IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

HEAT Challenges Ahead for CISOs

Jonathan Lee

Jonathan Lee
Senior Product Manager
Menlo Security

Biography

Jonathan Lee is a Senior Product Manager at Menlo Security (https://www.menlosecurity.com), a leader in cloud security. In this role he serves as a trusted advisor to enterprise customers, and works closely with analysts and industry experts to identify market needs and requirements, and establish Menlo Security as a thought leader in the Secure Web Gateway (SWG) and Secure Access Service Edge (SASE) space.

Experienced in leading technical development, launch and adoption of innovative security products, including email security, data loss prevention and end point security, Jonathan previously worked for Proofpoint and Websense. As an industry expert, media commentator and speaker, Jonathan is well versed in data protection, threat analysis, networking, Internet isolation technologies, and cloud-delivered security.

Keywords Browser security, Web security, Isolation technology, Cyber security, Cyber threat, Malware, Ransomware, Phishing, HEAT, HEAT attacks
Paper type Reference

Abstract

With the effects of the pandemic largely behind us, it was hoped that 2023 would bring calm and composure, but instead it has brought more turbulence. The impact of the Russian invasion of Ukraine continues to add to the growing cost of living crisis, and has made the threat landscape even more precarious. Threat actors have continued to expand and evolve their attack methods, leveraging new techniques and exploiting a series of emerging vulnerabilities. In this article, the author looks at four key emerging trends on the threat landscape which organizations can expect to see growing throughout 2023.

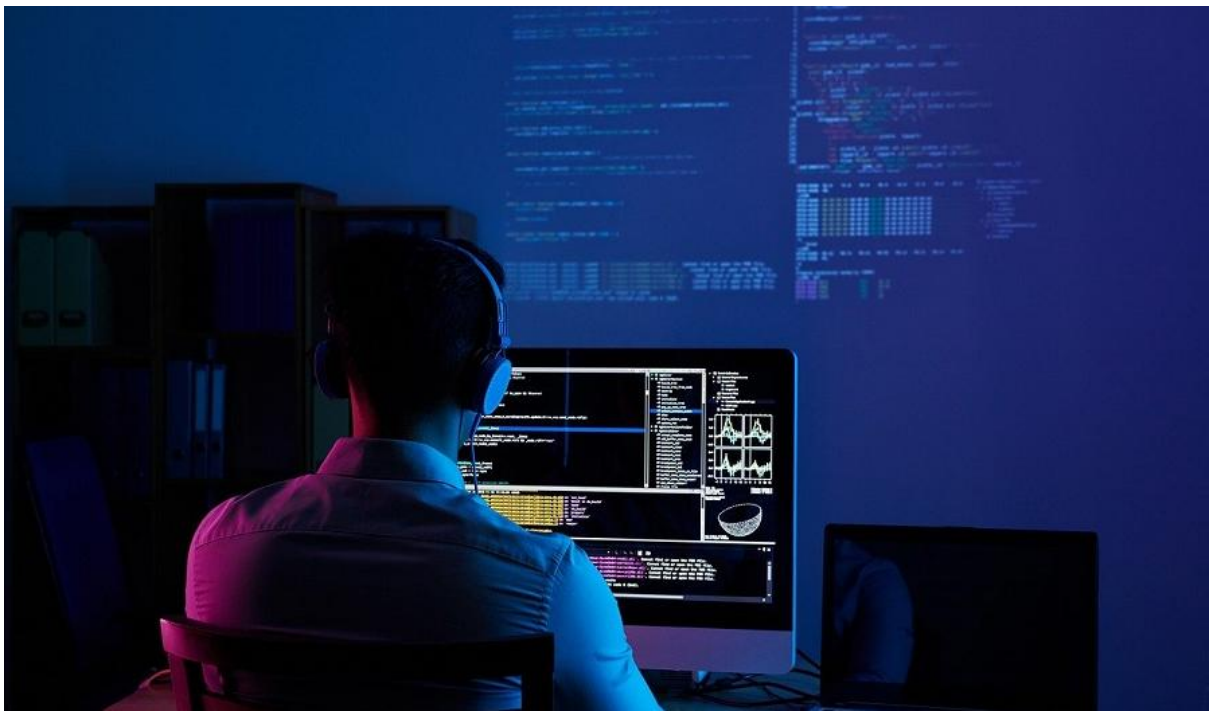
Introduction

Most IT professionals agree that cybersecurity is getting harder. The biggest reason for this is the types of attacks and attackers using 'highly evasive adaptive threats' (HEAT) techniques. While any cyber-attack has the potential to lead to major business disruption, it is ransomware, cyber extortion, and phishing attacks, and the significant consequences they cause which have risen to the top of the priority list for many organizations.

As the threat landscape heats up, attackers are continuing to evolve their tactics to try to stay ahead off defenses, and organizations must now shift their mindset from one of post-breach detection, to one of prevention with a focus on stopping threats before they reach the endpoint.

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**



HEAT attacks

Moves from threat actors to understand common technologies across the security stack and tailor attacks to bypass these tools is a pressing problem for enterprises. Indeed, modern threats are becoming increasingly advanced and evasive as adversaries come up with ways of getting around defences that are all too often inadequate or outdated.

Throughout the last year, The Menlo Labs team has been tracking a distinct and notable rise in Highly Evasive Adaptive Threat (HEAT) techniques – a class of cyber threats that have been tailored to evade protective tools such as firewalls, secure web gateways, malware analysis including sandboxing, URL reputation and phishing detection technologies.

Menlo Labs identified a 224% increase in 2021, and we're expecting a similarly alarming increase this year as attackers have further evolved their attack methods. If firms continue to lean heavily on traditional detect and respond security techniques, attackers will find success in HEAT-based endeavours.

Basic security failures

Unfortunately, basic security failures at even some of the most renowned organizations in the world continue to offer open doors for attackers to step through and begin to wreak havoc. For example, take the attack on Uber in September 2022. Here, a lone threat actor was able to gain administrative control over the ride hailing giant's IT systems and security tools owing to an exposed PowerShell script that contained admin credentials to the firm's privileged access management (PAM) platform.


IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

It's a telling example. It doesn't matter how extensive an organization's security investments might be, or how sophisticated their technologies. Often, threat actors can use simple and proven methods such as social engineering techniques to find ways around them.

This example hasn't just reiterated that there is simply no silver bullet or panacea to stopping attacks. The Uber breach also showed multi-factor authentication (MFA) push notifications to be exploitable, causing widespread concern and a demand for the use of FIDO2 passkeys and hardware tokens in replace of passwords. This is something we might begin to see gather momentum in 2023. However, it will take a lot of work to implement it on a widespread basis, and even then, we foresee attackers simply finding the next weakest link in the chain.

Browser-based attacks

The third trend we see accelerating through 2023 is browser-based attacks. Undoubtedly the biggest attack surface available for threat actors to exploit today, it is critical that the security sector takes greater steps to protect this space.

Several vendors are already looking at ways to add security controls directly inside the browser, moving away from traditional methods of improving protection with a separate endpoint agent or via the network edge where firewalls or secure web gateways are used.

It's pleasing to see major names such as Google and Microsoft making headway in this domain. Both organizations are developing and implementing built-in controls inside their respective Chrome and Edge browsers to secure at the browser level, rather than the network edge.


IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

However, threat actors seem to be determined to remain one step ahead. Browser attacks are increasing, with attackers exploiting new and old vulnerabilities, and developing new techniques such as HTTP Smuggling.

As a result, remote browser isolation (RBI) is becoming an increasingly core principle of Zero Trust security that stipulates that no device or user – not even the browser – can be trusted.

One size doesn't fit all

It is vital for organizations to remember that one size simply doesn't fit all when it comes to security, and bespoke technology combinations and strategies are still the way to go.

Recent reports from Gartner have suggested that many organizations are pursuing strategies focused on security vendor consolidation, cutting the number of providers they are working with for their security needs. This has been particularly prevalent in more complicated arenas such as secure access service edge (SASE) and extended detection and response (XDR).

The motivation is less cost focused, and more about reducing complexity and improving risk management abilities. While policies of continuous improvement are always going to be encouraged when it comes to security, it is important that organizations don't discard best of breed solutions in the process.

Adopting zero trust

Policies such as Zero Trust will go a long way in improving security postures.

Fortunately, this is a positive trend that we can expect to see in 2023, with many organizations already exploring Zero Trust as a policy in a more active manner. According to a survey from Verizon, presented in its 2022 Data Breach Investigations Report[1], 82% of respondents revealed that they had adopted or were considering adopting a Zero Trust approach to security.

What is the benefit of Zero Trust? Unlike outdated detect and respond solutions that weren't built for cloud operating models and browser-based operations that now dominate our working world, Zero Trust has been designed to address risks in the current environment.

It recognizes trust in a network as a vulnerability, demanding that all traffic (be it emails, documents, websites, videos or other) should always be scrutinized and verified. Equally, it advocates the 'principle of least privilege' where users are only given access to the enterprise resources and applications they truly need to carry out their daily tasks effectively. Together, these policies build resilience. Should attackers gain access to a network, they won't be able to move freely, mitigating or limiting the potential damages of any attack.

There are tools available to support organizations in achieving Zero Trust in the truest sense, with isolation technology being a prime example. Isolation works by moving the browser execution process away from the desktop and into the cloud,

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

rendering only safe web content on the endpoint. Resultantly, no active content from the internet – be it good or bad – is ever downloaded directly to the endpoint.

Unlike other technologies, isolation isn't 'almost safe'. Rather, it can wholesale stop cyberattacks at source, 100% of the time by ensuring that attackers never have an opportunity to execute their payloads.

In summary

As the adoption of cloud accelerates and the shift to remote and hybrid working continues, the daily routines for most workers revolve around the browser, and cyber-criminals are continually look for ways to innovate and remain relevant as trends and market dynamics evolve. As the evolution in HEAT attacks continue and attackers exploit key gaps in traditional security defenses, security leaders will need to be more agile in dealing with adversity and security teams will need to adapt faster to the ever-changing threat landscape if they are ever to defend the organization from HEAT attacks in the future.

Reference

1 2022 Data Breach Investigations Report. Verizon. Available at: https://www.verizon.com/business/resources/reports/dbir/