Press Release

Arelion DDoS Threat Landscape Report Identifies Europe as the DDoS Battlefield in 2022

Peak attack traffic is still rising and is up 19% from 2021.

Stockholm, 18 May 2023 – Arelion has today announced the findings of a new DDoS Threat Landscape Report, with a unique perspective on key global DDoS trends observed in 2022 from traffic data on its #1 ranked Internet backbone, AS1299. The report investigates the overall impact of DDoS attacks, the evolution of specific attacks vectors and the significance of major social and geopolitical events. The findings reveal that Europe saw the greatest concentration of DDoS activity in 2022, most likely a consequence of the war in Ukraine.

As with previous years, DDoS attacks appear to reflect major geo-political challenges and social tensions and have become an increasingly significant part in the hybrid warfare arsenal. As the Ukrainian authorities sought a safe harbor for digital state registries and databases, Arelion saw the distribution of attacks move away from active conflict areas into global cloud centers - both as a result of damage to local network infrastructure, but also as local databases and applications were strategically migrated into the cloud. Conversely, in the rest of the world, Arelion observed lower Asia-US DDoS activity and fewer DDoS attacks to and from South America in 2022.

Attack distribution and intensity

In 2022, peak attack traffic in Mega Packets Per Second (Mpps) was up 19% from 2021. This trend reflects overall Internet traffic growth but is also due to a continuing shift towards fewer, but more spectacular attacks.

Whilst there has been an increase in the number of large attacks (both in terms of bits and packets), the report reveals the vast majority of attacks are still small and mostly driven by free tier stress test or DDoS-as-a-Service attacks instigated by amateur cybercriminals. Arelion saw the biggest increase in the 5-20 & 20-50 Gbps attack ranges – mainly through DNS and NTP attacks, but also memcache due to the method’s high amplification factor.

In part thanks to the industry wide anti-spoofing initiative, *the DDoS Traceback Working Group,* the number of DDoS attacks on Arelion’s global backbone decreased by over 30% in 2022 - with 50% fewer attacks directed towards customers.

Commenting on the discoveries of the report, Mattias Fridström, Chief Evangelist at Arelion said:

“These findings reinforce the need for a basic level of customer protection to mitigate the abundant smaller attacks, together with a solid insurance policy for the larger ones. Thankfully we are seeing a power-shift in the DDoS arms race: there is now a more decisive response by network and IT infrastructure owners to cyber threats, and they are gradually starting to fight back with better cooperation and by closing the inherent weak spots in the network that cybercriminals have exploited for so long.”

The full report can be downloaded here.

About Arelion
Arelion solves global connectivity challenges for multinational enterprises whose businesses rely on digital infrastructure. On top of the world’s #1 ranked IP backbone and a unique ecosystem of cloud and network service providers, we provide an award-winning customer experience to customers in more than 125 countries worldwide. Our global Internet services connect more than 700 cloud, security and content providers with low latency. For further resilience, our private Cloud Connect service connects directly to Amazon Web Services, Microsoft Azure, Google Cloud, IBM Cloud and Oracle Cloud across North America, Europe and Asia.

Discover more at Arelion.com, and follow us on LinkedIn and Twitter.

Media contacts for Arelion:
Jeannette Bitz, Engage PR
+1 510 295 4972
jbitz@engagepr.com

UK
Lorena Duke, Ascendant Communications
+44 (0) 20 8334 8041
arelionpr@ascendcomms.net

Arelion
Martin Sjögren, Senior Manager PR and Analyst Relations
+46 (0)707 770 522
martin.sjogren@arelion.com