2023 ANNUAL STATE of EMAIL SECURITY REPORT

ISSUED MARCH 2023

COFENSE

CONTENTS

LETTER FROM THE CISO

As I transition from behind the scenes of this report, I wanted to take a moment to share some of my thoughts on what we've seen over the past year. Taking on the role of CISO has added some additional insight as I stepped back into the role of practitioner again. Now that I review our cyber insurance and 3rd party questionnaires, it has given me perspective into why organizations have started asking more questions about simulation metrics.

Something that hasn't changed over the last year, your SOC still needs HELP! As teams continue to deal with workforce shortages, remote work and burnout, optimizing processes and automation are even more critical to defend the perimeter. As I've spent time with incident responders and attended conferences to hear from practitioners, it's clear the community demands products and solutions to integrate together rather than stand-alone products. It's this reason that we've continued to enhance our APIs, while also expanding our integration partnerships, allowing you to quickly identify threats hitting the inbox and moving those IOCs to your other controls to defend against the adversary quickly.

Have you followed the trend of adding a Cyber Threat Intelligence (CTI) team? We continue to hear from customers that are building out teams to become more proactive in defending against the threat landscape. But adding more threat feeds isn't productive – or helping your SOC automation. This is why we have stood firm on our "human-vetted" intelligence, to ensure you can depend on adding IOCs to your automation. It's more critical than ever to ensure your intelligence feeds are actionable intelligence allowing you to reduce noise and provide context to those alerts.

As I think about the conversations I've had with SOC teams, it's become clear they have a love-hate relationship with the reporting of suspicious emails versus employees just deleting them. Our intelligence is enriched because users report suspicious emails. The SOC can benefit from those suspicious messages being reported by extracting the IOCs and taking action to mitigate a threat. However, the button that is often used is the "delete" button by the user who is just flat-out annoyed with "spam" and wants it to stop. As I scanned through the simulation campaigns sent over the year, it suddenly occurred to me why users struggle with whether or not to report an email. It's because you're sending the wrong types of simulations, coupled with punitive programs putting additional pressure on the user to just report the email. Simulate the threats making it to the inbox – NOT the topics already blocked by your spam filters, aka your Secure Email Gateway. *I'm looking at you "eCard/Valentines" campaign fans.*

As you read this report, you'll find it difficult to identify the simulation section as we've reported in years past. That was intentional. For years we've pushed our security awareness teams to align their programs to "real phish." For the past few years, we've only added templates based on real phish we've observed. That too is intentional. But what you find are some highlights of what we observed over the year and how you can adjust your Security Awareness and Incident Response programs to better defend against the phishing threats making it to your users' inboxes. It has been an exciting year talking to customers who have experienced the impact of the network effect.

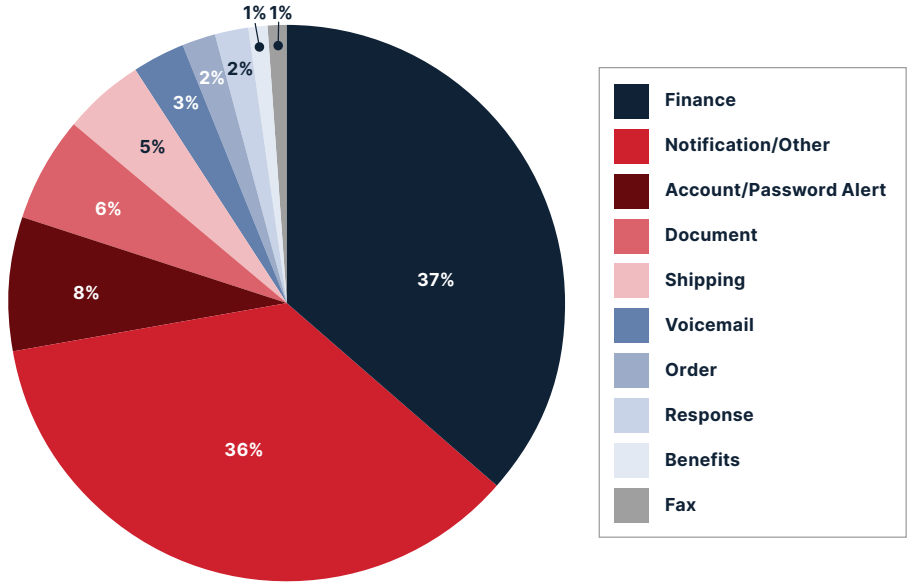
Tonia Dudley
VP, CISO at Cofense

> *It's more critical than ever to ensure your intelligence feeds are* ***actionable intelligence*** *allowing you to reduce noise and provide context to those alerts.*
>
> **Tonia Dudley**
> **VP, CISO at Cofense**

EXECUTIVE SUMMARY

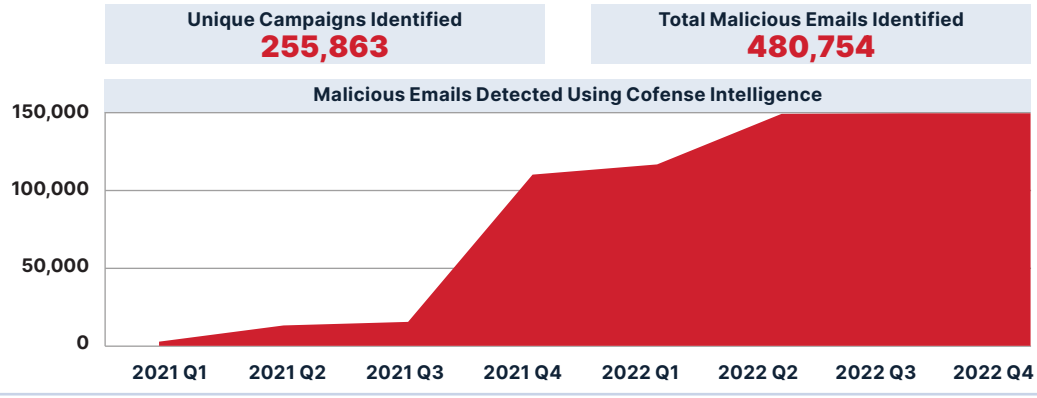
In 2022, cybersecurity threats increased exponentially and it's no surprise the vast majority involved phishing. As threats increase in frequency, intensity, and sophistication, the need for rapid and actionable intelligence has never been greater. As a result of this increased frequency, Cofense Intelligence saw 569% more malicious phishing emails, had a 478% increase in the number of credential phishing related Active Threat Reports published and identified a 44% increase in malware. Based on this data, we conclude that credential phishing was the cyber threat of choice in 2022.

FIGURE 1: TOP THEMES IN ACTIVE THREAT REPORTS



Due to this increase in threat activity, we were able to detect, auto-quarantine, and remove a record-setting number of malicious emails and phishing campaigns that were missed by Secure Email Gateways (SEGs) as seen in Figure 2.

FIGURE 2: COFENSE AUTO-QUARANTINE SUMMARY



Cofense Intelligence saw

569%

more malicious phishing emails, had a

478%

increase in the number of credential phishing related Active Threat Reports published and identified a

44%

increase in malware.

Thanks to the power of Cofense Intelligence, we saw a

626%

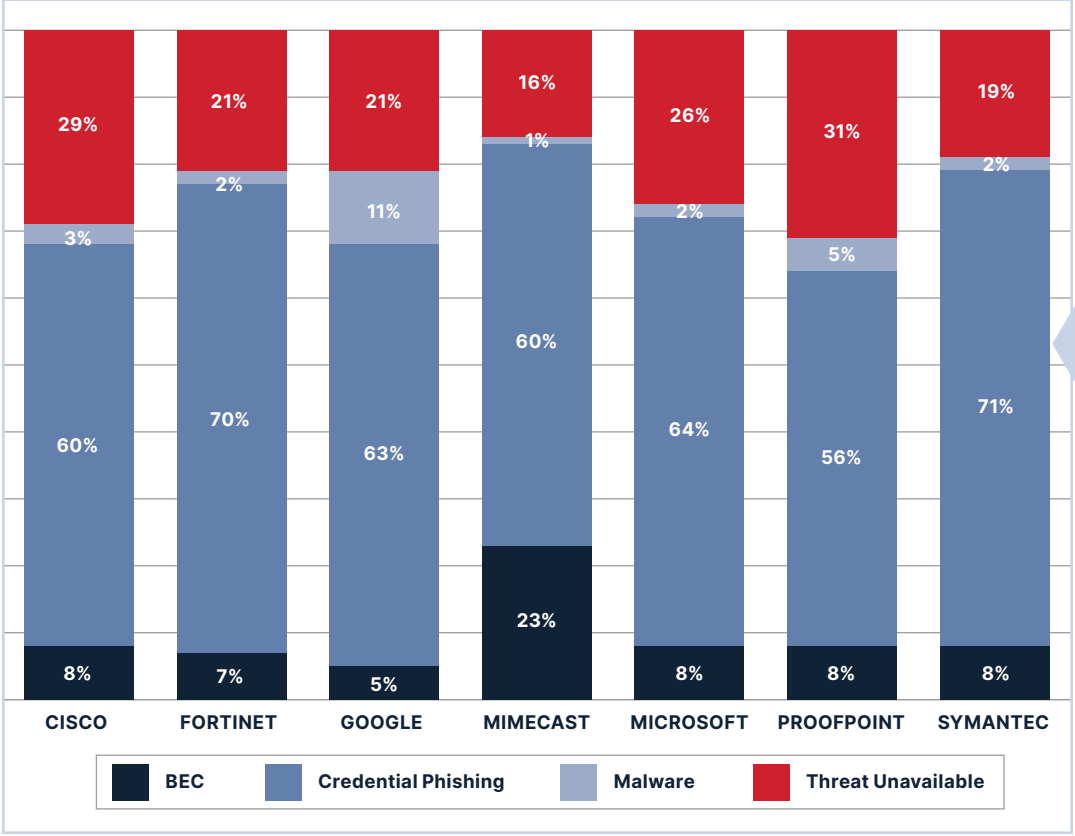
YoY increase in emails detected and auto-quarantined from customer inboxes worldwide.

Phishing is a major threat because it is so simple. Often, we hear of large, destructive attacks that sound extremely advanced, beyond the comprehension of security-minded individuals. It is important to remember the initial access is often acquired well before the incident occurs and may come from simple phishing campaigns that have no apparent connection to any advanced persistent threat group. In the aftermath, as these sophisticated attacks make the news, organizations should not become so consumed with searching for specific indicators of compromise (IOCs) or malware that they ignore the emerging phishing threats. As threats increase in frequency and intensity, it is not only critical, but a fundamental necessity to protect and defend against daily emerging phishing attacks.

Over the past decade, we have built an unrivaled standard of phishing expertise. Our goal is to contribute the phishing expertise necessary to turn humans around the world into the strongest link in the security chain, and to translate the resulting human efforts into machine learning, phishing threat intelligence, and automated action(s).

With our global network of 35+ million human reporters, we crowdsource millions of suspicious enterprise emails that are processed, enriched, and analyzed by our unique intelligence insights. At times, even removing threats within seconds before users have the chance to interact with them.

FIGURE 3: PERCENTAGE OF MALICIOUS EMAILS MISSED BY SEG IN 2022



How did your SEG stack up? These are real threats detected by our Phishing Defense Center (PDC) that are bypassing your current email controls.

Last year, we provided analysis on phishing threats with a 99.996% accuracy rate. Through our global network effect, we can identify trends and tactics and provide an understanding of what the phishing landscape will look like as we move forward in 2023. Our crowdsourced methodology provides an unparalleled aperture into the malicious emails that are reaching enterprise inboxes.

BASED ON OUR INTELLIGENCE, THE TOP FIVE HIGHLIGHTS OF THE EMAIL SECURITY LANDSCAPE ARE:

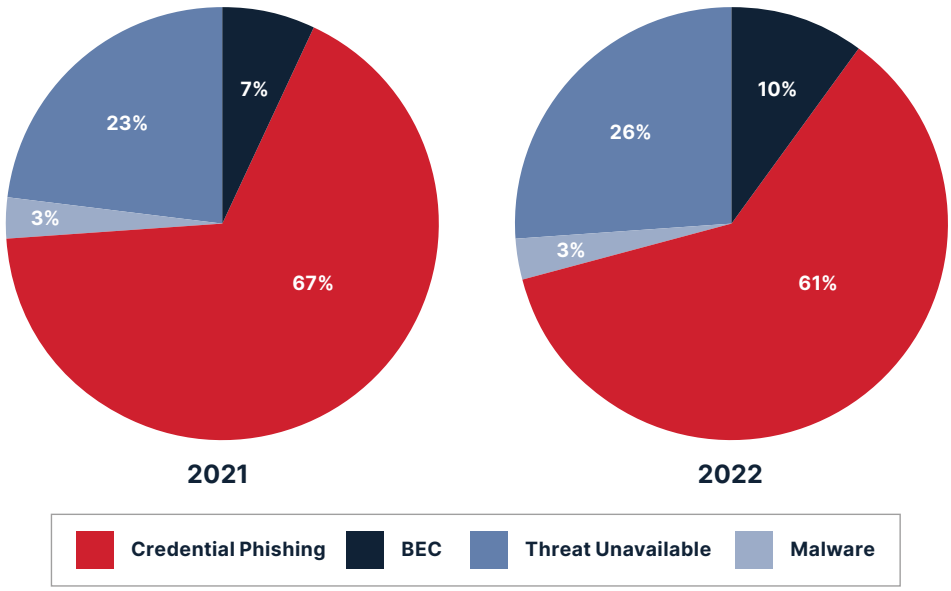
- **Credential Phishing is the top attack vector with a 478% increase in malicious emails identified**
- **Emotet & QakBot remain the top malware families to watch**
- **BEC continues to be one of the top cybercrimes for 8th year in a row**
- **Web3 technologies used in phishing campaigns increased 341%**
- **Telegram bots as exfiltration destinations increased 800%**

The cybersecurity landscape is always evolving, so it is imperative to stay on top of the latest trends and tactics. To learn more about what our intelligence trends revealed, here's a more in-depth look at what we discovered last year.

TOP FIVE Top Attack Vector in 2022: Credential Phishing

It was no surprise to see credential phish still rank as the leading threats seen by our Phishing Defense Center (PDC) customers. As one of the several collection inputs to Cofense Intelligence, it's also no surprise to see an increase of 478% of credential phishing-related Active Threat Reports published. This threat category still plays a significant role in the ransomware attack chain, as well as BEC. Wait, BEC? How does that connect? When a user falls susceptible to a credential phish, while the password may have been reset, the threat actor remains persistent in the inbox by adding auto-forwarding rules for keywords related to financial transactions (i.e. invoice, purchase order, quote). These emails are then, in turn, used to target downstream organizations with BEC/Vendor Email Compromise threats.

FIGURE 4: MALICIOUS THREATS OBSERVED BY PDC



As one of the several collection inputs to Cofense Intelligence, it's also no surprise to see an increase of

478%

of credential phishing-related Active Threat Reports published.

TOP FIVE Emotet & QakBot Remain the Top Malware Families to Watch

Throughout 2022, we analyzed and assessed top malware families seen in Figure 5. However, in this report, we wanted to provide a quick reference guide for understanding the malware families that made up the highest volume of phishing campaigns disseminated in 2022.

There are several characteristics that can make a malware family more appealing to threat actors, such as the malware features, cost, and complexity. In combination, these properties determine how well malware aligns to a threat actor's agenda for a phishing campaign. Figure 5 shows the top 5 malware families in 2022.

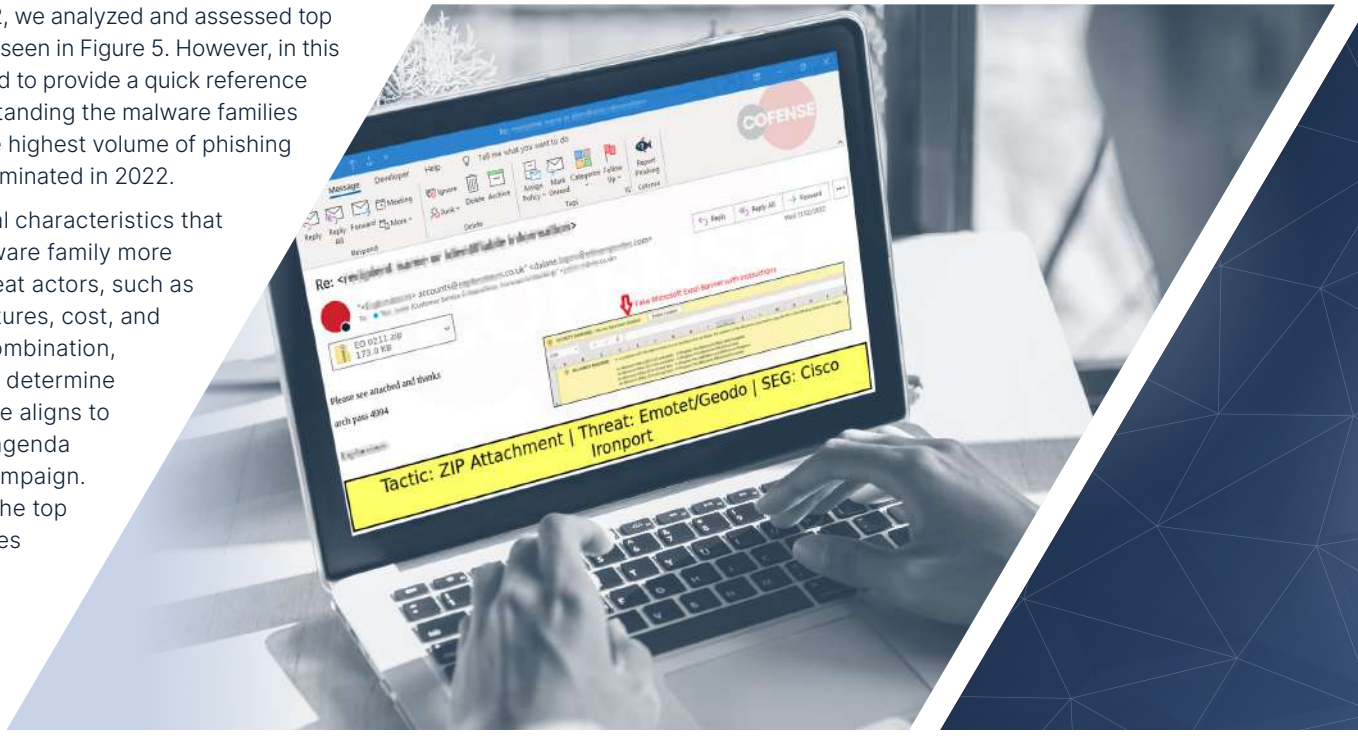
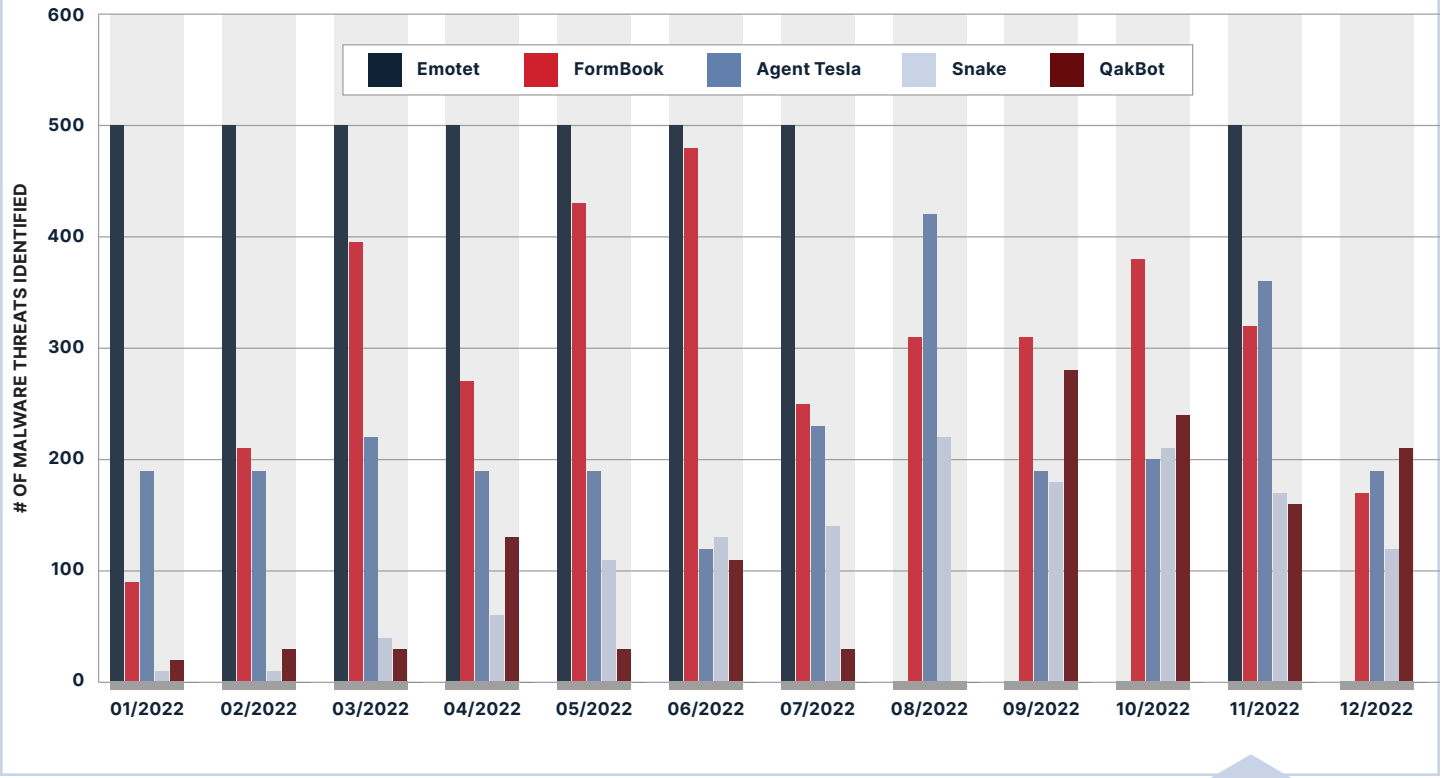


FIGURE 5: TOP 5 MALWARE FAMILIES IN 2022



The continued position of Emotet (and consequently malware loaders, which are often the first stage of a compromise) at the top of the list is a testament to its outscaling of all other malware-delivery campaigns. There was an overall increase in volume for keyloggers and Remote Access Trojans (RATs). Information stealers saw the largest increase with malware families like FormBook being high commodities in the phishing threat landscape. We continued to watch Snake Keylogger in 2022, which is a staple in the phishing threat landscape as it is a keylogger written in .NET. It can monitor a user's keystrokes, scan applications to steal saved credentials, and exfiltrate this data through a variety of protocols. Although it is not as popular as other malware families such as FormBook or Agent Tesla, it did maintain a significant presence throughout 2022, and its usage continues to increase. This banking trojan malware type passed RATs due to a high volume of QakBot phishing emails. Despite not having as high of volume as others in the Top 5, Qakbot remains at the top of our list of families to watch since it has been far more successful at bypassing SEGs and reaching inboxes.

Want more detailed insights on Emotet and QakBot? Make sure you read the strategic analysis starting on page 15!

Figure 6 shows the most common characteristics of each malware family and the capabilities that we observed in phishing campaigns of malicious emails that would have reached inboxes.

FIGURE 6: MALWARE CHARACTERISTICS

MALWARE FAMILY	INFORMATION	KEYLOGGING	REMOTE ACCESS	LOADER CAPABILITIES	BACKDOOR CONTROLS
Emotet/Geodo	✓			✓	✓
FormBook	✓	✓			
Agent Tesla	✓	✓	✓		
Snake	✓	✓			
QakBot	✓	✓	✓	✓	✓

TOP FIVE BEC Continues to be One of the Top Cybercrimes for the 8th Year in a Row Related to Financial Losses

In 2022, Business Email Compromise (BEC) continued to be one of the leading cybercrimes related to financial losses for the 8th year in a row. With BEC responsible for billions in global losses with victims in 90% of the world, it's no wonder scammers outside of Nigeria have started taking notice of the successes of BEC. While SEGs have evolved from spam filters to now being used to detect and potentially block malware, malicious links, and ransomware attacks, many fail at detecting conversational-based phishing attacks such as this.

Over the last year, BEC actors attacked with many different techniques, including requesting checks, wire transfers, payroll diversions, and gift cards. While many of these techniques are nothing new, we have observed a continued blending of tactics to make detection and mitigation even more difficult for organizations. By using and blending these attacks, threat actors continue to bypass SEGs to manipulate users into sending billions of dollars year after year.

Successfully Bypassing Two-Factor Authentication (2FA) to Gain Access to Accounts

By putting the "compromise" in BEC, threat actors continued to use credential phishing attacks to gain access to organization inboxes to perform man-in-the-mailbox (MiTMbox) attacks. Once an attacker gains access to an organization's email account, they will routinely create email forward rules to monitor all traffic coming in and out of the account. In some cases, they will create rules that include the words "purchase order," "invoice," or other financially based transactions between clients.

Once the threat actors identify an invoice or opportunity to re-route the transaction, the threat actors pounce, replying to the known and trusted email thread with new information. In some cases, this will come from a look-alike domain, and in other cases this will come from the compromised infrastructure itself. By modifying and forging invoices with new banking and account numbers, scammers are able to re-route business transactions and invoices to accounts under their control. Unfortunately, many of these attacks are caught too late for a successful financial reversal.

One of the best ways to mitigate against these attacks is to use two-factor authentication (2FA), as the requirement for a second piece of information makes it virtually impossible to log into an account without the second piece of information. However, in 2022, Microsoft published a technique used by scammers called adversary-in-the-middle (AiTM) that successfully bypasses 2FA authentication. Through hijacking the session cookie, BEC attackers are able to gain access to the user's account.

Payroll Diversion Attacks Still Flying Under the Radar

"Are you in the office? I need to update my direct deposit. Can I provide a voided check?" is still a technique used by BEC actors today. Dubbed payroll diversion scams, threat actors target Human Resources departments that have financial authority to change the financial records of employees. While attackers made a shift in mid 2014 to target enterprises and corporations, these attacks largely go unreported due to the same stigmas and lower losses as gift card scams. We continued to track wave after wave of payroll diversion attacks through our Cofense Reporter™ submissions from customers, meaning these attacks are still successfully bypassing email gateways.

BEC THREAT TECHNIQUE

"Are you in the office? I need to update my direct deposit. Can I provide a voided check?"

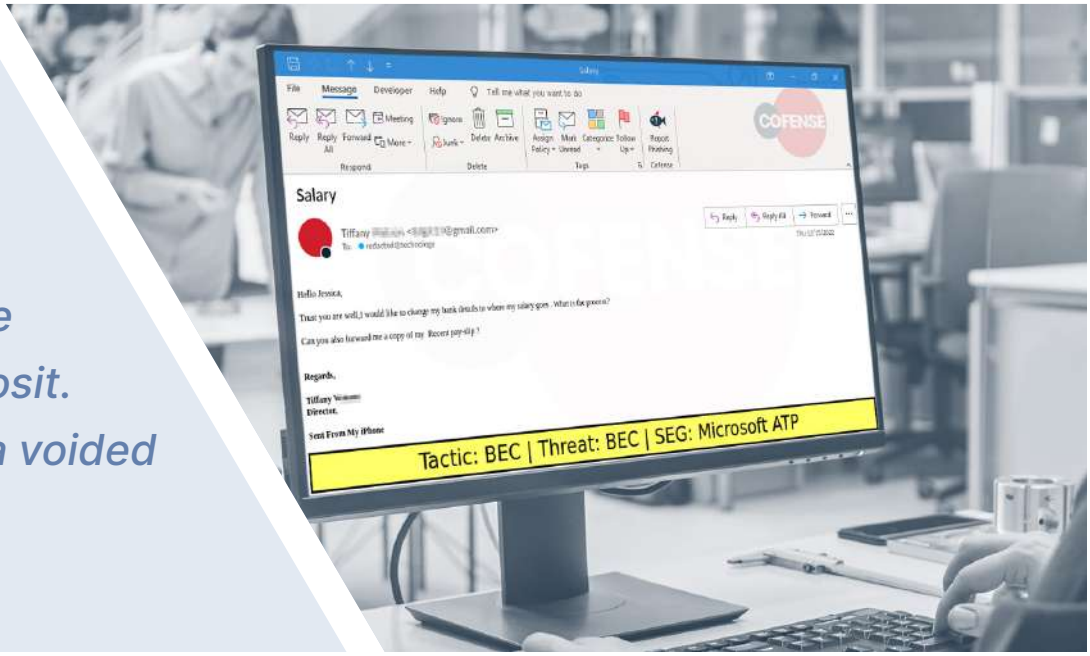
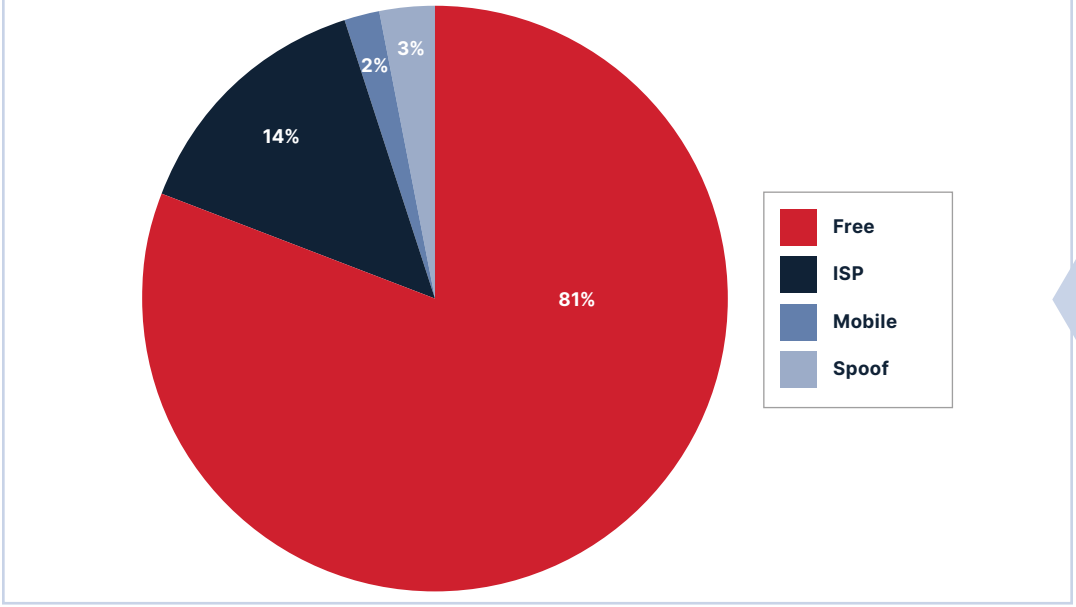


FIGURE 7: BEC DOMAINS



What do you get when you analyze 10,000 email accounts used to send over 25,000 emails? You get visibility into which type of email accounts used by threat actors go undetected.

Also noteworthy, we saw that nine different customers received an email from the same email address, which is clearly a spoofed domain.

Law Enforcement's Takedown of Cybercrime

Although BEC, ransomware, and other cybercrime operations carried on through 2022, our research indicated that threat actors felt pressure from the arrests as law enforcement agencies worldwide made significant strides combating cyber threat actors. Authorities arrested individuals suspected of involvement in the LockBit ransomware and JabberZeus banking trojan operations. The FBI infiltrated the Hive ransomware group starting in July, ultimately leading to the takedown of the entire operation in January 2023. Authorities in several countries arrested dozens of suspected BEC perpetrators, as well. Ransomware attacks and payouts both trended downward compared to 2021. If authorities continue to make high-impact arrests, we expect to see more downward pressure on phishing threats, as actors will be forced to adapt, harden their operations against intelligence efforts and/or decentralize.

SCAMMING THE SCAMMERS

To dig deeper into this conversational tactic, we spent some time interacting with real emails reported by users. In phases one and two of a multi-part study into the criminal ecosystem of gift card attacks, we responded to BEC phishing attacks to gauge the level of interaction from the scammers. During this phase of the research, we wanted to see how many responses it took to identify the cash out method for BEC attacks.

In phase one where we simply analyzed the delivery email, 6% of the analyzed emails presented themes of gift cards in the initial phish. In phase two, we responded to the scammers to try and identify the phishing theme. In 22% of these cases, we were able to identify gift card requests from the scammers. The significant jump signifies that for most gift card BEC attacks, scammers are looking for a response prior to asking for gift cards.

Attackers Still Request Gift Cards in 2022

In part three of our gift card study, we launched a successful counter-operation against BEC actors to better understand the gift card ecosystem plaguing organizations and small businesses. Just like many types of BEC attacks, scammers pretend to be someone in the organization with authority, asking for a quick or urgent task to be done. Once the user confirms, they're instructed to go to a retail store to purchase gift cards in different denominations. In some cases, attackers request the users' phone numbers to move the conversation outside of an organization's security structure and detection.

But what happens when scammers ask for gift cards? And more importantly, what happens when they *receive* gift cards? We took $500 dollars of gift cards and gave them to the scammers. We wanted to see what the conversations looked like, how quickly they were cashed out, and what insights we could gather from the research. Here is what we learned.

For the research, we used $25 worth of gift cards in each phish. While scammers typically asked for $500 or $1,000 dollars in gift cards, our researchers' true intent was to get cards in larger denominations, such as $100. It was surprisingly difficult to get the scammers to accept a $25 gift card as it broke their script and thought process for what was normally received, causing them to question the legitimacy of the funds soon to be stolen. Secondly, once the cards were sent the entire workflow was 24 hours or less for the card to be stolen, sold, then re-laundered into purchasing other goods online. We identified toy stores, greeting card stores, Amazon, and several other strange purchases once the cards were sold.

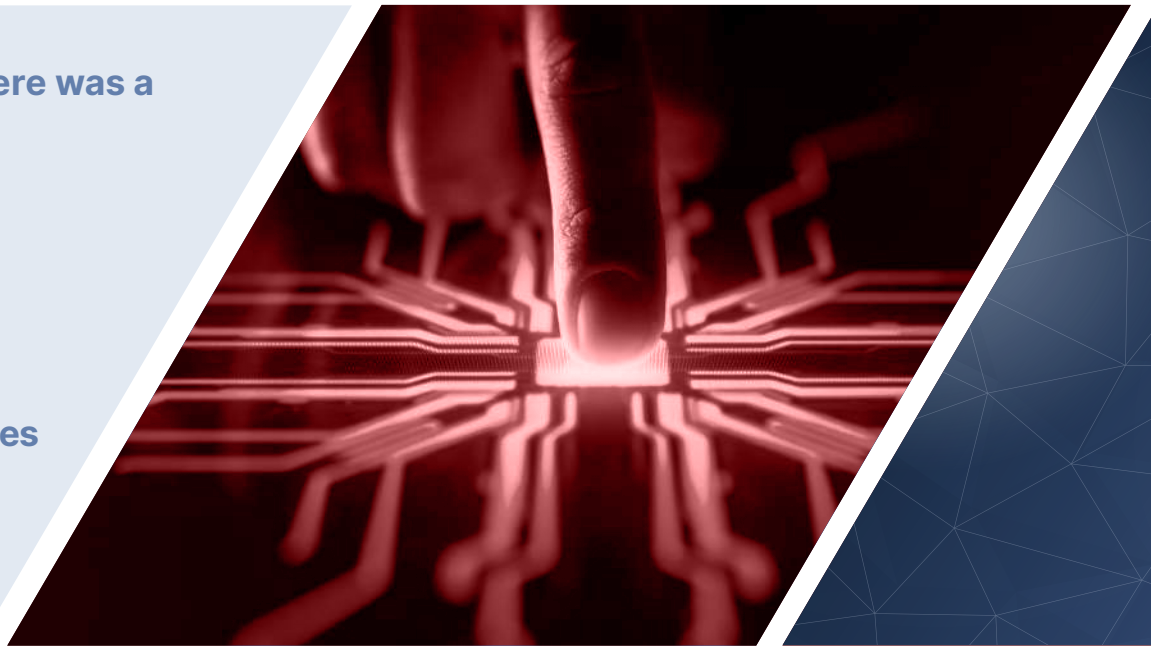
TOP FIVE Web3 Technologies Used in Phishing Campaigns Increased 341%

It's important for threat actors to carefully craft links or carefully select hosts for links in order to bypass SEGs. The malicious use of Web3 technologies as a link-crafting tool for phishing campaigns exploded in 2022. "Web3" refers to a set of technologies intended to decentralize common internet and computing activity. Users of Web3 protocols host content collaboratively, which removes the need for traditional hosting servers and makes censorship much more difficult. A fast-growing number of phishing campaigns used Web3 platforms to host malicious content throughout 2022, as evidenced by our strategic analysis, "Abuse of Web3 Technology for Evasive Phishing Grows Massively in 2022". Overall, in 2022 there was a 341% increase in Web3 Technologies used in phishing campaigns. Most browsers still require a "gateway" server to interact with Web3-hosted content, which gives organizations a chance to detect and block it. However, the technology will likely remain a useful weapon in threat actors' arsenals for the foreseeable future.

Overall, in 2022 there was a

341% INCREASE

in Web3 Technologies used in phishing campaigns.



TOP FIVE Telegram Bots as Exfiltration Destinations Increased 800%

Among phishing emails reaching inboxes over the course of 2022, the utilization of Telegram bots as exfiltration destinations for phished information increased gradually but significantly, resulting in a year-over-year increase of more than 800% between 2021 and 2022. The increase is largely associated with the now popular tactic of using HTML attachments as delivery mechanisms in credential phishing. While Telegram bots being used by threat actors to exfiltrate information is not new, it has not been commonly known for its use in credential phishing. Telegram bots have become a popular choice for threat actors, since they are a low-cost/free, single-pane-of-glass solution. Threat actors appreciate the ease of setting up bots in a private or group chat, the bots' compatibility with a wide range of programming languages, and ease of integrations into malicious mediums such as malware or credential phishing kits. Coupling the ease of Telegram bot setup and use with the popular and successful tactic of attaching an HTML credential phishing file to an email, a threat actor can quickly and efficiently reach inboxes while exfiltrating credentials to a single point, using an often-trusted service.

Among phishing emails reaching inboxes over the course of 2022, the utilization of Telegram bots as exfiltration destinations for phished information increased gradually but significantly, resulting in a year-over-year increase of more than 800% between 2021 and 2022.

PHISH SWIMMING IN MURKY WATERS

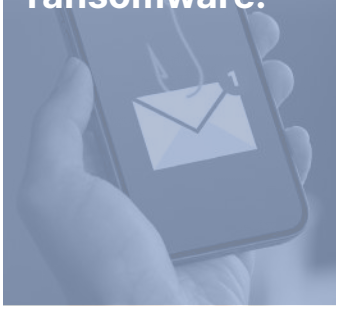
Downstream Impacts, Ransomware

The FBI's 2022 ICS report states that phishing email is the top crime for ransomware that targets organizations around the world. Ransomware is a primary downstream impact from email-based threats. In one common scenario, other malware families are delivered initially to gain a foothold, then followed by installation of ransomware anywhere from hours to weeks later. In another scenario, a credential phishing email campaign gives the threat actor credentials they can use to access systems to deploy ransomware directly. In both cases, it is important to look upstream at the chain of events that led to the ransomware and determine the payloads delivered within the email.

In 2021, there were well-known instances of BazarBackdoor being used to deliver ransomware. However, in 2022 there was a combination of phishing threats and we cannot point to one single major malware used to deliver ransomware. Rather than focusing on the outcome such as ransomware, readers should focus on credential phishing, delivery mechanisms, and the malware type known as "loaders" which can be used to deliver ransomware. It is preferred to use tools to help prevent the delivery of malicious-based emails. Operators of malware families like Emotet and Qakbot that offer the services of installing other malware on already-compromised computers (called "malware-installation as a service") are prime options for ransomware operators to gain initial entry. These services become partner or "affiliates" in a ransomware operation. In November of 2022, Qakbot was identified as the primary malware foothold used by the Black Basta ransomware gang.

While it is critical to monitor for ransomware at the endpoint, security teams may reduce the frequency and impact of endpoint events by focusing on credential phishing and an early-stage malware from malicious email campaigns that can in turn be used to deliver ransomware. We analyze these threats at great lengths and provide unique human-vetted expertise and analysis with actionable insights. We treat each malware infection as a potential vector for future ransomware attacks, reverse engineer the payloads and trace the steps that led to the infection to enable our customers to determine the flaws in their defenses and prevent phishing attacks. Using solutions such as Cofense Intelligence to help detect and prevent infections, while training employees to recognize and avoid interacting with malicious content can provide an intuitive line of protection that machines are not capable of. Phishing tactics are always evolving and becoming more complex.

In 2022, threat actors used a combination of phishing threats and we cannot point to one single major malware used to deliver ransomware.



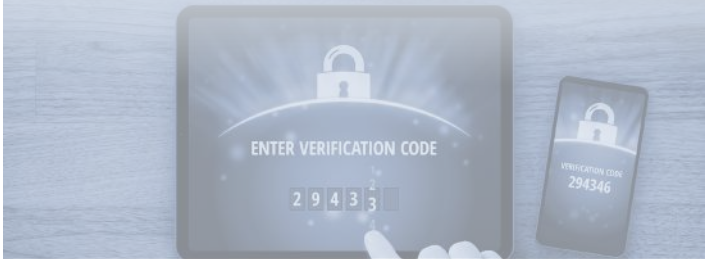
Big Breaches

Data breaches in 2022 seemed to come fast and furious, impacting several high-profile brands in the security sector including Cisco, Okta and LastPass. Large data breaches like this can be part of a cyclical pattern that involves phishing, since data breaches can begin with a phishing attack or contribute to future phishing activity.

- In May 2022, Cisco experienced a cyberattack where the attacker had to go to extreme lengths to hack into an employee's personal Google account that contained passwords synced from their web browser. Besides the credential theft, there was an additional element of phishing called vishing (voice phishing) and multi-factor authentication (MFA) fatigue where the threat actor prompt bombs the user with a flood of user authentications in hopes they will enable the attacker to gain unauthorized access. Once the threat actor has a foothold, they build their own backdoor accounts for access.
- In August 2022, the Okta event occurred where threat actors obtained credentials and unauthorized access to Workforce Identity Cloud (WIC) repositories hosted in GitHub and copied source code. Days after the Okta event, LastPass had an incident where credentials were obtained to extract information from a backup stored in a cloud-based storage service. The adversary copied customer vault data which was stored in a "proprietary binary format" that contained unencrypted data, website URLs, usernames and passwords, secure notes, and form-filled data.
- In August 2022, LastPass' incident opened the door to an even larger data breach in December which included user account information, billing, email addresses, telephone numbers and IP addresses. LastPass' big data breach affected users across their product suite, eventually disclosing loss of source code.

When large data breaches occur, it often results in the exposure of sensitive documents, personal information of employees or customers, and system, network, and application credentials. Compromised credentials may provide the threat actors responsible for the breach with temporary illicit access, but after the breach is discovered and/or publicized, it is much less likely that the credentials for those specific accounts will be useable. Instead, other sensitive and proprietary information (especially if published by the threat actors) can be employed in future phishing campaigns. Email addresses may be added to phishing target lists, and business process information may be used to craft targeted spear-phishing emails. Threat actors can also use information obtained from data breaches to conduct future credential phishing attacks. Credential stuffing attacks use stolen credentials from one website or system to gain access to other websites/systems where the user has the same credentials. Threat actors then continue the train of impacts by once again using any discovered sensitive information such as contact lists, new credentials, and business processes to boost future phishing activity and attacks.

Threat actors use sensitive information such as contact lists, new credentials, and business processes to boost future phishing activity and attacks.



World Events

Many major events happened across the globe over the course of 2022. Threat actors use these events on the world stage to design phishing campaigns. The Russia-Ukraine War captured the attention of many over the course of 2022. Cofense Intelligence observed a variety of phishing campaigns using the Russia/Ukraine conflict. Threat actors are weaponizing the conflict for financial gain by creating well-crafted credential phishing campaigns and donation scams. Threat actors using current events as themes within their email campaigns is quite common, and users should be universally vigilant against these threats. We have also seen a combination of lure tactics with a variety of emails using the Russia/Ukraine war as a lure reported to the Cofense Phishing Defense Center directly from enterprise users' inboxes. Other major world events used in campaigns include the death of Queen Elizabeth II and the Beijing Winter Olympics.

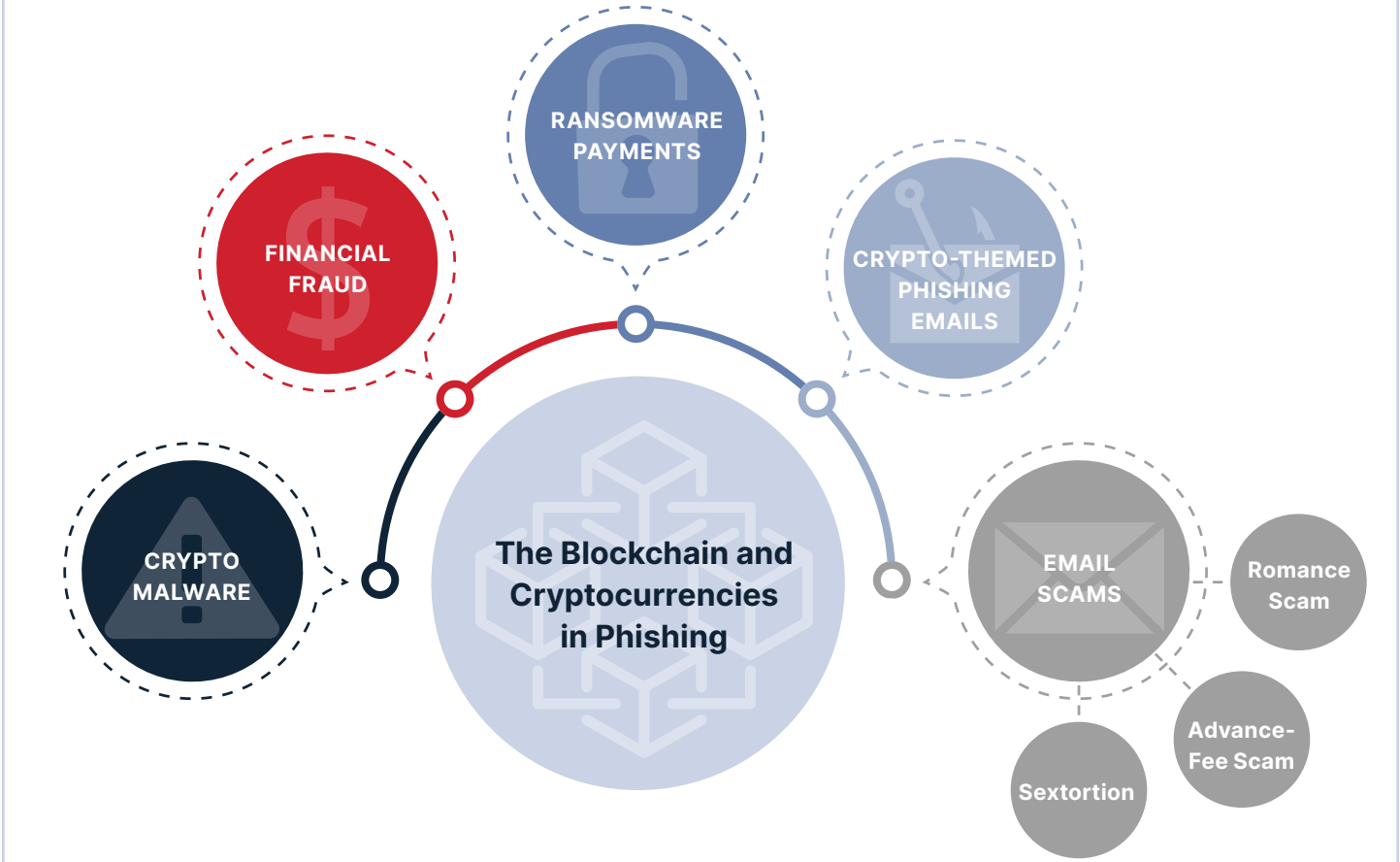
We observed that it is significantly more likely a tried-and-true phishing themes will be used rather than a stand-alone current event theme (as actors use a combination of methods and tactics). There will always be attempts to convince the receiver their mailbox is full and their password needs to be updated. Attached invoices of all sorts will make it to people's inboxes, along with shipping receipts, deposit receipts and voicemails. These sorts of lures were in the background throughout the year. Threat actors will be opportunistic with world events, but there is typically no reason to change from the more traditional (and dependable) lures, especially as those methods have proven to work. We continue to monitor phishing threats related to world events and will continue to identify malicious campaigns that are using the current events as a lure to target end users.

Blockchain, Cryptocurrency and NFT Phishing

Blockchain technology and cryptocurrencies are a popular topic for the general media, and consequently, a target for threat actors seeking financial gain. The blockchain is a public ledger used to store virtual currency secured by cryptography, or cryptocurrency. This type of digital currency differs greatly from legacy currency, such that banking controls for legacy currency make it difficult, if not impossible, for attackers to move currency out of an account. In contrast, a crypto wallet can be emptied almost immediately and the funds are unrecoverable.

Throughout 2022, we observed crypto-themed emails and phishing campaigns seeking to obtain digital wallets that contain tokens, but these are not the only malicious purposes for the digital assets. Due to the less-than-secure account controls, cryptocurrency is commonly used as payment methods for ransomware and sextortion campaigns, as well as within advance-fee and romance scams. Certain malware families also seek to steal cryptocurrency wallet keys stored on infected machines, while others are designed to use an infected machine to mine cryptocurrencies.

FIGURE 8: THE BLOCKCHAIN AND CRYPTOCURRENCIES IN PHISHING



We analyzed an uptick in crypto phishing emails, including one observation where threat actors used a convergence of crypto and the Russia/Ukraine war. The phishing email used the current Russia/Ukraine war as a lure to steal Bitcoin wallet data. We also detected another phishing threat spoofing OpenSea just days before they reported a successful attack that impacted seventeen users to steal over $1.7 million worth of non-fungible tokens (NFTs). This campaign used the excitement of a sweepstakes prize to lure victims to a spoofed OpenSea landing page. Threat actors used the domain "open-sia[.]io" to host the phishing page, which appears similar to the legitimate site. Once on the site, users were met with a spoofed OpenSea home page with the addition of a prize NFT at the top of the page. Users were requested to connect their wallet to claim the prize, even if it is already connected to their OpenSea account. Threat actors were seeking to gain access to a victim's digital wallet by requesting they enter their private key, mnemonic phrase, or attach their keystore file. The email was strategically crafted by threat actors and was successful in reaching enterprise users. Again, threat actors use multiple phishing methods to lure victims to obtain credentials for theft.

Crypto Phishing has seen a spike due to the transition from private individual use to increases in corporate and investment use. Once tokens are sent to a new wallet, the assets are unrecoverable for the financially motivated threat actor, which greatly increases the appeal of future attacks.

Crypto tokens are fungible, meaning they can be bought and traded several times much like a company stock. NFTs are also stored on the blockchain but are non-fungible, and they are often defined as 'one-of-a-kind' tokens that can be depicted by anything digital such as a drawing or animation. Cryptocurrency and NFTs have both become a way to make purchases, exchange currency, and invest. Organizations and users often exchange cryptocurrency and NFTs through online platforms like OpenSea or Coinbase. Many crypto- and NFT-themed phishing emails we have seen can be classified as credential phishing and are often finance-themed. Threat actors will spoof secure online platforms and even include links to domains they have registered that appear similar to legitimate sites. The overall goal of these campaigns is to gain access to a user's digital crypto wallets or NFTs, which are often accomplished by compromising login credentials, private wallet keys, security phrases, and keystore files. As a comparison, using SWIFT to send a bank wire can have some success in recovering a wayward wire sent to the wrong account number. This is not the case for digital assets; once tokens are sent to a new wallet, the assets are not recoverable. This greatly increases the appeal of these attacks for the financially motivated threat actor.

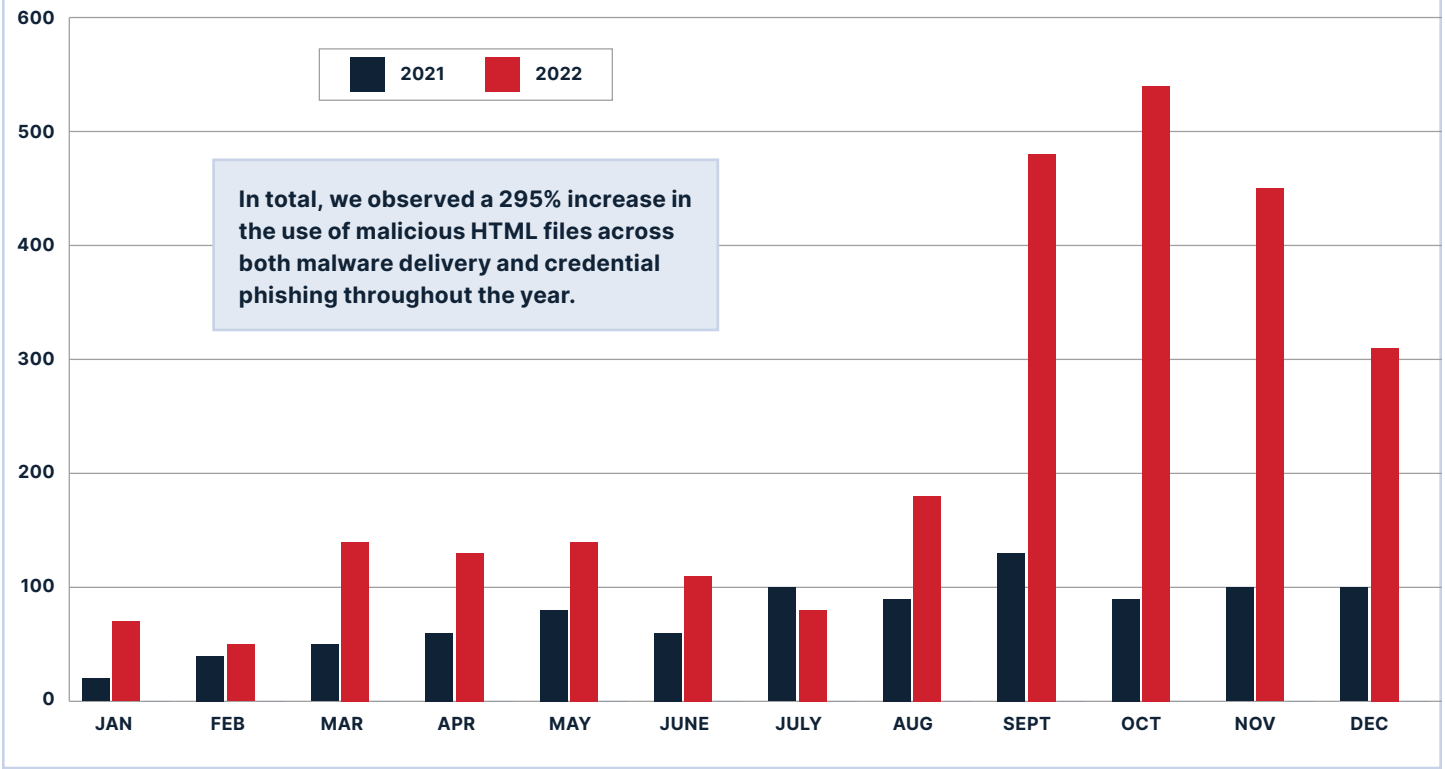
Energy Sector (Critical Infrastructure) on High Alert

Energy companies and other critical infrastructure organizations were on high alert in 2022, following a series of high-profile ransomware and phishing email-based attacks observed in the previous year. Although they remained prime targets for high-volume credential phishing campaigns throughout the year, fewer organizations were breached compared to 2021. We tracked an advanced campaign in 2022 that targeted the energy sector with the majority of its emails. The threat actors used chemical supply companies as themes or spoofed senders. We reported that 100% of the observed emails spoofing or themed around chemical supply targeted the energy sector.

Malicious HTML Attachments

From 2021 to 2022 we observed an increase of over 300% in HTML files delivering malware. This was particularly driven by QakBot, which used HTML files that were either attached or downloaded via links embedded in the email in many of its campaigns. QakBot's last campaign using Office macros was mid 2022, but QakBot threat actors began experimenting before that point with other delivery mechanisms, particularly HTML files, in early Q2 of 2022. Overall usage of HTML files as a delivery mechanism started to ramp up in early March, which coincided with Microsoft's announcement that macros would be disabled in its Office products. In addition to their increasing use in malware delivery, HTML files also continued to be used to deliver credential phishing throughout the year. In total, we observed a 295% increase in the use of malicious HTML files across both malware delivery and credential phishing throughout the year.

FIGURE 9: USE OF HTML ATTACHMENTS IN MALICIOUS EMAIL CAMPAIGNS



Adobe is the Top Domain Abused to Deliver Phishing Emails

In 2022, Cofense Intelligence reported that the abuse of hosting providers to deliver malicious files has become a popular method for threat actors to bypass security and deliver malware in credential phishing attacks as seen in Figure 10. It is common to see trusted cloud providers like Amazon AWS, Google, SharePoint, and other well-known organizations such as Adobe abused by threat actors. Lately, a wider variety of less-common hosting providers have been seen. In some cases, fake providers have been created by threat actors such as Clickfunnels.com domains. Threat actors abuse legitimate services such as Dropbox, DocuSign, and other legitimate and trusted domain names in order to ensure malicious emails reach inboxes.

FIGURE 10: TOP DOMAINS ABUSED IN PHISHING EMAILS REACHING INBOXES

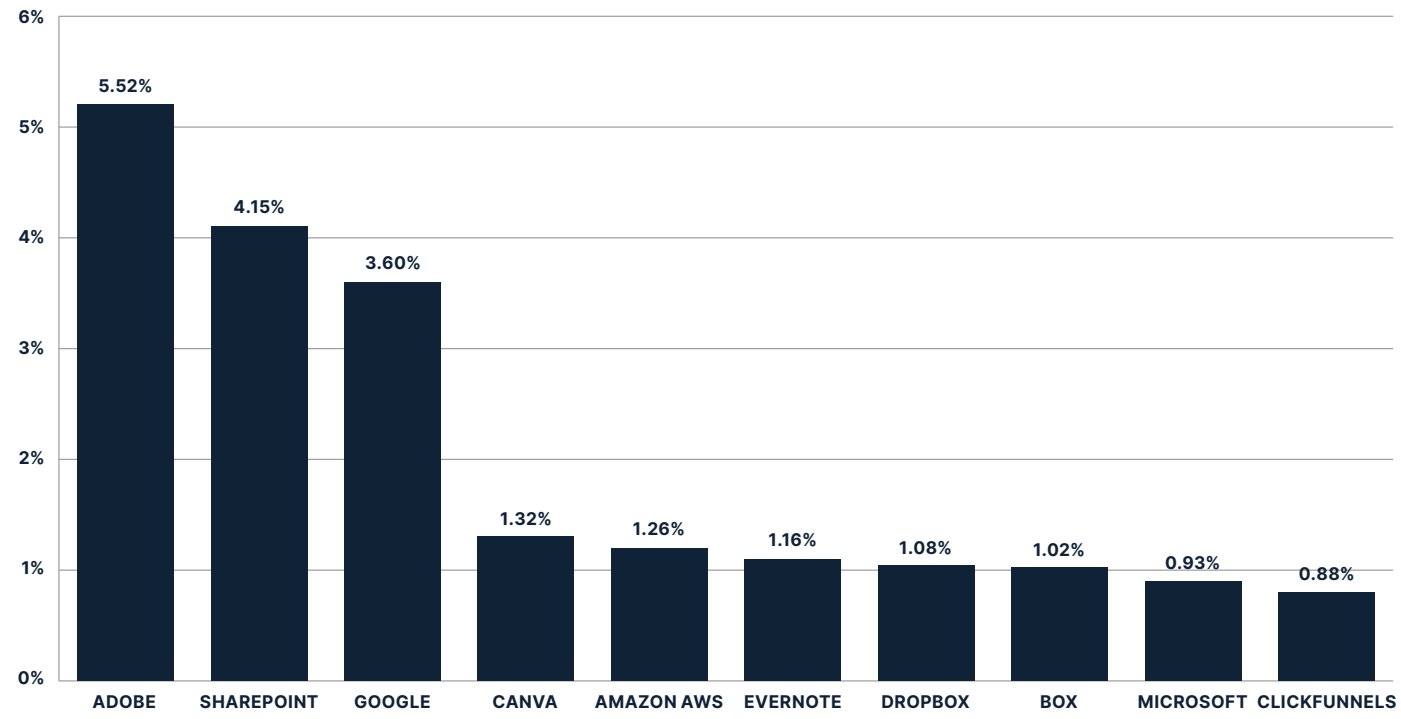
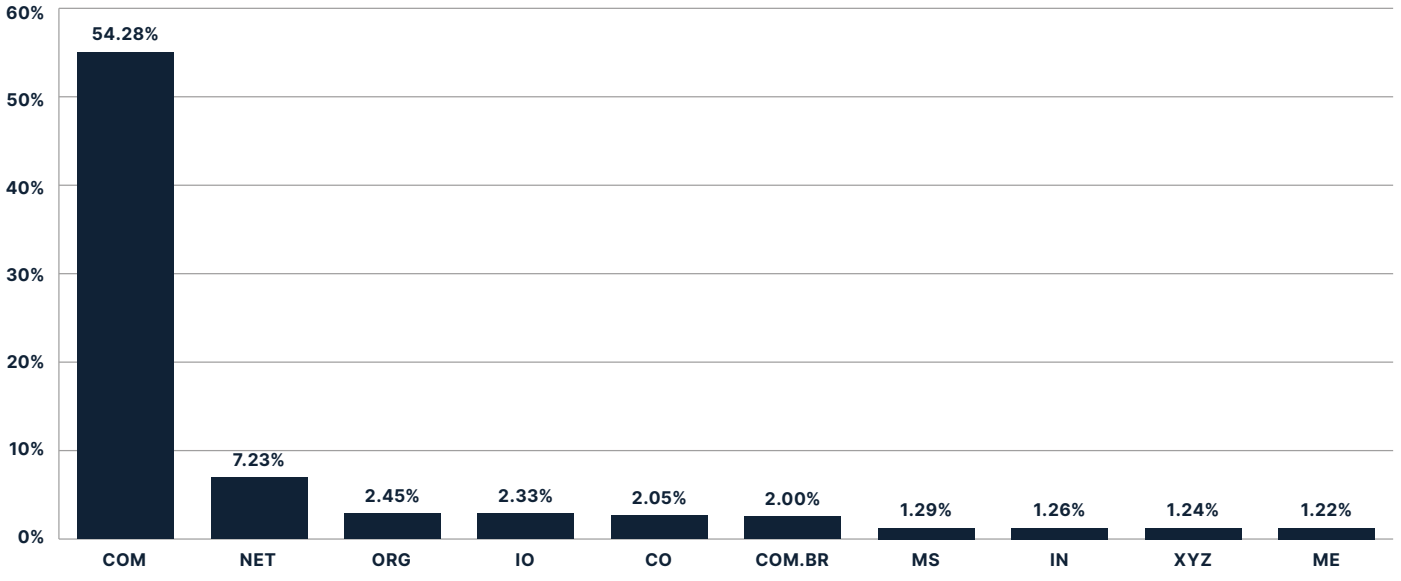


FIGURE 11: TOP LEVEL DOMAINS (TLDS) USED IN CREDENTIAL PHISHING IN 2022



Top Malicious Attachment Types Reaching Inboxes

Cofense Intelligence identified file attachments such as .pdf, .html, and .htm, as the top 3 file extensions on email attachments that reached users in SEG-protected environments as seen in Figure 12. In Q4, for the first time in quite a while, .pdf no longer made up more than .htm and .html files combined, as overall HTML attachment usage rose to 44.97% of the total. The file extensions of .pdf, .html, .htm, .shtml, and increasingly .xlsx are typically used for credential phishing. It is important to note that .pdf and .xlsx files will contain links to credential phishing pages, while .html, .htm, and .shtml will either present a credential phishing page when opened or automatically redirect to one. Next, the file extensions in the top 10 (.docx and .xlsx) were most often used to deliver malware via a known vulnerability and bug called Microsoft Office Memory Corruption Vulnerability (CVE-2017-11882) that allows the attacker to perform arbitrary code-execution. Also, .docx and .xlsx have been seen in malicious Office macros as this approach is easy to execute and has extremely low barriers to entry which remains a method to watch in 2023. We have identified that .docx and .xlsx have been seen delivering small volumes of credential phishing via embedded URLs. The archive compressed file name in the top 10 (.zip) was used to deliver such a wide variety of malware and phishing that it is impossible to narrow it down to a single most commonly delivered threat.

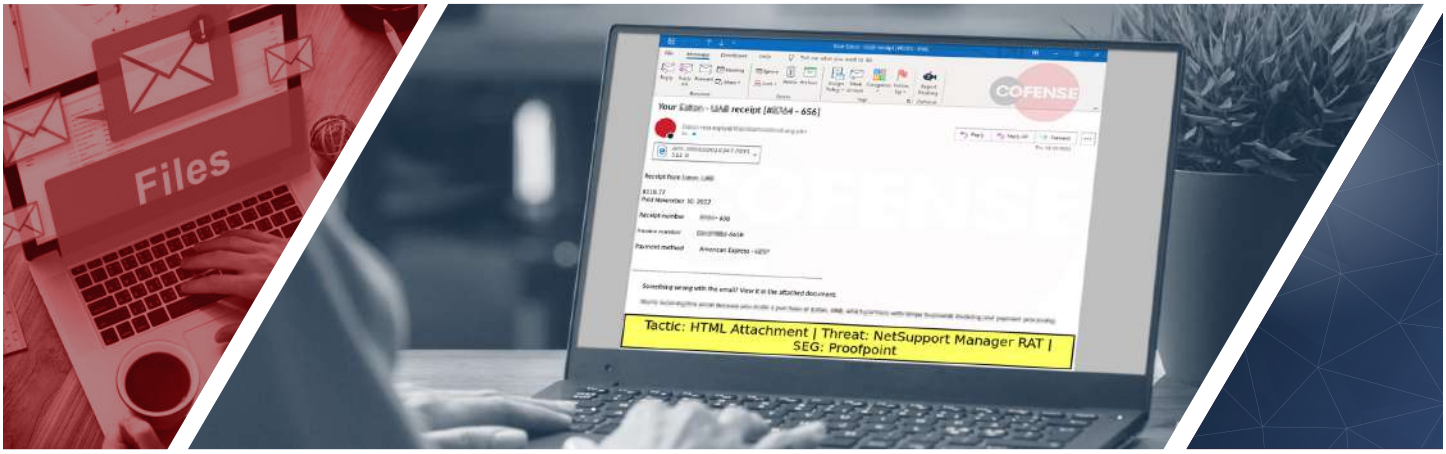
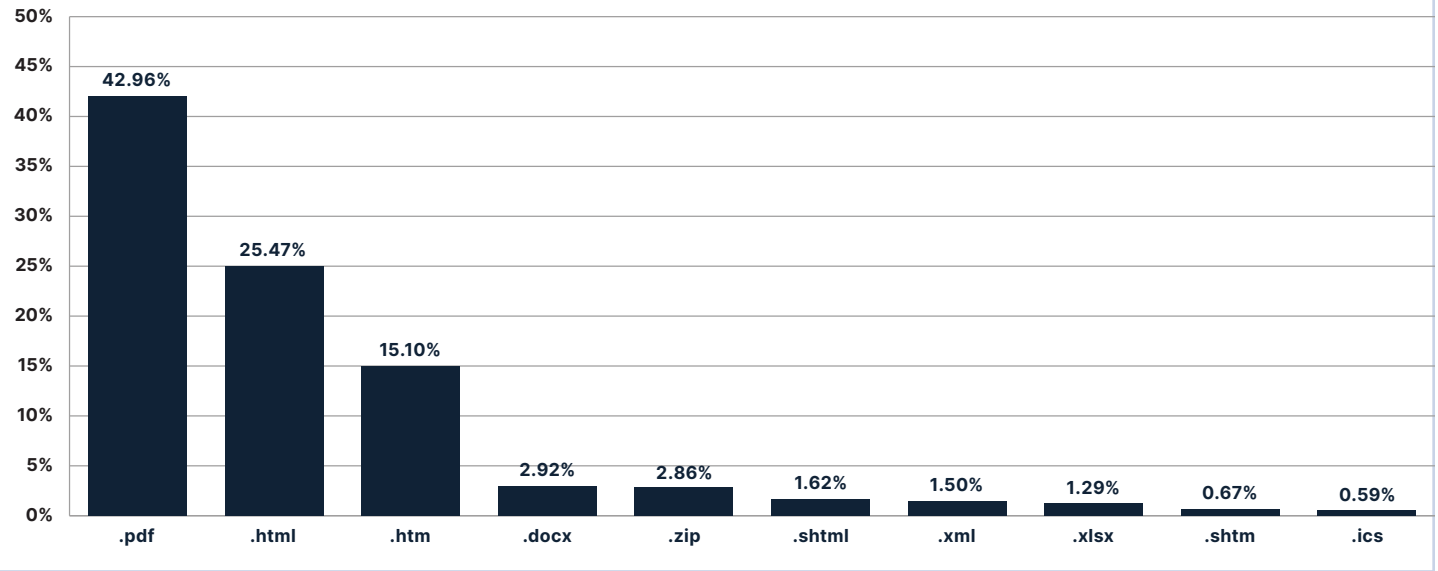


FIGURE 12: TOP ATTACHMENT TYPES USED IN PHISHING EMAILS REACHING INBOXES



Emotet Phishing Emails Exploit 2022 Tax Season, Spoofing IRS

During the 2022 tax season, Emotet consistently employed financial themes in its phishing campaigns and has exploited the arrival of the United States tax season to construct emails targeting end users who need to file tax returns. In March 2022, Cofense Intelligence observed phishing emails using W-9 tax form lures to deliver Emotet payloads. In past years, we reported on Emotet taking advantage of tax season to deliver W-9 themed malicious documents; in 2022, the tactic was further improved. Emotet operators started to include the United States IRS logo, a specific mention of the organization employing individual recipients, and a password to access the attached password-protected archives. When the Office macro-laden spreadsheets enclosed in the password-protected archives were opened, a request to enable macros is presented to the user, and if they accept/allow macros to be enabled, Emotet .dll files are delivered to the victim's computer.

Return of Emotet Phishing Emails

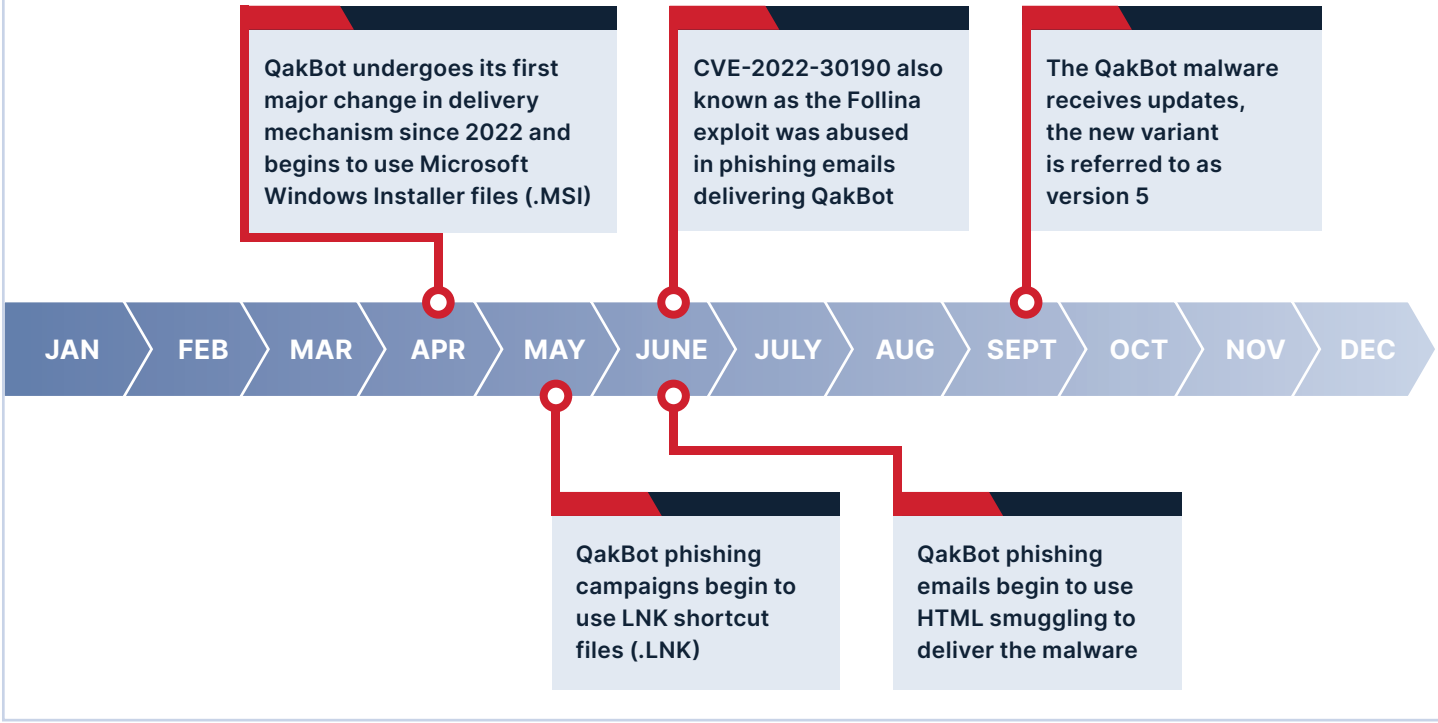
In the beginning of Q3, we saw large volumes of Emotet emails, until around mid-July when the campaign activity ceased. Later in October and November, we saw a sudden increase in Emotet C2 traffic. Emotet began sending malicious emails after three months of relative inactivity. It is suspected that Emotet authors were using their downtime to make significant changes intended to improve the effectiveness of their malware delivery campaigns. In the past, Emotet authors have been known to make significant changes to the malware's delivery methods before coming back from extended hiatus.

Malware Foothold: QakBot

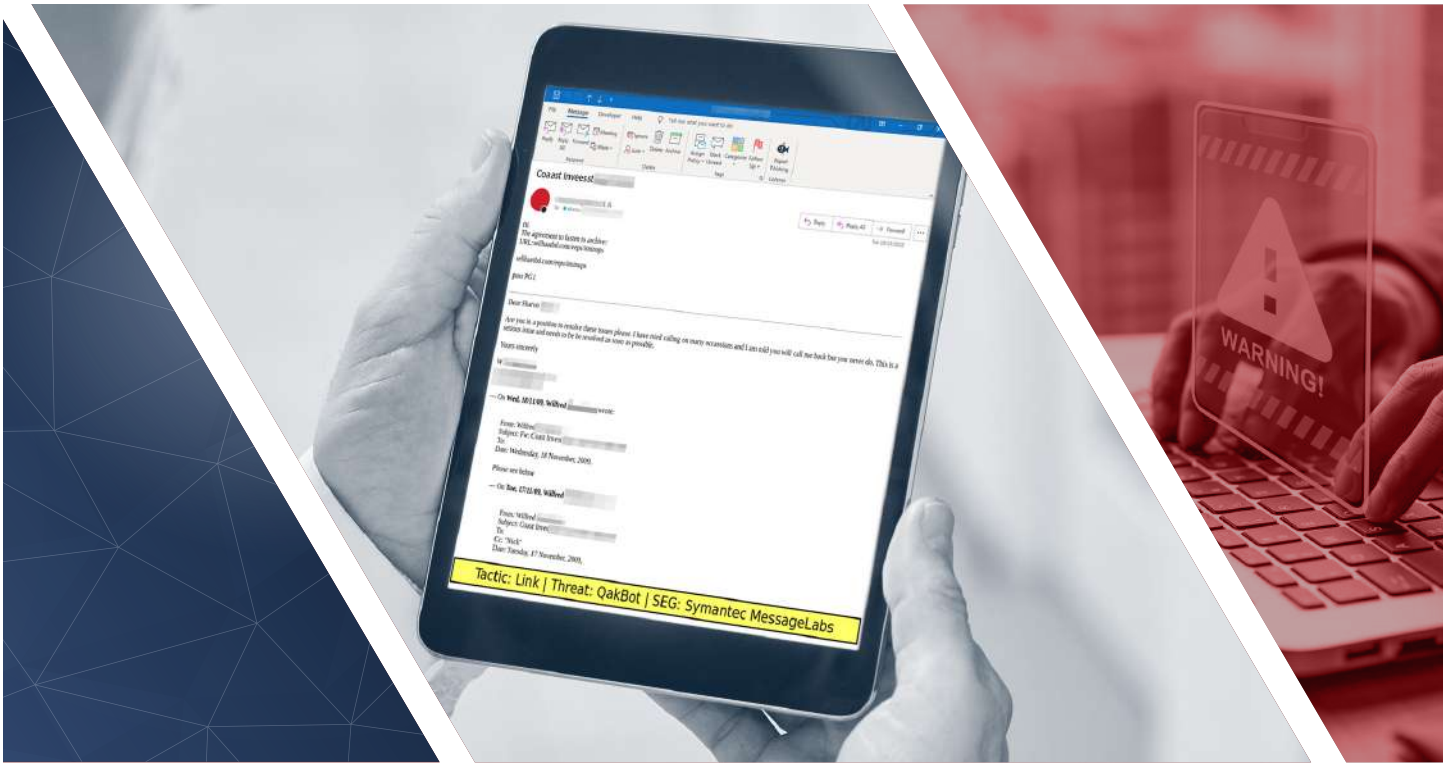
Cofense Intelligence identified QakBot as one of the malware families to watch in 2022. Throughout the year, it was the top malware family seen in phishing emails reported to the Cofense Phishing Defense Center (PDC) from inboxes. The success rate of the phishing emails reaching enterprise inboxes can be attributed to the use of hijacked email threads and embedded URLs, among other tactics, techniques, and procedures that are known to aid in bypassing security. In Q3 of 2022, threat actors using the new version 5 of QakBot made several changes to their phishing tactics. The most notable new tactic employs attaching malicious HTML files to deliver the payload. This new tactic does not utilize an embedded payload or redirect URL, as typical of most malicious emails delivering via HTML file attachments. Instead, the malicious payload is hardcoded into the HTML file, dropping when the HTML is executed inside the browser. This makes the delivery mechanism versatile and stealthy. The HTML file drops the payload locally without having to reach out to an external resource. QakBot continues to evolve defensive mechanisms against malware analysis, and phishing emails delivering QakBot continue to successfully reach inboxes. This makes QakBot the malware family to continue to watch, especially since a successful QakBot infection can lead to more costly threats like ransomware.

The QakBot banking trojan, also known as QBot or Pinkslipbot, was first released in 2007 and has become a prominent threat that is effective at reaching users' inboxes. Throughout 2022, we saw QakBot campaigns go to extensive lengths to bypass security measures, avoid detection, and obstruct analysis tactics. The most notable changes were to the delivery of the malware, but we also saw the malware itself receive updates particularly to the command-and-control servers when QakBot updated to version 5 in September.

FIGURE 13: QAKBOT MALWARE FAMILY TIMELINE



Near the beginning of 2022, Microsoft announced they will be changing the default Office settings to block Visual Basic for Applications (VBA) macros from files downloaded from the internet which was expected to disrupt malicious use of the macros. As such, we saw major malware families such as QakBot seek new delivery mechanisms. More particularly, QakBot's delivery methods changed drastically for the first time since June 2020. QakBot operators tried several new delivery mechanisms to deliver and install their malware; Microsoft Windows Installer (MSI files), LNK shortcut files, the Follina exploit (CVE-2022-30190) and HTML smuggling.



Noteworthy Mentions

Phishing Attacks Supported by Illicit Marketplaces – "Phishing as a Service (PaaS)"

For years, illicit online marketplaces have been a critical part of the phishing threat landscape, allowing threat actors to buy and sell access to compromised accounts and servers to phishing activity. This reality continued throughout 2022, as phishing threat actors presented a consistent demand for compromised email accounts and websites. As an illustration, we conducted a focused study of several publicly available online shops running a platform named Ofux, which offers everything a phishing threat actor might need: email sending capability, access to websites for hosting malicious content, and access to hacked individual email accounts. Threat actors who compromise accounts and websites may choose not to expand their efforts into phishing or spam operations, but these marketplaces still give them a chance to monetize their work. Meanwhile, buyers can take advantage of access to reputable assets at low prices. Further, the "Phishing as a Service" business model provides phishing kits and cybercriminals as a managed service for threats in today's marketplace. Phishing campaigns that use such legitimate but compromised assets are more likely to reach targeted users, highlighting the need for robust email defenses, and even stronger employee/user education.

Conti Leaks Demonstrated Importance of Phishing in Ransomware Operations

Cofense Intelligence provided analysis on the Conti Ransomware Gang Leaks in 2022, which became a valuable resource for security researchers. The leaks could also be used by threat actors with a desire to emulate Conti activity. Seeing the strategies, tactics, resources, profits, and daily discussions of a premier ransomware group could demystify their activities and convince others that a similar operation is feasible.

The Conti leaks bore several important lessons for those defending against both ransomware and phishing. For us, the combined takeaway of these lessons is that phishing was central to Conti's success. At the time of the leaks, they were continuing to invest massive resources into it as a pillar of their lucrative ransomware operation.

- Conti paid operators of malware such as Emotet and Trickbot to conduct phishing campaigns and establish footholds in target organizations before distributing those footholds to a team of hackers who specialize in expanding access.
- Some of Conti's specialists were involved in crafting semi-random phishing templates to increase victim click rates.
- Conti members and affiliates were thoroughly attentive to email security measures and tested to make sure their emails reach inboxes on popular platforms.
- Conti's phishing and intrusion operators are taught to pay attention to cybersecurity research on their own activity.

This could potentially motivate new ransomware operators to enter the landscape, improve the operations of existing low-level ransomware operators, and/or entice recruits to join phishing operations that support ransomware. The leaks may also cause existing threat actors to become more concerned with the security of their operations.

FIGURE 14: OPERATE AS BUSINESS – TOP TO BOTTOM MODEL	
DEPARTMENT	**DESCRIPTION**
C-SUITE	**Sets design and targets businesses – EASTERN EUROPE, WEST AFRICA**
IT WING	**Carries out hacking, malware, email monitoring – GLOBAL**
HR/RECRUITMENT	**Recruits IT wing, financial actors – EASTERN EUROPE, WEST AFRICA**
FINANCE/BANKING	**Sets process for wire transfers and money laundering – GLOBAL, LOCAL**
ENFORCERS	**Ensures financial cooperation and following of orders – GLOBAL**
ADMINS	**Maintain shell companies and legitimate business liaisons – LOCAL**
BURN PARTY	**After successful schemes, enterprise burns all materials – GLOBAL**

Source: US Secret Service

Whaling in Bulk

Targeted phishing efforts against executives and other high-profile individuals are often referred to as "whaling" within the security industry. While "whaling" emails can be extremely customized for a single individual, they can also be conducted in bulk with a considerable failure rate, but with minimal effort in hopes that one email will be successful.

As a prime example, we reported on a credential phishing campaign that spoofed DocuSign and bypassed SEGs in 2022. Through initial collaboration with Cofense Intelligence customers and subsequently with the Cofense Phishing Defense Center (PDC), we determined that it was a whaling campaign to exclusively target executive-level employees, primarily CFOs. Emails from the campaign were sent to executives with the CFO title, but were also seen targeting CEOs, directors, and board members. The campaign targeted individuals in the insurance, real estate, manufacturing, professional services, and mining sectors. The emails spoofed DocuSign and claimed to deliver documents related to settlement agreements and other financial documents.

Industry Overview

HEALTHCARE	• Hit hard with BEC • Resilience is a bit lower than the overall average. This workforce tends to be more likely to access email via mobile devices, with a lag in reporting time.
FINANCIAL SERVICES	• Greatest visibility across simulation and threats seen by PDC • Highest resiliency rate for simulations, driven by a mature reporting culture • Highly regulated, driving scenario frequency
UTILITIES	• The second highest that observed 'threat unavailable,' which aligns with the geofencing or restricted user agents as this industry saw increased threats related to political tensions.
PROFESSIONAL	• Highest BEC – 3x the overall average • Significant increase in BEC threats over previous year • Resiliency rate is almost a point lower than the overall rate
REAL ESTATE	• Hit hard with credential phish – 6 percentage points above the overall average • One of the lowest groups experiencing BEC, but with the nature of their business model, more likely seeing more via SMS requests
GOVERNMENT	• Credential phish and BEC top the category most seen by this industry

FIGURE 15: COFENSE PHISHING DEFENSE CENTER INDUSTRY TRENDS

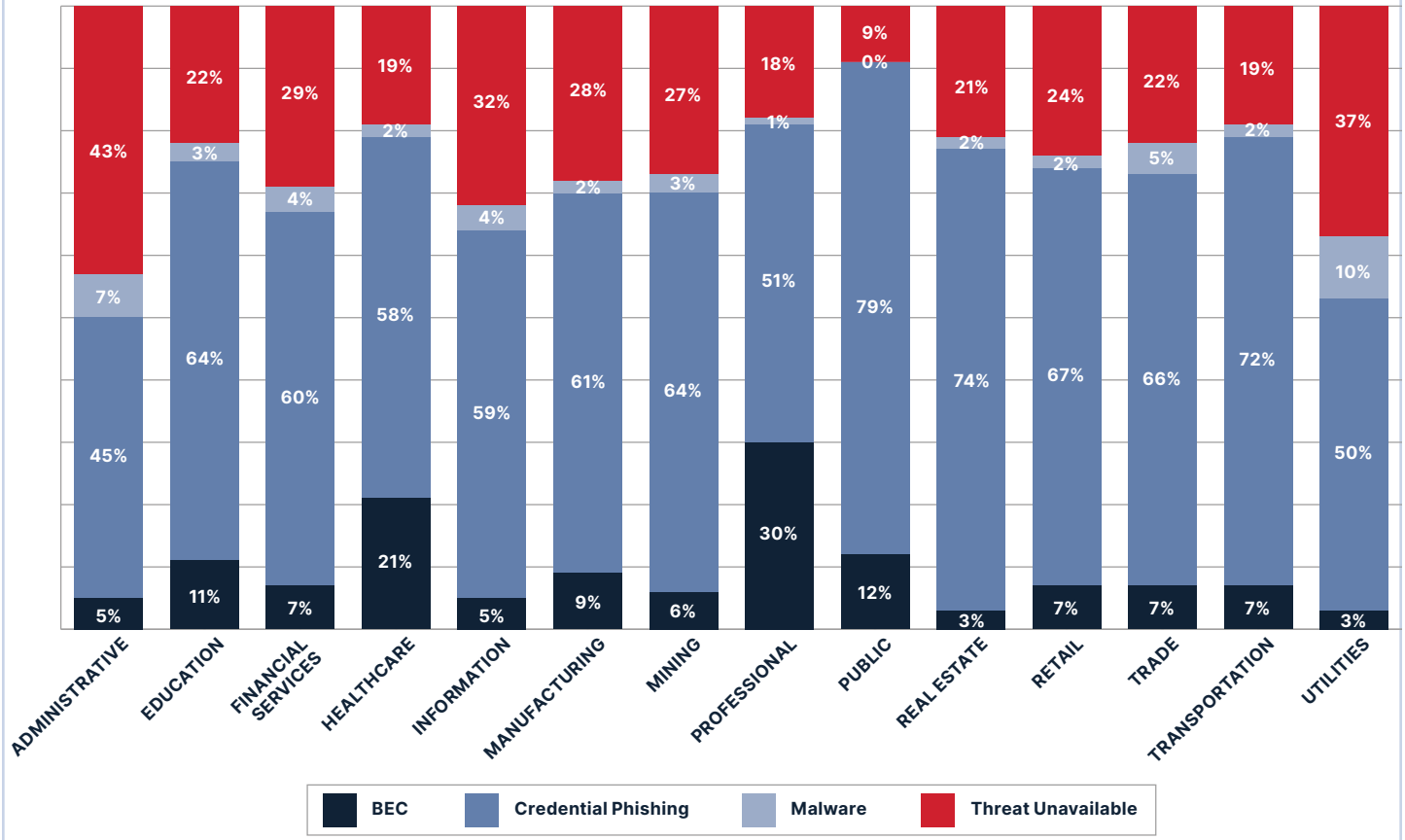
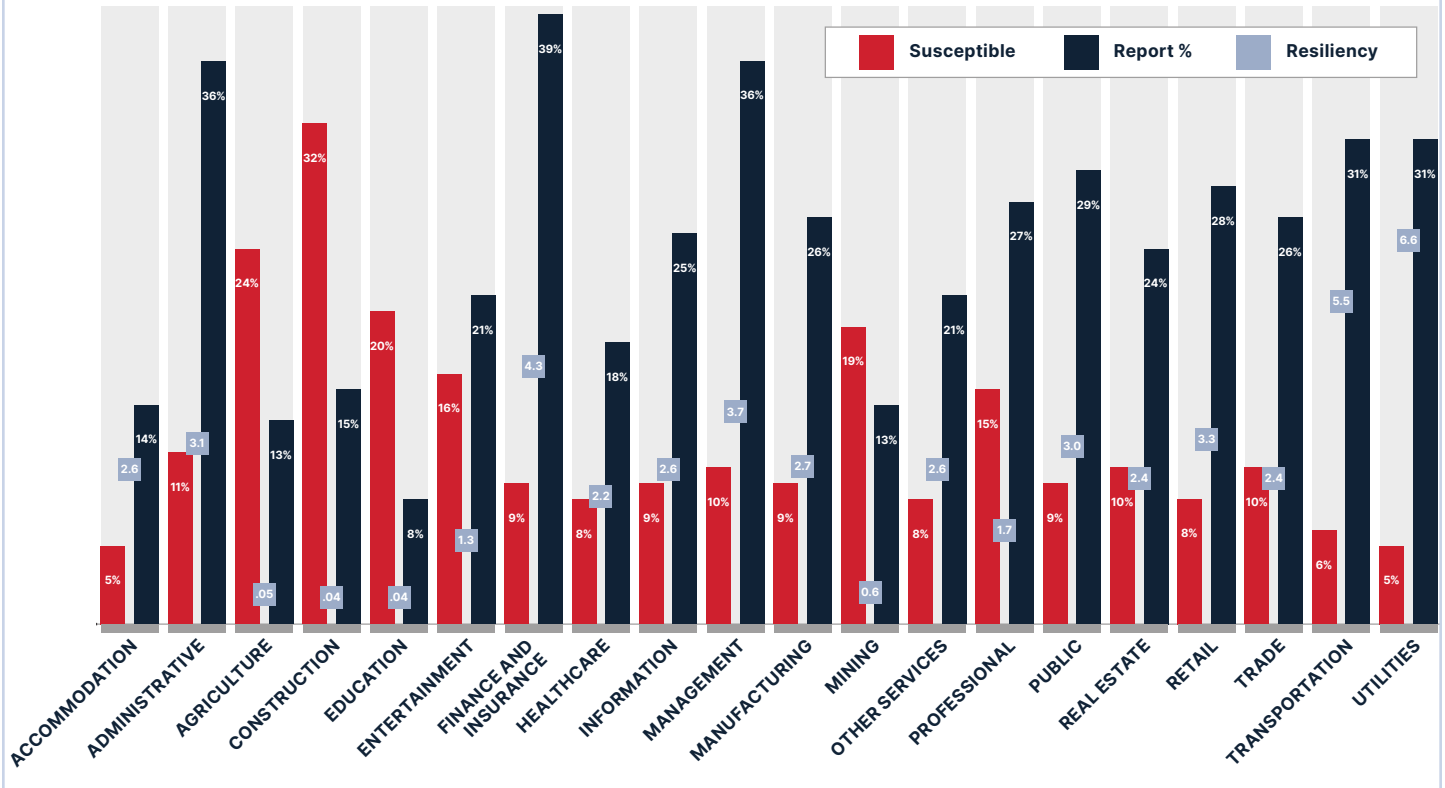


FIGURE 16: SIMULATION INDUSTRY TRENDS



SO NOW WHAT?

How to Enhance your Email Security

With the increase in ransomware, nation state attacks, and major incidents in general, pressure continues to drive visibility of an organization's Information Security program by boards, corporate executives, and cyber insurers. With this pressure, organizations continue to evaluate ways to mitigate risk and assess what controls need to be added or enhanced. By adding controls to their email security program, organizations can raise their overall security posture.

We observed that customers with a full End-to-End Email Security solution, as seen in Figure 17, have a resilience rate double that of customers with simulation-only programs. We continue to encourage organizations to align their simulation program to threats making it past their SEG and landing in inboxes. With credential phish continuing to lead the way for real phishing threats, organizations continue to experience an increased appetite for use of real-life simulations. Last year, we reported only 29% of scenarios used a credential threat, while this year this category increased to 34% of scenarios. We also observed a slight increase in attachment scenarios. This too aligns with the threats we observed as threat actors continue to leverage .html/.htm files that are difficult to block.

FIGURE 17: END-TO-END EMAIL SECURITY VS SIMULATION ONLY

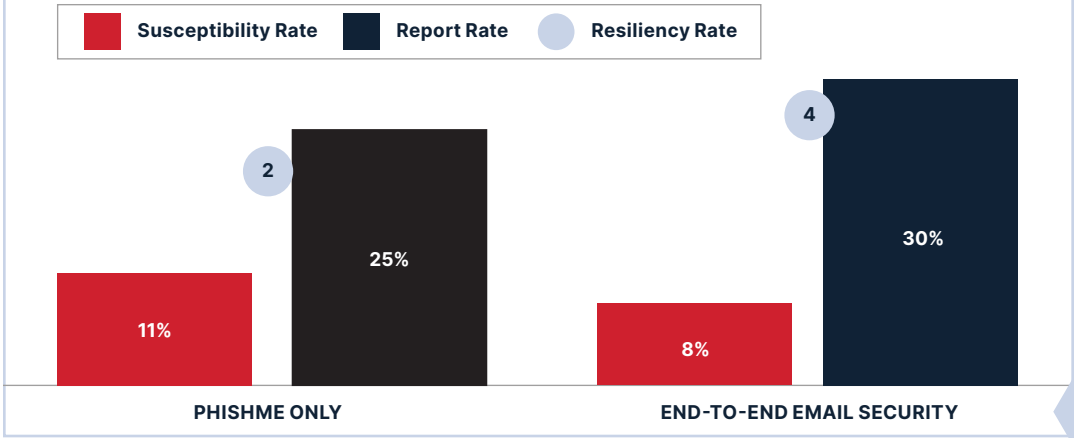
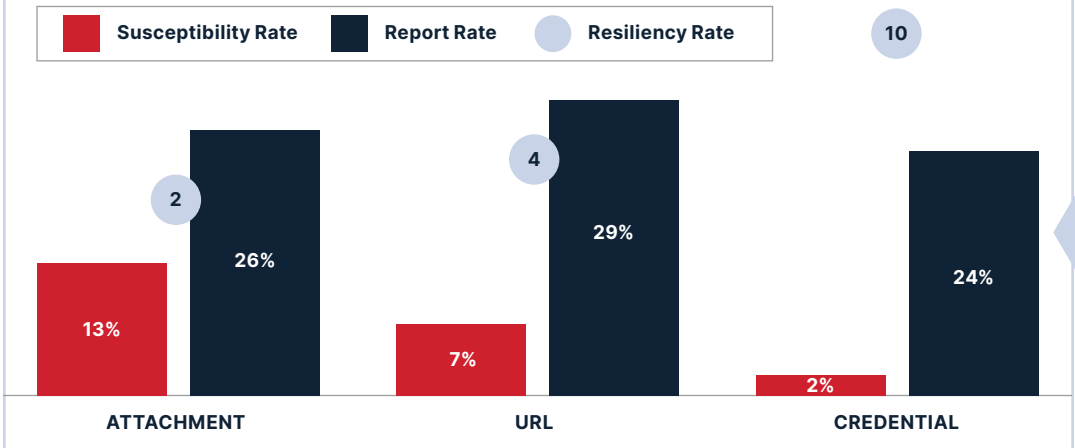


FIGURE 18: RESILIENCY BY THREAT TYPE



With credential phish continuing to lead the way for real phishing threats, organizations continue to experience an increased appetite for use of real-life simulations. Last year, we reported only

29%

of scenarios used a credential threat, while this year this category increased to

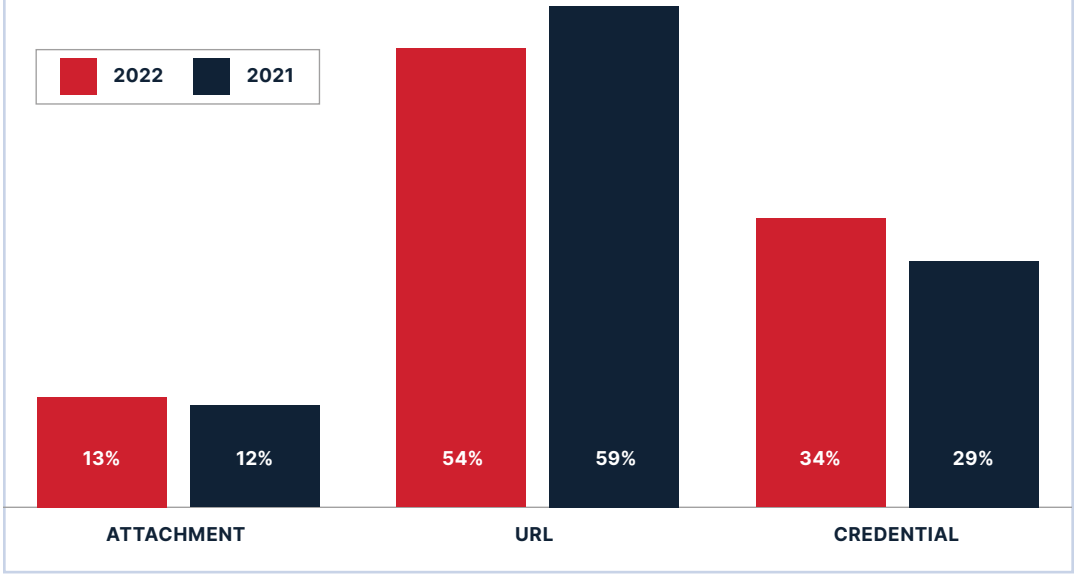
34%

of scenarios.

PDC customers are 2x as resilient as customers who use PhishMe

With credential phish as the top threat, according to our simulations, you're more resilient to this threat type.

FIGURE 19: SCENARIO TYPE USAGE BY YEAR



Still need more recommendations to enhance your program and strengthen your reporting culture? Let's review the use case detailed in Figure 20 below. This organization in Figure 20 started running its simulation program in 2019 but wanted step up the reporting culture. The program operator engaged our Professional Services team to identify real phish that were already being reported by users to use for their simulation campaigns. The team launched a 5-day phishing simulation bootcamp to bolster reporting among users that were not actively using the Reporter button. Over the year, the team also adopted a new hire simulation program and addressed repeat clickers. As you can see from the results in Figure 20, not only did they reduce their susceptibility rate, but their reporting rate had a double-digit increase. What you can't see from these numbers is the effect this had on reducing the amount of non-malicious emails being reported, such as spam and business communications. Why is this a big deal? Ask your SOC!

FIGURE 20: YEAR-OVER-YEAR RESILIENCY IMPROVEMENT

METRICS	2022	2021
RESILIENCY	5.13	3.59
SUSCEPTIBILITY	8%	10%
REPORTING	42%	29%

What you can't see from these numbers is the effect this had on reducing the amount of non-malicious emails being reported, such as spam and business communications. Why is this a big deal? Ask your SOC!

Checklist: Protect Your Organization from Top Threats

BEC/Vendor Email Compromise

This threat type is very difficult to simulate. Even when you make efforts to simulate something similar to what your organization might experience, you run the risk of overburdening your executive team that may need to respond to users trying to verify if they sent the email.

- ✔ Ask your CEO and other senior executives to talk about this threat in company all-hands meetings and inform the company they will never ask for "special favors" or gift card purchases.
- ✔ Send newsletters with real examples of phishing messages reported by users. Peer recognition can go a long way!
- ✔ Collaborate with your finance team to review and update processes related to vendor master changes related to the banking information.
- ✔ Many SEGs allow configuration settings that will allow increased protections by blocking executive spoofing or allowing free email account domains. Do you need to allow @gmail.com accounts to send external email?
- ✔ REPORT! Report any losses to law enforcement. No matter the size of the loss, it's critical to report these incidents. The US Secret Service established a Global Incident Operations Center (GIOC), specific to BEC, to bring charges against these threat groups. It's been reported that a small $4,000 loss was able to be matched against a larger crime. Time is of the essence. If the loss is reported within 24 hours, the likelihood of reclaiming even a portion of the loss increases.

Credential Phishing

- ✔ Disable auto-forwarding rules across the organization. Unable to fully block? Review rules to work with the business to allow exceptions for legitimate business needs. Resetting a users' credentials due to a recent campaign? Check the auto-forward rules and remove rogue rules potentially set up by threat actor.
- ✔ Continue to increase the cadence of simulation scenarios using this threat type. It's not always easy to coordinate these campaigns but think of it as a tabletop exercise!
- ✔ Customize your Microsoft landing page with your company logo. Communicate to the organization to report any landing pages that don't fit the corporate branding standards.
- ✔ Enable MFA. Enhance the authentication experience to help users avoid MFA exhaustion. Microsoft recently provided additional enhancements for this very reason – number matching and location of request.

Attachments

- ✔ Threat actors continuously tune their tactics to land in the inbox and the same holds true with file attachments. As technology controls implement new configurations to block file types used by threat actors, they pivot to something new.
- ✔ Block malicious file types. This list continues to expand as threat actors leverage new file types to land in the inbox. Does your organization need to accept .html /.htm files externally? Who sends OneNote files externally?
- ✔ PDFs. This used to be the "safe" file type. No longer. Not only do threat actors embed links to login pages to steal credentials, we now observe PDFs delivering malware via a chain of links embedded within the PDF document.

Malware

- ✔ Remove local admin rights. Without the ability to run code locally, this will reduce the risk of malware executing if the user interacts with a malicious file or website.

CONCLUSION

As the threat landscape continues to evolve and threat actors continue to find more sophisticated ways to bypass standard email security solutions, your organization needs the resources that can enable them to identify, protect, detect and respond to all email security threats. And that's exactly our mission.

Cofense was built on the foundation that humans are critically important to your security program. Threat actors are constantly targeting people's hopes, fears, emotions, struggles and sympathies, to trick them into divulging their credentials. If your employees aren't trained properly, divulging these credentials opens your company to ransomware, malware and many other potential threats.

That's why it all starts with providing them with REAL simulations that replicate the REAL threats hitting their inboxes and putting tools in their fingertips to report those quickly and easily.

Once these malicious or suspicious emails are reported, we analyze these threats at great length and provide intelligent, human-vetted expertise and analysis with actionable insights. We treat each malware infection as a potential vector for future ransomware attacks, reverse engineer the payloads and trace the steps that led to the infection to enable our customers to determine the flaws in their defenses and prevent phishing attacks.

That intelligence, combined with our global network of more than 35+ million human reporters, enables us to have unique insights into email threats targeting your organization. Sometimes even detecting and removing advanced attacks BEFORE they reach your inbox.

How, you ask?

With our real-time, crowdsourced intelligence. If a malicious email is reported by a user in our global network, it can then be automatically quarantined from other inboxes, highlighting the power of the network effect.

Cofense email security expertise is built on human experience with millions of suspicious and malicious emails. These emails are crowdsourced from professionals all around the world, processed, enriched, and analyzed to provide a unique view of what the phishing landscape looks like as we move forward into 2023. This crowdsourced methodology provides Cofense an unparalleled aperture into the malicious emails reaching enterprise inboxes, providing customers the opportunity to react.

Cofense email security expertise is built on human experience with millions of suspicious and malicious emails. These emails are crowdsourced from professionals all around the world, processed, enriched, and analyzed to provide a unique view of what the phishing landscape looks like as we move forward into 2023. This crowdsourced methodology provides Cofense an unparalleled aperture into the malicious emails reaching enterprise inboxes, providing customers the opportunity to react.

We know that phishing tactics are always evolving and becoming more complex. So, our Cofense Intelligence provides a human-vetted layer to pinpoint the actual phishing emails out of the noise of suspicious-looking spam, rank those threats, and provide the automation to remove those phishing emails within seconds or minutes of reaching the inbox.

Looking at 2023 and beyond, we know email will continue to be one of the top attack vectors for cyber threats, and we are committed to providing best-in-class email security to keep our customers secure. With the only end-to-end email security solution powered by global intelligence from 35+ million human reporters, AI and machine learning, our solutions are made to evolve with the ever-changing landscape. To meet those demands, we continue to enhance our APIs, while also expanding our integration partnerships, allowing you to quickly identify threats hitting the inbox and moving those IOCs to your other controls to defend against the adversary quickly. As we continue to integrate with world-class partners around the globe, we couldn't be more excited to build on our 2022 momentum as we continue to strengthen our portfolio of email security solutions.

APPENDIX

List of Figures

COFENSE.COM