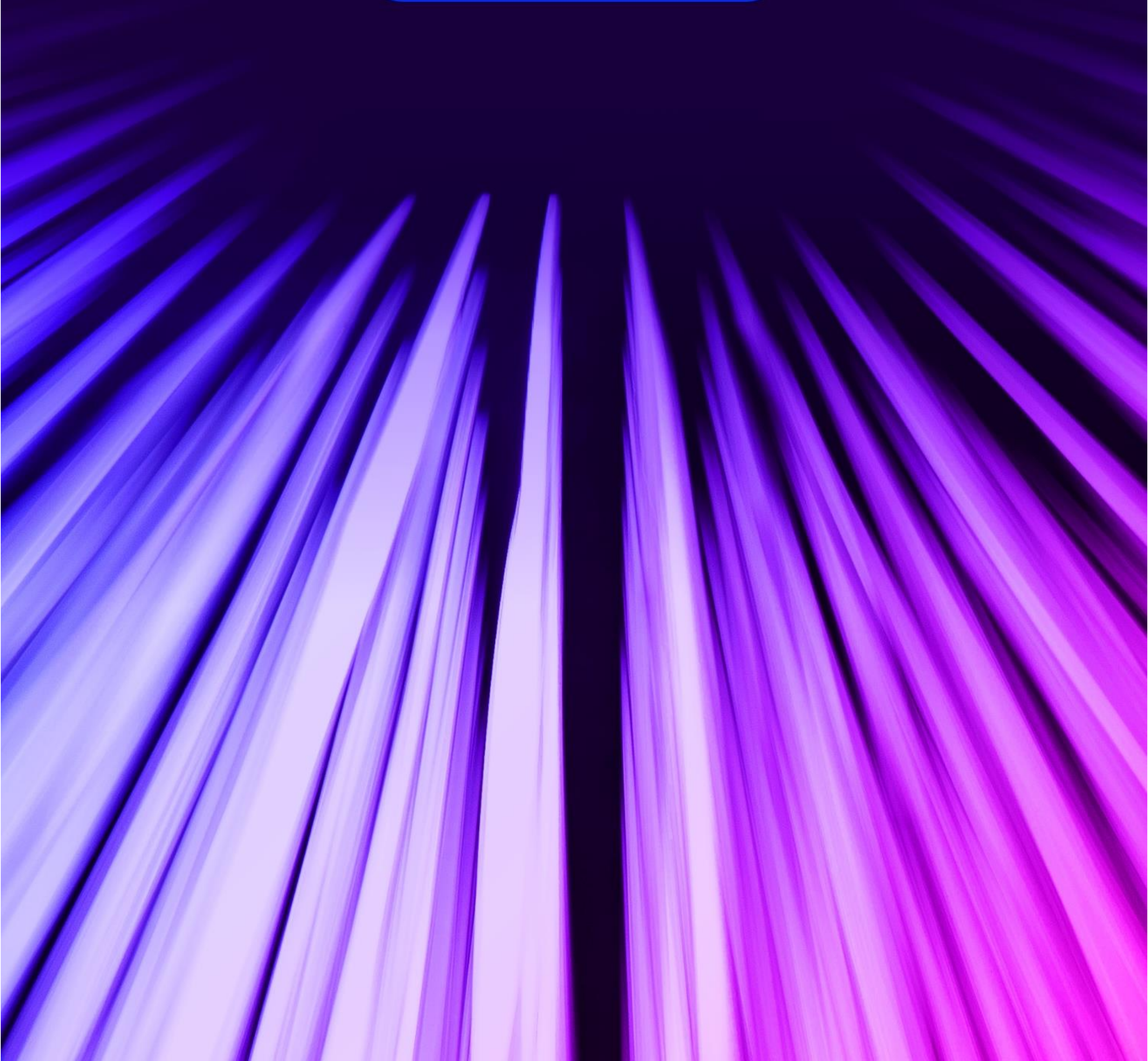
MAZEBOLT

DDoS Attack Round-up

JULY 2023 REPORT



Kenya is Under Fire

In July, there were several high-profile multi-target DDoS attacks, including one on Lithuania following NATO's event in Vilnius, and another on twelve Norwegian government ministries. Additionally, the gaming industry faced DDoS attacks with notable targets such as Sandbox Interactive and Neopets, a popular children's game in the US. However, the most vicious and dramatic attack of the month was the ongoing DDoS attack on Kenya, launched by none other than Anonymous Sudan.

The Kenyan government has been combating the massive DDoS attack campaign that has disrupted services on several crucial government online platforms for over a week. While several other organizations were also hit by the same attack, the major victim was the eCitizen portal, which provides access to over 5,000 government services for the public, and with it - countless citizens.

eCitizen provides crucial governmental services to the average Kenyan citizen: passport applications and renewals, e-visas for foreigners, driving licenses, identification cards, and national health records, among many others. In addition to the eCitizen portal, several leading media websites (including The Standard Group, and Kenya News Agency) were attacked, as well as ten university websites, seven hospitals, and Kenya’s transport agency’s website.

The DDoS attack also disrupted train-booking systems, utility payments, and mobile-money banking services, which the Kenyan government has been encouraging citizens to use. As a result, nearly 76% of the population in Kenya relies on these services, respectively.

This widespread DDoS attacks campaign still wages on, and at the time this report is written, there is no end in sight. This is one of the largest DDoS attack campaigns in recent times, effectively crippling the entire country. It is so broad that calculating the estimated overall financial damages is nearly impossible at this point.

Anonymous Sudan claims to be a group of hacktivists operating out of Sudan but is actually thought to be a Russian gang in disguise, with close ties to KillNet, and no actual relations to the global Anonymous movement. Since its inception, there has been speculation about the origins, ideologies, and motivations of Anonymous Sudan. Until last week, despite its name, it was suspected that the group had no connections to Sudan. But this latest attack raises some questions.

Read our full research about Anonymous Sudan's origins here.

Kenya is a known supporter of the People's Liberation Movement in what was then southern Sudan. The country hosted refugees and is suspected of supplying weapons and military equipment to South Sudanese rebels during the 1st Sudanese civil war. Sudan and Kenya have been part of the talks aimed at ending the civil war in South Sudan, and it is safe to say that the relationship between both countries is complex - but that doesn't seem to mind Anonymous Sudan, who decided to bring Kenya down to its knees, claiming Kenya in interfering with Sudanese internal affairs.

Whether this attack campaign is actually related to Sudan’s political ideologies is still unclear, it could be just a smokescreen for the suspected pro-Russian group.

What is clear, is that just like in recent attacks, when Anonymous Sudan threatens to shut down an organization, they usually succeed. The only reason for these DDoS attacks bypassing protection layers and causing severe downtime is misconfigurations in the DDoS protections deployed. Without continuous DDoS testing, uncovering and elimination of vulnerabilities, and a streamlined remediation process - organizations and governments will continue to go down and experience damaging downtime, despite having advanced and expensive DDoS protection solutions in place.

Date of attack	Country	Vertical	Duration of Attack	Downtime	Companies Affected	Estimated Damage	Press
July 3	Russia	Infrastructure	48 Hours	6 Hours	RZD, The Russian state-owned railway company	NA	Link
July 3	India	Infrastructure	12 Hours	Ongoing	Bangladesh Railway online ticket portal	NA	Link
July 8	USA	Gaming	36 Hours	Ongoing	Sandbox Interactive	60K USD	Link
July 8	Hungary	Infrastructure	10 Hours	6 Hours	Budapest Pride's official webpage	NA	Link

Date of attack	Country	Vertical	Duration of Attack	Downtime	Companies Affected	Estimated Damage	Press
July 8	USA	Social Media	1 Hour	1 Hour	Tumblr	**NA**	Link
July 10	USA	Gaming	36 Hours	Ongoing	Sandbox Interactive	**60K USD**	Link
July 11	USA	Media	48 Hours	Ongoing	Archive of Our Own (Ao3)	**NA**	Link
July 11	Lithuania	Government	24 Hours	Ongoing	Several websites in Lithuania, including the exhibition center LITEXPO	**NA**	Link

Date of attack	Country	Vertical	Duration of Attack	Downtime	Companies Affected	Estimated Damage	Press
July 12	Norway	Government	Unknown	Unknown	12 Norway Government Ministries	**NA**	Link
July 16	USA	Finance	30 seconds	30 seconds	PayPal	**NA**	Link
July 18	New Zealand	Government	2 Hours	Ongoing	New Zealand Parliament website	**NA**	Link
July 23	Spain	Government	4 Hours	3 Hours	Ministry of the Interior + La Moncloa, INE, Renfe, the Casa Real Central Electoral Board	**NA**	Link
July 26	USA	Gaming	8 Hours	Ongoing	Neopets	**NA**	Link

Date of attack	Country	Vertical	Duration of Attack	Downtime	Companies Affected	Estimated Damage	Press
July 27	Kenya	Government	1.5 weeks	Still ongoing for several days	Media websites including The Standard Group and Kenya News Agency, 10 university websites, including the University of Nairobi, seven hospitals and Kenya's transport agency's website, KPLC token systems, M-Pesa to bank services, and government services offered on the **e-citizen**	**NA**	Link
July 29	Spain	Telecom	6 Hours	5 Hours	Telefónica and Orange	**4.6MM USD**	Link
July 30	Israel	Infrastructure	24 hours	4 Hours	BAZAN Group - oil refinery operator	**NA**	Link