Menlo Security State of Browser Security Report Finds 130% Increase in Zero-Hour Phishing Attacks and Identified Nearly 600 Incidents of GenAI Fraud

Threat actors are increasingly using AI-powered attacks to exploit browser vulnerabilities, harvest user credentials, and employ evasion tactics to bypass traditional security defenses

MOUNTAIN VIEW, Calif., March 19, 2025 – Menlo Security, the industry leader of Secure Enterprise Browsers, today released its annual State of Browser Security Report. The report identifies several key drivers behind the sharp rise in browser-based attacks, including AI-powered attacks, phishing-as-a-service (PhaaS) and zero-day vulnerabilities. To compile the report, Menlo Threat Intelligence analyzed more than 752,000 browser-based phishing attacks and studied the trends now shaping AI-powered threats. The research reveals that a surge in generative AI-based threats has spurred a **140% increase in browser-based phishing attacks** compared to 2023, and a **130% increase specifically in zero-hour phishing attacks**.

Microsoft, Facebook, and Netflix were the brands most commonly impersonated in browser-based phishing attempts. Generative AI services are also increasingly impersonated – **in 2024, Menlo Security identified nearly 600 incidents of GenAI fraud,** in which imposter sites used GenAI platform names to manipulate and exploit unsuspecting victims.

"Interestingly, the majority of GenAI fraud was not for the purpose of credential theft," said Andrew Harding, VP of Security Strategy at Menlo Security. "Instead, these impersonation sites attempted to trick people into entering highly personal information. These fake GenAI platforms promise to generate a résumé or similarly personal document. In addition to cybercriminals stealing sensitive and personal information, the returned document is typically a PDF, where malware can hide out and be delivered. In the past year, Menlo Security successfully thwarted hundreds of incidents of such GenAI fraud."

Web browsers are the most widely used application for both work and personal activities. This widespread use and frequent vulnerabilities has enabled threat actors to evolve their tactics, shifting their focus towards sophisticated browser-based attacks. These attacks utilize subtle and powerful tactics that bypass traditional endpoint security defenses and network security controls.

Common attack vectors include malicious ads positioned on popular websites to distribute malware and steal credentials. Browser-based phishing attacks are prevalent, especially those leveraging Legacy Reputation URL Evasion (LURE) techniques, which evade web filters that attempt to categorize domains based on implied trust. Attacks through business collaboration tools like Slack or Microsoft Teams often involve brand impersonation techniques, and exploitation of browser vulnerabilities in major browsers like Chrome, Firefox and Edge remains a threat. The full report details real-world examples of each type of attack.

Key findings from the State of Browser Security Report include:

- Cybercriminals created nearly 1M new phishing sites each month, which represents a 700% increase since 2020
- Nearly 51% of browser-based phishing attempts involved some form of brand impersonation

- 75% of phishing links are hosted on good, trusted websites, with up to six days as the average window of exposure before legacy security tools begin blocking pages from zero-hour phishing attacks
- Phishing attacks hosted on subdomain providers increased by 51%, representing 24% of all phishing attacks
- Four of the top five hosting providers used by bad actors to host phishing attacks were based in the U.S., potentially reflecting the country's economic and political significance, increased digital transformation and remote work, and the growing reliance on U.S.-based cloud services and SaaS platforms housing critical data and financial information.
- Instances of attackers exploiting cloud services to host malicious content including phishing sites and ransomware is on the rise. AWS and CloudFlare accounted for nearly 50% of all instances of abused cloud hosting instances in 2024.

“Threat actors have advanced in speed and skills. They are using the same tools and infrastructure as professional engineers,” continued Harding. “We’re seeing a dangerous combination of zero-day attacks, advanced social engineering techniques, sophisticated phishing techniques, and readily-available phishing-as-a-service kits, all designed to infiltrate systems and steal valuable data. Our research has revealed a stark reality: **One in five attacks in 2024 displayed some form of evasive technique designed to evade traditional network and endpoint-based security controls**. This trend is only poised to escalate dramatically in 2025 as attackers adopt AI to increase both scale and effectiveness. Organizations must prioritize browser security to detect and stop such attacks.”

Download the full State of Browser Security Report to read the full research findings and analysis of major attacks and browser vulnerabilities. The report also offers five key insights from Menlo Security Threat Intelligence on how browser-based attack trends will shift in 2025, and what actions security teams can take to be prepared.

About Menlo Security

Menlo Security protects organizations from cyber threats that attack web browsers. Menlo Security’s patented Cloud-Browser Security Platform scales to provide comprehensive protection across enterprises of any size, without requiring endpoint software or impacting the end user-experience. Menlo Security is trusted by major global businesses, including Fortune 500 companies, eight of the ten largest global financial services institutions, and large governmental institutions. The company is backed by Vista Equity Partners, Neuberger Berman, General Catalyst, American Express Ventures, Ericsson Ventures, HSBC, and JPMorgan Chase. Menlo Security is headquartered in Mountain View, California. For more information, please visit www.menlosecurity.com.

Media Contact

Emily Ashley

ICR for Menlo Security

emily.ashley@icrinc.com