mimecast

Global Threat Intelligence Report

January - June

Introduction

To adapt to the latest cyberthreats, organizations large and small need to leverage good threat intelligence, quickly update their cybersecurity processes and infrastructure, and harden defenses around their businesses' communications, people, and data.

Mimecast generates threat intelligence through its analysis of more than 1.7 billion messages per day on behalf of more than 42,000 customers. Email and messaging are the channels through which most cyberthreats launch, allowing Mimecast to detect and analyze threats before they become widespread.

In this Global Threat Intelligence Report, Mimecast has distilled insights from our intelligence analysts for the first six months of 2024, combining our data with open-source intelligence from the cybersecurity community at large.

The report includes analysis of threat activity, statistics revealing attack trends, and a series of recommendations for businesses of all sizes to better mitigate the risks of cyberthreats.

We invite you to explore our H1 2024 threat intelligence report and look forward to sharing more insights in the future.

1.7 billion emails

42,000 customers

Executive Summary

The first half of 2024 emphasized the French saying, "Plus ça change, plus c'est la même chose" — the more things change, the more they stay the same.

The adoption of AI technology by both cyber attackers and defenders, for example, continues to promise massive changes in the way cybersecurity is conducted; so far, the impact has been limited on both sides. The battle for dominance of the cyber domain is unrelenting, as cybercriminal cloud services and as-a-service offerings continue to expand the availability of attack tools, phishing kits, and databases of stolen information. Law enforcement agencies have shown signs of adapting, with cross-jurisdictional collaboration resulting in the disruption of major groups.

Email continues to evolve as attackers reduce their reliance on malware attachments, opting for malicious links to legitimate cloud file-sharing services, such as SharePoint and Google Drive.

A temporary surge in attacks against medium-sized businesses has subsided, with small-business users again seeing the most threats. And credential theft has become a major focus of attackers, who then sell stolen credentials on underground markets or use them in credential-stuffing attacks to gain access to businesses' cloud services.

The future holds some predictable challenges.

As companies further migrate to the cloud and develop their infrastructure, the overall attack surface has expanded. The growing dependency on data stored within the clouds means security control is increasingly blurred, while the inherent reliance on third-party software and infrastructure makes supply chain security a major problem. In the face of continued ransomware attacks, maintaining data confidentiality, integrity, and availability—the CIA triad of information security—is a key to successful business outcomes, as attacks on data can lead to service interruption and a devastating impact on business operations. Finally, generative AI and machine learning will improve the targeting and content of phishing campaigns, driving the defender's requirement to be able to detect and quickly respond to new and novel attack techniques

1 Key Findings

1

Messaging attacks evolve from pushing malware to using links, with more layers of links providing some obfuscation from detection. This shift also requires more interaction from victims, including clicking through more links and responding to CAPTCHAs and false multi-factor authentication requests.

2

The banking, arts and entertainment, and travel and hospitality industries experienced the most malicious URL messages in Q2 2024, while the IT consulting and legal professional services sectors encountered the most spam and impersonation messages.

3

Attackers are using development services, such as Replit, to host and develop campaigns. File-sharing services, including SharePoint and Google Drive, are also popular ways of hosting intermediate documents that link out to credential harvesting pages.

4

Impersonation attacks dominated threats targeting European users, while spam accounted for most attacks in Africa. The Asia-Pacific region saw a dramatic spike in attacks against small businesses.

The Threatcast

This year promises surging spam, phishing, and disinformation attacks as a convergence of important world events conspires to produce plenty of subject matter from which to construct phishing lures and motivate attackers. In 2024, a massive election season kicks off with major votes in the United States and Europe, snap elections in France, and more democracies deciding their fate than in any previous year.[1] The continuing Russian invasion of Ukraine and the conflict between Israel and Hamas in Gaza have resulted in significant surges in disinformation attempts. Major sporting events — from the Summer Olympics and Paralympics in Paris to the recent Euro 2024 and COPA America football tournaments — have attracted attacks from a variety of groups.

Six major events during the first half of 2024 highlight the potential messaging and human-centric risks arising from the current threat landscape. Reports range from opportunistic hackers gaining more information about cloud users, compromise of cloud email systems, and misinformation driven by minority groups to gain more ground in elections.

1. 2024 is the biggest election year in history. The Economist. The World Ahead. 23 Nov 2023

Major events

Trello leaks 15 million user records[2]

Vulnerability: Insecure public API
Impact: Email addresses fuel future attacks

i-SOON insider leaks hacking info[3]

Vulnerability: Insider leak
Impact: Sensitive information about Chinese hacking operations made public

Lockbit operation disrupted by global effort[4]

Vulnerability: Law enforcement action
Impact: Disruption of major cybercrime organization

JAN.

Threat intelligence analysts discovered more than 15 million records of Trello users for sale on the Dark Web. A hacker used API calls to collect information from the overly permissive API that allowed anyone to query user accounts and find Trello boards associated with those accounts. The attacker harvested usernames, email addresses and full names — data that could power a variety of messaging attacks. Atlassian, the owner of Trello, changed the API to make it harder to collect such information going forward.

FEB.

More than 570 files totaling 170 MB of data describing the activities of Chinese security contractor Shanghai Anxun Information Co., known as "i-SOON," were uploaded to code-repository platform Github. The leak, which appears to have been perpetrated by a disgruntled employee, revealed that the company had carried out espionage operation for the Chinese government against more than 20 governments in foreign countries, including the United States and South Korea, and territories, such as Taiwan.

The United Kingdom's National Crime Agency, along with investigators from 10 global law enforcement agencies, disrupted the LockBit ransomware gang by taking control of the group's infrastructure and servers and confiscating about 11,000 domains in an action dubbed Operation Cronos. The LockBit group is thought to be responsible for a quarter of ransomware attacks in the past year and has received more than $120 million in ransom payments. The law enforcement operation included arrests in Poland, Ukraine, and the United States.

2. Atlassian Tightens API After Hacker Scrapes 15M Trello Profiles. Seals, Tara. Dark Reading. 24 Jan 2024 | 3. Hacking Contests, Bug Bounties, and China's Offensive Cyber Ecosystem. ETH Zurich. Whitepaper. 10 June 2024 | 4. A Global Police Operation Just Took Down the Notorious LockBit Ransomware Gang. Burgess, Matt. Wired. 28 Feb 2024

CISA releases details of Microsoft email hack[5]

Vulnerability: Stolen signing key
Impact: Exposed sensitive emails of highly placed U.S. officials

APR.

In a report published in April, the Cybersecurity and Infrastructure Security Agency (CISA) released details of an intrusion into Microsoft Exchange Online by the cyber espionage group Storm-0558, which is linked to the People's Republic of China. Using a stolen key created in 2016, the threat actors gained access to the email of more than 500 people at 22 organizations, including officials in the U.S. State Department, U.S. Commerce Department, and U.S. House of Representatives. The report follows a January 2024 Microsoft analysis of a second hack, which took place in November 2023, of Microsoft's executives' emails by a Russia-linked group.[6]

Insecure credentials leak data from Snowflake[7]

Vulnerability: Lack of multifactor authentication
Impact: Customer data leaked from cloud storage

MAY.

At least 165 customers of cloud-data provider Snowflake — Ticketmaster and Santander Bank were named in news reports — had data leaked after stolen credentials were used to gain access to their Snowflake accounts. The accounts were likely stolen through phishing attacks and either didn't have two-factor authentication enabled or allowed username and password access as a backup.

Disinformation attacks influence EU elections[8]

Vulnerability: Widespread misinformation attacks through email and social media
Impact: Increased polarization, potential impact on elections

JUN.

In May and June, disinformation surrounding European Union governments surged, according to the European Digital Media Observatory, a group focused on countering disinformation. Policymakers and democracy advocates worry that a similar surge in disinformation by foreign adversaries will not be effectively countered in the United States, as right-wing efforts to shut down disinformation clearinghouses have had some effect.[9]

5. Report on Microsoft Online Exchange Incident. CISA. Department of Homeland Security Advisory. 2 April 2024 | 6. Microsoft Actions Following Attack by Midnight Blizzard. Microsoft Security Response Center. Microsoft. 19 Jan 2024 | 7. UNC5537 Targets Snowflake Customer Instances for Data Theft and Extortion. Google Mandiant Blog. 10 June 2024 | 8. Convergence of Anger' Drives Disinformation Around E.U. Elections. Tsu, Tiffany. The New York Times. 7 June 2024 | 9. Stanford's top disinformation research group collapses under pressure. Menn, Joseph. The Washington Post. 14 June 2024

Threat landscape in charts

Overall, small and medium businesses saw a peak in attacks in the first quarter, while large enterprises saw fewer threats per user (TPUs) overall. While spam and impersonation attacks dominate the threat landscape, malicious links remain the favored way for attackers to attempt to infect end users' systems.

The Banking, Travel & Hospitality, and Arts & Entertainment industries were the most targeted, with attackers less focused on Human Resource departments, a perennial favorite. All charts are global. For a regionalized view representing Asia Pacific, Canada, Europe, Sub-Saharan Africa and the Middle East, United Kingdom and United States & Caribbean, visit Mimecast Threat Intelligence Hub.

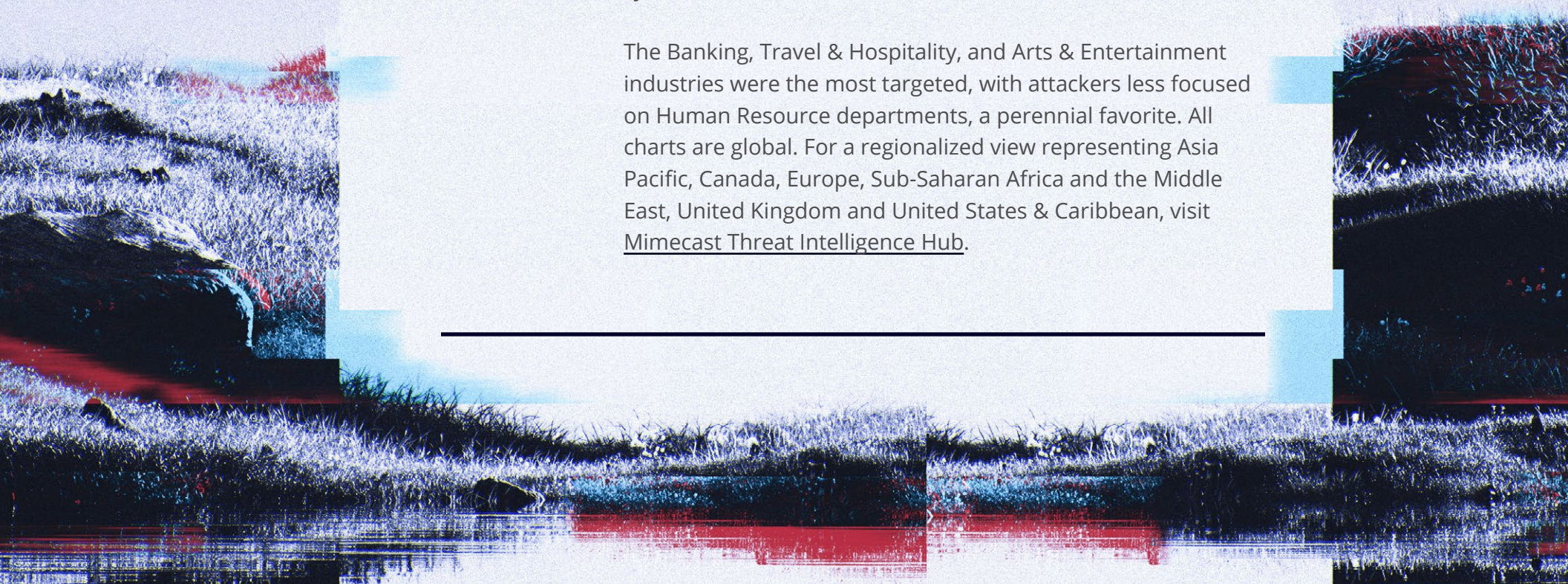
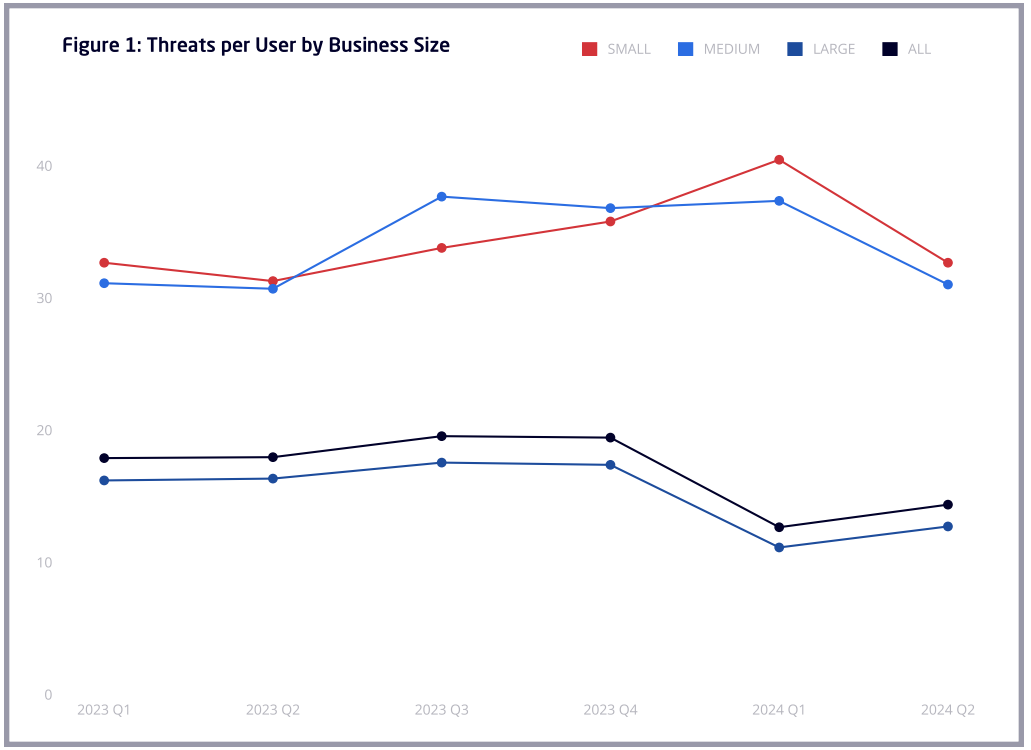


Chart one

TPUs by Business Size

Overall, the number of threats targeting users declined by about a third, dropping from 19 threats per user on average at the end of last year (Q4 2023) to 14 TPU for latest quarter (Q2 2024). The threats impacting large enterprises also declined in the first quarter, but rose in the second quarter of the year, while the TPUs for medium-sized businesses remained flat in the first quarter and then declined steeply in the second quarter to 31 TPUs.

Only small businesses had a significant increase in attacks to 40 TPUs in Q1—partially due to a spike in attacks in the Canada, Europe and US regions—in the first quarter, which subsided in the second quarter.



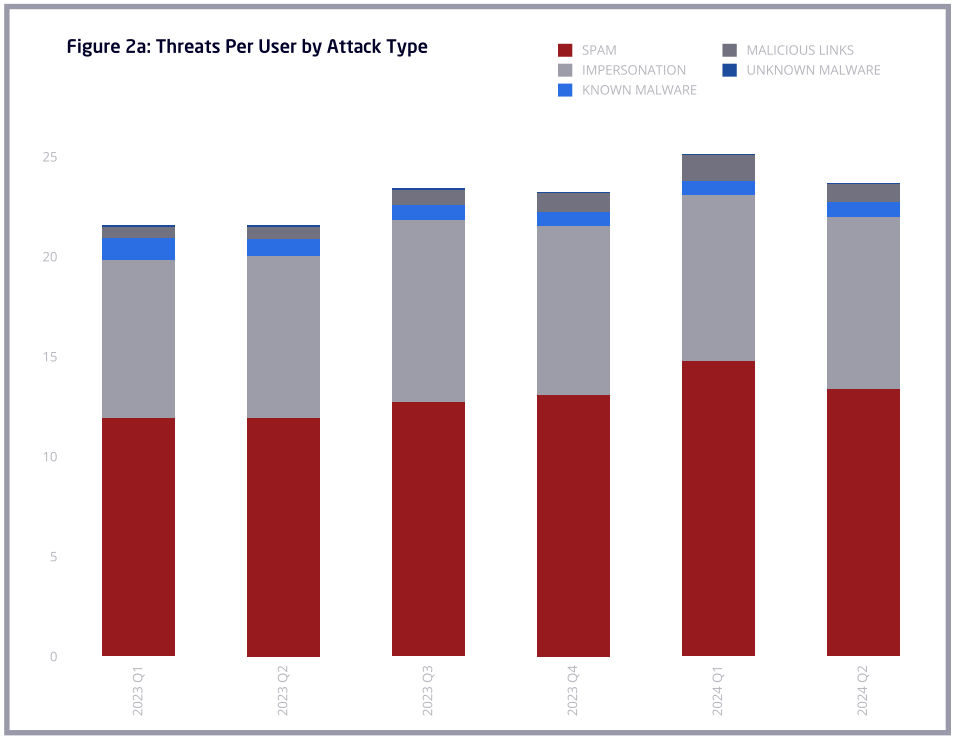
VIEW YOUR REGION

Chart two

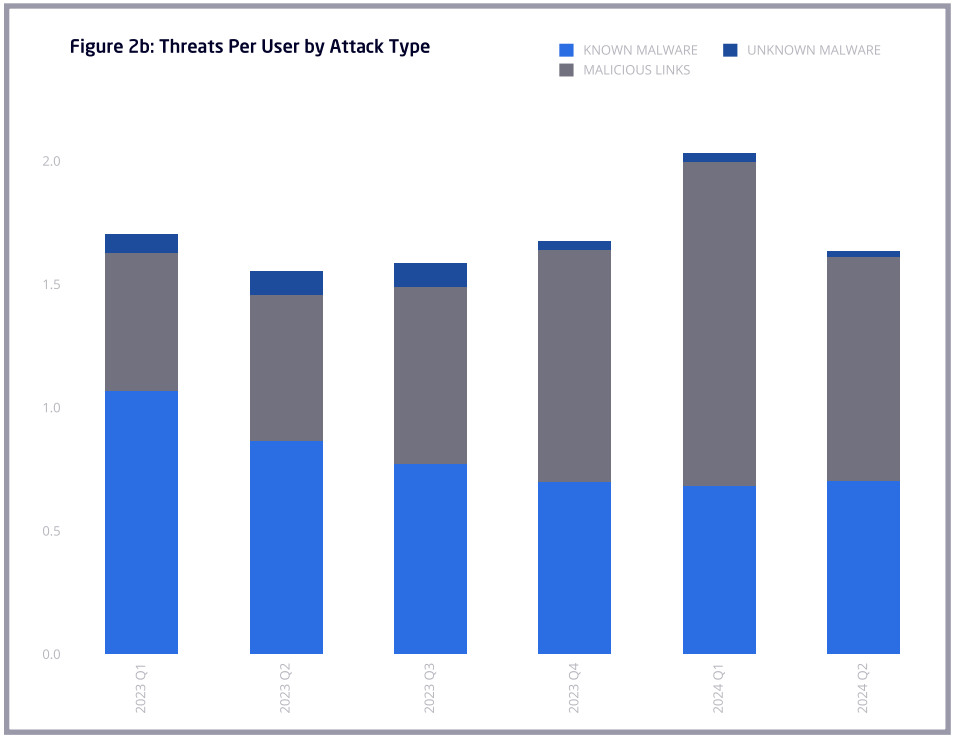
Impact of Attack Type on TPUs

Spam and impersonation remain the prominent attacks blocked by Mimecast, with the platform blocking 13 spam and nine impersonation attacks for the average user. Spam jumped in the first quarter of 2024, surging by 13% from the previous quarter (Q4 2023) and by 24% from the same quarter in 2023. While spam dropped off in Q2 2024, the category remained 12% higher than the previous year. Impersonation attacks held steady quarter-to-quarter, rising only slightly in the first two quarters of 2024 — 5% and 6%, respectively — compared to the same quarters a year earlier.

Non-spam, non-impersonation attacks reveal some interesting trends (see Fig 2b). Attackers continued to shift their strategy for payloads from email attachments to malicious links as the initial payload in their messaging attacks. Malicious links surged by 133% in the first quarter—more than doubling—and 53% in the second quarter compared to a year earlier. The average Mimecast user account encountered a third fewer links in Q2 compared to Q1, but the decrease is more likely due to the massive surge in the first quarter. Both known malware (blocked by antivirus defenses) and unknown malware (identified and blocked by sandboxing) dropped significantly compared to a year earlier, by 36% and 54% in the first quarter and second quarters, respectively.



VIEW YOUR REGION



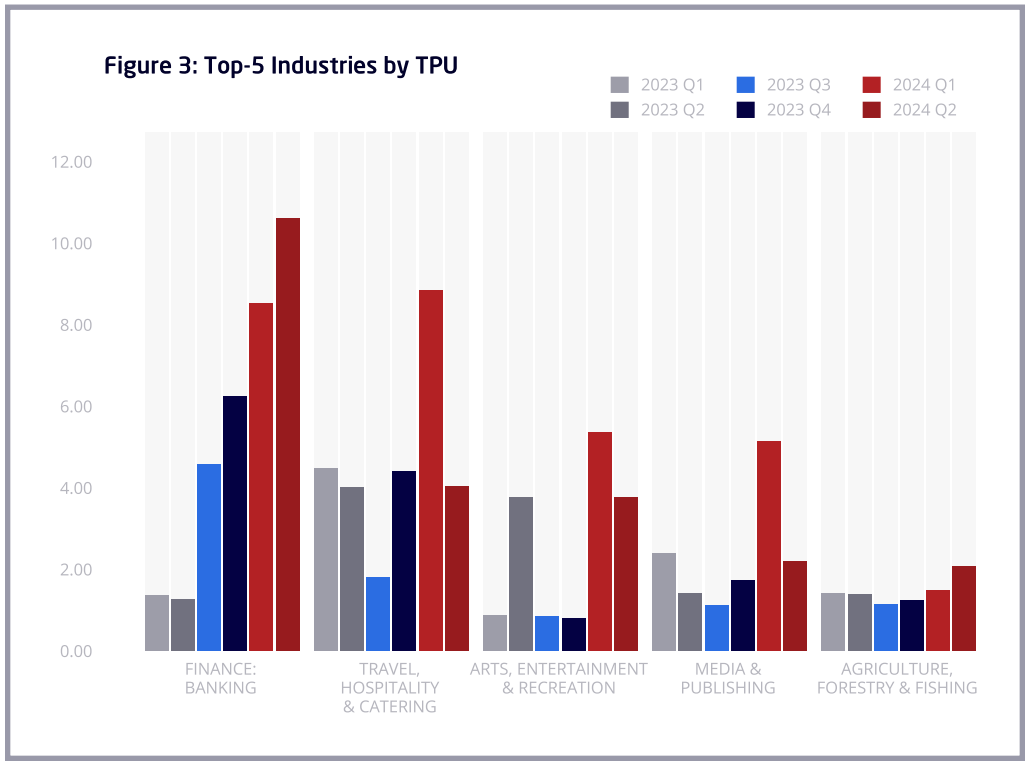
VIEW YOUR REGION

Chart three

Top Industries by TPU

The top targeted industries in the first half of 2024 were banking, travel & hospitality, and arts & entertainment, which saw 19, 13, and 9 attacks per user on average, respectively, discounting spam and impersonation attacks, which tend to dominate the threat picture. Overall, malicious URLs were the most prevalent, accounting for roughly 10 times more attacks than known malware and about 100 times more attacks than unknown malware.

In Q2 2024, users in the IT consulting and legal professional services sectors were targeted with a significant number of impersonation emails, with 208 and 56 messages per user blocked by Mimecast's services, respectively. Users in the scientific & technical, legal professional services, and IT consulting industries were targeted with the most spam, with Mimecast systems blocking more than 20 attacks per user on average.



VIEW YOUR REGION

Chart four

File Share Abuse Trends

Attackers continued to increase their use of links to deliver payloads to their victims, with the domain evernote.com the top abused file share for the first half of 2024, like the final quarter of 2023. Use of Google's file sharing services surged in the first quarter of the year, resulting in it taking second place, beating out sharepoint.com

As discussed in section 3 — Impact of Attack Type on TPUs — above, threat actors are increasingly favoring links to direct victims to phishing pages, drive-by download sites, and credential-stealing fakes. A scattered approach been taken to the use of file sharing sites that are not traditionally utilized for file hosting to further obfuscate their intent.

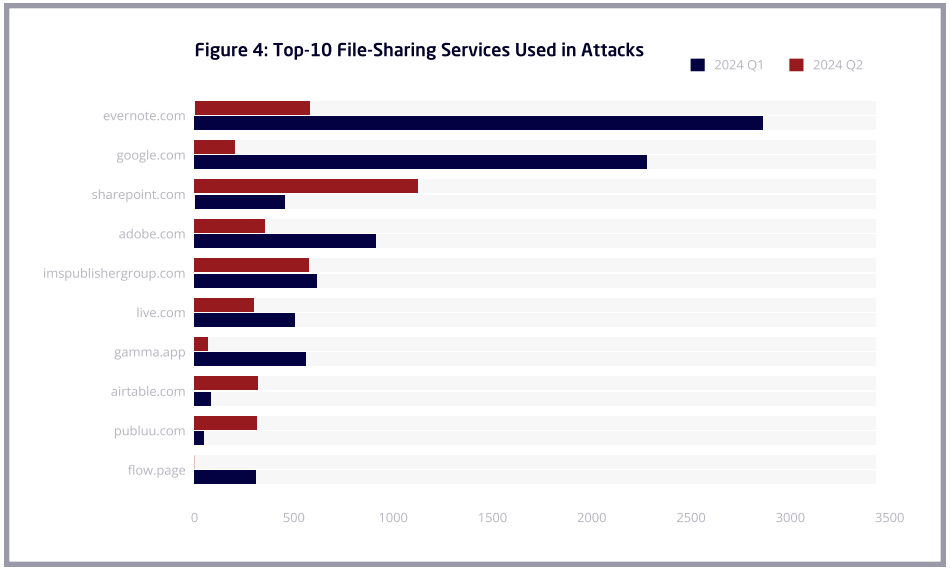
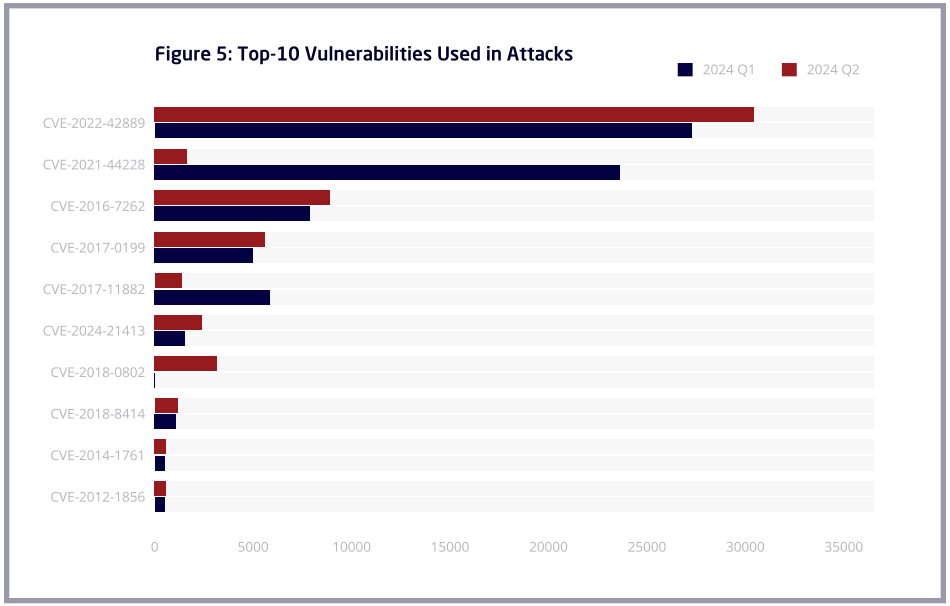


Chart five

Top Vulnerabilities Over Time

Most malicious code came from five exploited vulnerabilities, with a critical vulnerability in the Apache Commons Text library (CVE-2022-42889) taking the award for the most exploitation attempt, experiencing more than double the number of detections than the next most popular vulnerability. The second most popular (CVE-2021-44228) is one of the infamous Log4J2 vulnerabilities, which attackers used almost exclusively in the first quarter.



Major Campaigns Targeting Mimecast Users

3

TARGET Chemical & pharmaceutical companies
PAYLOAD Link leading to ransomware

01 BlackMatter Surge

Between April 23 - 25

An email campaign predominantly affecting chemical and pharmaceutical industry scientists and academic researchers targeted nearly 6,000 Mimecast customers. Since December 2023 all other individual ransomware signature detections have numbered in the region of 1,831 or less. The anomalous spike of nearly half a million detections has been associated with the BlackMatter ransomware-as-a-service (RaaS) group.

However, BlackMatter shut down in 2021and its source code subsequently used by other groups, such as LockBit 3.0 and Kasseika. Given previous leaks of ransomware source code and its reuse in other families of ransomware[10], Mimecast threat researchers gauge it highly likely that parts of BlackMatter's ransomware code is currently in active use by other groups and affiliates.

10. Lockbit 3.0 has BlackMatter ransomware code, wormable traits Tech target. Alexander Culafi. 30 Nov 2022

TARGET Opportunistic **PAYLOAD** An obfuscated LinkedIn link leading to malicious content

02

LinkedIn Redirect Abuse

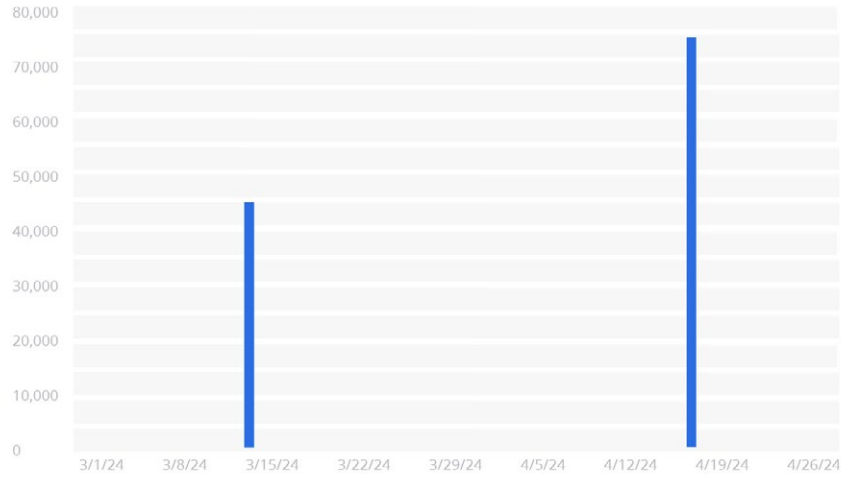
Between March and April

Two major campaigns between March and April 2024 targeted recipients with emails containing a special link to a LinkedIn domain that, if clicked, would redirect the victim to static — but malicious — content. The attack isn't a traditional open redirect, but a link constructed by an attacker using LinkedIn's ability to link to static content.

Mimecast detected at least 117,000 emails using the technique, with both campaigns notifying the recipient that they have an audio message for review. Clicking on the link, however, results in a chain of redirects that leads to a Cloudflare CAPTCHA verification page, and finally to a fake Microsoft Outlook sign-in page. The attackers also used an Amazon Simple Email Service (SES) account —a commonly abused service—giving the emails a greater probability of passing email security detections, such as SPF, DKIM and DMARC.

READ ARTICLE

hxxps://www.linkedin[.]com/redir/redirect?url=https%3A%2Flookerstudio%2Egoogle%2Ecom%2Fs%2FscrHqwjeA3k&urlhash=dcQj&trk=public_profile-settings_topcard-website



TARGET Beverage & construction industries **PAYLOAD** A phishing link embedded in an email leading to a file-sharing site

03

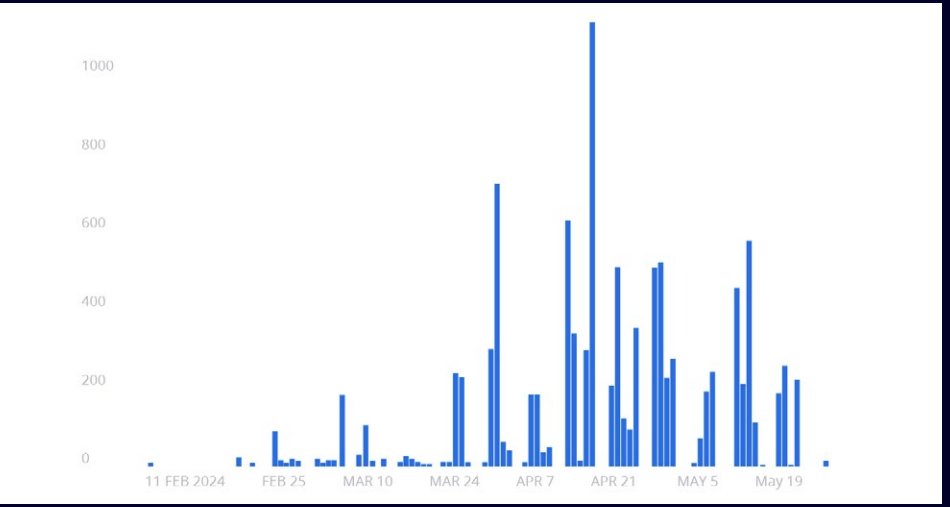
SharePoint/Google drive folders used as evasion technique

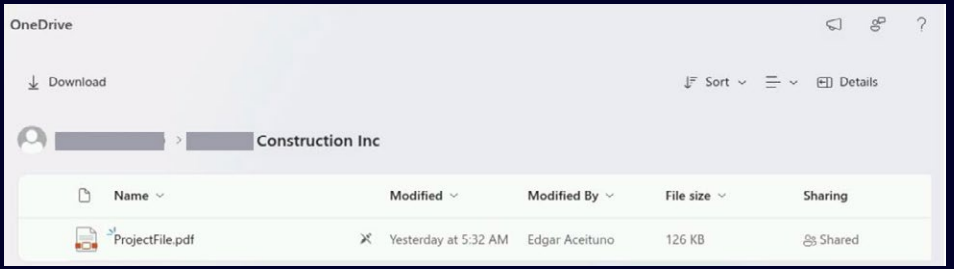
Between February and March

Attackers are using SharePoint and Google Drive to host malicious documents that appear to be bids for projects or invoices for services. The campaigns used compromised Office 365 accounts from companies in the same industry, increasing the likelihood that the target will consider the email legitimate.

Clicking on the document sends victims to a Microsoft credential harvesting page that was created with the Nakedpages phishing kit. Error information on one page refers to an I2P proxy, a privacy-focused network layer that allows for anonymous communication, which may indicate that the kit has a facility for exfiltrating data or communicating anonymously.

READ ARTICLE





TARGET Corporate employees **PAYLOAD** A malicious PDF document with an HTML file extension

04

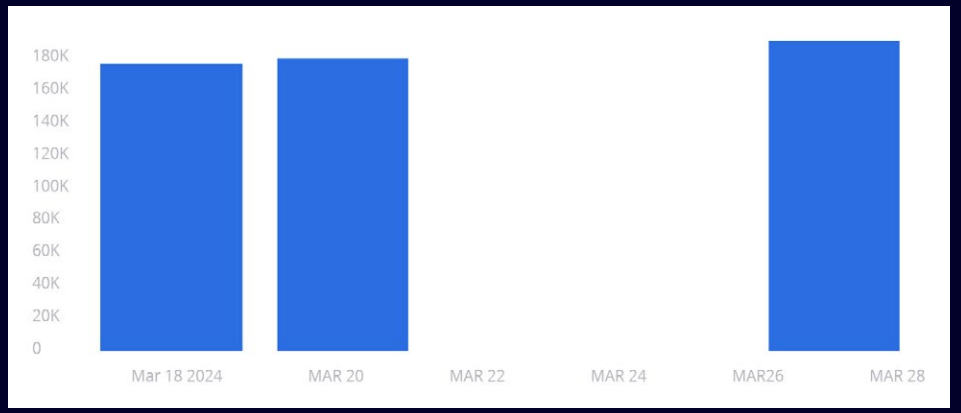
Using online AI tools as campaign infrastructure

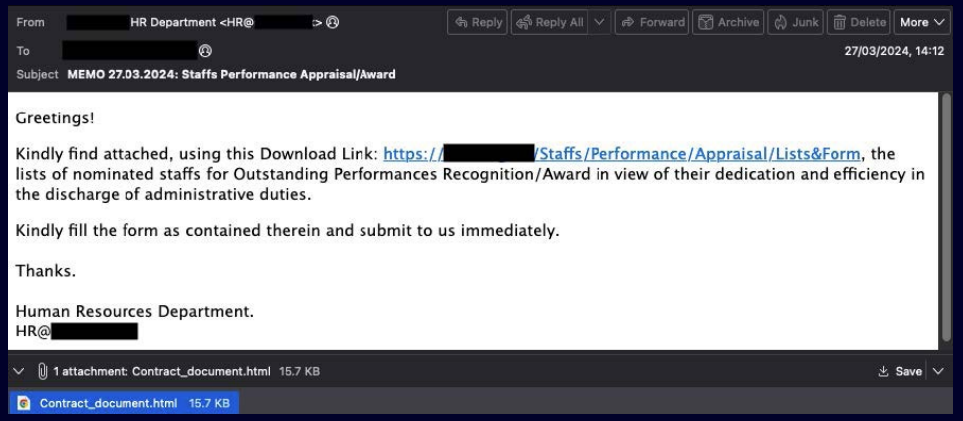
On three days in March

Attackers sent 380,000 emails through the Mailgun mass-mailing marketing service with an attached PDF document ending in an HTML file extension. Clicking on the file opens the PDF in the recipient's web browser, and displays two links to another page hosted on the Replit AI development service.

In each campaign, the attackers generally posed as internal HR teams distributing updates on employee performance appraisals, annual leave policies, or mandatory training. The final landing page is a credential-stealing page disguised as a Microsoft Outlook portal.

READ ARTICLE





TARGET Prominent Australian law firms **PAYLOAD** Links to intermediate stages on platforms, such as Atlassian, Archbee, and Nuclino

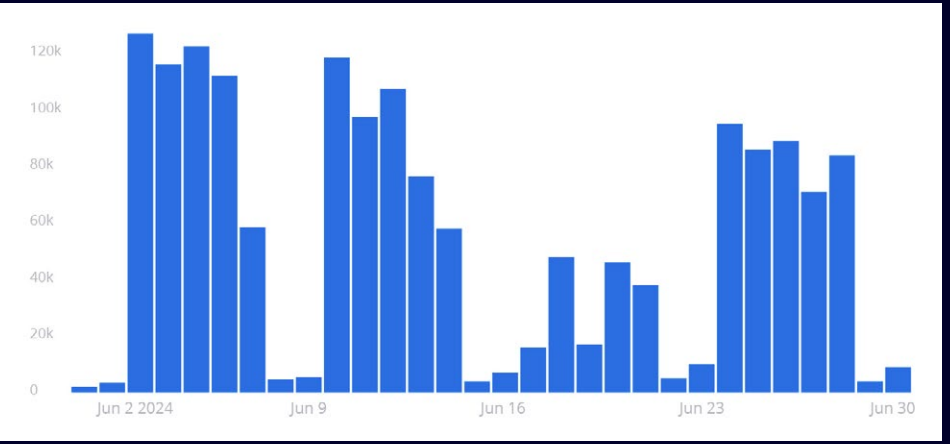
05

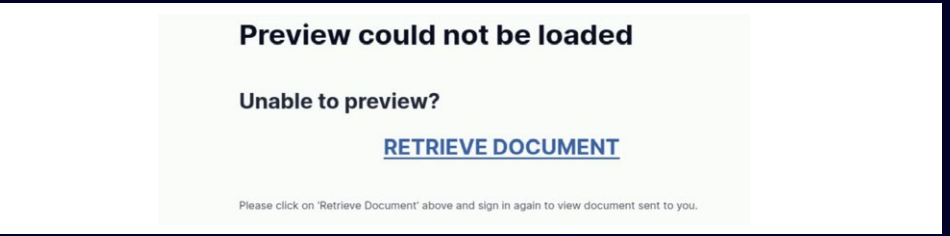
Abusing Atlassian, Archbee and Nuclino workspaces

Between May and June

A prolific campaign used obfuscated URLs in email messages to send users who clicked on the links to an intermediate page on one of several collaboration platforms, including Atlassian, Archbee, and Nuclino. The lure email in the campaign appears to come from an internal team claiming that the recipient's device is out of compliance and includes some detailed information about the user's system.

Like many modern campaigns, clicking on the link in the email will result in the victims clicking through a redirection chain. The destination is also common: a fake login page for Microsoft Outlook.





READ ARTICLE

TARGET Consumers **PAYLOAD** A variety of fake invoices, including a phone number to an AI-powered call center

06

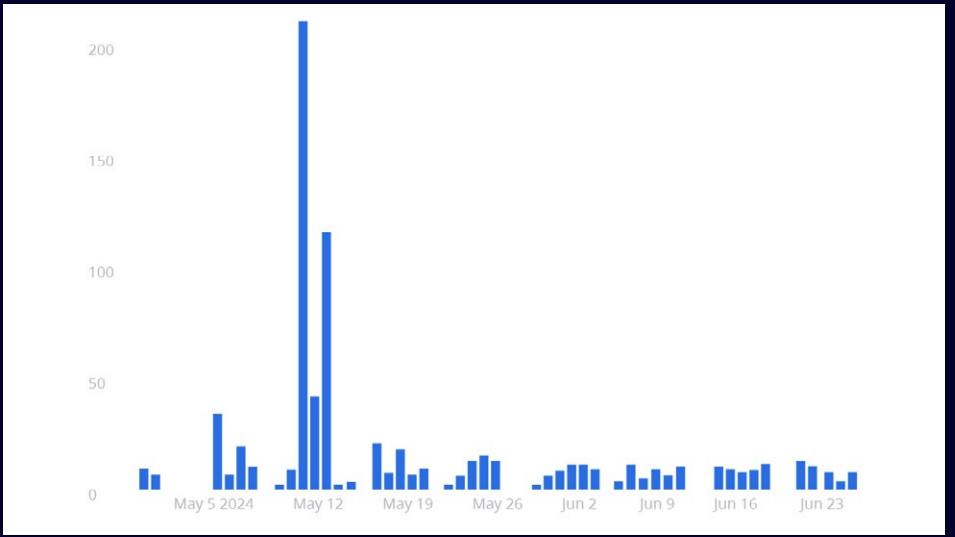
Email scams backed by AI bot call centers

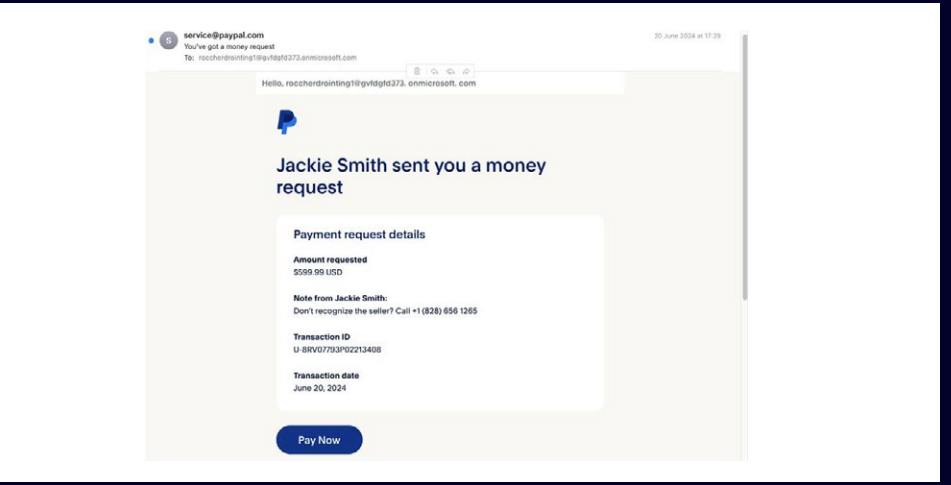
In May

Using Microsoft distribution lists—which allow for mass-emailing in a way that passes several email security checks, such as SPF and DMARC—attackers create messages that appear to notify the recipient of an imminent deduction or charge. Calling the phone number connects the user to a call center — increasingly automated by a large language model (LLM) — that collects the information desired by the fraudster.

In May, Mimecast detected more than 1.6 million email messages in this type of campaign targeting consumers.

READ ARTICLE





Recommendations

Threat-specific countermeasures

1

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 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 flag.

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

2

Segment the network and 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.

3

Harden user credentials, deploy MFA

Many malware 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. Requiring multifactor authentication can drastically reduce compromise of stolen accounts or credentials.

4

Provide awareness training

Humans are at the heart of an organization's systems, and therefore introduce human error into daily operations. If staff are made aware of cyber risks and how to identify them, this forms the first line of defense against many attacks, including those that leverage email.

5

Mandate more security from third parties

Attacks against businesses in the manufacturing, transportation, storage & delivery, and retail & wholesale sectors represent significant third-party risk of supply-chain compromise.

Companies 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 using external rating services and subjecting acquisitions to extra scrutiny.

6

Scan external network for open ports

Organizations should regularly scan their infrastructure for known exploitable routes, such as insecure open external network ports or public cloud environments. Using tools like Cloud Security Posture Management, companies can quickly identify misconfigurations in their public cloud. This will ensure that any publicly accessible server ports are closed or adequately secured and protected.

As an example, Mimecast has noted continuing increases in attacks against remote desktop protocol (RDP) ports, which account for 80% of effective ransomware compromises. Attackers will continue to look for open RDP ports to target organizations.

Best Practices and Advisories

31 JANUARY 2024 **US Cyber Command, CISA, FBI, ONCD**	**Hearing on CCP Cyber Threat** REFERENCE	The top cybersecurity officials for the United States voiced concern over the increase in activity of Chinese cyberthreat actors in the Asia-Pacific region, in particular the pre-positioning of compromises in critical infrastructure throughout the region. A China-linked actor, Volt Typhoon, has conducted attacks in the region starting as early as 2021.
14 FEBRUARY 2024 **Microsoft and Open AI**	**Staying Ahead of Threat Actors in the Age of AI** REFERENCE	Threat actors, including cybercriminals and nation-state adversaries, are experimenting with LLMs at various stages of the attack chain, including translation of text, making messages sound more business-like, and as a way to automate reconnaissance. APT groups known to be testing Open AI's ChatGPT for such efforts include the Russia-linked Forest Blizzard, the North Korea-linked Emerald Sleet, the Iran-linked Crimson Sandstorm, and the China-linked Charcoal Typhoon and Salmon Typhoon.
29 MARCH 2024 **CISA**	**Reported Supply Chain Compromise Affecting XZ Utils Data Compression Library, CVE-2024-3094** REFERENCE	An attacker successfully convinced a developer to accept updates to the open-source project, XZ Utils, which in reality was a backdoor into any system running the software. Spending years gaining the trust of the project maintainer, the backdoor was weeks away from being merged into major Linux distribution when a Microsoft developer discovered the code and notified the community.

2 APRIL 2024 **CISA**	**Cyber Safety Review Board Releases Report on Microsoft Online Exchange Incident from Summer 2023** REFERENCE	The report, the third incident reviewed by the Cyber Safety Review Board (CSRB), analyzes the May 2023 intrusion into Microsoft Exchange Online by Storm-0558, a hacking group linked to the People's Republic of China and considered the perpetrator behind Operation Aurora in 2009 and the RSA SecureID compromise in 2011. The attack exposed email accounts in the U.S. Department of State, U.S. Department of Commerce, U.S. House of Representatives, and 22 other organizations. The CSRB outlined recommendations for Microsoft in particular, cloud service providers in general, and cloud customers.
2 MAY 2024 **FBI, State, NSA**	**North Korean Actors Exploit Weak DMARC Security Policies to Mask Spearphishing Efforts** REFERENCE	In a common tactic among nation-state actors, North Korean cyber actors conduct spearphishing campaigns targeting journalists, academics, and policy officials who are subject matter experts in East Asian affairs. The activity — linked to the Kimsuky or Emerald Sleet actor — targets organizations with weak Domain-based Message Authentication, Reporting and Conformance (DMARC) mail policies to elude detection.
26 JUNE 2024 **CISA, FBI, ACSC**	**Exploring Memory Safety in Critical Open Source Projects** REFERENCE	These government groups have urged open-source software projects and their user bases to move to memory-safe programming languages. More than half of all lines of code (55%) are written in non-memory safe languages, and even projects written in memory-safe languages rely on components that are unsafe.

Mimecast recommendations/checklist

This highlighted section gives Mimecast users specific and actionable steps to protect their users from the threats in the report, with medium-level technical details.

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**

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**

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**

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**

Auto-Allow Policies

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. **Read more**

SIEM and XDR vendors

Utilize pre-built integrations with the majority of SIEM and XDR vendors to provide log capture and analysis for security policy enforcement. **View Integrations**

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**

End user reporting

It is recommended for end users to report potentially malicious messages received through Mimecast user tools to the Mimecast SOC for additional analysis. **Read more**

5 Conclusion

The evolution of the threat landscape continues to challenge cyber security teams, as the cloud-based digitalization of business operations has expanded. This situation has led to ransomware attacks, complex digital supply chain compromises, embedded vulnerabilities, and an increase in attacks on identification systems.

Overall, many of the trends hinted at in the last year became more apparent in the first half of 2024. Malicious links continue to become the preferred way for threat actors to deliver payloads to victims' systems. Employees at small and medium businesses continue to see more than twice the number of threats compared to users at large enterprises. And legitimate file-sharing services continue to be abused by bad actors.

Meanwhile cybercriminal groups continue to ramp up their activities. The impact of the significant law enforcement activity against prominent groups such as LockBit are likely to have resulted in a short-term dip in malicious activity, which is expected to return to normal levels later in the year.

In the near term the future holds some predictable challenges. As companies further migrate into the cloud and develop their infrastructure, the overall attack surface will expand. Ensuring new infrastructure is securely configured, and where possible, monitoring is in place, will assist facing this challenge.

Growing dependency on datasets within cloud storage means security is often outside the owner's control, while the inherent reliance on third-party software and infrastructure will make supply chain security a major problem.

In the face of continued ransomware attacks maintaining data availability is a key to successful business outcomes, as business interruption or denial of service becomes most costly to business reputation and service delivery. Backups are already increasingly targeted and require security focus to ensure they remain in a secure environment.

The human in the loop has always been a factor in identifying risks to an organization as they provide more direct access to relevant information or to a network. Targeting employees remains a highly successful attack vector and unlikely to change as a highly adaptable tactic.

The abuse of generative AI and machine learning will improve the targeting and content of phishing campaigns, driving the defender's requirement for technical indicators to be able to detect and respond to new and novel attacks.

mimecast

Mimecast is a leading AI-powered, API-enabled connected Human Risk Management platform, purpose-built to protect organizations from the spectrum of cyber threats. Integrating cutting-edge technology with human-centric pathways, our platform enhances visibility and provides strategic insight that enables decisive action and empowers businesses to protect their collaborative environments, safeguard their critical data and actively engage employees in reducing risk and enhancing productivity. More than 42,000 businesses worldwide trust Mimecast to help them keep ahead of the ever-evolving threat landscape. From insider risk to external threats, with Mimecast customers get more. More visibility. More insight. More agility. More security.

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.

Keep up to date from notifications to reports & regional webinars:

Mimecast Threat Intelligence Hub

Understand the largest cybersecurity gaps:

State of Email and Collaboration Security Report 2024