EMEA faces surge of DDoS attacks in H1 2023

By Lindsey Schutters

29 Oct 2023

A new report from Netscout, a network security and visibility solutions provider, reveals that the EMEA region experienced a significant increase in distributed denial-of-service (DDoS) attacks in the first six months of 2023. The report shows that EMEA was the most targeted region globally, with attackers launching the largest and fastest DDoS attacks against countries in the region.

Richard Hummel, the company's threat intelligence lead, commented on the findings and offered some advice for organisations in EMEA to protect themselves from DDoS attacks.

"During the first half of 2023, threat actors inundated EMEA with DDoS attacks. There was a substantial increase in attack activity in the region, with cybercriminals launching both the largest and fastest attacks we observed in this period against countries in EMEA."

SMBs grapple with staying ahead of cybersecurity challenges, new research reveals

13 Oct 2023

The report notes that a barrage of DDoS attacks hammered the satellite communications industry, resulting in an 87% increase in attacks against this industry in EMEA. Attack frequency rose from 71 in the back half of 2022 to 61,821 in half one 2023

"EMEA-based businesses have already displayed their capabilities when it comes to blocking DDoS attacks. This can be seen with organisations in the region blocking 37% t of HTTP/S application-layer attacks. In contrast to this, APAC only mitigated 1% of HTTP/S attacks," explained Hummel.

Implement a robust strategy

However, he warned that EMEA organisations should not be complacent and should implement a robust and effective cybersecurity strategy that can cope with DDoS attacks.

"Nevertheless, as the most targeted region globally, it is imperative for all organisations in EMEA to implement a powerful and effective cybersecurity strategy which is capable of mitigating DDoS attacks. This includes placing adaptive DDoS defences at every network edge to supress attacks."

Threat actors launched approximately 7.9 million DDoS attacks globally in half one of 2023, compared to just over 6 million of these attacks during in the same 2022 period. This represents a 31% increase year over year and 44,000 DDoS attacks per day.

This increase in attack frequency was also evident in Europe, the Middle East, and Africa (EMEA), with the region experiencing more than 2.4 million DDoS attacks – a 15% increase from the second half of 2022.

The basics of good cyber hygiene

Hummel also stressed the importance of regular testing and training for online infrastructure and employees. "It's also vital for businesses to regularly test their online infrastructure. This ensures any adjustments made to applications or servers are incorporated into the wider DDoS mitigation system, protecting vital online infrastructural components."

“Teaching employees about the basics of good cyber hygiene further strengthens institutions when it comes to defending themselves from emerging threats," he said.

"With the threat posed by DDoS attacks continuing to grow, implementing these measures will ensure organisations in EMEA, and across the rest of the world, are adequately protected from DDoS attacks."

According to the report the top five targeted countries in the region were France, Germany, Italy, Kenya, and Saudi Arabia.

ABOUT LINDSEY SCHUTTERS

Lindsey is the editor for ICT, Construction&Engineering and Energy&Mining at Bizcommunity
- #Computex2024: AMD and Qualcomm ignite the AI revolution at Intel's expense - 3 Jun 2024
- DCDT overhauls radio frequency spectrum policy - 31 May 2024
- Vodacom goes to war against spectrum pooling - 30 May 2024
- Icasa extends deadline for digital migration regulations review - 27 May 2024
- HPE takes aim at Cisco, emphasises partner ecosystem and AI focus - 24 May 2024

View my profile and articles...