AREA 1

PHISHING: TOP THREATS MISSED BY EXISTING DEFENSES

THE STORY BEHIND 100,000 MISSED PHISH

100,000 Reasons to Re-think Phishing Defense. And more...

Customers often deploy Area 1 Horizon™ anti-phishing service behind secure email gateways (SEGs), such as Proofpoint, Mimecast, Cisco IronPort, or Symantec, to catch phishing attacks missed by existing defenses.

FIGURE 1

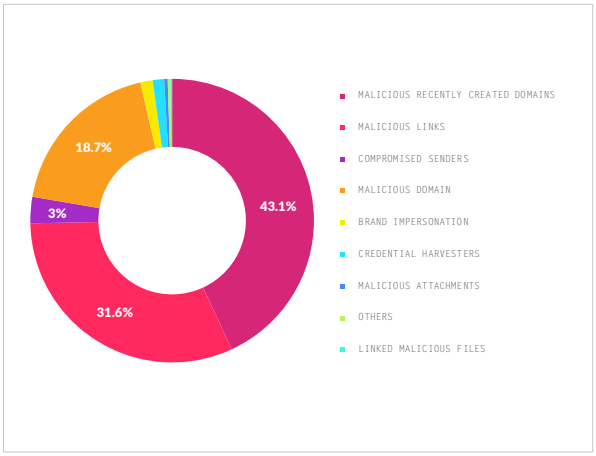
This report provides answers to two key questions that Area 1 is frequently asked: What type of phishing threats do SEGs miss? Why is the Area 1 service more effective at catching phishing email? The report reviews Area 1 detection data for a sample of customers that deploys our service as the critical security layer behind their SEG to detect and stop phishing email.

Over a recent three-month period, the Area 1 service analyzed over 240 million emails for these customers ***and caught nearly 100,000 phishing emails missed by their SEGs.***

For a typical company with 10,000 employee inboxes, ***that equates to over 3,100 phishing emails missed every week by SEGs and stopped by Area 1***. These emails would otherwise land in employee inboxes, bringing credential harvesting, malware, ransomware and other attacks that tie up security team resources investigating and remediating incidents. Even worse, 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 and Area 1 detects.

FIGURE 2



Malicious Recently Created Domains

Leading the list of phishing threats missed by SEGs and detected by Area 1 are emails that include malicious recently created domains. 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, 43.1 percent of malicious phish detected by Area 1 were sent from, or contained links to malicious, recently created domains. Another 18.7 percent of malicious phish were sent from, or included links to domains previously known by Area 1 to be malicious. In many cases, email judged by Area 1 to be malicious includes multiple threats, such as a malicious recently 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.

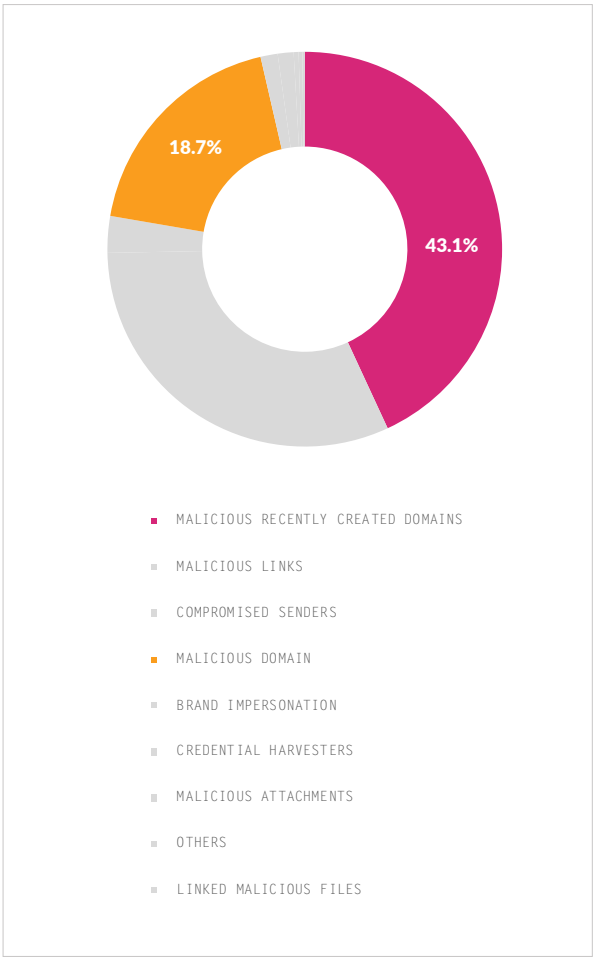


FIGURE 3

PROACTIVE WEB CRAWLING DISCOVERS UNKNOWN MALICIOUS DOMAINS

To detect malicious domains, Area 1 uses a number of techniques. Area 1 is the only cybersecurity company that continuously crawls the web to proactively identify phishing infrastructure before campaigns launch, detecting not only malicious domains but also malicious URLs, IPs, accounts, and payloads, on average discovering malicious infrastructure 24 days ahead of industry benchmarks. Just as Google indexes

PROACTIVE WEB CRAWLING DISCOVERS UNKNOWN MALICIOUS DOMAINS

commerce and content, Area 1 indexes the entire web—8 billion pages and 220 million top-level domains (TLDs) every couple of weeks—with the largest Web-crawling capability ever built, focused purely on discovering attacks and identifying campaigns.

For example, an Area 1 customer was sent an email that appeared to be from Amazon and requested that the recipient click a link and update payment information.

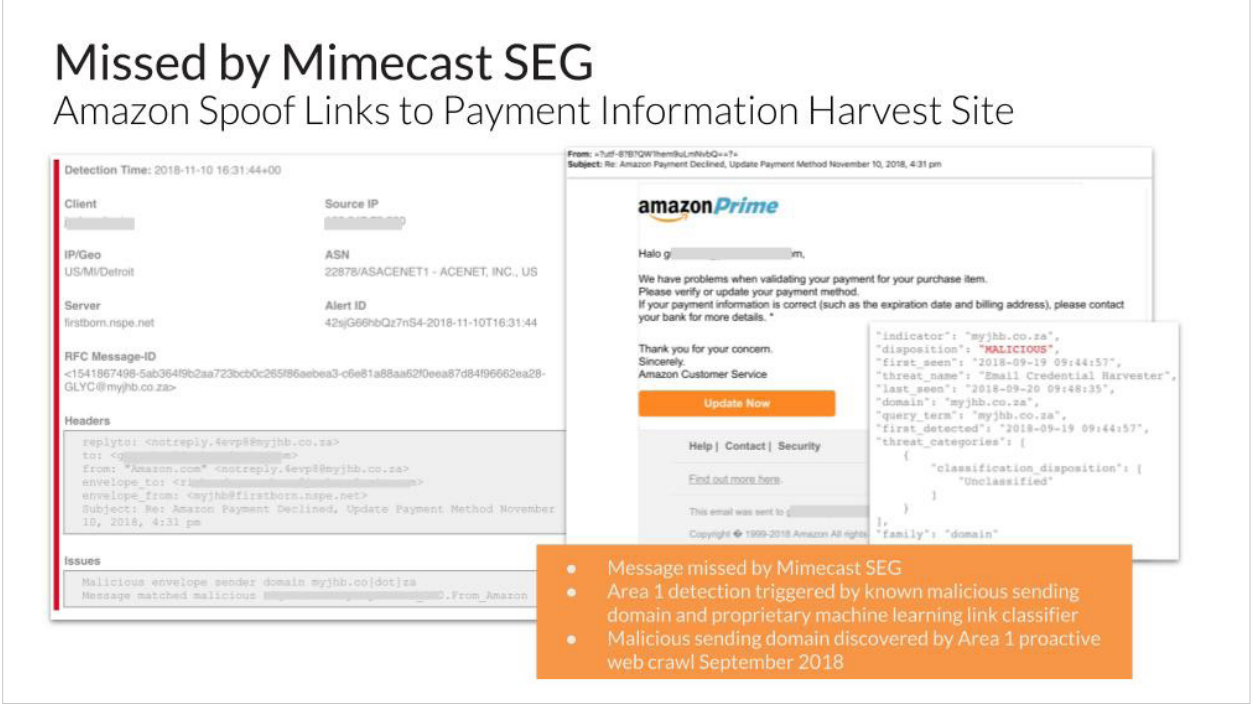


FIGURE 4

The email was judged benign by the customer's Mimecast SEG. The email was then analyzed by Area 1 and, because the sending domain had been discovered to be malicious a few months prior, using proactive web crawling, this email was judged to be malicious and was then blocked from delivery to the recipient's inbox.

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 malicious domains than other security technologies and better protection from phishing attacks.

Malicious Links

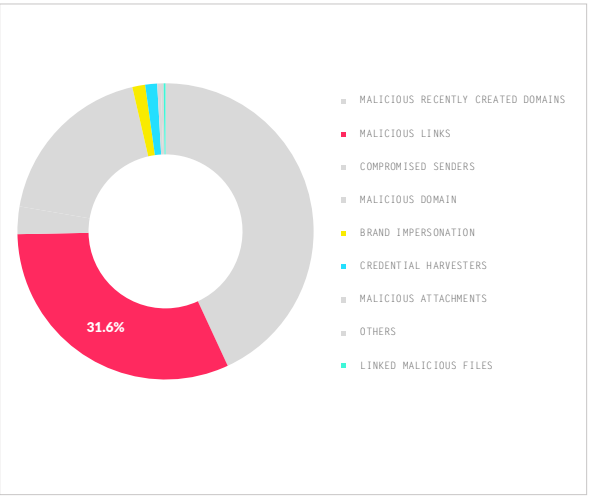


FIGURE 5

The second largest category of malicious phish that SEGs miss is phish containing malicious links. In this analysis, 31.6 percent of phish detected by Area 1 contained malicious links; another 3 percent of phish were from spoofed senders of trusted brands, 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 attacks 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 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

As an example, the Area 1 service detected and blocked a credential-harvesting attack that bypassed a customer's Proofpoint defenses.

In this case, the customer received an email from a web-hosting provider with a link to an invoice. Clicking the link displayed a login page for the victim to enter

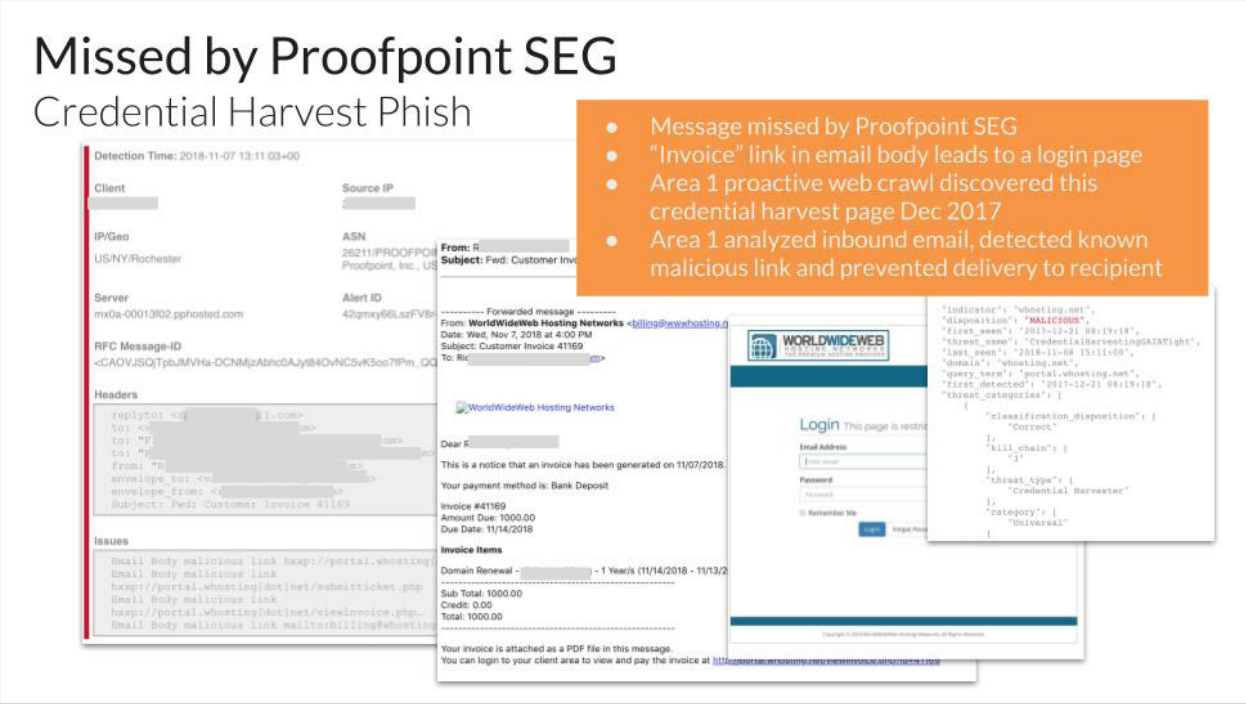


FIGURE 6

credentials and access the invoice. The email was scanned by Proofpoint defenses and judged benign. The email was then scanned by Area 1 Security, and the link was known by Area 1 to be a malicious link to a credential harvesting site. The malicious site was first discovered in 2017 by Area 1's high-speed web crawling technology. Because the URL contained in the email was known to Area 1 as a credential harvesting site, Area 1 judged the email to be malicious. The email was then blocked from delivery to the recipient's inbox.

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.

For example, a phishing email harboring a credential-harvesting attack was recently blocked by Area 1 after passing through Cisco IronPort SEG defenses.

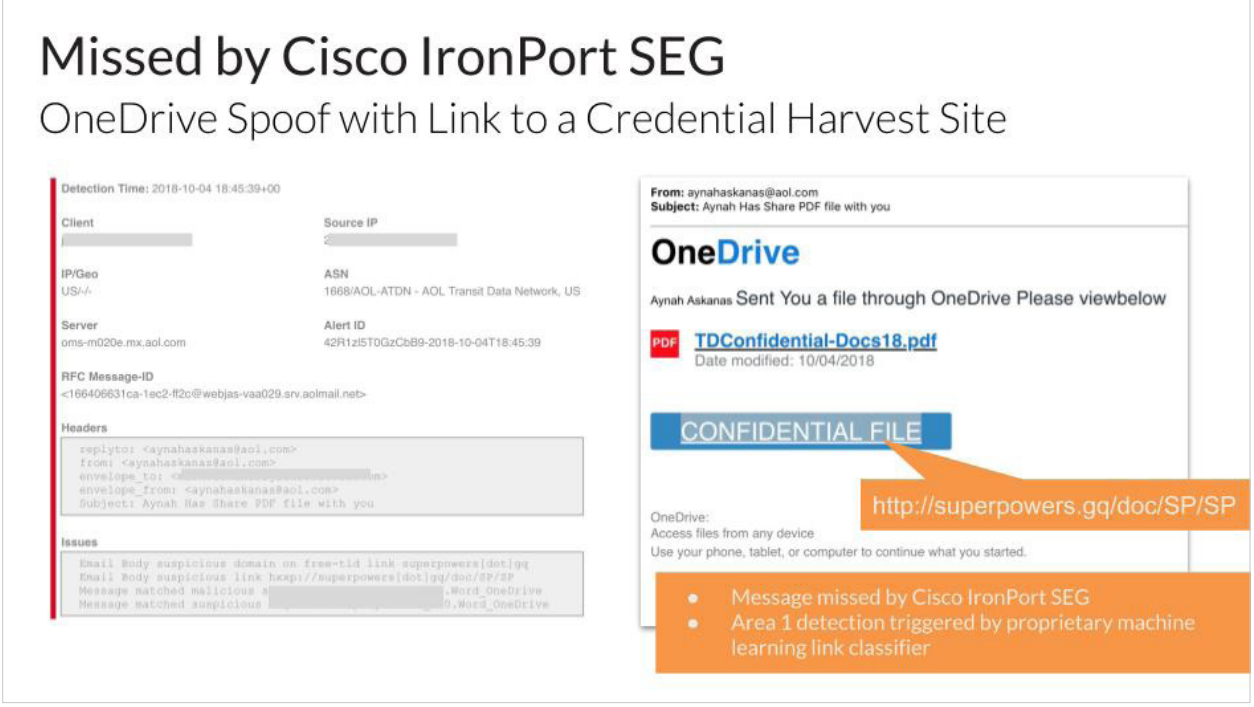


FIGURE 7

The email appeared to be from OneDrive and requested that the recipient click on a link to view a PDF. Using Area 1 proprietary ML classifiers that analyzed the URL and other message attributes, such as recognizing the frequently spoofed brand "OneDrive", the link was judged malicious, clearly not associated with the OneDrive domain, and the email was blocked from delivery.

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

In another case, an email claiming to be from a Canadian flower supplier was scanned by a Proofpoint SEG and released for delivery.

The Area 1 Horizon anti-phishing service then scanned the email and detected a suspicious link. The service instantly crawled the link, and using ML file analysis, identified malicious VBA code in a linked document and judged the email malicious. The email was blocked before delivery to the recipient's inbox, protecting the user from downloading malware.

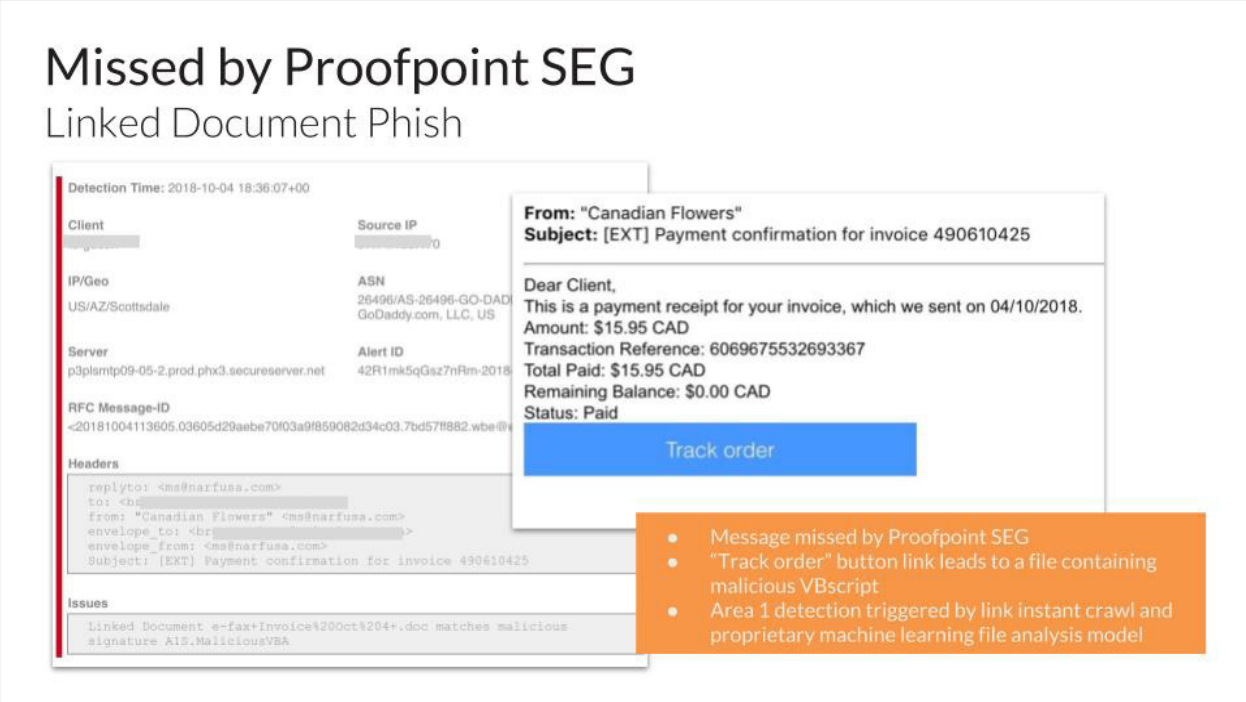


FIGURE 8

ADVANCED ANALYSIS TECHNIQUES DETECT BRAND IMPERSONATION EMAILS AND CREDENTIAL HARVESTING ATTACKS

SEGs are often challenged to defend against brand impersonation emails and credential-harvesting attacks. 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 malicious domains and links, Area 1 uses additional advanced techniques to identify brand impersonation and credential-harvest phishing attacks. For example, Area 1 technology detects 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 Microsoft brand-impersonation phishing email harboring a credential-harvesting attack was blocked by Area 1 after passing through a Proofpoint SEG.

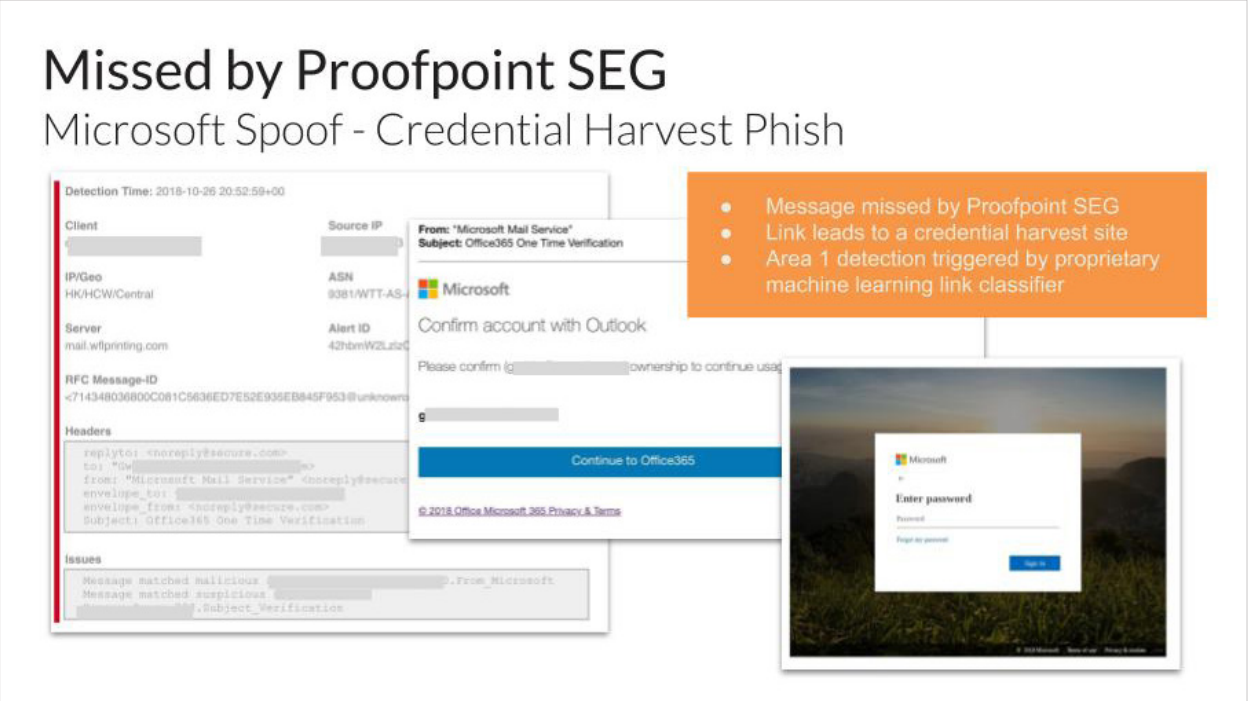


FIGURE 9

AREA 1

ADVANCED ANALYSIS TECHNIQUES DETECT BRAND IMPERSONATION EMAILS AND CREDENTIAL HARVESTING ATTACKS

In this case, the email appeared to be from Microsoft and requested that the recipient click on a link to verify an account. Using Area 1 proprietary ML classifiers that analyzed the URL and other message attributes, the email was judged malicious by Area 1, blocked from delivery, and the end user protected from a credential-harvesting site.

Compromised Senders

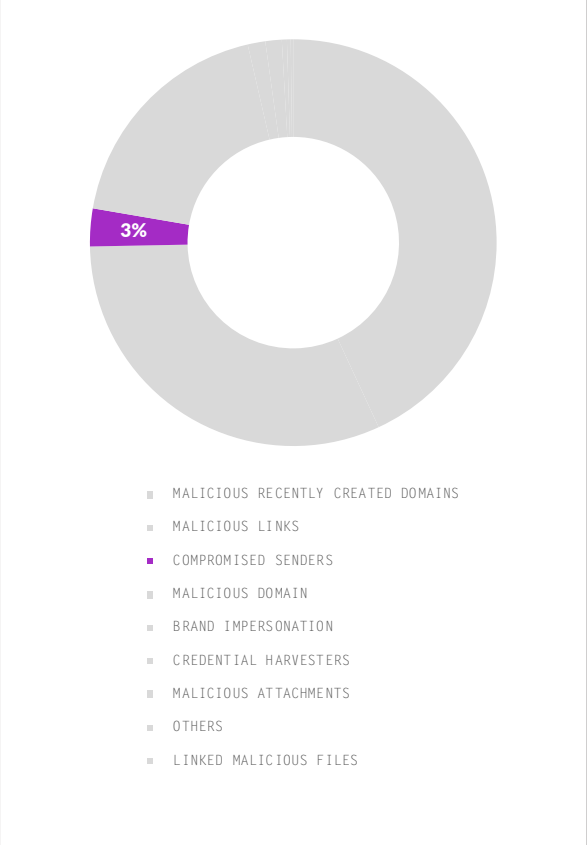


FIGURE 10

Another category of malicious phish that SEGs are challenged to defend against is phish origionating from compromised senders. 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, and 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 servers and IPs; we can identify email and URLs originating from these servers more effectively than legacy security technologies that rely on reputation-based detection.

COMPROMISED SENDERS

For example, an email that appeared to be a notification from a file transfer service requested the recipient click a link to receive files.

The email was scanned and judged benign by Cisco IronPort defenses. It was then analyzed by the Area 1 anti-phishing service. The Area 1 service

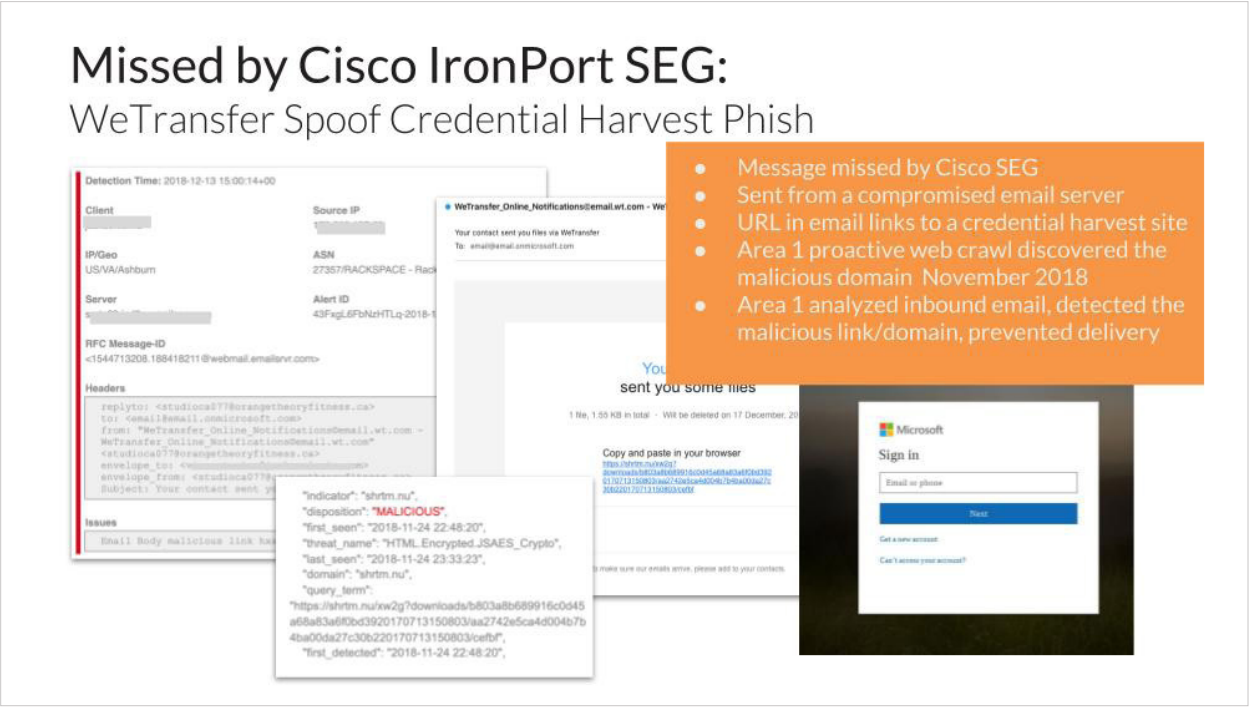


FIGURE 11

detected that the link in the email body was malicious. Area 1 discovered the link's domain to be malicious via web crawling the previous month, so the email was judged malicious and blocked from delivery.

In some cases, servers known to distribute nuisance spam initiate phishing email. Traditional email security defenses often label these emails "spam", or "bulk" or "greymail" because they originate from a known nuisance spam server. The 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.

For example, an email that appeared to be from Google Drive was judged by a Proofpoint SEG to be spam and released for delivery to the recipient.

COMPROMISED SENDERS

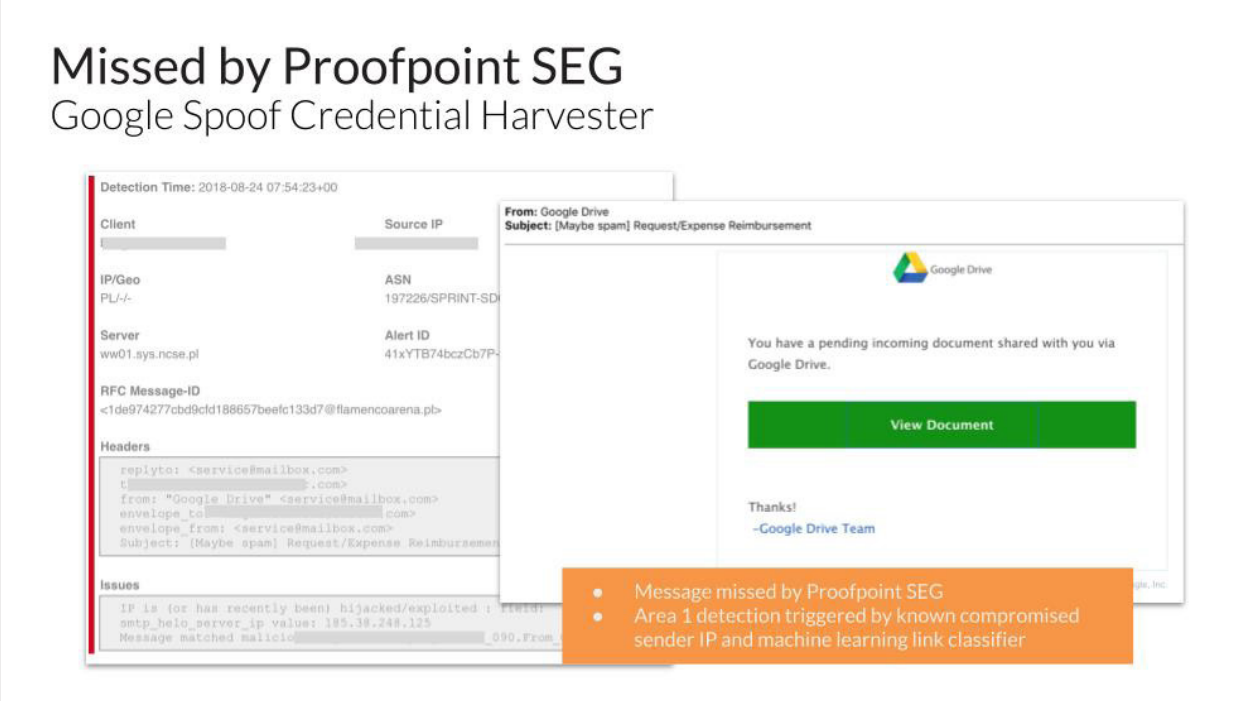


FIGURE 12

The email was then analyzed by Area 1 using a proprietary ML classifier that analyzed a link in the body of the email and other factors. These included recognizing references to the Google brand, in addition to checking the reputation of the sending domain. The email was judged malicious and prevented from delivery to the recipient, protecting the end user from a phishing attack.

Malware Attachments

SEG vendors have invested heavily in tools to improve detection of malware hidden in attachments, and yet, malicious attachments still evade detection. Although a small percentage, almost one percent of malicious phish detected by Area 1 included an attached file with embedded malware. To detect malicious attachments, such as files containing embedded malicious VBscript and JavaScript, the service

MALWARE ATTACHMENTS

analyzes file attachments, including compressed and nested files, using Area 1's preemptive threat information and multiple ML file analysis models.

For example, a customer received an email from a hotel with a request for payment.

FIGURE 13

The email was scanned by a Cisco IronPort SEG and judged benign. The email was then scanned by Area 1, and the attached PDF analyzed using proprietary ML file analysis, and found to be malicious.

In some cases, threat actors encrypt file attachments and include a password in the body of an email to prevent detection by security technologies. To analyze password-protected file attachments, the Area 1 service scans the email to discover passwords. If a password is found, the file is decrypted and analyzed to check for malicious code.

100,000 Reasons to Re-think Phishing Defense. And more...

The results from reviewing Area 1 detection data are clear. Effective protection from modern phishing attacks requires a new 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. Most 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 it continuously updates email analysis and threat detection models as bad-actor tactics evolve. This preemptive approach to phishing defense prevented over 100,000 phish from penetrating customer inboxes over a three month period, reducing the risk of cyberbreach, financial loss, data theft, brand damage and saving security teams from thousands of hours of incident response work. If phish are bypassing your email security defenses, Area 1 can help. Contact Area 1 for more information or for a free trial.

About Area 1 Security

Area 1 Security is the first to bring accountability to cybersecurity. Backed by top-tier investors, Area 1 Security is led by security, Artificial Intelligence, and data analytics experts who created a preemptive solution to stop phishing, the number one cause of cyber attacks.

Area 1 Security works with organizations worldwide, including Fortune 500 banks, insurance, and tech companies, and healthcare providers to realign their cybersecurity posture for combating the most significant risks, protecting customer data, and stopping attacks before they happen. Area 1 Security is a recipient of Inc. Magazine's "2018 Inc.'s Best Workplaces" in America. To learn more about Area 1 Security, visit www.area1security.com, join the conversation at @area1security or follow the blog for the latest industry news and insights on how to stop phishing.

Learn More INFO@AREA1SECURITY.COM