State of the Internet

The High Stakes of Innovation

Attack Trends in Financial Services

In an era characterized by unprecedented digital transformation, the financial services industry stands at the crossroads of innovation and risk. As technology reshapes the landscape of financial transactions, it simultaneously ushers in a new era of threats that target the heart of economic stability.

Attacks against financial services and its customers

9 billion

Number of web application and API attacks against financial services

Number 1

Financial services is the vertical with the most DDoS attacks, even surpassing the gaming industry

50.6%

Financial services has the highest number of phishing attack victims in Q2 2023

1 trillion+

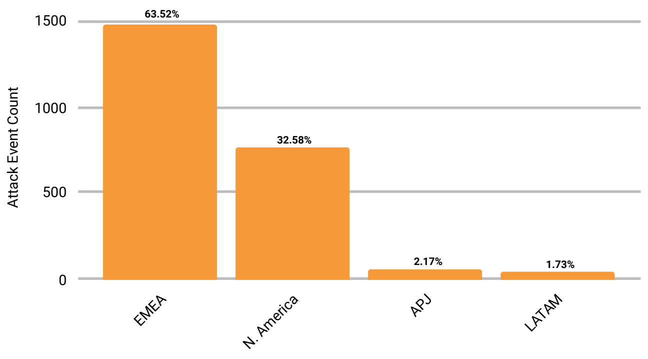
Number of malicious bot requests

Regional snapshots

The number of Layer 3 and Layer 4 DDoS attacks in Europe, the Middle East, and Africa (EMEA) is nearly double that of North America

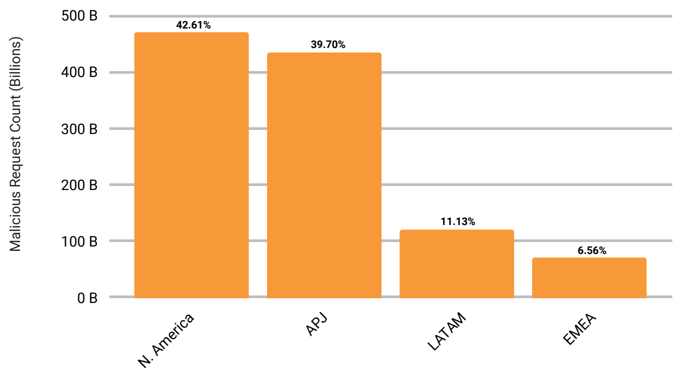
DDoS Attack Events by Regions: Financial Services

January 1, 2022 — June 30, 2023



Malicious Bot Requests by Region: Financial Services

January 1, 2022 — June 30, 2023



Asia-Pacific and Japan (APJ) is the second-most targeted region for malicious bot requests

Potential security risks to watch out for

Shadow APIs

Undocumented and untracked APIs can pose monitoring issues for companies that are not aware of who is using these APIs and in what manner.

Third-party scripts

Attackers can exploit client-side vulnerabilities or inject malicious code into third-party scripts that are loaded as part of the website. This puts financial services at risk of web skimming, which can lead to customers' data being stolen or used in unauthorized transactions.

Financial aggregators

The security gaps between financial aggregators and how data is collected can potentially create a new exploitation avenue for attackers, leading to identity theft.

Security recommendations and best practices

- Understand your attack surface to devise mitigation strategies and establish security controls
- Deploy API security tools for detecting and monitoring rogue APIs
- Use OWASP API Security Top 10 and MITRE ATT&CK framework to develop training and test plans for your red team/pen test groups
- Use a multilayered defense strategy, which includes running regular security audits and implementing advanced detection and mitigation
- Employ solutions like Client-Side Protection & Compliance (formerly Page Integrity Manager) that can mitigate the risks posed by client-side attacks
- Build an edge-based governance model to provide visibility into bot/API traffic
- Conduct a live exercise if you have not had a DDoS attack in the last three quarters; validate your playbooks and track trends for both size and speed to evaluate your risk based on current capabilities

For more information and insights about attack trends in the financial services industry, read our full report.

Download report

| Support | Published 10/23