AREA 1

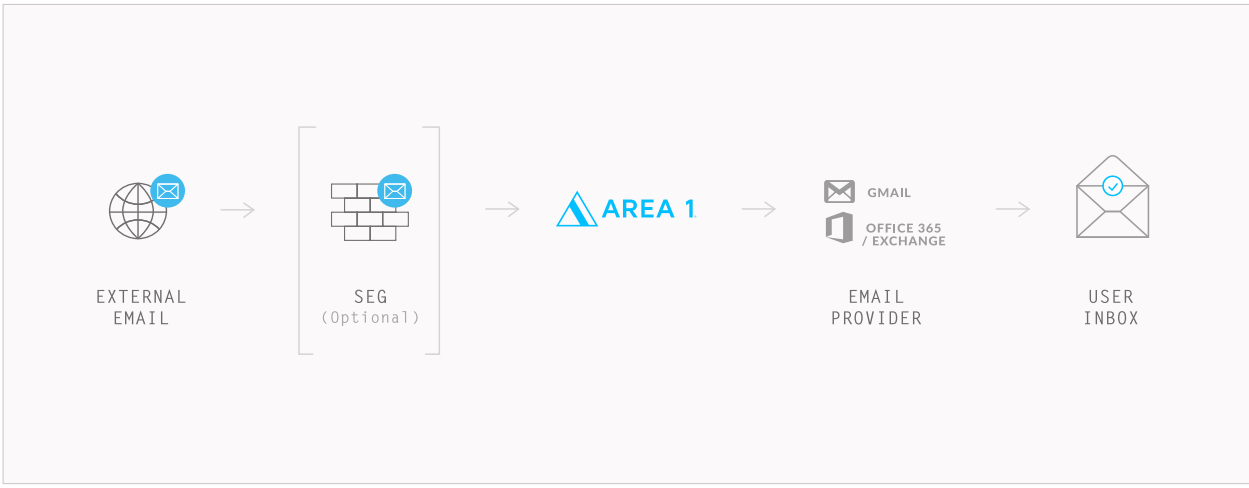
THE STORY BEHIND 140,000 MISSED PHISH

PHISHING: TOP THREATS MISSED BY EXISTING DEFENSES

140,000 Reasons to Rethink Phishing Defense

Customers deploy Area 1 Security behind -- or as a more capable replacement for -- secure email gateways (SEGs) such as Cisco IronPort, MessageLabs, Mimecast, Barracuda, Trend Micro or Proofpoint. And they only pay for the phish we catch, that their current defenses miss.

FIGURE 1



This annual report provides answers to two key questions that organizations using secure email gateways frequently ask: What type of phishing threats do SEGs miss? And how can we be more effective at blocking phishing attacks? The report reviews Area 1 detection data for a sample of customers that deploy our service as the critical security layer behind their SEG to detect and stop phishing email, and explains why the Area 1 service is more effective at blocking phishing attacks than any SEG.

Over a recent four-month period, the Area 1 service analyzed over 825 million emails for these customers ***and caught nearly 140,000 phishing emails missed by their SEGs.***

For a typical company with 10,000 employee inboxes, ***that equates to over 2,000 phishing emails missed every month by SEGs and stopped by Area 1***. These emails would otherwise land in employee inboxes, bringing Business Email Compromise fraud, credential

140,000 REASONS TO RETHINK PHISHING DEFENSE – *Continued*

harvesting, malware, ransomware and other attacks that tie up security team resources with incident investigation and remediation.

This matters, because phishing attacks are the root cause of over 90 percent of cyber breaches responsible for catastrophic financial loss, data theft, and brand damage.

By analyzing the Area 1 detection results for these phishing emails, we've identified the types of malicious phish that SEGs most often miss (Fig. 2) and Area 1 detects.

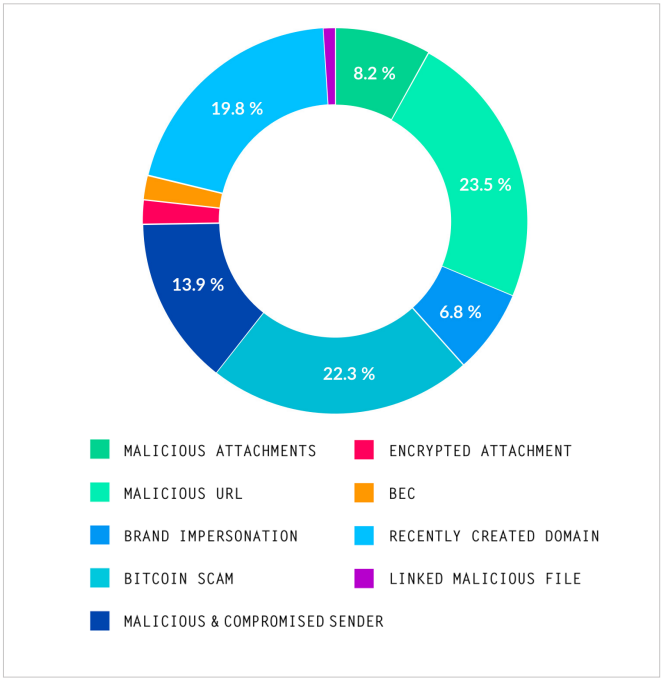


FIGURE 2

Malicious URLs

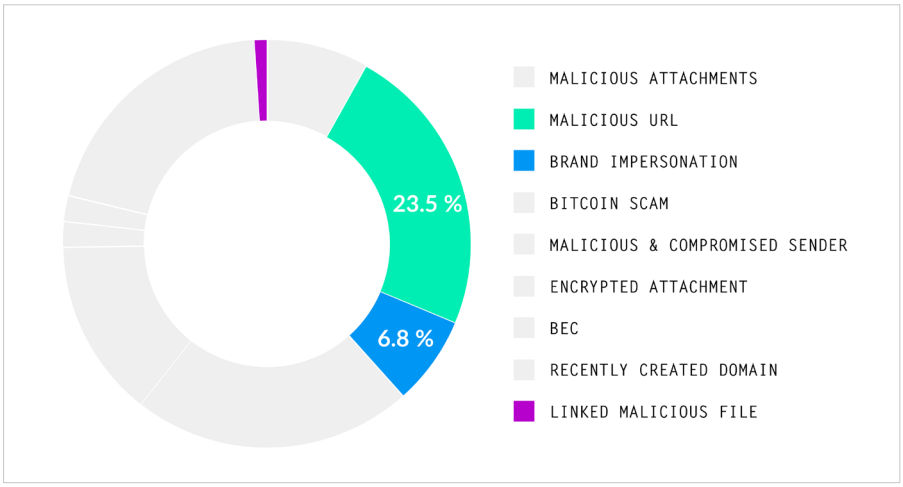


FIGURE 3

The largest category of malicious phish that SEGs miss is phish containing malicious URLs (Fig. 3).

In this analysis, ***23.5 percent*** of phish detected by Area 1 contained malicious URLs; and 6.8 percent of phish spoofed trusted brands,

MALICIOUS URLs – *Continued*

often with links to credential-harvesting sites or malicious files.

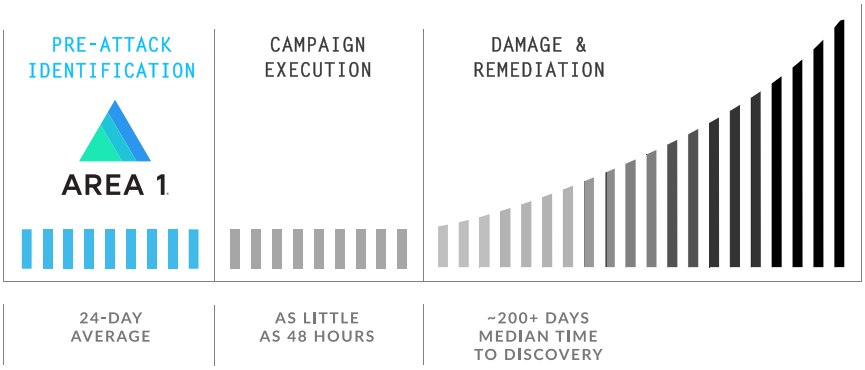
Emails containing links to malicious sites are a tactic used in a number of phishing attack types including credential harvesting, wateringhole, malvertising, and scripting attacks, to name a few. These attacks often start with phishing emails containing a socially engineered call-to-action URL that, when clicked, will open a site or file that implants malware or opens a login or information submission webpage.

The webpage enables theft of sensitive data such as account credentials or payment information.

Area 1 uses a number of techniques to detect malicious links, including proactive web-crawling, advanced email analysis techniques, instant crawling of links and proprietary machine-learning classifiers. The Area 1 technology fully follows URL redirections to the final destination, expanding shortened URLs and inspecting URLs buried in attachments.

PROACTIVE WEB CRAWLING DISCOVERS UNKNOWN MALICIOUS LINKS

Area 1 is the only cybersecurity company that continuously crawls the web to proactively identify phishing infrastructure before campaigns launch, detecting malicious URLs, domains, IPs, accounts, and payloads, on average discovering malicious infrastructure 24 days ahead of industry benchmarks, such as VirusTotal. Just as Google indexes commerce and content, **Area 1 indexes the entire web — 8 billion pages and 220 million top-level domains (TLDs) every two weeks** — with the largest Web-crawling capability ever built focused purely on discovering attacks and identifying campaigns.



DETECTING PREVIOUSLY UNKNOWN MALICIOUS LINKS WITH PROPRIETARY MACHINE LEARNING CLASSIFIERS

In addition to using proactive Web crawling to detect malicious links, the Area 1 anti-phishing service also uses proprietary machine-learning classifiers to analyze links in customer emails and detect previously unknown malicious links.

The service scans inbound emails for links, both in the body of an email and in files attached to an email. If a link is discovered that is unknown, sophisticated ML classifiers, which combine URL pattern analysis and other factors, are used to analyze the link and predict whether or not the link is malicious.

As an example (Fig. 4), a customer received an email that appeared to be from Chase bank, requesting account information be updated. The email was scanned by a Proofpoint SEG and judged benign. Area 1 then scanned the email, and identified that the sending domain spoofed the Chase brand and included a link that redirected to a fake Chase login page. The email was judged malicious by Area 1, blocked from delivery, and the end user was protected from a credential-harvesting site.

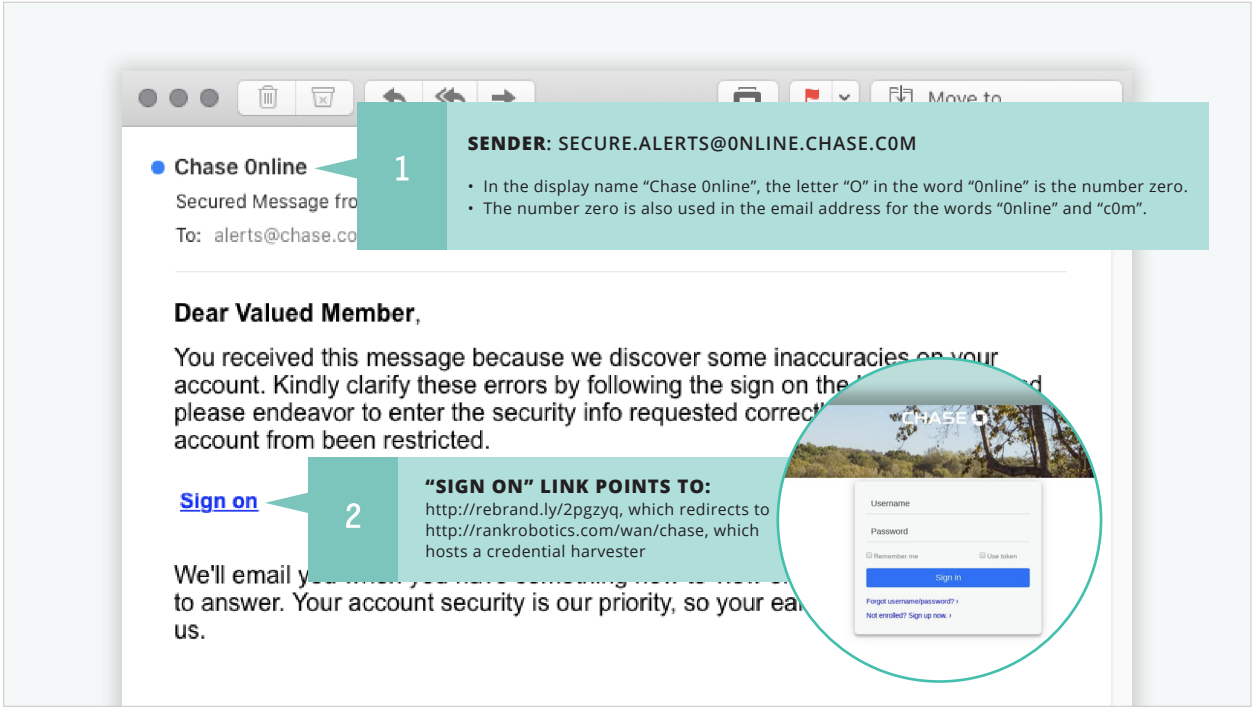


FIGURE 4

DETECTING MALICIOUS LINKED FILES WITH INSTANT CRAWL AND MACHINE-LEARNING CLASSIFIERS

In another case, a customer received an email with a link to a proposal from a vendor. The email was scanned by the customer's Symantec MessageLabs SEG, judged benign and released for delivery (Fig. 5).

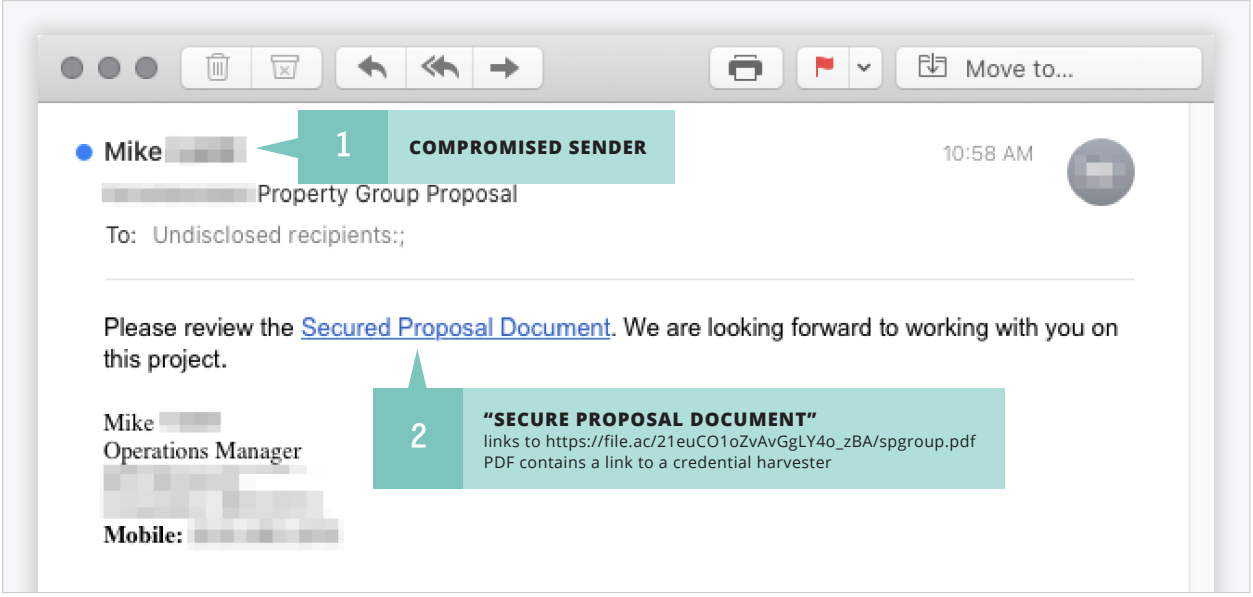


FIGURE 5

The Area 1 Horizon anti-phishing service then scanned the email and detected a suspicious link. The service crawled the link, analyzed the linked file and discovered a malicious link in the file. The email was judged malicious and blocked from delivery to the recipient's inbox, protecting the user from clicking on a malicious link to a credential harvesting site.

ADVANCED ANALYSIS TECHNIQUES DETECT BRAND IMPERSONATION EMAILS

SEGs are often challenged to defend against brand impersonation emails. With these attacks, threat actors craft emails that appear to be sent from trusted brands, but are in fact spoofed, and most include malicious links or attachments. In addition to the techniques discussed in the sections above for detecting

ADVANCED ANALYSIS TECHNIQUES DETECT BRAND IMPERSONATION EMAILS – *Continued*

malicious domains and links, Area 1 uses additional advanced techniques to identify brand impersonation phishing attacks. For example, Area 1 technology detects brand references and visual brand assets (e.g., logos) on domains or URLs using computer vision techniques. The Area 1 service then applies real-time infrastructure correlation to detect imposter sites. The service also detects the presence of credential-gathering forms on domains or URLs associated with commonly used brands but not hosted on typical IP address spaces associated with said brands.

As an example, a customer received an email that appeared to be from Square requesting the customer click on a link to submit supporting details for a payment dispute (Fig. 6).

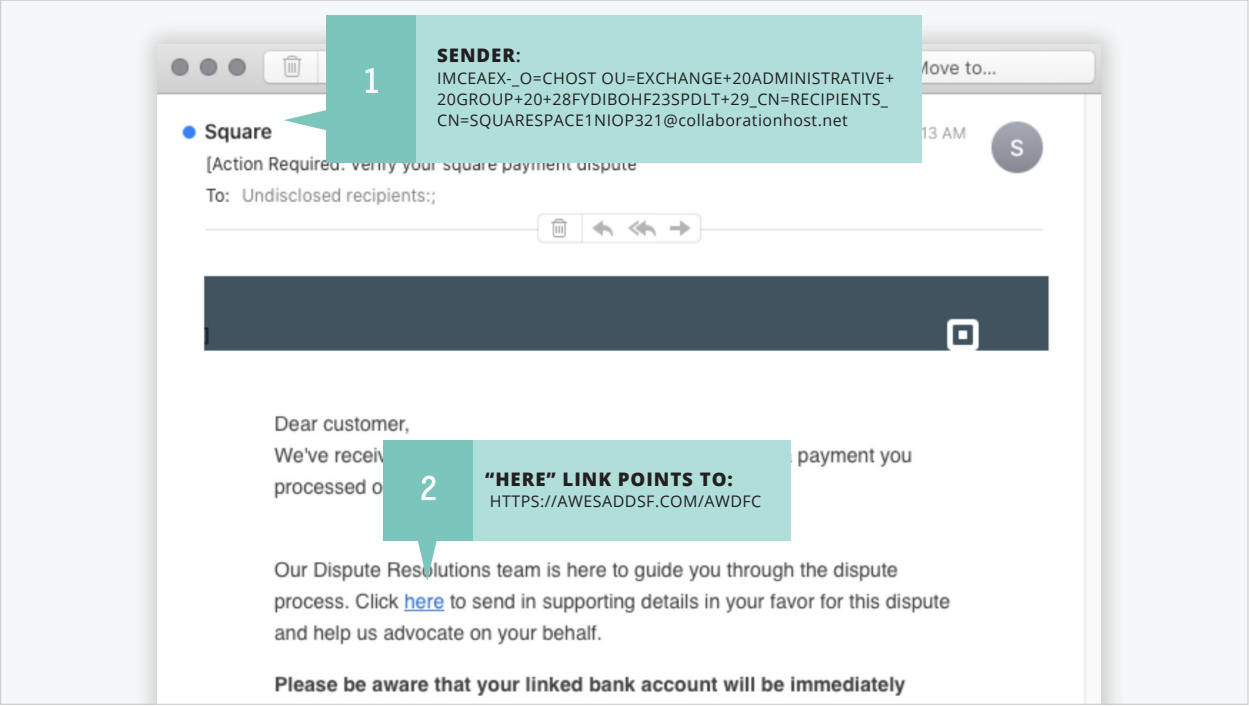


FIGURE 6

The email was scanned by the customer's Symantec MessageLabs SEG defenses and judged benign. The email was then scanned by Area 1; because the sending address and link were recognized as not originating from infrastructure associated with the Square brand, Area 1 judged the email to be malicious and blocked it from delivery.

Phishing with Fear - Bitcoin Phish

"Trust me."

Cybercrime has relied on this calling card of trust for years to engage with its victims: "Click on this link to login and renew your account." "Download the attached document and pay your invoice." Traditionally, threat actors have socially engineered their emails and phishing websites cleverly to win trust and steal credentials and account information or infect victim systems with malware.

However, we've seen a new and growing trend in cyber threats. Rather than "Trust me," the calling card of cybercrime is increasingly "Fear me -- and pay me, or else." That's extortion—and we're seeing a steady increase in these "phishing with fear" campaigns. In this analysis, we found that ***22.3 percent*** of the attacks that we caught that bypass SEGs were Bitcoin phish. Why?

Cybercriminals are finding that scareware is an easy way to make a fortune: Phishing emails demand payment in Bitcoin and threaten data destruction, or perhaps the release of an embarrassing video, or even physical violence if a demand is not met (Fig. 7).

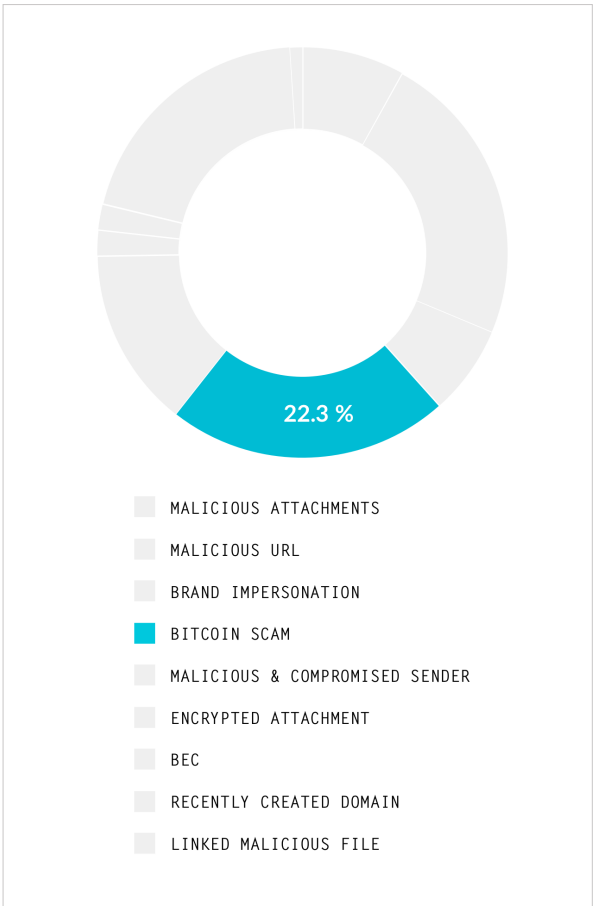


FIGURE 7

WHY DEFENSES DON'T STOP BITCOIN PHISH

Email security solutions have added functionality to fortify defenses, including stronger sender validation features with DMARC, time-of-click URL analysis to detect malicious links, and file sandboxing to detect hidden malware. But even these protections aren't sufficient to protect organizations from Bitcoin phishing campaigns.

WHY DEFENSES DON'T STOP BITCOIN PHISH – *Continued*

Threat actors send Bitcoin phishing emails from publicly available accounts such as Gmail or Hotmail, or from compromised email accounts that pass sender validation checks. And because the campaigns don't use malicious websites or malware, advanced email analysis techniques such as time-of-click URL analysis and file sandboxing are useless to detect these threats.

For example, a customer was recently sent an email claiming that the customer's OS was compromised and that the hacker now had access to the customer's device, files, contact lists and accounts (Fig. 8). The hacker demanded Bitcoin payment or an embarrassing video would be sent to the customer's contact list.

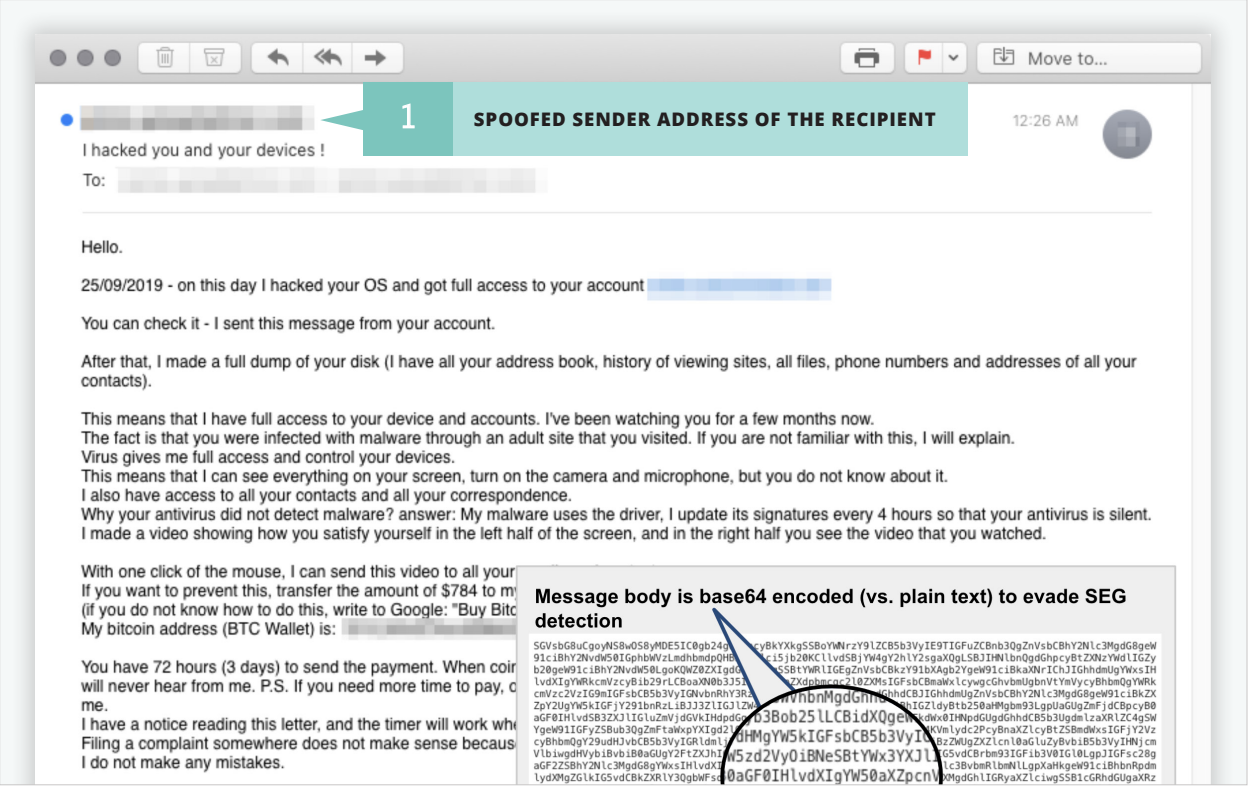


FIGURE 8

The email was scanned by Proofpoint defenses and judged benign. Area 1 scanned the email, detected that the message body was base64 encoded, decoded the body of the message, analyzed the resulting message text, detected that the email was a bitcoin phishing email, and prevented delivery to the recipient inbox.

Malicious Newly Created Domains

Another large category of phishing threats missed by SEGs and detected by Area 1 are emails that include malicious recently created domains (Fig. 9). Phishing emails often originate from, or include links to malicious domains. A frequent tactic of threat actors is to send email from recently registered domains to defeat reputation-based defenses.

In this analysis, ***19.8 percent*** of malicious phish detected by Area 1 were sent from, or contained links to recently created domains. In many cases, email judged by Area 1 to be malicious includes multiple threats, such as a malicious newly created domain in combination with malicious attachments, or a malicious link that leads to a site which harvests login credentials or downloads files containing malware. Because the Area 1 technology evaluates multiple factors before assigning a verdict to an email, detection effectiveness is maximized on these fast-flux phishing attacks, and false positives are minimized.

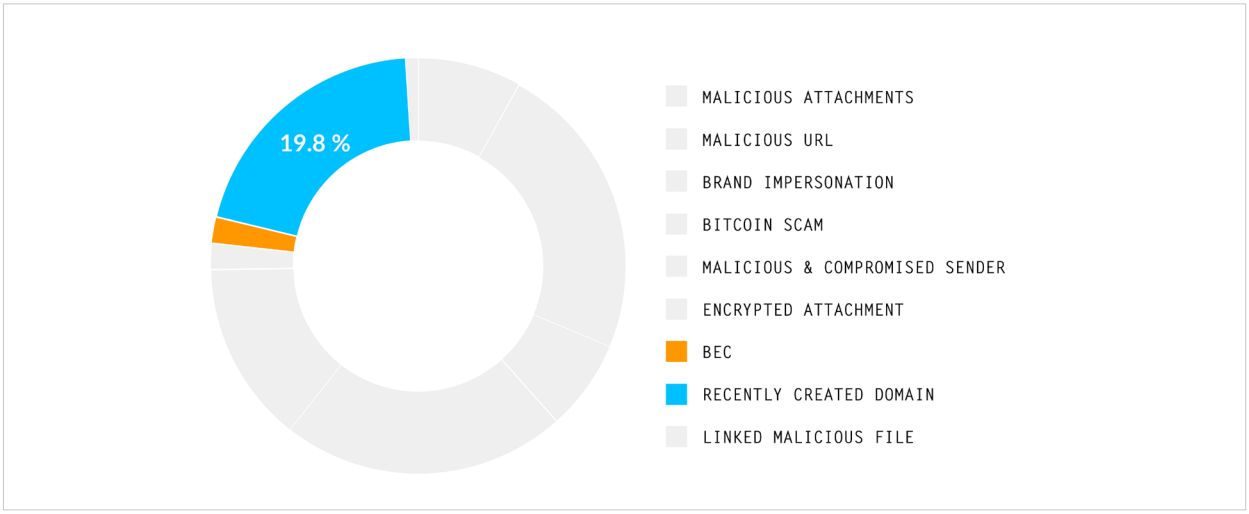


FIGURE 9

MALICIOUS NEWLY CREATED DOMAINS – *Continued*

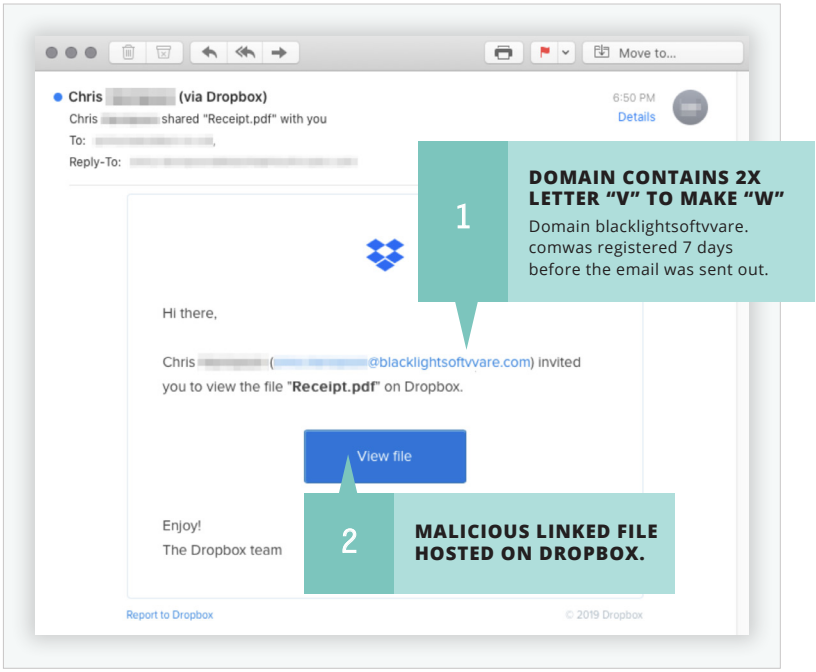


FIGURE 10

For example, a customer received an email that appeared to be an invitation from a supplier to view a receipt stored in Dropbox (Fig. 10).

The email was scanned by a Mimecast SEG and judged benign. The email was then scanned by Area 1 and found to include an email address from a suspicious, recently created domain and a link to a malicious document stored on Dropbox. The email was judged malicious and blocked from delivery.

BUSINESS EMAIL COMPROMISE EASILY BYPASSES SEGs

Another phishing attack type that is frequently found to use newly created domains to avoid detection is Business Email Compromise (BEC). BEC phishing messages are simple, with no links or attachments. They are socially engineered to trick their victims into taking digital or physical action -- particularly rogue wire transfers and diversion of funds. The absence of URLs and attachments to analyze, in combination with hackers' frequently sending these emails from compromised or newly created domains that easily pass sender reputation checks, creates a difficult challenge for traditional SEG detection engines. The messages look like any other normal business message.

However, using sophisticated matching models to check that messages appearing to be from an executive or associate actually originate from known or legitimate sending domains, and by analyzing subject and content language and sentiment, Area 1

BUSINESS EMAIL COMPROMISE EASILY BYPASSES SEGs – *Continued*

effectively detects BEC email that SEG defenses miss, and therefore prevents delivery of imposter email to employee inboxes.

For example, a senior payroll associate received an email that appeared to be sent by a Finance Controller interested in changing account information to a new financial institution (Fig. 11). The email was scanned by a Proofpoint SEG and judged benign.

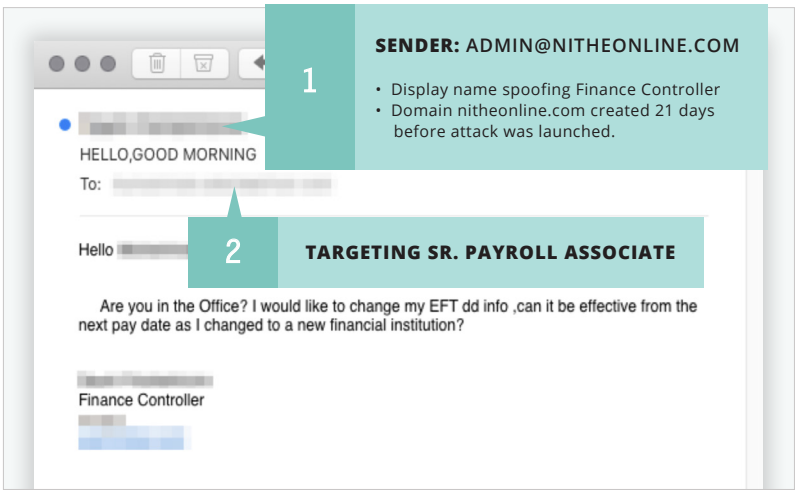


FIGURE 11

The message was then scanned using Area 1 detection models that recognized that the display name spoofed an employee, the sending domain was recently registered and that the body of the message was similar to other known BEC email detections, indicating a high likelihood that the message is a BEC. Area 1 detected and blocked this BEC attack preventing the loss of funds.

Malicious & Compromised Senders

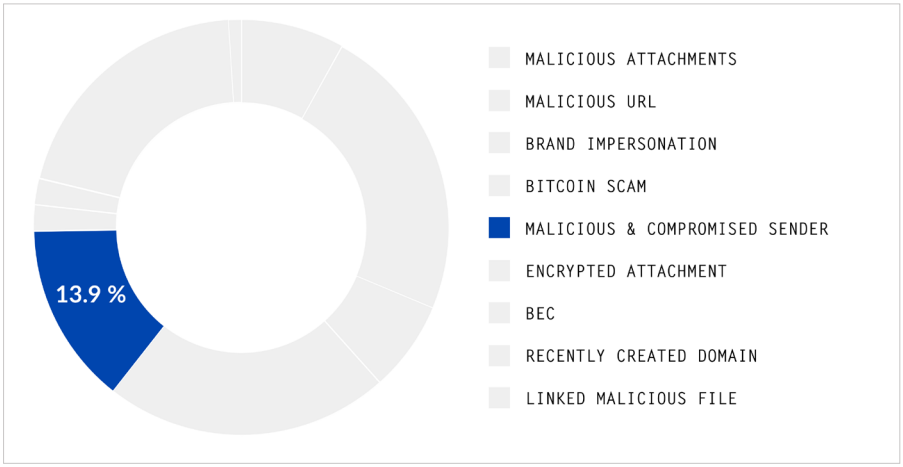


FIGURE 12

Another category of malicious phish that SEGs are challenged to defend against is phish originating from malicious or compromised senders (Fig. 12).

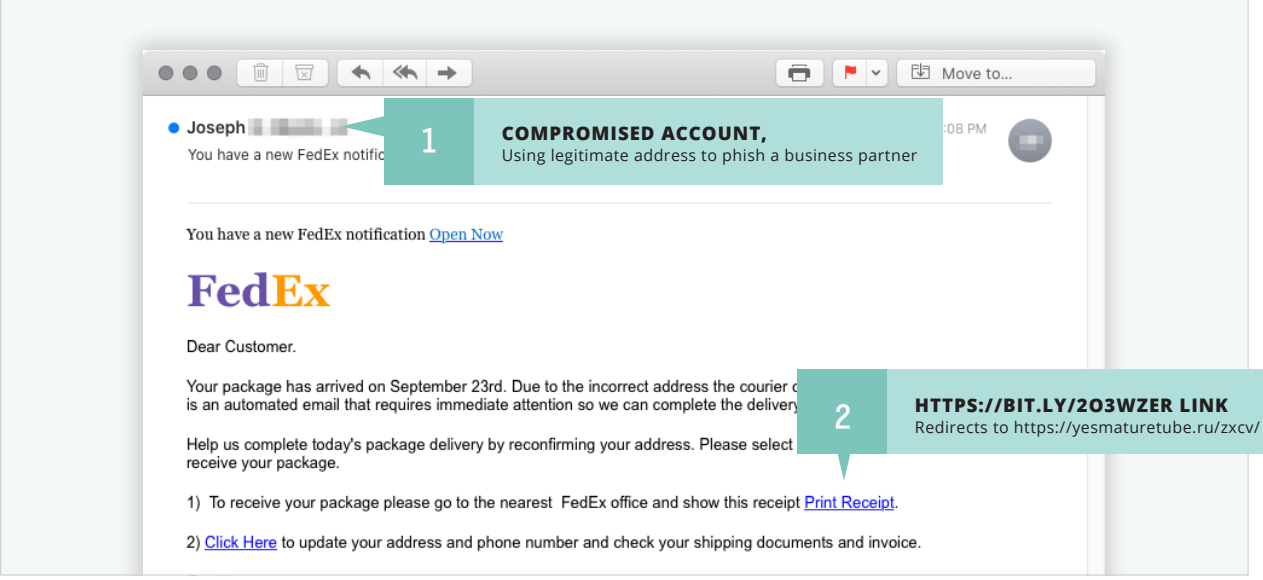
Threat actors frequently hijack or exploit other organizations' servers to send phishing emails or establish malicious web

pages for use in phishing campaigns. These servers and IPs are often legitimate, with established good reputations. Legacy defenses have no way to detect that a server is compromised until after a phishing attack is successfully executed, discovered, and reputation databases updated to indicate the server is compromised. By that time it's too late. The damage is done. Because Area 1 Security proactively crawls the web and monitors and tracks threat-actor activity in the wild, we discover compromised and malicious servers and IPs -- and identify email and URLs originating from these servers more effectively than legacy security technologies that rely on reputation-based detection.

For example, a customer received an email that appeared to be from FedEx requesting an address correction to complete delivery of a package (Fig. 13).

The email below was scanned by Proofpoint defenses. The sending domain passed SPF sender validation, and the email was judged benign by Proofpoint defenses. The email was then analyzed by the

FIGURE 13



Area 1 anti-phishing service, which detected that the sending domain (although valid) and the links in the email body were not associated with FedEx, and judged the email malicious. In fact, the sending email account was a compromised account at a reputable law firm.

In some cases, servers known to distribute nuisance spam initiate phishing email. Traditional email security defenses often label these emails to be "spam," "bulk" or "greymail" because they originate from a known nuisance spam server. Other defenses typically deliver the email to recipient inboxes or junk folders, missing the clues that the email is not merely nuisance spam but is actually a phish. Using advanced email analysis and ML classifier technologies, Area 1 is able to detect the 'spammy' phish that SEGs miss.

ADVANCED ANALYSIS TECHNIQUES DETECT MALICIOUS DOMAINS

In addition to proactive web crawling, the Area 1 service also uses additional techniques to detect inbound email originating from malicious domains. Techniques applied include sender validation checks, sender reputation analysis, domain registration history, and checks for domain obfuscation, including homographic analysis and punycode manipulation assessments. The combination of early visibility into phishing infrastructure and campaigns, plus advanced email analysis techniques and machine learning models, results in more effective detection of email originating from malicious domains than other security technologies and better protection from phishing attacks.

Malware Attachments

SEG vendors have invested heavily in tools to improve detection of malware hidden in attachments and yet, malicious attachments still evade detection. In fact, ***8.2 percent*** of malicious phish detected by Area 1 included an attached file with embedded malware (Fig. 14).

To detect malicious attachments, such as files containing embedded malicious VBscript and JavaScript, the service analyzes file attachments, including compressed and nested files, using Area 1's preemptive threat information and multiple ML file analysis models. In some cases, threat actors encrypt and password-protect file attachments or linked files and include a password in the body of an email to prevent detection by security technologies.

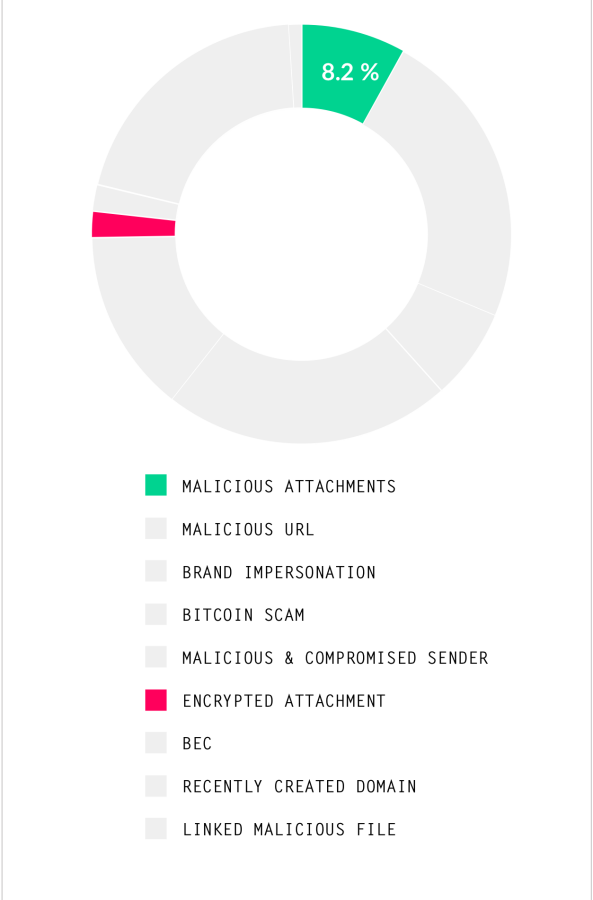


FIGURE 14

MALWARE ATTACHMENTS – *Continued*

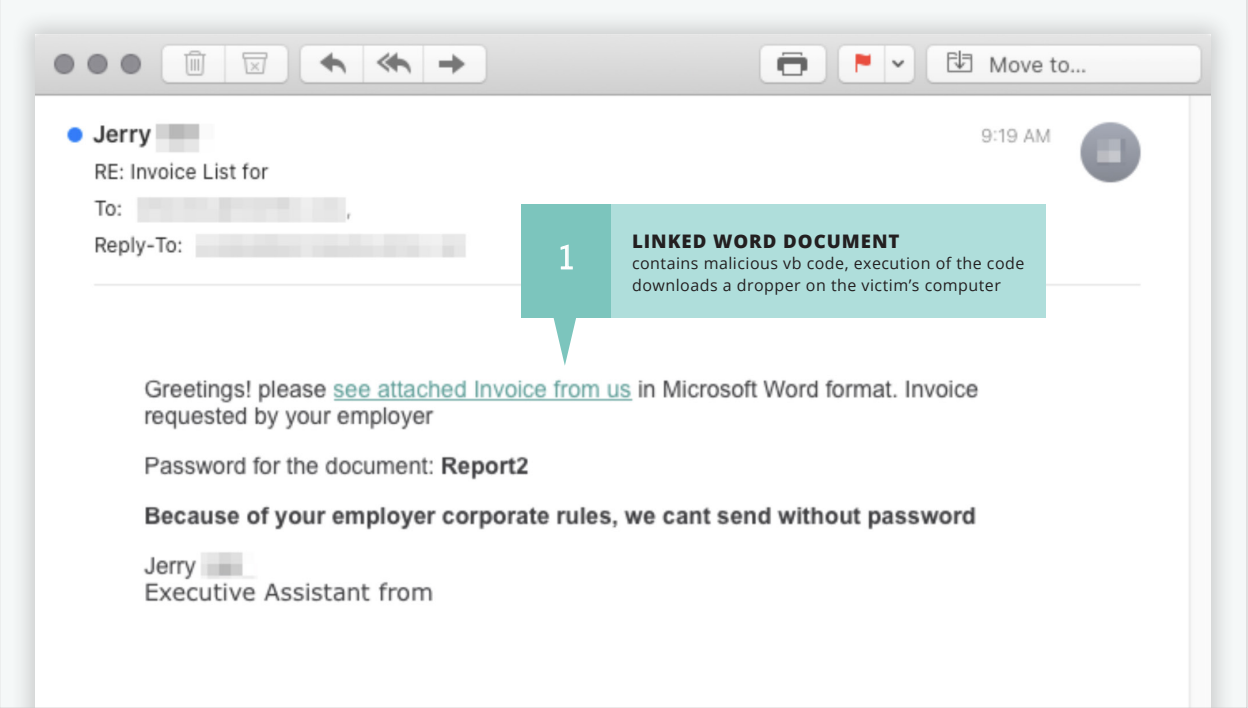


FIGURE 15

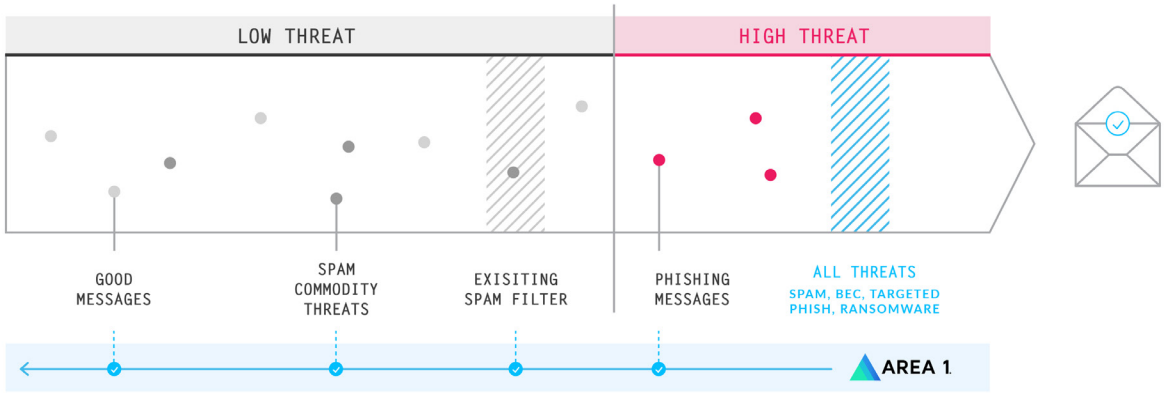
For example, a customer received an email that appeared to be from a vendor with a link to a password-protected Word doc for review (Fig. 15).

The email was originally scanned by Cisco Ironport and judged benign. It was then scanned by Area 1 and the linked Word document was extracted, analyzed using proprietary ML file analysis and discovered to contain malicious VB code that downloads a dropper to the victim's computer. The email was judged malicious and blocked from delivery.

140,000 Reasons to Rethink Phishing Defense

The results from reviewing Area 1's detection data are clear: **effective protection from modern phishing attacks requires a different approach to cybersecurity.**

Threat actors use the element of surprise to their advantage by continually evolving the phishing payloads, websites and techniques that they use to execute attacks. Conventional security defenses are backward-looking. They rely on knowledge of yesterday's active attack characteristics to detect the next attack, so they can't defend against modern attacks that are continually evolving.



Area 1 proactively monitors and analyzes threat actor activity and discovers phishing campaigns and infrastructure that are under construction. The service dynamically analyzes suspicious web pages and payloads -- and continuously updates email analysis and threat detection models as bad-actor tactics evolve. This preemptive approach to phishing defense prevented over 140,000 phish from penetrating customer inboxes over a four month period, reducing the risk of cyber breach, financial loss, data theft, and brand damage -- and saving security teams thousands of hours of incident response work.

If phish are bypassing your email security defenses, Area 1 can help.

Contact us to set up a free trial. You'll see what your current defenses aren't catching -- and you'll only pay us for the phish we catch, that your SEG is missing.

About Area 1 Security

Area 1 Security offers the only pay-for-performance solution in the cybersecurity industry - and the only technology that comprehensively blocks phishing attacks before they damage your business. Phishing is the root cause of 95 percent of security breaches.

Area 1 Security works with some of the most sophisticated organizations in the world, including Fortune 500 banks, insurance companies, and healthcare providers to preempt and stop targeted phishing attacks at the outset, improve their cybersecurity posture and change outcomes.

Learn more at www.area1security.com, join the conversation at @area1security or subscribe to Phish of the Week for the latest industry news and insights on how to deal with phishing.

▸ **To request a demo, visit:** https://www.area1security.com/try-area1/