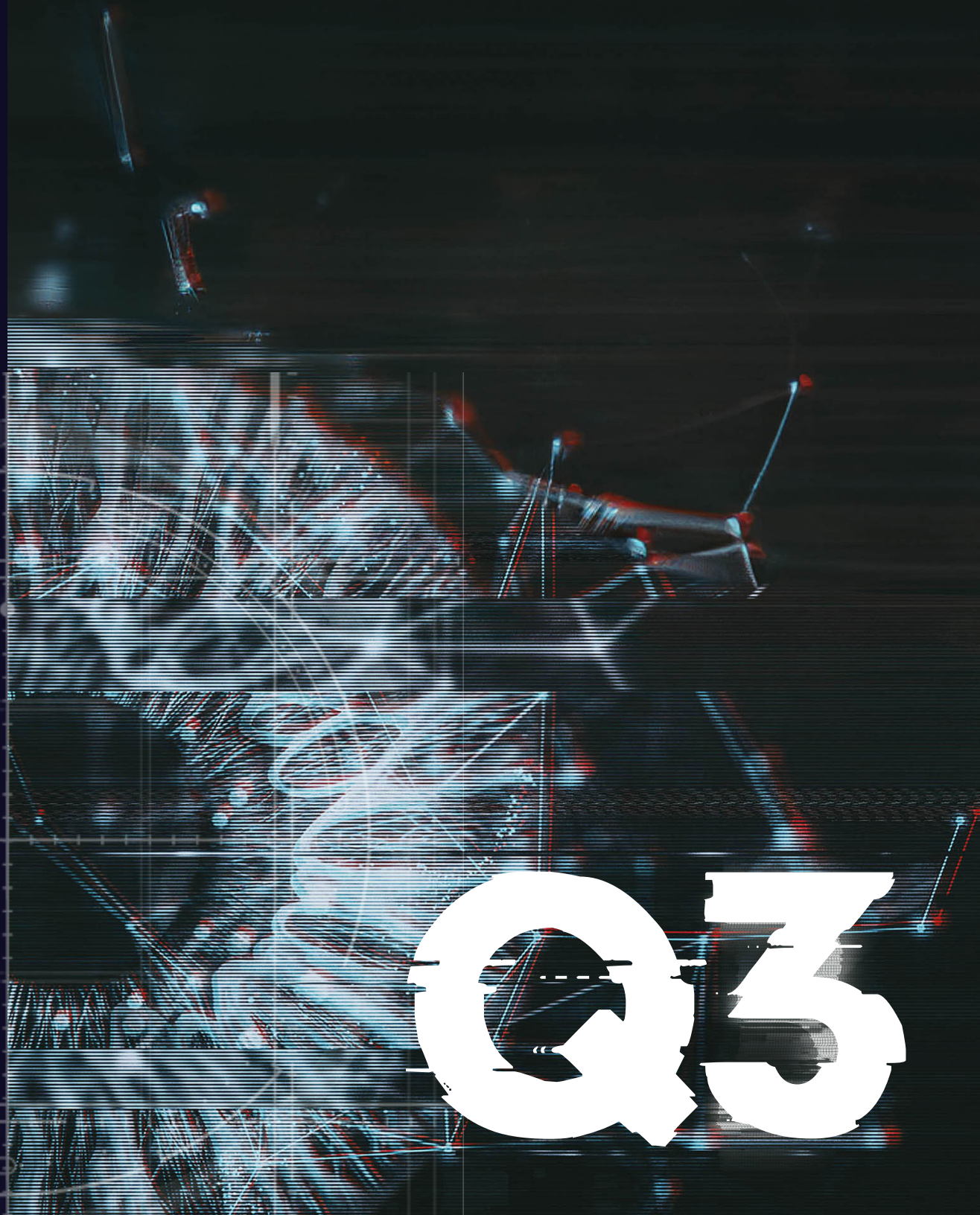
mimecast

Global Threat Intelligence Report

July-September 2023



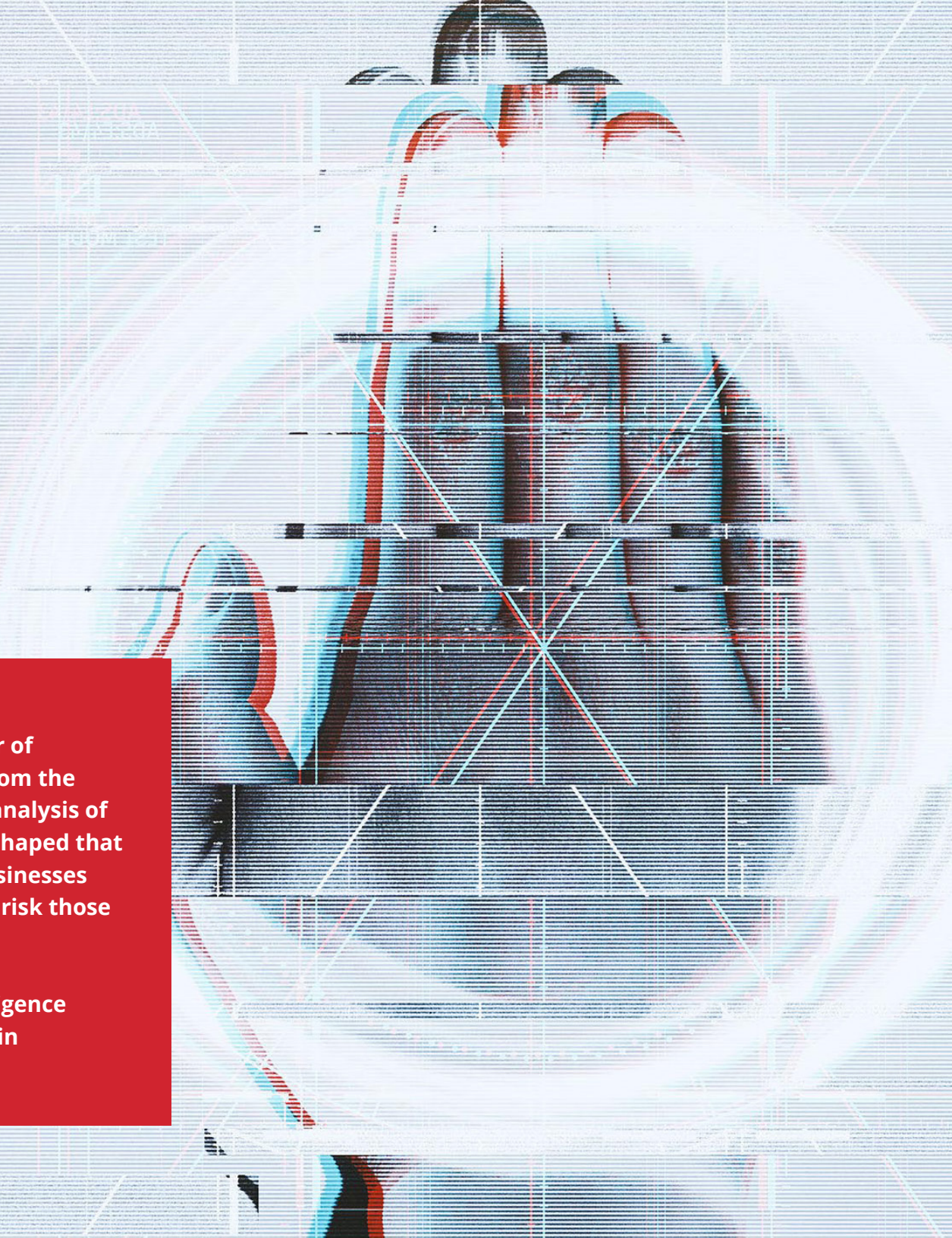
INTRODUCTION

Organizations large and small are increasingly looking to leverage good threat intelligence to update their cybersecurity infrastructures in real time and maximize protection of their businesses' communications, people, and data.

Mimecast generates threat intelligence through its analysis of more than a 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.

This report distills insights from the intelligence Mimecast generated throughout the third 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 Q3 2023 threat intelligence report and look forward to sharing more insights in the future.



EXECUTIVE SUMMARY

Attackers attempting to infiltrate businesses focused on a handful of significant zero-day vulnerabilities in the third quarter of 2023, even as they ramped up impersonation attacks. Our research shows that two-thirds of firms have suffered a ransomware attack in the past year, nearly all (97%) have been targeted by email-based phishing attacks, and the vast majority (76%) of security teams at organizations worldwide expect to have an attack with serious consequences using email as a vector.

2/3
firms have suffered a ransomware attack in the past year

97%
have been targeted by email-based phishing attacks

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 a billion emails per day, and Mimecast's cybersecurity experts analyze, investigate attacks, and test efficacy to develop sophisticated and timely threat intelligence that applies the latest protection across Mimecast's security solutions.

KEY FINDINGS

Impersonation increased, becoming more sophisticated as opportunistic cybercriminal groups used it to gain initial access to targeted organizations.

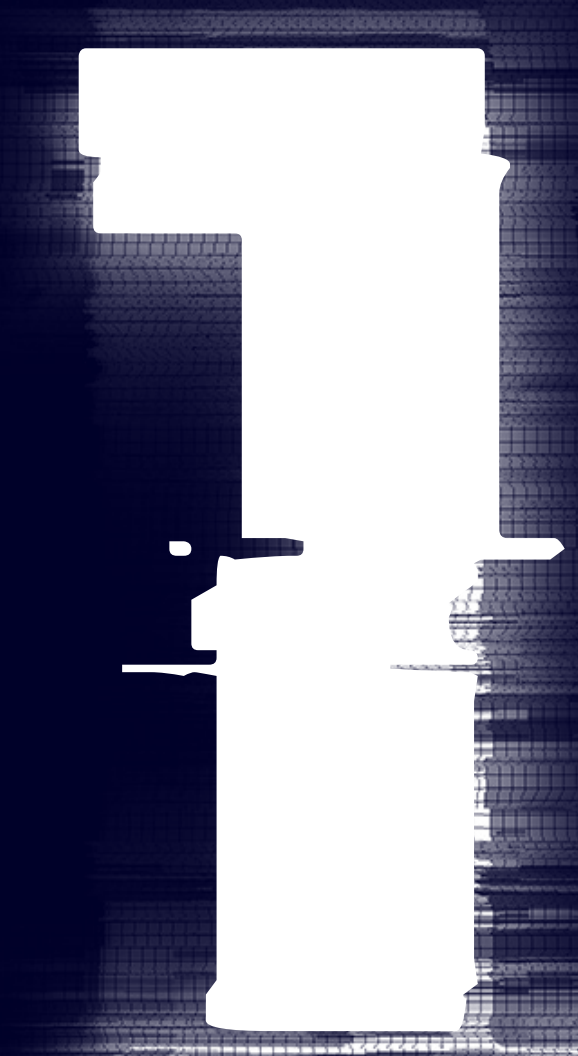
Zero-day exploitation of vulnerabilities became a greater threat, with attackers targeting flaws in MOVEit, multiple zero-day vulnerabilities in Microsoft software, and browsers and apps using the open-source libvpx and libwebp image libraries, among other issues.

Human resource firms, information technology software and services, and financial services (especially banking) **saw the most threats per user.** Consistently high levels of threat activity were also detected against the manufacturing, transportation, storage and delivery, and retail and wholesale industries.

Mimecast recommends that security professionals and risk managers review their service-level agreements to set minimum levels of data security and cybersecurity and find ways to monitor suppliers more closely. Acquisition targets should be subject to extra cybersecurity scrutiny.

Organizations should **configure their email infrastructure** to block the auto-loading of images, as we expect attackers to increasingly use image file types as carriers for malware and malicious content, such as QR codes leading to malicious sites.

ZERO-DAYS SURGE, CLOUDS ATTACKED



Multiple zero-day threats emerged during the third quarter of 2023, and threat actors added to their growing focus on cloud platforms and applications. We also saw several cybercriminal groups make notable strategic shifts in the quarter.

Security professionals continued to face widespread breaches caused by a critical vulnerability in the MOVEit managed file-transfer platform that began in Q2, at the end of May.

Then, the ransomware group Cl0p used the previously undisclosed vulnerability to compromise at least 200 — and more likely, 400 or more — businesses. Breach disclosures continued to trickle out during the third quarter. Many of the victims provided services to client organizations, which expanded the **impact of data breaches to more than 2,300 organizations.**

Other reports of new zero-day vulnerabilities in the quarter included critical security weaknesses in the open-source graphics libraries libvpx[1] and libwebp[2], which are likely to be incorporated into attacker tools going forward. The vulnerabilities in the two open-source graphics libraries could expose Google Chrome, Mozilla Firefox, and hundreds of applications.

While Cl0p is an opportunistic criminal group, state-sponsored and state-linked actors continued to take part in the cyber component of Russia's invasion of Ukraine. Russia-affiliated groups, such as Anonymous Sudan and Killnet, targeted government agencies and companies affiliated with Ukraine's allies, while Chinese hackers successfully **stole a consumer signing key from Microsoft in July.**

Both criminal and nation-backed groups continued the trend of targeting cloud services, following the many businesses that have shifted IT operations and other services to the cloud.

1. CVE-2023-5217 Detail, NIST National Vulnerability Database.
2. CVE-2023-4863 Detail, NIST National Vulnerability Database.

Credential phishing has become a major focus of email-based attacks, and threat groups are finding ways — such as **SQL-based lateral movement** and **consent phishing** — to get around the baseline security of the major triad of cloud services: Amazon Web Services, Google Cloud, and Microsoft Azure. In addition, cloud-based collaboration software platforms, such as Microsoft Teams and Slack, have become channels for phishing attacks and other attempts to steal credentials, with attacks increasing through those platforms during Q3 2023.

Meanwhile, threat groups experiencing their own challenges made shifts in strategy. The LockBit group appeared to cease activity for a week in August and may have been compromised. The Snatch Team ransomware group shifted its strategy and began commenting on its successful breaches, pointing out deficiencies in victims' cyber defenses to put pressure on companies to pay ransoms. Outing organizations' security shortcomings provides ammunition that insurers can use to avoid payments, **as well as fuel for potential lawsuits.** In late August, a multinational operation by law enforcement and private industry disrupted the Qakbot malware group and its associated infrastructure — used by many ransomware gangs to target victims — and coopted the network to distribute code to **remove the malware from affected computers.**

76%

expect a serious email-based compromise will impact their company this year

72%

anticipate a similar attack through their collaboration tools

Looking ahead, security professionals' concern over email-based attacks remains high, **with 76% expecting that a serious email-based compromise will impact their company this year** and **72% anticipating a similar attack through their collaboration tools.** Publicly traded companies may find themselves targeted more often as ransomware groups consider whether the new Securities and Exchange Commission rules for disclosure of breaches will make companies more likely to pay ransoms.

QUARTER THREE 2023 IN CHARTS

Uptick in threats for medium-sized firms

01

Small- and medium-sized companies face a greater number of threats than their larger counterparts.

Impersonation increased

02

Impersonation attacks become more sophisticated as opportunistic cybercriminal groups used it to gain initial access to targeted organizations.

PDFs still dominate, Excel becomes more common

03

Attackers' use of PDF and Microsoft Excel formats is growing. Our data shows attackers' use of malicious PDF files increased by 158% in Q3 2023 from the prior quarter, while the use of various Excel formats increased by 86%.

Top targeted industries

04

Human resource firms, information technology software and services, and financial services (especially banking) saw the most threats per user. Consistently high levels of threat activity were also detected against the manufacturing, transportation, storage and delivery, and retail and wholesale industries.

Attachment vulnerabilities

05

Most attackers relied on exploiting two vulnerabilities using malicious attachments: a flaw in the equation editor for Microsoft Office (CVE-2018-0802) and a bypass of Microsoft Office's security features (CVE-2016-7262).

01 Encounter rates: uptick in threats for medium-sized firms

Users at small- and medium-sized companies face a greater number of threats than their larger counterparts[3] because opportunistic attackers tend to see smaller companies as easier targets for phishing and ransomware campaigns. In addition, because of their smaller size, email threats targeted at specific internal groups — such as accountants or developers — will have an outsized impact on smaller companies.

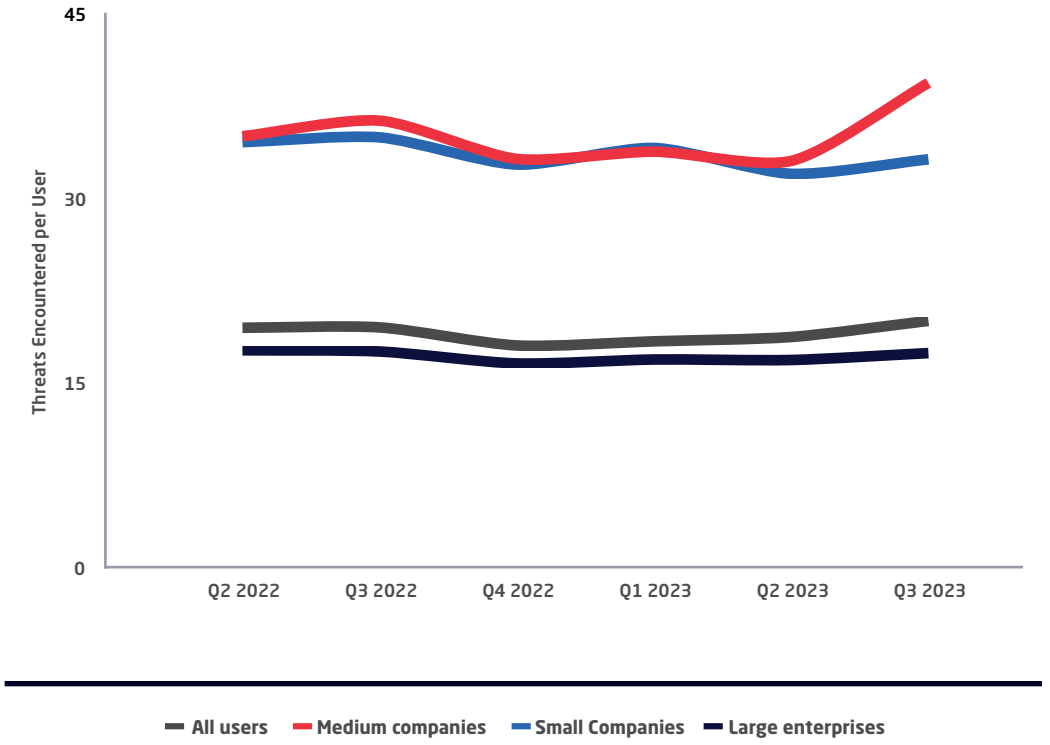
Medium-sized companies specifically have seen more threats per user in Q3 (see Figure 1), with Mimecast blocking nearly 40 malicious emails for each user per quarter, up from 33 last quarter.

For CISOs and security managers, this seemingly modest number of threats can quickly overwhelm their resources when multiplied across the entire employee base — especially because attackers only need a single success.

This increase in threats per user (TPU) is likely due to a combination of factors: Attackers see mid-sized companies as a profitable combination of vulnerability and potential cash value, and they often are good third-party launching points from which to compromise larger partner companies.

FIGURE 1 - Users at medium-sized companies saw more threats

Small (blue line) and medium-sized (red line) companies see more threats on average each quarter, but in the third quarter, users at medium-sized companies saw a significant uptick in threats.



3. As Attacks Rise, SMBs Need a Cybersecurity Playbook, Mimecast Cyber Resilience Insights Blog

02 Encounter rates: impersonation on the rise

On average, users saw more non-spam, non-malware threats in Q3 2023 compared to Q2 2023. While the number of spam messages encountered by the average user increased 7% in the third quarter from the previous quarter, both the number of impersonation attempts and malicious links sent to each user increased by double digits — 12% and 22% respectively. Overall, URLs continue to be a less frequent threat than impersonation, which rivals spam for the most encountered type of email attack.

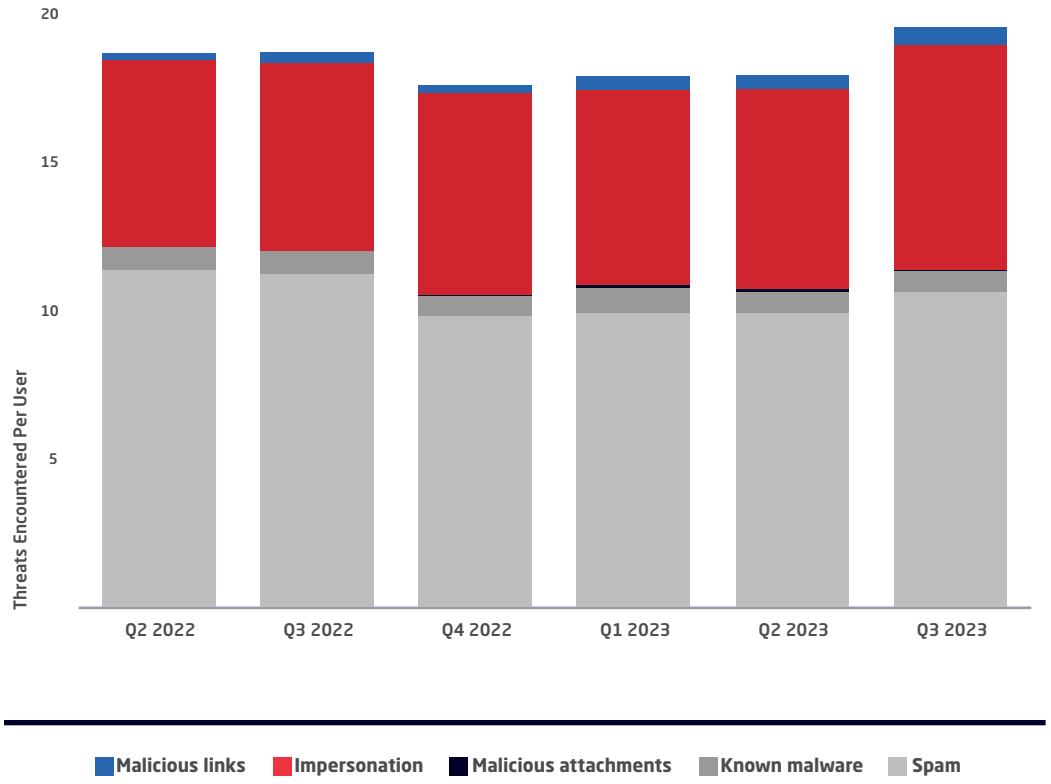
Impersonation attacks are a key tactic of state-linked groups seeking to establish initial access into targeted networks, and the cyber component of Russia's invasion of Ukraine likely contributed to the increase in impersonation attacks. Traditionally, Russian tactics target a specific adversary or region; but because other countries are aiding in Ukraine's defense, the attacks now appear to be embracing broader targets. In fact, attacks targeting organizations outside of Ukraine **outnumber those against Ukrainian targets.** The result is a spilling over of malicious email attacks to other regions — 116 cyberconflict-related attacks targeted Ukraine in Q2, compared to 489 attacks targeting organizations in other countries, such as Poland, Germany, and France. That resembles the **widespread spillover impact of NotPetya in 2017**.

Opportunistic cybercriminal groups are also adopting impersonation as a core technique to gain initial access to targeted networks.

Mimecast technology filters dangerous emails as they are detected. For example, impersonation attacks neutralized by the spam layer are never seen by the impersonation detection layer and are therefore not included in the red portion of each bar in Figure 2.

FIGURE 2 - Attacks using impersonation and malicious links increase

Users saw more threats using spam, impersonation, and malicious links in Q3 2023.



03 Attachments: PDFs still dominate, Excel formats become more common

Users see relatively few malicious attachments due to the success of current defenses. Nonetheless, attackers' use of PDF and Microsoft Excel formats is growing. Part of the reason for the low encounter rates for attachments is that attackers typically use them against specific targets in spear phishing or business email compromise (BEC) attacks, focusing on executives and accounting departments.

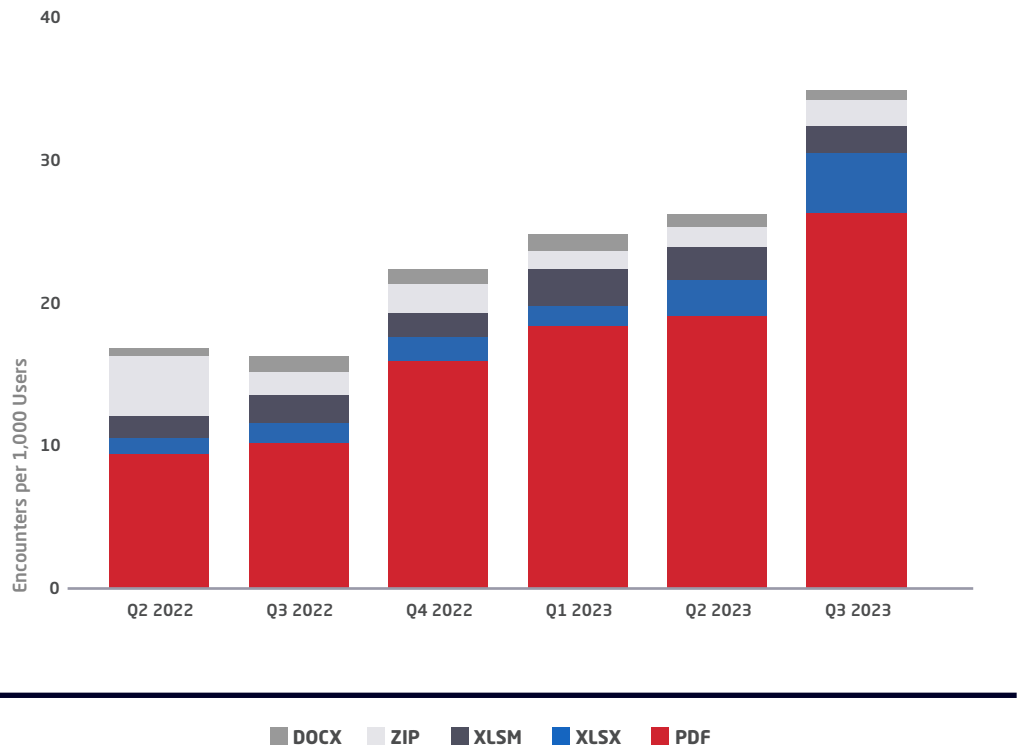
Our data shows attackers' use of malicious PDF files increased by 158% in Q3 2023 from the prior quarter, while the use of various Excel formats increased by 86%. Microsoft Word documents used in malicious attacks declined 46%.

Overall, Mimecast sees attackers reducing their reliance on malware sent as attached files in favor of links that can be dynamically modified. Links give the attacker the capability to change the payload on the fly and deploy additional covert capabilities.

The data on attachment-based attacks comes from Mimecast's third level of protection, Attachment Protect, which stops the more sophisticated attack attempts that escape first and second-level detections. As a result, the number of threats per user is lower than you might expect.

FIGURE 3 - Malicious PDF and Excel attachments increase

Users are seeing more PDF files (red) and Excel formats (blue shades) as malicious attachments (per 1,000 users).



04 Industry snapshot: targeting business operations

Attackers returned to pre-pandemic targets in Q3 2023, focusing on the internal groups and external services that are critical to business operations. Their top targets were human resource firms, information technology software and services, and financial services, especially banking.

Average users in those industries encountered threats at a rate far above the average for all industry sectors. There were 9.3 threats per user (TPUs) in human resources and recruitment, 5.5 (TPUs) for IT software and services and 4.1 (TPUs) in banking.

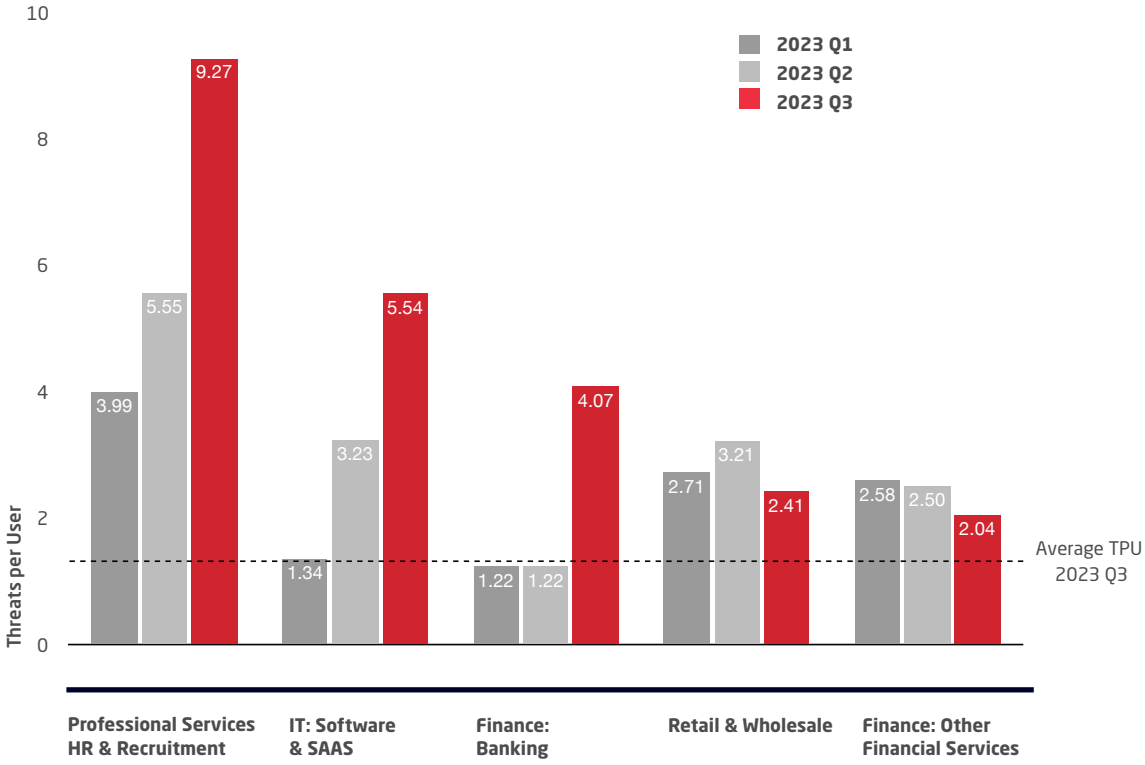
IT services and banking, ranked numbers two and three this quarter, and saw much less activity in previous quarters.

Mimecast has seen consistently high levels of malware activity sustained at volume since the pandemic commenced. This is now normalizing back to the opportunistic criminal and financial targets such as HR, banking, IT services and legal.

This trend has been apparent, but gradual since the start of 2023. The retail and wholesale industry ranked number four for attacks against its users in Q3 2023.

FIGURE 4 - Average threats per user by top industry targets

Companies in the HR and recruitment sector encountered seven times as many threats per user as the average business.



05 Vulnerability snapshot: most common email attack uses 5-year-old flaw

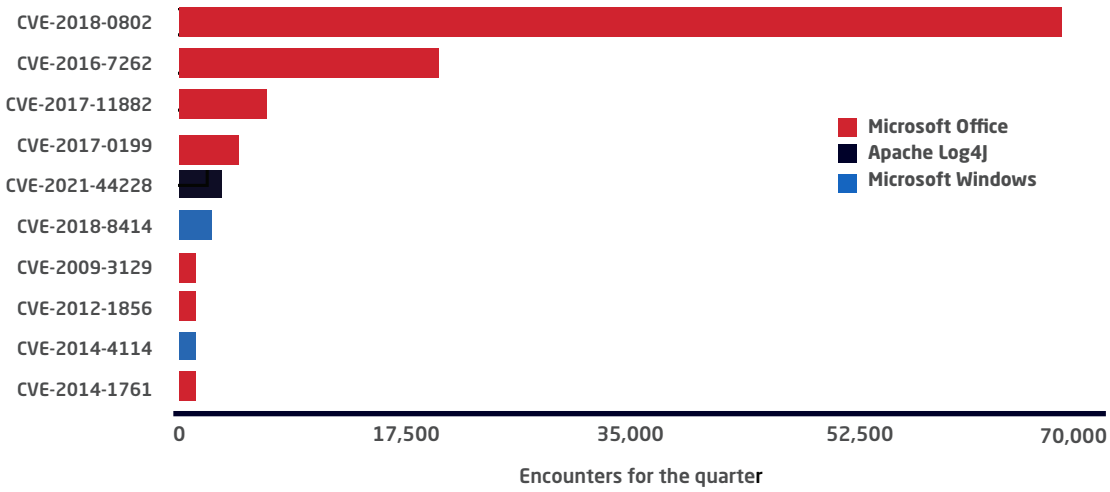
Most attackers relied on exploiting two vulnerabilities — both at least five years old — using malicious attachments: A flaw in the equation editor for Microsoft Office (CVE-2018-0802) and a bypass of Microsoft Office's security features (CVE-2016-7262). Because attachments are scanned only after passing other checks, such as spam protections, the threat data included here represents the more sophisticated attacks.

Data from the U.S. Cybersecurity and Infrastructure Security Agency (CISA) shows that many vulnerabilities encountered by companies do not arrive in email but target appliances and servers.

For example, among the most exploited security issues in 2022 were an SSL credential exposure in Fortinet virtual private network (VPN) appliances, three issues in Microsoft Exchange Server, and an authentication bypass in the Zoho ManageEngine.

FIGURE 5 - Top vulnerabilities encountered in email-based attacks

Two vulnerabilities accounted for most of the malicious attachments, both at least five years old.

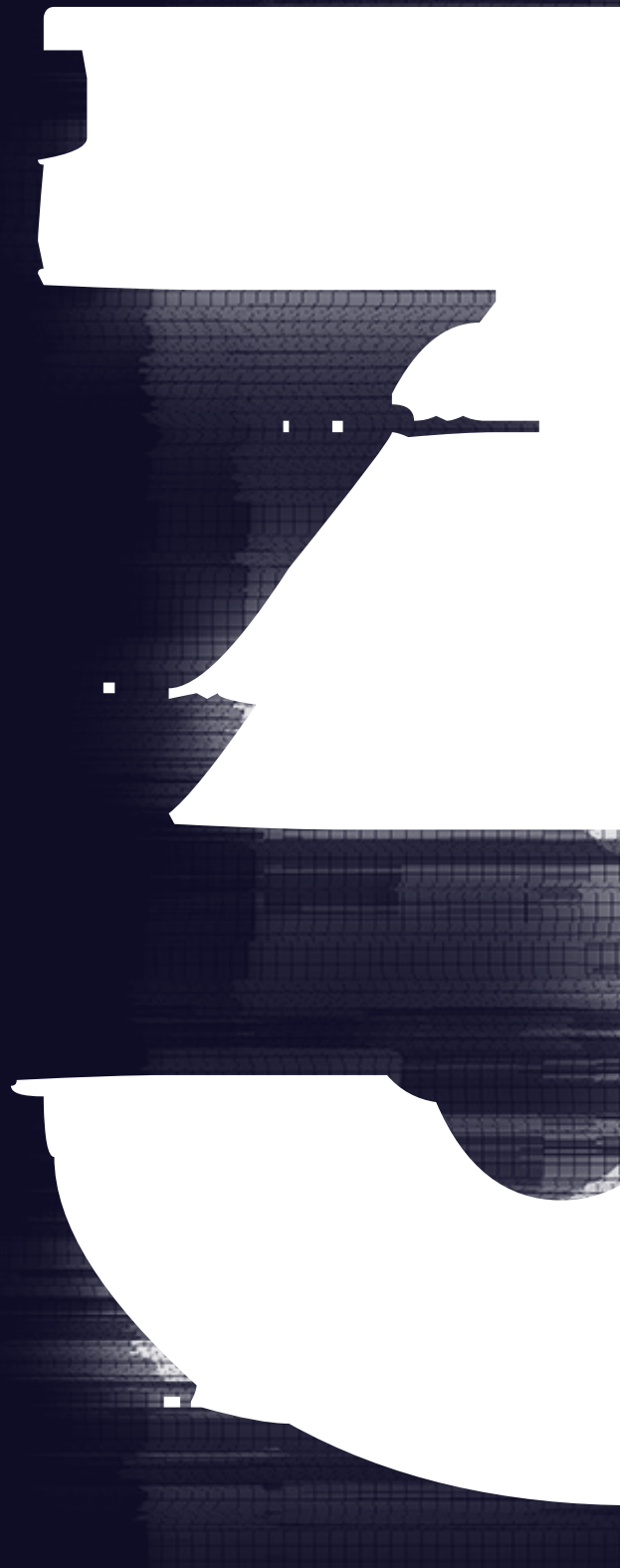


NATIVE SECURITY IS NOT ENOUGH

Beyond these vulnerabilities, Microsoft represents the lion's share of third-party email services. Some businesses have come to rely on the native security provided by Google Workspace and Microsoft 365; but because the two services account for 95% of all cloud email adoption, attackers are constantly and actively seeking ways to bypass their security and target their users.

For that reason, their native security is not enough. Attackers have already found ways around many of their defenses. Research conducted by a **cyber insurance firm** found that companies using cloud email services — such as Microsoft 365 or Google Workspace — see fewer attacks than those using on-premises email servers, but that companies using third-party email security solutions improved performance even further.

Companies recognize the need to close gaps in native security services, with 94% of security leaders seeking better security protections than those that come with their cloud email services. Mimecast was the best performing email security solution, with its users submitting 22% fewer claims to the insurer than the average organization.



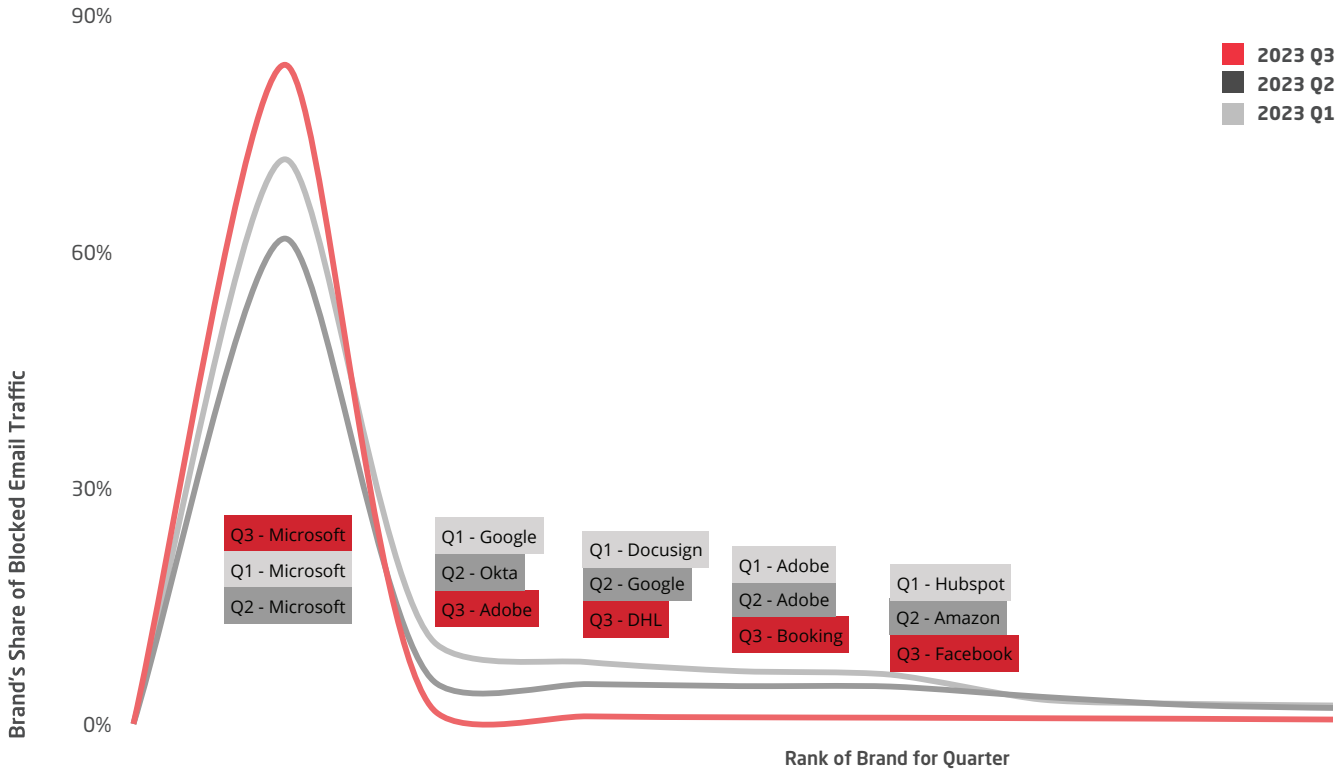
Attackers move faster than platforms

Cybercriminals are exploiting known vulnerabilities to launch attacks far faster than most organizations can patch their systems. The Known Exploited Vulnerabilities (KEV) Catalog, for example, documents which vulnerabilities attackers have already exploited, with 188 vulnerabilities from 2021, 120 from 2022, and 78 from 2023 exploited by attackers to date. Only a handful of vulnerabilities, however, account for most email attacks, making threat intelligence a key to knowing which exploits are most common and to helping harden the network and users against them.

Keeping up with which vulnerabilities have been exploited, how to defend against the attacks, and which exploits are currently being used to infect users is not only a difficult and increasingly complex task, but is often one that security teams do not have time to do properly.

FIGURE 6 - Microsoft dominates brand impersonation, even more so in Q3

Email attacks impersonating the Microsoft brand dominated phishing and BEC lures.



Email service providers typically do not have the intense focus on security to process the necessary intelligence and provide protection for their customers. To minimize email-based risks, companies should follow the best practice of layered security for the top attack vector — email.

Third-party security services bring focus and expertise

Attackers are increasingly using major providers' cloud services to launch attacks, with an increasing amount of spam and phishing coming from public domains, such as gmail.com and outlook.com.

Mimecast blocks thousands of malicious email messages targeting Microsoft 365 accounts every day utilizing their own services, such as Microsoft Dynamics 365 Customer Voice (see Figure 7 and 8). These attacks — along with those from other public services, such as gmail.com and yahoo.com — can be difficult for the average worker to differentiate in a sophisticated phishing attack.

In July, Mimecast saw a large spike in emails originating from compromised O365 accounts that contained .eml attachments. While this is not a new technique, threat actors continue to use these methods to circumvent security solutions. To increase their chances of success, attackers often make use of several layers within these campaigns, such as obfuscation within JavaScript.

Multiple variations of this threat with an embedded .eml attachment have been seen over the past quarter, using reputable companies and other lures to achieve the same result.

FIGURE 7 - Attacks impersonating Microsoft's domains

Mimecast sees thousands of attacks using Microsoft 365 accounts on a daily basis.

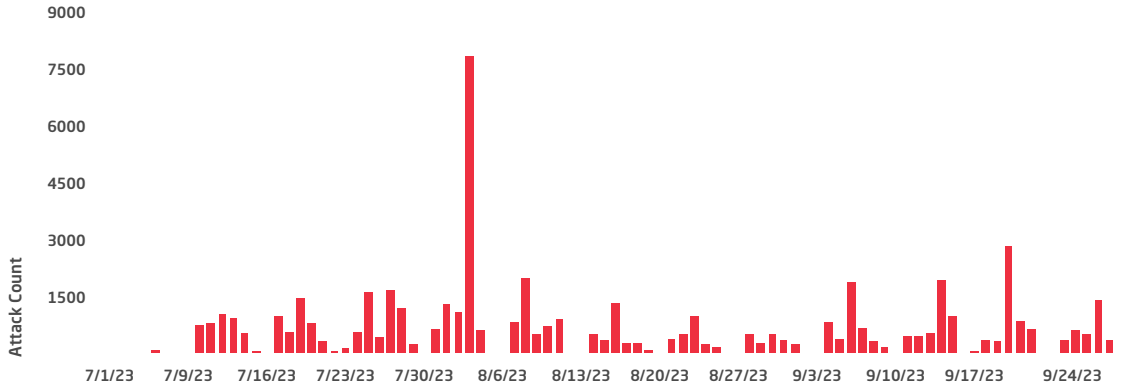
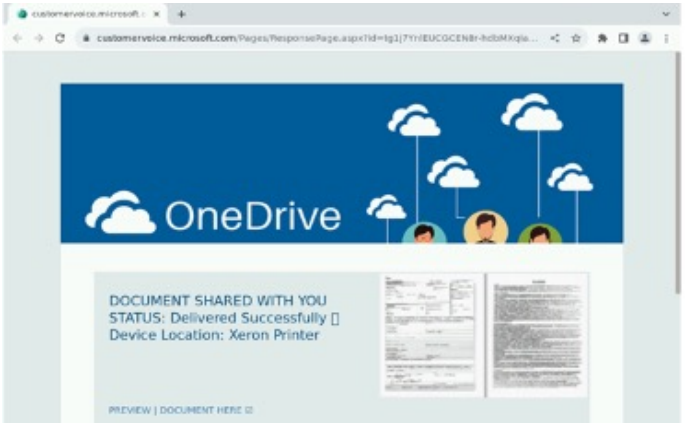


FIGURE 8 - Microsoft 365 Dynamics customer voice phishing page



While individual users can — and should — be educated on how to use email more securely, technology backed by third-party threat intelligence can more consistently protect users and their companies from email-based attacks.

Companies, for example, should ensure that they are protecting their email and collaboration channels by using the DMARC email authentication protocol to prevent their brands from being coopted for use in spear phishing attacks.

In addition, opening links in sandboxed environments can prevent a successful credential phishing attack.

In the end, email-service providers, such as Microsoft 365 and Google Workspace, do a great job delivering email and even reducing spam. However, managing the security of your users requires more:

A security provider focused on protecting businesses and workers from ever-evolving threats.

THREAT ASSESSMENT

Threat actors continue to focus on expanding the ways they can gain initial access into companies, including adopting collaboration software — such as Microsoft Teams — and expanding their Living off the Land (LotL) techniques to include a greater variety of programs. The underground economy continues to produce more advanced tools — the third quarter saw the rising popularity of a customized phishing platform used by at least 500 threat actors.

Some notable successes in thwarting threat actors include the Qakbot botnet takedown by a multinational group of law enforcement and private-sector firms, and the fact that pressure on cybercriminal actors to decrease ransoms has become so strong that at least one group (LockBit) is considering putting limits on its affiliates to negotiate ransom amounts.

Additionally, the Emotet group has once again paused its operations, but whether this can be considered a success for defenders is unclear, as the group has previously shuttered operations only to appear again.

MAJOR EVENTS 2023 Q3

1 JUL

BlackCat Advertising Campaign

Analysis finds BlackCat ransomware gang using "malvertising" to gain initial access to business networks.

Read article

3 JUL

Emotet Hibernates?

Emotet operation appears to enter dormant period again, according to several sources. However, Mimecast has detected ongoing operations by the group.

Read article

13 JUL

TeamTNT Phishes for Credentials

TeamTNT targets cloud credentials and kicks off cryptocurrency mining campaign.

Read article

2 AUG

Phishing Through Microsoft Teams

Midnight Blizzard group uses compromised M365 tenants to send malicious Teams messages and target credentials.

Read article

3 AUG

Living Off the Land Grows More Popular

Hackers are finding more ways to use the executable files present on targeted systems — including Microsoft Office programs — to download malicious code.

Read article

17 AUG

QR Codes in Phishing Campaigns

Attackers use QR codes to bypass email-security solutions and redirect victims to phishing sites, focusing on companies in the energy, manufacturing, and insurance sectors.

Read article

25 AUG

Qakbot Takedown

A multinational effort between law enforcement and technology providers resulted in the disruption of the Qakbot malware and botnet and the dissemination of an uninstall file to affected systems.

Read article

5 SEP

Threat Group Targeting Okta Super Admins

Attackers targeted at least four Okta customers with social-engineering campaigns that aimed to bypass two-factor authentication security protecting the accounts. Mimecast began detecting the attacks in May.

Read article

6 SEP

BEC Phishing Kit Uncovered

Researchers uncover W3LL threat actor, which has been selling a custom phishing kit customized for BEC attacks and bypassing MFA to more than 500 other threat actors.

Read article

12 SEP

More Phishing Through Microsoft Teams

Storm-0324 (aka, TA543 and Sagrid), a distributor of cybercriminal tools, has widely adopted phishing lures sent through Microsoft Teams.

Read article

12 SEP

WebP Vulnerabilities Threatens Mass Attacks

Two vulnerabilities in the WebP open-source image library used by browsers, email clients, and other applications are found to have already been exploited by nation-state actors, attacks that presage potential compromises for months, if not years, as consumers patch.

Read article

18 SEP

Cybercriminal Affiliates Low-Balling Ransoms?

Worried that too many "affiliates" are discounting ransoms, the LockBit ransomware group discusses the imposition of a minimum ransom set at 3% of the victim company's annual revenue.

Read article

26 SEP

ZeroFont Technique Sees Resurgence

The phishing tactic of embedded zero-font-sized text has undergone some refinements and now attempts to make emails look more reputable by using zero-font text at the beginning of the message — text which often shows up in the message list of popular email clients.

Read article

Top Advisories

Government sources issued many advisories focused on email security during the quarter, including warnings of an increase in attacks on Outlook Online and descriptions of fast-turnaround extortion and cryptocurrency scams.

In addition, government researchers noted that many ransomware attacks continue to rely on well-understood techniques to monetize any initial compromise of an organization's network.

6 JULY [NCSC] Active Cyber Defense (ACD) – The Sixth Year Report

The number of malicious sites taken down by the UK government fell in 2022 to 1.8 million campaigns and 2.4 million URLs, from 2.7 million campaigns and 3.1 million URLs in 2021. While the frequency of attacks has remained stable, the servers behind extortion emails and cryptocurrency investment scams have short uptimes (1 hour to 1 day, on average), resulting in the attacks ending before they could be taken down.

Reference

12 JULY [CISA] Enhanced Monitoring to Detect APT Activity Targeting Outlook Online

The US Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) warned critical infrastructure agencies that advanced persistent threat (APT) groups had begun targeting Outlook Online with attacks using a Microsoft account (MSA) consumer key to forge tokens.

Reference

30 AUG [CISA, FBI] Identification and Disruption of QakBot Infrastructure

CISA and the FBI released a joint advisory following the August 25 takedown of the Qakbot botnet. The advisory included a description of the takedown, which severed the connections between command-and-control servers and victims' machines, as well as indicators of compromise. The FBI worked with industry partners to share information, including indicators of compromise, to help defenders detect Qakbot infections and remediate compromises.

Reference

11 SEP [NCSC, NCA] Ransomware, extortion and the cybercrime ecosystem

Ransomware and wiper malware have caused massive disruptions to business operations in the past five years. Showing their adaptability, however, today's cybercriminals are focused more on monetizing opportunistic data breaches using well-understood attack techniques.

Reference

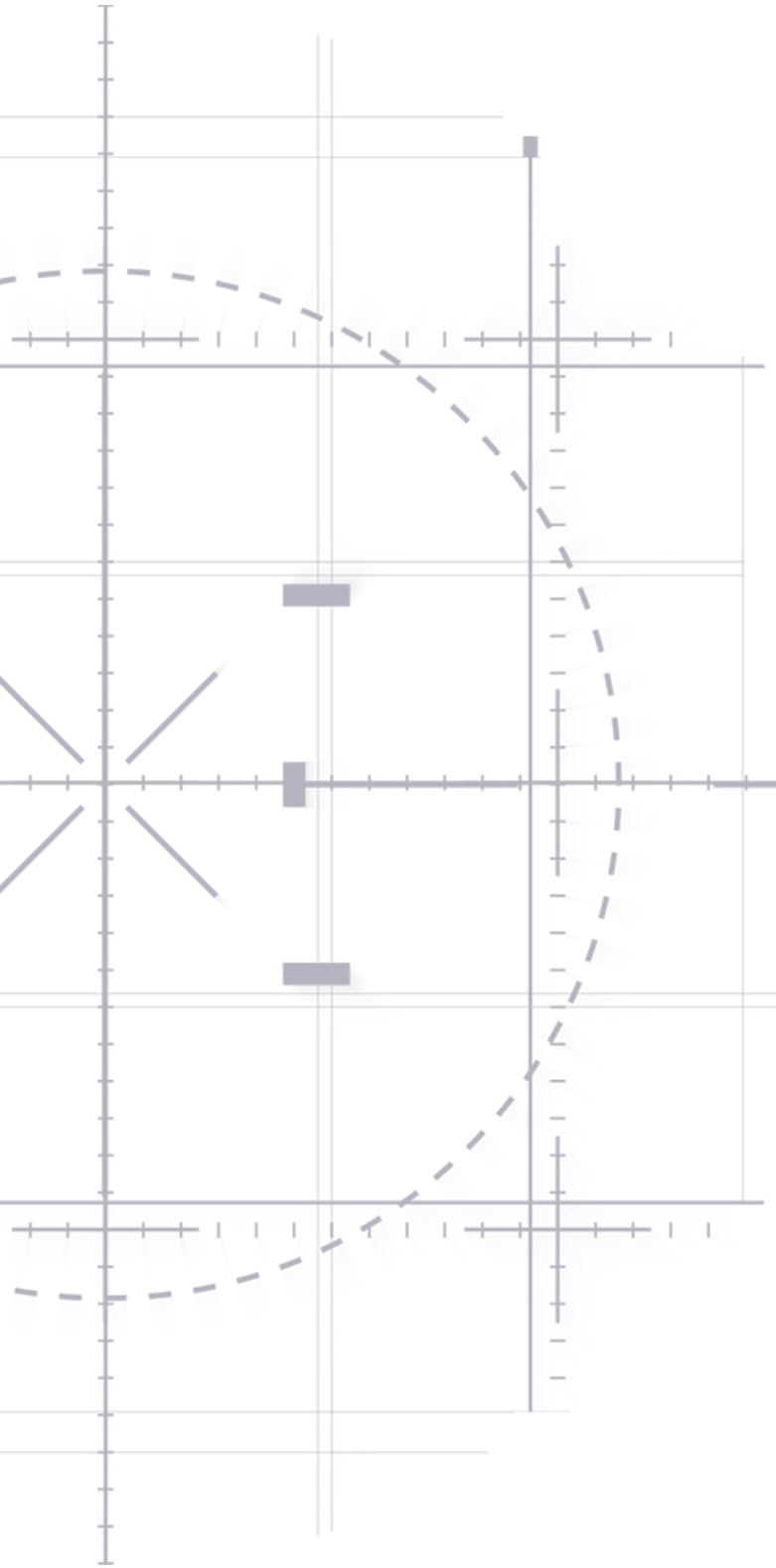
12 SEP [NIST] WebP Vulnerabilities (Chrome: CVE-2023-5217 and CVE-2023-4863; Apple: CVE-2023-41064)

Both Google and Apple fixed zero-day vulnerabilities in the libwebp library that were being exploited by nation-state actors. The library is not just used by browsers; it's also used by other applications, including those on mobile devices, which may not be updated as quickly as other consumer software.

Reference

HOW TO TAKE ACTION

Cybercriminals are tailoring threats to take advantage of current events using all available attack vectors but particularly those that can be mass delivered such as phishing, spam, and impersonation emails. Organizations should seek to maintain adequate standards of cyber hygiene through the appropriate use of hardening techniques for organizational assets.



Threat-specific countermeasures

Mandate more security from third parties

Attacks against organizations in the manufacturing, transportation, storage and delivery, and retail and wholesale sectors represent significant third-party risk of supply-chain compromise. Organizations should review their service-level agreements to set minimum levels of data security and cybersecurity and find ways to monitor their suppliers more closely, such as external rating services, as well as subject acquisitions to extra scrutiny.

Block images in email messages

Attackers are increasing their use of image-based file types as a way to sneak in phishing lures and malicious code while evading detection. Mimecast's analysis has identified threat actors also using encryption and foreign language text, accompanied by encryption, within images to escape notice. Companies should configure email clients to prevent the loading of images in messages and isolate any images that users explicitly request.

Note: Cybergraph Users should leverage **trusted sites** to ensure banners load correctly.

Scan external network for open ports

Organizations should regularly scan their external network to ensure any publicly accessible server ports are closed or adequately secured and protected. Mimecast has noted continuing increases in attacks against remote desktop protocol (RDP) ports that have accounted for 80% of effective ransomware compromises. Attackers will continue to look for open RDP ports as a way to compromise organizations.

Segment the network & log internal traffic

Attackers, especially during a ransomware attack, can quickly move laterally throughout a network. Segmenting the internal network and putting critical assets in their own enclaves can reduce the damage caused by ransomware and other attacks. Monitoring internal traffic, especially communications into specific segments, can result in earlier detection of threats.

General recommendations to combat threats

Maintain backups of critical systems & data
Organizations hesitate to pay ransoms, doubting ransomware groups' data recovery promises. To minimize downtime and costs after an attack, robust backups, especially of critical data, and routine recovery process testing are vital. In a ransomware event, backups might be the sole recovery option. Cloud backups often yield better results, but organizations should opt for the most suitable backup method.

Increase user awareness & training
Educating users in current phishing techniques will significantly aid companies in foiling phishing attacks and credential theft. Users should be regularly trained using examples of current attacks and be given specific strategies to help determine whether an email is suspicious. In addition, vulnerable users should have focused training in conjunction with restrictive security policies. Users also should be instructed to report suspicious email messages to IT security to help determine when attackers are targeting specific individuals.

Harden user credentials
Emotet and ransomware threats exploit common passwords to infiltrate networks. Recent attacks highlight how weak passwords contribute to breaches. Strengthen any network by enforcing robust passwords, especially for privileged users. IT security must eliminate default admin passwords.

Implement phishing-resistant multi-factor authentication
Adopting an additional factor of authentication, especially a phishing-resistant technology, can result in a significant reduction in credential-based attacks, as part of a zero-trust approach to security. Companies that add pervasive multifactor authentication to both their cloud and internal infrastructure will reduce their risk by an order of magnitude.

Prioritize vulnerabilities & patch quickly
Though thousands of vulnerabilities are reported yearly, only a few are exploited. To enhance security, focus on regular updates for critical software. Threat intelligence helps spot and prioritize actively exploited vulnerabilities for quicker patching. Mimecast foresees a rise in zero-day exploits due to cybercriminals adopting advanced tools like AI and machine learning. Prioritize securing key internet-exposed systems and software, like VPNs and remote desktop tools, as they carry higher risks.

Resources

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

CISA
Known exploited vulnerabilities catalog
Updated Weekly

NCSC
Spotlight on shadow IT
27 July 2023

CISA
Review of the attacks associated with Lapsus$ and related threat group report
10 August 2023

CISA
Open source software security roadmap
12 September 2023

CISA
Phishing guidance: stopping the attack cycle at phase one
18 October 2023

Methodology

The data in this report is derived from analysis of more than a billion emails per day monitored by Mimecast on behalf of its 42,000+ global customer organizations and compiled by the Mimecast Threat Intelligence Center.

Mimecast's threat detection engine proceeds from simple to increasingly sophisticated filters and eliminates threats at each layer as they are detected. This means that threats identified by the spam layer will be stopped there and not scanned by subsequent layers. So, simple and obvious impersonation threats, for example, may be neutralized by the spam layer and, therefore, not included in our data for impersonations detected.

Steps specific to Mimecast Customers

Actionable steps to protect your users from the threats in the report, with medium-level technical details.

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.

Single sign-on
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. **Read more**

Impersonation protection
Optimize Impersonation Protection as per best practice guidelines of two 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 three hits or more with the admin hold action. **Read more**

Safe file
Consider safe file for at risk departments who do not require access to editable attachments within Attachment Protection. **Read more**

DNS authentication policies
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 legit mail being rejected/quarantined for DMARC failures. **Read more**

Re-writing of URLs
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. **Read more**

Anti-spoofing lockout
Utilize Anti-spoofing lockout, if possible, to add an extra layer of protection, however, ensure you are aware of any entity who is spoofing your domain, as this policy will reject and not hold mail. **Read more**

Capture and review logs
Regularly capture and review logs on your Mimecast account to enforce security policies

Third-party threat feeds
Leverage bring-your-own threat intelligence to take advantage of any third-party threat feeds for automatic rejection of matching indicators. **Read more**

WORK PROTECTED.™

Advanced Email & Collaboration Security

mimecast®