Press Release

Arelion DDoS Threat Landscape report reveals cyber warfare mirroring trends in ground war

Peak traffic is still increasing and is up 18% from 2022

Stockholm, April 25 2024 – Arelion has today announced the findings of its latest DDoS threat landscape report with a unique perspective on key global DDoS trends observed in 2023 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 in a cyberattack context. The findings reveal that cyber warfare is now an established part of nation state conflict and is not limited to just governmental assets. The ground war in Ukraine reflects attack trends in countries such as Russia and Ukraine – and neighbouring countries like Poland.

Global conflicts and their impact on cyber-attacks

As in 2022, heightened geopolitical tensions continue to manifest themselves in the digital ecosystem as hotspots of DDoS activity. Globally, there has been an increase in HTTP application-layer attacks. Prominent DDoS attacks have included those by pro-Russian groups like REvil, Killnet, and Anonymous Sudan, with some high-profile attacks against websites in Europe and the US.

Average bps has been continuously increasing since the conflict started in February 2022. It is clear that DDoS is a significant weapon in the hybrid warfare arsenal – there is a direct correlation between DDoS activity during November-December 2023 and the intensity of the ground war.

During late 2023 and the beginning of 2024, Arelion observed a significant increase in DDoS attacks towards Poland. The average attack strength (Gbps) rose nearly fivefold over the year, and the actual number of attacks skyrocketed. Most of these attacks used the DNS amplification vector and targeted data communications service providers and network infrastructure. This development is closely tied to the conflict in Ukraine, and various hacking groups have singled out Poland as a target.

Attack distribution and intensity

The largest volumetric attack in 2023 peaked at 960 Gbps (up 18% from 2022). This came from a UDP-based attack in Europe. At 343 Mpps, the largest pps attack came from a multi-vector TCP SYN, SSDP Amplification attack in North America.

Year-on-year, attack strength (in terms of both Gbps and Mpps) is increasing. This is predominantly driven by DNS amplification attacks. Average attack duration fell from a consistent level towards the end of 2023 – largely as a consequence of the increase in DNS amplification.

These results demonstrate the continued importance of volumetric protection. Attacks of this size are enough to bring down many larger networks, let alone on-prem devices and the networks they are attached to.

Attack types

Following steady growth over the past four years, DNS Amplification was the most common type of attack in 2023, and by the end of the year, it constituted 80% of all attacks.

The most common attack vector in 2023 was UDP over HTTP (port 80) and HTTPS (port 443). The increasing popularity of the QUIC protocol makes it an easy target for amplification attacks, posing a greater challenge to defend against than attacks using TCP as the data transport layer. Towards the end of the year, a new type of DDoS attack based on HTTP/2 was widely used to bring down web sites – in particular, within the banking and government sectors in Sweden and other countries. This type of attack presents challenges for networks everywhere because mitigation is less straightforward.

Attackers are now mainly exploiting compromised or acquired virtual machines (VMs) and virtual private servers (VPS). Unlike compromised IoT device botnets, virtual servers offer more bandwidth and computational resources. Additionally, there is a rising trend in bulletproof hosting over the past two years.

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

“While the findings of this year’s report have also revealed that there is an overall decline in packets-per-second and that attack duration is down, it shows that hackers are increasingly working smarter, not harder.” He explains, “Larger, more intensive attacks over slightly shorter periods ultimately cause the same damage overall and, with improved DNS amplification, fewer packets-per-second are needed for an effective attack, which is one less thing that could trip the existing defenses of an organization."

“As such, 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 is as great as ever. Arelion, with its key role in the global Internet community, continues to work on this kind of ‘passive DDoS protection’ – an important tool in the war of attrition against malicious DDoS traffic.”

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

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