CYREN

A New Vision for Phishing Defense

White Paper — July 2022

A New Vision for Phishing Defense

Table of Contents

Introduction

According to a 2022 survey by Osterman Research, the majority of cybersecurity leaders do not have an effective ability to prevent business email compromise and phishing attacks from reaching employee inboxes. This is a practical assessment rather than a dire one. In response to the persistence of inbox threats, organizations provide frequent user security awareness training and have implemented processes for users to submit suspicious messages to their security operations center for analysis and incident response.

Despite these efforts, the frequency of breaches caused by email attacks continues to rise and the effort required by cybersecurity teams to prevent successful email attacks increases inkind. The latter is the hidden costs of phishing. Investigating suspicious email alerts, identifying confirmed threats, and cleaning up affected mailboxes costs businesses thousands of hours each year, causing stress and burnout for cybersecurity executives and analysts alike.

Percent of organizations using Microsoft 365 that reported one or more sucessful email attacks in 2022:

89%

"Phishing, BEC, and Ransomware Threats for Microsoft 365 Customers: 2022 Benchmarking Survey," Osterman Research

Businesses can lift this burden from users and cybersecurity teams. To optimize management of latent inbox threats, organizations need to continuously monitor mailboxes for malicious and suspicious content that has slipped past the email or network perimeter. This specialized and perpetual detection capability must be coupled with automated incident response so confirmed threats are quickly removed from users' mailboxes without the labor-intensive process of remediating malicious emails across the organization.

Adding detection capabilities at the inbox also creates a new opportunity to increase the effectiveness of user security awareness training. Rather than expecting users to individually fill the detection gap for these threats, this new approach uses machine learning and other detection frameworks to spot suspicious messages and alert users to potential threats. Armed with contextual information about suspicious indicators of an email, users are better equipped and more likely to apply their knowledge. The result is users are less involved in spotting threats but when the organization does require their help, it is a much more efficient process that reduces the volume of alerts, reduces the time it takes to respond to threats, and makes users less likely to fall for scams.

The Hidden Cost of Defense

The hidden cost of defending against credential phishing and business email compromise includes the hours spent administering and participating in security awareness training, reporting suspicious messages for analysis, analyzing suspicious email alerts, and preempting confirmed threats before they impact the organization. The magnitude of the cost is driven by the maturity of the people, processes, and technology involved. Inconsistent and manual processes combined with inadequate detection (low maturity) result in high cost while repeatable and automated processes with accurate detection capabilities (high maturity) result in low cost. As with any approach to risk management, it is critical that the cost of the defense is markedly lower than the cost of the risk.

False positive rate of user-submitted suspicious email alerts

41%

Osterman Research

Number of hours annually to analyze alerts per 1,000 users

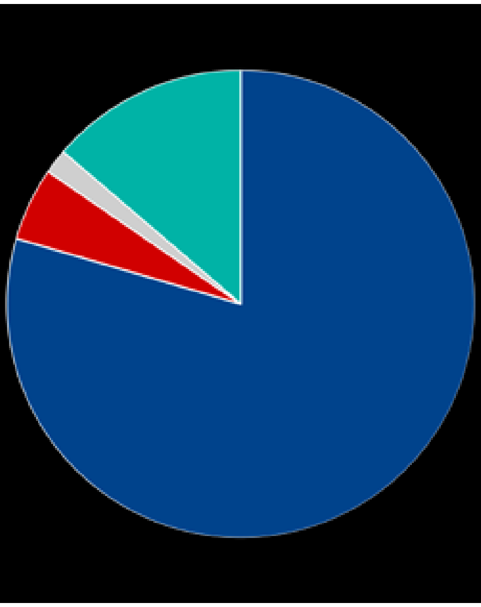
2,381

Cyren Calculator

There are also the human costs. Alert fatigue associated with targeted phishing and business email compromise is real. SOC analysts are overwhelmed with the volume of alerts from users, 41% which are false positives. It has been widely reported that alert fatigue leads to missed, ignored, or delayed responses. This, in turn, creates anxiety for Chief Information Security Officers and other executives held accountable for repelling threats like account takeover, financial fraud, and ransomware.

Phishing is a Leading Indicator

According to Cyren research, the majority of attacks that reach mailboxes are phishing (79%). Phishing is the likely precursor attack to other threats like account takeover and ransomware.



The Limits of Detection

No technology can detect all of the threats, all of the time, and with a low rate of false positives. Message content does not always neatly align with two classifications: clean or malicious. For example, Cyren Inbox Security incident data shows that 9% of confirmed threats cannot be detected at time of delivery to the user because of low-confidence classification or delayed detonation.

Classifying suspicious content as clean or malicious requires cooperation among detection engines, email users, and security analysts. Modern inbox security solutions apply adative banners that alert users to suspicious aspects of a message. This approach is an improvement over static banners like, “Caution: this email is from an external sender,” and allows users to apply lessons learned from security training in real-time and to potentially real threats.

When this kind of user engagement is coupled with processes that allow the user to enrich the incident and submit it to security analysts for investigation, it provides the final piece in an optimized defense against the full spectrum of inbox threats.

Integrated Cloud Email Security

A new way to maximize existing investments in email security is Integrated Cloud Email Security (ICES). By using the native APIs provided by cloud platforms like Microsoft 365, ICES is able to provide continuous monitoring, detection, and automated incident response capabilities for all mailboxes. This approach extends defense-in-depth with the secure email gateway or other email security filters like Microsoft 365 Defender and reduces reliance on employees to spot threats.

ICES can be deployed quickly and easily, using the native APIs provided by cloud email platforms. There is no need to change MX records or rip and replace an existing secure email gateway. The ICES platform should be extensible to support the business' needs as attack vectors evolve due to changes in the digital workplace. Initially, ICES platforms focus on filling the gaps left by legacy email security filters, but over time, this extensible nature of the ICES architecture will lend itself to other communication paths. This means organizations will reap the benefits of continuous monitoring, detection and response for all messaging threats. ICES also removes the burden on security analysts and email administrators by automating the remediation process and providing the tools required for in-depth forensic analysis, allowing a rapid response when new threats appear.

Essential Features of an ICES Solution

Essential ICES capabilities include:

CONTINUOUS SCANNING – *CATCHES EVASIVE AND DELAYED DETONATION THREATS*

Emails in all folders should be scanned on receipt, and after that, continuously, to spot zero-day and well-crafted attacks. A variety of techniques need to be applied to detect targeted phishing, impostor or spoofed emails, and account compromise. These should include: real-time fetching of URLs and other remote content, extensive header analysis; cousin or lookalike domain detection; lexical analysis searches for words and phrases that are indicative of social engineering attacks; and attempted impersonation of executives, customers or business partners.

USER EMPOWERMENT – *PROVIDES SMART BANNERS AND SELF-SERVICE TOOLS TO ACTIVATE SECURITY TRAINING*

A complete and effective ICES solution should give users an easy-to-use framework to help catch phishing emails and make informed decisions about how to respond to questionable messages. This framework should include adaptive warning banners and self-service tools that plug directly into the mail client for ease of use. The system should insert warning banners to alert users to suspicious messages and clearly indicate reasons the message is a potential threat. Users should also be able to perform on-demand security scans of messages they suspect are false negatives and submit them for professional analysis.

AUTOMATED REMEDIATION – *SAVES TIMES AND REDUCES EXPOSURE BY REMOVING ALL INCIDENTS OF AN ATTACK*

The time and effort required to manually remediate affected mailboxes is a massive drain on company resources, and often requires valuable operational staff to spend time doing a job they weren’t hired to do. ICES solutions need to lift this burden by automatically combing all instances of an attack into a single case, and eliminating it based on flexible remediation policies. Remediation policies might vary for different user groups based on risk levels.

MANAGED INCIDENT RESPONSE – *ENABLES FASTER INVESTIGATION AND RESOLUTION OF INCIDENTS*

Suspicious messages identified by detection engines and end-users require analysis from experts available 24x7x365. This includes responding to end-users with results of their reported messages to hone their skills and encourage continued participation. Post-incident forensic analysis is necessary to continually adapt and improve detection of novel tactics. Even businesses with robust security operation centers can benefit from outsourcing these tasks to specialized teams with global visibility of threats across many organizations and industries.

INTEROPERABLE – *PRESERVES EXISTING MAILFLOWS AND USER TRAINING PROGRAMS*

Securing the cloud email environment requires optimizing existing investments and efficiently closing gaps in detection and incident response. An ICES platform should transparently deploy without disrupting email security filters like Microsoft 365 Defender and security awareness training platforms. Email perimeter defenses and user education programs often refined over several years and are highly tailored for each organization.

Conclusion: The Inbox as a New Line of Defense

Secure email gateways were not architected to defend against today's sophisticated, evasive phishing attacks, and not all attacks can be prevented from reaching users. The perimeter email security a secure email gateway (SEG) or Microsoft 365 Defender provides is no longer enough. It's time to apply continuous security to the inbox that includes the best of machine detection, user training, security automation, and managed services.

The emerging technology area of ICES provides a new opportunity to protect organizations against evasive phishing attacks by deploying continuous email monitoring, detection, and response to create real defense-in-depth for email, complementing the initial defense offered by the SEG while automating rapid remediation and thus removing the burden on an organization's security response team. Email administrators and security personnel are further enabled with incident management workflows and true integration of the "wisdom of the crowd" from users and external security analysts, without impacting user productivity.

About Cyren

Cyren (NASDAQ: CYRN) protects more than a 1 billion users around the world from sophisticated and emerging email-, malware-, and web-based attacks every day. Our embedded threat detection, threat intelligence, and inbox security solutions help enterprises, service providers, and technology companies prevent breaches and eliminate countless hours of incident response time.