New Fastly Threat Research Reveals 91% of Cyberattacks Targeted Multiple Organizations Using Mass Scanning to Uncover and Exploit Vulnerabilities

August 20, 2024

Additional findings show unwanted bots, short-lived IP addresses and out-of-band domains used by adversaries to commit cybercrime and avoid detection

SAN FRANCISCO--(BUSINESS WIRE)-- Fastly, Inc. (NYSE: FSLY), a leader in global edge cloud platforms, today released the " Fastly Threat Insights Report ," which found 91% of cyberattacks – up from 69% in 2023 – targeted multiple customers using mass scanning techniques to uncover and exploit software vulnerabilities, revealing an alarming trend in attacks spreading across a broader target base. This new report provides the latest attack trends and techniques across the web application and API security landscape.

The Fastly Threat Insights Report builds on the 2023 " Fastly Network Effect Threat Report ," and is based on data collected April 11 to June 30, 2024 from Fastly's Network Learning Exchange (NLX), the collective threat intelligence feed for Fastly's Next-Gen WAF , and Out-of-Band (OOB) Domains as well as traffic signaled by Fastly Bot Management from April 1 to June 30, 2024. Fastly's Next-Gen WAF protects over 90,000 apps and APIs [1] and inspects ~5.5 trillion requests per month [2] across some of the world's largest e-commerce, streaming, media and entertainment, financial services, and technology companies.

Among the report's key findings:

- **Adversaries performing mass scanning:** 91% of attacks originating from NLX sources targeted multiple customers; 19% targeted over 100 different customers. This is a significant increase from Q2 2023 insights, where 69% of NLX sources targeted multiple customers.
- **Bots comprise more than one-third of Internet traffic** : A significant amount of global internet traffic is attributed to requests generated by automation tools; approximately 36% of traffic originated from bots, while the remaining 64% came from human users.
- **Dramatic increase in usage of out-of-band domains** to actively exploit three WordPress Plugin CVEs (CVE-2024-2194, CVE-2023-6961, and CVE-2023-40000). Seven out-of-band domains were used to inject malicious content, install backdoors, and track infected applications.
- **Short-lived IP addresses help attackers evade detection:** 49% of IP addresses added to NLX were listed for just one day, with the average duration being 3.5 days. Attackers use IPs for a short period to avoid detection, highlighting the importance of adaptive security controls that can mitigate varied threats.
- **High Tech remains top industry targeted,** accounting for 37% of attacks, although slightly down from last year at 46%. Other top industries for 2024 include Media & Entertainment (21%) and Financial Services (17%).

"By performing mass scanning, attackers increase the likelihood of discovering vulnerable systems. The more targets scanned, the higher the probability of finding at least one exploitable weakness," said Fastly Staff Security Researcher Simran Khalsa. "It's not enough to respond to attacks. We must anticipate them, continuously adapt, and stay one step ahead. Based on trillions of requests across our global customer base, this new report provides an overview of the current threat landscape and actionable insights for security teams to help protect their valuable assets."

To read the complete report, visit https://learn.fastly.com/security-threat-insights-report .

About Fastly, Inc.

Fastly's powerful and programmable edge cloud platform helps the world's top brands deliver online experiences that are fast, safe, and engaging through edge compute, delivery, security, and observability offerings that improve site performance, enhance security, and empower innovation at global scale. Compared to other providers, Fastly's powerful, high-performance, and modern platform architecture empowers developers to deliver secure websites and apps with rapid time-to-market and demonstrated, industry-leading cost savings. Organizations around the world trust Fastly to help them upgrade the internet experience, including Reddit, Neiman Marcus, Universal Music Group, and SeatGeek. Learn more about Fastly at https://www.fastly.com , and follow us @fastly .

---

[1] As of March 2022.

[2] Trailing 6-month average as of August 1, 2024.

Source: Fastly, Inc.

Media Contact
Spring Harris
press@fastly.com

Investor Contact
Vernon Essi, Jr.
ir@fastly.com

Source: Fastly, Inc.