Bromium Use Case

Ransomware

Cybercriminals have turned to ransomware as the latest go-to tool for attacking and extorting businesses. Ransomware is typically delivered via email attachments or drive-by downloads from compromised websites. Once the user clicks on the attachment, the malware executes, proceeds to encrypt user files and issues a ransom message demanding payment for unencrypting the affected data. Some variants also traverse the organization, further locking down sensitive data.

WHY IT MATTERS

The success of ransomware campaigns such as Locky and TeslaCrypt, as well as the high profit margins that ransomware attacks yield, suggest that these attacks will continue to plague enterprises. Just one variant, CryptoWall, accounted for approximately $325 million in damages, according to a 2015 report by the Cyber Threat Alliance. New ransomware variants—accompanied by advanced evasion techniques—are introduced every day and traditional signature-based tools and threat detection solutions will never stop all ransomware attempts.

BROMIUM SOLUTION

Bromium uses CPU-enforced isolation—creating lightweight micro-virtual machines—that secure any untrusted tasks a user performs, such as clicking on a Web link or opening an email attachment. If a website or email attachment is malicious, the Bromium micro-VM isolates the malware—including zero-day ransomware seen for the first time—preventing the endpoint from being compromised.

KEY BENEFITS

- **Complete protection with no "detection gap."** Unlike other solutions that claim to stop 99% of threats, Bromium runs every untrusted user task in a CPU-enforced micro-VM
- **Protects unpatched endpoints.** No dependencies on browser, operating system or Java versions, vulnerabilities which are routinely exploited by ransomware variants.
- **Delivers full visibility.** Administrators can allow malware to run through the full attack cycle, providing complete attack context and visualization for forensics purposes.

HOW IT WORKS

1. An attacker will often leverage an exploit kit and a compromised website or craft a phishing email designed to infect users with ransomware. With file-based attacks, to increase the chances of the user opening the file, the attacker will typically package files in .Zip format with names containing words such as "internal," "invoice," "fax," or "statement."
2. If an unsuspecting user downloads the file and opens it, they'll find a malicious PDF or Microsoft Office document that, once opened, will proceed to infect their system with the ransomware.
3. On a Bromium-protected endpoint, however, the untrusted document is opened in a separate, isolated micro-VM with no network or desktop access.
4. When the user closes the document, any attempts by the ransomware to alter files, elevate privileges or move laterally, are automatically defeated, leaving files on the desktop system unchanged.

CUSTOMER SUCCESS STORY

Several users at a large financial services customer reported attacks after visiting legitimate business websites. These attacks exploited vulnerabilities in Internet Explorer and Adobe Flash. Upon successful exploitation, attackers downloaded and executed three different instances of crypto-ransomware. Because the endpoints were protected by Bromium, all threats were fully isolated with no impact to the endpoint systems. The complete attack chain and resulting artifacts were preserved for analysis.

Bromium®

For more information on Bromium Advanced Endpoint Security, contact your Bromium sales representative or email sales@bromium.com