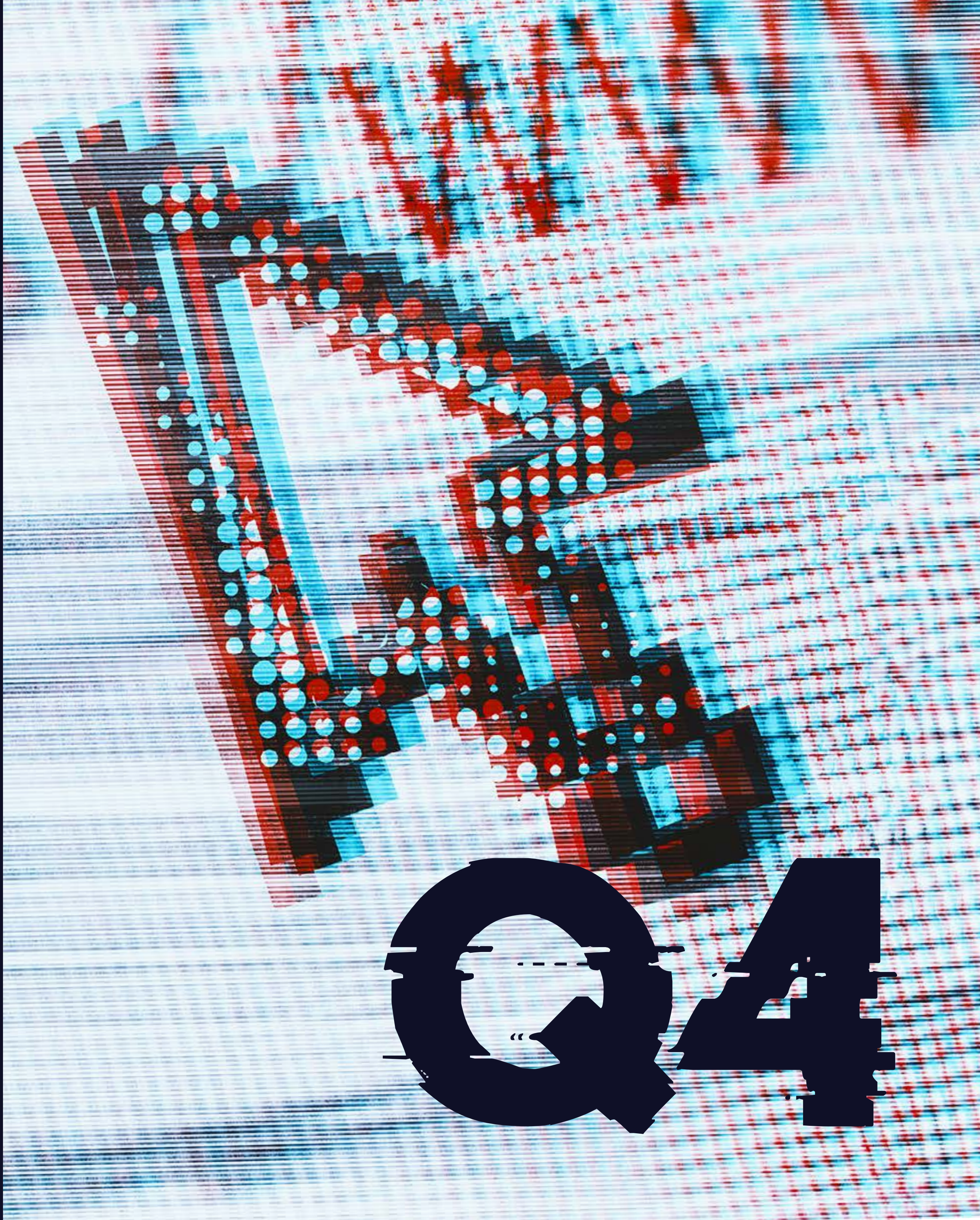
mimecast

Global Threat Intelligence Report

October-December 2023



INTRODUCTION

Too often, organizations receive threat intelligence as individual analyses of specific incidents, giving security teams a narrow view of the threat landscape. In this Global Threat Intelligence Report, Mimecast aims to put the previous three months' worth of incidents into context and give companies the tools they need to understand where attackers are headed and where defenses could be improved.

Mimecast generates threat intelligence through its analysis of 1.7 billion emails per day on behalf of more than 42,000 customers. Because email is the channel through which most cyber threats launch, Mimecast sees many new threats before they become widely known.

+ 1.7 Bill	emails per day
42 000	customers

This report distills insights from the intelligence Mimecast generated throughout the fourth quarter of 2023 and combines it with external intelligence from the cybersecurity community at large. It includes an analysis of threat activity, a series of top-line statistics that shaped that activity, and recommendations for what small businesses and large enterprises alike can do to mitigate the risk those threats pose.

We invite you to explore our Q4 2023 threat intelligence report. We look forward to sharing more insights in the future.

EXECUTIVE SUMMARY

The fourth quarter of 2023 saw attackers continuing to shift their delivery methods toward using links for initial payloads, slowly moving away from sending malware as email attachments. In addition, threat actors are increasingly using QR codes to get around defenses designed to block malicious links and obfuscate their attacks.

Following attacks on major casinos earlier in the year, attackers continued to focus on travel, hospitality, and catering companies in Q4 2023, resulting in the sector becoming the second most targeted industry for the quarter, surpassed only by attackers' efforts against the banking sector. While campaigns directed at human resources and recruitment services have subsided somewhat, the sector remains the third most targeted.

Mimecast Threat Intelligence team

Mimecast's threat intelligence team is comprised of a globally distributed set of engineers, scientists, analysts, and threat researchers that aid the Mimecast Security Operations Center (MSOC). Threats are continuously monitored across more than 1.7 billion emails per day. Mimecast's cybersecurity experts reverse-engineer attack tools, investigate attacks, and test the efficacy of indicators of compromise to quickly develop threat intelligence and protections across its solutions.

KEY FINDINGS

Sectors

The sectors that experienced the most attacks in the fourth quarter of 2023 were financial institutions; travel, hospitality, and catering; and human resources and recruitment services. These attacks were driven by ransomware, data theft, and business email compromise (BEC). Additionally, across all industries, average users at small and medium-sized firms encountered more than twice the number of threats as those at large companies.

Links vs. Attachments

For the first time, the average user was more likely to encounter a malicious link than a malicious attachment in Q4 2023. In the past, attackers were more likely to use known malware to deliver payloads.

Geopolitics

Geopolitical tensions have increased, leading to more cyberattacks with more than 100 hacker groups claiming participation in the Israel-Gaza conflict alone. Nation-states are using cyber operations to gather intelligence on rival governments and attack critical infrastructure and information systems.

Generative AI

Attackers are using generative AI and machine-learning models to create more convincing phishing lures and translate attacks into other languages. Technical threat indicators, such as domain reputation, browser isolation, and malware analysis, will be increasingly necessary to block attacks.

QR Codes

A surge in using QR codes to obfuscate links has continued, serving the same purpose as URL shortening schemes but with an additional benefit to attackers, as victims have already become acclimated to snapping pictures of QR codes.

EXTORTION CAMPAIGNS GROW, CYBERATTACKS FOLLOW GEOPOLITICS

Ransomware and breach-for-ransom campaigns continued to grow in Q4 2023, with one of the larger groups, ALPHV Blackcat, compromising more than 1,000 victims with ransomware and data extortion and reaping more than $300 million in ransom payments by the end of the quarter.

Attack strategies have evolved from crypto-ransomware (where attackers encrypt data and hold the decryption key) to breach-for-ransom campaigns (where attackers steal sensitive data and threaten to release the sensitive information unless paid) to double- and triple-extortion strategies (where attackers combine tactics for more direct consequences).

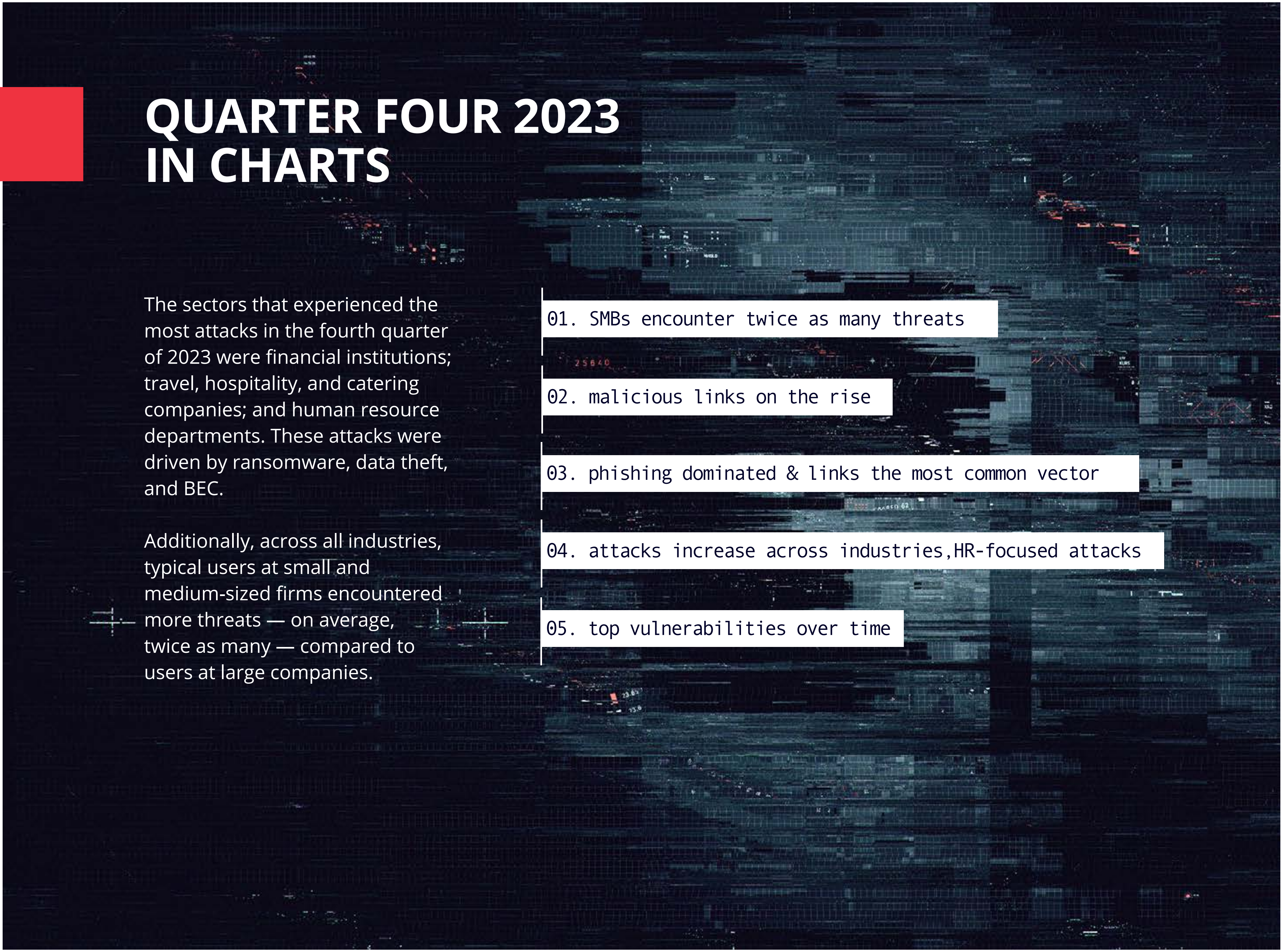
Ransomware and information-stealing groups have started using more sophisticated techniques, such as stealing tokens and account identifiers from Google Chrome. These successful tactics have led to a consolidation of the number of ransomware tools — with 43 malware families used for extortion in 2023, down from 95 in 2022 — signaling that cybercriminals and their affiliates are settling on a known set of popular platforms. Four groups — LockBit, Cl0p, ALPHV/BlackCat, and Play — dominated the ransomware landscape during the quarter, accounting for 88% of all ransomware activity.

However, while ransomware and data-breach incidents increased in 2023, companies are resisting extortion attacks. Ransom payment rates have plummeted, hitting a low of 34% in Q2 2023, down from 85% at the beginning of 2019. (The rate that companies acquiesced to ransom demands ticked up slightly in Q3 2023.) Three shifts in business security operations and the economics of ransomware are likely driving the change: Companies are less trusting of cybercriminals' ability to recover data; organizations have had time to (slowly) improve their security posture; and paying ransoms to threat actors from certain nation-states now violates federal laws.

Ransomware groups are aiming to reverse the trend. Starting on Oct. 1, the LockBit ransomware group put in place new rules regarding negotiations with victims, warning its "affiliates" that offering large discounts on ransom fees is no longer acceptable.

The geopolitical situation deteriorated with the Oct. 7 terrorist attack on Israel by the militant group Hamas. Like other global conflicts, such as Russia's invasion of Ukraine, cyberattacks have increased significantly as nation-state cyber operations, groups linked to either side, and hacktivist supporters ramped up their attacks against web sites, critical infrastructure, and computer systems. At least 90 pro-Palestinian threat actors and 23 pro-Israeli threat actors conducted attacks in Q4 2023.

There are already some signs that machine-learning models and generative AI are changing the threat landscape as well. For example, phishing lures are becoming much more convincing and easier to tailor to specific geographies because of the adoption of generative AI by threat actors, according to Mimecast's threat intelligence team. In addition, researchers have been able to upload malicious code to GitHub linked to machine-learning components, such as PyTorch, like attacks on other open-source supply chain components.



QUARTER FOUR 2023 IN CHARTS

The sectors that experienced the most attacks in the fourth quarter of 2023 were financial institutions; travel, hospitality, and catering companies; and human resource departments. These attacks were driven by ransomware, data theft, and BEC.

Additionally, across all industries, typical users at small and medium-sized firms encountered more threats — on average, twice as many — compared to users at large companies.

01. SMBs encounter twice as many threats

02. malicious links on the rise

03. phishing dominated & links the most common vector

04. attacks increase across industries,HR-focused attacks

05. top vulnerabilities over time

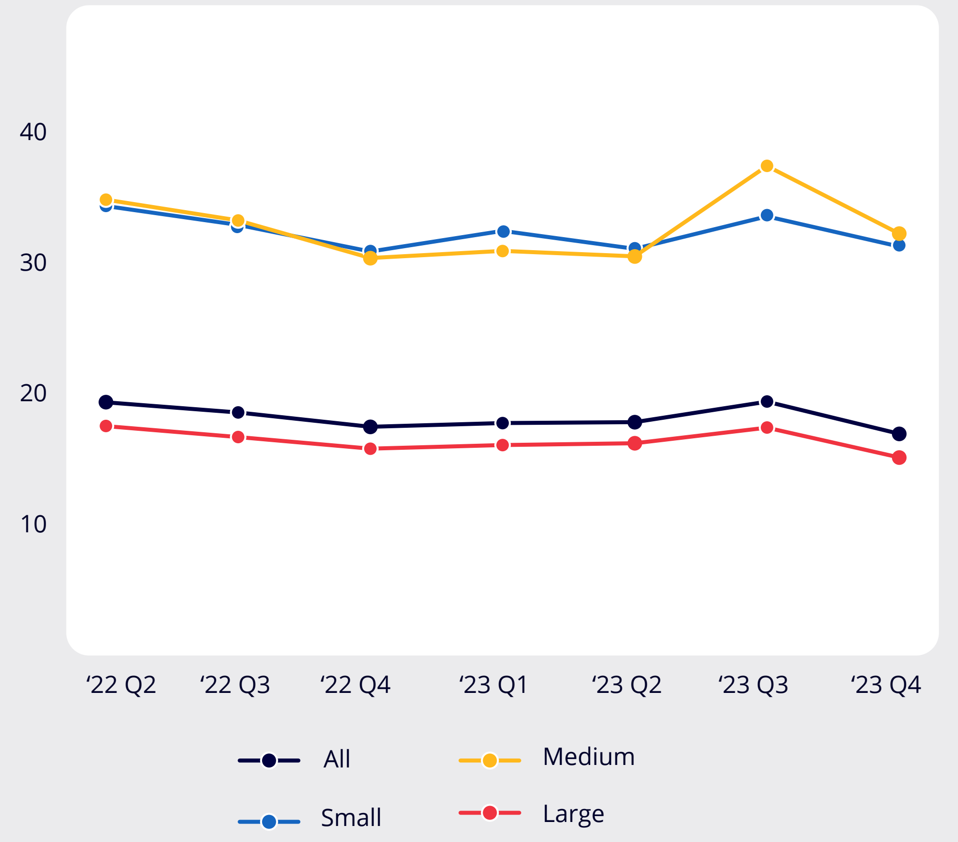
Encounter rates: SMBs encounter twice as many threats

The significant uptick in threats seen in Q3 seems to have subsided, but medium-sized companies still saw slightly more threats per user (TPU) than smaller firms in Q4. Average users at small and medium-sized businesses (SMBs) encountered more than twice the number of threats — 31 and 32 TPU, respectively — than users at large companies, who saw about 15 TPU in Q4.

The larger risk for SMBs is due to a greater share of employees in critical roles; targeting those users results in a higher level of threats per user. In addition, because SMBs rely on credential-based cloud services for much of their operations, attackers are more focused on credential theft, a common phishing goal.

The fourth quarter of each year tends to see a lower volume of threats, compared to the preceding quarter, so the drop in TPU across all organizations is common.

Figure 1. Threats per user by company size



2 Encounter rates: malicious links on the rise

Spam and impersonation both declined in Q4 2023 but continued to dominate malicious activity directed at users' email inboxes, with Mimecast defenses blocking 9.5 and 6.3 emails classified as either spam or impersonation, respectively, per average user. The unknown malware category, which Mimecast blocks based on detecting exploit code in attachments, is too small to be visible on the first chart.

By removing the two largest categories of threats — spam and impersonation — another trend becomes evident. In Q4, for the first time, the average user was more likely to encounter a malicious link than a malicious attachment. With users ignoring the overwhelming volume of email messages blocked as either spam or impersonation (phishing), attackers are clearly shifting from delivering payloads as malware to sending links to malicious sites, which then deliver the payload.

Figure 2a. Threats per user by type of threat

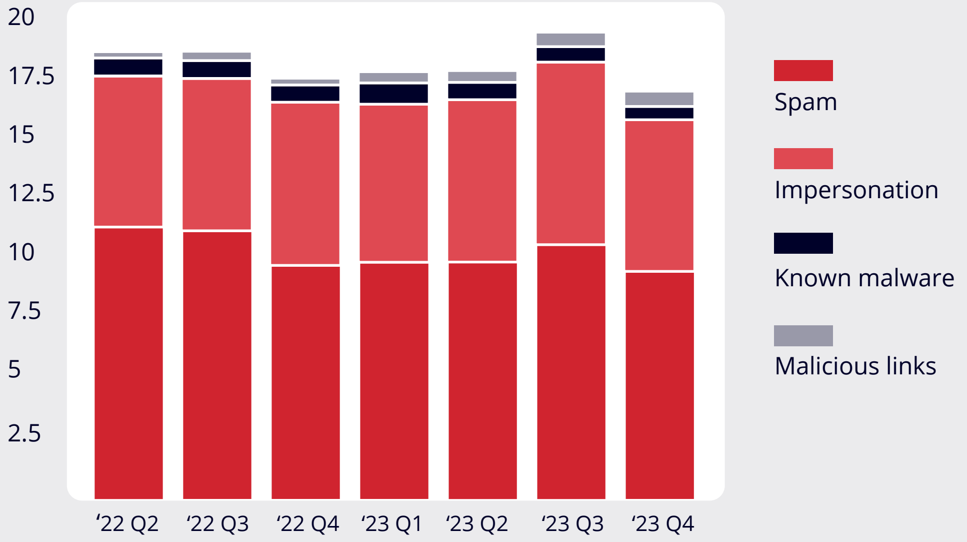
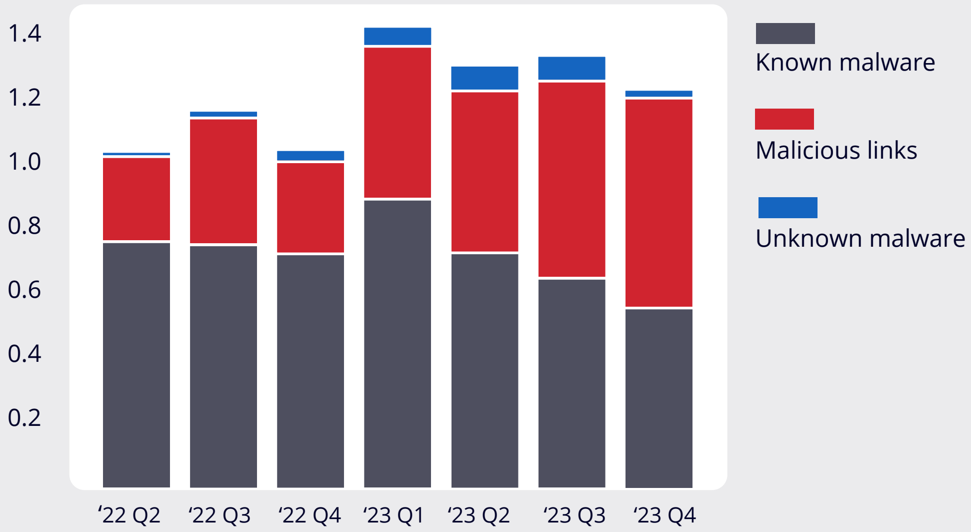


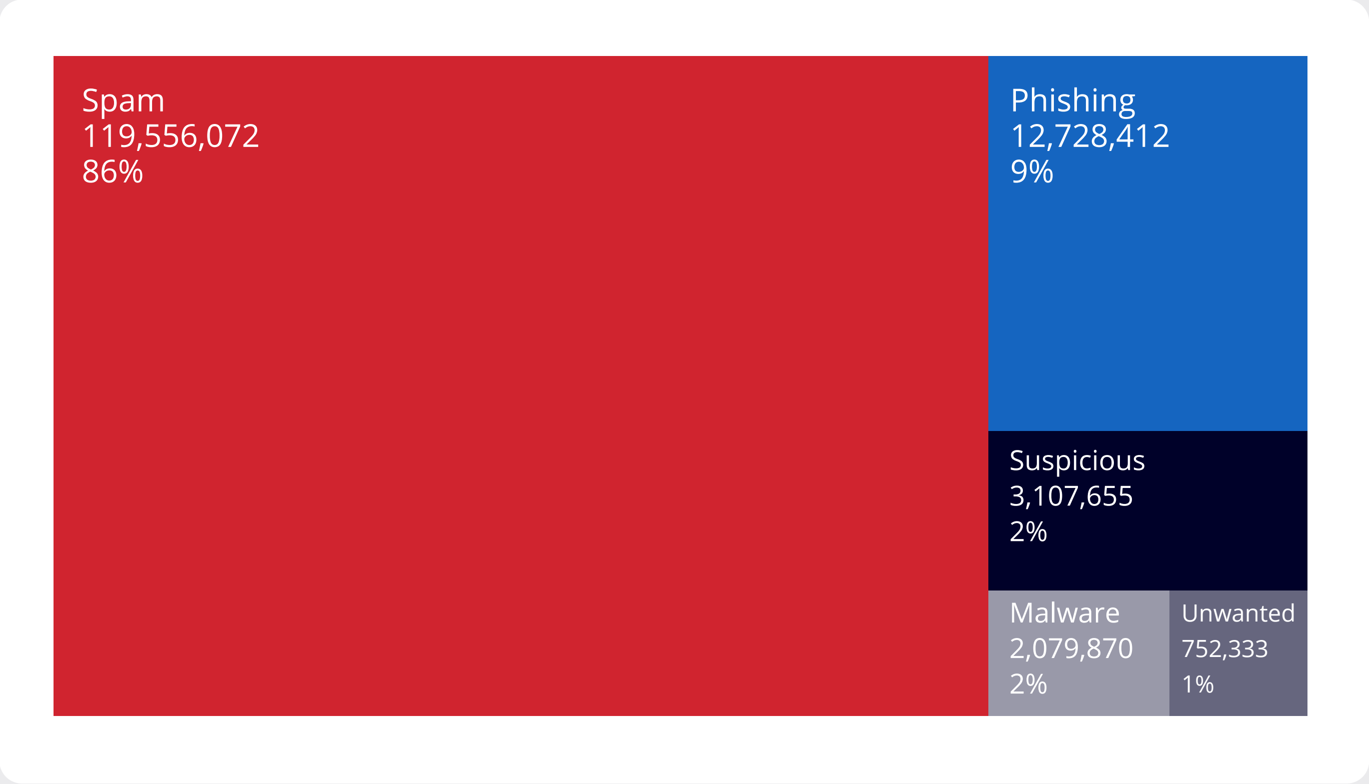
Figure 2b. Threats per user for malware & malicious links



3 Threat types: phishing dominated active threats, with links the most common vector

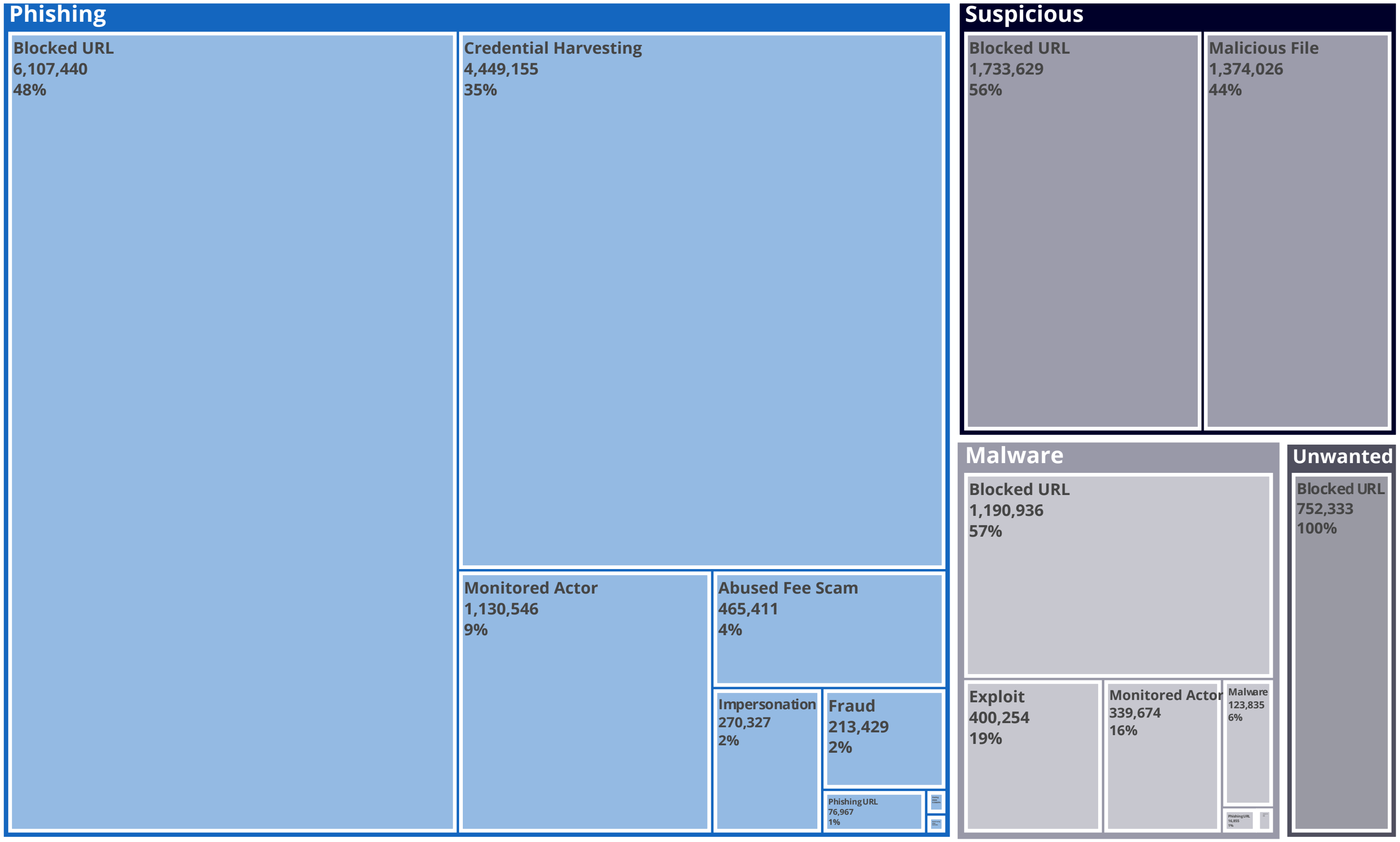
While spam continues to account for the largest volume of malicious and suspicious email messages rejected, accounting for 86% of all blocked messages (see Figure 3(a)), looking at the top threats apart from spam highlights interesting trends (see Figure 3(b)).

Figure 3a. Relative volume of all threats



Malicious URLs continue to make up the largest portion of all major detection types, including phishing, malware, and suspicious and unwanted emails. Credential harvesting is the second most identified attribute of phishing attacks, underscoring the importance of strong credentials — and hardening them with multifactor authentication — to protect businesses as they increasingly adopt cloud services and infrastructure.

Figure 3b. Malware and malicious links

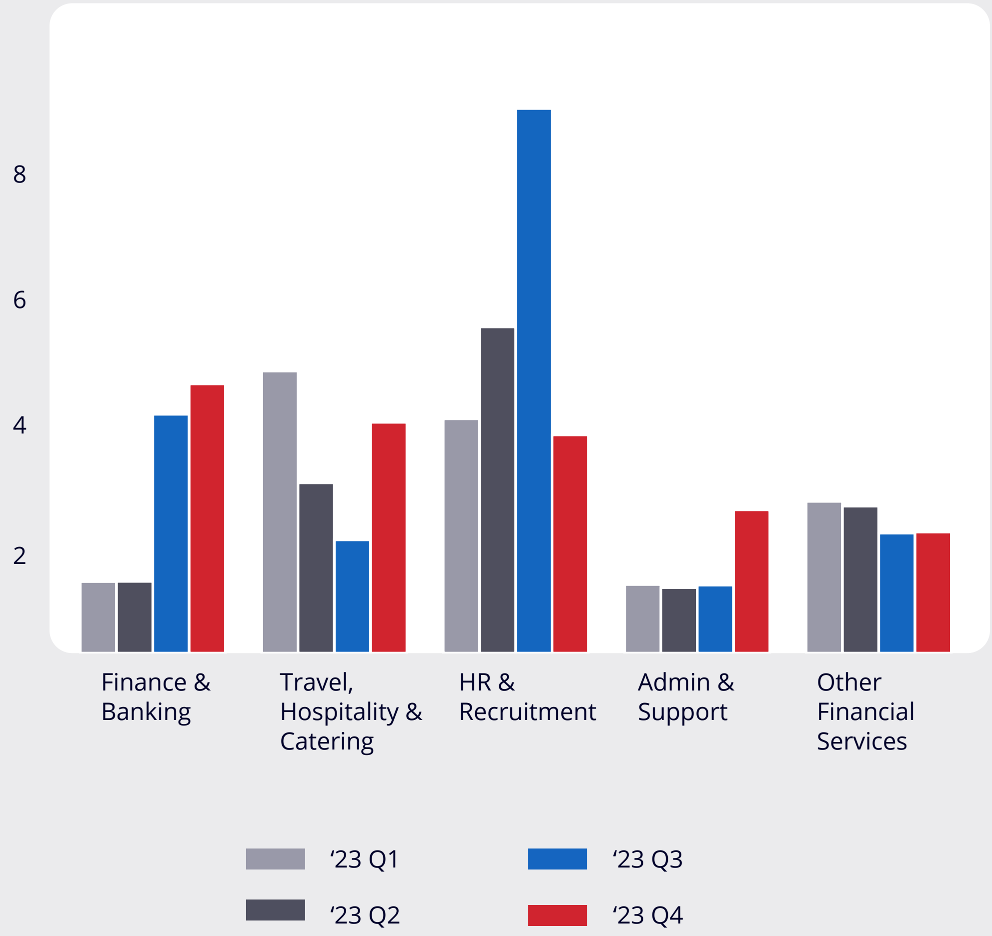


Industry snapshot: attacks increase across industries, while HR-focused attacks subside

The average number of attacks, excluding spam and impersonation, fell in Q4 2023, with users in the formerly most attacked sector — human resources and recruitment services — encountering 60% fewer threats than in the previous quarter, causing that sector to drop to third place in Q4 2023. Meanwhile, the IT software and software as-a-service sector dropped out of the top five most targeted sectors, falling all the way to No. 20 in Q4 2023.

However, the remaining sectors all saw increases in the most significant threats, which include known malware, malicious links, and unknown malware, over the prior quarter. Users in the banking sector continued to encounter a significant number of attacks, as did users in the travel, hospitality, and catering industry, which includes casinos. The average user across all industries encountered 1.2 threats during the quarter, slightly less than the average of 1.3 threats per user in Q3 2023.

Figure 4. Top 5 threats per user by Industry for malware & malicious links



5 Vulnerability snapshot: top vulnerabilities over time

The total number of vulnerabilities decreased over the quarter, which is a typical pattern for the fourth quarter as businesses close and both attackers and victims take a break at the end of the year.

The top-5 vulnerabilities showed distinct usage patterns. The most common vulnerability used in malware — a remote code execution flaw in the Equation Editor in Microsoft Office 2007 through 2016 (CVE-2018-0802) — was the workhorse of attackers in Q4 2023. Another attack exploiting a memory corruption vulnerability in Microsoft Office (CVE-2017-11882) saw minimal use until a spike in the third week of November corresponding with the most popular shopping days of the year.

Only a single vulnerability in the top-5 list — and only two in the top-10 list — were from 2023, highlighting the notion that attackers tend to prefer exploiting what they deem to be the most vulnerable software, even if the exploited flaw tends to be old.

Figure 5a. Total vulnerabilities blocked in Q4 2023

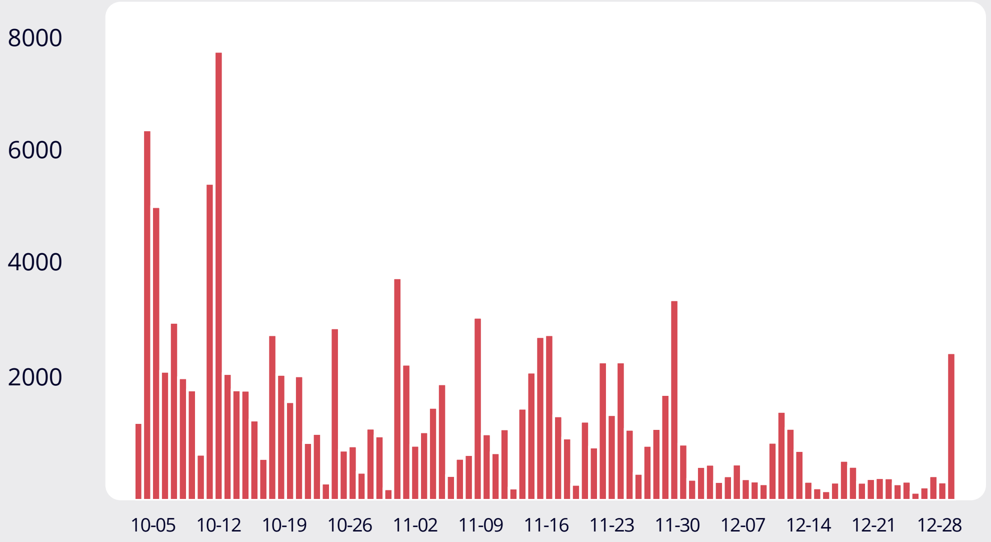
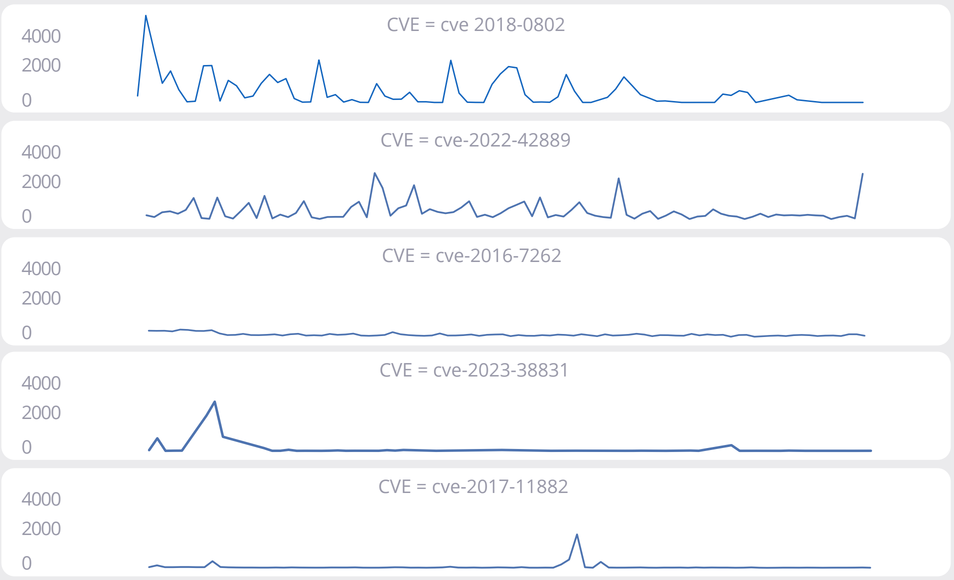


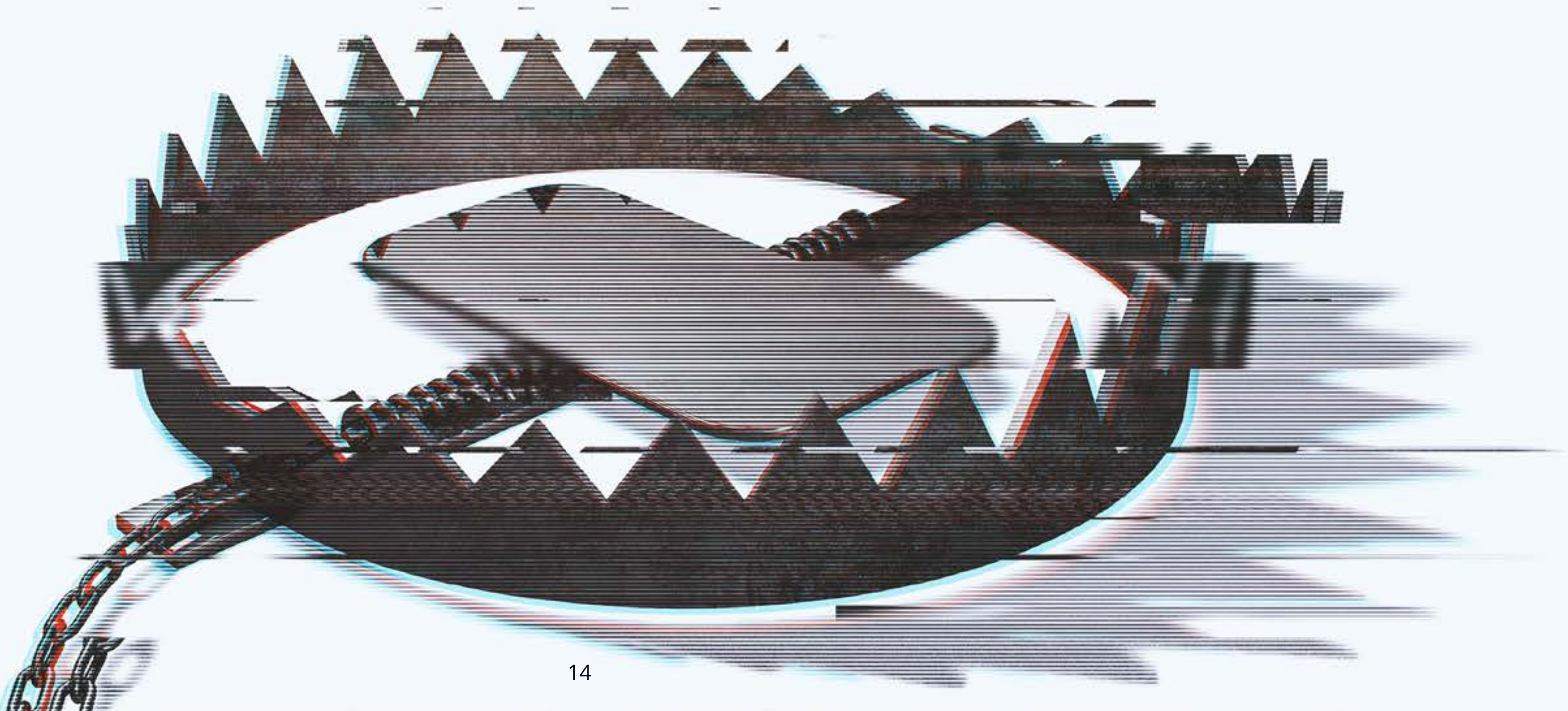
Figure 5b. Top 5 vulnerability detections for Q4 2023



BRAND ABUSE BECOMES MORE CONVINCING

Almost every type of email attack uses legitimate brands to gain trust and convince users to take actions that undermine their security, such as parting with sensitive information or clicking on links. During Q4 2023, for example, one threat actor used SendGrid's email marketing service to send out email campaigns that impersonated human resource departments and asked targeted users to click on a link that appeared to be from a Microsoft SharePoint Online server.

As attackers increasingly use generative AI to create official-sounding notifications and abuse legitimate services to bypass reputation-focused defenses, brand abuse will only become more problematic.

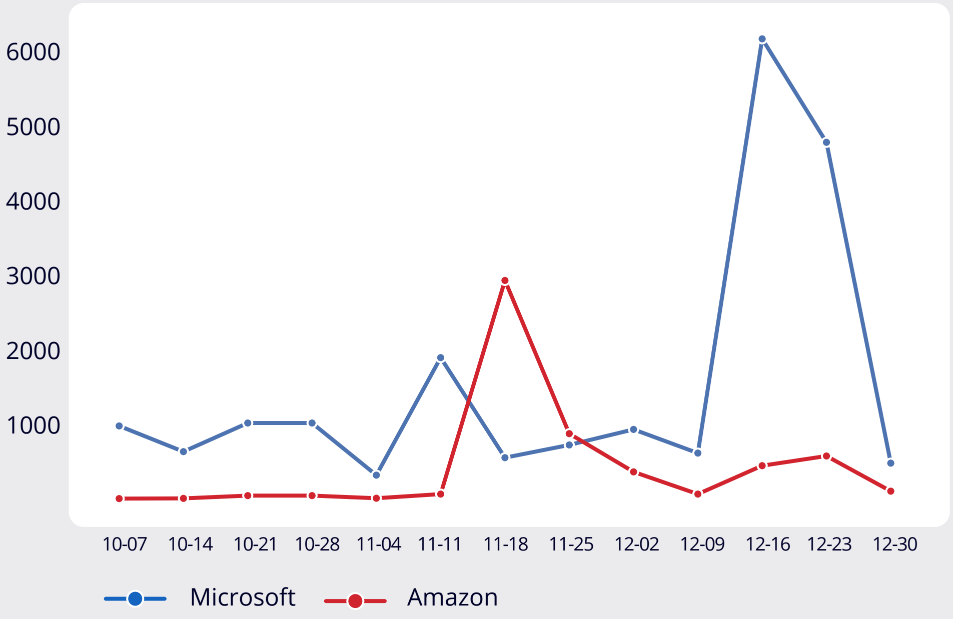


Attackers use different brands depending on context

The perennial impersonated brand is Microsoft, as data from our Q3 2023 report demonstrated. However, specific events may result in attackers using other brands to attempt to gain trust. In 2020, during the coronavirus pandemic, for example, Amazon, Apple, and the Social Security Administration were the top-three most impersonated brands.

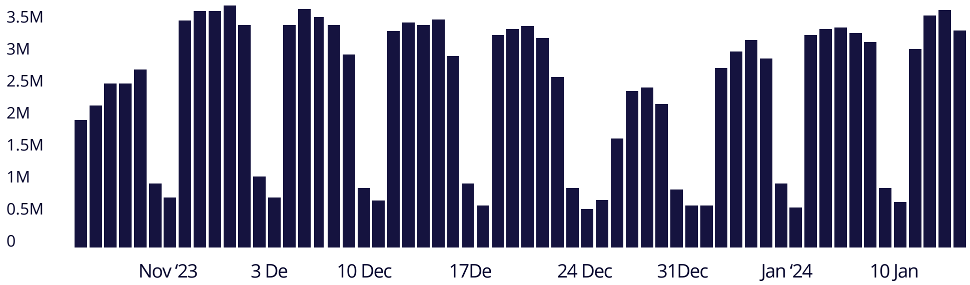
In Q4, attackers again switched up their brand-impersonation tactics. Looking to capitalize on the holiday shopping season, fraudsters ramped up their impersonation of Amazon, leading to a spike of spam and phishing detections for the brand. During the two weeks before Black Friday, considered to be the start of the holiday shopping season in the United States, Mimecast detected more Amazon-branded threats than Microsoft-branded threats.

Figure 6. Attackers switch focus to Amazon prior to holiday shopping



Meanwhile, attackers are using QR codes to obfuscate the destination of a link, while also relying on branding to convince users that QR codes are from official sources. This has moved from a niche attach methodology to mainstream as seen with emails that contain QR codes exceeding 3.5 million per day regularly (see figure 7). Mimecast has documented two major campaigns using QR codes — one branded as Microsoft password reset and the other as DocuSign.

Figure 7. QR Code detection over 60 days

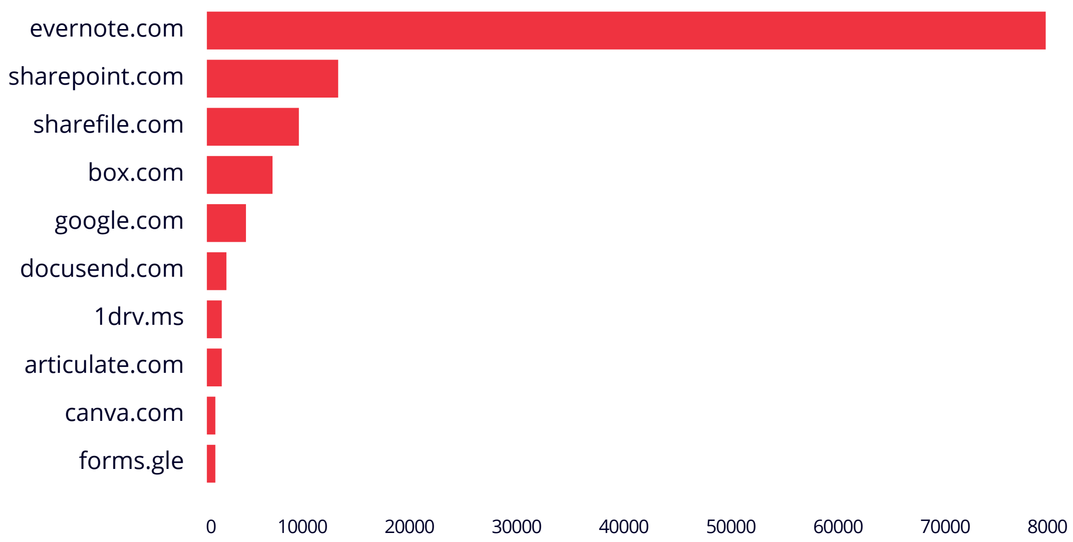


File-share abuse is about brands

Attackers increasingly are using links rather than attachments for payloads — whether the payload is a phishing site for stealing credentials or malware for the victim to download. To escape detection by security solutions and garner users' trust, attackers are widely using file-sharing sites that have trusted brands to serve up malicious content (see figure 8).

The top brand for file-sharing sites for the past three quarters is the notetaking and sharing service Evernote. Microsoft SharePoint comes in a distant second, while ShareFile managed storage service follows in third place.

Figure 8. Evernote tops popular domains for phishing attacks



THREAT ASSESSMENT

Attackers have doubled down on techniques for bypassing multifactor authentication (MFA) mechanisms. EvilProxy, a phishing-as-a-service (PhaaS) platform, targeted the financial and insurance industries with an attack that uses a proxy to bypass MFA, while another group used the DadSec PhaaS platform to send victims to a proxy that acts as an adversary-in-the-middle (AitM) to capture MFA requests and compromise victims' Microsoft 365 accounts.

Ransomware operators have continued to increase their focus on energy companies in Q4. Initial access brokers (IABs) actively sought out credentials and compromised systems within the networks of energy operators.

Nation-state cyber conflicts heated up following the terrorist attack by Hamas on Israeli civilians and Israel's military response and invasion of Gaza. Added to the online operations that continue as part of the Russian-Ukraine conflict, state-sponsored cyberattacks have become more common.

MAJOR EVENTS Q4

1 Oct

Phishing Attacks Continue Against Hospitality Sector

Attackers targeted the hospitality sector with sophisticated phishing attacks, leading to breaches such as those of MGM and Caesars. Mimecast data shows the hospitality sector was the No. 2 target in Q4.

READ ARTICLE

3 Oct

EvilProxy Phishing Attack Targets U.S. Firms

Researchers describe an attack using emails disguised as notifications from job board Indeed.com that had a redirection vulnerability. The attack was launched through PHaaS platform EvilProxy and targeted executives in the banking and insurance industries.

READ ARTICLE

9 Oct

Hacktivists Race into Israel-Hamas War on Both Side

Dozens, and more likely hundreds, of sites and networks came under attack as cyber operations ramped up following Hamas' terrorist attack on Israel and Israel's subsequent military response. The International Committee of the Red Cross released rules of engagement for civilian hackers to minimize harm to civilians during the war.

READ ARTICLE

17 Oct

Attackers Combine DadSec Phishing, Cloudflare

In what has become a typical combination to bypass two-factor authentication, an AitM phishing attack used fake emails containing a link, Cloudflare's Turnstile tool for human verification, and a fake Microsoft 365 site to convince users to part with their log-in credentials and their two-factor codes.

READ ARTICLE

18 Oct

State-Sponsored Actors Target WinRAR Flw

The Russia-linked threat actor Sandworm, also known as FrozenBarents and Black Energy, impersonated a Ukrainian drone warfare training school and sent out a malicious ZIP file exploiting a vulnerability in the WinRAR archiving utility.

READ ARTICLE

6 Nov

Iranian Group Targeting Israeli Sectors

The Iran-linked group Agonizing Serpens continued a campaign of data-theft and wiping attacks aimed at Israel's higher education and technology sectors. The attacks are not related to ransom but aim to cause massive data loss.

READ ARTICLE

12 Nov

Energy Sector Faces Increasing Attacks During Winter

IABs are actively seeking out stolen credentials and other methods of compromising energy networks. Reported ransomware attacks on the energy sector increased through the latter part of 2023, especially in North America, Asia, and the European Union (EU).

READ ARTICLE

29 Nov

Financial Service Phishing Delivers LUMMA Malware

Phishing emails using fake invoices led to a malicious site that redirects users to a JavaScript file that installs the information stealing LUMMA malware.

READ ARTICLE

6 Dec

ChatGPT Protections can be Bypassed to Create Phishing Email

The BBC used the paid version of ChatGPT and prompt engineering to create a private bot dubbed Crafty Emails that performed nearly all the malicious phishing tasks requested by the news service. The service created variations of popular scams, such as the "Hi Mum" scheme asking for money from a parent and spear-phishing emails. The bot made creating culturally distinct versions easy as well.

READ ARTICLE

19 Dec

Law Enforcement Shutter ALPHV Site

The data-leak and negotiation sites for the ALPHV/BlackCat ransomware gang disappeared from the Internet, following reported action by law enforcement. The U.S. Department of Justice claimed to have shut down the sites and offered 500 victims a decryption tool, but the group later reportedly recovered access to the sites.

READ ARTICLE

TOP THREAT CAMPAIGNS Q4

Each quarter, we select a subset of the threats to analyze in this report. Some campaigns have significant volume, which is apparent from the sparklines (see below) showing the number of threats detected during the quarter, while others show interesting attack techniques or targeting.

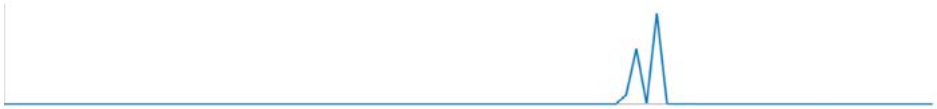
Microsoft QR codes

Since the pandemic, QR codes have become extremely popular, and Mimecast regularly blocks campaigns using the next-generation barcode to obfuscate links. Consumers and workers are increasingly becoming accustomed to QR codes, whether to access a digital menu at a restaurant, collect details about an event, or install new software at the click of a link. As a result, users' suspicion of obfuscated links has declined, making them more likely to scan the codes bypassing organizational security.

During Q4, Mimecast encountered a phishing attempt that impersonates a company requesting that the targeted victim set up Microsoft authentication. Because the content of the email is an image — and there is nothing for the user to click on — many security solutions will not catch the attack. When scanned, the link behind the QR code will send the user to a page that attempts to phish their Microsoft Office 365 credentials.

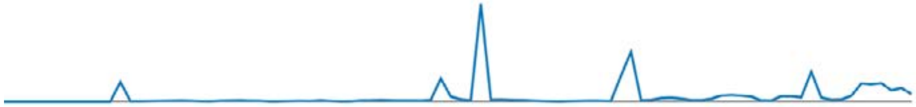
DocuSign QR codes

Attackers don't just favor QR codes for Microsoft-branded phishing; they happily abuse other infrastructure as well. Mimecast encountered a campaign in Q4 that focuses on the secure document sharing service DocuSign. The campaign disguises a malicious link as a QR code purportedly leading to document shared from a payroll department.



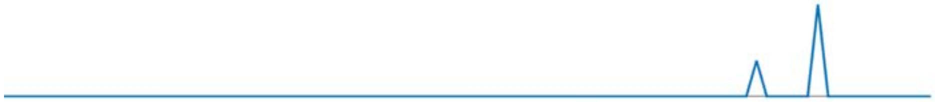
Google App Script attacks

Attackers conducted several campaigns using Google App Script, a rapid application development platform designed to create business applications for integration into Google Workspace. Based on JavaScript, Google App Script can access data from Google's Gmail, calendar, and personal storage spaces. Attackers have abused the technology through software vulnerabilities to create phishing pages, using the linked applications to deliver malware.



Mexico Bank fraud spam campaign

A banking fraud group created a significant URL-based campaign in December primarily targeting Latin American countries, especially Mexico. The group uses modest spam campaigns — consisting of 1,000 to 6,000 emails — sent from domains registered by the threat actor. Victims who click on the links included in the emails will download malware to their systems. Mimecast has identified two URL formats used by the group in its campaigns, which extend back to April 2023.



Meta Instagram impersonation

Another significant campaign impersonates Meta Instagram with a notification that appears to indicate a violation of copyright infringement. Initial versions of the alert aren't not convincing, as they contain grammatical mistakes and use a very informal tone. Attackers do, however, use legitimate cloud infrastructure services, such as Salesforce, to send the notifications, allowing the messages to bypass initial filters. The goal of the group behind the attacks is to allow attackers to bypass two-factor authentication and gain access to accounts.

TOP ADVISORIES

Government sources issued many advisories focused on enterprise security during the quarter, including warnings of the continued use of spear phishing by the Russian threat actor Star Blizzard and the increased use of insecure third parties to compromise targets.
In addition, the NSA and CISA compiled a list of ten common cybersecurity misconfigurations that could lead to a breach.

5 Oct [NSA/CISA] NSA and CISA Red and Blue Teams Share Top Ten Cybersecurity Misconfigurations

The National Security Agency (NSA) and Cybersecurity and Infrastructure Security Agency (CISA) published a top-10 list of the most common cybersecurity misconfigurations in large organizations, such as leaving applications in their default configuration and lack of network segmentation. For each misconfiguration, the agencies also listed attackers' most used tactics, techniques, and procedures.
REFERENCE

7 Nov [FBI] Ransomware Actors Continue to Gain Access through Third Parties and Legitimate System Tools

The attacks targeted third-party service providers and management tools to compromise targeted businesses, often in the gaming and hospitality sectors. Attacks on third-party gaming vendors targeted small and tribal casinos, while callback-phishing attacks led to data theft and ransomware installed on corporate systems.
REFERENCE

16 Nov [FBI/CISA] Data Theft and Extortion Targets Enterprises Through Third-Party IT Providers

The Federal Bureau of Investigation (FBI) and CISA released an analysis of the Scattered Spider group, which poses as IT help-desk staff and directs employees to run commercial remote access tools, bypassing multifactor authentication.
REFERENCE

7 Dec [NCSC/NSA/FBI/CISA/ACSC/CCCS] Russian FSB Cyber Actor Star Blizzard Continues Worldwide Spear-Phishing Campaigns

The Russia-linked group Star Blizzard has targeted a wide variety of organizations with spear-phishing attacks based on well-researched lures and social and professional contacts, with the end result typically the delivery of a malicious link. The group appears to mainly target organizations in the United States and the United Kingdom, but campaigns have also targeted organizations in NATO countries and nations neighboring Russia.
REFERENCE

19 Dec [CISA/FBI] #StopRansomware: ALPHV Blackcat

The FBI and CISA released a joint advisory describing the indicators of compromise (IoCs) for the latest ransomware released by the ALPHV/BlackCat group, ALPHV Blackcat Ransomware 2.0 Sphynx. As of September 2023, the group had compromised over 1,000 entities, of which three-quarters are in the United States and collected nearly $300 million in ransom payments.
REFERENCE

HOW TO TAKE ACTION

Cybercriminals and threat actors commonly target privileged roles, unpatched vulnerabilities, and insecure supply chains and third parties. Organizations should take steps to protect the most privileged users and find ways to slow down attackers.

Threat-specific countermeasures

General recommendations to combat threats

Steps specific to Mimecast customers

Threat-specific countermeasures

Threat-specific countermeasures

Protect sensitive positions

Attackers are broadly hitting specific business roles, therefore organizations should segment certain personnel from potentially malicious content, such as executables and scripts within documents. For example, Salespeople and executives shouldn’t receive or execute code, while IT administrators should be monitored using anomalous behavior detection.

Slow down attackers using segmentation and deception

Some attackers — specifically ransomware groups, such as Cl0p — are developing their own zero-day exploits to target previously unknown vulnerabilities. Network segmentation can cordon off sensitive parts of the network from attackers, while deceptive techniques, such as honeytokens, can both slow the attackers and alert defenders.

Develop a secure supply chain strategy

Attackers are increasingly targeting third parties and professional services as alternative pathways into targeted networks. Organizations should create minimum security requirements for their partners and service providers and find ways to measure compliance. It is also recommended that transactions be made through dedicated or authenticated systems, which builds user suspicion when requests for payment come in via email.

Educate users and block malicious QR codes

QR codes have taken off as attackers look to obfuscate their use of images to sneak links into spam, phishing, and other email-based attacks. In addition to preventing the loading of images by default*, organizations should educate their workers on the dangers posed by QR codes. Mimecast provides the ability to determine whether a QR code leads to malicious payload and block those that do.

Note: CyberGraph users should leverage trusted sites to ensure banners load correctly.

General recommendations to combat threat

Assess your attack surface areas

With many organizations moving to cloud services, the overall attack surface has grown. Companies should embrace a zero-trust approach to workers' access to company resources, requiring reauthentication when necessary and main strict visibility into all assets.

Minimize your attack surface by blocking unused services

If an organization doesn't use or expect to use certain web content hosts and websites, they should be blocked. For example, if Dropbox is not a corporate standard, it shouldn't be allowed. Similarly, if Excel documents should not be sent in email, controls must be put in place to prevent such actions.

Prioritize vulnerabilities for patching

Attackers continue to shrink the time between the disclosure of a vulnerability and the release of exploits and attacks targeting the identified security issues. The list of known exploited vulnerabilities (KEVs) maintained by the U.S. Cybersecurity and Infrastructure Security Agency (CISA) grew to 1,053 software flaws by the end of Q4 2023, but patching every issue in the KEV catalog isn't enough. Organizations should use different vulnerability metrics and their knowledge of critical systems to prioritize patching.

Make credentials resistant to phishing

Our data (see Figure 3) shows that phishing is the second most common attack type after spam, with attackers typically using the email attack to steal credentials from users. For that reason, organizations should focus on minimizing the impact of a successful phishing attack. Adopting an additional factor of authentication, especially phishing-resistant technology, can result in a significant reduction in credential-based attacks as part of a zero-trust approach to security. Organizations that add pervasive multifactor authentication to both their cloud and internal infrastructure will reduce their risk by an order of magnitude.

Steps specific to Mimecast customers

- It is recommended to utilize single sign-on from your identity provider or leverage Mimecast's built in multi-factor authentication to reduce an attacker's ability to leverage email as their attack vector. **LEARN MORE**
- Ensure DNS authentication policies honor DMARC records. A second policy scoped to a policy group with the DMARC Fail action set to Ignore/Managed and Permitted Senders will provide an effective bypass for any legitimate mail being rejected/quarantined for DMARC failures. **LEARN MORE**
- Optimize Impersonation Protection as per best practice guidelines of 2 hits set to tag Subject/Body and include a separate C-Level/VIP policy based on name match with a hold for admin review. In addition, create another policy for any detections of 3 hits or more with the admin hold action. **LEARN MORE**
- Setting an aggressive re-writing of URLs will ensure all URLs are scanned upon click but be aware that anything that looks like a URL will be re-written e.g., IP addresses and internal links. **LEARN MORE**
- Consider setting Auto-Allow policies to 'strict' instead of 'allow' to ensure that spam scanning is not bypassed at an organizational level for external email recipients. This should be set in conjunction with 'Auto Allow Spam Detection' to hold for review to ensure no potentially malicious messages bypass scanning. **LEARN MORE**
- Utilize pre-built integrations with the majority of SIEM and XDR vendors to provide log capture and analysis for security policy enforcement. **LEARN MORE**
- Leverage bring-your-own threat intelligence to take advantage of any third-party threat feeds for automatic rejection of matching indicators. **LEARN MORE**
- It is recommended to deploy end user tools to report potentially malicious messages to Mimecast SOC for additional analysis. **LEARN MORE**

If you are unsure of the effect of any of the proposed settings, please reach out to your Mimecast account manager, customer success manager or log a call with Mimecast support.

RESOURCES

Here is a list of government resources (webinars, papers, advisories) that security groups can visit to better understand the threats and defenses.

- **CISA/NSA** NSA and CISA Red and Blue Teams Share Top Ten Cybersecurity Misconfigurations
  5 October 2023
- **CISA** CISA Releases New Resources Identifying Known Exploited Vulnerabilities and Misconfigurations Linked to Ransomware
  12 October 2023
- **CISA** Phishing Guidance: Stopping the Attack Cycle at Phase One
  18 October 2023
- **CISA/NSA** CISA, NSA, and Partners Release New Guidance on Securing the Software Supply Chain
  9 November 2023
- **CISA/NCSC** CISA and UK NCSC Unveil Joint Guidelines for Secure AI System Development
  26 November 2023
- **CISA/NCSC /ACSC/FBI** Russian FSB cyber actor Star Blizzard continues worldwide spear-phishing campaigns
  7 December 2023

CONCLUSION

The fourth quarter of 2023 solidified many of the trends from previous quarters. Attackers are increasingly using brands to fool users into trusting spam and phishing attacks, often marrying the brand with a QR code or a link to a legitimate file service. Geopolitical tensions have heated up following Hamas' attack on Israeli civilians and Israel's subsequent retaliation, resulting in more attacks related to the conflict and a new set of topics for phishing lures.

Attackers slightly changed the sectors they targeted in Q4 2023, focusing on finance, such as banking and other services; professional services, such as HR and accounting; and the travel, hospitality, and catering sector. While campaigns targeting the human resources and recruitment services sector have subsided somewhat, the industry remains the third most targeted sector.

WORK PROTECTED.™

Advanced Email & Collaboration Security

mimecast®