GreatHorn

WHITE PAPER

Combating Phishing with Modern Email Security

A Unique Approach to Protecting Enterprises Before, During, and After an Email-Borne Attack.

CONTENTS

INTRODUCTION

Many email-borne attacks, like spear phishing and business email compromise, rely on the pretexting of key employees in an organization. Cybercriminals are successful because they use psychological manipulation to trick users into making security mistakes or giving away sensitive information. If the phisher can gain the recipient's confidence and trust, then the attacker can swiftly extract information, commit fraud, or gain system access.

The types of email attacks that prey on human error present a unique challenge for organizations and the security solutions they rely on to protect them. The evolution of email threats from nuisance spam to sophisticated, targeted phishing campaigns calls for modern email security.

What makes a cloud email security platform modern? Simply put, it's the incorporation of multiple layers of defense—adaptive threat detection and blocking, integrated user education, and simplified email threat removal into a single platform for complete protection before, during, and after an email attack.

CONVENTIONAL vs. MODERN

CONVENTIONAL EMAIL SECURITY FOCUSES PRIMARILY ON PERIMETER DEFENSE CAPABILITIES—FLAGGING NUISANCE SPAM OR BLOCKING KNOWN "BAD" MALWARE SENT AS EMAIL ATTACHMENTS. IT'S TIME FOR A NEW APPROACH.

Just a couple of decades ago, viruses like *ILOVEYOU* and *Anna Kournikova* arrived spreading mostly via email. At this time, securing email was a relatively straight-forward endeavor. Security vendors needed to scan the content of inbound and outbound messages for viruses and telltale signs of spam. However, modern-day attacks like business email compromise (BEC) make securing email much more difficult.

BEC attacks don't typically rely on malicious attachments. They can linger for days, weeks, or months—comprising scores or hundreds of separate communications. Their content may be brief, conversational and familiar: hardly the kind of language that can be flagged without also generating staggering numbers of false positives. What's needed is a new approach to email security.

Modern email security that protects beyond known "bad" malware–one that encompasses adaptive threat detection and strict adherence to business processes designed to mitigate risk. Modern email security must also incorporate robust incident response tools and procedures that minimize the impact of the threats that evade detection. Ultimately, such an approach needs to be flexible enough to stave off evolving threats.

Anti-virus and anti-spam solutions have been around for decades, but the battle for email security is far from over. Indeed, email-borne threats are on the rise and are still amongst the most potent tools in an attacker's toolkit. Today, technology-dependent organizations face an expanding list of email-related threats. Nuisance spam and malicious email attachments now stand alongside targeted phishing attacks and CEO/executive impersonations. Even the most textbook attacks today use elements of localization and customization. For example, Microsoft has noted how a campaign that sent malicious attachments to small businesses in the U.S. used localization, making the message and attachment appear to come from well-known, local businesses to help trick email recipients to open the malicious email attachments.

To complicate matters, organizations are increasingly reliant on cloud-based platforms. Ideal for supporting a mobile workforce, such platforms offer little in the way of a corporate perimeter to defend and strain the ability of legacy security and monitoring tools. At the same time, compromises of cloud-based messaging platforms like Office 365 allow attackers to burrow deep inside an organization, gaining access to and exfiltrating reams of sensitive communications and data without notice.

Organizations need more than simple file scanning and border checks.

Present-day, email-based attacks require the application of adaptive threat intelligence and continuous monitoring of the entire email lifecycle–from message delivery to message deletion. Modern email security tools need to complement security user-awareness training and reinforce email security policies and business processes for handling confidential information in ways that better shape end-user behavior.

Now, the majority of email-based attacks use a combination of attack techniques. This infrastructure is what makes threat intelligence a critical component of modern email defense. Simple emails may provide a beachhead in an organization, but the malicious infrastructure is what allows attackers to expand and move laterally within organizations laying the groundwork for persistent attacks.

Modern email security solutions integrate multiple threat intelligence feeds that add a layer of protection: spotting emerging campaigns, flagging new malware variants and toolkits, and blocking suspicious and malicious domains that are part of command and control infrastructure. Today, threat intelligence no matter how up-to-date is not enough to effectively combat sophisticated phishing attacks.

Many of today's most widely-used email security tools rely heavily on threat intelligence, in some form, as the primary threat detection tactic yet, few vendors will admit it. Even the best threat intelligence is unlikely to spot phishing emails because they closely resemble legitimate email traffic and typically lack malicious links or attachments. By dialing up the sensitivity of email filtering and scanning features, administrators end up quarantining a great number of clean, legitimate messages. This can hamper business productivity and irritate employees/executives. It also places the burden of manually reviewing "false positives" caught up in an unwieldy net onto IT staff.

STRIKING A BALANCE

MODERN EMAIL SECURITY MOVES AWAY FROM A SIMPLE, PERIMETER-BASED DEFENSE BY STRIKING A BALANCE BETWEEN MULTIPLE LAYERS OF EMAIL THREAT DETECTION AND AUTOMATED RESPONSE ACTIONS.

Addressing both the philosophical and technological components of email security.

The challenges of most email security solutions have as much to do with a philosophical mindset as they do tactics. In particular, the over-reliance of threat intelligence is symptomatic of an antiquated, perimeter/gate mindset. Where the only role of email security is similar to that of an airport security agent: check everything that comes through against a predefined list of "bad" things and let everything that doesn't "match" through. In the case of airport screening, if something slips through the perimeter defense, recourse can be disruptive and potentially ineffective. The airport security staff may shut down a terminal (or the airport) or run manual security checks on people who have already cleared. The same is true for email security where so-called "incident response" is often limited to suspending accounts or using PowerShell scripts to identify email that is already in an employee's inbox.

Modern email security solutions strike a balance between combining multiple layers of email threat detection and automated response actions. Such an approach moves away from a simple, perimeter-based defense and toward a modern approach to email security. This approach tries to prevent the majority of email threats from reaching end users, while simultaneously protecting users and organizations from the email threats that do make it through.

This new approach involves two additional primary areas of consideration: user engagement protection and integrated incident response.

User Engagement

User engagement leverages and expands upon user education that originates from security awareness training. Studies have found that user awareness training is effective at conveying knowledge about email-borne threats like phishing and malware but is often ineffective at changing end-user behavior.

Modern email security complements the often compliance-driven awareness training with contextualized warnings/banners, business process development, and technology that help users make smart decisions.

For example, phishing awareness training may instruct users to check the email address of the sender and not simply rely on the sender name, which can easily be spoofed. However, such advice is often useless on a mobile device where it can be very difficult to look beyond the display name of an email.

Modern email security makes this easier by cautioning users when there is a disparity between the sending address and the supposed sender, flagging an otherwise "good" email (one that passes email authentication, etc.) as being different from the one usually used by the purported sender.

Taking these kinds of prompts one step further, modern email security can contextually reinforce business processes. For example, it may remind users looking at an email purporting to be from a top executive that wire transfers can't be authorized over email. The goal in all instances is to turn the users into security assets by providing in situ guidance and context for individual email messages.

Threat Remediation

When malicious or suspicious email messages are identified, organizations need tools and procedures to remediate that threat across their organization.

These could include quick, comprehensive threat identification and removal capabilities, insight into user engagement with newly identified threats (i.e. "User X spotted the phishing email. How many others received the same email? How many clicked the link?"), and so on. Each of these components should continuously inform the other stages in the cycle so that over time, security improves and naturally attunes itself to an organization's unique risk profile and tolerance.

Modern capabilities extend defenses to cover three primary classes of email threats.

As mentioned previously, traditional email threat detection relies on a combination of methods including IP and sender-based blacklists with heuristic analysis of message content to identify spam, phishing, and other undesirable content. Scanning of inbound email message content like URLs and attachments has provided a measure of protection against threats such as, malware, malicious "drive-by download" websites, and more. But, such detection methods can be easily bypassed, especially since the most sophisticated email attacks don't include attachments or links of any kind until an initial conversation has been started. So now we have the task of discerning phishing attacks from the normal course of business. A multilayered threat detection platform builds on existing email security features that spot "known-bad" messages and attachments.

Modern capabilities extend defenses to cover three primary classes of email threats: phishing patterns and techniques, communication patterns, and message fingerprints.

01

Phishing patterns and techniques

Advanced, machine learning tools can identify phishing emails by identifying evidence of common patterns and techniques that distinguish a phishing email from legitimate correspondence.

For example, for internal communications, does the display name in the email match that of a legitimate employee? Does the sending domain match your organization's or that of a popular application? Conversely, is there evidence of typosquatting, IDN homograph attacks and so on?

02

Communication patterns

Does the recipient for this message have a history of corresponding with this sender? Has the sending account sent other messages to individuals within the receiving organization? What do those patterns of email communication look like? How does this exchange compare to those earlier exchanges?

03

Message fingerprints

How does the email authentication like Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting & Conformance (DMARC) for this message compare to what we typically see from this domain?

In other words, modern email security addresses the larger challenge by combining threat detection techniques to flag suspicious or malicious email, even in the absence of a malicious attachment or suspicious email metadata.

ORGANIZATIONS WHO STRUGGLE TO CONTAIN EMAIL-BASED THREATS WOULD SIGNIFICANTLY BENEFIT FROM MODERN EMAIL SECURITY.

For example, email sender address spoofing is still one of the most common techniques used by attackers. To thwart such attacks, effective email security tools need to be able to identify whether the sender name that appears in the email and email address in the 'From' line match each other. Beyond that, it is extremely useful to know whether they are in line with what we've seen from this sender before. Any discrepancies should be flagged, providing warning and context to the recipient even when the message is not blocked outright. The recipient would have been warned and would be on guard for a scam. Such contextualized warnings are more effective than the indiscriminate, universal warnings (prefacing subject lines with "EXTERNAL" for example) that quickly become mundane and are then ignored by end users.

Advancements in machine learning technology, enable some email security tools to analyze both an individual message and prior communications from the sender and sending organization. When each new message is evaluated against expected communication patterns, atypical or suspicious email messages that deviate from past behavior jump out. Perhaps the sender has never before mentioned wire transfers. Or maybe the email uses an anomalous return path unlike anything prior from that sender and sending domain. Such clues are easy to spot using machine analysis but almost impossible for humans to uncover—especially at scale.

It's no secret that threat actors are constantly evolving and email detection capabilities need to as well. But, emergent threat detection and automated threat correlation capabilities, powered by machine learning technology, can monitor the latest threats and attack profiles across industries, while keeping track of malicious command and control infrastructure. Such approaches can stop emergent phishing, watering hole, and email-borne attacks in their tracks.

BUILDING ON AWARENESS

SECURITY AWARENESS TRAINING ALONE DOES NOT GUARANTEE YOUR EMPLOYEES WILL MAKE THE RIGHT DECISION WHEN PRESENTED WITH A REAL-LIFE PHISHING ATTEMPT.

Today, most sophisticated attacks hinge on social engineering techniques that fool your employees.

This is why detection features that can spot phishing attacks and build on user-awareness training are every bit as important as the raw scanning and detection capabilities.

Beyond that, however, organizations need to understand their biggest risks and exposures and operationalize email security throughout their organization. Email isn't just used to launch attacks on victim organizations. It is also a favored avenue for stealing data and intellectual property from compromised firms. Organizations need to identify sensitive stored data on their networks and develop (and enforce) business processes that dictate how such information is shared and communicated—both internally and externally. Establishing such processes and coupling them with contextual reminders helps to ensure adherence to corporate information security policies.

In recent years, countless firms have stepped in to offer user awareness training for organizations. While useful, training is too often isolated and disconnected from the day-to-day activities of users. Despite its significance, security awareness training alone does not guarantee your employees will make the right decision when presented with a real-life phishing attempt.

Raising red flags: Modern email security enhances the value of security awareness training by providing automatic and "in the moment of risk" feedback.

Contextual, threat-specific banner messages, highlighted text, sandboxed links with warning pages, and other visual prompts warn end-users before they interact with the message content.

Such features close the loop on security awareness training: using prompts in context to call end-users' attention to features of an email exchange that are concerning, and then leaving it to them to apply the knowledge that they have at the point of interaction. For example, messages with links to infrastructure that has been involved in prior attacks might contain a warning that the threat detection engine finds the message suspicious and why. By raising the red flag with the recipient, a damaging outcome (clicking on the suspicious link) might be avoided, while false positives can be disregarded.

Similarly, modern email security can help your organization reinforce critical secure business processes.

Business email compromise attacks often target lax business processes around money and data transfers, to the benefit of cybercriminals.

Modern email security can reinforce secure business processes with reminders to users that key off of message content, subject lines and so on. For example, email messages discussing wire transfers, the transmission of W-2 forms, or other personally identifying information can trigger "in the moment of risk" banner messages and other queues to remind your users about company policies requiring a phone or in-person authorization for such actions. Those warnings can prompt out of band communications that can quickly expose the ruse.

INTEGRATED RESPONSE

NO SECURITY SOLUTION WILL PREVENT 100% OF THREATS. SO, MODERN EMAIL SECURITY NEEDS TO EXTEND WELL BEYOND SCANNING AND DETECTION TO ENCOMPASS INCIDENT RESPONSE.

In cases where a malicious threat slips by initial scanning, modern email security should also be engineered to make it easier for security staff to investigate those incidents and remediate any threat they pose.

It is rare for email-based attacks to target just one person within an organization. In the event of a compromise, targeted firms want to understand the full scope of a malicious campaign. That's why incident response is a critical component of modern email security.

Threat intelligence capabilities applied to email traffic can enhance your security team's ability to do incident response. For example, identifying users throughout an organization who have clicked on suspicious or known malicious links early is critical when isolating and remediating attacks.

However, such capabilities are not often part of email security platforms. Even today, incident response might fall to security staff using custom scripts or third-party tools to determine which employees have interacted with a specific threat. Identifying victims and targets can take anywhere from several minutes to several hours depending on the scope of the attack and the size of the organization. Even then, an incident response team still must remediate the threat by resetting passwords, isolating compromised systems, and removing malicious installs. And, without clear data on who has interacted with the threat, these disruptive remediation steps are often performed on anyone who came into contact with a malicious message, regardless of their behavior.

Such a brute force approach results in significant and unnecessary business disruption for employees who received but did not respond to the attack. At larger organizations, these disruptive manual investigations and remediation measures keep the window of exposure to new threats open longer.

The alternative? Modern email security platforms that allow you to query your environment using a wide range of indicators. These include the sender, recipient, return path, and IP address. By querying identifiable information like the URL that appeared in a successful email phishing attack or the name of a file attachment, IT staff can quickly determine who received the message within their organization and, if necessary, recall offending messages directly from victims' email inboxes with the click of a button, eliminating the chance of exposure.

EVALUATION MUST-HAVES

EMAIL CONTINUES TO BE THE #1 ATTACK VECTOR. TARGETED PHISHING AND SOCIAL ENGINEERING ATTACKS ARE INCREASING IN THEIR SOPHISTICATION AND EFFECTIVENESS.

When evaluating email security solutions, remember to keep in mind the following features.

Email security isn't merely "basic blocking and tackling" for your enterprise. These days, email-based threats including malicious links, attachments, spear phishing campaigns, and business email compromise are among the most-used tools of sophisticated cybercriminal groups and nation-state actors.

These attacks, which often go unnoticed, can be stepping stones to much larger and more serious compromises of your network that include unauthorized money transfers, credential theft, and even the destruction of key systems and data.

The growing sophistication of email threats demands a new approach to email security. Legacy email threat detection platforms that merely scan inbound messages for spam and malicious attachments are blind to stealthy, "low and slow" attacks like business email compromise.

When evaluating email security solutions, keep the following features in mind:

Adaptive Threat Detection, Contextual Cues "In the Moment of Risk," and Integrated Incident Response.

Adaptive Threat Detection

Your email security solution should offer superior and dynamic detection of both known and emerging threats. The recent emergence of ransomware has raised the stakes for detecting malicious software before it has a chance to spread in your environment. Take a close look at your vendor's threat detection capabilities and ask about how it handles new and emerging threats or whether it supports the signature-less detection of generic threats.

Malware like wipers and remote access trojans (RATs) are just one aspect of email security. Your email security should also leverage threat intelligence to get a jump on emerging command and control (C2) infrastructure, suspect senders, spear phishing campaigns and other targeted campaigns. Make sure your email security platform is informed by robust threat intelligence.

Contextual Cues "In the Moment of Risk"

Many inbound messages fall into a gray area between "clean" and "suspicious." This is why arming your employees with the proper threat awareness and education is vital. Your email security software should reinforce those lessons: helping to highlight suspicious elements of messages in ways that allow the end user to make the best decision about whether a given message is suspicious or legitimate.

Integrated Incident Response

Attackers are likely to target more than one individual inside your organization and execute multiple avenues of attack. Detecting and deleting new threats is just the first step in protecting your organization. Your email security platform should also provide you with robust incident response features that let you build out from any detection to quickly remediate similar threats across your messaging infrastructure. If wider investigations are warranted, your messaging platform should provide the tools to do robust incident response to email-borne threats and attacks.

GreatHorn protects organizations from more advanced threats than any other email security platform. By combining its highly sophisticated threat detection engine with accessible user context tools and integrated incident response capabilities, GreatHorn Email Security shields businesses from both sophisticated phishing attacks and fast-moving zero-day threats, freeing security teams from the tedium of email security management while enabling them to respond to genuine threats faster than ever before.

By combining deep relationship analytics with continuously evolving user and organizational profiling, GreatHorn's cloud-native email security platform provides adaptive, anomaly-based threat detection that secures email from malware, ransomware, executive impersonations, credential theft attempts, business services spoofing, and other social engineering-based phishing attacks.