Top 5 insights

1. Web application and API attacks in the financial services industry grew by 65% when comparing Q2 2022 with Q2 2023, accounting for 9 billion attacks in 18 months. This was driven in part by cybercriminal groups' active pursuit of zero-day and one-day vulnerabilities as pathways for initial intrusion.

2. Financial services continues to see a rise in Layer 3 and Layer 4 DDoS attacks and has surpassed gaming as the top vertical. This increase appears to be caused by the dramatic surge in the power of virtual machine botnets and pro-Russian hacktivism motivated by the Russia–Ukraine conflict.

3. The Europe, Middle East, and Africa (EMEA) region accounts for 63.52% of Layer 3 and Layer 4 DDoS events, continuing the "regional shift" trend observed last year. The number of attacks against this region was nearly double the number of the next top region. We surmise this is due to the attacker groups' financial and political motivations against European banks. Additionally, this shows how easily adversaries can quickly switch their attention.

4. While the financial services industry has fewer third-party scripts than other industries (30%), it is prone to attacks like web skimming. However, financial services organizations are proactively fighting back with the adoption of solutions to comply with the new requirements of the Payment Card Industry Data Security Standard (PCI DSS) v4.0.

5. The ascending number of malicious bot requests (1.1 trillion), which spiked by 69%, exemplifies the continued assaults against financial services customers and their data via attacks like account takeovers and risks posed by financial aggregators.