Menlo Security report reveals less than three in 10 organisations are equipped to combat the growing wave of web-based cyber threats

Submitted by: Origin Comms Ltd
Wednesday, 16 March 2022

Web malware (47 per cent) and ransomware (42 per cent) now top the list of security threats that organisations are most concerned about. Yet despite the growing risks, less than a third (27 per cent) have advanced threat protection in place on every endpoint device that can access corporate applications and resources. This is according to new research, ‘The state of threat prevention: evasive threats take center stage’ (https://info.menlosecurity.com/Evaluating-evasive-threats-in-todays-cyber-landscape_report.html), published today by Menlo Security (http://www.menlosecurity.com/), a leader in cloud security, exploring what steps organisations are taking to secure themselves in the wake of a new class of cyber threats – known as Highly Evasive Adaptive Threats (HEAT) (https://www.menlosecurity.com/press-releases/menlo-security-finds-cloud-migration-and-remote-work-gives-rise-to-new-era-c

As employees spend more time working in the browser and accessing cloud-based applications, the risk of HEAT attacks increases. Almost two-thirds of organisations have had a device compromised by a browser-based attack in the last 12 months. The report suggests that organisations are not being proactive enough in mitigating the risk of these threats, with 45 per cent failing to add strength to their network security stack over the past year. There are also conflicting views on the most effective place to deploy security to prevent advanced threats, with 43 per cent citing the network, and 37 per cent the cloud.

“Threat actors seek to exploit gaps in traditional security defences and the fact that security capabilities haven’t really changed over the past decade. One of the areas of focus for attackers is using web threats and we’re seeing more and more of them successfully deployed using HEAT techniques. Last year, we saw Nobelium use HTML smuggling, a HEAT tactic to avoid static and dynamic content analysis, to deliver malware and ransomware attacks. The fact that these are successful means their usage will increase, which could have devastating consequences for companies of all sizes,” explains Mark Guntrip, Senior Director of Cybersecurity Strategy, Menlo Security.

“Working practices have changed and companies must stop relying on traditional tools and strategies that just don’t cut it anymore. Adopting a prevention-driven approach to security is the only way to achieve this and using isolation-powered security to do so stops the browser from having any direct interaction with the website and content and ensures that HEAT attacks don’t stand a chance.”

Competing security priorities

According to the research among 500+ IT decision makers in the UK and US, hybrid/remote working (28 per cent) is the biggest challenge organisations expect to face this year when it comes to protecting their corporate network from advanced threats. This is followed by budget restrictions (15 per cent), the presence of unmanaged devices (14 per cent), and out-dated security solutions (13 per cent).

There are also a number of competing priorities for IT professionals when it comes to improving their

security posture in 2022. Training staff tops the list (61 per cent), followed by technology investment to protect the corporate network (60 per cent), adapting to new ways of working (50 per cent), and investing in skilled security members at 45 per cent.

Additional research findings:

Although 55 per cent of respondents have invested in their security stack over the past year and 27 per cent have advanced threat protection in place, it is not having the desired effect as attacks are still successfully penetrating their defence lines.

Half of respondents believe that firewalls are an effective way of mitigating HEAT attacks, and 31 per cent favour VPNs.

Organisations believe that the threat of a cyber attack is a case of ‘when’ not ‘if’, regardless of size. Consequently, IT decision makers are most concerned about the reputational damage (62 per cent) and financial loss (57 per cent) that a security breach could have on their business.

According to Guntrip: “Organisations need to prioritise a review of their network security solution stack. HEAT target web browsers as the attack vector and employ techniques to evade detection by multiple layers in current security stacks, including firewalls, Secure Web Gateways, sandbox analysis, URL Reputation and phishing detection, so clearly a new strategy is needed.”

What are HEAT attacks?

The Menlo Labs research team has been analysing Highly Evasive Adaptive Threats (HEAT) (https://www.menlosecurity.com/blog/too-hot-to-handle-why-modern-work-has-given-rise-to-heat-attacks/), which bypass traditional security defences, including firewalls, Secure Web Gateways, sandbox analysis, URL Reputation, and phishing detection. The team observed a 224 per cent increase in HEAT attacks in the second half of 2021 (https://www.menlosecurity.com/press-releases/menlo-security-finds-cloud-migration-and-remote-work-gives-rise-to-new-era-c

Used to deliver malware or to compromise credentials, which in many cases leads to ransomware payloads, HEAT attacks include at least one of four evasion techniques:

Evades Both Static and Dynamic Content Inspection
Evades Malicious Link Analysis
Evades Offline Categorisation and Threat Detection
Evades HTTP Traffic Inspection
Survey Methodology

The survey questioned 505 IT decision makers across the United States and United Kingdom, including CIOs and CISOs, on the HEAT landscape, how businesses are responding to threats, and what their security challenges and priorities are for 2022. The interviews were conducted by Sapio Research in February 2022 using an email invitation and an online survey.

About Menlo Security

Menlo Security protects organisations from cyberattacks by eliminating the threat of malware from the web, documents, and email. Menlo Security's isolation-powered cloud security platform scales to provide comprehensive protection across enterprises of any size, without requiring endpoint software or impacting the end user-experience. Menlo Security is trusted by major global businesses, including Fortune 500 companies, eight of the ten largest global financial services institutions, and large governmental institutions. Menlo Security is backed by Vista Equity Partners, Neuberger Berman, General Catalyst, American Express Ventures, Ericsson Ventures, HSBC, and JP Morgan Chase. Menlo Security is headquartered in Mountain View, California. For more information, please visit www.menlosecurity.com.

Media contact:
Mandy Hassall
Origin Communications
M: 07855 359889/T: 01628 822741
amanda@origincomms.com