Key insights of the report

Akamai researchers observed that the number of DDoS attack events in EMEA has been continuously rising, with higher peaks, since the beginning of 2019.

More than one-third of all DDoS attack events globally are in the EMEA region.

The complexity and severity of DDoS attacks in the EMEA region have been transformed by geopolitical motives, such as hacktivism, with the potential for life-threatening consequences.

Of all the DDoS attack types, the DNS DDoS are among the most prevalent, according to Akamai research. Specifically, we observed the NXDOMAIN (nonexistent domain) vector, also known as the Pseudo-Random Subdomain vector, flooding DNS nameservers with requests for nonexistent domains.

More than one-third of DDoS events used multiple attack vectors — as many as 12 — to increase success.

In EMEA, the vertical with the highest number of Layer 3 and Layer 4 attacks is financial services; for Layer 7 attacks, it's commerce.

EMEA governments and nations have been rethinking the power of infosecurity by enacting new legislative measures, such as NIS2 and DORA, to help positively influence IT and cybersecurity strategies, including better resilience and protection against DDoS.