

Invisible Enemies

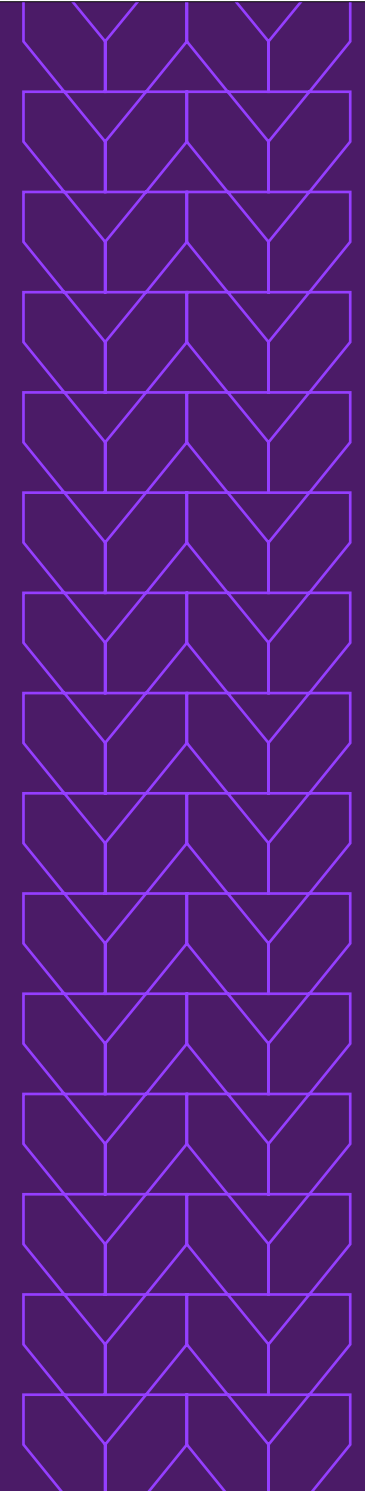
The Top Evasive Web Threats That Defy Detection

eBook



Contents

Defying detection and thriving at scale	3
Web threat #1: MFA bypass	4
MFA bypass attack in action	5
Web threat #2: HTML smuggling	6
HTML smuggling attack in action	7
Web threat #3: SEO poisoning	8
SEO poisoning attack in action	9
Web threat #4: Malicious password-protected files	10
Malicious password-protected file attack in action	11
Gain control over web-based threats	12



Defying detection and thriving at scale

Security today has a big problem — it's centered around detecting and responding to threats. But what if threats aren't detectable — then what? The answer is what attackers are zeroing in on. They know that if they can remain invisible, traditional barriers that “stop the bad stuff” won't apply, and they can carry out their attacks discreetly.

The way adversaries attack isn't the only change over the last decade. Being a threat actor is dramatically more accessible than it once was. Many of today's threats do not require advanced technical skills for cybercriminals to craft. There are tools and services that they can purchase or rent. And often, it simply boils down to understanding how to exploit the human element. If an attacker can get a human to click and provide credentials, they have the initial access to get them into your networks and remain undetected.



Browser-based threats on the rise



An increase in browser-based work and blind spots has incited a surge in browser-based attacks and compromised devices.

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.¹ However, the web browser — until now — has not been considered a significant target for cybercriminals. Adversaries are known to exploit PCs, desktops, and operating systems. And current security stacks reflect this with layers of firewalls, Secure Web Gateways, sandbox analysis, URL reputation, and phishing detection solutions.

Defense in depth has reached its limitations for protecting the new, expanded attack surface. Since the web browser is the most deployed enterprise application in every company — and not protected by network and endpoint security — security gaps have become more pronounced. Without insight, control, and protection from threats inside the browser, IT and security teams must rely on a detect-and-respond approach. However, this fails by definition because it is a reactive approach.

This ebook explores the growing trend of evasive web threats — helping you understand how adversaries carry out their attacks, why you might be susceptible, and how to protect your organization.

¹ <https://chromeenterprise.google/cloudworker/guide/>

Web threat #1: MFA bypass

What it is.

As browsers and applications became more sophisticated, organizations turned to authentication techniques. One popular choice was multi-factor authentication (MFA), considered “unhackable” since it was rolled out to consumers in the early 2000s. The reality is that nothing remains unhackable. Like other longstanding security technologies, MFA has been a puzzle for malicious actors to solve as long as it has secured users.

Phishers, scammers, and other malicious actors are financially motivated to find ways around MFA to steal valuable data. Today, we see them succeed using MFA bypass. A few ways threat actors can bypass MFA include MFA fatigue, token theft, and man-in-the-middle attacks.

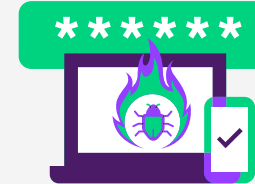
How it works.

MFA bypass is successful because of how traditional security defines malicious behavior. In the case of this attack type, nothing malicious is happening that traditional layers can detect. No one is knocking down a door. Instead, they intercept the key – in this case, the credentials and the token that the MFA provider issues – and use it to gain entry.

Not only that, but MFA bypass is difficult to prevent because of the element of surprise and speed at which victims are compromised. Even if a fraudulent sign-in page is detected and placed on the deny list, ransomware gangs can quickly spin up another domain and continue to target other individuals in the organization. No amount of deny-listing, URL filtering, or phishing training can stop the attacks in time. Plus, because MFA often uses out-of-band communications such as SMS text, the whole process is often outside the view of the security team.

What makes you susceptible to attack.

- **Lack of control:** MFA relies on users’ personal mobile devices for authentication – many unmanaged.
- **The human element:** Users are accustomed to MFA, and if attackers make enough requests, users will likely slip up and click to approve access.
- **Lack of visibility and security:** Traditional layers of security don’t recognize MFA bypass behaviors as malicious, which is necessary to detect and stop the attack.



Microsoft reported a massive phishing series against 10,000 organizations that used MFA bypass.²

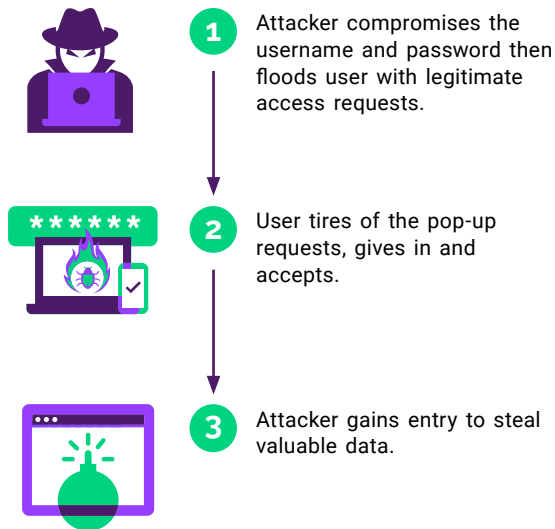
To prevent an MFA bypass attack, you must secure every click on every device, which requires analyzing the entire access journey in order to identify irregularities in the path.

² <https://www.bleepingcomputer.com/news/security/microsoft-phishing-bypassed-mfa-in-attacks-against-10-000-orgs/>

MFA bypass attack in action

Because threat actors are so creative, many MFA bypass techniques exist. We've called out three of the most common methods below.

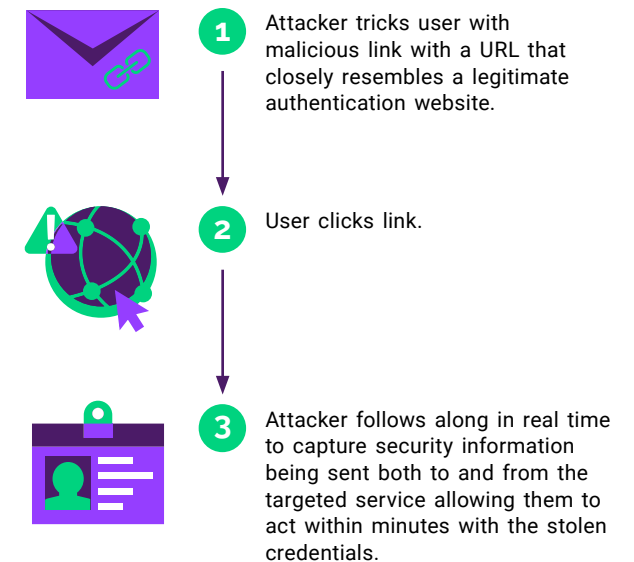
MFA Fatigue



Token Theft



Man-in-the-Middle



MFA bypass in the wild: Oktapus Ransomware

Attackers sent Okta (MFA tool) customers a text message or an email that contained a link to a fraudulent Okta authentication page. Victims were prompted to enter their username and password into a web form and asked for their 2FA code. Attackers monitored users' actions in real time, allowing them to act within minutes to use the credentials as soon as they were compromised.



Web threat #2: HTML smuggling

What it is.

HTML smuggling has gained popularity with cybercriminal groups. Nobelium, the notorious group behind the SolarWinds attack, is among those known to use the evasive technique to distribute malware.

As the name suggests, attackers “smuggle” an encoded malicious script within a specially crafted HTML attachment or webpage. Using HTML5/JavaScript features, attackers deliver file downloads typically in one of two ways:

1. Deliver the download via Data URIs on the client device.
2. Creates JavaScript blobs embedded with malicious content and masked with the appropriate MIME type that results in a dynamic file download once on the client side.

How it works.

Both techniques enable an attacker code to construct the file at the browser level and download the file to the endpoint without any user action. This technique evades file content inspection engines completely as they don't recognize this activity as a file download at all. Even if a policy dictates that all file downloads should be blocked, the drive-by-download techniques will bypass these engines and end up on the endpoint.

Because these attacks impersonate trusted, well-known brands, including Dropbox, Adobe Acrobat, and Google Drive, users are less likely to question opening the HTML in their web browser.

What makes you susceptible to attack.

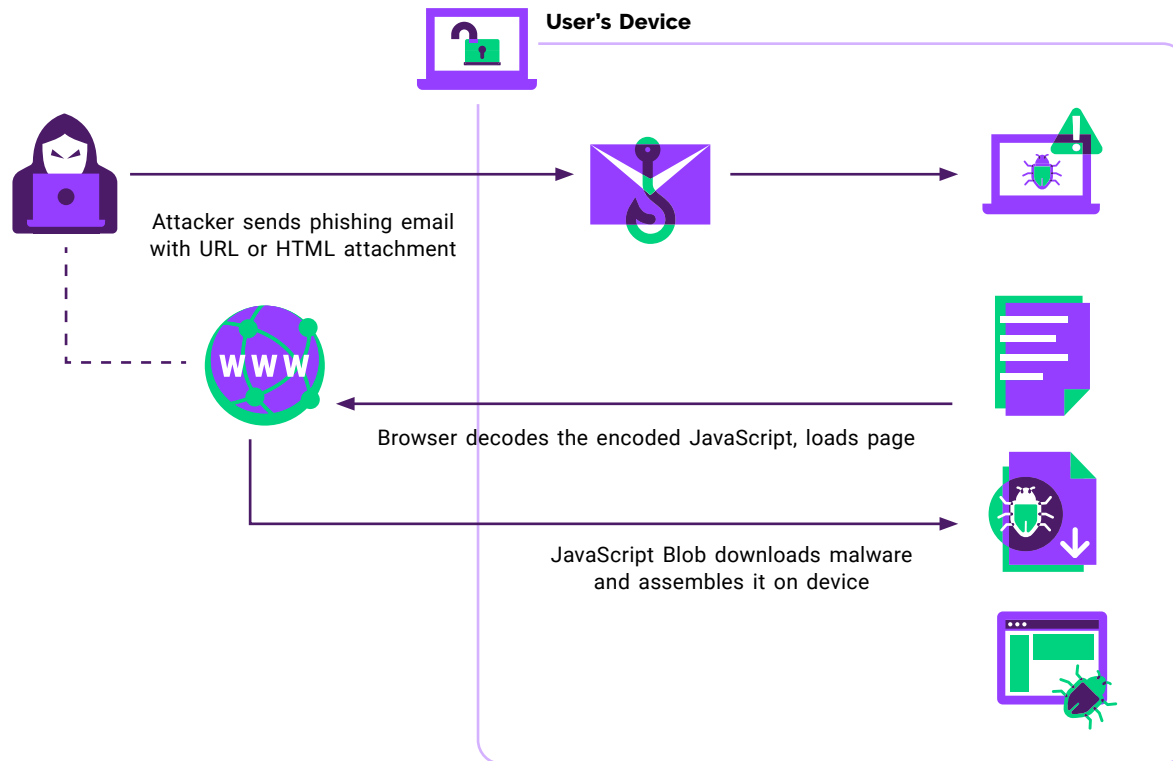
- **Standard perimeter controls:** Standard perimeter controls such as web proxies, email gateways, and sandboxes do not detect this highly evasive threat. They typically only check for suspicious attachments or anomalous traffic based on signatures and patterns. HTML smuggling tags along with legitimate uses of HTML and JavaScript that happen in daily business operations.
- **Lack of visibility and isolation:** To see and stop HTML smuggling requires visibility into the browser and the ability to isolate to see what's inside before releasing the content to the endpoint.



According to the MITRE ATT&CK framework, HTML smuggling is a common technique threat actors use to gain initial access.

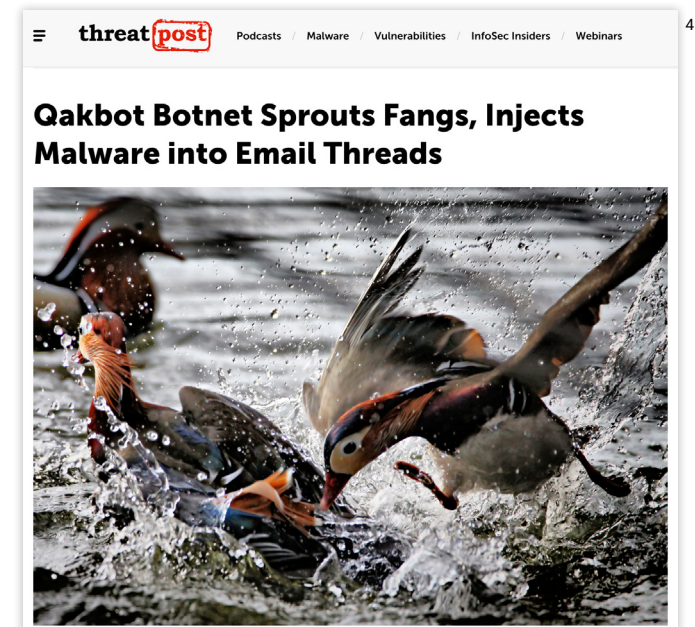


HTML smuggling attack in action



HTML smuggling in the wild: Qakbot

HTML smuggling has recently targeted the banking sector. Qakbot, which was found in the wild in 2007, has been continually maintained and developed. Today, it is the leading banking Trojan around the globe used to steal banking credentials.



Web threat #3: SEO poisoning

What it is.

SEO poisoning, or search poisoning, is an attack method in which cybercriminals create malicious websites to infect visitors with malware or phish them for sensitive information. Adversaries can also carry out the attack by compromising benign websites by inserting specific keywords to increase the rankings of the site and then hosting malware on it.

How it works.

Attackers use sponsored links to appear at the top of search results. Using SEO keywords and phrases, attackers make content appear relevant and trustworthy to unsuspecting internet users.

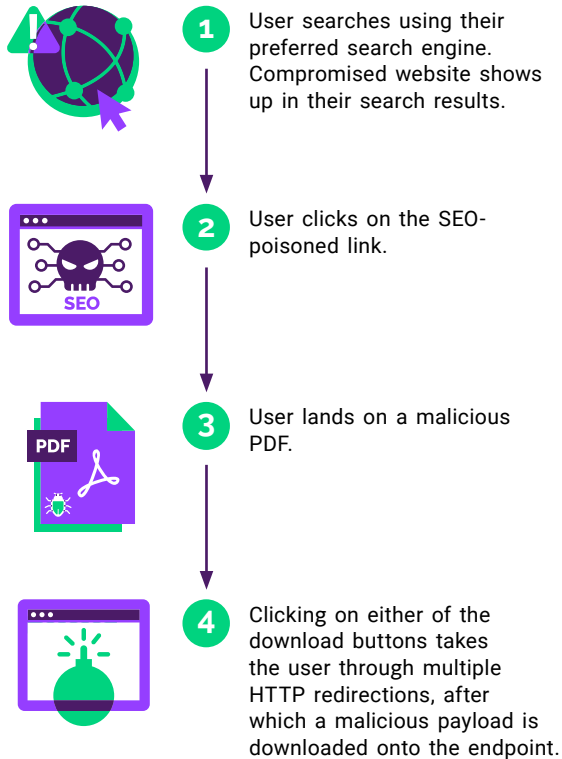
An example of this would be an attacker creating a malicious website with cookie recipes before the holiday season. Knowing it is a popular time to bake, they would incorporate phrases such as “Best Sugar Cookie Recipe” and pay to rank higher in the search. Because the website appears on the first page, it instills trust and increases the chance that internet users will click on the site. Unbeknownst to the user, the attacker inserted a malicious PDF of the “recipe” for the reader to download.

What makes you susceptible to attack.

- **Reliance on the reputation layer:** SEO poisoning attacks easily bypass the reputation layer of security. Categorizing websites as good or bad does not work. From the outside, the website is trustworthy – it has keywords and ranks highly. It’s not until a user clicks on a malicious file that it delivers the malware on the endpoint.
- **Lack of isolation:** These attacks have been specifically designed to target the user directly. Once the user clicks the malicious file, it automatically infects the endpoint. There is no isolation where the file’s contents are inspected before downloading onto the endpoint.



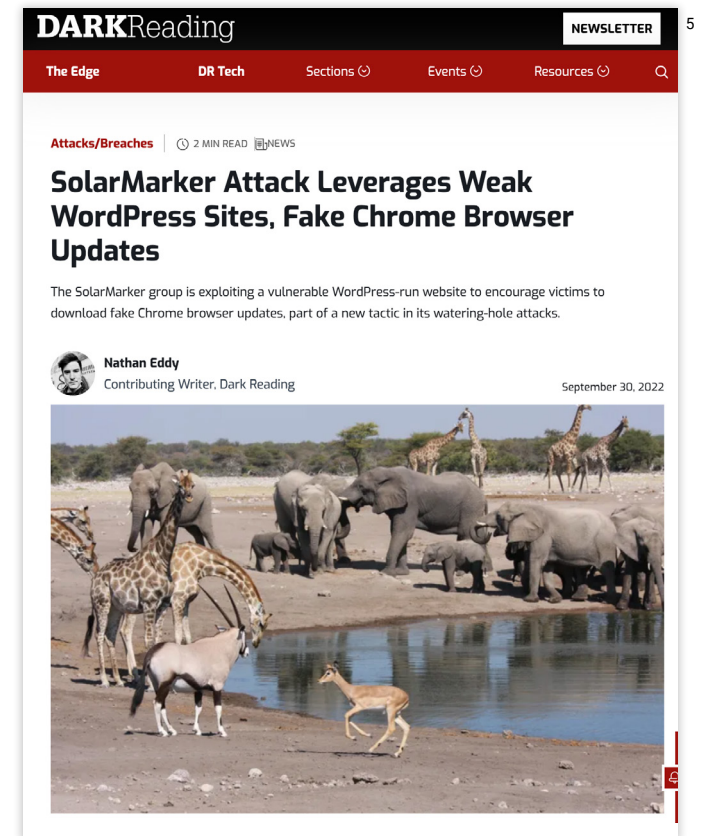
SEO poisoning attack in action



SEO poisoning in the wild: SolarMarker Malware

Because of remote work, the browser is where work happens. According to a recent survey from Menlo Security, three-quarters of respondents believe that hybrid and remote workers pose a significant threat to their organization's security. We are seeing that come true with threats like the SolarMarker Malware. While a classic example of a supply chain-style attack, it demonstrates how attackers have quickly pivoted to exploit the increase in browser usage and cloud-based applications.

While analyzing the malware, we found some well-known educational and .gov websites serving malicious PDFs.



Web threat #4: Malicious password-protected files

What it is.

Of all the web threats that defy detection, a malicious password-protected file attack has the lowest barrier to entry.

Password-protected files are used every day for legitimate business purposes – and more often than not, security policies are set to allow these files to protect productivity. But because they are locked by a password, they bypass scanning methods performed by sandboxes which leaves a large vulnerability.

How it works.

A malicious document is password protected and delivered inside an email with the password. The attack easily tricks unsuspecting users into opening the malicious file.

What makes you susceptible to attack.

- **Traditional anti-malware detection:** Because the files are password protected, traditional anti-malware detection tools cannot scan the attachment for malicious code.
- **Inability to strip malicious code:** You need to be able to strip documents of suspicious code, such as macros but maintain the structure and composition of the document.
- **Allow/deny password-protected files:** Security solutions that allow or deny password-protected files are not granular enough. The policy decision is generally left to the business and out of the security team's hands.

Yes

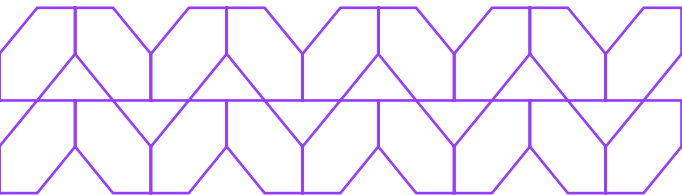
Allows all malicious password-protected files through

No

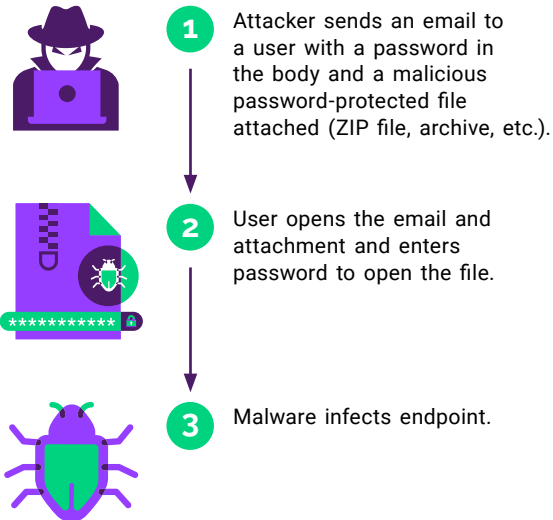
Blocks legitimate files that are needed for productivity



of malware is delivered in archives.⁶ Archives are now the most popular file type for delivering malware as attackers bypass perimeter security controls.



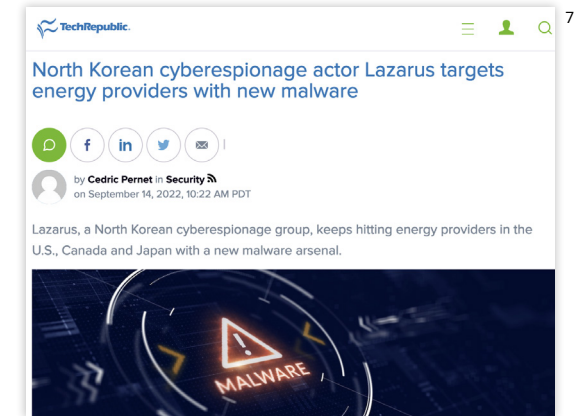
Malicious password-protected file attack in action



Malicious password-protected files in the wild

Lazarus Group

The infamous Lazarus Group is a fan of malicious password-protected file attacks as their initial access method. They use security company logos as a decoy on documents in their malicious campaigns. One such example was the use of the Mandiant APT1 threat report.



Nation-state groups

Nation-state groups aligned with China are getting increasingly proficient at bypassing security solutions through messages bearing malicious lure archives distributed via Dropbox or Google Drive links.



7 <https://www.techrepublic.com/article/lazarus-targets-energy-providers/>

8 <https://thehackernews.com/2023/03/researchers-uncover-chinese-nation.html>

Gain control over web-based threats.

The attacks outlined in this e-book and their respective evasive characteristics can be categorized as Highly Evasive Adaptive Threats, or HEAT attacks.



A HEAT attack is a class of cyberthreat that leverages web browsers as the attack vector and employs various techniques to evade multiple layers of detection in current security stacks.

Returning to protecting against each web threat, because the HEAT attacks had legitimate uses, simply blocking them didn't work. Now, organizations need to prevent the use of these techniques altogether.





Making HEAT attacks never happen in the first place is the only way to stop them.

Better visibility and control inside the browser are must-haves to detect and block highly evasive threats. As these threats continue to evolve, so must our technology used to defend against them. In modern-day defense, this includes security policies, which should be as adaptive as the threats targeting our users.

Invisible enemies have no power when you use a Zero Trust approach to security with Isolation technology. In the browser, all content – malicious or not – is treated as bad and executed in an abstract layer in the cloud. Should users approve a malicious MFA request, click on a malicious HTML attachment, land on an SEO-poisoned webpage, or unlock a password-protected file – it all happens on a virtual browser in the cloud. By protecting every click, you can feel secure, knowing that potential threats like malware and ransomware never come anywhere near the endpoint.

While attackers are busy trying to defy detection, your protection no longer relies on detecting at all. Users are only exposed to sanitized, safe content – cutting off any opportunity for initial access.

HEAT attacks are defined by four characteristics that will now be familiar to you based on what you've learned about web threats:

Evasive Web Threat	HEAT Evasive Characteristic
 MFA bypass	Evades URL filtering, email security tools, and HTTP page/content inspection
 HTML smuggling	Evades file-based inspection
 SEO poisoning	Evades URL filtering
 Malicious password-protected files	Evades URL filtering, file-based inspection, and email security tools

These are some examples. Most of these threats employ multiple HEAT evasive characteristics.

About Menlo Security

Menlo Security protects organizations from cyberattacks by eliminating the threat of malware from the web, documents, and email. It focuses on protecting the single biggest productivity driver for knowledge workers — the web browser.

Menlo's Cloud Security Platform prevents threats from entering an organization and secures data and application access in a single, global cloud-based offering. Our Elastic Isolation Core™ creates separation between the user, content and applications where security, policy and visibility are applied. With deep visibility inside the browser, adaptive policy enables the prevention of threats before they happen, as opposed to detecting and responding, organizations eliminate all threats, including Highly Evasive Adaptive Threats (HEAT) across web, email, SaaS applications and private applications.

HEATcheck

Menlo Security provides a lightweight penetration assessment to help organizations better understand any susceptibility to various HEAT attacks. The assessment leverages various real-world HEAT attacks currently being used by threat actors, safely allowing organizations to deduce their exposure. Menlo's [HEATcheck tool](#) does not deliver actual malicious content.

Get in touch with us.

[Contact us](#) today to learn if your organization is currently susceptible to these top web threats, but most importantly, how you can make them never happen in the first place.

www.menlosecurity.com

(650) 614 1705 | ask@menlosecurity.com

