CYREN

A New Vision for Phishing Defense: Inbox Detection & Response

White Paper — February 2020

CYREN

A New Vision for Phishing Defense: Inbox Detection & Response

Table of Contents

INTRO: A NEW VISION FOR PHISHING DEFENSE 2

EVASIVE PHISHING IS BYPASSING TRADITIONAL DEFENSES 4

Phishing is Following the Malware Curve 5

THE LIMITATIONS OF CURRENT EMAIL SECURITY ARCHITECTURES 5

Time-of-Click Protection Is Not a Panacea 6

PHISHING DEFENSE-IN-DEPTH 7

ESSENTIAL FEATURES OF AN IDR SERVICE 8

CONCLUSION: THE INBOX AS A NEW LINE OF DEFENSE 10

Intro: A New Vision for Phishing Defense

Gartner's recommended adaptive security architecture that describes the concept of prevent-detect-respond-predict has been widely adopted in cybersecurity for years. But, until now, this framework has not been wholly applied to email security, which has historically focused on the prevention aspect delivered by a secure email gateway at the network perimeter.

Even in that single task, namely protecting against today's attacks, research data shows that this traditional email gateway security model is increasingly failing. In recent surveys by Osterman Research, 70 percent of IT security managers in general and 78 percent of Office 365 email administrators reported suffering security breaches in 2018, with email phishing attacks cited as the leading cause. A key reason these phishing attacks are able to bypass existing defenses is their increasing sophistication and growing use of detection evasion techniques. Use of such techniques has been made more pervasive by their inclusion in offerings from an increasingly robust phishing-as-a-service ecosystem that provides low-cost, high-quality and easy-to-use phishing campaign tools and services on the Dark Web.

Percent of organizations using Office 365 that reported one or more IT security breaches in 2019:

78%

"IT Security: Office 365 Benchmarking Survey," Osterman Research

To enhance security in the face of these phishing threats, organizations need to move from a gateway-based single-pass inspection model to a new layered security model that includes continuous email monitoring and detection. This new approach scans every message for threats and anomalous behaviours post-delivery and when a threat is identified, can automatically "claw back" suspicious messages from all impacted inboxes. This addresses a second shortcoming in the current email security model—the labor-intensive process of investigating, containing, responding to and remediating malicious emails across the organization.

Adding defensive capabilities at the inbox also presents a new opportunity to better leverage the "wisdom of the crowd" in an automated, structured way. In the old email security model, users haven't had real help in identifying potential threats and reporting suspicious emails to security teams, despite the resources poured into security training. This new email security model supports the incorporation of a lightweight add-in to the email client that gives users a way to flag any and all suspicious emails (not just spam) for on-demand, automated scanning. The scan results both enrich threat intelligence with forensic data, and are immediately shared with the users, who have a choice of next steps.

Finally, defenses should reinforce machine learning algorithms using the outputs captured by continuously scanning emails, monitoring user behaviors, and tracking URLs. Through analysis of this data, they can better detect anomalies and predict what the next threat might look like.

Evasive Phishing Is Bypassing Traditional Defenses

The inbox is a target, and no secure email gateway (SEG) will completely protect against today's email threats, which are more advanced and evasive than ever before. Phishing is an industry-wide problem due to the increasing speed at which phishing attacks occur, increasing sophistication in phishing techniques, and the rise of the "phishing-as-a-service" industry.

Researchers at Cyren are seeing a multitude of clever phishing attacks targeting business email, app, and system credentials. Once attackers gain access to a set of legitimate credentials, they can launch a multi-phase Business Email Compromise attack that uses the organization's own internal communications to listen, learn, and execute their end game. For instance, an attacker might target and then observe the inbox of a well-placed user to learn when an executive is going on vacation, what payments are coming due, and who is responsible for vendor payments, information that can be used to plan a convincing wire fraud attack.

Percent of phishing kits for sale on the dark web using at least one evasive technique to make detection more difficult:

87%

Cyren Security Lab

Percent of phishing kits targeting Microsoft Office 365 credentials:

25%

Cyren Security Lab

Increasingly common tactics to make detection more difficult include things like delayed activation, URL encoding to deceive phishing crawlers, HTML encryption (i.e., encrypting the phishing site with AES encryption), host and IP blocking, legitimate cloud service abuse, and other measures intended to block security systems from evaluating and seeing the true nature of a phishing site.

In addition, deeply technical phishing-as-a-service providers are making turn-key phishing campaigns that include these evasive techniques available to a wide audience of non-technical criminals.

Phishing is Following the Malware Curve

"Evasive malware" has a long history and is a term that has been in use for decades. The concept of evasive phishing is relatively recent, but is clearly following an evolutionary path similar to malware, with the use of evasive techniques becoming more common. Analysis by the Cyren Security Lab of malware sent to Cyren's cloud sandbox array showed that 99% of malware was using at least one detection evasion technique, and one breakdown of a single piece of malware found it used 29 different evasion techniques.

While Cyren researchers are yet to uncover phishing schemes that incorporate this level of technical misdirection, in a recent study they found that 87% of phishing kits for sale on the dark web come equipped with at least one technique intended to reduce the likelihood of detection.

The Limitations of Current Email Security Architectures

Secure email gateways (SEG) were designed to stop spam and malware before they reach an organization's mail server. They can do this quite well, especially when they include advanced detection capabilities, like inline sandboxing, and they support security protocols, like SPF, DKIM, and DMARC. Undoubtedly, SEGs are an important element in a defense-in-depth strategy.

However, even the best of SEGs do not deliver comprehensive email security and fail to block every malicious email. Considering the volume of email received by companies today, even low percentages of missed malicious emails translate into hundreds or thousands delivered monthly.

A SEG has just one chance to determine whether an email is clean before deciding to deliver it, delete it, or quarantine it. And once the SEG delivers an email containing a threat, the damage is done. It doesn't matter if the SEG is updated to protect against that particular threat in the future, because the threat is already active in the network.

Some types of SEGs tend to be difficult and time-consuming to configure. That in itself is a security risk because critical features may be overlooked or misconfigured, resulting in security gaps that will only come to light after an attack has succeeded.

Time-of-Click Protection Is Not a Panacea

Time-of-click protection gives the SEG one last chance to detect a phishing email that contains a URL, at a single point in time.

In the usual implementation, when a user clicks on the URL, the SEG looks it up in a database of known phishing sites. It typically does not perform real-time analysis of the content on the destination server.

Users are taught to look for suspicious URLs, but most time-of-click protection rewrites URLs—so to the average user, all protected URLs will look suspicious. The end result is a flood of false alerts that erode productivity and overload the support team.

As perimeter security, SEGs can deliver – but as every security professional understands, no defense will catch all threats. Even SEGs with advanced detection capabilities will have limitations in exposing account takeover attacks, spear phishing, cousin domain spoofing, and many unknown threats. Phishing emails are going to get through. Once that happens, the SEG cannot perform the necessary next steps of "detect, respond, predict." That leaves the targeted organization unable to defend itself against attacks it isn't even aware are in progress.

Phishing Defense-in-Depth

A new category of email security is emerging – Inbox Detection and Response (IDR). By using the native APIs provided by cloud platforms like Office 365, IDR is able to complete the full cycle of Gartner's adaptive security architecture. IDR provides continuous monitoring, detection, and incident management capabilities for all emails in the mailbox, adding phishing defense-in-depth to a SEG's first-scan "prevention" while completing the other missing elements of the security model, shown below.

IDR creates a feedback loop based on the outputs captured by continuously scanning emails, monitoring user behaviors, and tracking URLs, to reinforce machine learning algorithms. Through analysis of this data, organizations can better detect anomalies and predict what the next threat may look like. In addition, IDR can push intelligence to SEGs and other security assets, strengthening the organization's security posture as a whole.

The SEG remains as the first security layer, providing the cleanest pipes possible and protecting from known and many unknown threats.

Data collected through the framework is correlated to determine whether an email is malicious and remediation action should be taken. Incident and case management workflows help email admins and security analysts eliminate false positives and investigate, contain, respond to, and remediate threats.

IDR protects against new threats by scanning every email in every user's mailbox and rescanning when a new threat is discovered. It monitors behaviors and user interactions in the mailbox and identifies anomalies. It also provides a framework for users to interact with detection technologies, incorporating user feedback quickly and automatically to identify and protect against phishing attacks.

IDR can be deployed quickly and easily, using the native APIs provided by email platforms. There is no need to change MX records or rip and replace an existing SEG. The IDR platform should be extensible to support deployment of multiple security technologies. Initially, it will be focused on filling the gaps left by the SEG, but over time, this extensible nature will lend itself to providing integration of technologies often deployed elsewhere, such as sandboxing, anti-malware and DLP. This means organizations will reap the benefits of continuous monitoring, detection and response for all threats. IDR also removes the burden on security analysts and email admins 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 IDR Service

Essential IDR features include:

CONTINUOUS SCANNING – *CATCHES POTENTIAL PHISHING MESSAGES AFTER SEG PROCESSING*

Emails in all folders should be scanned on receipt, and after that, continuously, whenever a new threat is discovered.

ONGOING PROTECTION FROM NEW AND EVOLVING THREATS – *CATCHES NEW EVASIVE PHISHING THREATS IN SECONDS*

Speed of detection and time to protection is key, but some phishing threats can evade initial detection. Combining continuous monitoring with rapid speed of detection and automated remediation would allow an IDR solution to protect from new evasive phishing threats in seconds. When an email previously classified clean is later discovered to contain a threat, IDR should "claw back" the email, removing it from every mailbox across the business.

SENDER BEHAVIOR ANALYSIS – *PREVENTS TARGETED ATTACKS, SUCH AS BUSINESS EMAIL COMPROMISE*

A variety of techniques need to be applied to detect impostor or spoofed emails in the inbox. These should include: 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.

MAILBOX BEHAVIOURAL ANALYSIS – *EXPOSES SUSPICIOUS ACTIVITIES AND ACCOUNT TAKEOVER ATTACKS*

Mailbox behaviour analysis should profile mailboxes to create a baseline of trusted behaviors and relationships by feeding historical data, such as trusted senders and domains, numbers of emails sent and received in a given period, times emails are typically sent and received, etc., into machine learning models. Then mailboxes should be continuously monitored for anomalous behaviours and predictive analytics used to detect threats. User actions should also be analyzed and compared with others across the business to look for behaviors that indicate, in real-time, that an attack may be occurring.

URL BEHAVIOURAL ANALYSIS – *PREVENTS CREDENTIAL THEFT*

URL behavioural analysis should protect users from credential stealing phishing sites, which are often the first stage of an account takeover attack. Such a capability will analyze URLs extracted from emails for suspicious signs, follow them to their final destination, and examine the destination web page for evidence it may be a phishing site.

CROWD-SOURCED USER DETECTION – *PROVIDE SELF-SERVICE TOOLS FOR USERS TO PROTECT THEIR INBOXES*

A big benefit of an IDR solution should be to give users an easy-to-use framework to help catch phishing emails and make informed decisions about how to respond to questionable messages. This self-service tool plugs directly into the mail client for ease of use. Once a user submits a message for investigation, it can be automatically scanned and classified, which eases the burden of user support on the IT team.

INCIDENT MANAGEMENT – *ENABLES RAPID INVESTIGATION, CONTAINMENT, RESPONSE AND REMEDIATION*

An incident should be created whenever an email contravenes a policy or is reported by a user who requests an on-demand scan. An inbox security administration portal must provide incident and case management and workflow, and extensive IOC and forensics information be exported to a SIEM.

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 SEG provides is no longer enough. It's time to apply continuous security to the inbox, which can be considered the new perimeter.

The challenge for organizations is determining which threats are the most dangerous. The attacks that matter are those that are highly targeted. These tend to use detection evasion techniques, and the attackers behind them are quick to pivot to a new approach when a previous approach has failed.

The emerging technology area of IDR 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, without impacting user productivity.

About Cyren

More than 1.3 billion users around the world rely on Cyren's 100% cloud security solutions to protect them against cyber attacks and data loss every day. Powered by the world's largest security cloud, Cyren (NASDAQ: CYRN) delivers fast time-to-protection with award-winning email security, cloud sandboxing and DNS filtering services for business, and threat intelligence solutions for service providers and security vendors like Microsoft, Google and Check Point.