HEAT
SHORT STORIES

# Highly evasive threats run rampant as bad actors sidestep existing enterprise security

Threat actors are always in search of the path of least resistance for their exploits. As network security and endpoint protections have become increasingly robust, the browser has emerged as one of the most prevalent and least defended enterprise applications in use. Hackers have been quick to exploit the browser in novel and evasive techniques to create a beachhead for phishing and ransomware.

Despite continued investments in cybersecurity, threats still get through and users are impacted every day. While security awareness training has helped users to recognize the most blatant attack attempts, such an approach will never catch 100% of threats. This is why simple attacks remain so effective against commonly deployed security solutions.

An increase in browser-based work has incited a surge in related attacks and compromised devices. At least 50% of evasive threats are coming from categorized/trusted websites within the browser.

The web browser — the most deployed application in the enterprise — has the dubious distinction of being the least secured. Every enterprise user is likely to have multiple browsers across the variety of devices that they use to access the web, enterprise cloud, SaaS applications, and email. As a result, the browser has become one of the most popular targets for mounting phishing and malware attacks. Unfortunately, existing security controls, such as secure web gateways (SWGs), endpoint detection and response (EDR) solutions, and firewalls have fallen short of stopping these attacks. Attackers understand how how these common security solutions work, and have evolved their tactics to include highly evasive and adaptive threats to get around them. So, despite the increased investment enterprises are making in their security stacks, their users are more exposed than ever.

Users spend 75% of their working time in the browser to access the cloud, SaaS-based applications, and other web-based tools pivotal to productivity, efficiency, and collaboration.

Threat actors have found cracks in the armor of today's enterprise security defenses that allow a new class of potent and effective threats to sneak through. Called Highly Evasive and Adaptive Threat (HEAT) attacks, these new threats exhibit sophisticated techniques, such as dynamic behavior, fileless attacks, and delayed execution to avoid detection and evade traditional security measures. Because these threats are designed to attack the blindspots of firewalls, SWGs, and EDR solutions, they can be particularly challenging for security professionals to identify and mitigate. Highly evasive and adaptive threats specifically target the vulnerable web browser and deliver malware, compromise user systems, and steal sensitive data.

## Highly evasive threats are increasing in volume and sophistication

Enterprises have continued to build defenses against "traditional" attack vectors, deploying firewalls, SWGs, EDRs, sandbox analysis, URL reputation engines, phishing detection, and more. Because the web browser typically lacks adequate protection, IT and security teams are forced to rely on detection-based approaches, which can only identify signatures of known threats and fail to block evasive threats that specifically target the browser. The need for visibility, control, and protection from threats within the browser has become increasingly apparent. Until enterprises fully adopt browser security, threat actors will continue to use highly evasive and adaptive threats to penetrate enterprise networks as displayed by these recent attacks:

## Highly Evasive Threat Example One

***Okta Hackers hit over 130 organizations with successful multi-factor authentication (MFA) bypass technique***

The threat actor responsible for recent attacks on Twilio and Cloudflare has been linked to a larger phishing campaign targeting 136 organizations, resulting in the compromise of 9,931 accounts using MFA bypass. The attacks sought to obtain Okta identity credentials and two-factor authentication (2FA) codes from employees of targeted organizations with most victim organizations based in the U.S., India, Canada, France, Sweden, and Australia. The phishing kit used was previously undocumented. The motives behind the campaign remain unclear, but it's suspected to be for espionage and financial gain, allowing the threat actor access to confidential data, intellectual property, corporate inboxes, and funds.

## Highly Evasive Threat Example Two

***Russian nation-state threat actors continue to infiltrate the diplomatic corporations of countries in support of Ukraine***

Russian intelligence, specifically the hacker group Nobelium/APT29, has been involved in an espionage campaign targeting foreign ministries, diplomats from NATO-member states, and other entities in the European Union and Africa. This campaign coincides with attacks on Canadian infrastructure, believed to be linked to Russia as well.

Nobelium/APT29, previously known for the SolarWinds supply chain attack, initiates the attacks with well-crafted spear-phishing emails that lead to malicious sites, which employ the highly evasive technique of HTML-smuggling to avoid detection and deliver malicious payloads. Although no significant damage has been reported as of yet, Canadian authorities stress the importance of protecting critical systems and applying mitigations.

42% of malware is delivered in archives. Archives are now the most popular filetype for delivering malware as attackers bypass perimeter security controls.

## Highly Evasive Threat Example Three

***Aggressive malware campaign targets healthcare organizations to gather data and gain remote control***

An aggressive threat actor is targeting the finance and healthcare sectors using a highly evasive malware variant and SEO poisoning, a commonly known URL evasion technique classified as Legacy URL Reputation Evasion (LURE), to evade traditional security measures and manipulate search engine results.

This aggressive campaign involves multiple layers of obfuscation, privilege escalation, and data gathering. The successful infection enables the threat actor to gain and maintain remote control of the victim's device and gather sensitive information. Given the severity and ongoing nature of the attacks, organizations, especially those in the healthcare sector, are advised to be on high alert and take appropriate measures to protect their systems.

## Highly Evasive Threat Example Four

***Threat actor uses Google's open source GC2 tool for data exfiltration and account compromise targeting media giant***

The Chinese nation-state group APT41, or Barium, targeted a Taiwanese media giant leveraging Google's open source Command and Control (GC2) tool and a malicious password-protected file hosted on Google Drive using LURE evasion techniques. This targeted campaign highlights two important trends: Chinese threat groups are increasingly using publicly available tools like GC2, and attackers are using legitimate cloud services to avoid detection — links to trusted cloud services don't set off alarms.

Google emphasized that cloud services have become lucrative targets for cybercriminals and state-sponsored actors, either for hosting malware or as infrastructure for command-and-control (C2) operations. Various malware variants have been found stored on Google Drive as ZIP archive files in phishing campaigns. The continued use of cloud services as attack vectors underscores the need for robust security measures to protect accounts from credential compromises.

## Highly Evasive Threat Example Five

***New phishing-as-a-service kit simplifies Microsoft 365 phishing attacks***

The "Greatness" phishing-as-a-service (PhaaS) platform has experienced a surge in activity targeting organizations using Microsoft 365 in the United States, Canada, the U.K., Australia, and South Africa. The platform provides cybercriminals with all the tools needed to conduct successful phishing campaigns, including the necessary infrastructure, obfuscated JavaScripts, and imagery needed to successfully impersonate a Microsoft 365 page and steal user credentials as well as session cookies.

Once the attackers obtain the session cookie, they can access the victim's email, files, and data in Microsoft 365 services. Stolen credentials are often used to breach corporate networks, leading to more dangerous attacks, such as ransomware deployment.

Every minute, a new phishing site mimicking well-known brands is launched.

## How can enterprises protect themselves against highly evasive, browser-based threats?

A new breed of solution is required to stop these highly evasive threats. Existing on-premises and cloud-based network security, which rely on signatures of known threats, or AI solutions trained on network-based telemetry, fail to detect unknown phishing threats and other evasive techniques. Organizations need preventive browser security solutions that provide complete visibility into all web traffic and enable dynamic policy enforcement. Only then can IT and security teams identify and prevent highly evasive threats from targeting users.

Given the shift toward evasive threats increasingly used by threat actors today, Menlo Security has introduced a suite of prevention capabilities designed to detect and block highly evasive threats targeting the browser. HEAT Visibility performs inline analysis to provide end-to-end visibility into every browser session. This visibility helps to accelerate incident response by providing context-rich, actionable intelligence around highly evasive browser based threats — a dataset which is invisible to other solutions.

Using multiple AI-based techniques, including Computer Vision, URL risk scoring, and analysis of web page elements, Menlo Security's HEAT Shield can accurately determine in real time if a link being opened is a phishing site designed to steal users' credentials. HEAT Shield provides real-time protection for the browser, surfacing action-oriented threat intelligence on highly evasive threats and zero hour phishing attacks, delivering the information that security and IT teams need to better secure their organizations, while providing a seamless browsing experience for their end users.

MENLO
SECURITY

**To find out more, contact us:**

**menlosecurity.com**
**(650) 695-0695**
**ask@menlosecurity.com**

## About Menlo Security

Menlo Security eliminates evasive threats and protects productivity with the Menlo Secure Cloud Browser. Menlo delivers on the promise of cloud-based security—enabling Zero Trust access that is simple to deploy. The Menlo Secure Cloud Browser prevents attacks and makes cyber defenses invisible to end users while they work online, reducing the operational burden on security teams.

Menlo protects your users and secures access to applications, providing a complete enterprise browser solution. With Menlo, you can deploy browser security policies in a single click, secure SaaS and private application access, and protect enterprise data down to the last mile. Secure your digital transformation with trusted and proven cyber defenses, on any browser.

Work without worry and move business forward with Menlo Security.