MENLO SECURITY

State of Browser Security:

Defending browsers against zero-hour phishing attacks

Mini-report

The time for browser security is now.

Over the past six months, the Menlo Security Threat Research team has uncovered a 198% increase in browser-based phishing attacks, with 30% classified as evasive. While the surge in browser usage has led to increased productivity and flexibility, it does not come without risk in this threat environment. That shift in threat action poses a real concern for enterprises—especially when it comes to cybersecurity.

Many organizations run browsers in their enterprise and rely on existing network-based security controls to protect against web-based threats. These zero-hour phishing attacks can evade such controls. Enterprises can no longer keep their users safe behind traditional detection-based network controls and with ongoing end-user training. Attackers recognize this opportunity and are combining evasive phishing attacks and social engineering techniques to target users through the browser and to steal user credentials.

Isn't this just the same old phish?

At their core, these attacks are an evolution of phishing–but they are not the same. They are dynamic and evasive and traditional security tools are not detecting them effectively. Zero-hour phishing attacks utilize a range of techniques together:

- Smishing,
- AiTM (Adversary In The Middle) frameworks,
- Image-based phishing,
- Brand impersonation,
- Multi-factor authentication (MFA) bypass.

What should I do now? 3 keen insights

CISOs need to retarget defenses in an environment where threats have changed their focus, because compromised user credentials are often just the first step in a cybercrime campaign that can ultimately lead to a ransomware outbreak or intellectual property theft. The Menlo Security Cloud has seen these techniques combined more frequently. These attempts to steal credentials are consistent with the recent attacks on Twilio, Caesars, and the recent breach at the software company Retool.

Undeniably, humans remain a point of exposure, the weakest link, when it comes to cybersecurity concerns. As the "pilots" of those exposed browsers, users need some help. This report contains 3 insights based on data from the Menlo Security Cloud that can help CISO and the security teams make better decisions in this changing environment.

INSIGHT ONE

Phishing attacks have evolved dramatically.

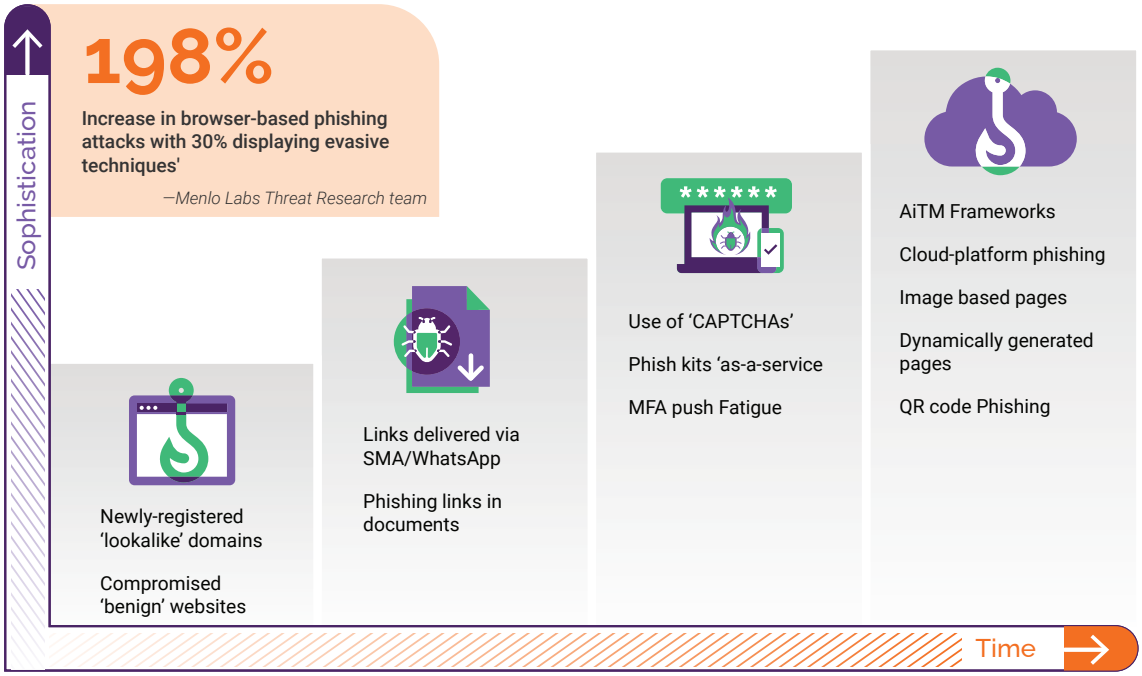

Illustration 1: Evolution of phishing

Many cyberattacks start with some form of a phishing lure in order to steal credentials, gain access to corporate applications, and force an account takeover. Phishing is the most common initial attack vector because it works. 16% of global data breaches start with phishing[1].

In addition to evasive tactics, the attacks are using automation and GenAI tools to improve their own quality and the volume of their threat action. Attackers now produce thousands of phishing attacks with unique threat signatures. And these contain fewer language errors, the tell-tale sign that enables human eyes to spot these threats if they do evade traditional controls.

[1] IBM Security. (2023). Cost of a Data Breach Report 2023. IBM. https://www.ibm.com/downloads/cas/E3G5JMBP

In a recent 30-day period, the Menlo Security Threat Research team identified:

Over 31k

browser-based phishing attacks
mounted against Menlo Customers'

Over 31,000 browser-based phishing attacks mounted against Menlo customers. These targeted enterprise attacks span across multiple industries, regions, and are used by notorious threat actors such as Lazarus, VIPER and Qakbot.[2]

The surge of browser-based attacks is not coming from known malicious or spurious fly-by-night sites. In fact, 75% of phishing links are hosted on known, categorized, or trusted websites.

75%

of phishing links are hosted on known, categorized, or trusted websites.

500

different enterprises

under attack in a single month

Phishing also seems to be spreading. Historical reporting showed that the largest enterprises were impacted, but now attacks target more organizations, with 500 different enterprises under attack in a single month.

(*The attacks indicated in this research were stopped by browser security even when they exhibited evasive techniques.)*

[2] Lazarus—https://www.menlosecurity.com/blog/lazarus-group-browser-exploit-effect
IPER—https://www.menlosecurity.com/blog/vip3r-new-actor-old-story-great-success/
Qakbot—https://www.menlosecurity.com/blog/an-anatomy-of-heat-attacks-used-by-qakbot-campaigns

These phishing attacks aren't isolated to just a specific industry or region. No matter how much education or web security tools are used, phishing continues to run rampant and impact enterprises across every vertical. To prevent the ramifications of such attacks, proactive measures and effective browser security control are essential to protect sensitive information from being stolen and monitor accounts for any signs of suspicious activity.

INSIGHT TWO

Evasive phishing threats are the new attack tool.

Until recently, cybercriminals had other means to gain entry into enterprise systems. Unpatched vulnerabilities on public facing systems have been fruitful targets. Attackers maintained a focus there, exploiting vulnerabilities in operating systems, applications, and legacy security infrastructure. But recent high-profile breaches have brought attention to that tactic, and threat action has evolved.

The web browser has become a significant target. Current security controls, which include firewalls, secure web gateways (SWGs), sandbox analysis, and URL reputation checks, cannot stop browser focused attacks. The new evasive techniques such as HTML Smuggling, AiTM, or encrypted files are quickly becoming the primary means for credential theft. To further complicate the problem, phishing has expanded beyond the traditional email or O365 paths. Attackers are focusing their phishing attacks on cloud sharing platforms or web-based applications, opening up additional pathways into organizations.

Recently, the Menlo Labs Threat Research team exposed the EvilProxy phishing campaign on 'indeed.com', which actively targeted executives in senior roles, exposing them to potential credential theft and account compromise. These hijacked victim's session cookies were used to login to the legitimate Microsoft Online site, impersonate the victims, and bypass non-phishing resistant MFA.

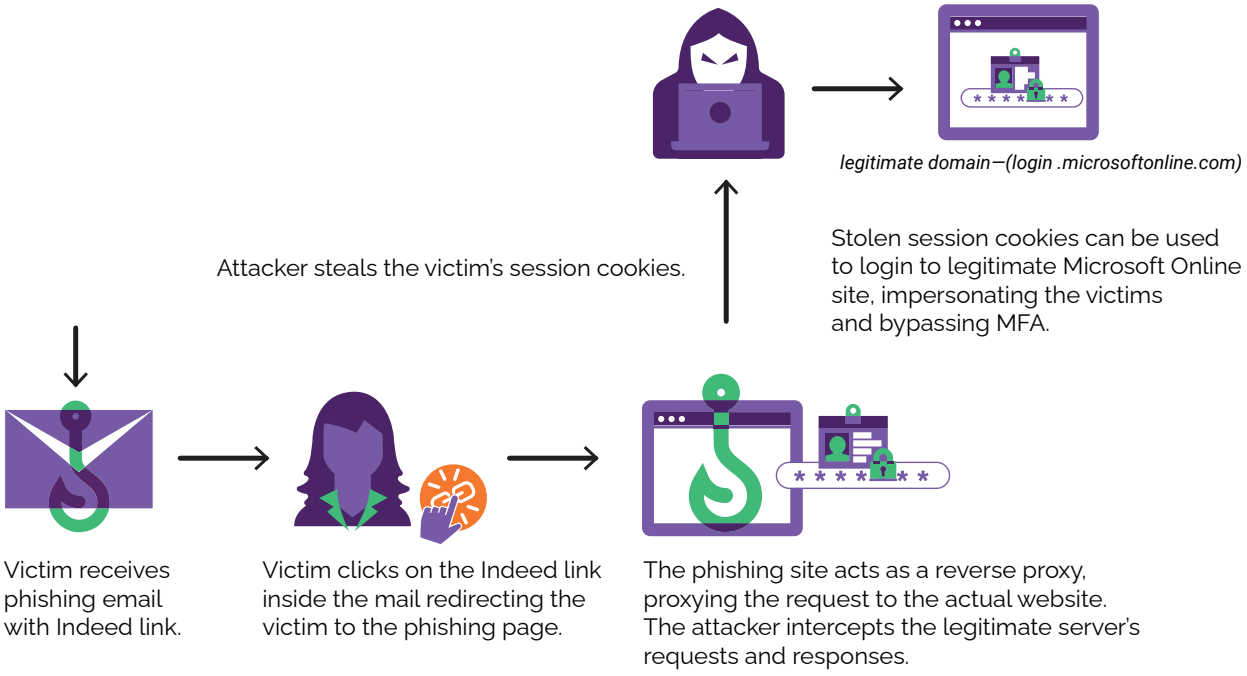

Illustration 2: MFA Bypass attack chain representation

Attackers have developed tools to craft high quality large scale attacks that target the browser. Cybercrime tools, such as phish kits (PhaaS) and ransomware-as-a-service kits (RaaS), have simplified the process of launching sophisticated attacks. These kits provide attackers with pre-made templates, scripts, and resources lowering the bar to craft and deploy their malicious campaigns. Tools like this also make it easier for rudimentary attackers to create convincing and fraudulent websites or emails for the purpose of stealing sensitive information from its intended victims.

The Menlo Labs Threat Research team observed that **30% of phshing attacks display "evasive" characteristics** and meet the definition of zero-day phishing.

The goal of these attacks has been two-fold: ransomware delivery and credential stealing.

The Menlo Labs Threat Research team detected cybercrime campaigns that pose a significant new risk to organizations because a plurality of these attacks evade traditional tools:

Over **550,000 browser-based phishing attacks** were detected during the year.

That volume represents a nearly **200% increase** during the last 6 months of 2023.

Menlo Labs has identified over **31,000 threats that employ evasive techniques**, that were designed to bypass commonly deployed security solutions and that **actively targeted browser users**.

The increase in Legacy URL Reputation Evasion (LURE) attacks has been marked. Menlo Security's Threat Research team saw a **dramatic 70% increase in Legacy Reputation URL Evasion (LURE) attacks in 2022.**

More than 73% of LURE attacks originated were seen **coming from categorized websites based on 1 million URLs analyzed** by the team.

Legacy URL Reputation Evasion (LURE) is a growing evasive phishing technique that specifically targets browsers to bypass web categorization of commonly deployed security tools like secure web gateways and URL reputation filters. Threat actors capitalize on this technique by hijacking trusted sites, or by creating a new site and leaving it dormant until its URL/domain is trusted. They then use these URLs and destination sites to launch phishing attacks. This has been a consistent trend during 2023: Phishing attack sneaking AWS phishing sites into malicious Google ad campaigns.

During such an attack, the user opens the web URL believing it to be authentic. Because the URL is in a safe category, it is neither blocked by the SWG, nor URL filters. The user is subsequently compromised, either with malware or because they are induced to enter their credentials.

The challenge for enterprise security stems from security tools still relying on classic network signals and traditional endpoint telemetry alone. These approaches fail to identify evasive threats such as LURE. Even AI models trained on network-based telemetry fall short because Firewalls and SWGs lack visibility into browser telemetry. This weakness has spurred the growth of this attack vector. Without improved visibility into browser specific telemetry, security teams will remain exposed to zero-hour phishing attacks. Leaders within enterprises reassess their approach to network, endpoint, and system security and consider whether their users are exposed to these new threat vectors and whether they can identify and prevent threats at their earliest stage.

INSIGHT THREE

Traditional tools miss browser-based attacks.

Network and endpoint security tools, in their current forms, leave enterprises exposed to zero-hour phishing threats. These attacks are specifically designed to bypass commonly deployed security tools and serve as the primary means for ransomware, data exfiltration, and cyber espionage. Similarly, traditional tools do not defend against browser vulnerabilities, unpatched browser extensions, and drive-by downloads.

During the report period, Menlo Labs Threat Research team has discovered:

- **11,000+ zero-hour phishing attacks** that exhibit no signature or digital breadcrumb, meaning no existing SWG or endpoint tool was able to detect and block these attacks.
- **That six days is the average latency** between a zero-hour phishing attack erupting and being added to the detection mechanism for traditional tools.

‘Protection Buffer’—Zero-hour Phishing

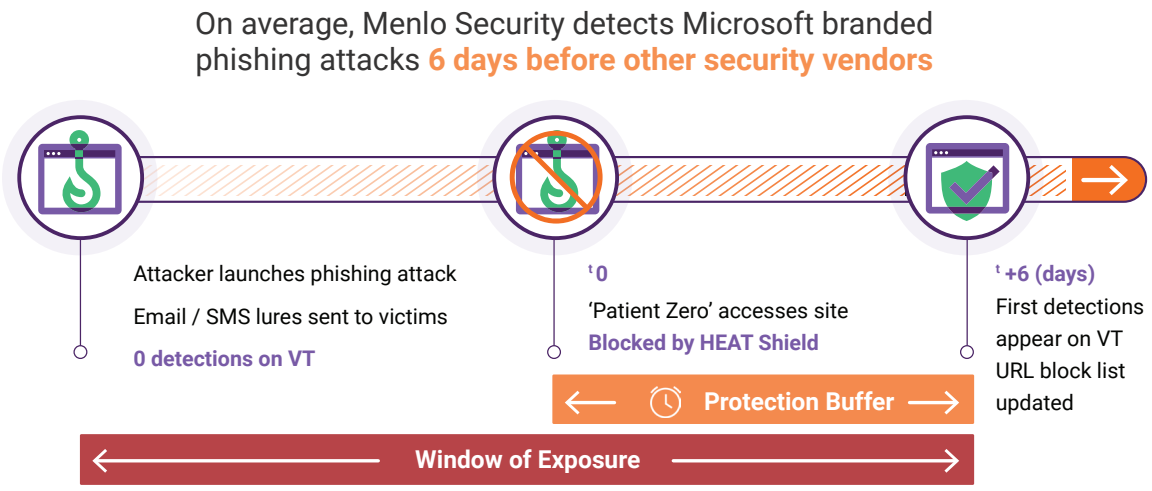

Illustration 3: Menlo Security’s Protection Buffer against zero-hour phishing attacks

While web, email, and endpoint security do offer partial protection, the browser remains critically exposed. And despite best efforts even with proper end-user education, sophisticated phishing attacks are constantly evolving and are still getting through by disguising malicious actions inside the browser as innocuous behavior. This is why they’re such potent threats.

In order to avoid detection, evasive techniques are often combined with one another in targeted attacks to avoid detection, and include tactics such as:

- Adversary-in-the-middle (AiTM)
- Open redirect chains
- QR Codes
- Hosting phishing sites on cloud development platforms
- Hosting malicious payloads on Content Delivery Networks (CDNs)

These techniques require improved browser security and can only be detected through inspection that goes beyond network signals and static HTTPS payloads. Detecting and thwarting these attacks requires live inspection of the web session, the Document Object Model and the dynamic elements that are produced from HTML, embedded media objects (such as images), JavaScript, and CSS.

Giving attention to browser security complements existing network security and endpoint technologies and closes the risk gap created by these new attacks.

CONCLUSION

Menlo Security is the Browser Security you need.

The browser is the business application enterprises can't live without, but it has fallen behind from a security and manageability perspective. Menlo Security eliminates the browser attack surface by allowing IT and security teams to properly manage their existing browsers, protect their users, and secure application access and enterprise data in order to provide a comprehensive browser security approach. Menlo's Browser Security solution is able to accurately identify and block phishing attacks 6 days ahead of any other security vendor. This 'protection buffer' significantly decreases the time between a user's first access to a malicious site and the point at which one or more vendors on VT flag it as malicious.

Menlo's Browser Security solution works across any device, and any browsing providing end-to-end visibility into every browser session and delivering real-time dynamic policy control to effectively stop evasive malware and zero-hour phishing attacks from infecting user systems and enterprise networks. Leveraging Menlo Security's AI-powered secure cloud browser can be used to identify visually similar websites impersonating known brands and services ensuring both speed and accuracy at scale, all while ensuring a seamless user experience on any browser.

To learn more about phishing and how browser security can eliminate the browser attack surface, visit menlosecurity.com or email us at ask@menlosecurity.com.

MENLO SECURITY

To find out more, contact us:

menlosecurity.com

(650) 695-0695

ask@menlosecurity.com

About Menlo Security

Menlo Security enables organizations to eliminate threats and fully protect productivity with a one-of-a-kind, isolation-powered cloud security platform. It's the only solution to deliver on the promise of cloud security—by providing the most secure Zero Trust approach to preventing malicious attacks; by making security invisible to end users while they work online; and by removing the operational burden for security teams. Now organizations can offer a safe online experience, empowering users to work without worry while they keep the business moving forward.