mimecast

RISK RADAR

THREATS IN FOCUS

INDUSTRY SNAPSHOTS

RECOMMENDATIONS

MEET THE RISK RADAR SQUAD

THE GLOBAL THREAT INTEL REPORT 2025

01.

INTRODUCTION

In the first nine months of 2025, Mimecast processed more than 24 Trillion data points for its nearly 43,000 customers, flagging more than 9.13 billion threats during the nine-month period. The data reveals trends, including greater usage of trusted services, the preferred attacks against specific industries, and signs of AI usage among cyber threat groups. To best defend business systems, companies need to be aware of what techniques attackers are employing.

In our 2025 Global Threat Intelligence report, Mimecast has collected threat data from across our platform, focusing on the risks posed by business communications, collaboration environments, and workers. Along with insights from our intelligence analysts and open sources, this threat report aims to take vitals of the global threat landscape.

DEFENDING AGAINST THESE RISKS REQUIRES REFRAMING CYBERSECURITY AS NOT ONLY A TECHNICAL CHALLENGE BUT A HUMAN AND GOVERNANCE ONE. IN GENERAL, COMPANIES NEED TO FOCUS ON SECURITY HYGIENE, INCLUDING AWARENESS TRAINING AND HARDENING SYSTEMS. WHILE TECHNICAL VULNERABILITIES REMAIN IMPORTANT, THREAT ACTORS INCREASINGLY RECOGNIZE THAT PEOPLE AND UNMANAGED SYSTEMS ARE THE WEAKEST LINKS IN ORGANIZATIONAL SECURITY.

EXECUTIVE SUMMARY

02.

The cybersecurity landscape in 2025 underscores both attackers' persistence and the iterative improvements in attack techniques. Financial platforms, regulatory agencies, and city governments have all found themselves in the crosshairs, and the adversaries range from profit-driven ransomware operators to disciplined state-aligned teams.

Human workers remain the most consistent point of attack, with shadow IT and AI-driven social engineering providing attackers with both new tools and new targets. Social engineering tactics — from business email compromise (BEC) to credential phishing — are evolving into AI-powered operations that are increasingly able to mimic vendors, partners, and employees with credible email chains. Attackers have also further adopted the tactic of shifting communication channels (from email to voice, for example) and of using legitimate online services as the foundation of their offensive infrastructure.

Shadow IT creates blind spots for defenders, allowing exploitation of tools and services outside of organizations' managed security controls. Whether through third-party wallet integrations in financial services or personal collaboration tools in corporate environments, attackers weaponize convenience against organizations. Remote work further compounds this challenge, as employees operate from less secure environments, often with minimal oversight or lack of awareness about their colleagues' identities. Limited visibility enables undetected intrusions until significant damage occurs.

Finally, the rise of generative AI has dramatically lowered the barrier for highly convincing attacks. Threat actors can now automate spear-phishing campaigns, generate synthetic voices and video, and craft messages that evade traditional detection tools. This amplifies the scale and precision of social engineering, turning what were once niche, labor-intensive attacks into scalable operations. As a result, organizations must adapt by ensuring employees are prepared to recognize AI-augmented attacks and by adopting AI internally to improve business workflows and security operations.

03. KEY FINDINGS

01

HUMAN ELEMENT UNDER ASSAULT

Threat actors increasingly target the human link in the attack chain as the most vulnerable element, doubling down on phishing attacks and social engineering with schemes such as ClickFix and AI-augmented phishing attacks.

02

BEC ATTACKS EMBRACE AUTOMATION

Business email compromise (BEC) has become more sophisticated with attackers using automated conversation chains to further the illusion that a worker is communicating with a legitimate vendor and that a senior executive is taking part.

03

MULTI-CHANNEL ATTACK STRATEGIES

Attacks increasingly incorporate a change of communication channels, such as including a phone number for the victim to call in a phishing email, which helps attackers bypass organizational defenses and minimizes visibility into attacks.

04

LEGITIMATE SERVICES WEAPONIZED AT SCALE

Continuing the trend of living off the land, living off trusted services (LOTS) has become more common, with attackers finding new ways to incorporate a wider variety of legitimate services — such as Adobe Pay, DocuSign, and Salesforce — into their attack chains.

05

NOVEL OBFUSCATION METHODS

Attackers constantly adopt new file formats that allow code execution or better obfuscation, such as hiding JavaScript in Scalable Vector Graphics (SVG) files or using QR codes to make it harder for users and security software to verify links.

THREAT ACTORS CONTINUE TO EVOLVE IN 2025, WITH MAJOR CYBERCRIMINALS GROUPS TARGETING A WIDE SWATH OF INDUSTRIES, SUCH AS RETAIL, AVIATION, INSURANCE, TECHNOLOGY, MANAGED SERVICE PROVIDERS (MSPS), AND CRITICAL INFRASTRUCTURE.

RISK RADAR 04.

Social engineering and manipulation of human behavior are increasingly important pages in these cyberattackers' playbooks, as they shift from traditional malware-based attacks to human-oriented tactics targeting messaging and collaboration platforms. Scattered Spider, also known as Storm-0875 or Octo Tempest, is a highly adaptive, well-resourced group that excels at sophisticated social engineering tactics, often impersonating IT teams or help desks. Another group, TA2541, uses virtual private servers to send phishing emails masquerading as requests for quotes and purchase orders, which eventually lead to malicious scripts embedded in files on Google Drive and OneDrive.

These threat actors also embody another shift in tactics: The increase in usage of trusted services as a primary attack vector to deliver their payload and conduct attacks. Trusted services complicate the work of detecting and preventing these threats using traditional security controls. Organizations need to focus on policies, procedures, and user awareness to complement technical security controls and make their workforce more resilient to these human-oriented attacks.

Threat actors have also adopted methods that make reversing their attacks and attribution more challenging. Cyberattackers' increasingly use compromised systems— especially developing technology hubs in Southeast Asia and Africa — to launch their attacks complicating attempts to trace the origin of attacks, as researchers can only track adversaries to these jumping-off points. The ability to use advanced proxy networks, compromised home routers, and common affiliate networks that distribute an attacker's workforce further obfuscates the attribution process.

Despite that, Mimecast collects a trove of data from attackers' attempts to infiltrate and compromise our customers' systems, shedding light on the latest techniques and trends.

THREATS IN FOCUS.

SINCE OUR 2024 REPORT, CYBERCRIMINALS AND RANSOMWARE GANGS HAVE GREATLY EXPANDED THE USE OF TRUSTED SERVICES TO AVOID TECHNICAL DEFENSES THAT MIGHT OTHERWISE BLOCK THEIR ATTACKS — ADOPTING A GREATER VARIETY OF SERVICES AND USING THEM FAR MORE FREQUENTLY.

The constant abuse of these services has now become the de facto standard for attacks: Threat actors use DocuSign, Intuit, and PayPal to send notifications of invoices due with a call-back number to switch the communications channel; they abuse email service providers such as SendGrid and Mailgun to bypass email authentication and block lists; and increasingly, they are rewriting links to foil security solutions that rely on reputations.

While living off trusted services (LOTS) helps attackers bypass technical controls, artificial intelligence has augmented their own attack chain allowing them to create more convincing phishing messages and automated email campaigns that fool the human element. While exploitation continues to be used in a minority of cases, attacks using ClickFix and AI-generated email messages have become the norm.

CLICKFIX

Attackers have increasingly shifted toward exploiting user's trust to bypass technical security precautions. Mimecast has documented the increasing use of the ClickFix technique — a social engineering scam where attackers use fake error messages or verification prompts to trick users into copying and running malicious commands on their own devices. A typical ClickFix attack chain uses website pop-ups or phishing landing pages to urge users to copy-and-paste a script onto the Windows command line or a PowerShell terminal. Doing so typically leads to the installation of infostealers, remote access trojans (RATs), ransomware, and credential stealers.

First detected in March 2024, the use of ClickFix has rapidly proliferated across the threat landscape. Mimecast detected multiple malware campaigns leveraging ClickFix in 2025, which has taken off in popularity, increasing by more than 500% in the first six months of the year. Overall, ClickFix accounted for nearly 8% of attacks reported, second only to phishing.

900,000

DETECTIONS OF THE TECHNIQUE ACROSS OUR CUSTOMERS IN THE UNITED STATES AND THE UNITED KINGDOM.

2M

OF MALICIOUS SVG FILES DETECTED, USING A VARIETY OF SOCIAL-ENGINEERING LURES

CAPTCHAS FOIL THREAT GATHERING

Legitimate and custom CAPTCHA services allow threat actors to both better trick victims and slow threat researchers' ability to detect attacks. By embedding CAPTCHAs on landing pages or within attack chains, threat actors block automated security crawlers and threat analysis tools from accessing and analyzing malicious content, simultaneously taking advantage of CAPTCHA's legitimacy. Sophisticated JavaScript obfuscation further disables functions[1] like right-click or keyboard shortcuts, hampering manual investigation and dynamic analysis by human analysts.

Mimecast data shows that these advanced deceptive techniques are on the rise, with thousands of unique malicious CAPTCHA-protected URLs being detected each month. Most recently, the cybercriminal group Scattered Spider has used CAPTCHAs to foil defensive analysis, with more than 900,000 detections of the technique across our customers in the United States and the United Kingdom.

SVG USAGE ON THE RISE

Phishing campaigns are increasingly exploiting the Scalable Vector Graphics (SVG) format to embed malicious JavaScript and other executable code in seemingly benign images. The malicious SVG files often execute code when opened, redirecting users to phishing pages or malware-download sites. Between mid-February and mid-March, Mimecast detected more than 2 million instances[2] of malicious SVG files, using a variety of social-engineering lures, such as voice messages and multi-step redirections involving fake PDF downloads.

Threat Actors will often also use obfuscation techniques — such as Base64 encoding and encryption — to evade security controls. Techniques such as AutoSmuggle, a tool released in May 2022[3], make hiding JavaScript in SVG files even easier.

Mimecast expects attackers to continue using SVG images, expanding into a wider range of image formats to deliver and exploit systems in the future. There are many novel ways that images can be used, including composite images with QR codes, non-visible code or beacons in a single pixel, or embedded executables.

1. https://www.mimecast.com/threat-intelligence-hub/captcha-obfuscation/
2. https://www.mimecast.com/threat-intelligence-hub/svg-attachment-abuse/
3. https://cofense.com/blog/svg-files-abused-in-emerging-campaigns/

ABUSE OF NOTIFICATION SERVICES

Email notification services are continuing to be abused to deliver malicious content. Instead of using low-reputation infrastructure, threat actors rely on known providers that organizations already trust, including:

- DocuSign
- Adobe Sign
- Intuit
- PayPal
- HelloSign

The abuse of trusted notification services such as PayPal, DocuSign, and Intuit is a rapidly growing and significant threat to organizations. Attackers increasingly leverage these essential workflow tools to deliver malicious emails that blend seamlessly with legitimate business communications, making detection by both users and security systems extremely challenging.

This trend is marked by a high dependency on trusted notification platforms, which are exploited for a range of attack techniques including:

Business Email Compromise (BEC) scams that use minimal content in the notification body and request a callback to a threat actor-controlled number, enabling further social engineering.

Phishing links and QR codes embedded within files hosted on these notification services, directing victims to credential harvesting sites or malware.

Large-scale callback operations that combine notification services with other platforms, such as Microsoft SRS, to reach a wide array of targets and increase the likelihood of successful compromise.

USAGE OF REMOTE MONITORING AND MANAGEMENT

Threat actors are increasingly turning to legitimate Remote Monitoring and Management (RMM) tools—such as ScreenConnect (ConnectWise), TeamViewer, AnyDesk, and LogMeIn—to gain initial access to victim computers. This marks a significant shift from traditional tactics that relied on delivering malicious files or attachments via email. By abusing trusted RMM software, attackers can bypass many security controls, as these tools are commonly used by IT teams and their presence often does not raise immediate suspicion. Instead of sending malware-laden attachments, attackers now use phishing emails or social engineering to trick users into installing these legitimate RMM agents, granting remote access without triggering standard security alerts.

READ MORE

CHANGE OF COMMUNICATIONS CHANNEL

Another significant trend this year is the increasing use of multi-channel attacks, where threat actors initiate contact with victims through email and then transition to phone communication to further their schemes. In campaigns such as Business Email Compromise (BEC), phishing, and malware distribution, attackers start with a convincing email—often impersonating executives, IT staff, or trusted vendors—to establish a plausible scenario or sense of urgency. Once initial contact is made, they follow on to phone communication. This approach is highly effective because it leverages the personal and immediate nature of voice communication, making victims more likely to comply with requests to visit malicious websites, make fraudulent payments, or download malware.

The transition from email to phone allows attackers to bypass traditional email security controls and exploit psychological tactics such as authority, urgency, and familiarity. During the phone call, attackers use real-time persuasion, answer questions, and address doubts, which reduces skepticism and increases the likelihood of victim compliance. This method has been observed in high-profile attacks, including executive impersonation and IT support scams, and is further amplified by the use of AI-generated voices and deepfake technology. The result is a more convincing and harder-to-detect attack chain, making this email-to-phone transition a major area of concern for organizations in 2025.

THE THREAT LANDSCAPE IN CHARTS.

THE TELEMETRY FROM MIMECAST SECURITY SERVICES HIGHLIGHTS TRENDS IN ATTACKER BEHAVIOR.

Not only are threat actors increasingly using trusted services as the foundation for their campaign infrastructure, but the detection shows signs that attackers are increasingly using AI-generated messages to create more phishing attacks[4].

Data from various industries shows the most commonly faced threats, from impersonation attacks on the Professional Education sector to phishing attacks against Real Estate brokers and malware targeting Manufacturing.

MIMECAST ANALYZED TRILLIONS OF DATA POINTS ANONYMOUSLY ACROSS CUSTOMERS TO GAIN INSIGHT INTO THE LATEST TACTICS AND TECHNIQUES BEING USED BY THREAT ACTORS.

[4] https://www.mimecast.com/blog/how-chatgpt-upended-email/

01 LIVING OFF TRUSTED SERVICES (LOTS)

Threat actors continue to weaponize legitimate business services to bypass security controls and exploit organizational trust relationships. Beyond notification services, attackers exploit a broader ecosystem of trusted platforms to host malicious content and redirect victims. These campaigns leverage established providers that organizations already trust, including:

- SendGrid or Salesforce CRM for email delivery,
- SharePoint or Google Drive for hosting, and
- Cloudflare for CAPTCHAs.

PHISHING NOW ACCOUNTS FOR 77% OF ALL ATTACKS, UP FROM 60% IN 2024, LIKELY DUE TO ATTACKERS USING AI TO DRAMATICALLY INCREASE PHISHING VOLUME. THE GRAPH BELOW SHOWS THE OBFUSCATION METHODS, PAYLOAD TYPES, AND DESTINATION DOMAINS OF THESE MALICIOUS LINKS.

Virtual meeting room and hosting service DocSend, for example, has become much more popular, rising to become the most abused service in 2025, jumping from the fourth most abused service in the latter half of 2024. Adobe, Google, Microsoft SharePoint, and email marketing service GetResponse were popular ways for attack campaigns to start, while the most popular destination remained DocSend, but other popular ones include “smart link” service Click Magic, a known purveyor of adware, and Google.

Link-rewriting abuse is a tactic where attackers compromise tools that sanitize email links—like secure email gateways—to create safe-looking links with hidden malicious redirects. Since these links come from trusted sources, users and security tools are more likely to trust them, making it harder to distinguish between legitimate and malicious activity.

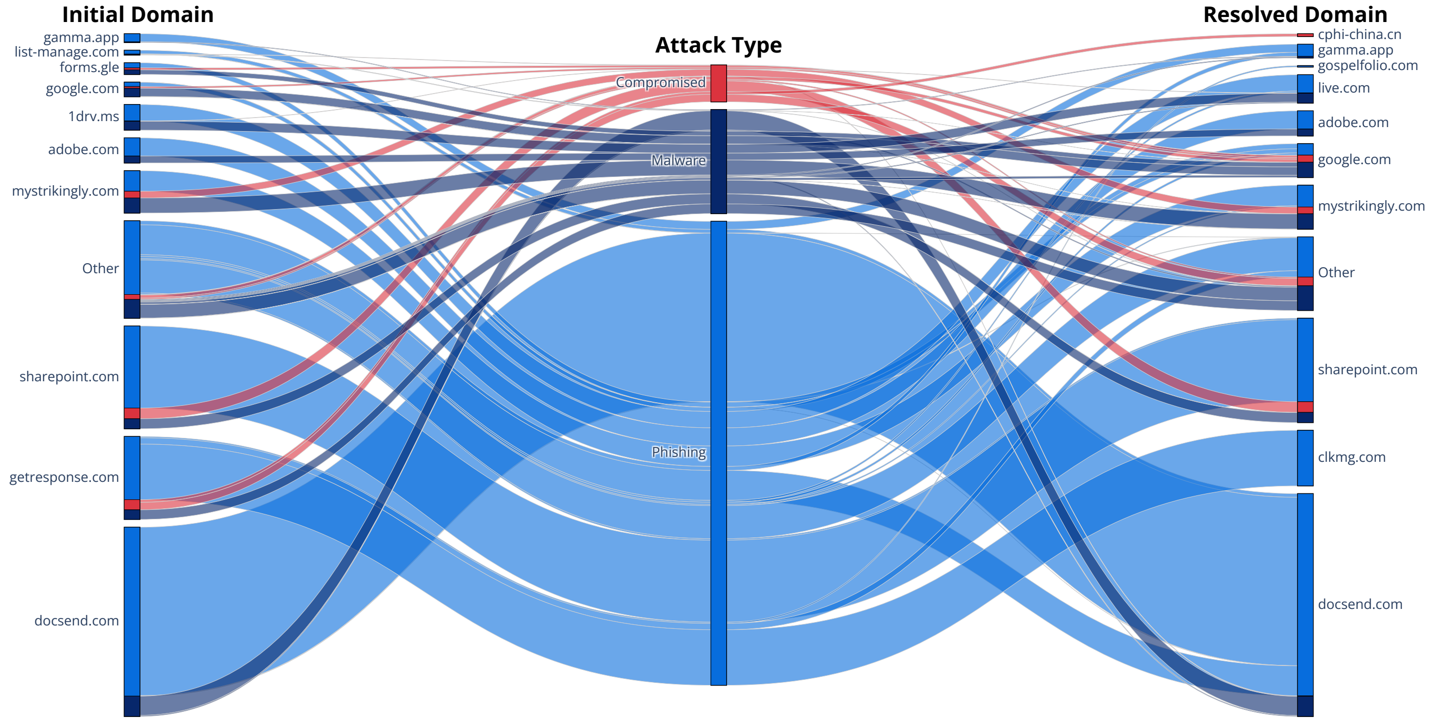
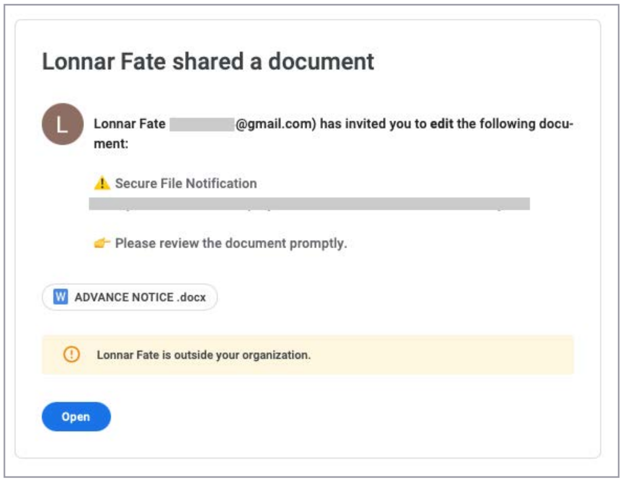


Chart 01: The top legitimate domains used by attackers include DocSend, GetResponse, and Sharepoint, which resolve to pages on DocSend, ClkMg.com, and Microsoft SharePoint.



Lonnar Fate shared a document

Lonnar Fate [redacted]@gmail.com) has invited you to edit the following document:

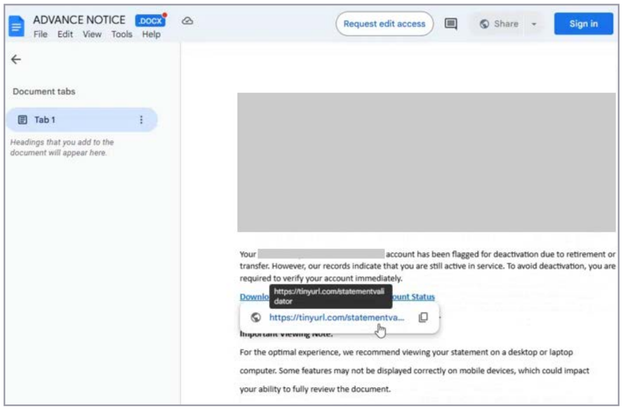
⚠️ Secure File Notification

[redacted]

👉 Please review the document promptly.

ADVANCE NOTICE .docx

Lonnar Fate is outside your organization.



[redacted]

Your [redacted] account has been flagged for deactivation due to retirement or transfer. However, our records indicate that you are still active in service. To avoid deactivation, you are required to verify your account immediately.

Downlo https://tinyurl.com/statementvalidator ount Status

https://tinyurl.com/statementva...

Important Viewing Note:

For the optimal experience, we recommend viewing your statement on a desktop or laptop computer. Some features may not be displayed correctly on mobile devices, which could impact your ability to fully review the document.

CAMPAIGN DETAIL

Malicious campaigns distributed through Google Docs lead victims to files containing obfuscated links. These campaigns employ URL shortening services to disguise the true destination, directing users to websites that automatically download MSI files containing remote monitoring and management (RMM) tools like LogMeIn Resolve Unattended. These legitimate RMM applications have become a preferred initial access vector, allowing attackers to establish persistent remote control over compromised systems while appearing to use authorized business software.

READ MORE

RECOMMENDATIONS

Countering attacks that exploit trusted services requires organizations to move beyond traditional technical filtering and implement comprehensive security hygiene practices. Organizations must align their security controls with actual business operations while preparing for increasingly sophisticated AI-enhanced attacks.

- Create a baseline for business-critical environments to understand normal activity patterns, enabling detection of anomalies when trusted services are misused for malicious purposes and blocking untrusted services.
- Implement least privilege and separation of duty principles to prevent single points of failure across systems and user access.
- Deploy layered security controls that continue protecting when individual defenses are bypassed, rather than relying on isolated defenses, and use multiple detection systems to gain comprehensive visibility.
- Prepare for AI-enhanced attacks that create increasingly authentic-looking messages, making both technical controls and human awareness training critical defensive layers.

#02 COLLABORATION THREATS

Collaboration platforms fundamentally changed communication — and how threat actors operate. The platforms create persistent repositories where nothing truly disappears. When compromised these tools, provide comprehensive organizational visibility, enabling lateral movement and the hosting of malicious content within trusted environments. The persistence of data amplifies risk, as platforms retain years of conversations, credentials, and strategic plans that traditional email systems might purge. This accumulated intelligence allows attackers to build detailed profiles of targets, understand internal processes, identify key personnel, and craft highly convincing social engineering attacks.

Security teams now face the challenge of protecting dynamic, persistent environments where the line between internal and external, trusted and untrusted, continues to blur.

Mimecast threat data sampled from Microsoft Teams, SharePoint and OneDrive environments show that platform threats are mostly malware. Because most enterprise collaboration is among closed groups, spam and phishing tend to be less of a threat, while malware is either inadvertently forwarded attachments and links or self-propagating threats. However when we strip back the malware layer the really interesting data surfaces, highlighting the usage of phishing and untrustworthy links.

INTERESTINGLY, THE TRAINING AND TOOLS CATEGORY CONTAINED THE MOST MALICIOUS CONTENT, WITH 96% OF THE URLS ASSIGNED A CLASSIFICATION OF HIGH OR MEDIUM RISK. IN ADDITION, THE SOCIETY CATEGORY, WHICH INCLUDES POLITICS, HAD A HIGH PROPORTION OF RISKY CONTENT AS WELL.

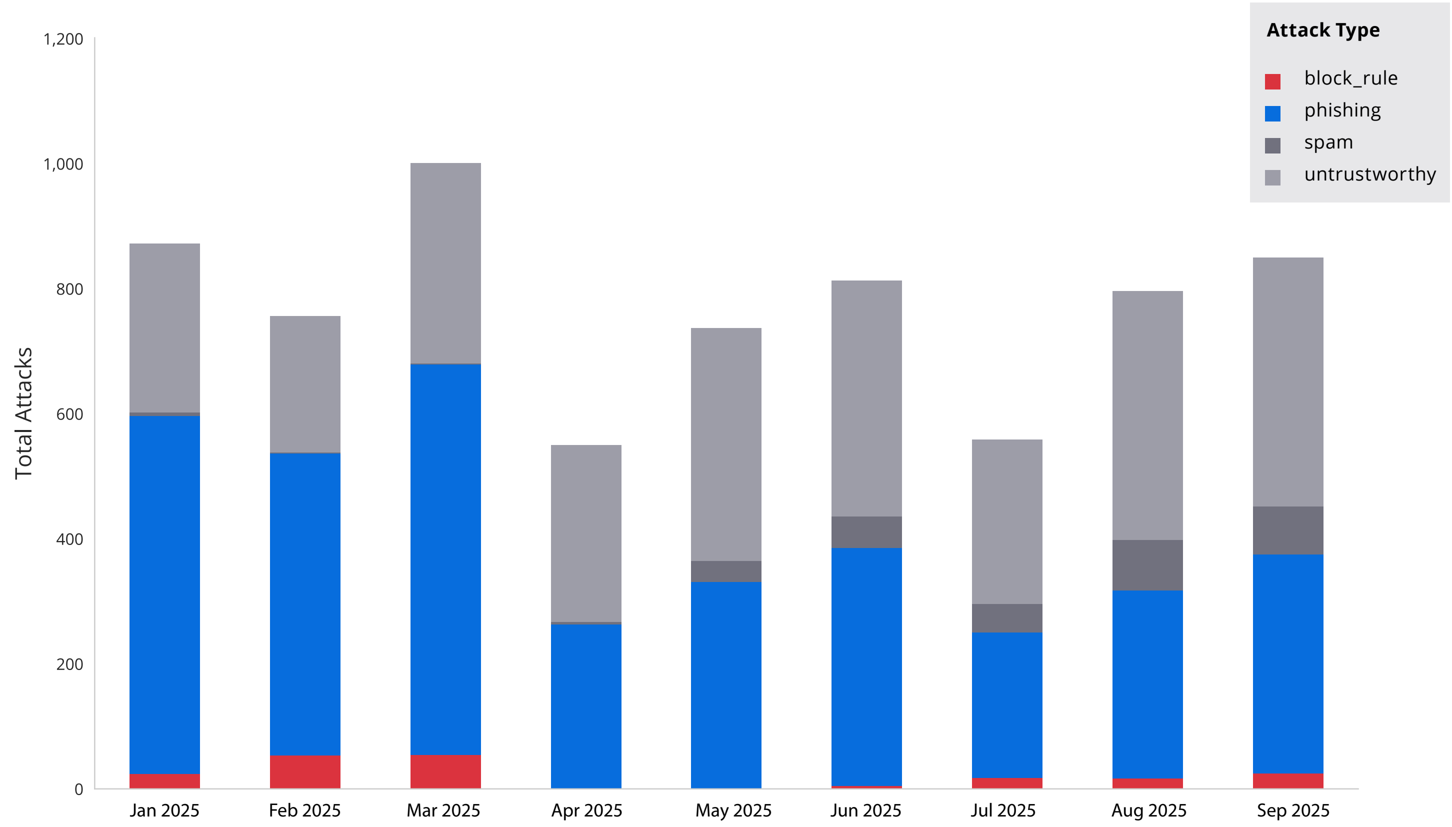
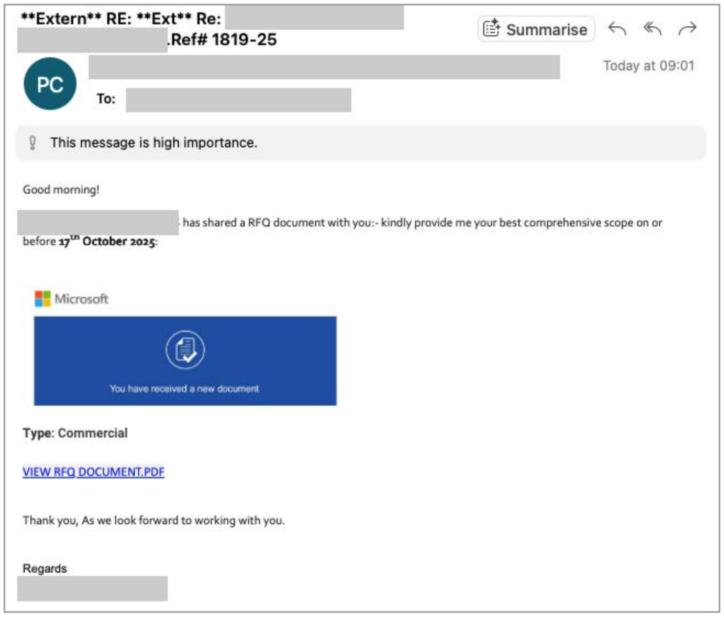


Chart 02: Detections of malware dominate collaboration environments (not shown), while spam and phishing make up the second and third-most encountered threats.

CAMPAIGN DETAIL

Cybercriminals distribute phishing emails disguised as business solicitations, directing recipients to malicious files hosted on SharePoint and Google Drive. These campaigns utilize compromised Office 365 accounts to increase legitimacy and often employ sender domains from industries related to the target organization, enhancing the likelihood of user engagement. The hosted files contain links that redirect to credential harvesting sites designed to capture legitimate login information. By leveraging trusted cloud platforms and industry-specific domains, these attacks bypass traditional email security filters while exploiting the trust relationships organizations maintain with familiar business platforms.

READ MORE



Extern RE: **Ext** Re: [redacted]
[redacted].Ref# 1819-25

[redacted]

Today at 09:01

To: [redacted]

This message is high importance.

Good morning!

[redacted] has shared a RFQ document with you:- kindly provide me your best comprehensive scope on or before 17th **October 2025**:

You have received a new document

Type: Commercial

VIEW RFQ DOCUMENT.PDF

Thank you, As we look forward to working with you.

Regards
[redacted]

RECOMMENDATIONS

Hardening business environments against collaboration platform threats requires comprehensive security measures that address both technical vulnerabilities and human factors. Organizations must implement robust controls that protect persistent data repositories while maintaining the collaborative functionality that drives business operations.

- Train employees on collaboration-specific threats and set clear protocols for secure information sharing across platforms.
- Use human-risk management tools to identify and block malicious links and files in collaboration environments.
- Deploy data loss prevention tools to monitor sensitive data movement and minimize information leakage across collaboration channels.
- Implement phishing-resistant multi-factor authentication and establish governance policies that define acceptable external sharing practices with vendors and partners.

This approach recognizes that collaboration platforms create unique security challenges due to their persistent nature and the valuable organizational intelligence they contain, requiring specialized defensive strategies beyond traditional email security measures.

#03 INDUSTRY SNAPSHOT

Attackers use different techniques against different industries, tailoring their approaches based on what works through experience and understanding of sector-specific vulnerabilities. By calculating the average number of threats detected per user for each industry and attack type, our analysts determined distinct threat profiles that reveal how threat actors adapt their tactics to exploit industry-specific workflows, regulatory requirements, and business practices. To show details of the most significant attacks, detections of spam and emails sent by low-reputation senders have been removed.

The Arts & Entertainment and Manufacturing sectors tend to be targeted by malware more often than other industries — likely due to their valuable intellectual property, complex supply chains, and the potential for operational disruption that ransomware can cause. These sectors often have legacy systems, specialized software that may have unpatched vulnerabilities, and highly privileged users without technical experience, making them attractive targets for malware campaigns.

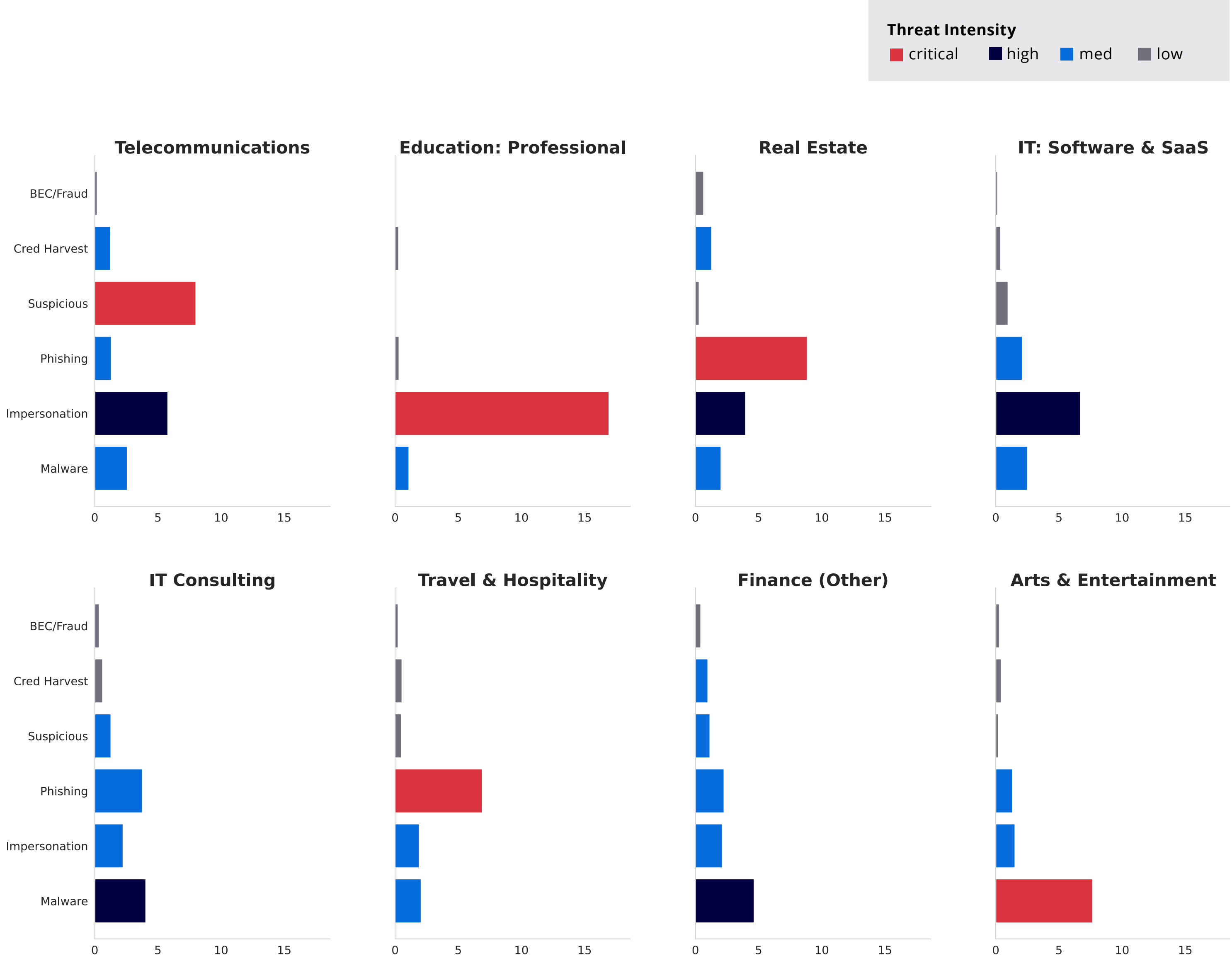
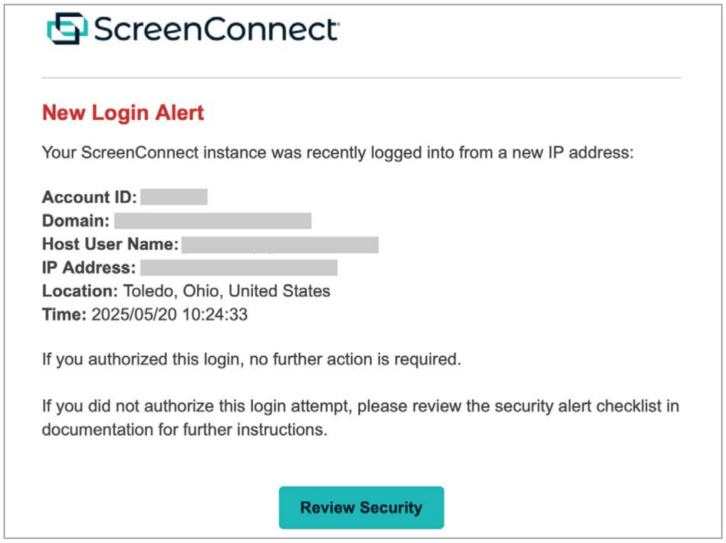


Chart 03: Threats per user (TPUs) for the Top-8 Industries

Workers at real-estate companies encounter significantly more phishing attacks than employees in other industries, driven by the sector's high-value transactions, frequent wire transfers, and reliance on email communication between multiple parties including buyers, sellers, agents, and attorneys. The time-sensitive nature of real estate closings creates pressure that attackers exploit through urgency-based phishing lures. Phishing is also a major threat for the Travel & Hospitality sector.

These patterns demonstrate that attackers conduct reconnaissance not just on individual organizations but on entire industries, developing specialized playbooks that exploit sector-specific business processes and pain points. Understanding your industry's threat profile is essential for prioritizing security investments and tailoring awareness training to the most likely attack scenarios your employees will face.



New Login Alert

Your ScreenConnect instance was recently logged into from a new IP address:

Account ID: [redacted]
Domain: [redacted]
Host User Name: [redacted]
IP Address: [redacted]
Location: Toledo, Ohio, United States
Time: 2025/05/20 10:24:33

If you authorized this login, no further action is required.

If you did not authorize this login attempt, please review the security alert checklist in documentation for further instructions.

CAMPAIGN DETAIL

A sophisticated phishing campaign is targeting the IT Software industry using adversary-in-the-middle (AitM) techniques to capture both passwords and multi-factor authentication (MFA) tokens of super-admin ScreenConnect users. Attackers leverage Amazon's Simple Email Service (SES) to send convincing phishing emails that bypass common security filters. Compromised super admin accounts give attackers full control over remote access infrastructure, enabling malware deployment and data theft.

READ MORE

RECOMMENDATIONS

Industry threat profiles should guide security prioritization, but organizations need comprehensive protection against all attack vectors.

- Align security controls with your industry's primary threat patterns while maintaining broad defensive coverage.
- Use risk-based analysis that accounts for both frequent industry threats and high-impact attacks like business email compromise.
- Implement defense-in-depth and zero trust frameworks as foundational security approaches.
- Tailor awareness training to emphasize attack types most common in your sector.

#04 BEC ATTEMPTS RISING AGAIN

Business email compromise (BEC) threats dropped during late February until early April — representing a temporarily shift to malware-based attacks — but quickly picked up in late spring and throughout the summer. The current BEC landscape shows attackers focusing on wire transfers and using urgent language, employing the classic "we need this money transfer now" pressure tactic — a trend that will gain strength as deepfake voice and video allow attackers to create convincing impersonations of executives during phone calls or video conferences. While requests for gift cards used to be popular, more recent BEC attack vectors focus on payment through fake invoices, bank account changes, payroll updates, and requests for aging reports or other financial information.

Wire transfers and invoice fraud remain the top two mechanisms used in BEC attacks, while help requests and payroll changes are less common. These financial-focused attacks typically involve larger sums and are harder to reverse than gift card scams, making them more attractive to sophisticated threat actors. The chart of tactics associated with BEC campaigns also shows that creating a sense of urgency and changing the communications channel are both increasingly common tactics, with attackers often combining email with phone calls or text messages. Meanwhile, the once popular gift card scam has largely disappeared following increasing awareness of the tactic and improved employee training programs that specifically warn against these requests.

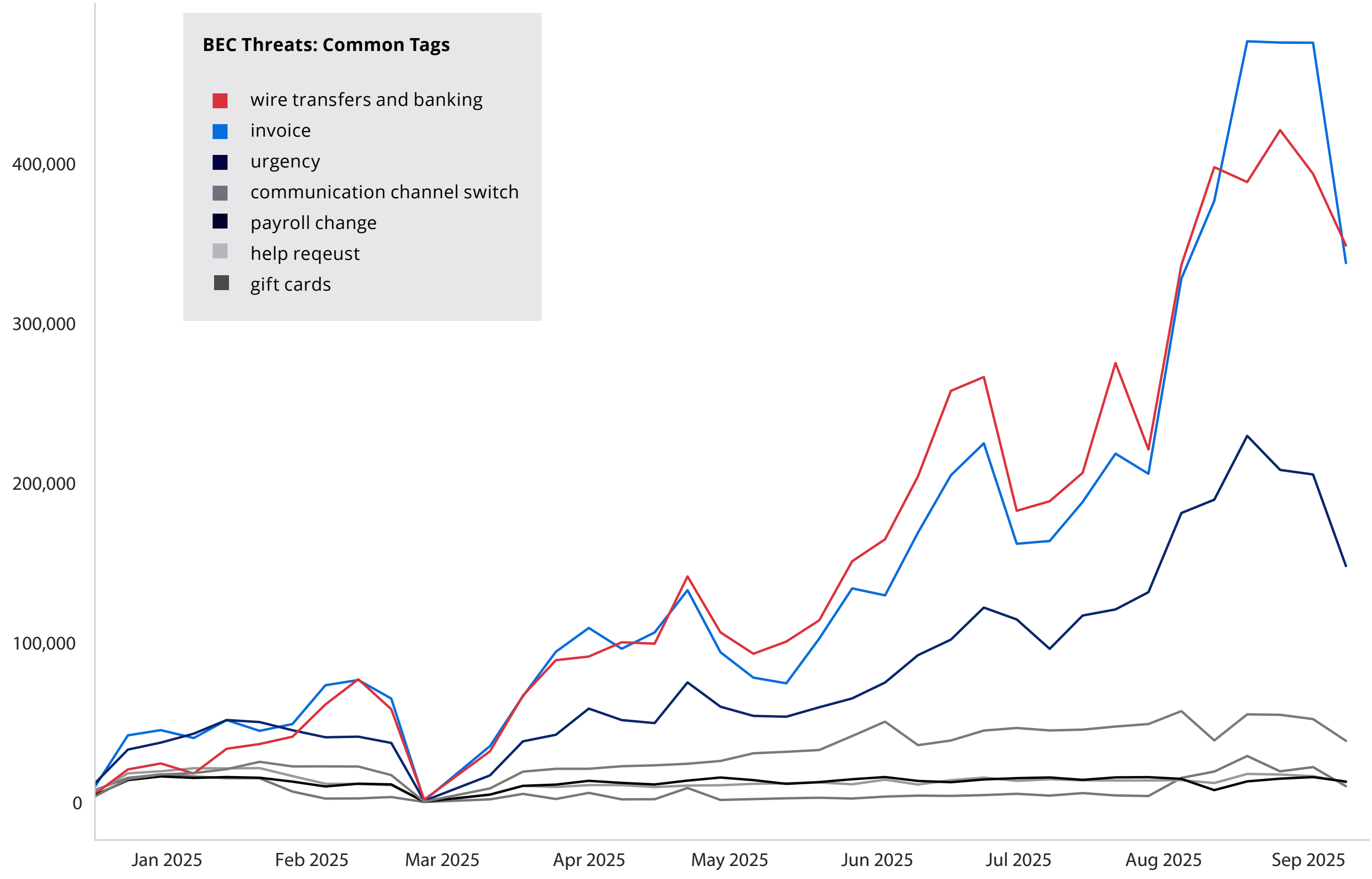


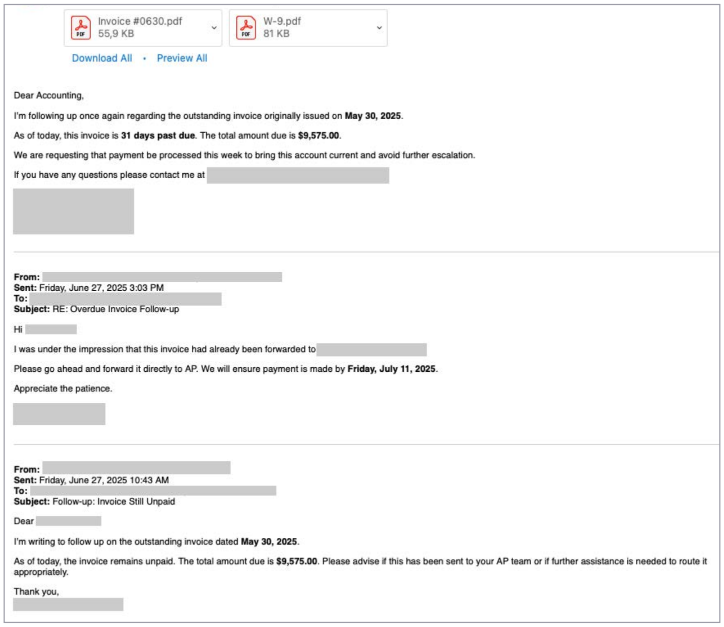
Chart 04: BEC Threats Common Tags Count per Week

CAMPAIGN DETAIL

Cyberattackers continue to refine their BEC attacks, from originally focusing on impersonating CEOs to now impersonating multiple sides of an email chain between a vendor and executives. During reconnaissance, attackers focus on obtaining accounting reports containing financial details like customer names, balances, and accounts payable contacts. These enable attackers to craft fraudulent invoice schemes. At the same time, human resources and payroll data are targeted through social engineering, often under the guise of routine HR processes or urgent business needs. By exploiting both financial and employee information, they increase their chances of successfully impersonating trusted parties and manipulating transactions.

To create the actual email chains, attackers rely increasingly on AI to fabricate the thread of messages between a vendor, the victim, and a purported third party, crafted to appear to be a CEO or senior executive urging quick payment of the invoice.

READ MORE



Dear Accounting,

I'm following up once again regarding the outstanding invoice originally issued on **May 30, 2025**.

As of today, this invoice is **31 days past due**. The total amount due is **$9,575.00**.

We are requesting that payment be processed this week to bring this account current and avoid further escalation.

If you have any questions please contact me at [redacted]

[redacted]

From: [redacted]
Sent: Friday, June 27, 2025 3:03 PM
To: [redacted]
Subject: RE: Overdue Invoice Follow-up

Hi [redacted]

I was under the impression that this invoice had already been forwarded to [redacted]

Please go ahead and forward it directly to AP. We will ensure payment is made by **Friday, July 11, 2025**.

Appreciate the patience.

[redacted]

From: [redacted]
Sent: Friday, June 27, 2025 10:43 AM
To: [redacted]
Subject: Follow-up: Invoice Still Unpaid

Dear [redacted]

I'm writing to follow up on the outstanding invoice dated **May 30, 2025**.

As of today, the invoice remains unpaid. The total amount due is **$9,575.00**. Please advise if this has been sent to your AP team or if further assistance is needed to route it appropriately.

Thank you,
[redacted]

RECOMMENDATIONS

Business email compromise requires both technical controls and strict financial processes to catch unauthorized bank account changes or payment requests lacking proper purchase orders. Company executives should establish secondary communication channels for verifying requests, and privileged employees need regular training.

- Prioritize awareness training as the primary defense against BEC attacks, as attackers may replicate executive communication styles.
- Implement multi-step verification processes before processing any invoice payments or money transfers.
- Establish secondary verification channels that bypass email when confirming financial requests.
- Maintain training programs that emphasize current BEC tactics, as reduced gift card scams demonstrate effective awareness education.

#05 TOP VULNERABILITIES OVER TIME

In 2024, nearly 40,000 vulnerabilities were reported to the National Vulnerability Database (NVD), or about 768 security issues every week. In 2025, the rate is on track to surpass an average of 900 vulnerabilities per week.

Yet volume tells only part of the story - Organizations have almost no chance to individually triage the influx of issues on a weekly basis, and overall, about 8.4% of vulnerabilities are high risk (of high or very high severity, and likely or very likely to be exploited). The remaining 91.6% create noise that makes identifying critical threats even harder.

VOLUME

NEARLY 40,000 VULNERABILITIES REPORTED TO NVD, AVERAGING ABOUT 768 SECURITY ISSUES PER WEEK.

RISK

8.4% OF VULNERABILITIES ARE HIGH RISK THE REMAINING 91.6% ARE LOWER RISK, CREATING SIGNIFICANT "NOISE" THAT COMPLICATES IDENTIFYING CRITICAL THREATS.

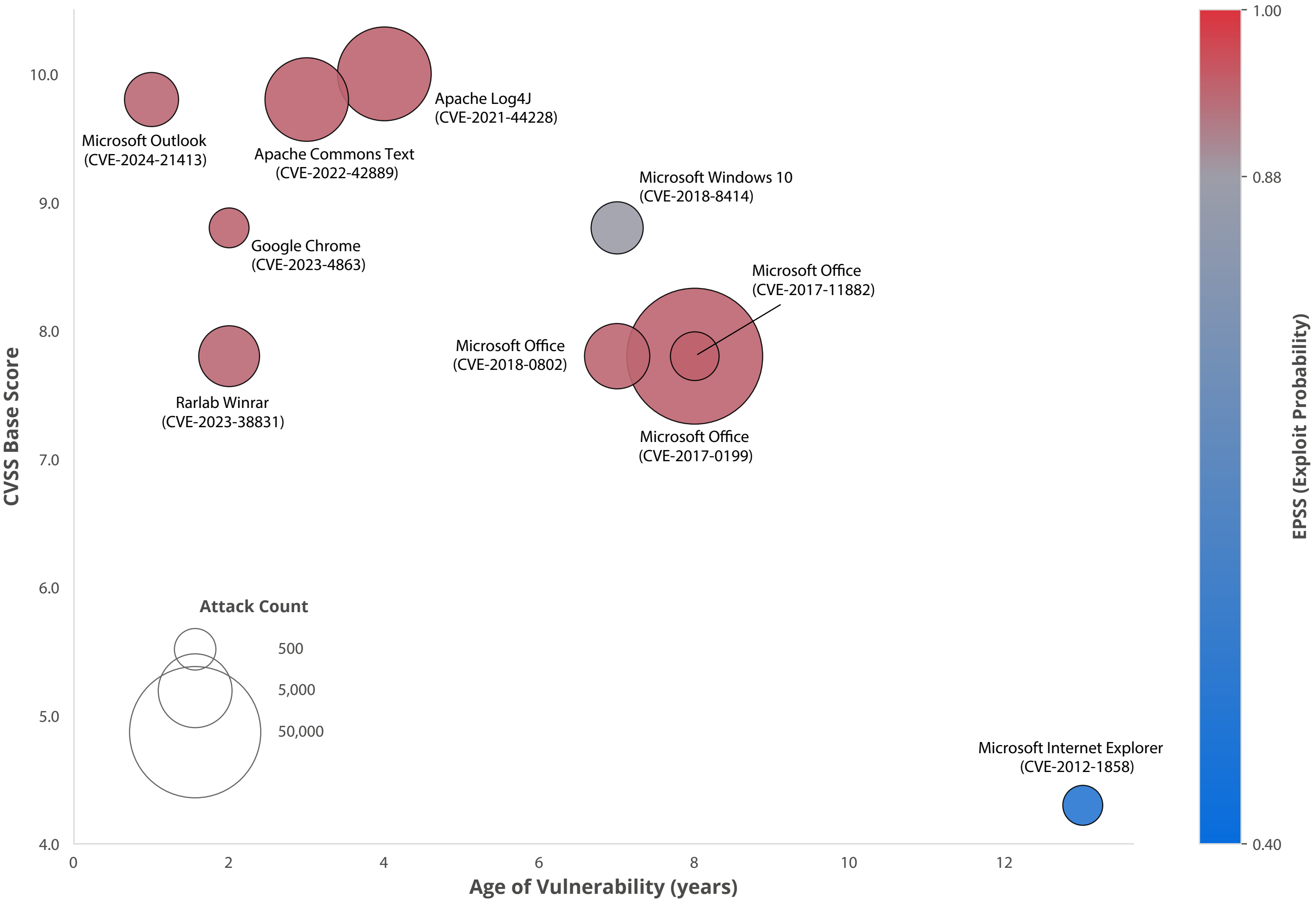


Chart 05: Top-10 Vulnerabilities: Age vs. CVSS (color=EPSS)

No wonder, then, that threat actors continue to exploit software vulnerabilities to gain access to corporate networks and compromise systems. The remediation gap remains alarming:

JAVA FLAWS HAVE A REMEDIATION HALF-LIFE OF 276 DAYS, WHILE VULNERABILITIES IN JAVASCRIPT PROGRAMS HAVE A MEDIAN FIXING TIME OF 163 DAYS. THIS MEANS KNOWN VULNERABILITIES REMAIN EXPLOITABLE FOR MONTHS, GIVING ATTACKERS AMPLE OPPORTUNITY TO WEAPONIZE PUBLISHED EXPLOITS AGAINST UNPATCHED SYSTEMS.

The disconnect between vulnerability disclosure and actual exploitation creates a dangerous window. While security teams scramble to assess each week's new CVEs, threat actors focus on proven vulnerabilities with available exploit code, particularly those in widely-deployed software like Microsoft Exchange, Fortinet devices, and Apache frameworks. Legacy systems compound this problem — patches may not exist for end-of-life software still critical to operations, forcing organizations to maintain vulnerable infrastructure that attackers specifically target.

RECOMMENDATIONS

To minimize the threat of exploitation of software vulnerabilities, companies need to implement a strong vulnerability remediation and attack surface management program that includes the maintenance of a Risk Register to track issues. In addition, companies should seek to prioritize any software security issues using both exploitability and reachability analysis.

- Malware is always a catchup game that you play, because with vulnerabilities, there is always a new one every day.
- Attack surface management and vulnerability management are both important.

MIMECAST CUSTOMERS

THIS BLOG POST SHOWS YOU EXACTLY WHAT TO DO NEXT TO STAY SECURE.

BLOG

TRACKED THREAT ACTOR ACTIVITY.

Cybercrime-as-a-service models — RaaS, PhaaS, and Initial Access Brokers — enable multiple actors to deploy identical infrastructure, making attribution increasingly unreliable. Rather than focus on malware signatures, Mimecast tracks Tactics, Techniques, and Procedures (TTPs) to systematically categorize threats. This approach identifies patterns across campaigns even when traditional attribution fails, providing clearer insight into evolving capabilities. The following profiles highlight the most prolific threat operations detected across our platform, their behavioral patterns, and potential impact.

SCATTERED SPIDER

MCT03050

First observed: 2022
Latest campaign: Aug 2025

GOAL

Credential harvesting, data exfiltration, extortion, and ransomware deployment.

TARGETED

Region

Primarily United States
United Kingdom
but activity is global

Sector

Broad, including retail, aviation, insurance, technology, managed service providers (MSPs), and critical infrastructure.

Scattered Spider is a highly adaptive, well-resourced threat group specializing in advanced social engineering, including phishing, smishing, and vishing, often impersonating IT or help desk staff to gain initial access. The group leverages adversary-in-the-middle (AiTM) phishing kits and fake login portals to capture credentials and session tokens, frequently targeting SaaS platforms and identity providers like Okta and Microsoft Entra ID. They exploit legitimate services and infrastructure, such as trusted email and notification platforms, to deliver phishing lures that evade security controls and appear credible to targets.

READ MORE

UAC-0050 (DAVINCI GROUP)

MCT01025

First observed: 2024
Latest campaign: Aug 2025

GOAL

Information theft, Financial theft, Psychological operations (PSYOP)

TARGETED

Region

Ukraine

Sector

Government ministries, local authorities, the Ukrainian military, and civilians caught in the malspam crossfire, related to the current conflict.

AC-0050 primarily gains initial access through phishing emails. These emails often impersonate Ukrainian government agencies (such as the Security Service of Ukraine, State Tax Service, or State Special Communications Service) and contain malicious attachments or links.

READ MORE

MCT03001

First observed: 2023
Latest campaign: July 2025

GOAL

Credential and data theft

TARGETED

Region

Australia

Sector

All

Predominantly use compromised account and services such as SendGrid, mail gun and O365 to distribute their campaigns. They tend to have header from addresses and display names associated with. gov.au but most of the time have forged or no recipients visible in the header To fields. The lures focus on tax related themes and mentions of their online Centrelink account.

READ MORE

STORM-1865

MCT01020

First observed: 2020
Latest campaign: Aug 2025

GOAL

Credential and data theft

TARGETED

Region

Global

Sector

Hospitality industry

This group is known for leveraging social engineering techniques to trick victims into opening and executing malware files, often hosted on free file-sharing platforms. The malware used by this group includes infostealers such as Redline, Vidar, StealC, and Lumma. The group has been observed conducting spear-phishing campaigns against hotel and resort guests and has also been linked to campaigns targeting YouTube channels using similar tactics. Latest campaigns include the use of Click-fix to download infostealers.

READ MORE

MCTO5005

First observed: 2024
Latest campaign: Aug 2025

GOAL

Financial

TARGETED

Region

Global

Sector

All

Make use of digital transactional management services such as DocuSign, Paypal and Adobe sign to send payment or documents signing lure. Threat actor sends either directly though these services or makes use of this service along with Microsoft SRS to mass mail to their targets. Focused on credential phishing and telephone-based scams.

READ MORE

MCTO3035

First observed: 2021
Latest campaign: Aug 2025

GOAL

Credential harvesting

TARGETED

Region

Global

Sector

Focused on Marketing/Social media teams

The scams use well-known brands such as Meta, Redbull branding to appear legitimate, falsely alerting users of trademark or copyright violations or job opportunities to gather credential information.

READ MORE

MCTO3028

First observed: 2018
Latest campaign: Aug 2025

GOAL

Credential harvesting

TARGETED

Region

Global

Sector

All

Well-resourced group with a large pool for compromised accounts. Focuses on legitimate service that allow them to circumvent security solutions such as ISP's that allowing spoofed relaying or well-known brands that have URL redirecting capabilities to give their phishing campaigns a higher chance of successes. They also make use of compromised accounts to test various security solutions before investing in sending their very large campaigns to ensure there are no detections in place.

READ MORE

READ MORE

MCTO3022

First observed: 2021
Latest campaign: Aug 2025

GOAL

Credential phishing

TARGETED

Region

UK

Sector

All

HR related lures around performance reviews, workplace conduct/training, bonuses. TA predominantly makes use of marketing platforms such as Benchmark, Mailer lite and Zoho to distribute their campaigns in combination with freemail and newly observed sending domains.

READ MORE

05.

CONCLUSION

Living off trusted services has become standard methodology, with the 500% increase in ClickFix attacks and sophisticated multi-party BEC conversation chains revealing how quickly social engineering techniques proliferate. Industry-specific targeting shows mature threat operations that understand business workflows, creating persistent blind spots where compromised collaboration platforms expose years of strategic intelligence.

Artificial intelligence fundamentally transforms the threat landscape through multiple vectors. AI-generated phishing content leveraging pattern-of-life analysis and deepfake technology creates hyper-targeted spear phishing and whaling campaigns indistinguishable from legitimate communications. Organizations adopting AI technologies face new insider risks from data loss and inappropriate use, potentially exposing personally identifiable information and intellectual property.

This AI enhancement amplifies attack sophistication while expanding organizational attack surfaces through uncontrolled technology adoption. Access brokerage markets expand as Initial Access Brokers provide cybercriminals streamlined entry points into targeted organizations. Shadow IT proliferation, legacy systems from mergers and acquisitions, and unmanaged endpoints create expanding attack surfaces beyond traditional security controls. Supply chain attacks grow in frequency and impact as adversaries recognize the multiplier effect of compromising trusted third parties, while content delivery networks and legitimate services face continued abuse through living off trusted services techniques.

Ransomware operators increasingly combine traditional encryption with extortion DDoS attacks, creating multiple pressure points for victims. The emergence of “harvest now, decrypt later” strategies targeting encrypted data anticipates future quantum computing capabilities, while attempts to capture data in transit increase through network vulnerability exploitation and insecure communications channels.

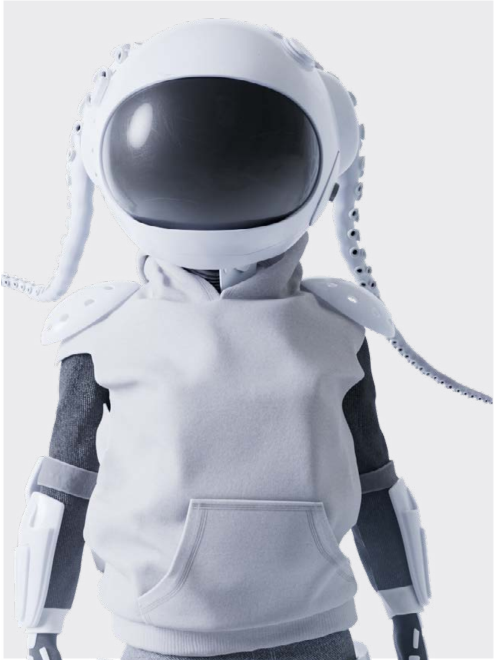
Organizations must implement comprehensive security hygiene addressing both technical vulnerabilities and human factors through layered defenses. The convergence of AI-enhanced attacks, expanding shadow IT environments, and sophisticated supply chain targeting demands a fundamental shift from reactive security measures to proactive human risk management strategies that treat people as the first line of defense.

- Attackers have shifted to exploiting human vulnerabilities and trusted infrastructure.
- Living off trusted services has become standard methodology.
- AI-generated phishing content leveraging pattern-of-life analysis and deepfake technology creates hyper-targeted spear phishing and whaling campaigns.
- Organizations adopting AI technologies face new insider risks from data loss and inappropriate use, potentially exposing personally identifiable information and intellectual property.
- Access brokerage markets expand as Initial Access Brokers provide cybercriminals streamlined entry points into targeted organizations, while shadow IT and legacy systems create attack surfaces beyond traditional security controls.
- Supply chain attacks grow in frequency and impact as adversaries recognize the multiplier effect of compromising trusted third parties.
- Ransomware operators increasingly combine traditional encryption with extortion DDoS attacks, creating multiple pressure points for victims.
- The emergence of ‘harvest now, decrypt later’ strategies targeting encrypted data anticipates future quantum computing capabilities.
- The convergence of AI-enhanced attacks, expanding shadow IT environments, and sophisticated supply chain targeting demands a fundamental shift from reactive security measures to proactive human risk management strategies that treat people as the first line of defense.

RISK RADAR SQUAD

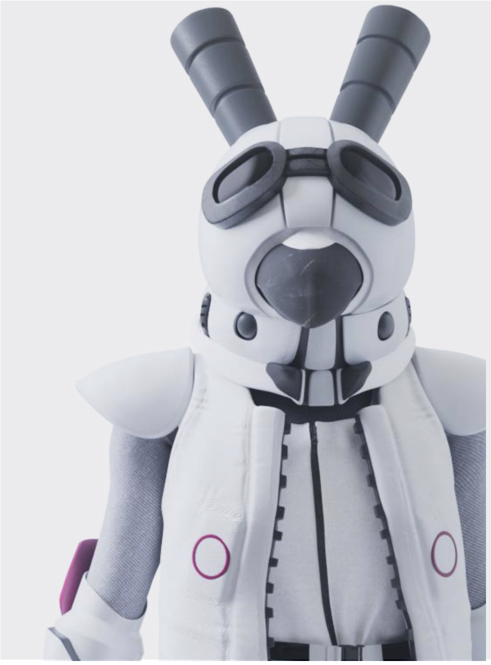
BAT

Detecting threats is their craft. Using echolocation, they emit high-frequency sounds that bounce off objects, giving them a detailed map of their surroundings. This helps them avoid obstacles, even in complete darkness.



OCTO

Masters of **analysis** with highly developed nervous system and large brain. They excel in adapting to their environment and overcoming challenges, making them a standout in threat intelligence.



CROW

Known for their problem-solving and teaching skills. Always educating, and taking **action**. Your go-to for cybersecurity risk mitigation strategies.