Protect against phishing attacks and drive-by exploits

Phishing has become the weapon of choice for cyber criminals. Despite operating a full spectrum of email security solutions including anti-spam, anti-virus, data security, and encryption, enterprises continue to be impacted by targeted spear phishing which results in credential theft and malware exploits.

Legacy email security solutions rely on a ‘good vs. bad’ determination provided by third party data feeds, or internally via large-scale email traffic and data analysis. Because spear phishing attacks target specific individuals within an organization, the email link is usually unique, as is the target user. Therefore, no third party reputation data is available, nor is there enough data to analyze internally to make an accurate determination. If the determination is incorrect, the first targeted “patient-zero” individuals are sent directly to a site where credentials can be stolen, or malware can be downloaded to an endpoint. A single error can facilitate a costly and damaging cyber attack.

A new approach is required.

Highlights

• Eliminates drive-by exploits by isolating all email links
• Stops credential theft
• Reinforces phishing awareness training with real-time, customizable, and dynamic end-user education messages
• Simplifies security infrastructure, requires no end-point software or appliances, and easily integrates with existing mail server infrastructure

1. Can’t keep pace with millions of variants
2. Generates false positive/negatives
3. Complex infrastructure leaves vulnerabilities

1. Secure Web Gateway
   - Antivirus Signatures
   - IDS/IDP
   - Firewall
   - Network Sandbox
   - Big Data Analysis

2. Secure Email Gateway
   - MALICIOUS EMAIL
   - WEAPONIZED DOCUMENTS
   - INFECTED WEBSITES
   - WWW

3. MS EXCHANGE
   - USER
   - 12% CLICK

1. 12% of trained users still click on suspicious links or attachments*
2. No training ties to infrastructure security policies

*Verizon’s 2016 Data Breach Investigations Report

12%
MALICIOUS EMAIL
PHISHING
ALLOW OR BLOCK?
12%
MALICIOUS EMAIL
PHISHING
ALLOW OR BLOCK?
12%
MALICIOUS EMAIL
PHISHING
ALLOW OR BLOCK?
12%
MALICIOUS EMAIL
PHISHING
ALLOW OR BLOCK?
12%
MALICIOUS EMAIL
PHISHING
ALLOW OR BLOCK?
12%
MALICIOUS EMAIL
PHISHING
ALLOW OR BLOCK?
12%
MALICIOUS EMAIL
PHISHING
ALLOW OR BLOCK?
12%
MALICIOUS EMAIL
PHISHING
ALLOW OR BLOCK?
12%
MALICIOUS EMAIL
PHISHING
ALLOW OR BLOCK?
The Solution: Isolation

Menlo Security’s Phishing Isolation solution eliminates credential theft and drive-by exploits caused by email attacks. By integrating cloud-based Phishing Isolation with existing mail server infrastructure such as Exchange, Gmail, and Office 365, all email links can be transformed to pass through the Menlo Security Isolation Platform. When users click on an email link, they are 100% isolated from all malware threats, including ransomware. Websites can also be rendered in a read-only mode which prevents individuals from entering sensitive information into malicious web forms.

With their users safely isolated, administrators can monitor behavior statistics, and provide customizable time-of-click messages that help reinforce anti-phishing awareness training. Administrators can also define workflow policies for groups or individuals that determine if or when web input field restrictions can be relaxed. With zero dependency on on error-prone threat detection methods, such as data analytics, Menlo Security Phishing Isolation is the only email security solution that protects every email user the instant it’s deployed.

Phishing Stats-at-a-Glance:

- Phishing is the most common targeted method of cyber attacks\(^1\)
- Nearly 50% of users open emails and click on phishing links within the first hour\(^2\)
- 12% of users click on suspicious links or attachments despite training\(^3\)
- Increasing volume and sophistication of phishing attacks are resulting in downtime and direct financial fraud\(^3\)
- The main perpetrators for phishing attacks are organized crime syndicates and state-affiliated actors\(^3\)

\(^1\) Gartner’s Fighting Phishing: Optimize Your Defense (Published: 17 March 2016)
\(^2\) Verizon’s 2015 Data Breach Investigations Report
\(^3\) Verizon’s 2016 Data Breach Investigations Report

1. Eliminates drive-by exploits by isolating all email links
2. By opening all email links in safe isolation sessions, MSIP protects every user against targeted spear-phishing and drive-by exploits, thus eliminating “patient-zero” infections
3. Enables teachable moments
Phishing Isolation Key Benefits

- Protects against phishing and eliminates drive-by exploits through isolation of all email links. MSIP Phishing Isolation provides the industry’s only solution that delivers protection from credential theft, while eliminating 100% of drive-by malware exploits.

- By opening email links in safe isolation sessions, MSIP protects against targeted spear-phishing and drive-by exploits without relying on error-prone threat detection.

- Requires no end-point software or appliances, and easily integrates with existing mail server infrastructure. MSIP Phishing Isolation is the first cloud-based (public or private) solution with zero dependency on end-point software or appliances. It integrates easily with existing mail server infrastructure such as Exchange, Gmail, and Office 365.

- Provides user-behavior stats and customizable training reinforcement which enable teachable moments. Because web sessions pass through the isolation platform, MSIP Phishing Isolation can provide visibility into user behavior, helping administrators determine which users are clicking on potentially risky links. Even if users do click on malicious links, all sites are safely isolated and have input-field restrictions. Administrators can use this information to create teachable moments by providing configurable, real-time warning messages which offer additional corporate phishing-awareness training.
Summary

As phishing becomes an increasingly popular method for cyber criminals to distribute malware, the Menlo Security Isolation Platform (MSIP) provides the industry’s only Phishing Isolation solution delivers protection from credential theft, while eliminating 100% of drive-by malware exploits. MSIP Phishing Isolation uses web isolation to protect end users from malicious email links that can cause malware infections or lead to phishing sites. With this unique approach, users can safely view sites with input-field restrictions, while configurable messages provide additional corporate phishing awareness training. MSIP Phishing Isolation requires no end-point software or appliances and easily integrates with existing mail server infrastructure such as Exchange, Gmail, and Office 365.