Menlo Security

CASE STUDY

Fortune 50 Global Investment Firm Counters Phishing Threats With Isolation

Menlo Security Phishing Isolation closes the gaps in email security infrastructure

According to the 2016 Verizon Data Breach Report, on average, 30% of phishing messages are opened and nearly 12% went on to click on malicious attachments or links, despite extensive training. Gartner notes that increasing volume and sophistication of phishing attacks are resulting in real financial damage to organizations in both downtime and direct financial fraud.

Challenges

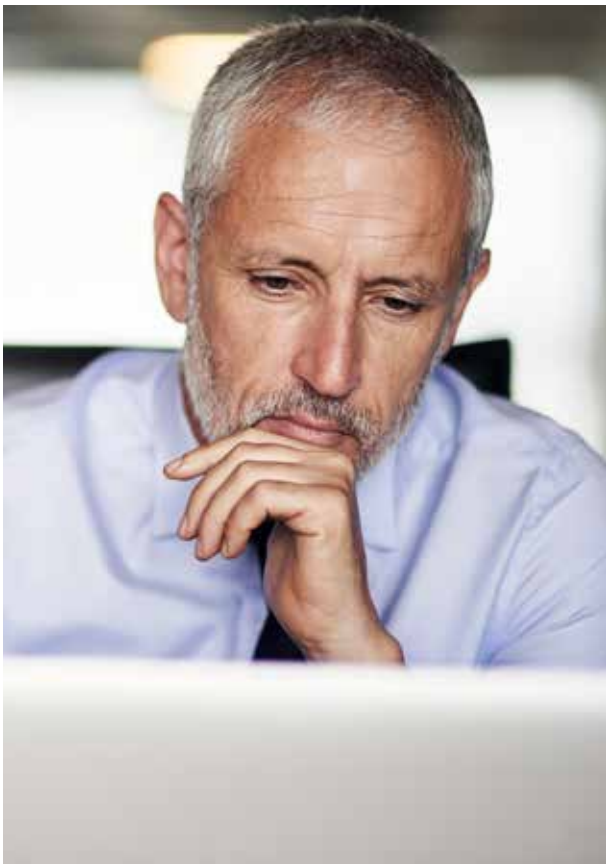
Despite operating a full spectrum of email security solutions including anti-spam, anti-virus, data security and encryption, targeted spear phishing resulted in ongoing credential theft and malware exploits. With stolen credentials in hand and malware successfully deployed, cyber criminals were able to launch sophisticated attacks on the network.

Solution

Integrating Menlo Security Phishing Isolation with their existing email infrastructure closed the security gaps by completely eliminating drive-by exploits and greatly diminishing the number of successful spear phishing attacks. Leveraging the Menlo Security Isolation Platform (MSIP), the firm executed all email links in the cloud, while providing its users a safe and educational experience.

Benefits

- Eliminates drive-by exploits by isolating email links
- Stops credential theft
- Reinforces phishing awareness training with real-time, customizable and dynamic end-user education messages
- Simplifies security infrastructure, requiring no end-point software or appliances, and easily integrates with existing mail server infrastructure
- Solution scales to isolate e-mail links and attachments in future deployment phases



The Pain Caused by Phishing

Serving millions of customers worldwide, this investment banking leader goes to great lengths to protect its trillions of dollars in assets. As a high-profile target for cyber criminals, nearly every aspect of its infrastructure is under constant attack. Email phishing attacks, in particular, were proving to be an increasingly serious threat. This is no surprise.

Despite multiple security defense layers and many hours and dollars spent on end-user training, phishing continues to be one of the most effective attack vectors for cyber criminals. According to the 2016 Verizon Data Breach Report, on average, 30% of phishing messages are opened and nearly 12% went on to click on malicious attachments or links, despite extensive training. Gartner notes that increasing volume and sophistication of phishing attacks are resulting in real financial damage to organizations in both downtime (such as "ransomware" attacks) and direct financial fraud (such as wire transfers)[1].

To combat email threats, the organization deployed multiple layers of security, each intended to address a specific part of the email security problem. Their architecture was similar to those of many other large enterprises, combining cloud and on-premises versions of anti-spam, anti-virus, data security, encryption, and sandboxing. Although these solutions are capable of defending against a broad variety of threats, they remain highly vulnerable to two of the most insidious attacks, spear phishing and drive-by malware exploits.

The spear phishing vulnerabilities stem from the fact that legacy email security solutions are largely based on reputation, that is whether an email link is known to be "good" or "bad". A link's reputation is determined via third party data feeds or internally by way of large-scale email traffic and data analysis.

In the case of spear phishing attacks, which target specific individuals within an organization, the email link is usually unique, as is the target user, hence there is no third party reputation data available, nor is there enough data to analyze internally to make an accurate determination. If the determination is incorrect, users 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 pervasive attack that can cause billions of dollars of damage.

This was precisely the pain the global investment firm was feeling.

[1] Fighting Phishing: Optimize Your Defense (Published: 17 March 2016)

A New Approach to Solving the Phishing Problem

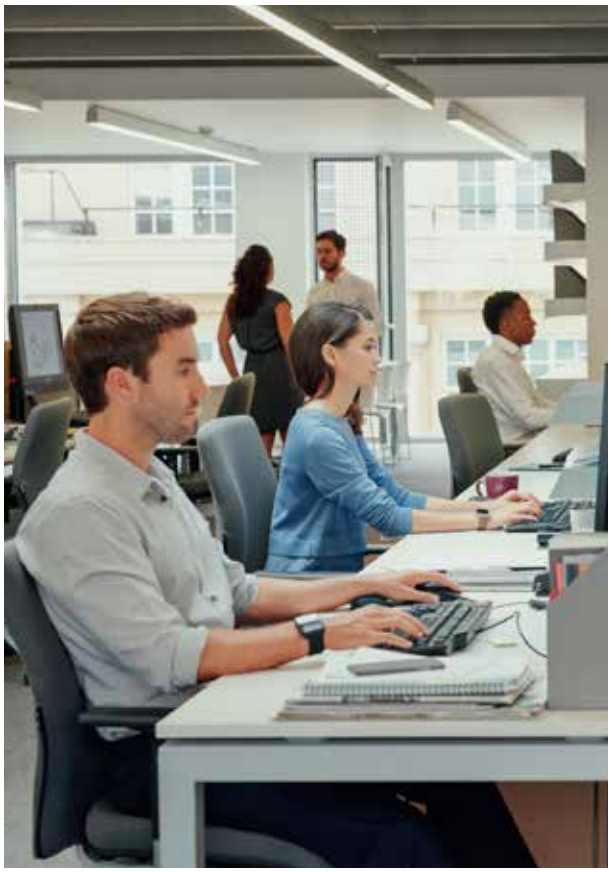
When the scope of the vulnerability became apparent, the IT team knew they needed an entirely new approach to solve their phishing problem. Having recently deployed the Menlo Security Isolation Platform (MSIP) to eliminate web-borne malware from uncategorized websites, the team was curious to learn how isolation could help bolster their email security infrastructure. They discovered that the Menlo Security Phishing Isolation service was able to address their needs and mitigate their vulnerabilities.

MSIP provides the industry's only Phishing Isolation solution that delivers protection from credential theft, while eliminating 100% of drive-by malware exploits. Menlo Security Phishing Isolation uses 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 they are provided information that helps them determine a site's legitimacy. This information is delivered via configurable messages which can 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.

Integration With a Corporate Phishing Awareness Campaign

As part of its ongoing war against phishing, the organization undertook a corporate-wide phishing awareness and training program, an effort given high priority and support by senior executives. With healthy funding and resources, the campaign included online training, testing, quick-reference cards, posters and more, all branded for consistent look and feel.

One advantage of the Menlo Security solution was its customizable nature. 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. When 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 warning messages at the time of click, which offer additional corporate phishing-awareness training. Administrators were not only able to reinforce corporate-wide policies, they were able to do it with tight alignment to the campaign brand. All campaign posters, videos, training, etc, had a common look and feel, as did the user messages being delivered by the latest component in their email security infrastructure.

Deploying the Technology in a Globally Distributed Enterprise

Menlo Security worked closely with the firm to develop a scalable architecture that would support hundreds of thousands of users across the globe. Integration with their existing Active Directory identity stores has allowed them to launch the service gradually, by provisioning role-based policies in a phased approach.

Because MSIP Phishing Isolation is the first cloud-based (public or private) solution with zero dependency on end-point software or appliances, deployment was simpler than other email solutions. It also integrated easily with existing mail server infrastructure such as Exchange, Gmail, and Office 365.

Problem Solved

By isolating all email links, Menlo Security Phishing Isolation provided the only solution that delivered protection from credential theft, while eliminating 100% of drive-by malware exploits. Because sessions pass through the isolation platform, Phishing Isolation provides visibility into user behavior, helping administrators determine which users are clicking on potentially risky links. When users do click on malicious links, all sites are safely isolated and have input-field restrictions. The firm's administrators are using this information to create teachable moments by providing configurable warning messages which offer additional corporate phishing-awareness training. For this financial institution, phishing isolation was the alternative they'd been looking for.

Menlo Security
934 Santa Cruz Avenue
Menlo Park, CA 94025
Tel: 650 614 1795
info@menlosecurity.com

menlosecurity.com