Annual State of Phishing Report

2021

COFENSE

Table of Contents

SECTION 1:

Executive Summary

If you think Cofense is a company that promotes phishing simulations to build naughty vs. nice lists to hand out pink slips for failing a "phish test," then I recommend abandoning this report now.

2020 year in review
In fact, in 2020 Cofense stood alone actively discouraging sending COVID-19 themed phishing simulations at the outbreak of the pandemic. The peanut gallery of information security experts grumbled on Twitter about the need for realism. While they were occupied retweeting, the Cofense customer community produced more REAL coronavirus/COVID-19 phishing email indicators than the entirety of the global cyber vendor landscape combined.*

Let that gel for a bit. The inventors of phishing simulations blocked COVID-19 themed PhishMe templates, yet our customers' employees reported more real COVID-19 phish than anyone else.

A Cofense theme for 2020 was shining a light on the phishing tactics that evade secure email gateway (SEG) detection. We published a stream of SEG bypass samples on our blog prompting many organizations to ask for help testing their email environments.

This report explains how Cofense is in a unique position to report on this. In fact, most of this report is focused on the REAL phish we see that bypassed multiple layers of automation, only to be smoked out by real humans who are backed by organizations that encourage reporting.

What went wrong in 2020
Over 1.5 million simulated phishing emails leave our PhishMe infrastructure every Monday. Unfortunately, some non-Cofense customers did not heed our cautionary tale of avoiding certain emotionally charged lures. 2020 claimed new CISO victims whose "awareness programs" publicly blew up on social media when the promise of a bonus in a phishing simulation to an organization cutting budget was not well received. 2020 pwned a security awareness vendor, too. While they were busy creating naughty employee lists for their Computer Based Training upsell, it was clear in their Incident Response webinar they didn't have a serious program in place to triage suspicious email reports.

Minimum effective dose
There is a problem in the awareness community that I'll write more about in the coming months. It boils down to this: Your organization isn't unique, and your security awareness program isn't special. You need just enough phishing simulations to produce enough employee reports to enable your operations team to stop a REAL phishing campaign. We have published data on how to achieve this in previous years that continues to be overlooked and replaced with elaborate wastes of time.

Unfortunately, when it comes to phishing detection and response, I'm seeing partial information being

*as measured by the COVID-19 Cyber Threat Coalition.

reported to boards that emphasizes the wrong data. If you are producing reports void of employee reporting metrics, you are doing it wrong. I'm still seeing awareness professionals playing gotcha games with individual business units, completely detached from how real phishing actually works. Let's not forget that organizations are taking these measures based on TRAINING data. What other training program exists where someone can lose their job for failing? All is not well in Security Operations Centers either. Everyone wants automation to do their job so they can be a threat hunter. Much like Homer Simpson's self-driving semi. The good news is, if you stop more phishing campaigns in progress, you have fewer alerts. This means, you get more time to work on bug bounties on the company dime...ehh...I mean be a "threat hunter." The fallacy is, if automation worked all the time, you wouldn't have an alert queue.

Malware is dead. Long live phishing.
We are no longer going to be producing a separate malware report like in years past. Instead, malware trends will be in this report. The vast majority of phishing campaigns are credential theft or conversational. While malicious attachments still play a role in phishing, the frequency of this has dramatically declined over the years. In fact, most phish attachments these days are not even malware, but instead, conduits to open a browser to further credential theft. While on the decline, we have our finger on the pulse of phishing related malware, and we will share that in this report.

Thank you for suffering through my ramblings. Our teams burned the midnight oil organizing this data and we appreciate your interest. We have been working on this phishing problem for years, and our insight is only made possible by servicing a growing global population of the largest organizations. This report wouldn't be possible without the data, and the data wouldn't exist without our amazing customers and their employees reporting phishing.

Aaron Higbee
Co-Founder & CTO

Setting the stage

While making the shift to a combined report, we also decided to take this opportunity to shift a few other notable mentions about the data. First, the time period covered in our research spans the calendar year. The next item relates to notifications to the user letting them know the security technology worked—"Invoice.docx was malicious and removed." While these alerts could appear suspicious to the end user, technically these messages are informational. Lastly, we adjusted how we make industry comparisons. Finally, throughout the report you'll find references to NAICS—North American Industry Classification Standard. We settled on this standard to align with other major research reports.

SECTION 2:

Let’s Get Started.

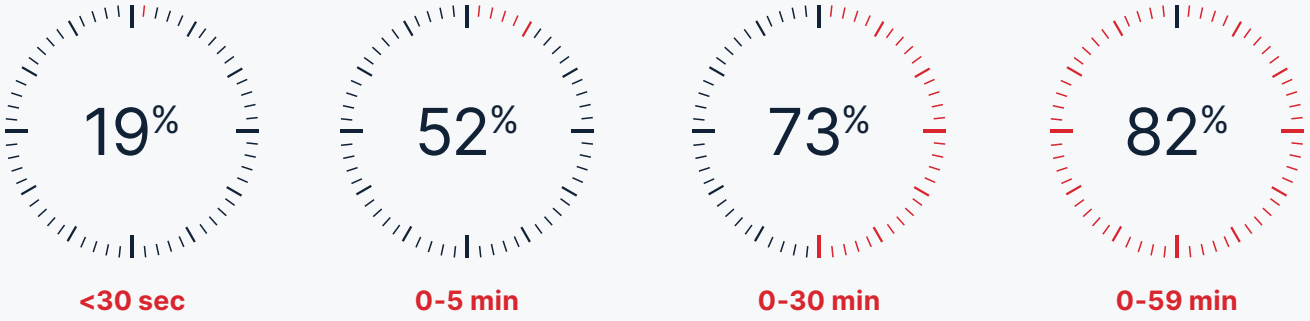
The Phishing Defense Center (PDC) Today

An enterprise customer asked us to manage their Cofense Triage application four years ago. This one-off project exploded into the Phishing Defense Center (PDC) staffed by a team of expert threat analysts, inside five locations across the globe, operating 24/7, processing millions of reported emails each year for large enterprises. What started out as a way of helping a customer shaped how we look at phishing detection and response today.

With Managed Phishing Detection and Response (Managed PDR) delivered through the PDC, we've gained even greater insight into the phishing threat landscape. In fact, we have a larger pool of enterprise phishing threat intelligence data than anyone else in the world. What's even more remarkable is getting to see firsthand that well-conditioned users report real phish quickly and that reduces overall risk to an organization.

We'll say that again:

Well-conditioned users report real phish quickly!



Average time it takes a user to report a suspected phishing email

It Only Takes One — To Bring Down an Entire Organization

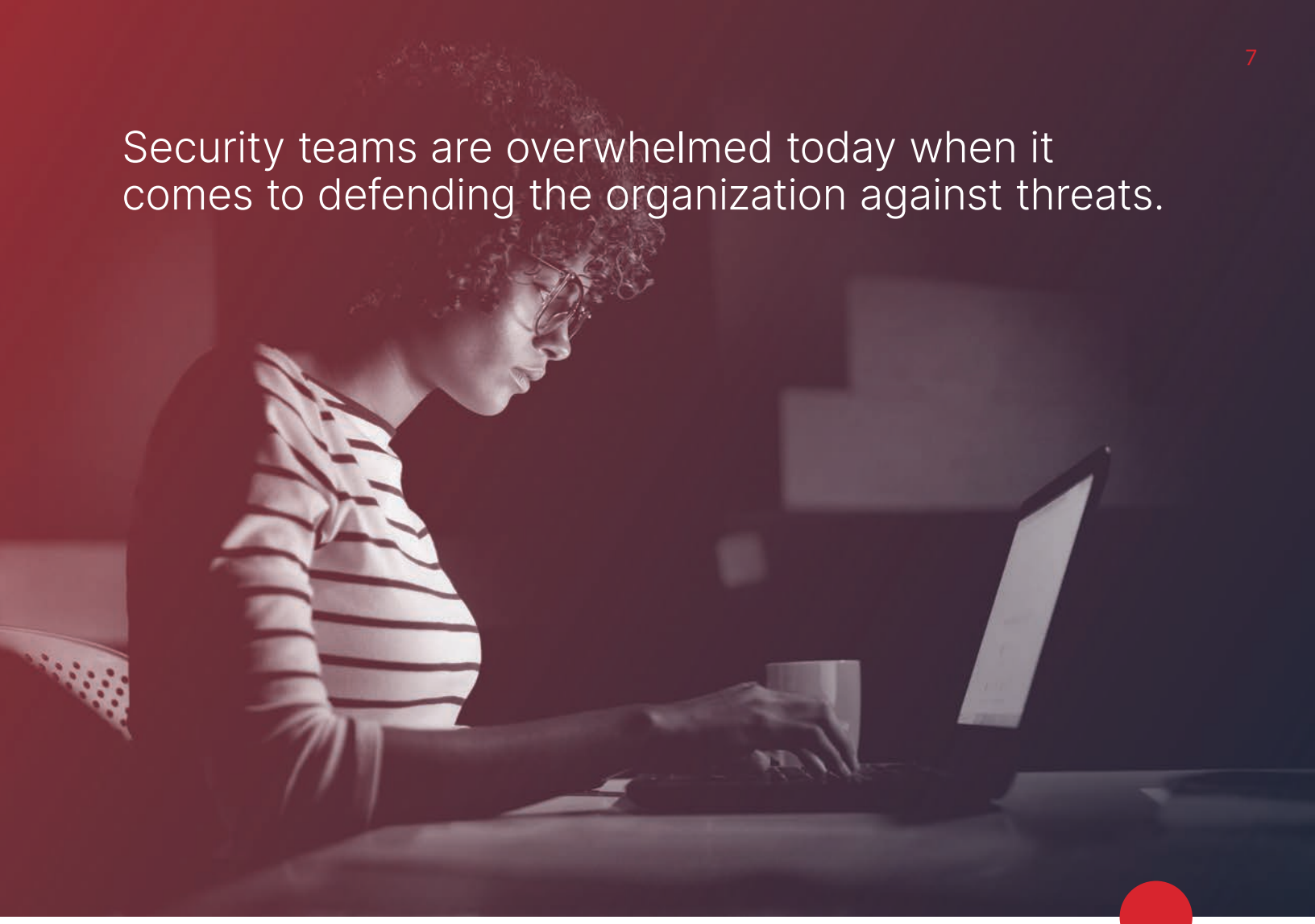
1 in 11 user-reported emails are malicious
As identified by Cofense in customer environments

We see more. We find more.

When we transitioned over to using the Cofense PDC services, we saw an increase in reporting of suspected phishing emails. The PDC team was able to determine much faster than we were what was and wasn't a phish.

Mining Customer

Security teams are overwhelmed today when it comes to defending the organization against threats.



Cofense PDC Phishing Facts

In the millions of emails the Cofense PDC analyzed, they determined:

- **57% were credential phish**
- **12% delivered malware**
- **6% were business email compromise or CEO fraud**
- **45% of the credential phish were Microsoft-themed**
- **17% were finance-themed**
- **9.3% of the reported messages were malicious:**
  - **38% had a URL only**
  - **36% had attachments**
- **Of the 255,000 malicious emails, we found nearly 100 unique malware families**

By enlisting the experts from the Cofense PDC, internal teams can get back to defending their perimeter and endpoints while the Cofense expertise focuses on the phishing threats. The PDC analyzes suspicious emails reported by customers' users and stops the phishing attack or notifies their security teams when they need to act.

Using the resources of the PDC, customers can rely on external expertise and access to a broad global network—25 million Cofense users who report suspected phishing emails—versus a limited internal-only view. With Managed PDR, security teams are able to focus their attention on incident response instead of the time-consuming process of analyzing reported emails.

Check yourself:

Cofense sees more phishing data than anyone else around the world across multiple industries.
How do you compare to your industry and other industries?

Percentage of Phishing Emails by Type and Industry

Industry	BEC (Business Email Compromise)	Malware	Credential
Administrative	6%	7%	58%
Construction	3%	31%	37%
Education	5%	2%	77%
Finance	6%	14%	57%
Healthcare	15%	5%	59%
Information	2%	4%	66%
Manufacturing	5%	10%	53%
Mining	4%	9%	59%
Professional	11%	12%	59%
Public	6%	8%	61%
Real Estate	3%	17%	58%
Retail	3%	2%	73%
Trade	9%	6%	71%
Transportation	9%	3%	67%
Utilities	3%	16%	48%

Fact: All Secure Email Gateways Leak

While your Secure Email Gateway (SEG) serves its purpose to remove many threats from your users' inbox, none are 100% secure.

Threat Actors Pivot Quickly—SEGs Can't Keep Up

Percentage of Phishing Emails by Type and SEG

SEG	BEC (Business Email Compromise)	Malware	Credential
Barracuda	4%	20%	67%
Cisco	11%	10%	55%
FortiNet	3%	4%	74%
Microsoft Defender for O365	4%	6%	62%
Microsoft EOP	2%	3%	67%
Mimecast	12%	9%	57%
Proofpoint	6%	19%	51%
Symantec	4%	19%	55%
TrendMicro	3%	18%	42%

The tactics, techniques, and procedures (TTPs) leveraged by phishing attackers range from tried-and-true to innovative. In 2020, Cofense Intelligence tracked several common delivery tactics used to defeat email gateways and other perimeter controls.

The threat actor has one goal—make it to the inbox. From there, the user does the rest.

Long-Standing TTPs Unfortunately Still Work

Credential-stealing campaigns account for over 50% of phish reported by end users to the PDC. These emails have been found in enterprise environments with diverse types of phishing defense, including SEGs and content filters.

Due to their nature, credential phishing campaigns are often more successful at evading defense technology. Credential phishing pages are inexpensive to host, with low upkeep cost, and attackers can easily change the infrastructure that supports them. Credential phish also leave few reliable and consistent indicators of compromise (IOCs), making it easier to stay ahead in the cat-and-mouse game of detection. The average lifespan of a phishing URL is less than 24 hours, making black lists irrelevant and human detection critical.

Remember, credentials are high value. They provide the keys to the castle for adversaries, sometimes allowing for long-term access to sensitive accounts and information. While threat actors constantly develop sophisticated techniques to evade SEGs and steal credentials, many still use tried-and-true methods with significant success. Data breaches and theft originating from stolen credentials are extremely common, giving threat actors access to sensitive data, web servers, end user accounts, and leave the organizational infrastructure vulnerable to other attack types.

Layering

The malicious pages threat actors stand up to capture credentials live for a very short time, putting Cofense in a unique position: we review reported messages within 60 minutes of human report. Globally. 24/7. These messages are quickly investigated and processed out to our global network so clients can automatically remove them from their mailboxes. One tactic we increasingly observed over the past year is the use of multi-stage websites for the user to navigate, also known as layering, that leveraged safe domains. As email security technology adds to and evolves their ability to detect malicious URLs within emails, threat actors are exploiting the use of popular services. These services are often deemed as safe or business critical and are not blocked or restricted.

Looking at the example below (Figure 1), we see the progression from the first page as a OneNote file hosting a link to the PDF document referenced in the email to the recipient or target. Once the recipient clicks the link to "View Document," they are presented with the login page with the option to select their email platform. Once they select "Sign in with Office365," they are prompted with the familiar Microsoft login page (of course this is not hosted by Microsoft) and once credentials are dropped they are handed the expected PDF document. However, the recipient is blind to the fact they just handed over their credentials to the threat actor.

There isn't anything malicious about this page, so any pre-processing of URL protections is not going to flag this as malicious.

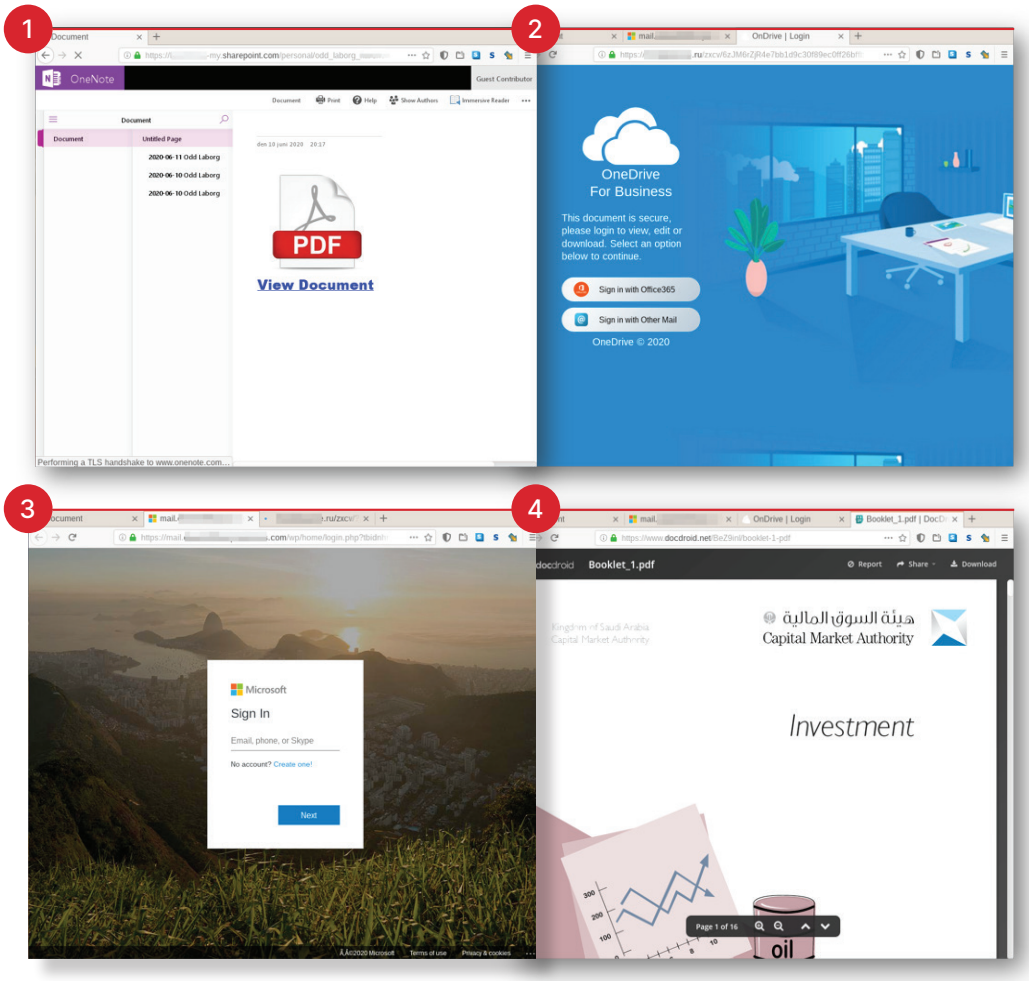


Figure 1 - Layering

Trusted platform abuse

Phishing threat actors are abusing trusted platforms with increasing frequency to deliver malware and credential harvesting pages (Figure 2). Credential phishing pages and malicious payloads are often hosted on legitimate web hosting or cloud services. This means that target recipients receive links that appear legitimate and point to trusted sites, often relied upon for daily business operations. Malicious emails reported directly to the Cofense PDC use a variety of such tactics to evade SEGs. Threat actors abuse trusted collaboration sites and cloud providers like Microsoft (SharePoint, OneDrive, O365), Google (Google Forms), Adobe, and Dropbox to deliver credential phish and malware. We also see them giving the user options to choose from the most commonly used email platforms. The phishing emails often contain URLs hosted on legitimate domains that maintain a broad consumer base to avoid being blocked by content rules and filters.

With increased use of trusted hosting platforms and the threat actor's ability to leverage these well-known alerts, how can organizations better protect against phishing? Deploy MFA (Multi-factor Authentication) and a phishing detection and response platform or managed service.

The most abused platforms include:

Microsoft

Adobe

Dropbox

Pick Your Own Webmail (multibrand options)

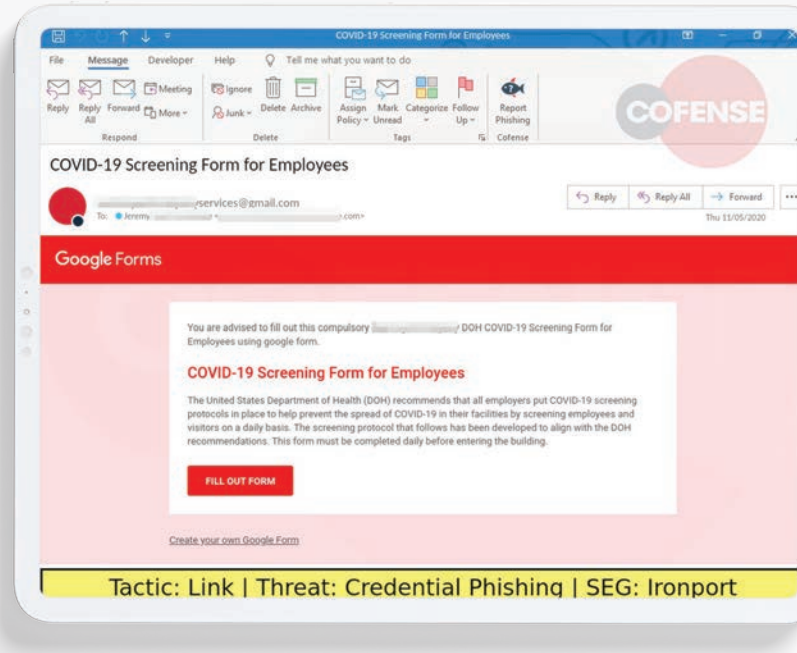


Figure 2 - Example of abusing trusted platforms.

Look-Back Attacks: Finding New Ways to Abuse Aged-Out Features

In 2020, CVE-2017-11882—also known as the Equation Editor vulnerability—and Office macro-enabled documents continued to dominate as the most popular delivery mechanisms for malware in phishing campaigns. CVE-2017-11882 is often used to download malware like information stealers and keyloggers, such as the prevalent Agent Tesla Keylogger. Office macros will almost certainly continue their prevalence in malware delivery, due to their importance in daily business operations.

Threat actors also evaded detection by abusing overlooked and often forgotten features within common software suites. Almost 30 years ago, Microsoft released Excel 4.0. This version was groundbreaking as it introduced macros to the Excel platform. While that version was depreciated within a year of its release, Microsoft has continued to provide backward compatibility for 4.0 macros in all Excel releases since.

Attackers have identified this legacy support and have capitalized on it as a method to evade detection from email security technologies.

Another example (Figure 3) of abusing older software features: a string of campaigns beginning in early June delivered Java Network Launch Protocol (JNLP) files, which allowed Java to load and run code files from remote sources. Oracle removed support for this feature in late 2018 with Java 11.0, but many users still run older versions. Despite its simplicity, this delivery mechanism evaded multiple SEGs, and was seen to deliver TrickBot, Expiro, and Ursnif malware targeting users in both English and Italian.

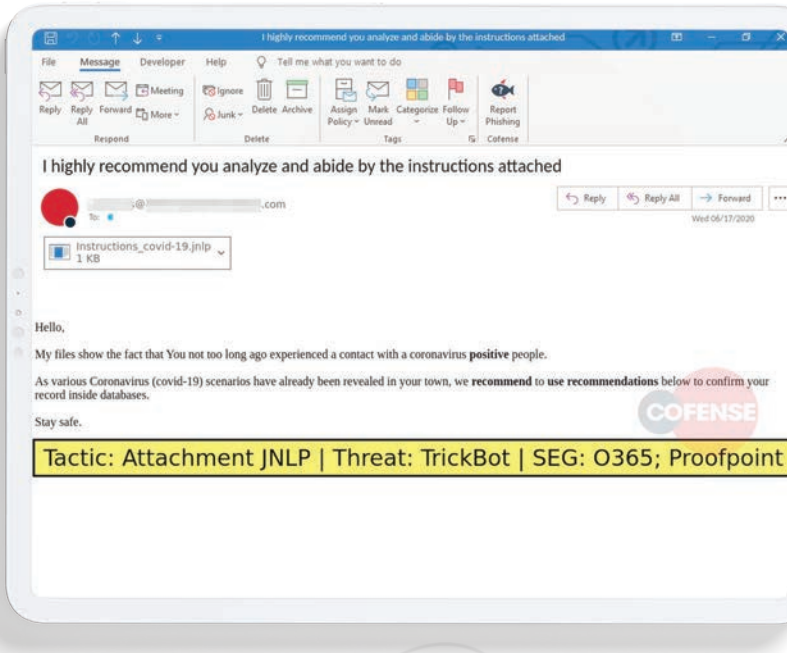


Figure 3 - Example of abusing trusted platforms.

A New Delivery Mechanism, Built to Evade

In 2020, GuLoader rose as one of the top malware delivery mechanisms in phishing, first appearing in Q1 and surging during Q2. GuLoader has been used to deliver remote administration tools, keyloggers, credential stealers, and other malware phenotypes.

While GuLoader is an executable, it is normally deployed through weaponized office documents that are built to bypass security controls and download the malware directly from the victim's computer system. GuLoader's continued evolution of sophisticated delivery and execution techniques make it increasingly useful in delivering threats.

Advanced Evasion Features

GuLoader uses advanced techniques at every stage of execution to try to evade network, email, and host-based security technology:

- **Email attachment scanning:**
  Obfuscation and encryption hide GuLoader's actual functions. Without executing at least a portion of it, an antivirus product cannot detect what it does.

- **Dynamic or sandbox analysis:**
  GuLoader contains false code instructions designed to thwart analysis tools and a wide array of tricks to avoid executing in virtual or sandbox environments.

- **Domain and network controls:**
  Threat actors using GuLoader store their malicious payloads on cloud platforms like Google Drive and Microsoft OneDrive. Organizations often treat these platforms as trusted assets and infrequently subject them to comprehensive analysis or blocking.

- **Network-based scanning:**
  Each malicious payload is encrypted with a key unique to its campaign, so neither the cloud services nor a network traffic analyzer is able to tell what it is.

- **Endpoint security products:**
  GuLoader can start up legitimate Windows programs and inject itself into their memory space, giving the malicious payload cover from endpoint analysis.

Responses matter

One of the key features in Cofense Triage is getting a response back to the user reporting the suspicious email.

Why is this important?
Almost 17% of the emails identified as malicious were related to a financial transaction. Finance teams are under extreme pressure to process invoices and payments in a timely fashion to keep the business running, especially during month or quarter end when financial reporting is critical. So, if a user hasn't heard anything back about the email they reported, they will most likely interact with that message.

Additionally, everyone wants to know that what they report matters. If there is no response on the status (received, analyzed, etc.) users are less likely to continue to report and the organizational risk increases.

SECTION 3:

The Big Phishing Campaigns of 2020—Emotet and Ryuk

If we learned anything from 2020, it's that threat actors' abilities to quickly adjust their methods to world events can be lightning fast. From Emotet to Ryuk, and let's not forget COVID-19, Cofense and our Cofense Labs and Intelligence teams worked overtime.

Last year brought an unprecedented amount of disruption, directly leading to an increase in both volume and variety of threat activity. Threat actors continued to advance their tactics, techniques, and procedures to ensure their emails would reach end users throughout the year.

Here's what we saw:

Emotet

Cofense has been tracking the Emotet botnet for several years now. This insight has enabled us to collect a massive set of data on the templates, malicious payloads, tactics, and continuous evolution of this pervasive botnet.

Emotet has seen multiple iterations over the years and has consistently advanced, adapted, and been a threat to organizations around the globe. The threat actors behind Emotet appear to spend a lot of time developing and advancing modules and overall functionality for their malware. Most of these modules focus on obtaining, stealing, and exfiltrating diverse types of data, including local and stored credentials, contact lists, and emails. Additionally, Emotet has also been known to drop multiple types of malware, such as: IcedID, QakBot, TrickBot, and Dreambot. In some cases, ransomware such as Ryuk and Conti have been deployed.

The primary method in which Emotet propagates itself is through malicious emails. Once an account has been compromised, Emotet scraps the user's emails and generates contact lists and unique phishing templates that are then sent out via the same compromised email accounts and systems. The tactic of using existing emails and responding to them as if it were a continuation of a previous conversation is known as a reply-chain attack.

Leveraging this new reply-chain tactic increased the variance and difficulty for detection by email security filters and gateways and increased the chance of tricking unsuspecting recipients. This provided them with a vast amount of capability to expand their phishing campaigns with a level of authenticity without having to worry about translations or common grammatical errors that we often see in generic phishing emails. Since the introduction of this new tactic, Cofense has also seen them begin to extract the attachments of those emails as well. This tactic and its use can be confirmed by the surge of Emotet phishing campaigns and infections that were seen throughout 2020.

Reply-chain emails solved several problems for Emotet in relation to their phishing campaigns.

Not only did it enable them to increase their infection rates dramatically, but it also provided them with a large repository of emails in many different languages from around the world.

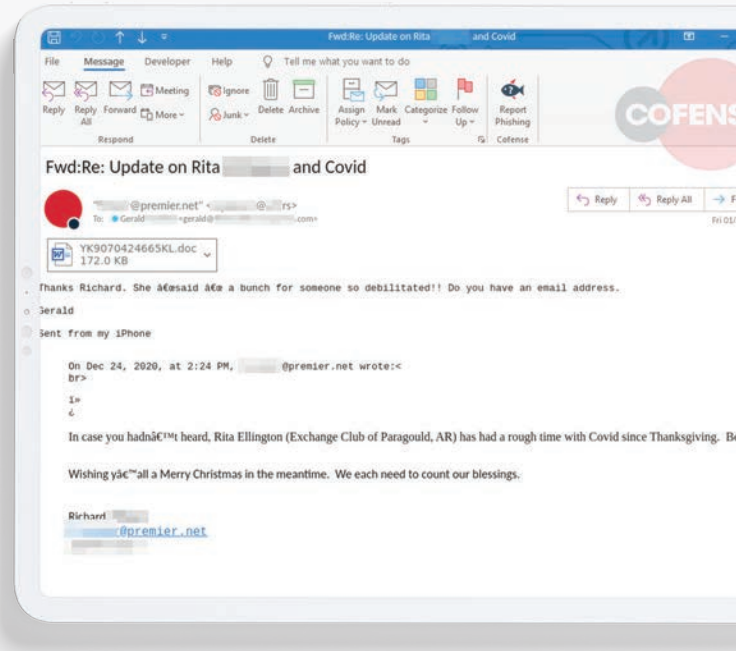
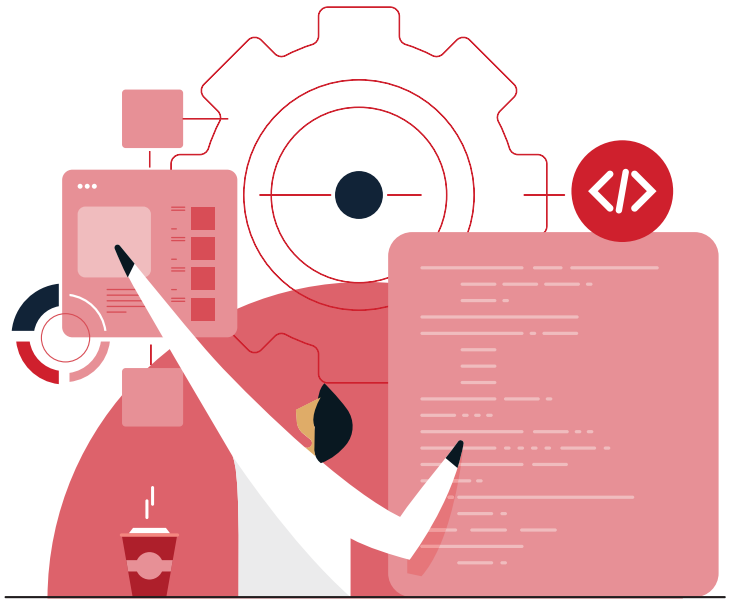


Figure 4 - Emotet Reply-Chain Sample

Emotet leveraged email attachments and URLs within its phishing campaigns. Weaponized Office documents were the attachment type of choice, and URLs pointed to compromised websites or services and often resulted in some form of download as well. In the past, these Office documents were standardized with little variance, and due to that threat defenders were able to quickly identify and implement email filtering and overall defense measures. However, over the past year, Emotet has evolved on this front and began employing a technique called "hash busting," which randomizes the malicious payloads just enough so that each has the potential of generating a unique hash value. Recent attempts to collect and calculate hashes on a broad sample set of malicious attachments have resulted in tens of thousands of unique hashes being seen over short periods of time.

As with any botnet, the bots must communicate with command-and-control infrastructure to receive updates and new commands/tasks. On any given day, there may be over 300 unique command and control domains, URLs, or IP addresses that are used by the Emotet clients that are installed on compromised systems. This list changes daily and is geographically dispersed. Most of these connections function as proxies and consist of compromised hosts, websites, and domains. As this layer of command and control continuously changes with newly compromised hosts and accounts, it also acts as a method of obfuscation for the actual backend infrastructure.



Having users who are trained to spot phishing attacks, detect reply-chain campaigns, and report suspicious emails can be the difference between a secure organization and full network compromise.

A final note on Emotet

On January 27, 2021, authorities from eight countries conducted a disruption operation against Emotet. According to the Europol press release, the action—named Operation LadyBird—targeted hundreds of servers worldwide. Authorities took over Emotet's primary servers, which give updates to infected computers. They issued an update that replaces the list of Emotet command-and-control (C2) servers with a list of C2 servers under law enforcement control. Ukrainian police also identified two Emotet operators, from whom they seized cash, computers, and other associated equipment. Finally, Dutch authorities recovered a trove of data stolen from Emotet victims, including email addresses, usernames, and passwords. They published a website allowing users to check whether their email address was in the compromised data. However, do not count Emotet out yet. Emotet has been so effective that abandoning it entirely would be highly likely to represent a lost opportunity for considerable profit.

The Ryuk Threat: Why BazarBackdoor Matters Most

On October 28, 2020, media reports and US Government (USG) notifications emerged regarding an active "credible" Ryuk ransomware threat targeting the US Healthcare and Public Health sector. This was reportedly based on chatter observed in an online forum that allegedly included members of the group behind Ryuk.

Cofense investigated this threat and observed increased activity against the healthcare sector. Our team assessed with high confidence that BazarBackdoor is the primary delivery mechanism currently used for Ryuk operations. Also, the team identified that similar phishing campaigns used to establish a foothold for Ryuk infections targeted other sectors as well.

What We Learned

Cofense assessed that Ryuk operators typically wait until their preferred delivery mechanism is successfully deployed to an intended target prior to deploying Ryuk ransomware itself. Up until TrickBot's disruption, Ryuk was most frequently delivered via TrickBot; however, our analysis indicated that the group behind Ryuk began leveraging BazarBackdoor to establish access to target systems in mid-September 2020. This aligns closely with announcements that US Cyber Command had taken action to disrupt TrickBot operations. The Cofense team assessed with high confidence that BazarBackdoor has been Ryuk's most predominant loader. BazarBackdoor is a stealthy malware downloader that is used by the same group as TrickBot. Typically, emails designed to appear as internal business communications are sent to victims within an organization, often with relevant employee names or positions. These emails usually contain a link, most often to a Google Docs page (See Figure 5), though other well-known file hosting platforms have been used as well. The Google Docs page will then present a convincing image with another embedded link. This link is typically to a malicious executable hosted on a trusted platform such as Amazon AWS. This chain of legitimate services makes it difficult to detect and stop these campaigns. Once in place on a victim's computer, BazarBackdoor uses specialized network communications to avoid detection and to contact its command and control (C2) locations. Part of these communications involve DNS lookups for .bazar domains, which is the reason behind its Bazar name. These C2 locations also often serve as payload locations. After BazarBackdoor contacts its C2 center it will then collect additional information which the threat actors can use to deliver customized reconnaissance tools, such as Cobalt Strike payloads. The threat actors can also choose to deliver other payloads such as Ryuk ransomware. The deployment of Ryuk ransomware is not automated, and therefore will not occur unless the threat actors decide the infected environment is a target.

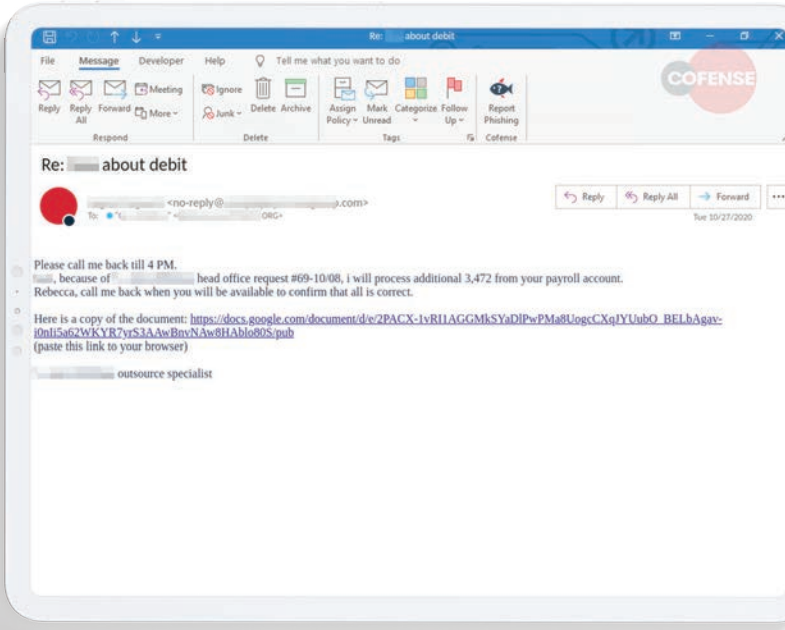


Figure 5 - Ryuk Example

It became clear that the recent efforts by multiple parties to cripple TrickBot seem to have been effective in transitioning the Ryuk actors to leveraging BazarBackdoor. It is worth noting that there are past connections between TrickBot activity and Emotet. While there is no direct evidence of current Emotet involvement in these campaigns, we cannot rule out future delivery of Ryuk via Emotet, given historical relationships between TrickBot and Emotet. As the TrickBot infrastructure appears to be in the process of restructuring, Cofense assesses that it may find use again as a delivery mechanism.

The Phish

Cofense Intelligence has identified several campaigns, targeting multiple sectors, that share strong similarities to the phishing emails reportedly used as initial attack vectors in Ryuk campaigns, as outlined by FireEye. Two subject themes stand out across several industry verticals we have confirmed were targets of BazarBackdoor. These subjects relate A) to employment termination, almost always including the word "termination," or B) to payroll, almost always including the word "debit," as shown in Figure 6. While the subjects remain the same, we observed two separate download services: via Google Docs or Constant Contact. We have included a list that highlights the different industries we have confirmed were targeted by such campaigns. However, we cannot assess whether Ryuk operators intended to further infect these targets with Ryuk ransomware. This is due to the fact that it appears likely that Ryuk operators have cast a wide net for potential infection vectors and choose which successful footholds to manually interact with and leverage.

It is worth noting, these campaigns began in mid-September 2020, which corresponds with the timing of coordinated offensive operations to disrupt TrickBot.

The sectors Cofense has directly observed targeted by Ryuk in these campaigns include:

- **Consumer Goods**
- **Healthcare**
- **Mining**
- **Energy**
- **Insurance**
- **Professional Services**
- **Financial Services**
- **Manufacturing**
- **Retail**

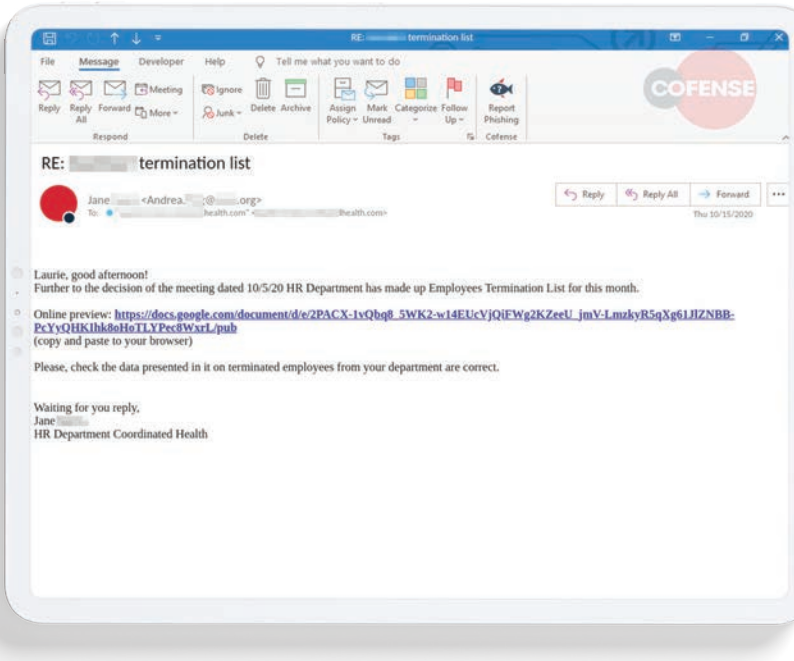
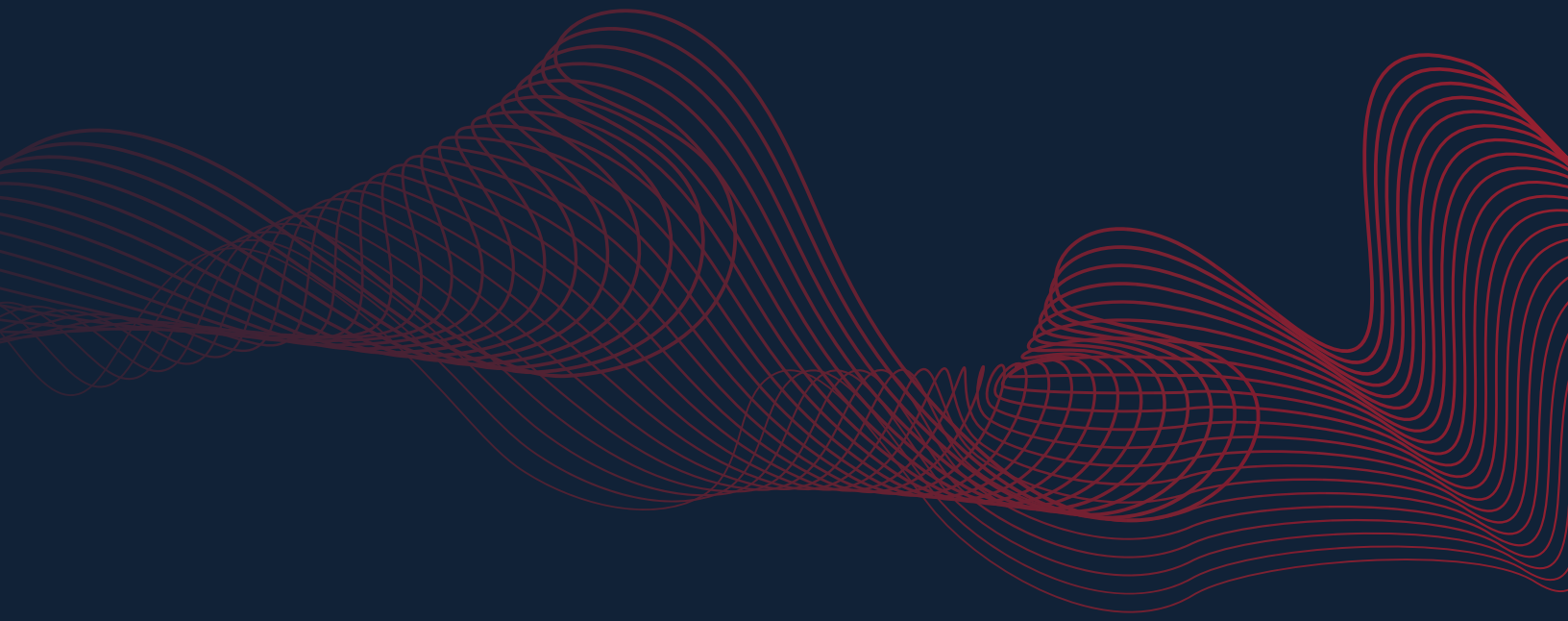


Figure 6 - Ryuk Example 2



SECTION 4:

How COVID-19 Changed the Threat Landscape

COVID-19 was certainly the source of the most disruption in 2020. During the peak of pandemic-themed campaigns, phishing emails predominantly delivered credential phishing and Agent Tesla keylogger, but threat actors also delivered ransomware, keyloggers, remote access Trojans, and information stealers.

And, while overall phishing volume did not increase, numerous phishing campaign themes speak to the virus and its impact. Pandemic-themed campaigns picked up steam in February and March, peaking in April as much of the world adjusted to the concept of a "new normal." Following April, as the first shudders of the economic impact were felt and millions of people shifted to remote work, threat actors were quick to pounce.

6 Frequent COVID-related Phishing Themes

- Pandemic updates and guidance **purporting to be from global, federal, or local health organizations**
- **COVID-19 office infection data/contact tracing**
- **Updates on remote working changes**—company news and meeting invites
- Federal financial relief packages for **small or medium business loans**
- **Teleconferencing platform invites** or required updates related to platforms like Zoom, Teams, WebEx
- **Financial claims related to COVID-19**

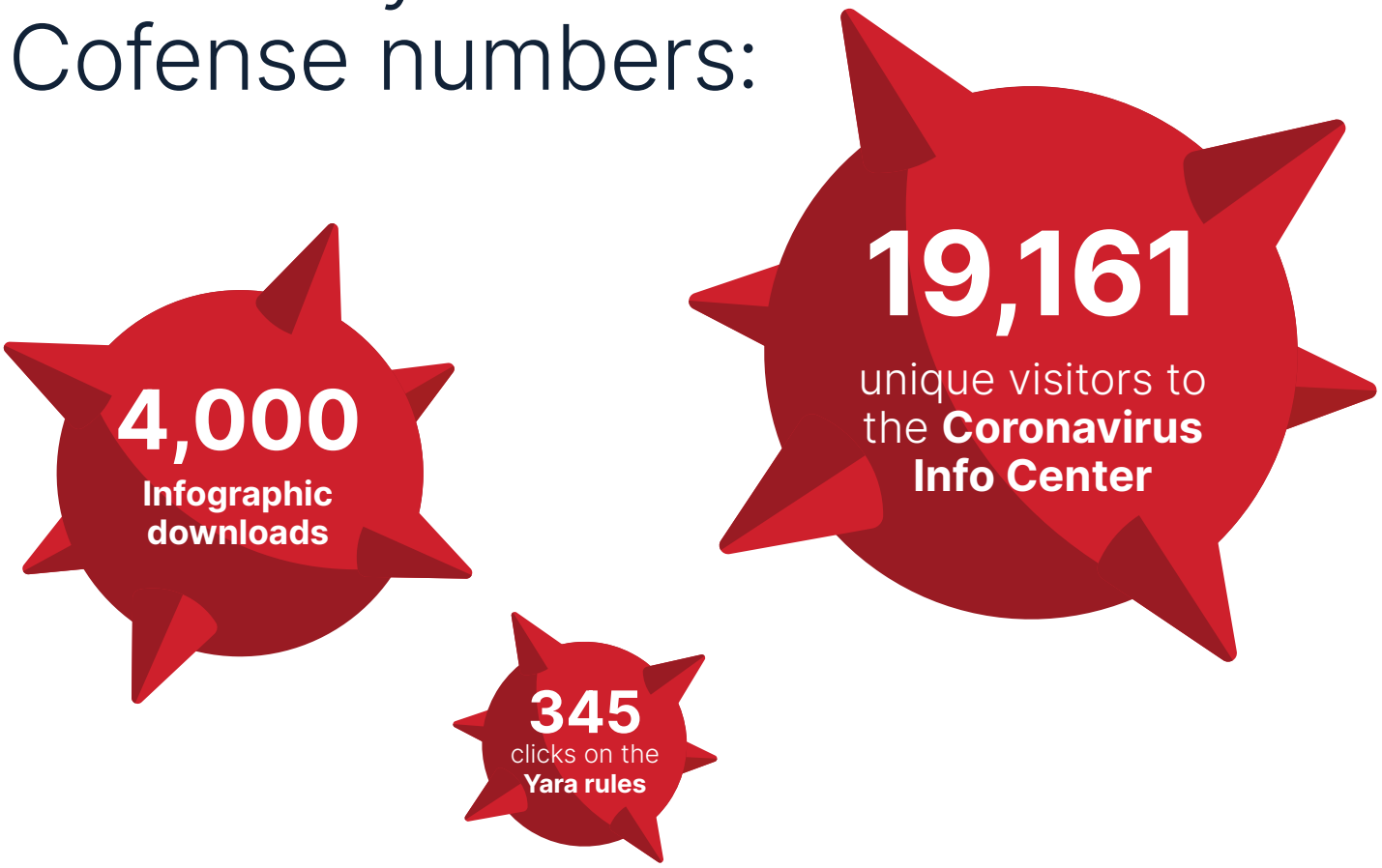
Cofense has seen sophisticated and novice campaigns alike delivered with the above-mentioned themes. Similarly, we observed COVID-19 themes used to deliver different malware families as well as credential phish and BEC/CEO fraud. Though campaigns dropped in volume after April's peak, themes continued to follow the news. In the coming months, be on the lookout for contact tracing and vaccination-themed campaigns.

When it came to running PhishMe simulations, we quickly pulled our templates with the COVID theme once organizations were kicking into their business continuity plans to quarantine.

Cofense created a Coronavirus Info Center so our customers—or anyone—could have one place to get the most up-to-date information about phishing attacks, threat actors, and of course, YARA rules.

See page 22 for key statistics.

COVID by the Cofense numbers:



Coronavirus blog post reads

4,161

Threat Actors Capitalize on Global Concern About Coronavirus in New Phishing Campaigns

490

Staff Members' Inbox Positive for Coronavirus-Themed Phish

469

Coronavirus Test Results Return **Data-Exfiltrating Ransomware**

381

Coronavirus Redefines the **Phishing Threat Landscape**

315

Coronavirus-Themed Phish **Continue to Surge**

450

Coronavirus Phishing Webinar Attendees

677

Phish Friday Podcast Downloads Coronavirus Awareness Training

SECTION 5:

Fighting Crafty Humans—Malware in 2020

No matter how much automation drives a phishing campaign execution, behind every phishing attack is a threat actor. These adversaries understand what motivates and moves humans to action. They understand the power of social engineering, and how to outwit defense technologies and uneducated users.

They know that they are in a game of cat-and-mouse with security researchers, and they find or develop new malware and delivery tactics to stay ahead.

Threat actors have improved at finding the “sweet spot” in social engineering.

They are identifying ways to make widespread campaigns appear targeted, as highlighted in the above overview of Emotet. In May, a credential phishing campaign targeted the energy and financial sectors using compromised business emails to target business contacts. It used analysis obfuscation tactics (like random URL text generation or privacy enabled domain registration details) to solicit and harvest email login credentials. The campaign also used tactics to appear legitimate, such as sending emails from compromised email addresses, complete with the compromised user’s signature and a theme unique to the business.

These emails evaded gateways and eased the target’s sense of caution by containing personal information from the compromised business, likely coming from a previously trusted contact, and by including relevant themes such as COVID-19 or important company updates. Initially this campaign targeted the oil and gas industry. From there it has spread to the financial sector.

Attackers are diversifying the malware used in phishing campaigns and finding new ways to monetize phishing.

In 2020, Cofense Intelligence identified a major diversification in malware families prominent in phishing. As of August 20, we saw 31 new or previously dormant malware families in phishing campaigns. Two major newcomers include Mass Logger and Avaddon ransomware. Mass Logger is routinely updated and modular in capability, while Avaddon suggests a return to broadly targeted ransomware operations. Increasingly, ransomware operators are pairing traditional ransomware with malware capable of data theft, then leaking the victim’s data to accelerate ransom payment. Avaddon ransomware seems to have joined this trend. Cofense Intelligence has seen these campaigns reach the inbox in different sectors and in environments protected by multiple SEGs.

We expect this trend of ransomware attackers leaking corporate data to force accelerated payment to continue, as it increases the pain for ransomware victims who may otherwise not pay. Organizations may be reputationally damaged by a data leak and, depending on laws and regulations, may be subject to fines and penalties. Data owners can potentially hold the organization liable and pursue litigation, exacerbating the cost.

New and Returning Malware in 2020:

Knowing your enemy is half the battle.
Here are the top trends Cofense saw in phishing-related malware throughout 2020. While a large percentage of commodity malware is detected every day, this is a listing of some of the more focused and continuously evolving malware families Cofense saw, impacting organizations around the world.

New in 2020:

Avaddon Ransomware
Cheetah Keylogger
FireBird RAT
Gamorrah Bot
Grandoreiro
Hive RAT
LolKek Malware
Mass Logger
Matiex Keylogger
RedLine Stealer
STR RAT

Returning after 9+ month dormancy, often with updates:

Chanitor/Hancitor
Cobian RAT
Dharma Ransomware
Expiro
LatentBot
Proyecto RAT
Qarallax RAT
Remote Manipulator System (RMS)
Sality

Returned in 2020 after months of dormancy, in higher dissemination than in 2019:

Black RAT
Nemty Ransomware
Hakbit Ransomware
BetaBot
Iced-ID
KPOT
Kutaki
Loda
Pyrogenic Stealer
Valak
Vidar Stealer

SECTION 6:

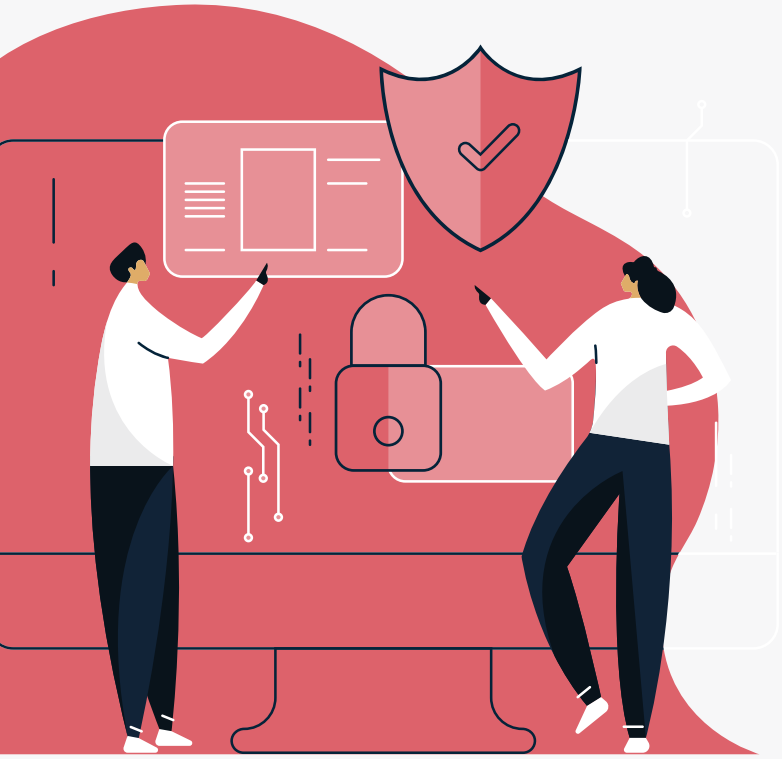
The Need for Decreasing Dwell Time

When malicious emails reach the inbox, the chance of at least one erroneous click remains high. Average click rate for credential phishing simulations in PhishMe customers in 2020 is 10.7%—meaning that during a real attack, almost 11 users out of 100 will likely click on the phish, potentially leading to compromise of their corporate credentials. The longer a malicious email stays in the inbox, the greater the chance of an erroneous click.

One metric of growing importance is dwell time—the elapsed time between an attacker gaining access to an environment and when they are detected, and the threat mitigated. Dwell time is composed of two key metrics—mean time to detect (MTTD) and mean time to remediate (MTTR). In their 2020 M-Trends report, Mandiant stated that global median dwell time is 56 days. Clearly, more work needs to be done. For phishing attacks, MTTD can be reduced through effective conditioning of end users to identify phishing threats and report them.

Mean time to remediate (MTTR) is currently impacted by:

- **The ability of security teams to effectively analyze today's phishing threats, and**
- **The ability of these same teams to hunt for, and eradicate, all copies of a malicious email within their environment**



When COVID-19 appeared and more people worked from home, "We needed to respond faster and remove emails in fewer steps."

Patrick Burch
IT Security Manager, Brasfield & Gorrie

Recently, the Cofense Phishing Defense Center observed a credential harvesting threat following a report by an alert user. The PDC subsequently observed the same payload URL in emails reported by 11 other organizations over a 7-day period. In the case of one organization impacted by this threat, we observed the same payload being reported by users 7 days after the threat was first identified. Email defenses are either failing to keep up, or security teams lack the capability to quickly remove threats that are known to exist in user inboxes.

Today, commonly used mechanisms such as PowerShell are fine for their intended purpose of compliance-based searching, where time is not of the essence, but they are woefully inadequate for email threat hunting. Search performance is constrained by unpredictable environmental throttling and by limited options to specify search scope. Attackers are quick to exploit these gaps with sophisticated threats like polymorphic phishing.

These inherent challenges lead to less than optimal threat response. For example, here at Cofense we are frequently told by our prospects and customers that email threat hunting doesn't occur unless a significant volume of reports of the same threat are received. Why? The age-old security problem—too much effort and not enough time. When it only takes a single compromise to cause major problems, email hunting needs to be simplified and fast.

SECTION 7:

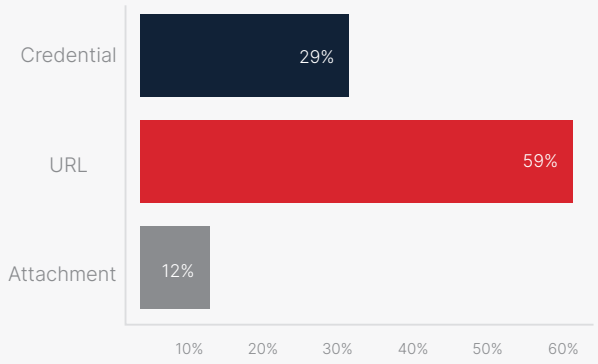
Stopping Attackers with Human Analysis and Reporting—PhishMe in 2020

You can't stop human attackers without human reporting and analysis.

As with other portions of this report, we're making a shift in what we cover in this section as it relates to **phishing simulation training**. In previous years, we dedicated an entire report focused on training metrics. This year, we are sharing the highlights.

PhishMe Data—Simulations

Chart: Type of Simulations by Customers with Reporter



2.7	3.4	2.8
Overall Resiliency Rate	*PDC Customers*	*Triage Customers (excluding PDC)*

Click to view by Industry NAICS chart

But what about training?

There is a reason we started with the phishing threat landscape and left the topic of training your users for the end. When it comes to training your users on threats leading to a data breach, simulating real threats is most effective. Threat actors are using real and relevant communications that your users regularly engage with—are you using these for your simulation templates?

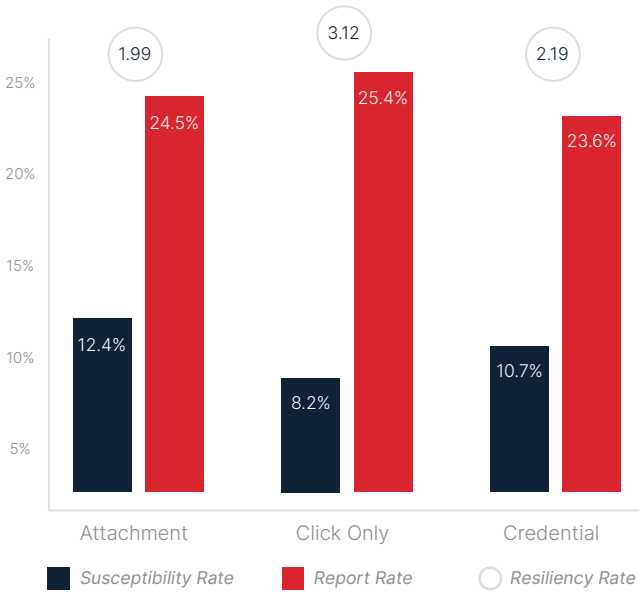
We've mentioned the SEG throughout this report and it is just as relevant when it comes to training your users. Users are busy. In organizations that are highly regulated, there is a LOT of pressure to check a box for training-related regulations. Business leaders want to know how many hours their departments are being kept from responding to customers, processing invoices, or taking sales appointments while in training; or what benefits are being derived from training. This is especially true when it comes to phishing simulations. While we've highlighted many emails that make it to the inbox, there are plenty that are stopped by the SEG. **Why does this matter?**

In order to make training relevant to your organization and prepare your users for the items that are most likely to make it to their inbox, aligning your phishing simulation scenarios to what they will most likely experience will have a greater impact on your organization's overall resiliency when it comes to real phishing.

The Basics

As we highlighted earlier, Cofense customers who subscribe to our Managed PDR service delivered through our Phishing Defense Center have higher resiliency rates. While both subscribers to the service and customers who manage their own solutions show good resiliency rates, the Managed PDR customers outperform with a resiliency score of 3.4 (compared to 2.7 for overall customers) because Cofense responds to every reported message.

Chart - Resiliency By Scenario Type

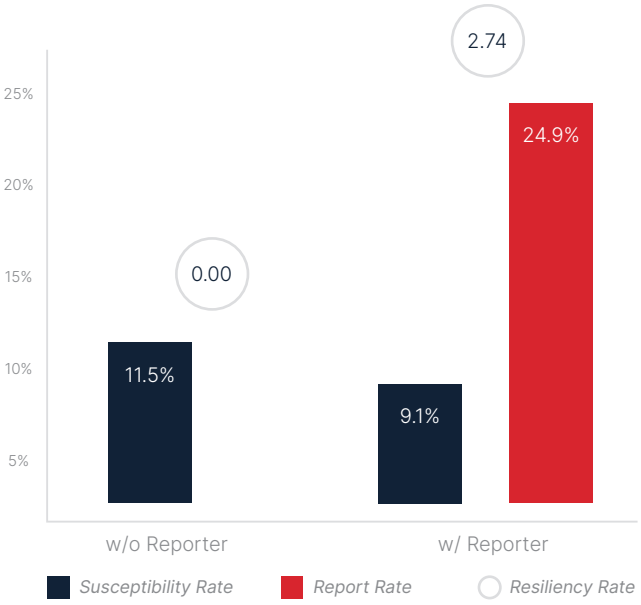


Susceptibility Rate = [susceptible recipients ÷ emails delivered]
This rate shows how many users were susceptible to the scenario versus the total number of emails delivered.

Report Rate = [users who reported ÷ emails delivered]
This is a percentage of users that reported the email, without being susceptible to it, compared to the total number of users who received the email.

Resiliency Rate = [reported on rate ÷ susceptibility rate]
This is the percentage of users who reported the email without being susceptible to it, compared to the percentage of users who fell susceptible.

Chart - 2020 Resiliency



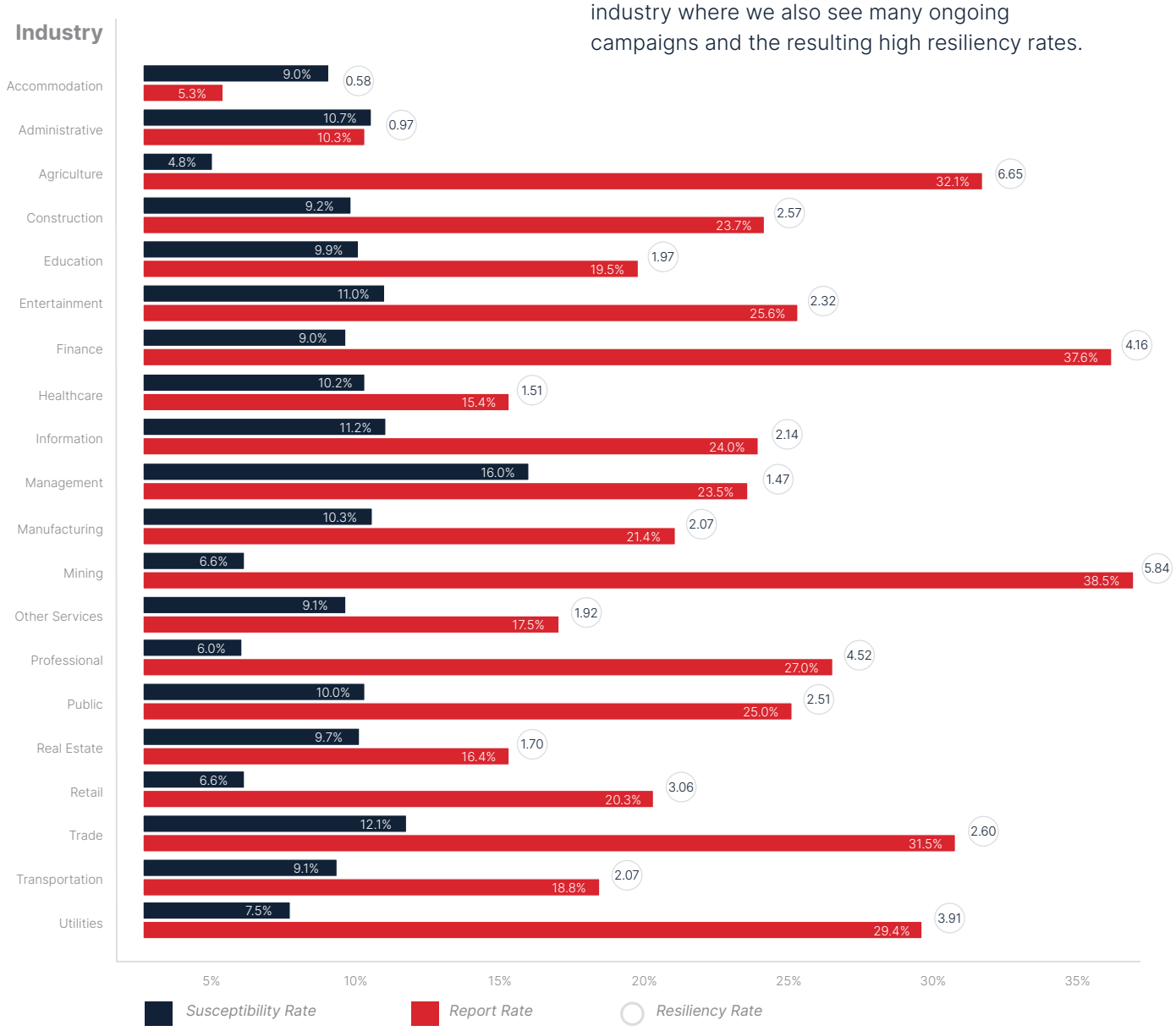
So Many Choices

When it comes to planning a simulation campaign, paging through the library of scenario templates is a daunting task. To help our Security Awareness operators in their planning process, we introduced "smart suggest," which assists in selecting templates that are relevant to their organization. Since implementing these suggestions, 30% of organizations have adopted the templates to better align with the phishing landscape that most realistically aligns with what their users would experience.

The data related to scenarios is interesting. As you can see in the graph on the left, the report rate for the three types of scenarios is relatively equal. However, the susceptibility rate for scenarios with Attachments or Credential requests are significantly higher than Click Only scenarios. The report rate is the opposite. Click Only scenarios have higher report rates. This suggests that the scenarios are effective in training users to spot all of the phishing types but especially good at spotting the Click Only phish. Accordingly, the resiliency against Click Only phish is higher than the other two types of scenarios. Moreso, we see that **57%** of the real reported phish are credential phish but only **29%** of the simulated scenarios use the credential template. **What this means is that more attention should be given to Attachment and Credential phish scenarios going forward.** Especially considering the impact to an organization of a successful Credential phish.

How different industries stack up

Looking at the resiliency by industry, this year we continue to see Mining in the lead. The Mining category includes many customers in the broader Energy sector, which is highly regulated, and customers will often run monthly or multi-month campaigns. Finance is another highly regulated industry where we also see many ongoing campaigns and the resulting high resiliency rates.



Training works. Conditioning works. Take the 70:20:10 Model for Learning and Development[2] where 70% of knowledge comes from job-related experience, 20% from interactions with peers or mentors, and 10% from formal education. The developers of the model concluded that hands-on experience—in this case phishing simulations—is the most beneficial for employees as it enables them to discover and learn and refine their skills. Also, they learn from their mistakes and receive immediate feedback on their performance. With PhishMe, this holds true. Your users want to be able to identify and mitigate a potential threat to your organization and quickly report. With training, they can.

2. Morgan McCall, Michael M. Lombardo and Robert A. Eichinger, Center for Creative Leadership, a nonprofit educational institution in Greensboro, N.C.

SECTION 8:

What We Might See in 2021

We expect the SOC to have a more active voice in enterprise email configuration.

Configuring a secure mail gateway properly can be challenging. The SOC finally gets tired of dealing with the rollercoaster of settings on the email gateway.

MFA: Phishing campaigns and tooling will be more aware of multi-factor-authentication.

2020 fast tracked companies' plans to move to an online platform like Microsoft 365 or Google Workspace, making the enablement of MFA more prolific. Attackers will adapt.

Techniques to evade Automated URL analysis will improve.

As outlined in this report, there are fewer attachment based phishing campaigns as attackers focus more on credentials. Attackers are already experimenting with CAPTCHA protected phishing sites.

Smishing will continue to be a big-nothing-burger.

The number of vendors that will sell a computer-based training series about the dangers of Smishing will increase. But do you know what will not increase? The cases of actual Smishing in the real world.

SECTION 9:

About Cofense

Cofense solves the problem of phishing emails that get past SEGs (Secure Email Gateways) and deliver threats to the inbox.

Combining automated response and human detection, our platform enables your teams to stop phishing attacks in minutes. While SEGs can validate an email's sender and to some extent its content, these technologies fail to stop phishing attacks every day. They simply cannot keep pace with threat actors' innovations, doomed to remain a step behind in the game of cat-and-mouse.

The Cofense Phishing Detection and Response (PDR) platform leverages a global network of over 25 million people actively reporting suspected phish, combined with advanced automation to stop phishing attacks faster and stay ahead of breaches. When an organization uses all of the Cofense solutions together, they can educate employees on how to identify and report phish, detect phish in their environment, and respond quickly to remediate threats.

Phishing solutions and products

Our Phishing Detection and Response platform catches the phishing emails that your secure email gateway inevitably misses.

We deliver the technology and insight needed to detect, respond, and stop phishing attacks.

Detection

Cofense PhishMe
Employee conditioning for resiliency against phishing

Cofense LMS
Streamlined employee computer-based training

Cofense Reporter
Real threats in real time from employees

Response

Cofense Triage
Identify, analyze, and mitigate threats

Cofense Vision
Auto-quarantine phishing threats

Integrations

Cofense Intelligence
Human-vetted phishing threat intelligence

Managed PDR

Managed PDR
Comprehensive managed phishing detection and response service

What Makes Cofense Unique

Automated Response + Human Detection
Cofense conditions end users to report suspicious emails. Automation accelerates the SOC's analysis of email reports and their ability to find and quarantine every phish in a campaign.

Patented technology delivers real-time detection and quarantine of phish. Our platform eliminates manual tasks like sifting through false positives to speed phishing response and lower the risk of breach. Purely focused on phishing, our phishing intelligence also enables your SOAR, SIEM, or TIP to get a holistic view of risk in your organization.

Network Effect
Over 25 million users are equipped with the Cofense Reporter button, forming the world's largest network of human phishing sensors. When users report phish, your SOC gains the visibility to remediate faster.

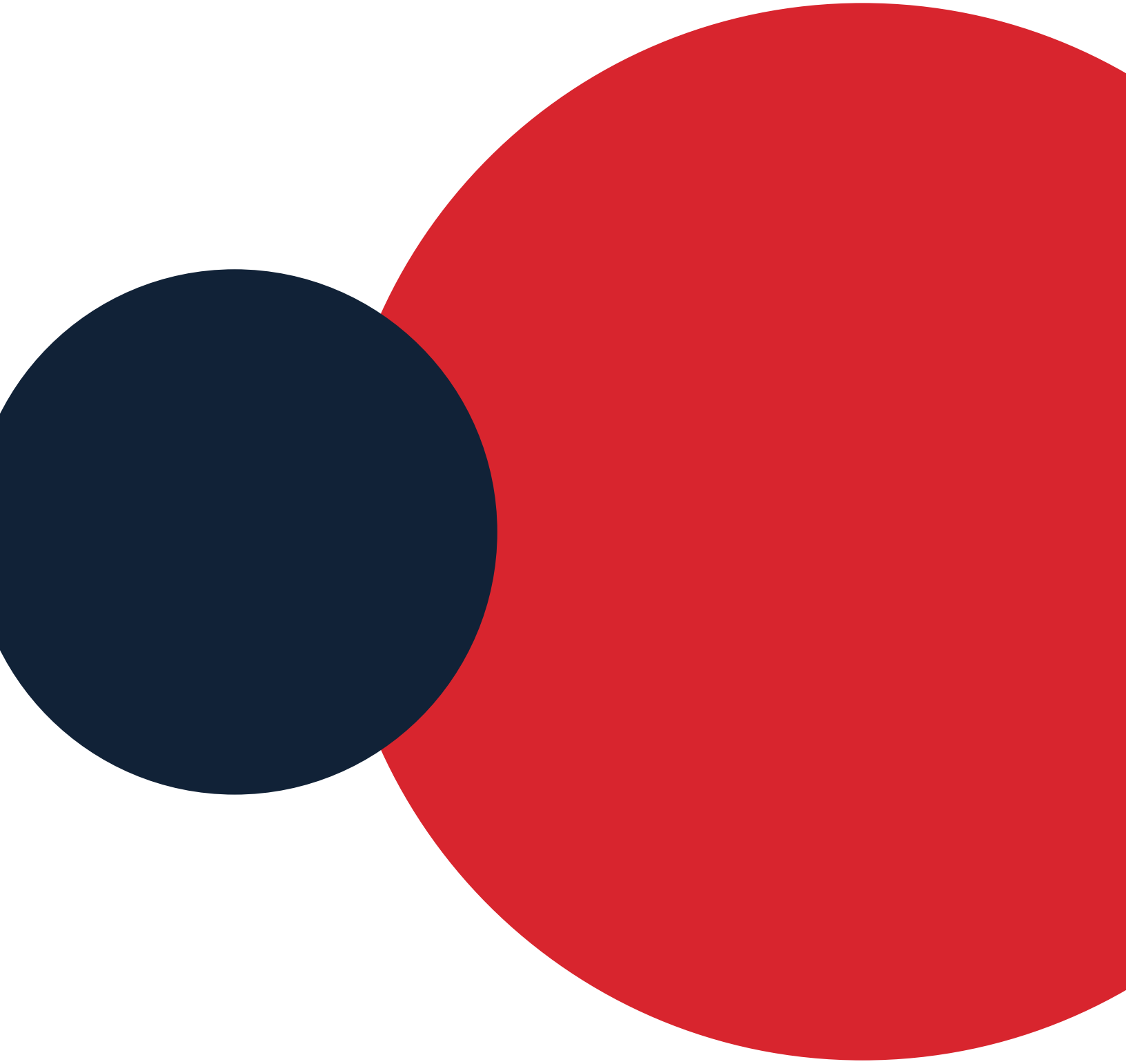
Phishing Intelligence

Cofense Intelligence maintains the largest, most accurate data set on phish that have hit the inbox.

Our Cofense Labs and Intelligence teams analyze millions of phish and malware samples annually. Their insights enable the SOC to prioritize threats and fine-tune perimeter controls.

Unbiased Insights
We are Switzerland for email security. Cofense sees and shares the email threats evading all SEGs. Regardless of which SEG your company uses, you need a phishing defense to fill critical gaps.

Focus
100% of our R&D is focused on developing solutions to stop phishing attacks.



COFENSE