AREA 1 SECURITY

IT STARTED OUT WITH A PHISH

How Did It End Up Like This?

2021 Security Report

AREA 1 SECURITY

TABLE OF CONTENTS

Introduction

It started out with a phish; how did it end up like this? Inspired from the lyrics of the song Mr. Brightside by The Killers, we've seen first-hand how phishing threats can end up as million-dollar ransom demands, financial fraud and other damages to organizations. We invite you to "open up [your] eager eyes" as we explore the threats targeting your inbox.

The past twelve months have brought unique challenges as the global COVID pandemic forced organizations to rapidly adopt new business procedures amid remote operations and disrupted supply chains. While it had always been business-critical, email became even more crucial.

The same can be said for the other side as threat actors focused on emails to launch a variety of attacks. Infamous incidents discovered and played out in the past year included the SolarWinds breach that highlighted the deadly impact of supply-chain attacks and numerous "successful" ransomware campaigns, including the Colonial Pipeline attack on public infrastructure and Kaseya supply-chain ransomware hack, prompting multiple FBI alerts and an executive order on improving cybersecurity.

While there's still plenty of uncertainty as we approach the post-COVID world, one thing is clear: inboxes aren't clean. Threats ranging from nuisance spam to difficult-to-discover but costly business email compromise (BEC) continue to target organization inboxes.

We analyzed a sampling of over 31 million threats discovered from May 1, 2020 to April 30, 2021 across organizations and found several interesting patterns. Read along to learn more.

AREA 1 SECURITY

Key Findings

01

IDENTITY IS THE KEY

As the saying goes, go for the lowest hanging fruit. In phishing, that fruit is the credential. Credential harvesters are the most common threat type in email.

*Nearly **10 percent (9.3%) of malicious attacks** involve credential harvesters.*

Why bring a battering ram, when you can just steal the keys to the door? Attackers look for the path of least resistance, so if you can spend three minutes crafting an email to steal credentials versus spending hours devising a way past firewalls and other protections, why wouldn't you go that route?

02

LOW VOLUME, HIGH RETURNS

Business Email Compromise (BEC) is the latest example of researching your target. They involve a lot more care and feeding than traditional phishing attacks.

*Although BECs make up a tiny volume of attacks, they represent the highest financial damage. In our data, BEC acccounted for **1.3% of attacks** but would have resulted in over **$354 million in direct losses.** The average BEC request in our findings is nearly **$1.5 million.***

03

TRUST NO ONE, LEAST OF ALL YOUR "FRIENDS"

*Identity deception using tactics like spoofing, domain impersonation and display name impersonation is used in nearly **9% of attacks.***

These attacks showcase the ease at which people can deceive the common user to gain access to their goals. In many cases, it's as simple as a display name change to seriously wreck someone's weekend and lose trust in who they're dealing with. Speaking of trust...

AREA 1 SECURITY

Key Findings — *Continued*

04

THE ENEMY YOU KNOW

What's even better than pretending to be Jan from accounting? How about being America's favorite retailer with a special offer just for you! Attackers impersonate known brands to add legitimacy to phishing campaigns.

The top 10 most impersonated brands make up over ***56% of all impersonation-based phishing attacks.***

These attacks will always present a challenge to most users. Things like the latest trends in the news or entertainment can spell big bucks for attackers.

05

WHAT ABOUT SPAM?

End user training does wonders in helping foster a culture of security in an organization. However, not every end user has their CISSP. True positive phishing submissions are amazing for the safety of an organization.

However, more than ***92% of user-reported phish*** *are not malicious and are actually benign, spam or bulk mail.*

Training isn't enough to stop the white noise heard by the security admins.

AREA 1 SECURITY

It Started out with a Phish

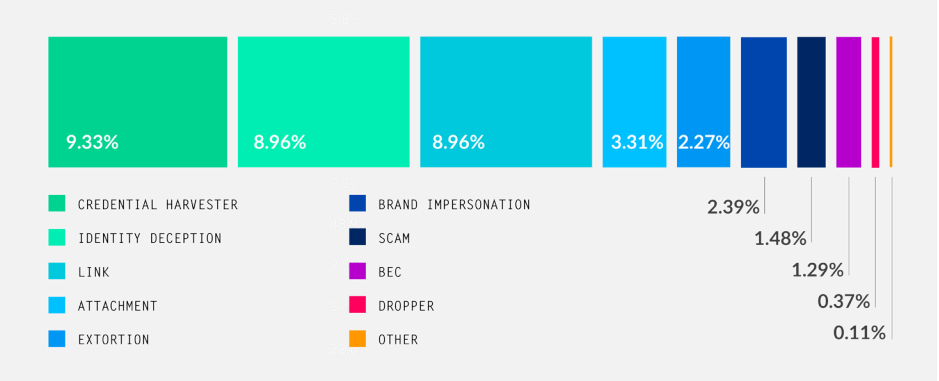
How did it end up like this?

Unlike the song by The Killers, there isn't a "brightside" to phish. (And you can blame us for getting the song stuck in your head.)

With unerring consistency, almost all breaches begin with an innocuous looking phish or an email. Low tech, low maintenance and practically free, phishing can be a profitable business model for attackers with low infrastructure costs due to the prevalence of inexpensive cloud-based email providers like Gmail. By using these legitimate hosting services, attackers can sneak under the email security radar straight into inboxes.

What looks like an harmless email from a long-standing vendor or even a routine email from the IT department can harbor devastating consequences if clicked, leading to shutdowns, loss of data or even financial costs in the millions. We cannot stress enough the importance of stopping these threats before they reach users.

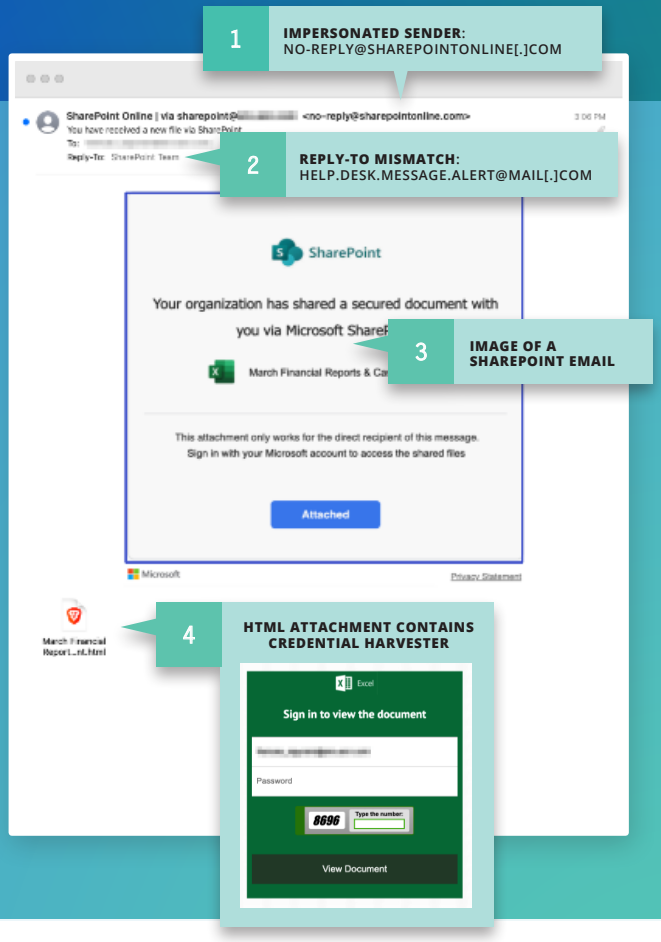
Here are the analyzed threat samples we discovered from May 1, 2020 to April 30, 2021 broken down below by volume.



(Detailed threat type descriptions can be found in the Appendix of the report.)

AREA 1 SECURITY

9.3% OF ATTACKS INVOLVED CREDENTIAL HARVESTING



Credential Harvesters:

Compromised Identities

When users open the front door, attackers don't need any backdoors. The largest threat type by volume in our findings, credential harvesters can refer to either the attack method or malware that steals a user's valid password, which is then used to gain access to unauthorized data.

Also considered a type of social engineering attack, credential harvesters typically start as a phishing email with a link to a fake login page made to look like a legitimate organization's site. Alternatively an email with weaponized attachments can also install credential-harvesting malware onto an end user's system.

While the websites and lures used range in sophistication, the most convincing attacks require advanced technology and trained security analysts to identify. By impersonating recognized brands and using legitimate cloud hosting services (e.g. Google Drive, Microsoft OneDrive, etc.) as part of their attack infrastructure, these attacks can bypass security systems and "security aware" users.

AREA 1 SECURITY

Supply Chain Attacks

Targeting Organizational Weaknesses (aka Your "Friends")

The SolarWinds and Kaseya incidents catapulted supply chain attacks into the spotlight due to its widespread impact and continued repercussions. As in this case, where many of the victims were renowned security organizations themselves, anyone can become a victim when attackers exploit trusted partners and third-party vendors.

Supply chain attacks don't all require surreptitiously sabotaging software to succeed. In fact, phishing attacks are one of the most common ways to start a supply chain attack. By compromising a trusted partner first, attackers can launch business email compromise (BEC) or ransomware attacks that result in financial loss in the millions. We'll explore these two attack types in more detail in the following sections.

TOP 7 ATTACK TECHNIQUES USED IN SUPPLY CHAIN ATTACKS

Compromised Partner IP / Domain

Attacker compromises a known good organization, sends messages using their domain and IP address.

Compromised Partner Account

Attacker compromises a valid organization. In some instances, organizations sending out phishing campaigns may be fronts or owned by threat actors.

Compromised Partner Account + URL Campaign

Attacker uses a compromised partner's domain to send phishing emails with links that host credential harvesters or malicious payloads.

Compromised Partner Account + New Domain

Attacker uses a new domain to send out phishing campaigns or reference new domains within a message from a compromised partner.

Compromised Partner Account + Malicious Payload

Attacker compromises a partner, leveraging a known employee name to send out messages containing a malicious payload.

Compromised Partner Account + Infiltrated Supply-Chain BEC

Attacker uses a compromised partner to send out BEC messages with no payload, often hijacking benign email threads to divert payment.

Partner Spoofing

Attacker spoofs a partner without actually compromising the partner. Domain spoofs or registered look alike partner domains are common.

AREA 1 SECURITY

Business Email Compromise (BEC):

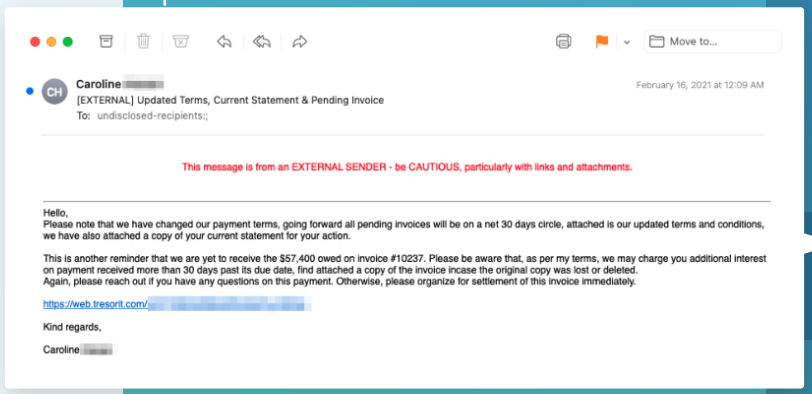
Low Volume, Low Tech, High Payouts

BEC attacks range from the easily recognizable spoofed sender to sophisticated supply chain attacks.

Type 3 and Type 4 both rely on exploiting established trust with existing partners and vendors. By adding in tactics like spoofing sender domains, hosting attachments in legitimate services and using timely lures, these malware-less attacks can create detection challenges for many security systems. Many Type 4 BECs also use partner account-takeover attacks where the partner victim is unaware they have been compromised. Later, the attacker pivots the thread to the attacker account to divert payment.

$57K
BEC FRAUD STOPPED

Attacker impersonates partner "Caroline's" account, sending an invoice-payment request from a malicious look-alike domain where two letters were transposed in the domain name (e.g. construction.com vs constrcution.com [not the actual domains used]). Attacker used legitimate cloud storage service Tresorit to host a fraudulent invoice.



BECS MADE UP ONLY 1.3% OF ATTACKS BUT WOULD HAVE RESULTED IN OVER

$354 MILLION IN DIRECT LOSSES

TYPE 1
Spoofed Executive, Sender or Domain

- *CXO as lures*
- *Inter-organization impersonation via spoofed sender and domains*

TYPE 2
Compromised Employee Account

- *Employees as lures*
- *Intra-organization impersonation via employee account takeover*

TYPE 3
Spoof Impersonating Supplier

TYPE 4
Infiltrated Supplier / Supply Chain Attack

- *Supply chain / partner employees as lures*
- *Inter-organization impersonation via spoof or supplier account takeover*
- *Long con with delayed call-to-actions*

AREA 1 SECURITY

Business Email Compromise (BEC): *Continued*

BEC TYPE 4 EXAMPLE

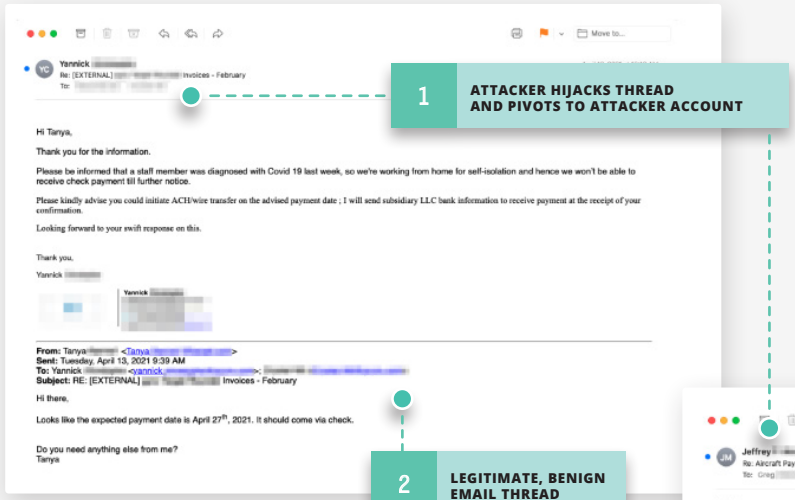
These attacks use partner account-takeovers to hijack legitimate, benign conversation threads before pivoting the conversation to the attacker's account

THE AVERAGE BEC REQUEST IS NEARLY

$1.5 MILLION

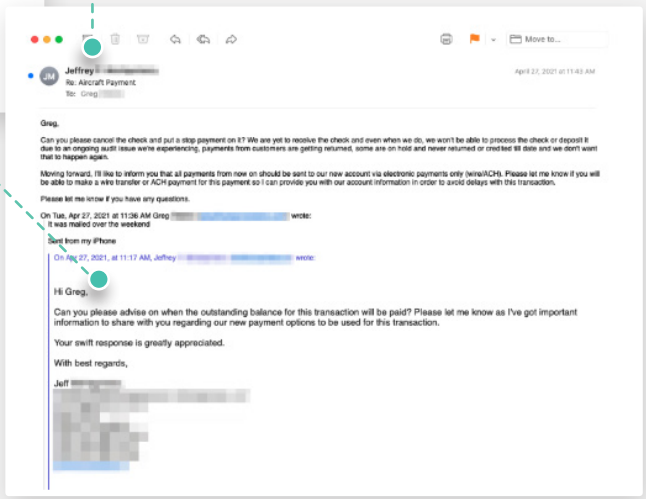
THE MEDIAN BEC ATTEMPT IS OVER

$260K



$4+ Million BEC fraud stopped

The attacker compromises a partner's account ("Jeffrey"), then hijacks a benign conversation thread. Sending from a malicious look-alike domain, the attacker pivots the thread to the attacker's account. The look-alike sender domain is identical to the benign sender domain but ends in .co instead of .com.



$250K BEC fraud with COVID lure stopped

The attacker compromises a partner's account ("Yannick") to hijack a benign email thread, pivoting the thread to the attacker's account. COVID lures are used to make the attack more convincing and timely. The malicious look-alike sender domain used is nearly identical to the benign sender domain; the attacker just added an extra letter (e.g. "buy.com" vs. "buvy.com" [not the actual domain used]).

AREA 1 SECURITY

Ransomware: *The End Stage*

High profile cases of ransomware such as the Colonial Pipeline attack, which also used credential harvesting, by now-defunct ransomware group DarkSide have prompted federal government warnings on their severity and disruption to services, not to mention their high financial costs.

In the case of Colonial Pipeline, the ransomware payment alone cost the company ***$4.4 million***, with additional system restoration costs estimated to be in the tens of millions. U.S. Homeland Security has cited losses from NotPetya, another "famous" ransomware variant, as high as ***$10 billion.*** Ransom demands have also increased, with the Kaseya ransomware claiming the largest demand on record at ***$70 million.***

The delivery of these devastating attacks are almost always via an email phish. In fact, the ransomware categorization only happens at the very end of the attack chain when data is already lost and a ransom demanded. Other than backing up data and having a recovery plan, **the most important thing an organization can do is to prevent that initial phish from getting in in the first place.**

FIVE RECENT RANSOMWARE TRENDS

01

Phishing has replaced remote code execution (RCE) as the preferred delivery method

02

Ransomware is increasingly sent via nested links in emails

03

Extortion is being used in conjunction with or as a backup for ransoms

04

The time between ransomware deployment to asset compromise has exponentially shortened

05

Threat actors are actively hiring in open marketplaces for "developers"

AREA 1 SECURITY

Ransomware:

How Ransomware Gets Executed On Victim Systems

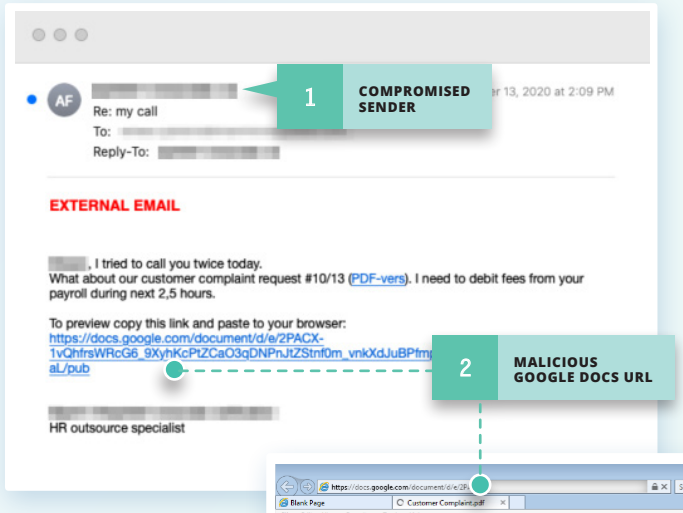
01 **Phishing emails are the first stage in the delivery mechanism**

02 **First stage loaders establish persistence via remote access trojans (RATs) for recon**

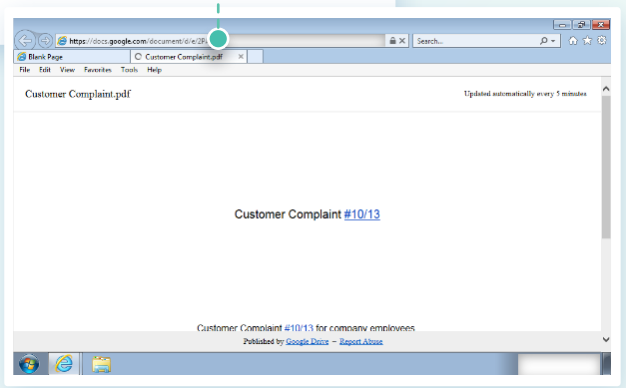
03 **Ultimate payload is delivered**

RANSOMWARE IS THE *FINAL* STAGE, NOT THE FIRST

RANSOMWARE EXAMPLES



Ransomware attacks are typically delivered through phishing attacks. In this example, a compromised sender sends a phishing email to a partner company. Nested links lead to the download of the BazarLoader malware, which eventually leads to infection with Ryuk ransomware.



The attacker uses a legitimate service (Google Docs) to host a seemingly benign page, seen below. If clicked, the link on this page leads to the download of the malicious payload.

AREA 1 SECURITY

Brand Impersonation:

Fake It Til You Make It

Organizations use their branding to establish reputation and cultivate trust with their customers. Attackers take advantage of this trust by using brand impersonation in their attacks.

Similar to identity deception, which we track separately, brand impersonation occurs when a threat actor impersonates a trusted company or well-known brand to add legitimacy to their phishing attack. Using stolen branding and images that are often identical to the legitimate brand, attackers use any methods to get victims to click.

As we saw in the earlier BEC example with COVID lures, these impersonations often focus on trending brands or events. With COVID as the main headline for the majority of 2020 and into 2021, it's no surprise that the World Health Organization (WHO) was the #1 most impersonated brand, beating annual "favorites" like Google, Microsoft and Target.

Top 10 Impersonated Brands

1. World Health Organization
2. Google
3. Microsoft
4. target
5. amazon
6. Pinterest
7. Marketo (An Adobe Company)
8. LinkedIn
9. facebook
10. T-Mobile

COVID Spotlight

As the use of web conference tools increased during the pandemic, attackers also began impersonating web conference brands. Here are top web conference brands ranked based on how often they're spoofed.

1. zoom
2. Cisco Webex
3. Microsoft Teams
4. Google Meet

THE TOP 10 IMPERSONATED BRANDS ACCOUNT FOR OVER 56% OF ALL SPOOF- AND IMPERSONATION-BASED PHISHING ATTACKS

IDENTITY DECEPTION IS USED IN NEARLY 9% OF ATTACKS

BRAND IMPERSONATION MAKES UP 2.4% OF ATTACKS BASED ON VOLUME

Vishing: *A Marriage of Inconvenience*

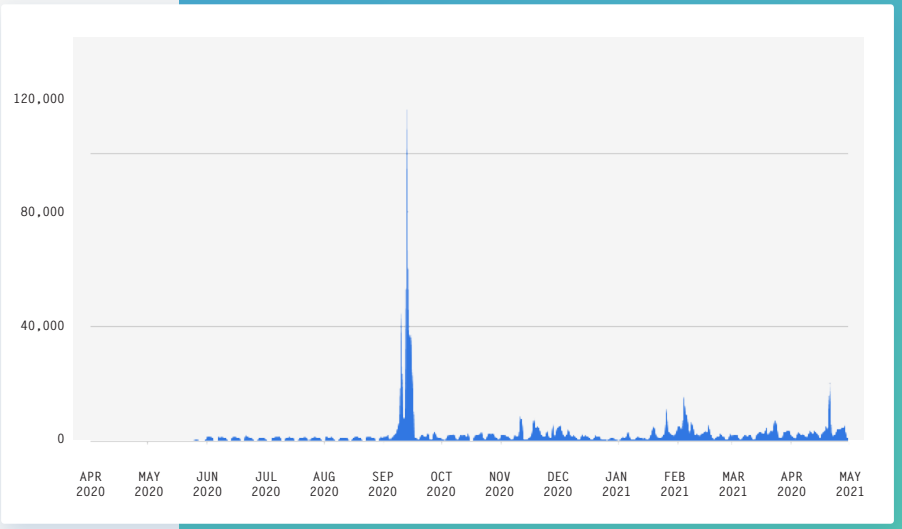
An interesting trend in the intersection of voice and email threats is vishing. Vishing, the short form for "voice phishing," usually refers to the practice of leaving fake voice messages in hopes that victims will call back to provide personal information which will be used in other attacks.

In our case, we have observed attackers combining email and voice vectors by sending emails with attachments of a voicemail recording, media file or a link to one. We have also observed attackers sending emails that had no malicious payloads, just simply a phone number. The attackers purported to be from reputable companies to entice targets to call the number and reveal personal information, such as bank details and credit card numbers. In some cases, the attackers would also attempt to walk victims through a series of steps on their computers that would result in the download of malware or would enable remote access to their system.

Cloud providers and traditional email security providers like Microsoft tend to miss these attacks, especially when the malicious link is embedded in an attachment. Combining obfuscations and redirections, attackers know these messages end up reaching the end user and will continue using these techniques until stopped.

Like many other attacks, an increase in vishing during a specific time period can indicate vishing campaigns. In our data, we saw a significantly high volume of vishing attacks in mid-September 2020, with smaller campaigns occurring around the winter holidays, February and May of 2021.

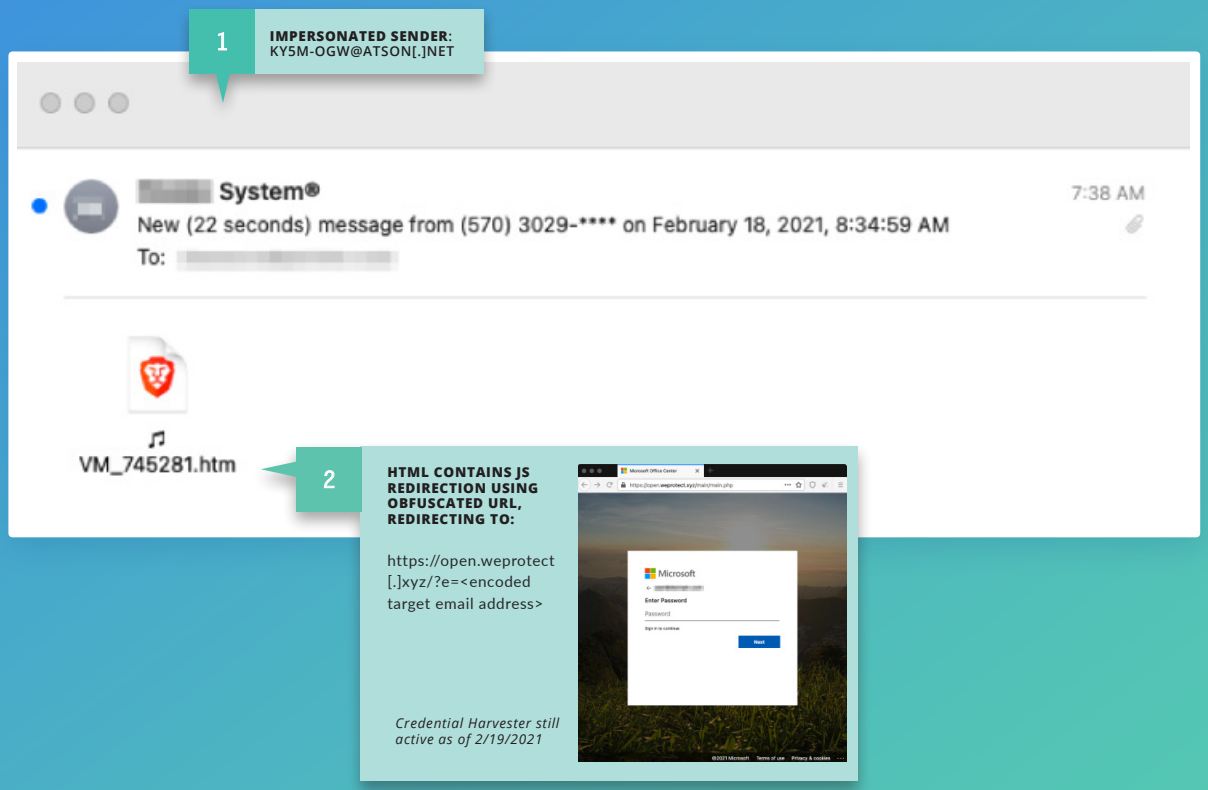
As seen in the chart below, vishing, like most cyber attacks, occur most frequently on weekdays when victims are more likely to check their emails.



AREA 1 SECURITY

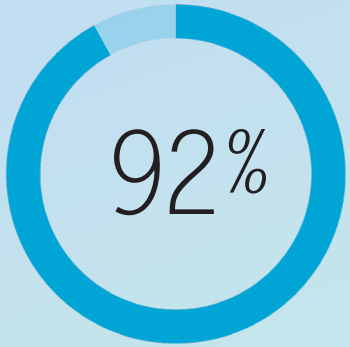
Vishing Example

In this example, the attacker uses display name spoofing to impersonate a legitimate organization. The email contains an .htm attachment purporting to be a voicemail message. In actuality, the attachment contains a Javascript redirection and obfuscated URL to redirect the victim to a credential harvester impersonating a Microsoft login page.



AREA 1 SECURITY

How Did We End Up Here?



MORE THAN 92% OF USER-SUBMITTED REPORTS ARE NOT MALICIOUS

Unlike spam and commodity malware, targeted attacks make up a relatively low volume, yet can cause substantial damage, as examples in this report indicate.

Attackers use a variety of tactics and techniques to evade detection from email providers and secure email gateways (SEGs). Tactics like leveraging stolen credentials fly under the radar since legitimate accounts and logins are used. Newly created domains used to spoof legitimate domains do not have any malicious reputation so can easily be missed by legacy security systems.

DOES SECURITY AWARENESS TRAINING AND USER-REPORTED PHISH WORK?

Security awareness training can be beneficial from an educational and awareness perspective, but it's not always effective at stopping threats. Many attacks use sophisticated impersonation techniques that fool all but the most skilled trained professionals. Not to mention with account takeover attacks, the victim typically does not even know they have been compromised.

User-submitted phish is often inaccurate and relying on these reports can increase time and resource costs for both end users and the IT/security department. In our findings, more than 92.1% of user-submitted "phish" were actually benign, spam or bulk mail. At the same time, security teams chasing after false-positives means less time to find and investigate actual threats.

AREA 1 SECURITY

Missed Threats within a One Month Period

Each row of missed threats in the chart below make up less than a 0.5% of that month's email traffic, but it just takes one missed threat to cause a security disaster. Our last column may also help put these threats in a different perspective.

ORGANIZATION INDUSTRY	EMAIL SECURITY SYSTEM USED	MISSED THREATS	TOTAL EMAIL VOLUME
Insurance Software	Microsoft 365	***517,968***	103,099,539
Pharmaceutical	Proofpoint	***448,440***	432,611,141
Food and Beverage	Cisco Email Security (IronPort)	***105,603***	420,088,334
Education	Custom	***90,763***	142,672,221

In Other Words....

More than *half a million* chances of a successful attack

Almost **15,000 threats in inboxes *per day*** for users to deal with

3,500+ user submissions a day IT has to deal with

45,000+ investigative hours for security teams *(at only 30 min per incident)*

AREA 1 SECURITY

Recommendations

Cyber criminals are always innovating, and staying a step ahead of them can be a challenge without the right people, processes and tools.
Here are our top recommendations to keep targeted threats out of your organization's inboxes.

01

LOCK DOWN IDENTITY

With attackers taking the easy route of stealing credentials, secure accounts and identities by adding additional protection likemulti-factor authentication (MFA).

Never reuse passwords and always change default passwords.

02

ESTABLISH PROTOCOLS AND PROCEDURES AGAINST FINANCIAL FRAUD

Establish and train on procedures to prevent financial loss in the case of BEC and financial fraud, such as requiring multiple approvers or "out-of-band" vendor verifications for transferring funds to new accounts.

Train users to avoid clicking on malicious content in phishing emails, but also train them on what to doif they fall for the phish.

03

TAKE A ZERO TRUST APPROACH WITH EMAIL

With email as the number one communication vehicle for organizations and attackers' rampant use of spoofing, it's imperative to verify all communication that happens within email.

Remove implicit trust by assessing the validity of messages beyond the sender to reduce risk from compromised partners. Choose a security system that can detect compromises and apply controls around compromised communications to extend zero trust to email.

AREA 1 SECURITY

Recommendations

Cyber criminals are always innovating, and staying a step ahead of them can be a challenge without the right people, processes and tools. **Here are our top recommendations to keep targeted threats out of your organization's inboxes.**

04

DON'T ALWAYS BELIEVE WHAT YOU SEE

Brand impersonations have gotten better with attackers hiring designers and stealing logos. Invest in solutions with advanced technologies like optical character recognition (OCR) parsing and natural language understanding (NLU) modeling to accurately detect phishing emails using impersonation and identity deception techniques.

05

FOCUS ON PREEMPTION

Threats are always easier to deal with before they reach end users. Implement security awareness, but don't rely on users to be the front line defense. With the majority of modern attacks starting with a phishing email, deploy a preemptive email security solution to keep threats out of your organization in the first place. Choose a cloud-based, dynamically scalable solution that uses advanced technologies to track attacker infrastructure to truly preempt attacks before they reach inboxes.

AREA 1 SECURITY

Area 1 Security uses advanced techniques, wide-scale threat indexing and attacker infrastructure tracking to preemptively detect and stop malicious attacks like those seen in this report from ever reaching inboxes.

To find out more about the attacks we're discovering, or to see what threats are already in your organization, we invite you to

SCHEDULE A COMPLIMENTARY PHISHING RISK ASSESSMENT

About Area 1 Security

Area 1 Security is the only company that preemptively stops Business Email Compromise, malware, ransomware and targeted phishing attacks. By focusing on the earliest stages of an attack, Area 1 stops phish — the root cause of 95 percent of breaches — 24 days (on average) before they launch. Area 1 also offers the cybersecurity industry's first and only performance-based pricing model, Pay-per-Phish.

Area 1 is trusted by Fortune 500 enterprises across financial services, healthcare, critical infrastructure and other industries, to preempt targeted phishing attacks, improve their cybersecurity posture, and change outcomes.

Area 1 is cloud-native, a Certified Microsoft Partner, and Google Cloud Technology Partner of the Year for Security. To learn more, visit **www.area1security.com**, follow us on **LinkedIn**, or subscribe to the **Phish of the Week** newsletter.

AREA 1 SECURITY

Appendix: Threat Type Descriptions

Credential Harvester — *Credential harvesters are sites set up by an attacker to deceive users into providing their login credentials. This type of attack presents the user with a page that imitates an account login page. Unwitting users who enter their credentials unknowingly provide attackers with the credentials to their accounts.*

Identity Deception — *Identity deception occurs when an attacker or someone with malicious intent sends an email claiming to be someone else. The mechanisms and tactics of this vary widely. Some tactics include registering domains that look similar (aka domain impersonation), are spoofed, or utilize display name tricks to appear to be sourced from a trusted domain. Other variations include sending email utilizing domain fronting and high reputation web services platforms such as G-Suite and O365.*

Link — *When clicked, a link will open the user's default web browser and render the data referenced in the link, or open an application directly (e.g. a PDF). Since the display text for a link (i.e., hypertext) in HTML can be arbitrarily set, attackers can make a URL look like it links to something benign while it is actually malicious. Malicious links can lead to arbitrary code execution or Remote Code Execution (RCE), credential harvesting, click fraud, unwanted installs or other compromises.*

Attachment — *An attachment is any file attached to an email that, when opened or executed, performs a series of actions set by an attacker. Attachments can often masquerade as other file types by using mismatching extensions or otherwise deceptive file names. Attachments can lead to malware installation, such as backdoors and remote access trojans (RATs), or contain links to other malicious content and files.*

Brand Impersonation — *Brand Impersonation occurs when a threat actor impersonates a trusted company or well-known brand to add legitimacy to their phishing attack.*

Extortion — *Extortion is a tactic used to coerce an entity to perform a set of actions they would not otherwise perform. Extortion is identified when an attacker contacts intended victims with instructions to follow in order to avoid compromise or release of sensitive data. Unfortunately, even following attacker instructions can still result in compromise. For this report, scareware is also included in this category. Scareware is a form of malware which uses social engineering to cause shock, anxiety, or the perception of a threat to manipulate users into downloading and/or buying unwanted software. Usually the purported malware isn't real and the software is non-functional or malware itself.*

Scam — *A scam is a broad category of fraud with the purpose of enticing a victim to provide money with the promise of a significant sum in return. The victim can be led to believe they are making an investment, which may involve the sender promising to pay the victim a large sum to transfer or process money, or may simply involve funding a fraudulent company for example.*

BEC — *Business Email Compromise (BEC) is an increasingly common, effective and costly targeted email attack that is designed to trick recipients into transferring funds, typically through forged invoices, to scammer accounts. BEC falls into various categories based on its sophistication, ranging from using a spoofed email to compromising a vendor in a supply-chain attack. In the latter example, it is not uncommon for the process to play out over several weeks while the scammer is grooming the victim by email and/or occasionally by phone. Our BEC ebook discusses the different types of BEC in more detail.*

Dropper — *A dropper is a malicious executable binary whose purpose is to decrypt, unobfuscate and/or extract a secondary malicious payload. Along with the malicious payload, the dropper may open a benign lure document to serve as distraction against the human target during the infection process. Typically, a dropper is extracted from a carrier file such as an Microsoft Office document, PDF, or other common container style document. Carrier files are usually engineered with an exploit that causes the viewing application to begin executing the attacker's code, leading to executing of the dropper and installation of malware.*

Other — *For the purpose of this report, other threat detection categories with statistically insignificant numbers have been consolidated into the "other" category. This includes IP policy (detection based on a customer-specific policy), target development (attacker information-gathering to facilitate a successful attack) and encrypted email (phishing messages that contain encrypted content as a means to circumvent email security systems), among others.*