Solution Brief

CONTAIN PHISHING ATTACKS

SAFELY OPEN ANY LINK, EVEN IF IT'S MALICIOUS

ELIMINATE RESTRICTIVE IT SECURITY POLICIES THAT LIMIT USER ACCESS TO SHARED URLs

DEFEND AGAINST PHISHING LINKS WITH NATIVE BROWSER PERFORMANCE AND USABILITY

PHISHING LINKS CONTINUE TO SKIRT LAYERED DEFENSES

Despite advancements in anti-phishing techniques and employee training, phishing attacks are increasingly popular. That's because they work so well. After all, employees need to click on links to do their jobs, and social engineering makes phishing links difficult to identify.

Phishing links are particularly effective because malicious websites are numerous and short-lived. Their content changes frequently to avoid accurate categorization. This is compounded by employees who quickly click on links with little forethought, and leave their email and chat clients open, creating an instantaneous pathway for cybercriminals.

AN INEXPENSIVE AND EFFECTIVE WAY TO DELIVER MALICIOUS PAYLOADS

Malicious phishing links are constantly evolving and take many forms:

- Spear phishing: scams targeting individuals by including their names, roles, or work processes
- Whaling: aimed at company officers and often written as legal notices, customer complaints, or executive issues
- Social engineering: disguised as appeals to human nature's willingness to trust and be helpful
- Inadvertent infection: sharing news or social media links that have been compromised

Phishing attacks are executed in numerous ways:

- Phishing links in email messages
- Malicious links in benign email attachments
- Targeted links or messages on social media platforms
- Shared links in chat programs

HP SURE CLICK ENTERPRISE, POWERED BY BROMIUM, USES APPLICATION ISOLATION TO KEEP PHISHING THREATS AWAY FROM THE HOST

HP Sure Click Enterprise uses virtualization-based security to protect organizations from phishing threats by opening every shared link in a protected micro-VM browser tab.

Using hardware-enforced isolation, each browser tab runs in its own secure container, completely isolated from the host—and from all other browser tabs to prevent cross-contamination. Closing the browser tab terminates the micro-VM along with any threat. The full malware kill-chain is sent to the HP Sure Click Enterprise Controller and shared with all other HP Sure Click Enterprise devices on your network, further hardening the infrastructure and reducing the overall attack surface.

APPLICATION ISOLATION: PROTECT BEFORE YOU DETECT

Contain Phishing Threats

Open every link in an isolated micro-VM browser tab. If malware is served, it is contained, so the host and the network are not at risk. Employees can now click with confidence.

Streamline IT Security and Reduce Costs

Drastically reduce triage time and stop wasting resources on false positives with HP Sure Click Enterprise's high-fidelity alerts. Eliminate reimaging, rebuilds, and emergency patching.

Share Real-time Threat Intelligence

Adaptive intelligence identifies and stops evasive attacks, shares real-time threat data across your network, and delivers full kill-chain analysis to your SOC.

Achieve Lasting Protection with Hardware-enforced Security

Only HP Sure Click Enterprise uses virtualization-based security to deliver hardware-enforced application isolation. Protect against unknown threats and polymorphic malware that easily slip past even the most advanced detection tools.

92% of organizations train end-users to identify and avoid phishing attacks.

- Wombat Security[1]

Phishing tricks users to install C2 and keylogging software to capture credentials that are used to authenticate into, and exfiltrate data out of organizations.

- Verizon DBIR 2017[2]

Learn more at https://www.hp.com/enterprisesecurity

1. https://www.wombatsecurity.com/press/press-releases/annual-state-phish-report-wombat-security-showssimulated-phishing-and-training
2. http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/