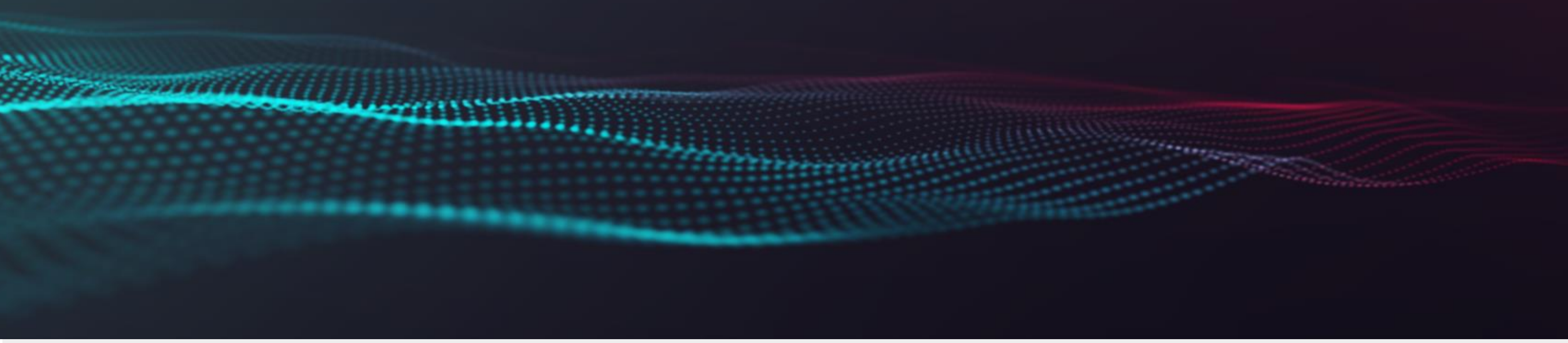
Enterprise Strategy Group | Getting to the bigger truth.™



ESG WHITE PAPER

The Threat Landscape HEATs Up with Highly Evasive Adaptive Threats

By John Grady, ESG Senior Analyst

January 2022

This ESG White Paper was commissioned by Menlo Security and is distributed under license from ESG.

Contents

Executive Summary

For as much as the nature of work and corporate environments has changed over the last decade, cybersecurity practices, tools, and strategies remain largely the same. Unfortunately, adversaries are highly motivated and consistently evolve to remain ahead of defenses. Attackers fully understand traditional cybersecurity approaches, including their limitations, which gives hackers a clearly defined blueprint that can be followed to ensure success.

Menlo Security has studied a variety of techniques attackers are using to successfully launch ransomware and phishing attacks and have termed these "highly evasive adaptive threats" (HEAT). HEAT attacks evade existing security defenses by understanding all the technology integrated into the existing security stack and building delivery mechanisms to evade detection. To meet the challenges posed by HEAT attacks, organizations must shift from a post-breach detection mindset to one of prevention, with a focus on stopping threats before they ever reach the endpoint.

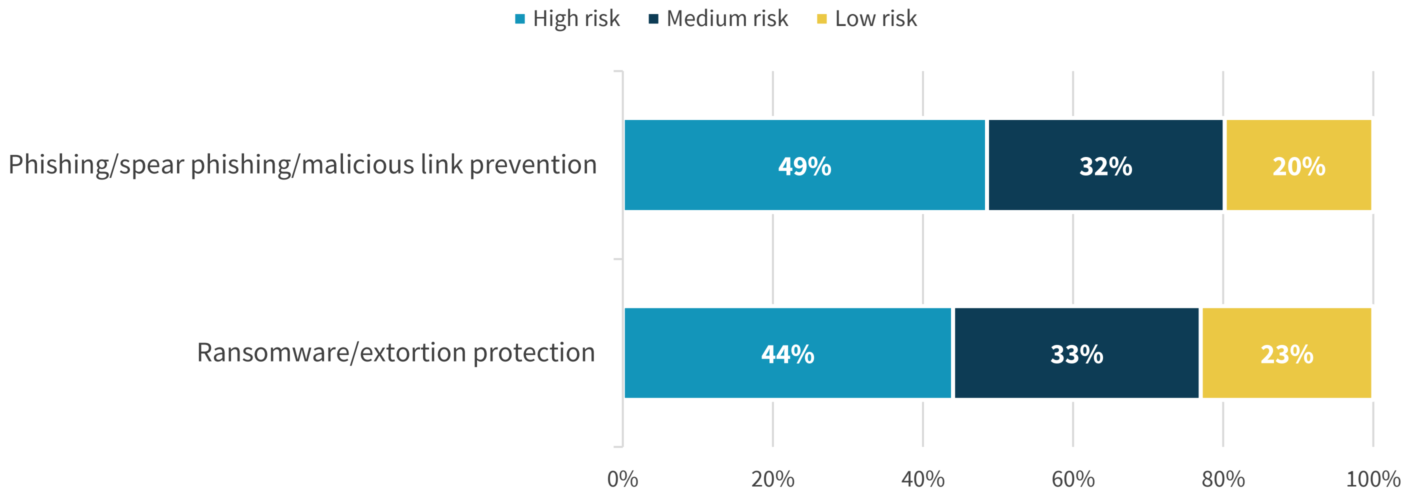
Highly evasive adaptive threat (HEAT) attacks evade existing security defenses by understanding all the technology integrated into the existing security stack and building delivery mechanisms to evade detection.

The Evolution of the Threat Landscape Continues

Over the last few years, cybersecurity has evolved from an IT-centric issue to a business priority for many organizations. While this is due in some part to the role of cybersecurity in supporting broader initiatives such as cloud adoption or digital transformation, the evolution of the threat landscape and resulting negative business impacts of successful attacks have played a major role as well. While any cyber-attack has the potential to lead to major business disruption, ransomware, cyber extortion, and phishing attacks have risen to the top of many organizations' priority lists due to the significant consequences they cause. In fact, ESG research shows that nearly half of organizations view phishing and ransomware attacks as a high risk to their organization (see Figure 1).[1]

Figure 1. Perceived Risk of Phishing and Ransomware Attacks

How would you prioritize the following threats in terms of the risk you believe they pose to your organization? (Percent of respondents, N=403)



Source: Enterprise Strategy Group

[1] Source: ESG Research Report, *Trends in Email Security*, August 2020.

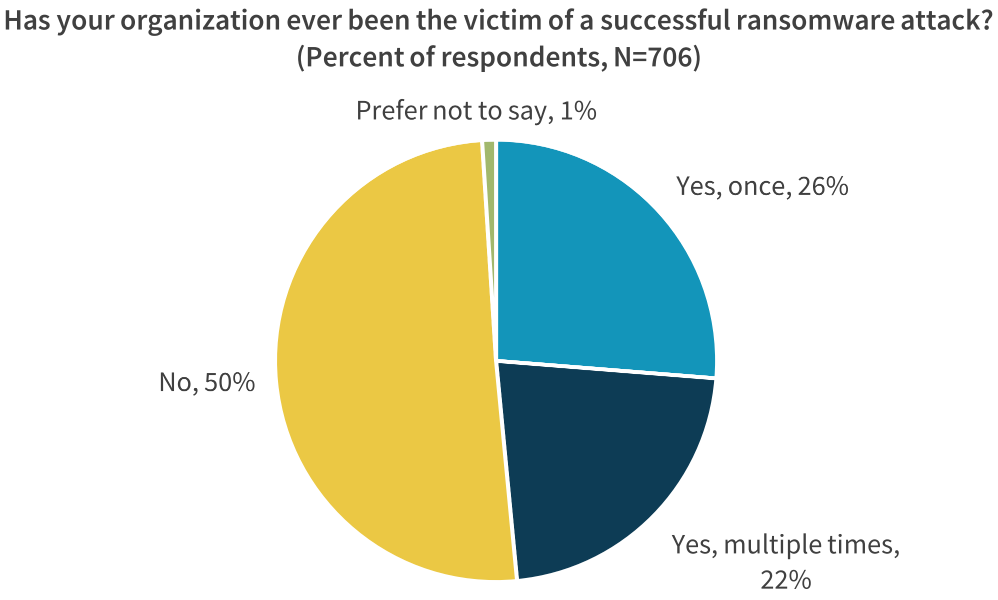
More tellingly, ESG has found that 22% of organizations say ransomware readiness is their most important business priority, and 46% indicate it is one of their top 5 business priorities.[2] High profile attacks against critical infrastructure (such as Colonial Pipeline) and IT suppliers (such as Acer and Kaseya) have helped push this issue even further into the mainstream and to the forefront of board agendas.

22% of organizations say ransomware readiness is their most important business priority, and 46% indicate it is one of their top 5 business priorities.

However, focusing solely on these headline-generating incidents, which often focus on some of the largest companies in the world, can obscure the fact that organizations of all types, sizes, and security maturity are dealing with this issue on an ongoing basis. Specifically, ESG research has found that 36% of organizations have experienced attempted ransomware attacks on a daily, weekly, or monthly basis, while an additional 27% have encountered ransomware on a sporadic basis over the last 12 months.[3]

Unfortunately, these attacks are often successful. Over a quarter (26%) of ESG research respondents indicated they had been the victim of a successful ransomware attack once, and 22% indicated it had happened on more than one occasion (see Figure 2).[4] Obviously security teams are aware of these issues and security vendors have attempted to update their offerings to defend against these attacks. Yet with so many organizations being impacted by ransomware and other financially motivated attacks, the question then becomes: how are attackers able to continually bypass defenses?

Figure 2. Successful Ransomware Attacks



Source: Enterprise Strategy Group

[2] Source: ESG Complete Survey Results, 2022 Technology Spending Intentions Survey, November 2021.
[3] Ibid.
[4] Ibid.

Defining Highly Evasive Adaptive Threats

Menlo Security has recently identified a set of techniques that adversaries are increasingly using to evade detection by traditional security tools. These attacks, which Menlo Security calls “highly evasive adaptive threats,” can be used for any type of attack that targets the user, endpoint, or applications, including ransomware (see Figure 2). Specifically, these attacks employ one or more of these four key characteristics:

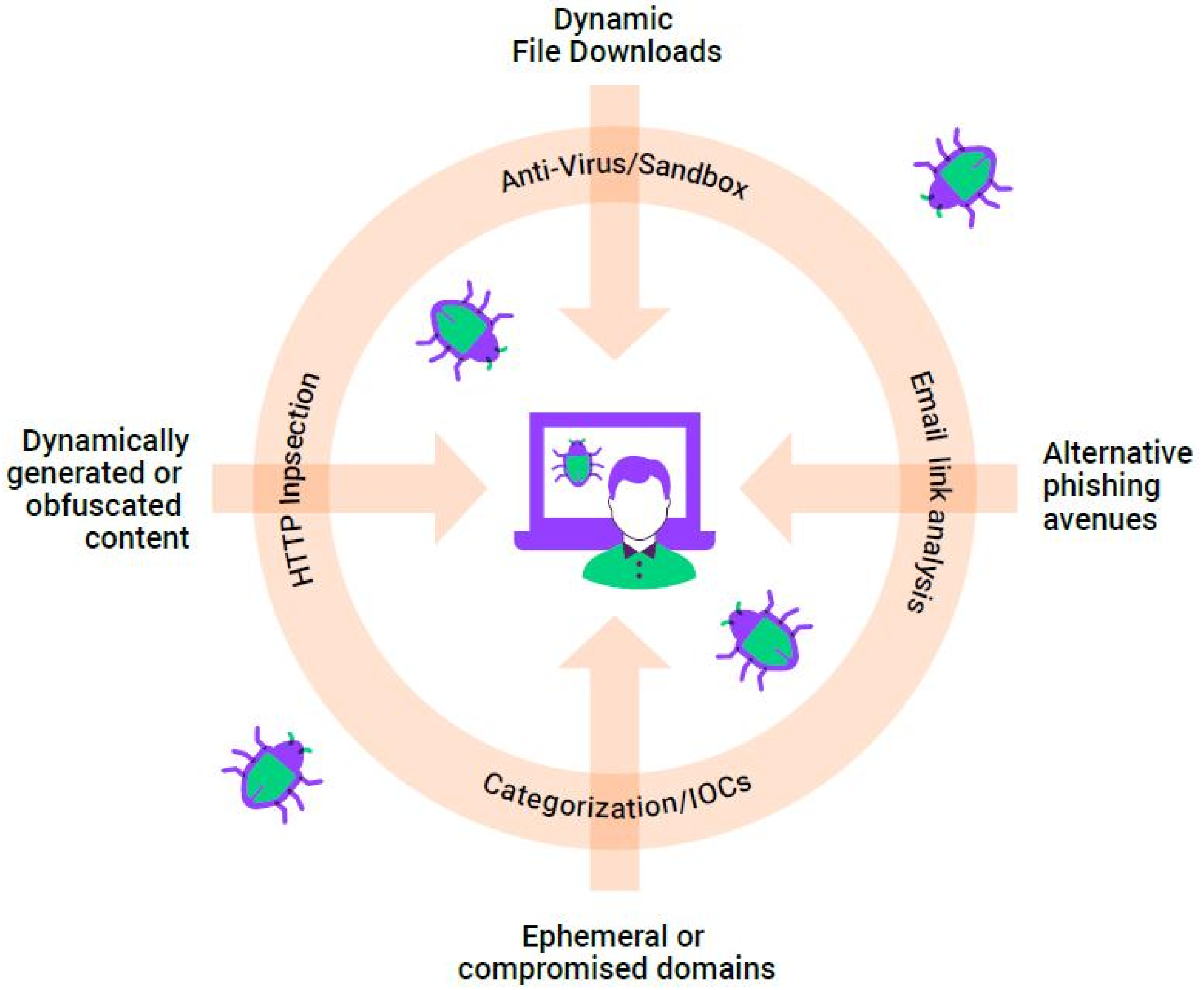
1. Dynamic file downloads. HEAT attacks use HTML smuggling to evade both signature- and code analysis-based detection methods. The technique uses legitimate HTML5 and JavaScript features to stealthily deliver downloads to the endpoint. An attacker will create an encoded JavaScript blob, and when the user clicks on the affected link, the browser decodes the script and assembles the malicious payload on the device. Because the malware is constructed on the device, there is no file to pass through traditional scanning mechanisms. Disabling JavaScript can mitigate the attack but is typically not feasible because of the impact to legitimate web pages. While these tactics are not new, they have seen increasing usage. The Nobelium hacking group responsible for the SolarWinds breach and other high-profile attacks has used this technique, and Menlo Labs is monitoring campaigns it has labeled Duri and ISOMorph, which use HTML smuggling well.

2. Alternative phishing avenues. The focus on phishing has traditionally centered on the email vector. But as users have been trained and conditioned to look for suspicious emails and email security tools have improved their ability to detect phishing links, HEAT attacks have shifted to other channels. Spear phishing on LinkedIn and other social media sites has become a common tactic to evade anti-phishing tools. Attackers may use connection invitations, content posts, or job offers to deliver malware payloads directly or via malicious URLs. Similarly, SMS messages have seen increasing usage by attackers to send malicious links to unsuspecting recipients. Regardless of the channel, the outcome is the same: credentials or other sensitive information are stolen before security teams even know there is an issue.

3. Ephemeral or compromised domain usage. While not a new technique, the ease with which attackers can spin up malicious sites makes it easier than ever for HEAT attacks to remain ahead of categorization engines. Before malicious behavior can be observed by offline web crawlers, attackers will pull down the site and create it elsewhere. In addition to using ephemeral sites and domains, attackers may take a more patient approach by building a site or set of sites and waiting days, weeks, or even months before using them for malicious activity. In both cases, the use of CAPTCHAs is often used to make the site appear more legitimate to victims, evade offline web crawlers, or even deliver the malicious content itself. Finally, attackers continue to compromise legitimate sites that are poorly defended and use them to serve malware, making defenses predicated on categorization much less effective.

4. Use of dynamically generated or obfuscated content. HEAT attacks can also generate exploit code at the browser to avoid detection via signatures that examine the source code of web pages, such as by using the Eval() function in JavaScript. Additionally, attackers may obfuscate JavaScript to make it unreadable to both security researchers and detection engines. Finally, attackers use website code manipulations through JavaScript to pull the real logos of the top-phished brands (such as Office365) to bypass engines reliant on visual detections.

Figure 3. Highly Evasive Adaptive Threats



Source: Menlo Security

Why Security Teams Should Be Thinking About HEAT Attacks

Most IT professionals agree that cybersecurity is getting harder. ESG research has found that 64% of respondents say network security at the edge has become more difficult than it was 2 years ago. The evolving threat landscape is a key driver of that complexity, with 41% indicating it was one of the factors most responsible for making network security at the edge more difficult.[5] With that being the case, why should HEAT attacks in particular warrant specific attention?

The biggest reason for this is the types of attacks and attackers using HEAT techniques. Microsoft observed the Nobelium group using HTML smuggling in a sophisticated spear-phishing campaign in May 2021.[6] Similarly, Trickbot, which is increasingly used for ransomware, has used HEAT techniques to deliver the initial payload of an attack. The reach of just these two threat actors has the potential to impact organizations of all sizes and types, and the fact that these tactics have already been seen in the wild point to the likelihood that HEAT attacks will only increase in prevalence.

[5] Source: ESG Survey Results, *Transitioning Network Security Controls to the Cloud*, July 2020.

[6] Source: Microsoft Threat Intelligence Center (MSTIC), *New sophisticated email-based attack from Nobelium*, May 2021.

This increase in the attack landscape is directly exacerbated by the fact that traditional tools and strategies fall short. While true that malware detection has evolved from signature-based approaches to more reliance on sandboxing and analytics, the improvement has only been incremental. These methods still rely on identifying malicious code, which gives attackers an opportunity to evade defenses.

Whether network- or endpoint-centric, traditional security models ultimately require there to be an initial victim somewhere before signatures or analysis engines can be updated accordingly.

For example, sandboxes may not be able to process obscure file formats or files of a particular size. Additionally, malware can be sandbox-aware, forcing organizations to decide whether to rely on post-deliver analysis or potentially impact user productivity by withholding the file. While endpoint products may seem to have the advantage by residing on the device itself, these tools are difficult to deploy to unmanaged devices and are often disabled by hackers in the first stages of an attack. Whether network- or endpoint-centric, these models ultimately require there to be an initial victim somewhere before signatures or analysis engines can be updated accordingly.

Further, work has fundamentally changed. For most employees, a significant amount of time is spent in the web browser. Whether accessing corporate SaaS applications, private applications that are increasingly web-based; doing research on the web; or even accessing email, the browser has become the cornerstone of many employees' daily routines. Further, while the browser has become the new office, the internet is now the network, and applications and data are everywhere, leading to a lack of visibility and control, which attackers increasingly take advantage of.

Finally, the skills shortage continues to loom large. While it is true that security spending overall is robust and very large companies may be in a better position to succeed, many organizations struggle to fully fund and staff their security teams. ESG has found that more organizations plan to increase cybersecurity spending (69%) than any other area of technology. Yet at the same time, nearly half of organizations (48%) report a problematic shortage of existing skills—again, more than any other area of technology.[7] Even large organizations may only employ a handful of dedicated security personnel. Noisy security tools often generate too many alerts with poor fidelity and context, making it difficult for understaffed teams to be efficient. This results in security teams having to jump from one issue to the next, ultimately impacting security effectiveness and giving attackers the advantage.

Key Considerations for Stopping HEAT Attacks

Obviously, there is no cybersecurity silver bullet. Attackers will continue to evolve their tactics to try to stay ahead of defenses. This is true both generally and with HEAT attacks specifically. However, organizations should focus on three key tenets to limit their susceptibility to these types of attacks: shifting from a detection to a prevention mindset, stopping threats before they hit the endpoint, and incorporating advanced anti-phishing and isolation capabilities.

Organizations should focus on three key tenets to limit their susceptibility to these types of attacks: shifting from a detection to a prevention mindset, stopping threats before they hit the endpoint, and incorporating advanced anti-phishing and isolation capabilities.

For detection to be successful, organizations need comprehensive visibility with no blind spots, well correlated data across a variety of sources, and the ability to instantaneously respond when incidents occur. For all but the most sophisticated organizations, this is a tall order. As a result, the goal should be to prevent as many threats as possible before they have any

[7] Source: ESG Complete Survey Results, *2022 Technology Spending Intentions Survey*, November 2021.

impact on devices or systems, rather than reacting after the fact. The widespread interest in zero trust is validation of this type of strategy. Limiting the blast radius and removing implicit trust from the environment have become more important than ever as complexity and diversity have grown. By shifting to a prevention mindset and incorporating zero trust principles, security teams can move away from a firefighting mentality and focus on proactively strengthening the organization's security posture by identifying and remediating vulnerabilities, hardening configurations, and threat hunting.

The next question becomes: Where should prevention be focused? As workers and resources have become increasingly dispersed, it has become critical for protection to be distributed as well. At the same time, HEAT attacks are designed to circumvent endpoint tools by assembling malware on the device and often disabling controls once delivered. Cloud-based, web-focused protection would seem to make the most sense to protect against these types of attacks, yet security teams should assess these tools carefully. Secure web gateways (SWG) have traditionally been deployed on-premises, focused on enforcing acceptable use policies, relied on signature-based threat prevention, and provided poor visibility into applications—limitations that prevent them from preventing HEAT attacks. Security teams should look for modern cloud-native SWGs that provide granular application visibility and control, inline content inspection, and advanced threat prevention capabilities that can stop HEAT attacks before they occur.

Finally, it is imperative that prevention capabilities include advanced isolation and anti-phishing protection. Signatures and analytics may help prevent some threats from impacting the enterprise, but HEAT attacks require an additional layer of protection. By preventing the browser from interacting with the endpoint, isolation ensures that stealthy threats like HEATs cannot gain a foothold. Similarly, with phishing protection expanding beyond traditional email channels, consistent protection against web, social, and SMS-led attacks has become increasingly important.

The Bigger Truth

Just like any business or industry, cyber-criminals are continually on the lookout for ways to innovate and remain relevant as trends and market dynamics evolve. The shift to remote and hybrid work and acceleration of cloud adoption has transformed the daily routines for most workers, with most of it revolving around the browser. It only makes sense from an attacker perspective to cast a line where the majority of fish are swimming.

HEAT attacks represent an important evolution in attacker techniques to exploit key gaps in traditional security defenses. The fact that some of the most well-known hacker groups are already using these methods for ransomware and other advanced attacks highlights how agile the adversary is and how quickly security teams must adapt to keep pace. With this in mind, security leaders should put emphasis on prevention, distributed protection away from the endpoint, and advanced anti-phishing and isolation capabilities to defend against HEAT attacks.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

www.esg-global.com contact@esg-global.com ☎ 508.482.0188