COFENSE
EMAIL SECURITY

2024

Annual State of Email Security REPORT

ISSUED FEBRUARY 2024

COFENSE
EMAIL SECURITY

IF YOU REALLY WANT TO KNOW THE CURRENT STATE OF EMAIL SECURITY, YOU HAVE COME TO THE RIGHT PLACE.

Contents

Introduction

Here's the reality.

In 2023, malicious email threats bypassing secure email gateways (SEGs) increased by more than 100%. In other words, your email security solutions aren't stopping the threats you think they are.

We know because:

- We are the only email security company with a global network of **35+ million trained employees** reporting suspected threats around the clock
- Our proprietary data provides unmatched industry insights with a **99.998%** accuracy rate
- No one else has over a decade of insights and intelligence into the threats that **EVERY SEG** misses
- Last year we caught a malicious email **EVERY MINUTE** that bypassed our customers SEG

Security threats are real, they continue to grow, and they are likely to penetrate an organization through email. Organizations simply cannot settle for 'Good Enough' email security and sole reliance on a SEG is not enough. As we all know, it only takes one breach to damage a company's financial status, brand reputation, and/or relationship with its employees and customers.

Each day, our analysts see thousands of threats that are bypassing all SEGs on the market.

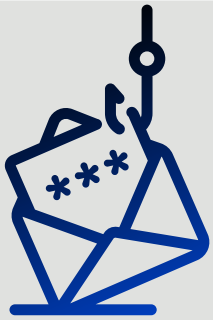
That's exactly why Cofense® has spent the last decade perfecting our phishing expertise, growing our network of Cofense-trained employees around the globe, and setting ourselves apart from the competition – simply put, we see and stop email threats that are missed by standard security controls before they do damage to an organization.

If you really want to know the current state of email security, you have come to the right place.

Let's dive into the numbers.

COFENSE
EMAIL SECURITY

2024 State of Email Security
By the Numbers

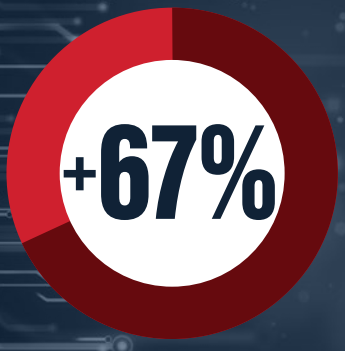


Over the last 12 months, **secure email gateways (SEGs) struggled to keep up with the evolving and sophisticated nature of today's phishing campaigns.**

We detected a **malicious email bypassing our customers' SEGs every minute.**

104.5%

Cofense saw a **104.5% increase** in the number of **malicious emails bypassing SEGs, per customer.**



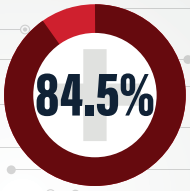
Credential phishing was the threat of choice in 2023, with a **67% increase in volume compared to 2022.**

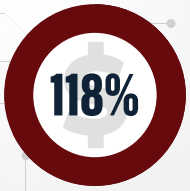
COFENSE
EMAIL SECURITY

2024 State of Email Security
By the Numbers

Email is still the **#1 threat vector** for cybercrime, with **90% of data breaches starting with a phish.**

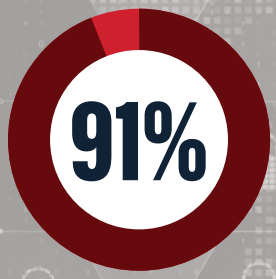
Phishing campaigns are evolving with an increase in tactics like vishing, smishing, brand impersonation, and QR code phishing that bypass SEGs. **Cofense reported a 331% increase in QR code active threat reports in 2023.**





Healthcare and finance remain the top targeted industries with **increases in malicious emails bypassing SEGs at 84.5% and 118%, respectively.**

New malware families, **including DarkGate and PikaBot**, have emerged to fill the gap left by the **FBI's dismantling of the Qakbot infrastructure.**



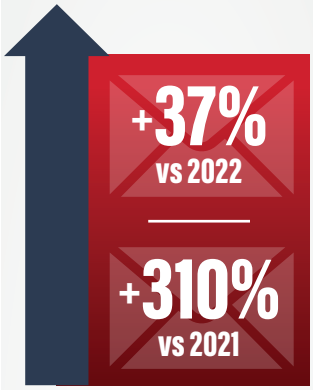
In 2023, credential phishing was responsible for **91% of active threat reports published.**

2024 State of Email Security

OVER THE LAST YEAR, cybersecurity threats continued to increase, with email acting as the primary threat delivery mechanism for attacks. With this increase, the need for rapid and actionable intelligence is mission-critical to protecting an organization from cyber criminals.

Uniquely powered by more than 35 million Cofense-trained employees, our phishing detection and response (PDR) solution detected a record-setting number of malicious emails and phishing campaigns that were missed by secure email gateways (SEGs).

In just two years, Cofense PDR uncovered almost 800 thousand unique malicious email campaigns with over 1.5 million emails detected worldwide. We have seen significant jumps in detected malicious emails year over year, and throughout the two years of data represented. Raw numbers of detected emails indicate 2023 had a 37% increase over 2022 and a 310% increase over 2021.



2023 saw a 37% increase in malicious threats compared to 2022, and a 310% increase in threats compared to 2021.

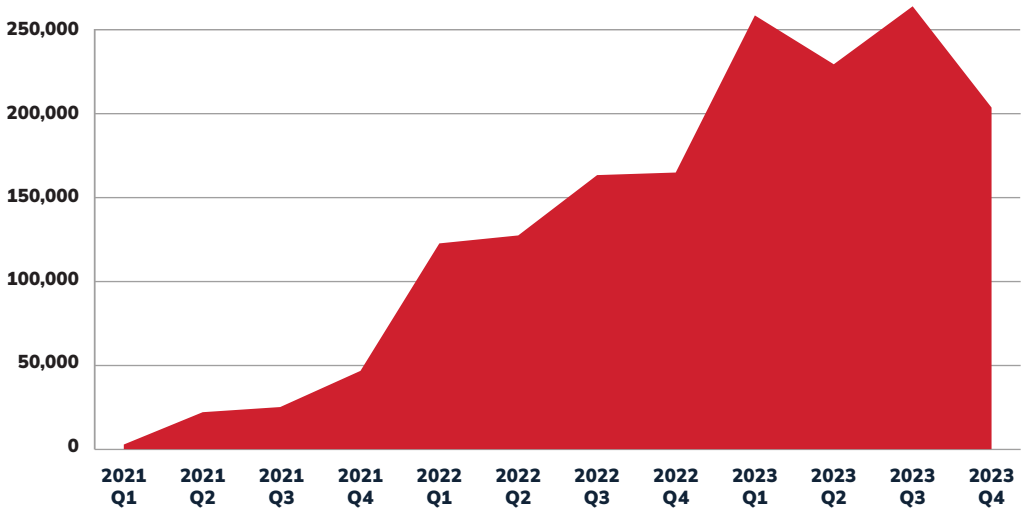
Cofense Intelligence

Cofense Auto-Quarantine Summary

Unique Email Campaigns Identified
770,892

Total Malicious Emails Identified
1,577,041

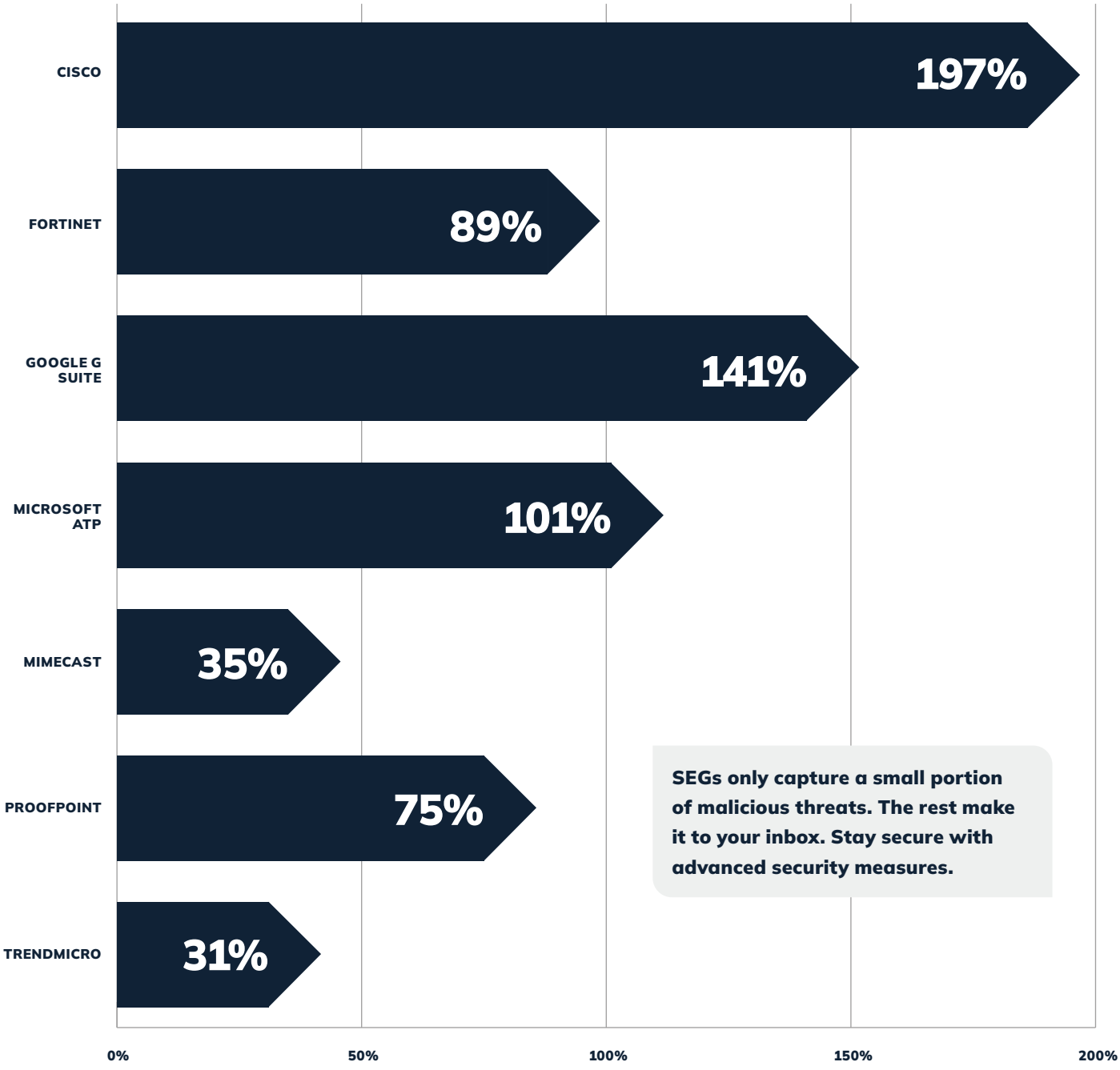
Total Malicious Emails Detected Using Cofense Intelligence



Today's organizations cannot settle for "good enough" email security. With the increasing frequency and severity of email attacks, it is essential to train your employees to identify and report malicious emails, while deploying industry-leading solutions to identify and remediate threats that are actively bypassing SEGs.

% Increase of Malicious Emails

that Bypassed SEGs*

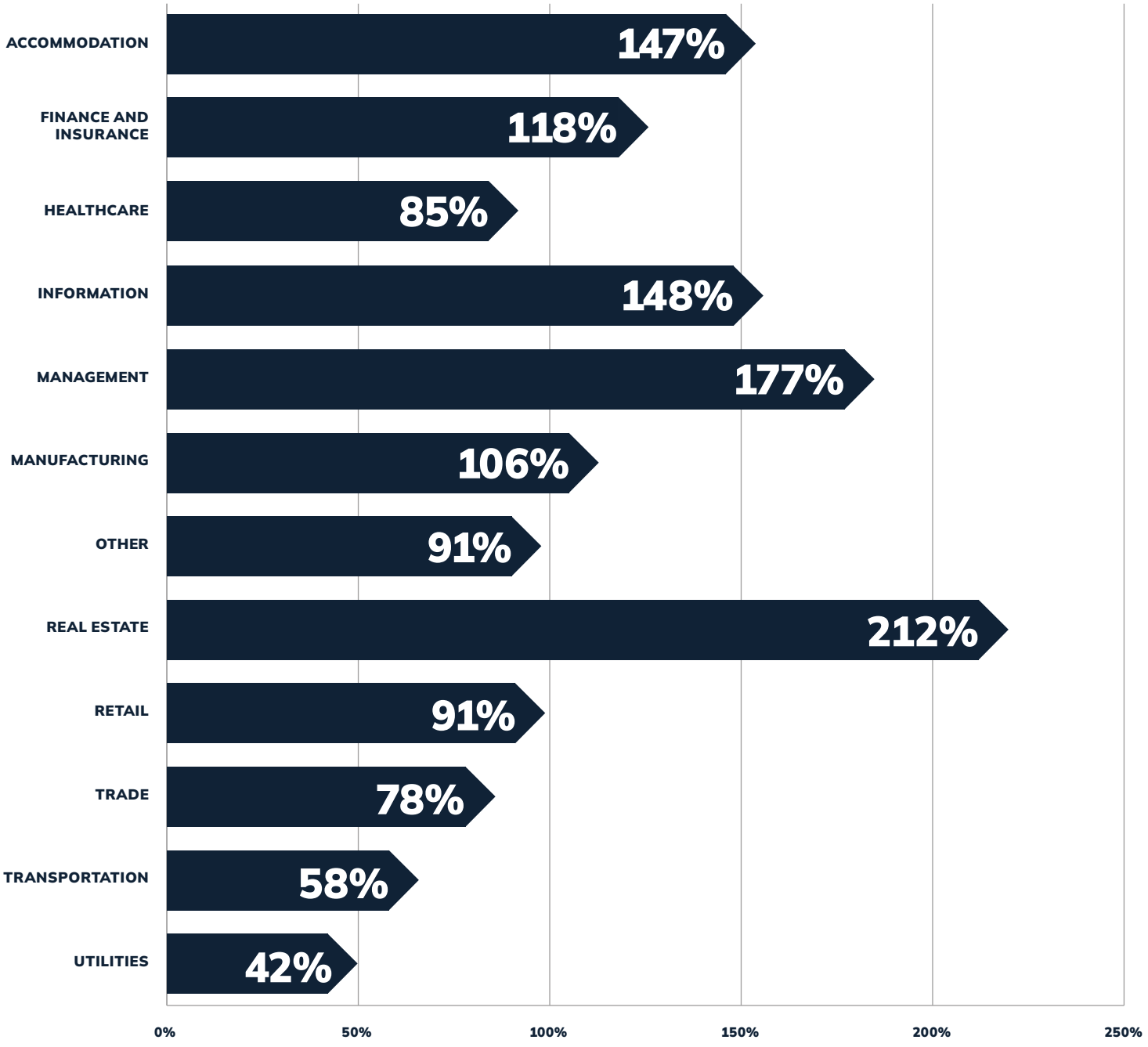


*This data is based on the percent change from 2022 to 2023 per Cofense PDC customer.

After a record-setting year, industry-specific SEG misses were all up across the board. Two of the most targeted industries in recent years, finance and healthcare, were once again key on threat actors' lists. But, new industries were key targets in 2023 with real estate and management seeing dramatic increases in malicious emails.

% Increase of Malicious Emails

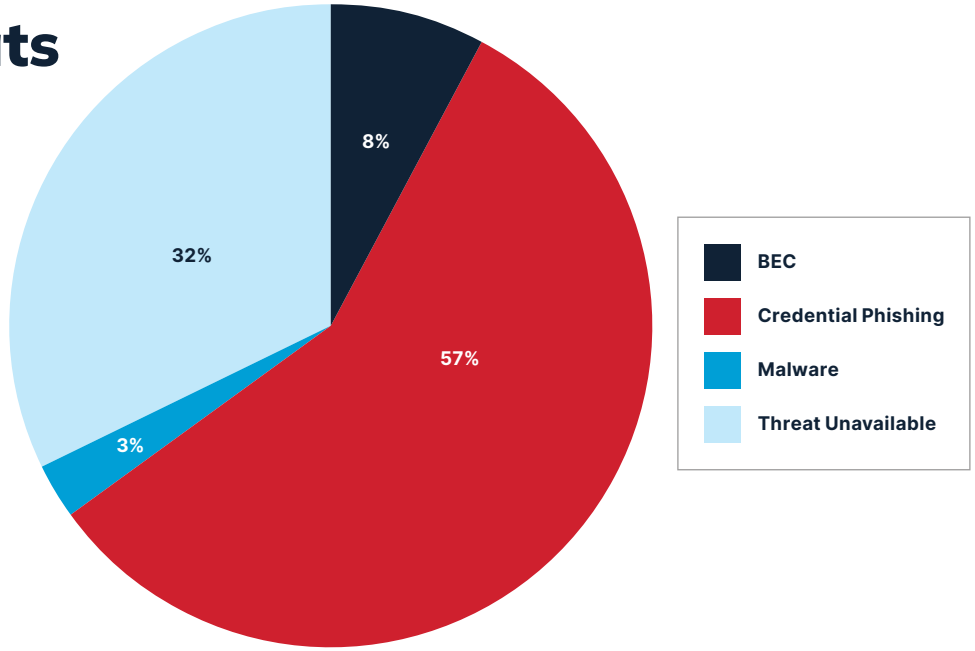
that Bypassed SEGs by Industry*



*This data is based on the percent change from 2022 to 2023 per Cofense customer, per industry.

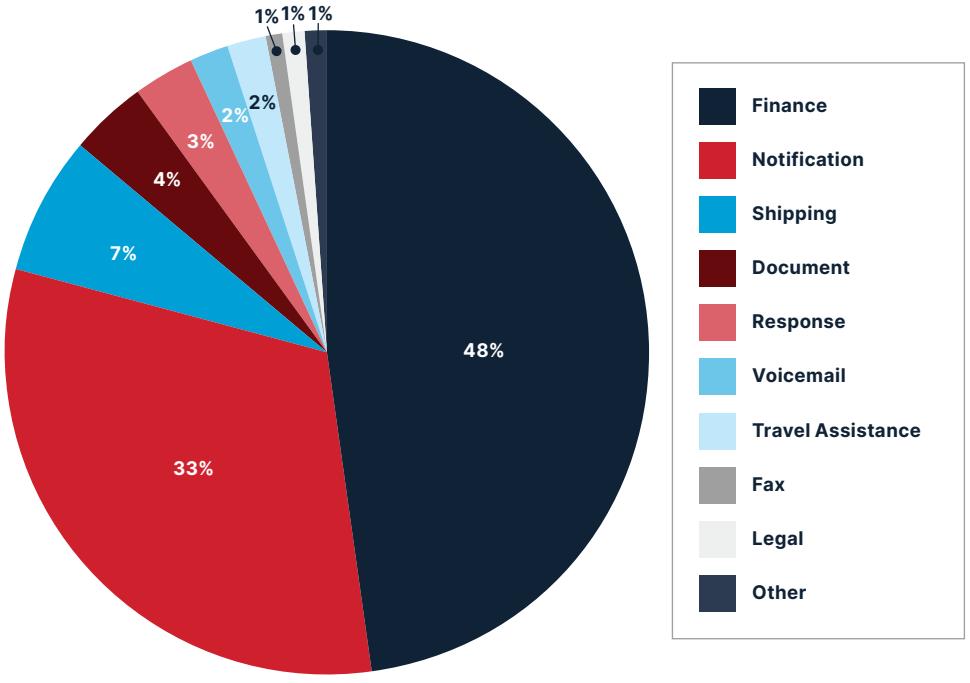
This year, credential phishing threats increased by 49% over 2022, which was already showing a large increase over 2021 data. In 2023, credential phishing was responsible for 91% of active threat reports (ATRs) published, with malware lagging significantly behind. Based on this data, we conclude that credential phishing was the threat of choice in 2023.

Malicious Threats Observed by PDC



The top themes in ATRs remain similar to last year, with finance themes and notifications securing the top two spots at 48% and 33% respectively. Cofense also saw a new theme, travel assistance, emerge. Travel assistance is a small contributor at 2% but one to watch going forward.

Top Themes in Active Threat Reports



ORGANIZATIONS CANNOT UNDERESTIMATE the power of simplicity when it comes to phishing attacks. While we often hear about highly advanced and devastating cyberattacks, the truth is that many of them start with basic phishing campaigns. These campaigns may seem unrelated to more sophisticated threats, but they can still serve as a gateway to serious breaches.

Top Email Security Trends to Watch

	**Credential Phishing Leads as Top Threat Vector Over the Last Year**
	**Use of QR Codes in Phishing Campaigns is Rapidly Increasing**
	**Threat Actors Lure Victims with Brand Impersonation and Vishing Campaigns**
	**Malware Tactics Continue to Evolve** Top Families to Watch Include: DarkGate and PikaBot, Emotet/Geodo, Agent Tesla, FormBook, Snake Keylogger
	**Google AMP** A New, Evasive Phishing Tactic
	**BEC** Costing Businesses Billions

Email Security Trends to Watch – The Details

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 revealed, here's a deep dive into the email security trends you need to stay on top of in 2024.

Credential Theft Phishing Leads as Top Threat Vector

As we look to the future of cyber threats, it's clear that credential phishing will remain a top concern. The Cofense team identified that 91% of active threat reports published in 2023 centered around credential phishing, a 67% increase in volume compared to the year prior.

This sophisticated form of attack often involves convincing individuals to give up their login information or other sensitive data, which can then be used to gain access to secure systems and networks.

Cofense reported a 67% increase in credential theft phishing volume over 2022.

Cofense Intelligence

Not only can credential phishing lead to devastating ransomware attacks and data breaches, but it can also pave the way for business email compromise (BEC) schemes that defraud companies out of millions of dollars. As we move into 2024 and beyond, organizations must take this threat seriously and work to implement robust security protocols that can protect against all forms of credential phishing like vishing, smishing, QR code phishing, and other dangerous cyber-attacks.

Use of QR Codes in Phishing Campaigns is Rapidly Increasing

QR codes in the phishing threat landscape are a major topic of interest and worth paying close attention to. QR codes change the attack vector and enable threat actors to trick victims into using their smartphones, which are typically not protected by enterprise controls and are therefore more vulnerable. Over the last year, Cofense reported a 331% increase in QR code ATRs issued.

As campaigns using QR codes grow in size and complexity, it is important to track not just the QR codes themselves, but also the context of the emails

> *"QR codes in the phishing threat landscape are a major topic of interest and worth paying close attention to."*

delivering the QR codes. Some of the emails bearing QR codes are delivered in attached files like HTM, PDFs, or Word documents. Others use images embedded in the email or QR codes rendered from external sources. The more recent QR code campaigns utilize a wide range of email themes rather than the earlier campaigns that primarily used multi-factor authentication as a lure for victims.

- When it comes to the URLs from the actual QR codes, there are many different characteristics, such as their purpose as a legitimate redirect, a link shortener, etc. or the fact that one of the redirect pages makes use of a Cloudflare CAPTCHA.
- The most common characteristics associated with URLs embedded in QR codes were CAPTCHA, multi-factor authentication (MFA), and URLs that had an open redirect to a credential phishing page.
- The most common sources of QR codes are either a code embedded in the email content or an attached .pdf, .htm, or .doc file.
- The subject of QR code emails was likely to be MFA themed, containing date and personally identifiable information that was redacted.
- The types of URL domains embedded in QR codes were malicious or compromised, legitimate, QR code related, and a standard link shortener service.
- Legitimate domains of URLs embedded in QR codes were Bing, Google, Baidu, and 5 other minor sources.

+331%

Cofense reported a 331% increase in QR Code Active Threat Reports (ATRs) issued.

Cofense Intelligence

Cofense was the first to alert the market about this growing threat early in 2023 and in Q4 2023, announced a first-of-its-kind solution that provides world-class security awareness training (SAT) and threat detection & response capabilities to specifically target QR code phishing threats.

Threat Actors Lure Victims with Brand Impersonation and Vishing Campaigns

Brand impersonation and vishing campaigns are techniques used by threat actors to deceive victims into clicking on malicious links or providing sensitive information. In brand impersonation attacks, cybercriminals use the name, logo, and other branding elements of a reputable company to trick victims into believing the communication is legitimate. Once they gain the trust of their victims, they exploit this relationship to carry out their malicious activities.

Vishing campaigns, on the other hand, often start with email but involve using voice calls or automated phone messages to manipulate victims into providing confidential information. The attackers may pose as representatives of a trusted organization or financial institution and use social engineering tactics to gain access to personal data such as login credentials or credit card numbers. Vishing attacks are becoming increasingly popular due to the ease of accessing personal information through phone numbers and the widespread use of smartphones.

Brand Impersonation: Cybercriminals use the name, logo, and other branding elements of a reputable company to trick victims into believing the communication is legitimate.

Vishing: Often start with email, and then voice calls or automated phone messages to manipulate victims into providing confidential information.

Cofense saw both of these tactics on the rise in 2023. Both vishing and brand impersonation tactics are very efficient at bypassing SEGs; they are often delivered without attachments or obvious links making it difficult for traditional file and text-based detection software to pick up on these forms of phishing. Additionally, because users interact with these tactics via non-traditional methods like personal smartphones and traditional telephones, these types of phishing take users outside the protections of their corporate environment and its security protocols.

We believe that the best way to secure your organization from these types of attacks is to implement a complete end-to-end email security solution. We recommend a holistic solution that combines Security Awareness Training and Threat Detection and Response to identify malicious threats quickly and stop them before they become detrimental to your company's data security while conditioning your employees to identify and report these types of malicious attacks. In 2023, Cofense introduced new simulation training to its SAT offering specifically focused on vishing and brand impersonation phishing tactics.

Malware Tactics Continue to Evolve – Top Families to Watch

Malware Characteristics					
Malware Family	**Information**	**Keylogging**	**Remote Access**	**Loader Capabilities**	**Backdoor Controls**
Emotet/Geodo	✓			✓	✓
FormBook	✓	✓			
Agent Tesla	✓	✓	✓		
Snake	✓	✓			
QakBot	✓	✓	✓	✓	✓
DarkGate	✓	✓	✓	✓	✓
PikaBot				✓	✓

MALWARE FAMILY DarkGate and PikaBot

A malware phishing campaign that began spreading DarkGate malware in September 2023 evolved to become one of the most advanced phishing campaigns active in the threat landscape. Since then, the campaign has evolved and is using evasive tactics and anti-analysis techniques to continue distributing DarkGate, and more recently, PikaBot malware.

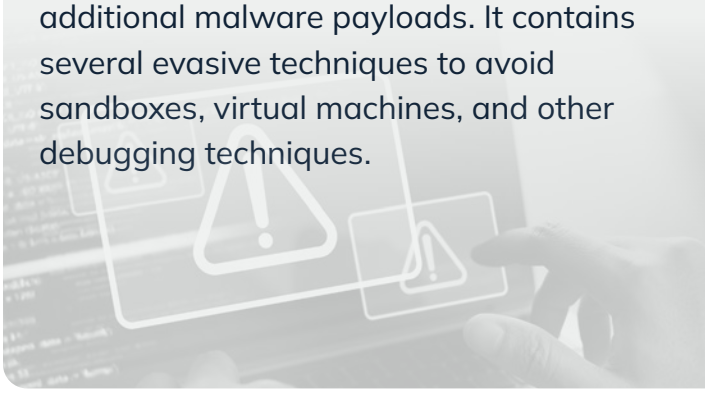
The campaign surged just one month after the last instance of QakBot activity and follows the same trends used by the infamous threat actors that deployed the QakBot malware and botnet. This campaign disseminates a high volume of emails to a wide range of industries, and due to the loader capabilities of the malware delivered, targets can be at risk of more sophisticated threats like reconnaissance malware and ransomware.

In August 2023, the FBI and the Justice Department announced they had disabled the QakBot infrastructure. Since then, QakBot has remained silent, with no significant activity seen from the malware infrastructure. While direct attribution between the QakBot threat actors and the new DarkGate campaign can be difficult, we can show the similarities between the two. At the time of this report, Cofense is watching this activity closely as there is a chance the threat actors are using this time to regroup and return even stronger in the future.

Starting with the timeline of the campaign, Cofense last reported on QakBot at the end of June, whereas DarkGate reports first emerged during July. The new campaign that is delivering DarkGate and PikaBot follows the same tactics that have been used in QakBot phishing campaigns. These include hijacked email threads as the initial infection, URLs with unique patterns that limit user access, and an infection chain nearly identical to what we have seen with QakBot delivery. The malware families used also follow suit to what we would expect QakBot affiliates to use. Along with many other capabilities, both malware families can act as loaders with the ability to add additional malicious payloads to unknown infected machines.

DarkGate was first seen in 2018 and is capable of cryptocurrency mining, credential theft, ransomware, and remote access.

PikaBot is a new malware family first seen in 2023. It is classified as a loader due to its ability to deliver additional malware payloads. It contains several evasive techniques to avoid sandboxes, virtual machines, and other debugging techniques.



Timeline of Qakbot and DarkGate/PikaBot Campaign*

*This data is based on Cofense Intelligence sightings.

The observed DarkGate/PikaBot campaign is a high-level threat due to the tactics, techniques, and procedures (TTPs) that enable the phishing emails to reach intended targets and the advanced capabilities of the malware being delivered.

During the campaign, Cofense identified several different infection chains, almost as if the threat actors were testing different malware delivery options. A favored infection chain to deliver the malware has been identified and follows in line with that seen in QakBot campaigns during May 2023.

The campaign began with a hijacked email thread to bait users into interacting with a URL that had added layers that limited access to the malicious payload only to users that met specific requirements set by the threat actors (location and internet browser). This URL downloaded a ZIP archive that contained a JS file(JSDropper, which is a JavaScript application used to reach out to another URL to download and run malware). At this stage, the user was successfully infected with either the DarkGate or PikaBot malware.

MALWARE FAMILY Emotet/Geodo

Emotet/Geodo may sound like names from a science fiction movie, but they represent one of the most destructive malware campaigns in recent years. This malware was first discovered in Europe in 2014, gained sophistication over time, and has spread across the globe, infecting countless computers and causing extensive damage to personal and professional networks.

The FBI opened its first related investigation in 2017. During their investigation, the FBI discovered that in some cases, malware was delivered as a banking trojan that recorded online banking credentials and then stole from victims' accounts. In other cases, Emotet allowed the installation of malware that enabled a ransomware attack.

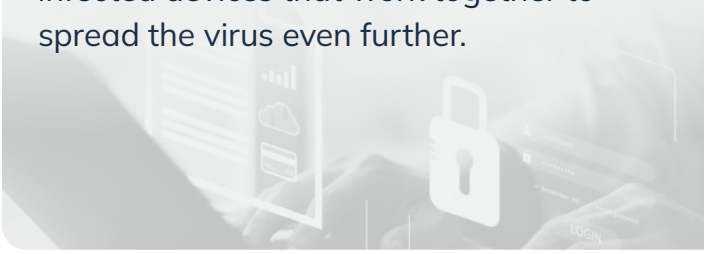
In 2021, law enforcement dismantled the foundational components of Emotet's operation. The unprecedented effort closed off access that had been maliciously opened on 1.6 million computers worldwide.

Emotet was hit hard but like any other malicious campaign the threat actors always seem to live to see another day. Long gaps in Emotet activity are common, often followed by surges of malicious email dissemination.

In 2023, Cofense researchers observed new activity in Emotet epochs 4 and 5. Emotet uses several botnets called epochs, each of which is assigned its own command and control (C2) infrastructure. In January, Cofense observed .dll file updates being sent to each epoch, almost certainly configuring bots to contact new infrastructure.

Emotet, which is often partnered with Geodo, is known for its ability to infiltrate and manipulate email accounts, tricking unsuspecting individuals into downloading infected files or clicking on malicious links.

Geodo, on the other hand, operates as a botnet, creating a network of infected devices that work together to spread the virus even further.



As predicted, after several months of inactivity, the Emotet botnet resumed email activity on March 7, 2023. The malicious emails seemed to be replying to already existing email chains, with the addition of an attached .zip file. The .zip files are not password protected and the themes of the attached files included finances and invoices.

Given its history of success, Emotet/Geodo poses a serious cybersecurity threat. We continue to encourage organizations to stay vigilant to avoid falling victim to this heinous threat.

MALWARE FAMILY Agent Tesla

The world of cybersecurity can be a daunting and complex place, especially when it comes to malware. One such malware is Agent Tesla, a keylogger written in .NET that can monitor keystrokes, take screenshots, steal passwords from a variety of applications, and exfiltrate this data back to the threat actor through common protocols, all while remaining undetected on the user's computer.

Agent Tesla first appeared in 2014 and has been a staple in the malware landscape ever since. This keylogger was originally advertised on a Turkish website as a remote access tool to monitor your personal computer. It could compile your passwords,

monitor your keystrokes, and avoid being caught by your endpoint's anti-virus. The Agent Tesla Keylogger executable is typically delivered via a direct attachment to an email. The chief exfiltration method over the past year remains SMTP but FTP, HTTP, Discord Webhooks, and Telegram are often seen as well.

Agent Tesla has gone through a variety of upgrades over the years. Besides changes intended to ensure that every new release can bypass anti-virus scans, it now advertises the ability to steal credentials from over 55 applications including web browsers, VPN applications, FTP applications, and mail clients. It also continues to improve its ability to circumvent or avoid sandbox technologies. While at first it only used SMTP to communicate back to the attacker, it now also supports communication over FTP, HTTP, Discord Webhooks, and Telegram.

Agent Tesla can steal credentials from over 55 applications including web browsers, VPN applications, FTP applications and mail clients. Cofense has seen phishing emails delivering Agent Tesla through both attachments and links bypassing the leading secure email gateways (SEGs).

Agent Tesla was originally sold as a remote access tool, and it could be argued that it functions no differently from legitimate remote access tools like GoToMyPC or LogMeIn. US prosecutors have successfully argued that someone selling and instructing users how to "install the product in ways that are arguably deceptive," has crossed the legal line and can be criminally prosecuted under computer misuse laws. Other remote access tools have been sold in this manner and the sellers have been prosecuted and sent to prison. Some developers explicitly included warnings to "only use the product in a legal way" in an attempt to avoid prosecution but this was not held up in court.

Cofense has seen phishing emails delivering Agent Tesla through both attachments and links bypassing the leading SEGs. However, Agent Tesla keylogger's behavior on an endpoint should typically be detectable by modern endpoint security suites and network activity monitors.

As cybercriminal techniques continue to evolve, it's important to stay informed and take the necessary steps to safeguard your organization against these persistent threats. Cofense can help; our Phishing Detection and Response (PDR) solution is uniquely positioned to help you stop threats like these.

MALWARE FAMILY FormBook

FormBook consistently places in the Top 5 malware families most commonly seen by Cofense. FormBook is an information-stealer type malware, primarily focused on accessing information about infected computers, as well as saved credentials or forms from browsers, applications, cryptocurrency wallets, and instant messaging platforms.

This malware is known to infect computer systems through malicious emails that trick unsuspecting users into opening it. Once installed, FormBook can steal sensitive information such as passwords, credit card details and browsing data without the victim's knowledge.

FormBook is primarily focused on accessing information about infected computers, as well as saved credentials or forms from browsers, applications, cryptocurrency wallets, and instant messaging platforms.

It first appeared for sale in early 2016, and more recently it was updated and rebranded as XLoader in late 2020. It's simple, easy to use, has many capabilities, and is highly popular in the market.

FormBook has infected millions of computers worldwide. Its use is often seen in cybercrimes such as identity theft, blackmailing, and financial fraud. As such, both individuals and businesses must take proactive steps to safeguard their systems against this threat.

MALWARE FAMILY **Snake Keylogger**

Snake Keylogger, a staple in the phishing threat landscape throughout 2021 and 2022, continues to pose a significant risk to individuals and organizations in 2023. Snake Keylogger, a particularly dangerous threat written in .NET, is designed to secretly monitor and record every keystroke on a computer, including usernames and passwords, scan applications to steal saved credentials and exfiltrate this data through a variety of protocols delivering it back to the hackers to use or sell on the dark web. What makes the Snake Keylogger so concerning is its ability to evade detection by antivirus software and remain undetected on a target system for long periods of time.

Snake Keylogger made its first appearance in November 2020 and can still be purchased today for anywhere from $25 to $500. Although it is not as popular as other malware families such as FormBook or Agent Tesla, it does maintain a significant presence and its usage is increasing.

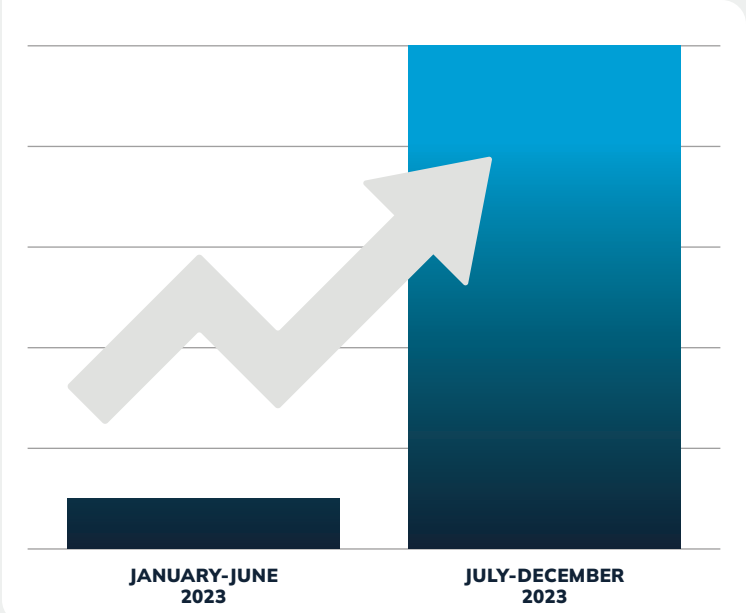
Snake Keylogger is designed to secretly monitor and record every keystroke on a computer.

Google AMP – A New, Evasive Phishing Tactic

A new phishing tactic utilizing Google Accelerated Mobile Pages (AMP) has hit the threat landscape and proven to be very successful at reaching intended targets. Google AMP is an open-source HTML framework used to build websites that are optimized for both browser and mobile use. The websites that we observed in these campaigns are hosted on Google.com or Google.co.uk, both of which are considered trusted domains to most users. This phishing campaign not only employs Google AMP URLs to evade security but also incorporates a multitude of other TTPs known to be successful at bypassing email security infrastructure.

Cofense observed a 1,092% increase in Google AMP emails bypassing SEGs in the last six months of 2023 compared to the first six months.

Cofense Phishing Defense Center (PDC)



BEC –
Costing Businesses Billions

Although business email compromise (BEC) did not make it on our list of top trends to watch, it's still a clear and present danger for organizations and worth mentioning. BEC remains one of the most devastating cybercrimes for the 8th consecutive year. With billions lost globally and victims in 90% of countries around the globe, we've seen scammers continue to exploit this type of crime with great success. While spam filters have transformed into malware detectors, they often fail to catch conversational-based phishing attacks, leading to billions of dollars being stolen year after year.

BEC is a subset of credential phishing but because of its popularity and successful track record, it is often talked about as a category of its own. By gaining access to an organization's email account, scammers can perform man-in-the-mailbox attacks. They create email forward rules to monitor all incoming and outgoing traffic. When they find an opportunity to redirect a transaction, they reply to the email thread with new information, often from a look-alike domain or compromised infrastructure. By modifying invoices with new account details, scammers successfully reroute funds, making it difficult to reverse the transactions.

Two-factor authentication (2FA) is a recommended defense against these attacks. However, scammers have found a way to bypass 2FA through an adversary-in-the-middle technique, gaining access to users' accounts by hijacking session cookies.

Another technique still flying under the radar is payroll diversion scams. Targeting human resources departments, threat actors manipulate financial records to redirect employees' direct deposits. These attacks often go unreported and unnoticed, allowing scammers to continue their fraudulent activities.

Traditional defenses are no longer enough to protect against BEC attacks. Organizations must stay vigilant and implement robust security measures to safeguard their finances and sensitive information.

FBI data identifies $51 billion in exposed losses due to business email compromise.

FBI

$51 billion

COFENSE
EMAIL SECURITY

Press Inquiries
TJ Scholl, Director of Communications
tj.scholl@cofense.com

Cofense® is the original and leading provider of security awareness training and phishing simulation, offering global enterprise-level advanced email threat detection and remediation solutions. Cofense PhishMe® and Cofense Phishing Detection and Response (PDR) offer the world's only platforms to leverage over 35 million Cofense-trained employees who actively report suspected phishing and other dangerous email threats in real-time. Exclusive only to Cofense, this reporting system ingests and catalogs thousands of threats per day that are missed by current email gateway technologies and then eradicates those threats from customer inboxes. In short, Cofense sees and stops threats other email security systems miss. Please visit www.cofense.com or connect with us on X and LinkedIn for additional information.