

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.

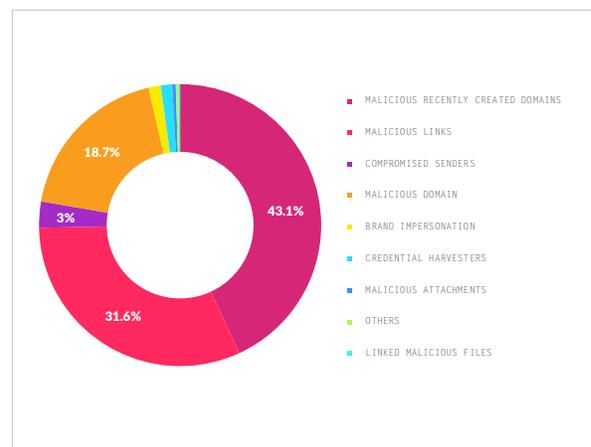
Over a recent three-month period, the Area 1 service analyzed over 240 million emails for these customers **and caught nearly 100,000 phishing emails missed by their SEGs.**

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.

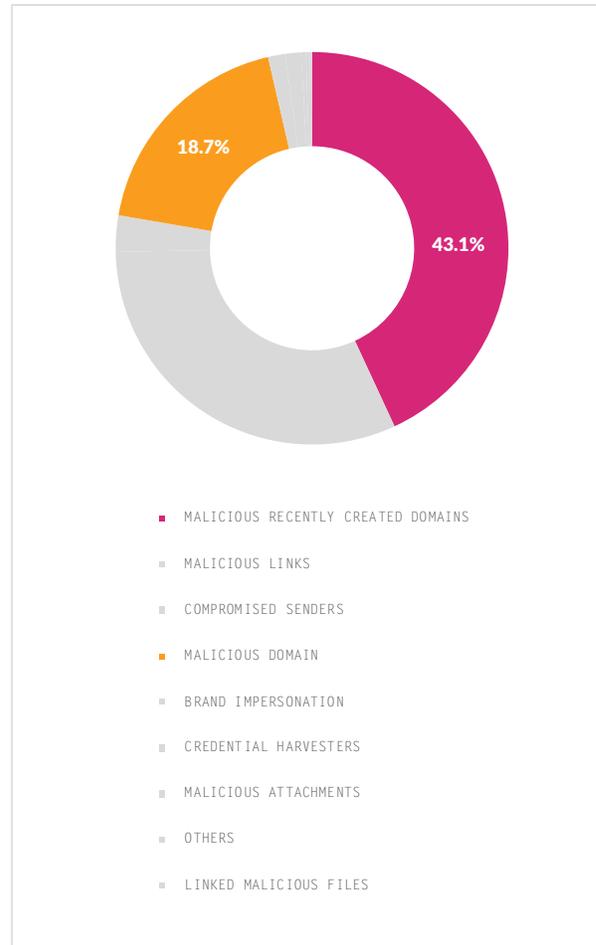


FIGURE 3

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

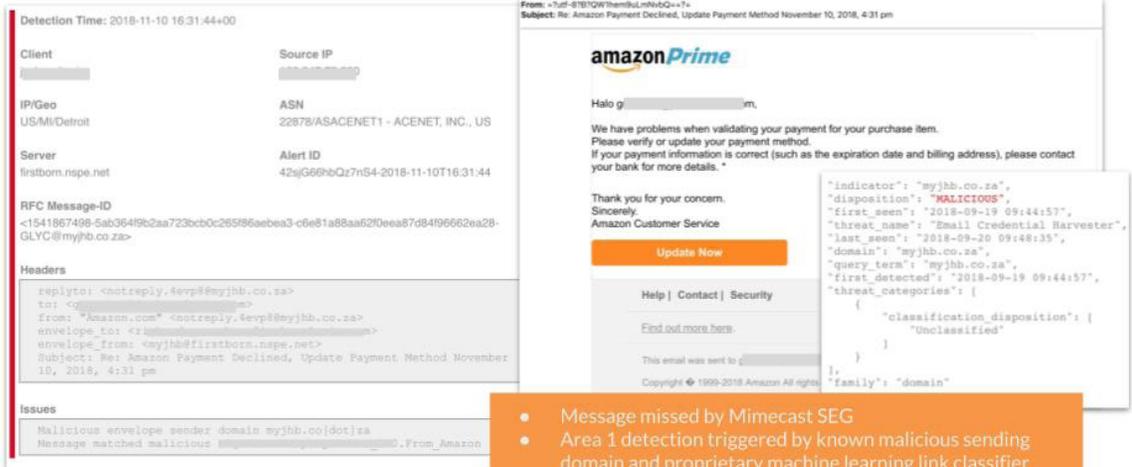
launch, detecting not only malicious domains but also malicious URLs, IPs, accounts, and payloads, on average discovering malicious infrastructure 24 days ahead of industry benchmarks. Just as Google indexes

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.

Missed by Mimecast SEG Amazon Spoof Links to Payment Information Harvest Site



- Message missed by Mimecast SEG
- Area 1 detection triggered by known malicious sending domain and proprietary machine learning link classifier
- Malicious sending domain discovered by Area 1 proactive web crawl September 2018

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

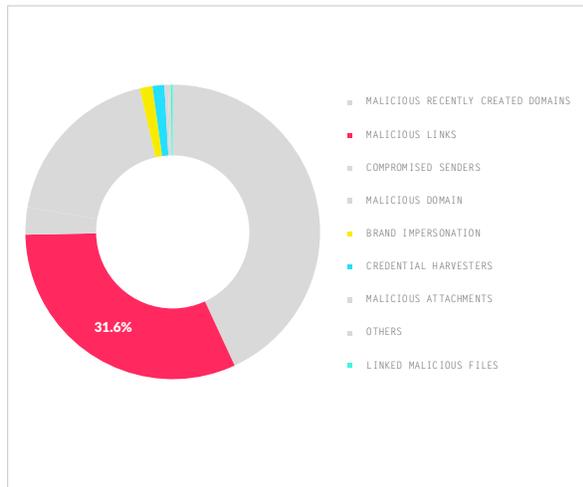


FIGURE 5

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

Missed Message by Proofpoint SEG Credential Harvest Phish

Detection Time: 2018-11-07 13:11:03+00

Client	Source IP
IP/Geo	ASN
US/NY/Rochester	26211/PROOFPOINT
Server	Alert ID
mx0a-0001302.pphosted.com	42qmy66LszFV8
RFC Message-ID	
<CAOVJSQjTpbJMVHa-DCNMpAbhcAJy84OvNC5vK5oo7Pm_QC>	

Headers

```

reply-to: <[redacted]@[redacted].com>
to: <[redacted]>
cc: "P"
cc: "P"
from: "P"
envelope-to: <[redacted]>
envelope-from: <[redacted]>
subject: Fwd: Customer Invoice 41169
                
```

Issues

```

Email Body malicious link http://portal.whosting.net
Email Body malicious link http://portal.whosting.net/submitticket.php
Email Body malicious link http://portal.whosting.net/viewinvoice.php
Email Body malicious link mailto:billing@whosting.net
                
```

- Message missed by Proofpoint SEG
- "Invoice" link in email body leads to a login page
- Area 1 proactive web crawl discovered this credential harvest page Dec 2017
- Area 1 analyzed inbound email, detected known malicious link and prevented delivery to recipient

Forwarded message

From: WorldWideWeb Hosting Networks <billing@wwhosting.net>
Date: Wed, Nov 7, 2018 at 4:00 PM
Subject: Customer Invoice 41169
To: [redacted]

Dear [redacted],

This is a notice that an invoice has been generated on 11/07/2018.

Your payment method is: Bank Deposit

Invoice #41169
Amount Due: 1000.00
Due Date: 11/14/2018

Invoice Items

Domain Renewal - [redacted] - 1 Year(s) (11/14/2018 - 11/13/2019)	Sub Total: 1000.00
	Credit: 0.00
	Total: 1000.00

Your invoice is attached as a PDF file in this message.
You can login to your client area to view and pay the invoice at <http://portal.whosting.net>

WorldWideWeb Hosting Networks

Login This page is restricted

Email Address:

Password:

Remember Me

```

{
  "indicator": "whosting.net",
  "disposition": "MALICIOUS",
  "first_seen": "2017-12-21 08:19:18",
  "threat_name": "CredentialHarvestingGATight",
  "last_seen": "2018-11-08 15:11:00",
  "domain": "whosting.net",
  "query_term": "portal.whosting.net",
  "first_detected": "2017-12-21 08:19:18",
  "threat_category": [
    {
      "classification_disposition": [
        "Correct"
      ]
    },
    {
      "kill_chain": [
        "CI"
      ]
    },
    {
      "threat_type": [
        "CredentialHarvesting"
      ]
    },
    {
      "category": [
        "Malware"
      ]
    }
  ]
}
                
```

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.

Missed by Cisco IronPort SEG

OneDrive Spoof with Link to a Credential Harvest Site

Detection Time: 2018-10-04 18:45:39+00

Client	Source IP
US/A	1668/AOL-ATDN - AOL Transit Data Network, US
IP/Geo	ASN
US/A	1668/AOL-ATDN - AOL Transit Data Network, US
Server	Alert ID
oms-m020e.mx.aol.com	42R1z15T0GzCbB9-2018-10-04T18:45:39

RFC Message-ID
<166406631ca-1ec2-f2c@webjas-vaa029.srv.aolmail.net>

Headers

```

reply-to: <aynahaskanas@aol.com>
from: <aynahaskanas@aol.com>
envelope-to: <aynahaskanas@aol.com>
envelope_from: <aynahaskanas@aol.com>
Subject: Aynah Has Share PDF file with you
                    
```

Issues

```

Email Body suspicious domain on free-tld link superpowers[dot]gq
Email Body suspicious link http://superpowers[dot]gq/doc/SP/SP
Message matched malicious aynahaskanas@aol.com Word OneDrive
Message matched suspicious http://superpowers[dot]gq/doc/SP/SP
                    
```

From: aynahaskanas@aol.com
Subject: Aynah Has Share PDF file with you

OneDrive

Aynah Askanas Sent You a file through OneDrive Please viewbelow

PDF [TDConfidential-Docs18.pdf](#)
Date modified: 10/04/2018

CONFIDENTIAL FILE

http://superpowers.gq/doc/SP/SP

OneDrive:
Access files from any device
Use your phone, tablet, or computer to continue what you started.

- Message missed by Cisco IronPort SEG
- Area 1 detection triggered by proprietary machine learning link classifier

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.

Missed by Proofpoint SEG

Linked Document Phish

Detection Time: 2018-10-04 18:36:07+00

Client	Source IP
US/AZ/Scottsdale	26496/AS-26496-GO-DADDY
IP/Geo	ASN
	GoDaddy.com, LLC, US
Server	Alert ID
p3plsmtp09-05-2.prod.phx3.secureserver.net	42R1mk5qGsz7nRm-2018
RFC Message-ID	
<20181004113605.03605d29aabe70f03a9f859082d34c03.7bd57f882.wbe@>	

Headers

```

replyto: <ms@narfusa.com>
to: <b...>
from: "Canadian Flowers" <ms@narfusa.com>
envelope-to: <br...>
envelope-from: <ms@narfusa.com>
Subject: [EXT] Payment confirmation for invoice 490610425
                    
```

Issues

```

Linked Document e-fax+Invoice%20Oct%204+.doc matches malicious signature AiE.MaliciousVBA
                    
```

From: "Canadian Flowers"
Subject: [EXT] Payment confirmation for invoice 490610425

Dear Client,
 This is a payment receipt for your invoice, which we sent on 04/10/2018.
Amount: \$15.95 CAD
Transaction Reference: 6069675532693367
Total Paid: \$15.95 CAD
Remaining Balance: \$0.00 CAD
Status: Paid

Track order

- Message missed by Proofpoint SEG
- "Track order" button link leads to a file containing malicious VBscript
- Area 1 detection triggered by link instant crawl and proprietary machine learning file analysis model

FIGURE 8

ADVANCED ANALYSIS TECHNIQUES DETECT BRAND IMPERSONATION EMAILS AND CREDENTIAL HARVESTING ATTACKS

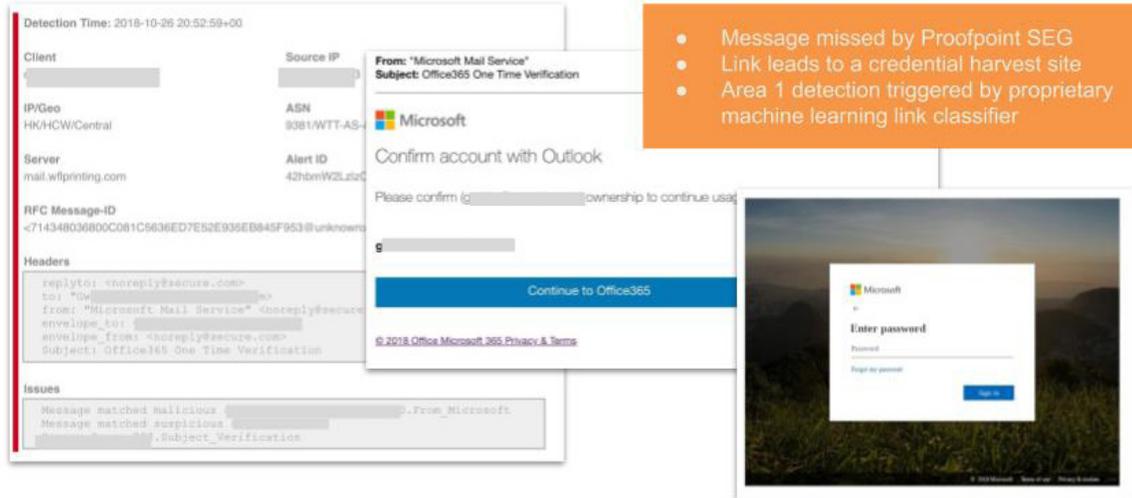
SEGs are often challenged to defend against brand impersonation emails and credential-harvesting attacks. With these attacks, threat actors craft emails that appear to be sent from trusted brands, but are in fact spoofed, and most include malicious links or attachments. In addition to the techniques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

Missed by Proofpoint SEG

Microsoft Spool - Credential Harvest Phish



- Message missed by Proofpoint SEG
- Link leads to a credential harvest site
- Area 1 detection triggered by proprietary machine learning link classifier

FIGURE 9

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

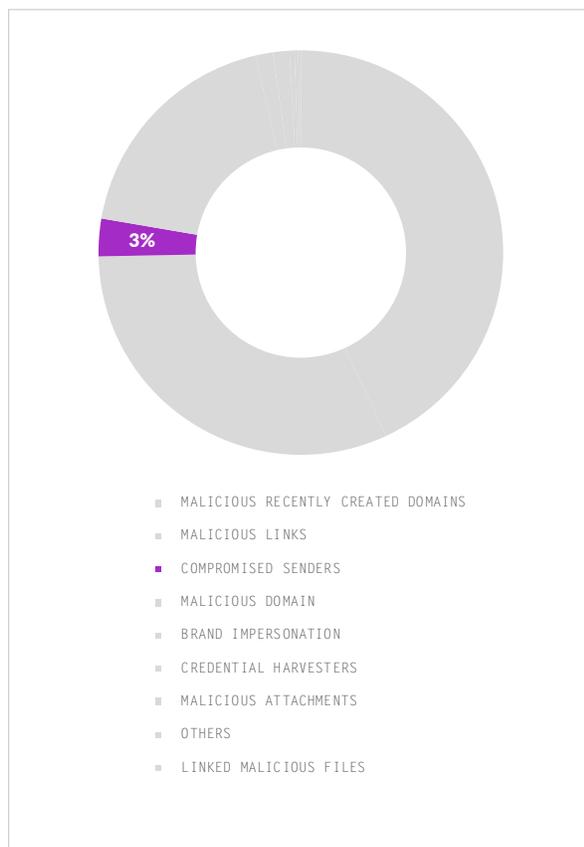


FIGURE 10

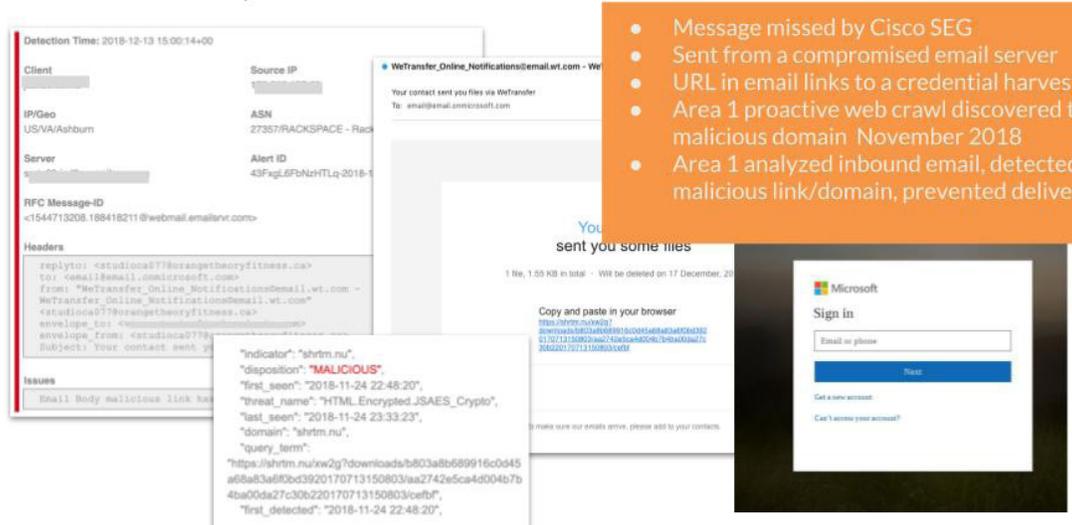
Another category of malicious phishing that SEGs are challenged to defend against is phishing originating from compromised senders. Threat actors frequently hijack or exploit other organizations' servers to send phishing emails or establish malicious web pages for use in phishing campaigns. These servers 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

Missed by Cisco IronPort SEG: WeTransfer Spoof Credential Harvest Phish



- Message missed by Cisco SEG
- Sent from a compromised email server
- URL in email links to a credential harvest site
- Area 1 proactive web crawl discovered the malicious domain November 2018
- Area 1 analyzed inbound email, detected the malicious link/domain, prevented delivery

Indicators: "shrm.nu", "disposition": "MALICIOUS", "first_seen": "2018-11-24 22:48:20", "threat_name": "HTML.Encrypted_JSAES_Crypto", "last_seen": "2018-11-24 23:33:23", "domain": "shrm.nu", "query_sims": "https://shrm.nu/sw2g?download=b803a8b689916c0645a88a83a680b43920170713150803aa2742e5ca4d004b7b4ba0da27c30b220170713150803cebf", "first_detected": "2018-11-24 22:48:20"

Issues: Email Body malicious link harvested

Microsoft Sign in: Email or phone, Next, Get a new account, Get a new account?

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 "greymlail" 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

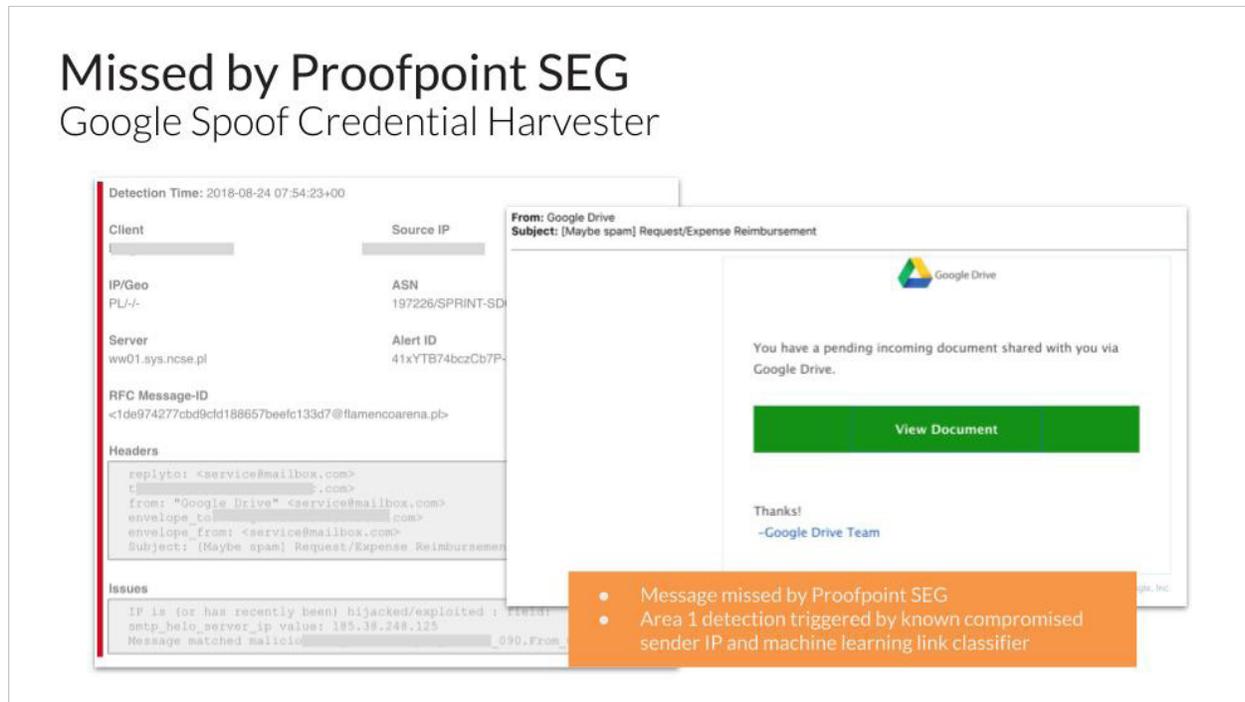


FIGURE 12

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.

Missed by Cisco IronPort SEG: Malicious Attachment Phish

Detection Time: 2018-10-19 09:49:01+00

Client	Source IP
IPGeo	ASN
US/VA	16417/IRONPORT
	Ironport Division,
Server	Alert ID
osa13.hc1983-11.phms.com	42c1Mc2HPTzPV

RFC Message-ID
-L02P265MB07174EC43DB146FEF8CF8AE2F90@L02P265MB071

Headers

```

reply-to: <accounts@abbeyhotelbath.co.uk>
From: "Accounts" <accounts@abbeyhotelbath.co.uk>
envelope-to: <accounts@abbeyhotelbath.co.uk>
envelope_from: <accounts@abbeyhotelbath.co.uk>
Subject: [EXT] Payment Note From Abbeyhotelbath UK
                    
```

Issues

```

Attachment Payment Note From Abbeyhotelbath.pdf matches malicious signature
A13.MaliciousPDF
Message matched malicious [redacted].URL_Adobe
Message matched suspicious [redacted]
Message matched suspicious [redacted]_Finance_Score_263
Message matched suspicious [redacted]97.Word_Adobe
                    
```

From: Accounts
Subject: [EXT] Payment Note From Abbeyhotelbath UK

Please find our BACS invoice payment advice attached to this email.

Kind regards,

Emma-May Peacock
Accounts Assistant

t: 01225 461603
e: accounts@abbeyhotelbath.co.uk
Contact address: 1 North Parade Bath BA1 1LF

 Virus-free. www.avg.com

- Message missed by Cisco IronPort SEG
- Attached PDF is malicious
- Area 1 detection triggered by proprietary machine learning file analysis model

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](https://twitter.com/area1security) or follow the [blog](#) for the latest industry news and insights on how to stop phishing.

► Learn More INFO@AREA1SECURITY.COM