MENLO SECURITY

Tech Brief

Preventing Highly Evasive Adaptive Threats (HEAT) at the Initial Access of the MITRE ATT&CK Framework

Threat actors are constantly evolving their techniques to find the path of least resistance and gain a foothold into an organization to steal data and user credentials, or to demand a ransom. One of the many ways attackers are doing this is through web browser vulnerabilities.

Google has reported that knowledge workers spend an average of 75 percent of their workday using a web browser. The adoption of cloud applications and an increase in remote workforces has likely increased this figure, resulting in expanded attack surfaces and an increase of data that needs to be protected.

Given both the increase and proliferation of data, security professionals today have a monumental task of protecting users, no matter where they're located or what device they're working from.

To better understand how threat actors operate, many look to the MITRE ATT&CK framework, a knowledge base of cyberadversary behavior and taxonomy for adversarial actions across the attack life cycle. This framework is used to help companies understand the various components of the attack kill chain, so they can prioritize prevention, detection, and response measures.

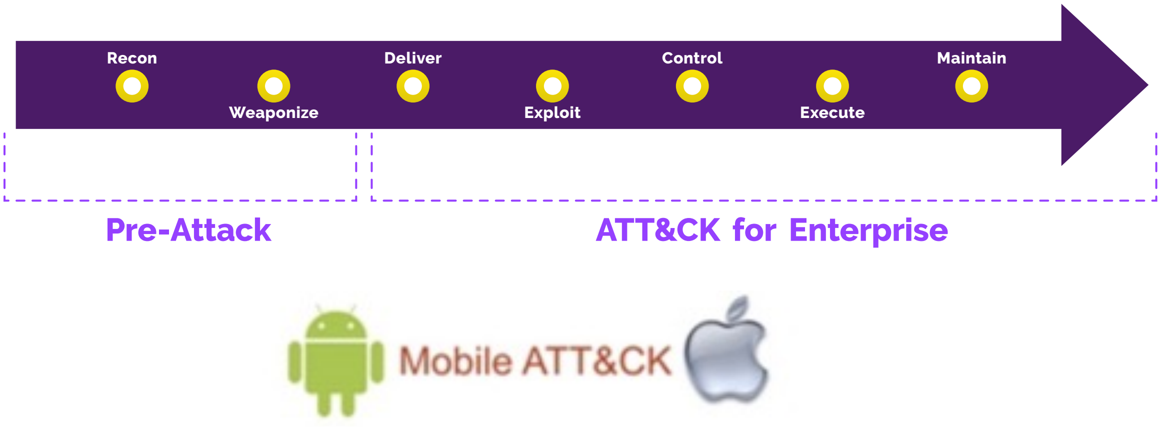


Figure 1: The MITRE ATT&CK framework is composed of three phases: Pre-ATT&CK, ATT&CK for Enterprise, and ATT&CK for Mobile
Source: https://nsfocusglobal.com/threat-model-attck/

The MITRE ATT&CK framework's Pre-ATT&CK — or Phase 1 — tactics include target selection, reconnaissance, and identification of open vulnerabilities and weaknesses within an organization. This includes testing and staging of various malware deliveries and phishing penetration.

Adversaries are taking a hands-on approach and targeting potential victims that are more vulnerable to attack based on their role, industry, or influence on others. Once an adversary has identified and observed their intended target, they will move on to Phase 2.

Phase 2 tactics are centered around the attack on the enterprise itself. These steps include initial access, execution, persistence, privilege escalation, defense evasion, credential access, discovery, lateral movement, collection, exfiltration, and command-and-control (C&C). In Phase 2, adversaries gain access to the enterprise's systems and information, spread laterally, and successfully execute their attack.

While multiple layers of security are important, initial access is the critical point for adversaries to be able to gain a foothold into an organization. This foothold can be used to download and serve malware to endpoints that can lead to ransomware.

Primary Attack Vectors and Highly Evasive Adaptive Threats (HEAT)

The two primary techniques used by adversaries to infiltrate enterprises through these initial access points are drive-by compromise and phishing, according to the MITRE ATT&CK framework.

Each of these techniques leverages Highly Evasive Adaptive Threat (HEAT) tactics to bypass traditional security defenses and pose significant risk to organizations. 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.

Drive-by compromise

In a drive-by compromise, adversaries compromise legitimate websites to gain access to a user's system. In this case, when a user visits a compromised website as part of a regular browsing session, their web browser is targeted and exploited simply by visiting the website. HEAT techniques used here include:

- **Legacy URL Reputation Evasion (LURE):**
  Here, attackers use seemingly benign ephemeral domains or compromise poorly defended websites to act as phishing sites or serve malware. This occurs before categorization engines have had time to properly categorize these websites.

- **Obfuscated, embedded JS files**
  Many legitimate websites today use obfuscation on their scripting so that sensitive data contained within it cannot get pulled out. Adversaries know this and naturally take advantage of it by obfuscating the JavaScript code and making it unreadable to detection engines in order to launch their malicious code once it is at the browser level.

- **Dynamic downloads via Blob:**
  Adversaries have been known to smuggle data and files past content filters by hiding malicious payloads inside of seemingly benign HTML files. These HTML files can store large binary objects, also known as JavaScript Blobs, that can later be constructed into file-like objects and deliver a malicious file on the end user's device that bypasses any security defenses in place. Data may also be stored in data URLs, which enable media types or MIME files to be embedded inline inside HTML files.

Phishing

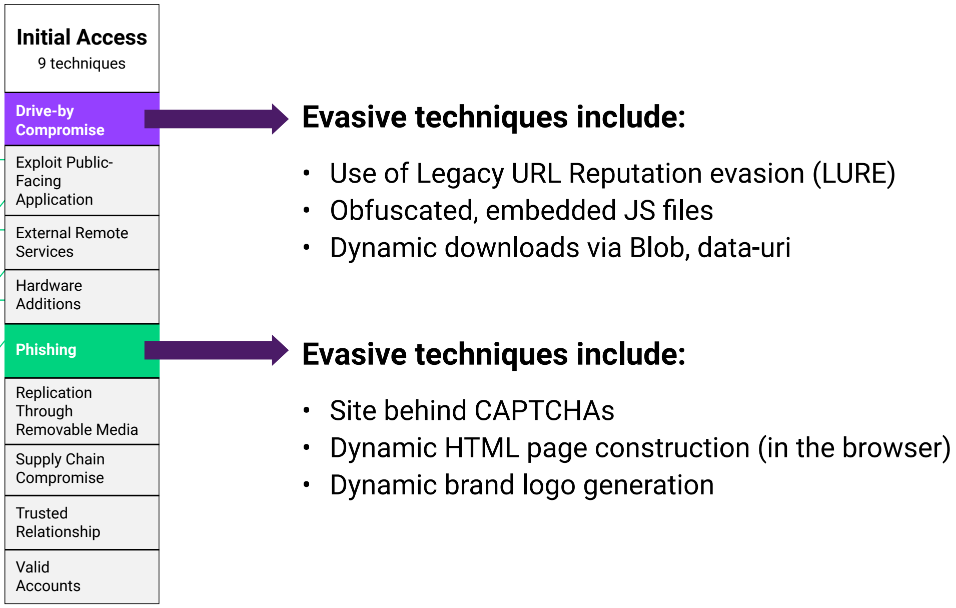
Then there's phishing. While many security teams are aware of phishing attacks, threat actors are shifting their tactics by not solely focusing on email as the vector. Instead, adversaries use various forms of website manipulation and spearphishing tactics via professional networks, collaboration tools, and SMS texting.

- **Site behind CAPTCHAs:**
  CAPTCHAs and phishing logos in various HEAT attacks are being used to make sites appear more legitimate to victims, evade offline web crawlers, or even deliver the malicious content itself.

- **Dynamic HTML page construction (in the browser:**
  HEAT attacks can also generate exploit code, crypto-mining code, or phishing kit code at the browser level to avoid detection from inspection engines that examine the source code of web pages. Attackers do this by obfuscating the JavaScript code to make it unreadable and launch malicious code at the browser level.

- **Dynamic brand logo generation:**
  Finally, attackers will also use website code manipulations to convert benign-looking images to images that impersonate known brands (such as Office365, Amazon, and PayPal) to bypass inspection engines that rely on visual detection for phishing purposes.

Though many organizations invest heavily in advanced detection and response technologies, most if not all still fail to prevent these HEAT attacks from compromising a user's credentials or stealing sensitive information.



Initial Access
9 techniques

Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Phishing
Replication Through Removable Media
Supply Chain Compromise
Trusted Relationship
Valid Accounts

Evasive techniques include:

- Use of Legacy URL Reputation evasion (LURE)
- Obfuscated, embedded JS files
- Dynamic downloads via Blob, data-uri

Evasive techniques include:

- Site behind CAPTCHAs
- Dynamic HTML page construction (in the browser)
- Dynamic brand logo generation

Traditional Secure Web Gateway (SWG), anti-virus, or sandbox solutions are designed to look for specific patterns, remote file requests, or signatures, but HEAT attacks bypass these technologies.

Stopping HEAT attacks at the point of initial access requires a preventative approach to security. This means organizations cannot rely on their existing solutions — such as AV, EDR, or XDR — to prevent HEAT attacks, as they're capable of detecting malicious activity only after it is already in the network.

HEAT Attacks Prompt Malware Payload Surge

Cloud infrastructure, remote workforces, and SaaS applications are all paving the way for adversaries to launch targeted attacks, including destructive ransomware campaigns. According to a survey report by CyberRisk Alliance's Business Intelligence Unit, 35 percent of the initial attack vectors for organizations successfully infected with ransomware were a result of Cloud Infrastructure as a Service (IaaS) or Platform as a Service (PaaS). Additionally, an analysis of over half a billion malicious URLs by the Menlo Labs research team revealed that 69 percent of those websites leveraged HEAT tactics. The team also observed more than a 224 percent increase in HEAT attacks being used to deliver sophisticated malware like ransomware over the second half of 2021.

With many security solutions available, why are ransomware attacks still so successful?

Simply put, because threat actors are creatures of habit, as long as those habits are effective. It's evident that detection and remediation solutions are not effective if they're not coupled with preventative technology. Ransomware will continue to surge if organizations struggle to keep up with their cloud security posture.

Preventing Initial Access

Preventing initial access requires focusing your security defenses on where the actual attack occurs – in this case, within the web browser.

Most companies still focus on faster detection and response technologies, even though these defenses detect HEAT attacks only after the endpoint is already infected and most likely compromised. Whether companies rely on file inspection performed by anti-virus software or sandboxes, malicious email link analysis, website categorizations, or even HTTP inspection engines, many traditional security stacks are rendered useless when dealing with HEAT attacks.

Protecting organizations against HEAT attacks begins with prevention. Organizations should look to the SASE framework to ensure that security and connectivity is applied closer to users, applications, and data, not just the network. This framework leverages a Zero Trust strategy to limit access to sensitive data, and grants permission only to those users who need access to certain systems or information. By incorporating this framework and investing in advanced anti-phishing and isolation capabilities, organizations can shift their security posture to a more preventative approach and help eliminate HEAT attacks.

MENLO
SECURITY

To find out more, contact us:

menlosecurity.com
(650) 695-0695
ask@menlosecurity.com

About Menlo Security

Menlo Security enables organizations to eliminate threats and fully protect productivity with a one-of-a-kind, isolation-powered cloud security platform. It's the only solution to deliver on the promise of cloud security—by providing the most secure Zero Trust approach to preventing malicious attacks; by making security invisible to end users while they work online; and by removing the operational burden for security teams. Now organizations can offer a safe online experience, empowering users to work without worry while they keep the business moving forward.

© 2022 Menlo Security, All Rights Reserved.