Menlo Security launches free Security Assessment Toolkit to help companies identify Highly Evasive Adaptive Threats (HEAT) fuelling ransomware and data and credential theft

Submitted by: Origin Comms Ltd
Tuesday, 21 June 2022

Infosec Europe 2022, ExCeL, London; 21 June, 2022 – Menlo Security (https://www.menlosecurity.com/), a leader in cloud security, today announced that it has released the HEAT Security Assessment Toolkit designed to provide organisations with the ability to assess their levels of protection and current exposure to Highly Evasive Adaptive Threats (HEAT). Since July 2021, Menlo Security has seen a 224% increase (https://www.menlosecurity.com/press-releases/menlo-security-finds-cloud-migration-and-remote-work-gives-rise-to-new-era-o in HEAT attacks. These attacks allow threat actors to deliver malicious content, including ransomware, to the endpoint by adapting to the targeted environment.

The HEAT Security Assessment Toolkit includes a HEAT Check test and a HEAT Analyzer that runs on the Splunk Platform. The HEAT Check enables customers to run a light penetration test to identify if they are susceptible to HEAT attacks. The Menlo Security HEAT Analyzer App for Splunk provides organisations with visibility around HEAT attacks that their network may have been exposed to over the past 30 days.

What is a HEAT Attack?
Highly Evasive Adaptive Threats (HEAT) are a class of cyber threats targeting web browsers as the attack vector and employs techniques to evade multiple layers of detection in current security stacks including firewalls, Secure Web Gateways, sandbox analysis, URL Reputation, and phishing detection. HEAT attacks are used as the initial access point to deliver malware or to compromise credentials, which in many cases leads to ransomware attacks.

“Ransomware, data and credential theft and other malware are on the rise. Couple this with the Log4J vulnerability, the Lazarus and Conti groups increased attacks targeting web browsers and the result is security teams worldwide facing a nearly non-stop barrage of incidents,” said John Grady, Senior Analyst, ESG. “Tools such as the HEAT Security Assessment can help ensure companies are aware of potential attacks before they have a chance to happen.”

HEAT Security Assessment Toolkit
The HEAT Security Assessment Toolkit provides a lightweight penetration and exposure assessment to help an organisation better understand their susceptibility to HEAT attacks.

“HEAT attacks are defined by the techniques that adversaries are increasingly using to evade detection by traditional security tools,” said Mark Guntrip, senior director of cybersecurity strategy, Menlo Security. “HEAT techniques can be used individually or in combination for any type of attack that targets the user, endpoint, or applications, including ransomware. The HEAT Security Assessment Toolkit is critical to helping companies ensure they are protected against these attacks.”

HEAT Check
The HEAT Check enables customers to run a light penetration test to find if they are susceptible to HEAT attacks. The assessment leverages several real-world HEAT attacks currently being used by threat actors,

safely enabling the user to determine their exposure.

The HEAT Check does not deliver actual malicious content. It uses an industry standard EICAR file to test an organisation's existing HEAT exposure. If the EICAR file is delivered without triggering an alert inside an organisation’s current security stack, then the security technology is not providing the requisite level of protection to defend against HEAT attacks.

Menlo Security HEAT Analyzer App for Splunk
To assess current HEAT exposure, the HEAT Analyzer, now available on Splunkbase (https://splunkbase.splunk.com/app/6416/), provides organisations with visibility around HEAT attacks that their network may have been exposed to over the past 30 days. This assessment tool analyses the company’s web traffic to determine the scale of HEAT exposure currently in their network and identifies the associated websites that were accessed.

The Menlo Security HEAT Analyzer provides organisations with a simple and effective way to perform a URL & category analysis of the visited websites. The HEAT Analyzer Report will highlight a customer’s exposure to HEAT attacks as well as the number of legacy URL reputation evasions, including click time mis-categorisations, specific categories serving up Legacy URL Reputation Evasion techniques (LUREs), as well as frequently seen domains.

How to Get the HEAT Security Assessment Toolkit
To get started using the Heat Security Assessment Toolkit and understand your susceptibility to HEAT attacks, please visit https://www.heatcheck.security/

The HEAT Analyzer app is available now on Splunkbase (https://splunkbase.splunk.com/app/6416/)

For a video demonstration of the HEAT Security Assessment Toolkit:
https://vimeo.com/721568134/17fb9bb97f.

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 (https://www.menlosecurity.com/customers/), including Fortune 500 companies, eight of the ten largest global financial services institutions, and large governmental institutions. The company 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:
Amanda Hassall, Consultant
Origin Comms

M: +44 (0)7855 359889
T: +44 (0)1628 822741
Amanda@origincomms.com