Bromium Use Case

Spear Phishing

Spear phishing is an email spoofing fraud attempt that targets a specific organization, seeking unauthorized access to confidential data. Spear-phishing messages are designed to appear to originate from a trusted source—often from an individual in the recipient's own company—and are not typically initiated by random hackers. More likely they are conducted by highly motivated perpetrators out for financial gain or to steal intellectual property.

WHY IT MATTERS

Spear-phishing campaigns are the favored strategy for attackers looking to gain a foothold in an organization. Leveraging links to malicious URLs or weaponized document attachments, today's advanced, targeted spear-phishing attacks easily evade existing gateway Web and email filters, as well as endpoint defenses. User training is also elusive—according to the latest Verizon Data Breach Investigations Report, almost a third (30%) of phishing messages were opened in 2015.

BROMIUM SOLUTION

Each email attachment or Web link is opened in a CPU-enforced micro-virtual machine (micro-VM), ensuring that any malware is completely isolated from the endpoint hardware and underlying operating system.

KEY BENEFITS

- Users can click on anything without risk of breach, in the office or on the go.
- Endpoints are isolated and protected at all times.
- Users are protected without having to use different browsers or perform new workflows.
- No reliance on detection-based analysis or URL blacklist, which are easily evaded.

HOW IT WORKS

1. An attacker researches your organization and employees and carefully crafts a customized email that looks as if it came from a trusted sender on a relevant subject.
2. The attacker sends the email to a target employee or group of employees, inserting a malicious Web link or malware-laden attachment.
3. When the target employee opens the email, Bromium instantly opens the attachment or link in a lightweight CPU-enforced micro-virtual machine.
4. Malware that enters the micro-VM can't access vital data, the operating system of the protected endpoint, other applications or the corporate network.
5. When the user completes the task, the micro-VM is discarded, and along with it, any malware, either known or zero-day, that may be present. Spear-phishing attacks become a non-issue.

CUSTOMER SUCCESS STORY

An employee at a Bromium healthcare customer received an email masquerading as a legitimate communication regarding an invoicing task. Attached was a business-automation script for Excel spreadsheets. The document was in fact a weaponized Microsoft Excel document designed to install the Dridex Trojan on a user's system. Although this macro-based malware employed high-level obfuscation techniques and advanced evasion, Bromium isolated the threat preventing any damage while still recording each step of the attacker's activity for forensic purposes.

Br Bromium®

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