



Q1 2025

# Sublime

# Email Threat

# Research Report

## Introduction

Welcome to the first Sublime Email Threat Research Report, a retrospective of the threats we've observed across our customer base.

This report looks back at the first quarter of 2025, examining how email-based threats have evolved quarter over quarter across organizations of all sizes. Our analysis of detection data across customer environments highlights several trends that security practitioners should be aware of to maintain effective defenses.

## Contents

1 Introduction	12 Trend 3 Threat uniqueness and customization	18 Conclusion
3 Executive Summary	13 Trend 4 Evasion techniques by attack type	19 Recommendations
4 Trend 1 Continued evolution of BEC and social engineering	17 Trend 5 Evasion stacking	20 Methodology
8 Trend 2 Emerging attack vectors		



# Audience Takeaways

This report is designed for security leaders and practitioners responsible for email security in their organizations. It provides:

1

Actionable intelligence on emerging email threat tactics, techniques, and procedures (TTPs)

2

Industry-specific threat analysis to help tailor defensive strategies

3

Technical insights into evasion techniques used by sophisticated threat actors

4

Data-driven recommendations for security control improvements

5

Early warning of emerging attack vectors to inform security roadmaps



# Executive Summary

In Q1 2025, email threats continued to evolve rapidly, with adversaries demonstrating increased sophistication in both novel attack vectors and evasion techniques. Our anonymized telemetry shows significant growth in the following attack types:



## QR code phishing

While QR code attacks spiked in use last year there is still a significant amount of observed phishing attempts. Along with this increase in attack volume, the variety of evasion techniques has also increased.



## OAuth phishing

An increasing amount of all credential theft attempts now target OAuth. These adversary in the middle (AITM) attacks steal authentication tokens.



## Living Off Trusted Sites (LOTS)

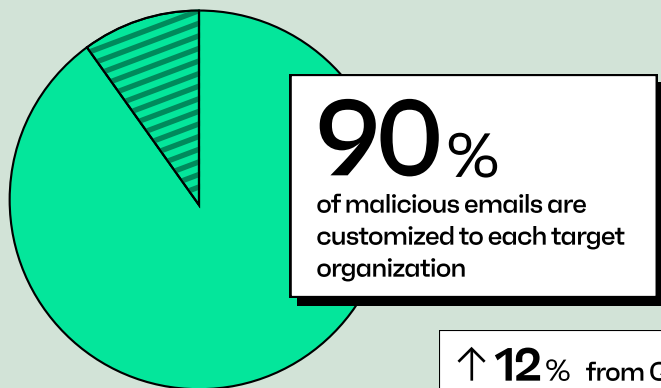
We are observing a growing trend of attacks abusing trusted cloud services. These include enterprise services (Microsoft 365, Google Workspace, DocuSign), as well as consumer services (Venmo, PayPal).



## GenAI threats

Significant increase in BEC/fraud campaigns with evidence of AI-generated content. GenAI is helping bad actors create and automate targeted attack campaigns faster than ever. [Google reports<sup>1</sup>](#) Iranian APTs as Gemini's heaviest threat actor user to craft tailored email attack campaigns.

## Key insights



### ■ Targeting by industry

Attack customization varies significantly by industry, with Manufacturing, Education & Non-Profit, Healthcare, and Technology & IT experiencing the most specialized targeting.

### ■ Increased evasion

We saw a dramatic rise in evasion stacking across all attack types, with campaigns often leveraging more than one technique to bypass detection.

### ■ Leading attack type

BEC/Fraud attacks continue to pose the highest financial risk, with specific industry targeting patterns. For example, Financial Services is targeted most by VIP/executive impersonation.



To stay ahead of today's rapidly evolving email threats, organizations need a layered, adaptive detection strategy that blends AI, ML, behavioral analysis, and threat intelligence complemented with other defense-in-depth controls to effectively counter the full spectrum of email threats.



# Trends

- 1 Continued evolution of BEC and social engineering
- 2 Emerging attack vectors
- 3 Threat uniqueness and customization
- 4 Evasion techniques by attack type
- 5 Evasion stacking

## TREND 1

### Continued evolution of BEC and social engineering

#### KEY POINTS

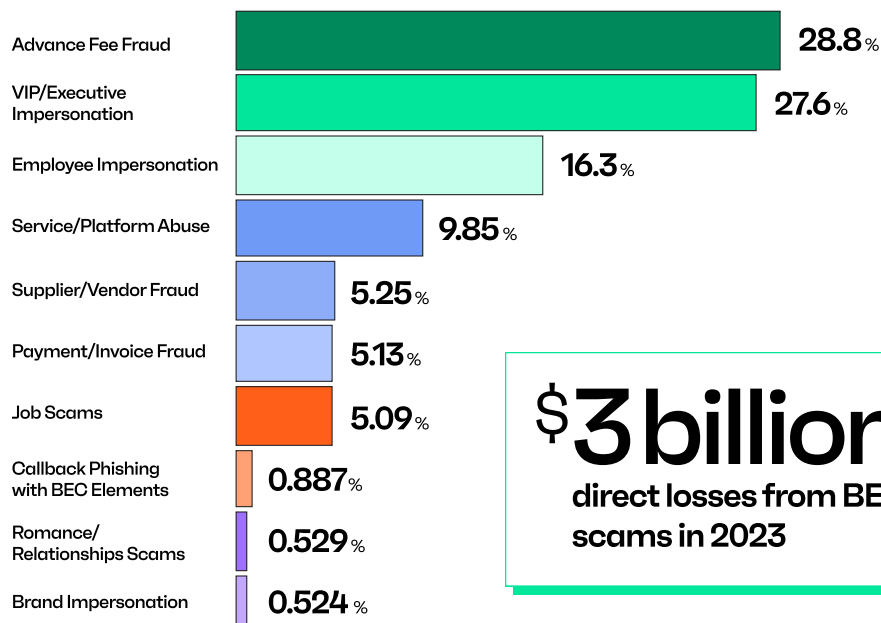
- BEC remains the highest financial cybercrime risk to most organizations.
- There are clear industry-specific targeting patterns.
- Infrastructure Services faces the highest rate of employee impersonation.
- Financial Services is targeted most by VIP impersonation.

27.2 %

43.4 %

BEC and related social engineering attacks continue to represent the highest financial cybercrime risk to most organizations. According to the [FBI Internet Crime Complaint Center's 2023 report<sup>2</sup>](#), BEC scams accounted for direct losses of \$3 billion in 2023—the highest loss vector of any cybercrime.

#### Distribution of BEC/Fraud



**\$3 billion**  
direct losses from BEC  
scams in 2023

**FIGURE 1** Overall distribution of observed BEC-themed attacks

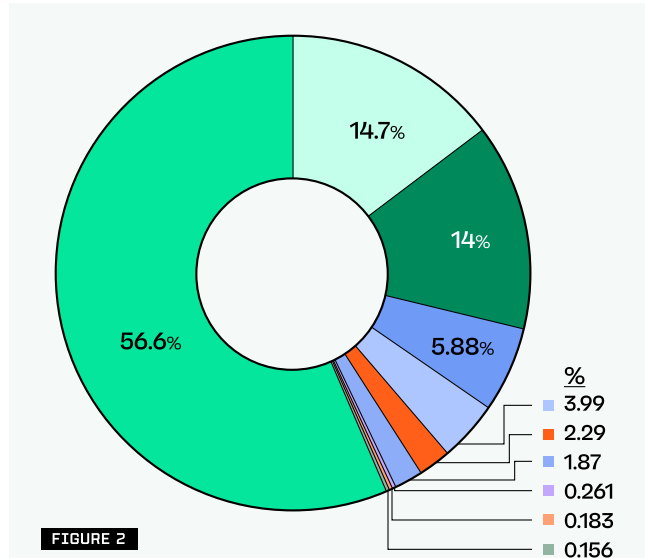
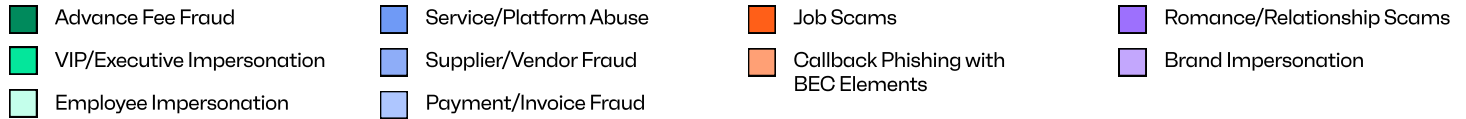


## TREND 1 Continued evolution of BEC and social engineering, cont.

### Breakdown by industry

Our analysis of BEC attack patterns reveals distinct targeting preferences across industries:

#### Figures 2-4 Key

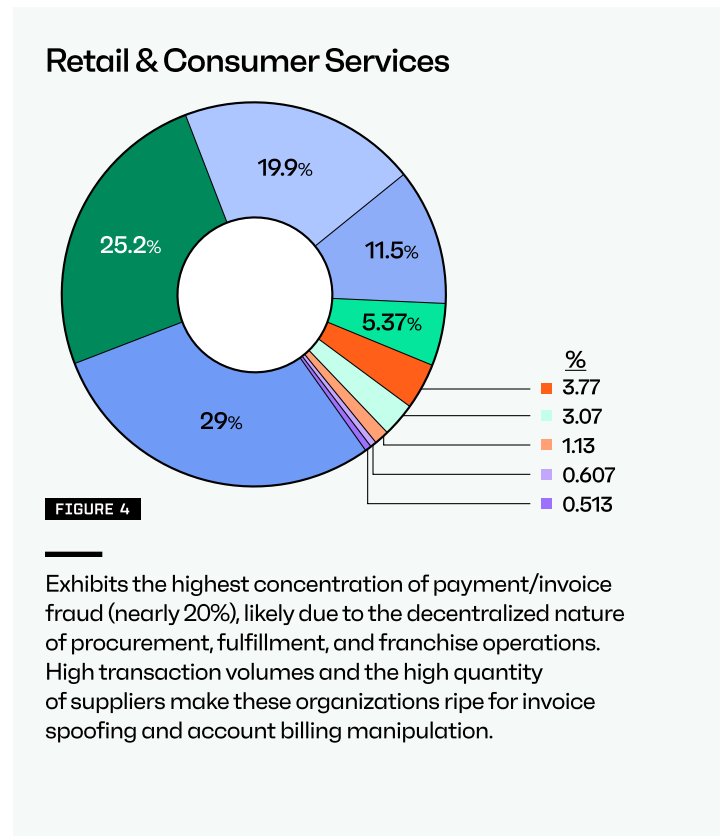
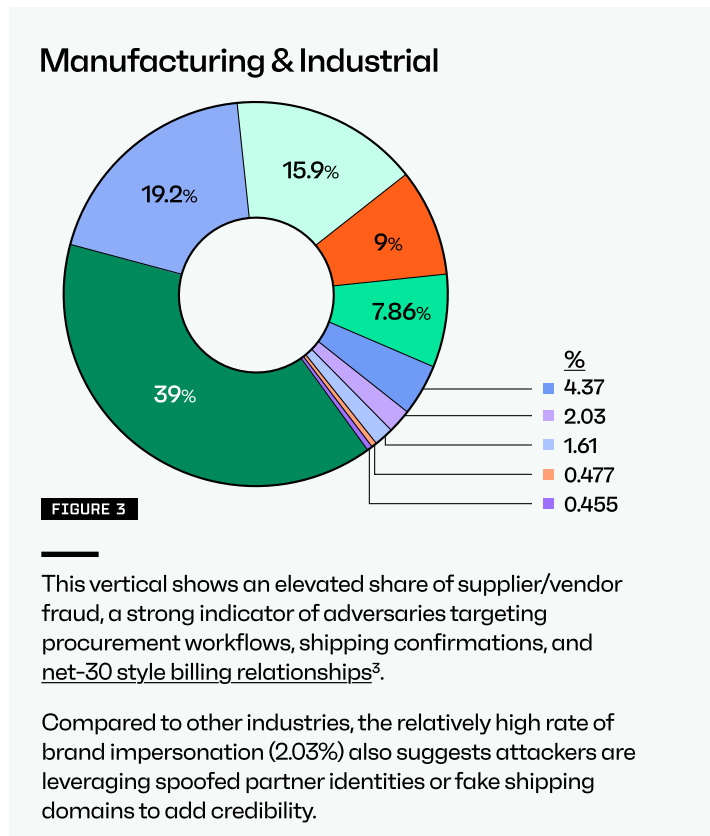


### Financial Services

# 70%

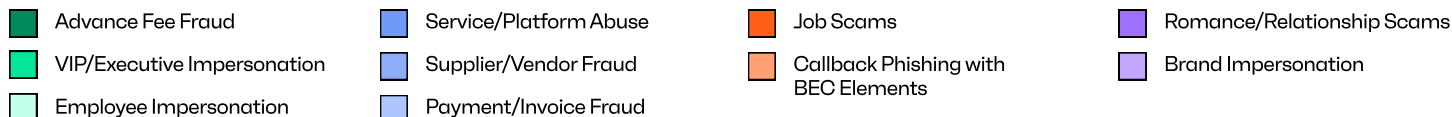
VIP/executive and employee impersonation dominate, comprising over 70% of observed BEC patterns.

These attacks often leverage urgency and familiarity to bypass human defenses. Interestingly, despite strong financial controls in this sector, attackers continue to target highly privileged users and abuse trust relationships.



## TREND 1 Continued evolution of BEC and social engineering, cont.

### Figures 5-8 Key



### Infrastructure Services

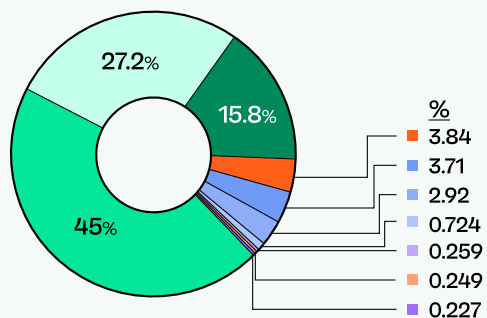


FIGURE 5

Notably impacted by employee impersonation (27.2%) and job scams, which together suggest adversaries are blending internal impersonation with hiring-related lures. This is particularly relevant in industries with a high contractor or seasonal labor presence, where verification processes may be weaker.

### Government & Public Sector

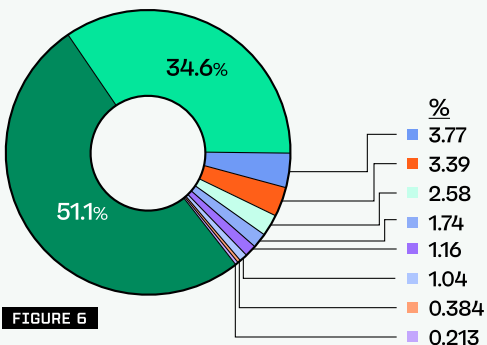


FIGURE 6

While VIP impersonation (34.6%) remains dominant, this sector shows broader attack diversity than others. The presence of callback phishing, job scams, and even romance scams (albeit rare) suggests attackers are experimenting with more consumer-grade lures, possibly due to public sector targets being more personally accessible or having less centralized controls.

### Professional Services, Technology & IT

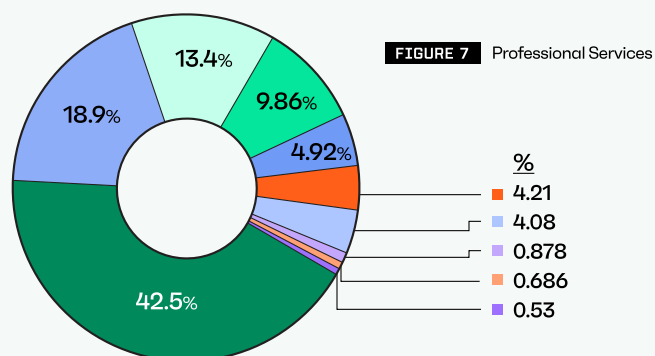


FIGURE 7 Professional Services

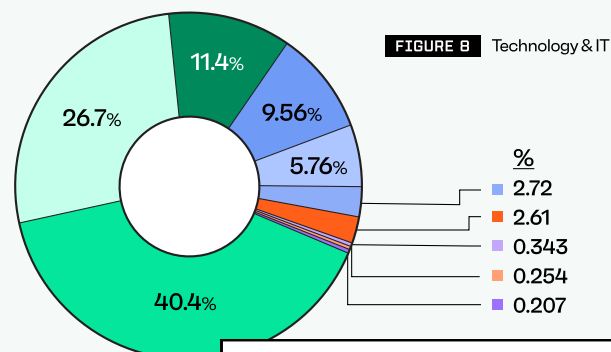


FIGURE 8 Technology & IT

**67.1%**

VIP/executive and employee impersonation in the Technology & IT industry.

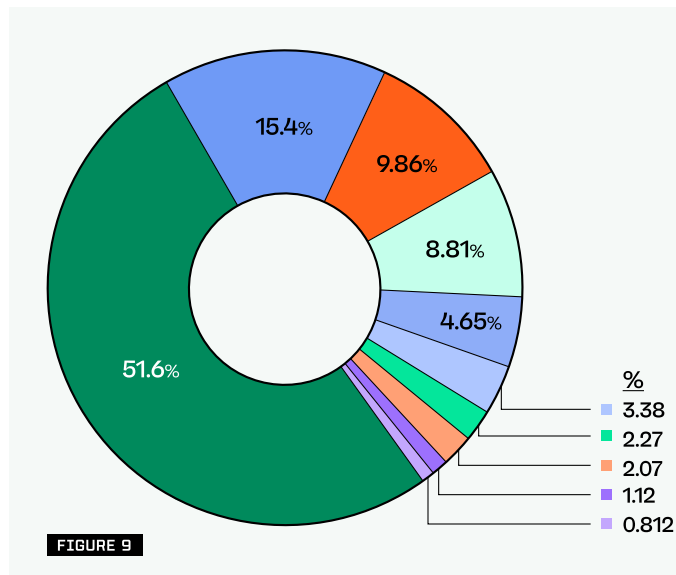
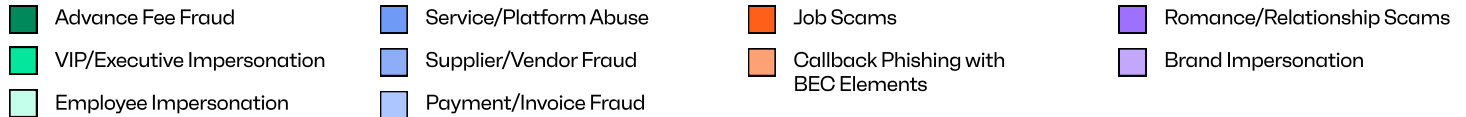
Both industries show high rates of impersonation (employee and executive), likely due to flat org structures and heavy reliance on email.

Interestingly, Technology & IT shows slightly elevated callback phishing with BEC elements (2.72%), indicating that attackers may be adapting their tactics to bypass increasing defender capabilities through multi-stage engagement.



## TREND 1 Continued evolution of BEC and social engineering, cont.

### Figures 9-10 Key

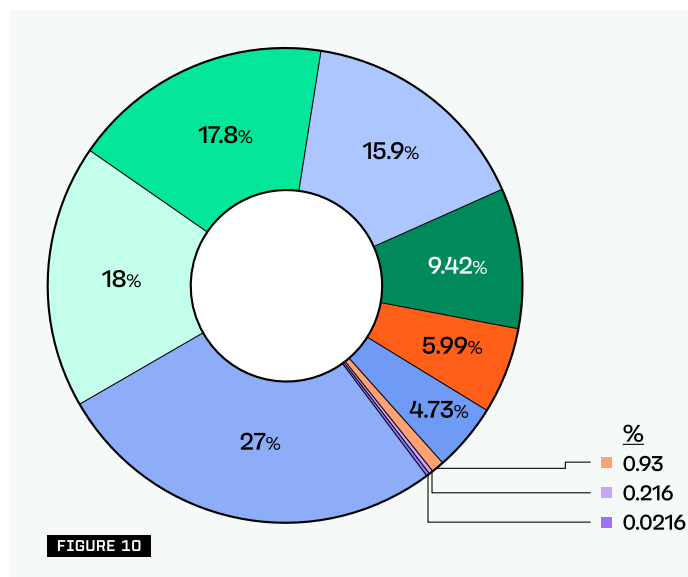


### Education & Non-Profit

# 51%

## Employee Impersonation

Stands out with over 51% of attacks leveraging employee impersonation, suggesting a trend toward exploiting authority gaps between admin staff and faculty/donors, or taking advantage of less mature identity controls. The relatively low presence of traditional financial fraud types may reflect lower perceived ROI for attackers but higher success rates for basic impersonation tactics.



### Healthcare

# 62.8%

## Organization-level impersonation and vendor fraud attacks faced by the Healthcare industry

Organization-level impersonation (35.8%) and vendor fraud (27%) are the most common BEC attack types, indicating that attackers are targeting trusted relationships within and between organizations to maximize the likelihood of success and financial impact.

These industry-specific patterns align with trends identified in the [Verizon 2024 DBIR<sup>4</sup>](#), which found that BEC tactics vary significantly by industry, with attackers tailoring their approach to organizational structures and business processes.



TREND 2

Emerging attack vectors

KEY POINTS



■ SVG-based attacks provide sophisticated evasion capabilities.



■ Living Off Trusted Sites (LOTS): Continued increase in exploiting trust of mainstream cloud services to evade traditional detection methods.



■ QR code phishing increased 75% compared to Q4 2024.

In Q1 2025, we identified several novel evolutions of known tactics and techniques that made these attack chains more difficult to detect.

Continued use of QR codes as a delivery mechanism

QR code phishing<sup>5</sup> has continued its strong growth trajectory through Q1 2025. First emerging as a significant threat in late 2023, this technique has now become a mainstream attack vector.

↑ 40-60%

Our data shows a 40%-60% increase in QR code phishing campaigns compared to Q4 2024, with these attacks now accounting for 2.5% of all phishing attempts.

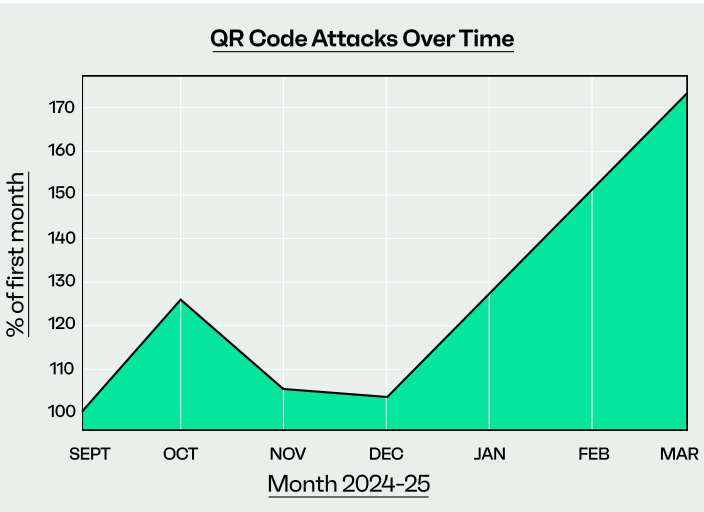


FIGURE 11 Continued Use of QR Codes as a Delivery Mechanism in Credential Phishing Attacks

QR codes are particularly effective in bypassing traditional email security controls because:

- They contain no malicious text or URLs for content filters to detect.
- They circumvent URL rewriting and sandbox analysis.
- They exploit the increasing normalization of QR codes in legitimate business communications.
- Users often pivot off a secure device and onto a generally unmonitored personal device (mobile phone).

Some common lures include fake password resets, document sharing notifications, HR impersonations, voicemail notifications, W-2/tax notifications, and multi-factor authentication (MFA) requests.



TREND 2
Emerging attack vectors, cont.

SVG Attacks by Industry–Normalized to First Month = 100%

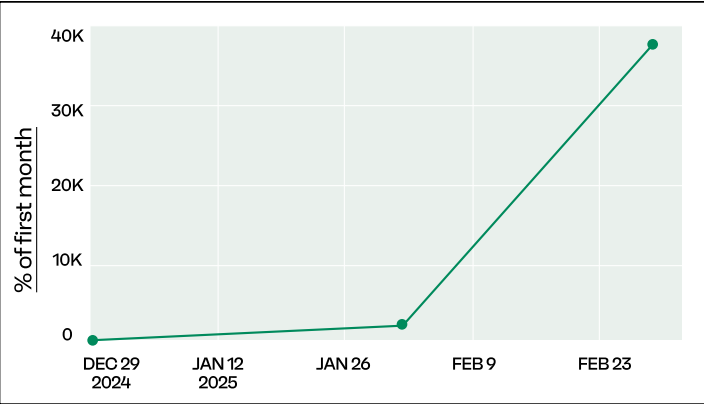


FIGURE 12
Financial Services

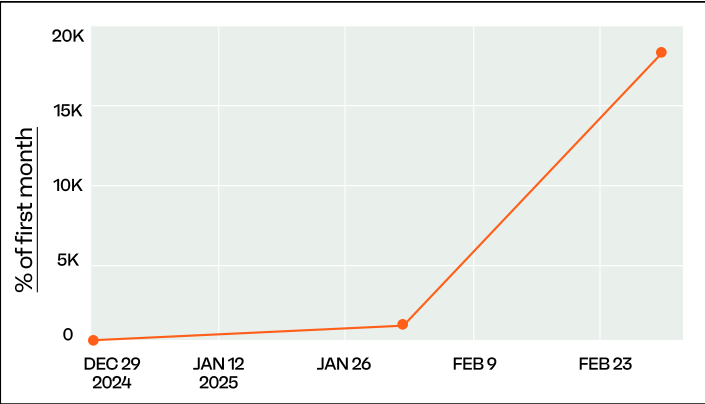


FIGURE 13
Education & Non-Profit

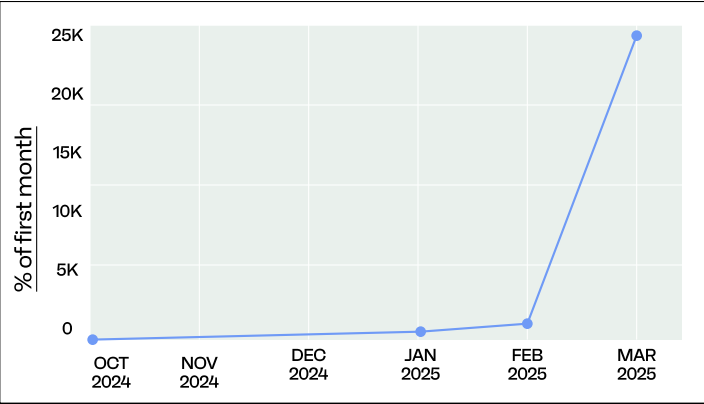


FIGURE 14
Technology & Cybersecurity

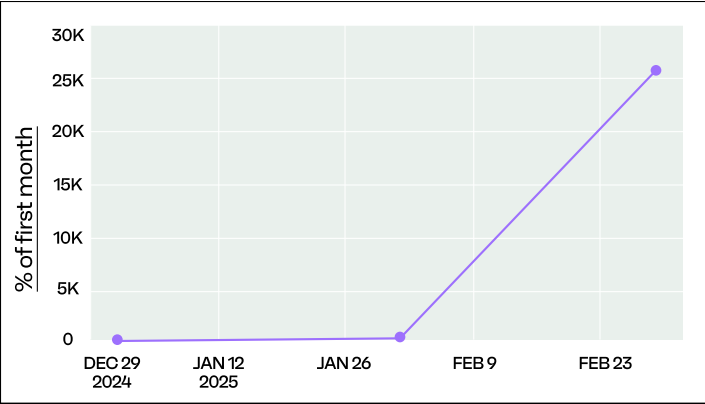


FIGURE 15
Professional Services

The rise of SVG attacks

We've observed a significant increase in attacks leveraging SVG files as an attack vector.

↑

47,000%

increase in SVG phishing campaigns compared to Q4 2024

Our data shows a 47,000% increase in SVG attachment based phishing campaigns compared to Q4 2024, with these attacks now accounting for 1% of all phishing attempts.

These attacks typically involve emails containing EML attachments with embedded SVG files that contain malicious JavaScript code, including base64-encoded content and potentially harmful event handlers.

SVG attacks are particularly concerning because:

- They can leverage base64 encoding to obscure malicious content.
- The files can contain embedded event handlers that execute automatically.
- Many email security solutions don't deeply inspect SVG files for malicious JavaScript.
- SVG is increasingly used for legitimate business purposes (logos, signatures, etc.), making it difficult to block entirely.

TREND 2 Emerging attack vectors, cont.

Living Off Trusted Sites (LOTS)

LOTS attacks (a type of service abuse) take advantage of trusted web services used by many organizations to download malware, launch phishing campaigns<sup>6</sup>, communicate with command-and-control (C2) servers, or exfiltrate data.

Similar to Living Off the Land (LOTL) techniques, LOTS takes advantage of the fact that sites like DocuSign, SharePoint, or OneDrive are already being used for legitimate business purposes, so they blend in well and can't be blocked outright.



What percentage of attacks leverage legitimate cloud services, and how has this changed over the past 6 months?

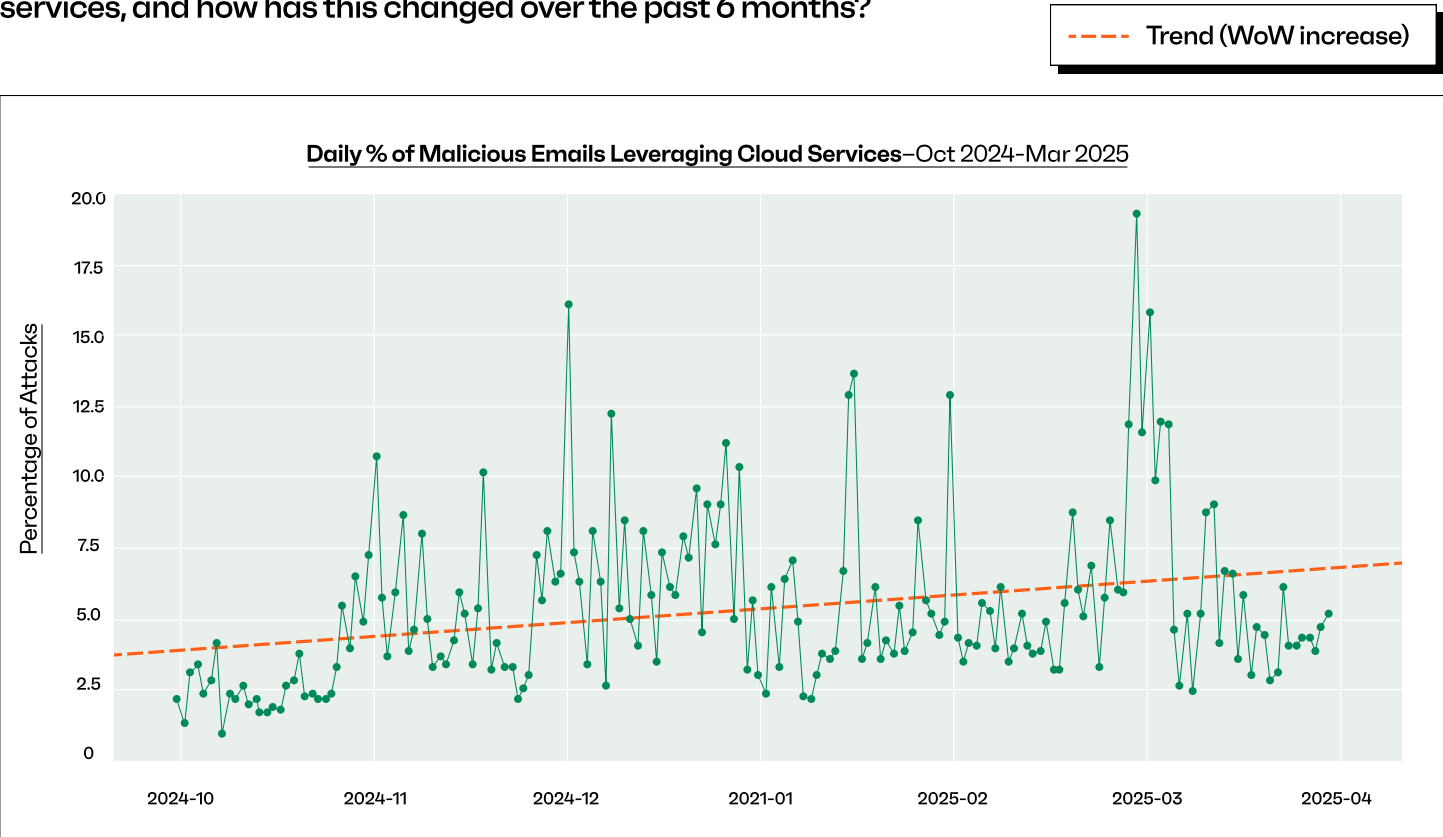


FIGURE 16 Daily Percentage of Malicious Email Leveraging SaaS Infrastructure from Oct 24 - Mar 25

Our analysis shows that an average of 7.89% of attacks in Q1 2025 leveraged legitimate cloud services, a slight decrease from 8.24% in the same period last year, representing a 4.25% relative decrease year over year.

While the overall percentage of LOTS attacks has remained relatively stable since Q4 2024, the sophistication of these attacks continue to evolve, with more complex payloads, evasion techniques, and services being exploited.

2024

8.24%

2025

7.89%

TREND 2
Emerging attack vectors, cont.

Which cloud services are most frequently abused by attackers, and are there industry-specific patterns?

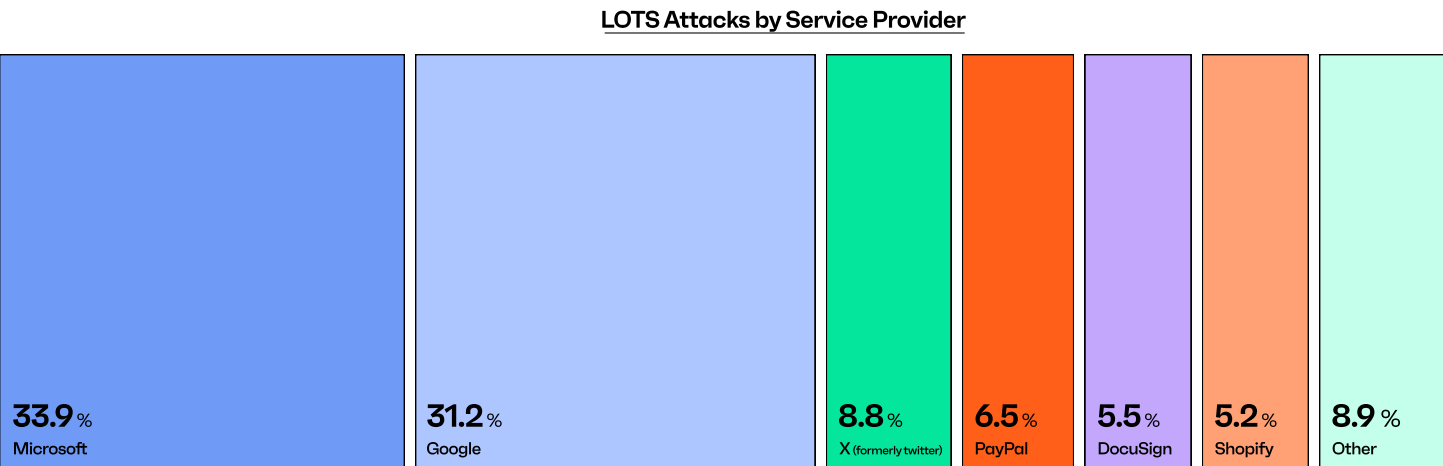




FIGURE 17
Breakdown of Service Providers commonly abused in LOTS Attacks

Our data shows distinct patterns in which cloud services are abused across different industries. Within our telemetry, we found that these were the most frequently abused services:




Microsoft SharePoint/OneDrive

Accounts for 34% of all LOTS attacks, with particularly high prevalence in Healthcare and Financial Services sectors.




Google Workspace

Represents 31% of LOTS attacks, with higher rates in Technology & IT and Financial Service industries.




X (formerly Twitter)

Comprises 8.8% of LOTS attacks, and is commonly used in spam campaigns, hence the near identical numbers across all sectors.



PayPal

Accounts for 6.5% of all LOTS attacks, with Government & Public Sector and Technology & IT seeing the most campaigns.



DocuSign

Accounts for 5.5% of all LOTS attacks, with Government and Financial Service sectors seeing the most campaigns.

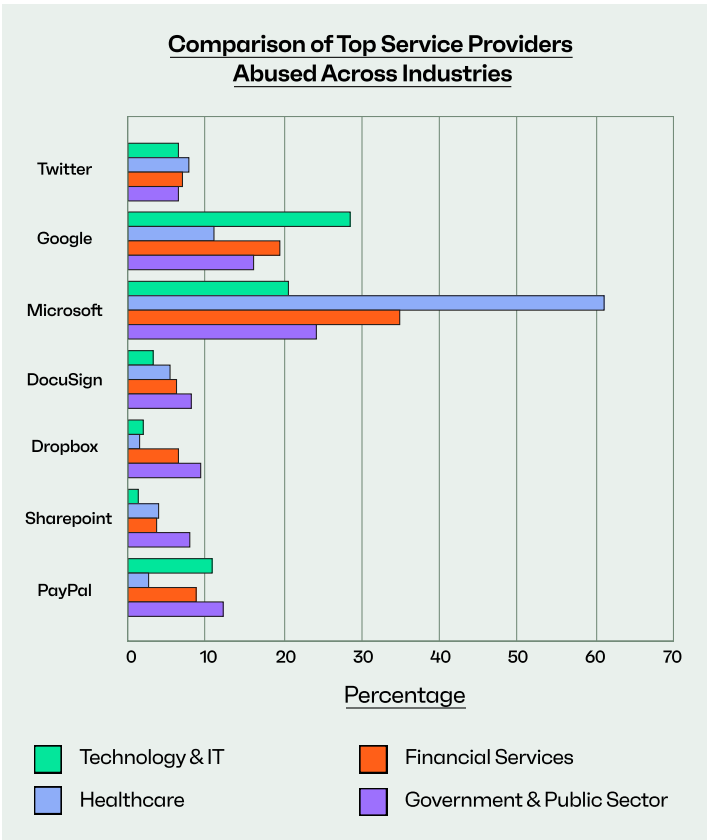


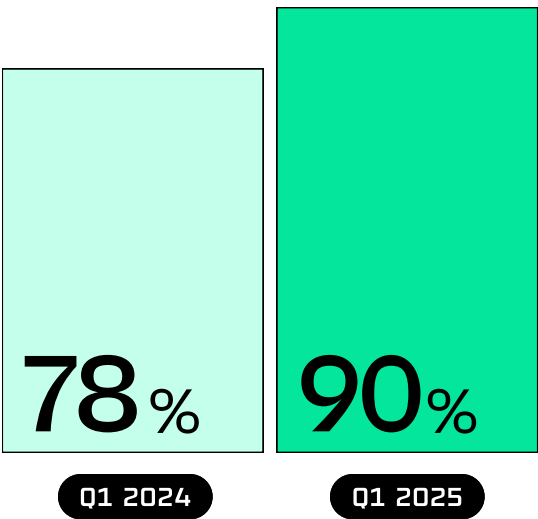
FIGURE 17
Most commonly exploited service providers in LOTS attacks by Industry

TREND 3

Threat uniqueness and customization

KEY POINTS

- Signature and reputation-based defenses are often ineffective against unique, targeted campaigns.
- 90% of malicious emails are customized to their target organization.
- Professional Services, Manufacturing & Industrial, and Education & Non-Profit sectors face the most customized attacks.



Our analysis reveals that attackers are sending more customized attacks tailored to their targets.

On average, 90% of malicious emails detected in Q1 2025 were customized to their target organization in some way, representing a 12% increase from our observations in Q1 2024.

Customization includes a combination of personalization via mass phishing kits, templates, and brand logos, as well as AI-generated, unique content tailored specifically to the recipient and organization.

The distribution pattern demonstrates attackers' accelerating ability to create tailored campaigns at scale, likely leveraging automation and AI to customize attacks while maintaining operational efficiency.

What is the average "customization factor" of attacks targeting specific industries?

To quantify the degree of attack customization by industry, we calculated Kullback-Leibler (KL) divergence scores (see Fig 18) comparing each sector's TTP distribution against an industry-agnostic baseline.

Higher KL divergence values indicate more distinctive, specialized attack patterns that significantly diverge from the baseline, suggesting attackers are using more tailored tactics against these industries.

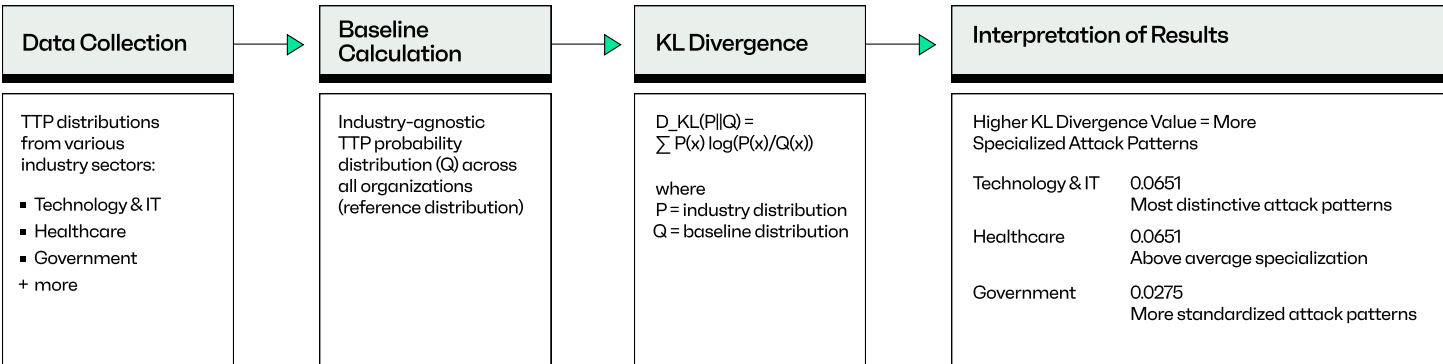


FIGURE 18 Overall Distribution of observed BEC-themed attacks

TREND 3 Threat uniqueness and customization, cont.

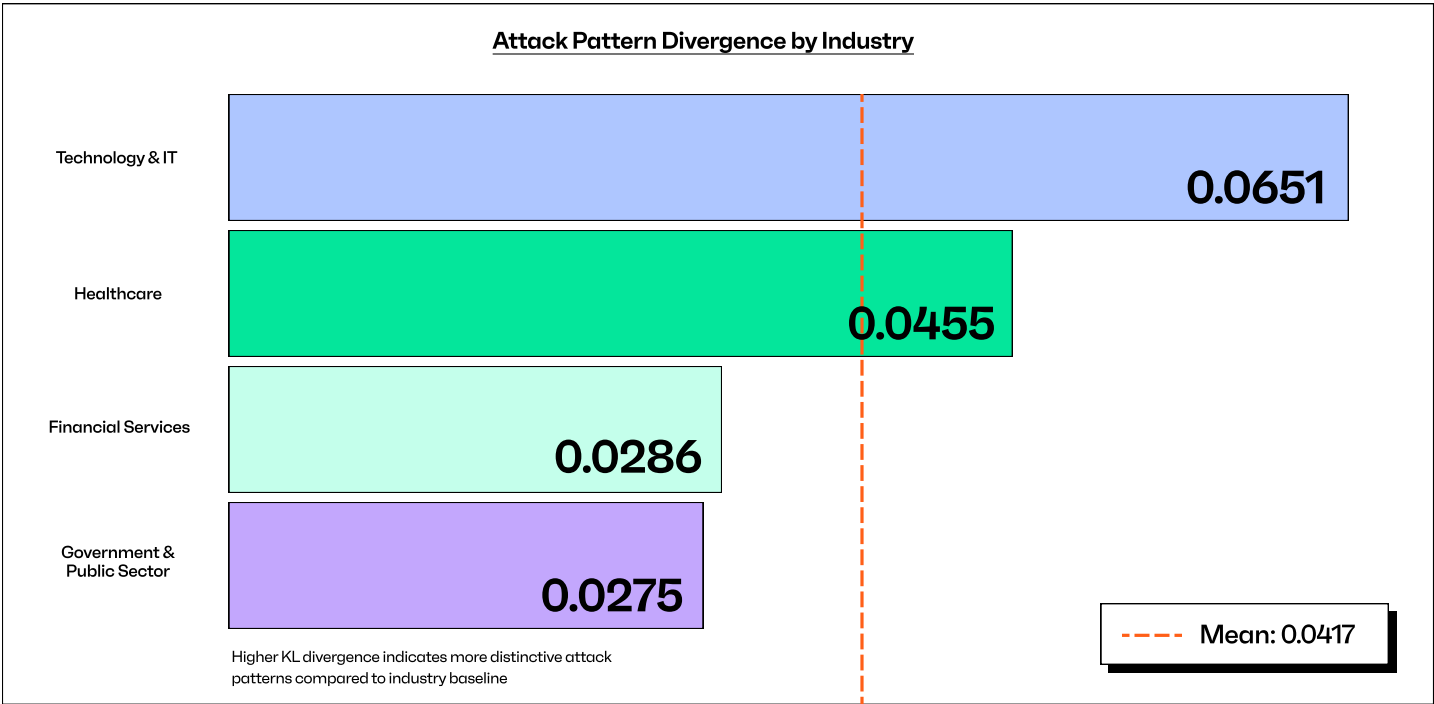


FIGURE 19 Attack Pattern Divergence using Kullback-Leibler Divergence Analysis of TTP Distribution

As shown in Figure 19, Technology & IT organizations experience the most customized attack patterns, followed by Healthcare. These sectors face highly specialized threats that leverage industry-specific lures, terminology, and workflows.

At the lower end, Government & Public Sector and Financial Services show less distinctive attack patterns. However, this doesn't indicate less sophisticated targeting—rather, it suggests attackers employ a broader range of techniques against these sectors.

We can only speculate attacker motives, but some contributing factors may be:

Broader attack surfaces

Users in these industries often use corporate email addresses for various personal accounts, increasing exposure through breached credentials and enabling bulk targeting.

High-value targets

The potential value of compromises in these sectors may justify greater resource investment by attackers across multiple vectors.

Complex organizational structures

These sectors often have diverse sub-organizations with varying security postures, motivating attackers to use multiple approaches.

TREND 3

Threat uniqueness and customization, cont.

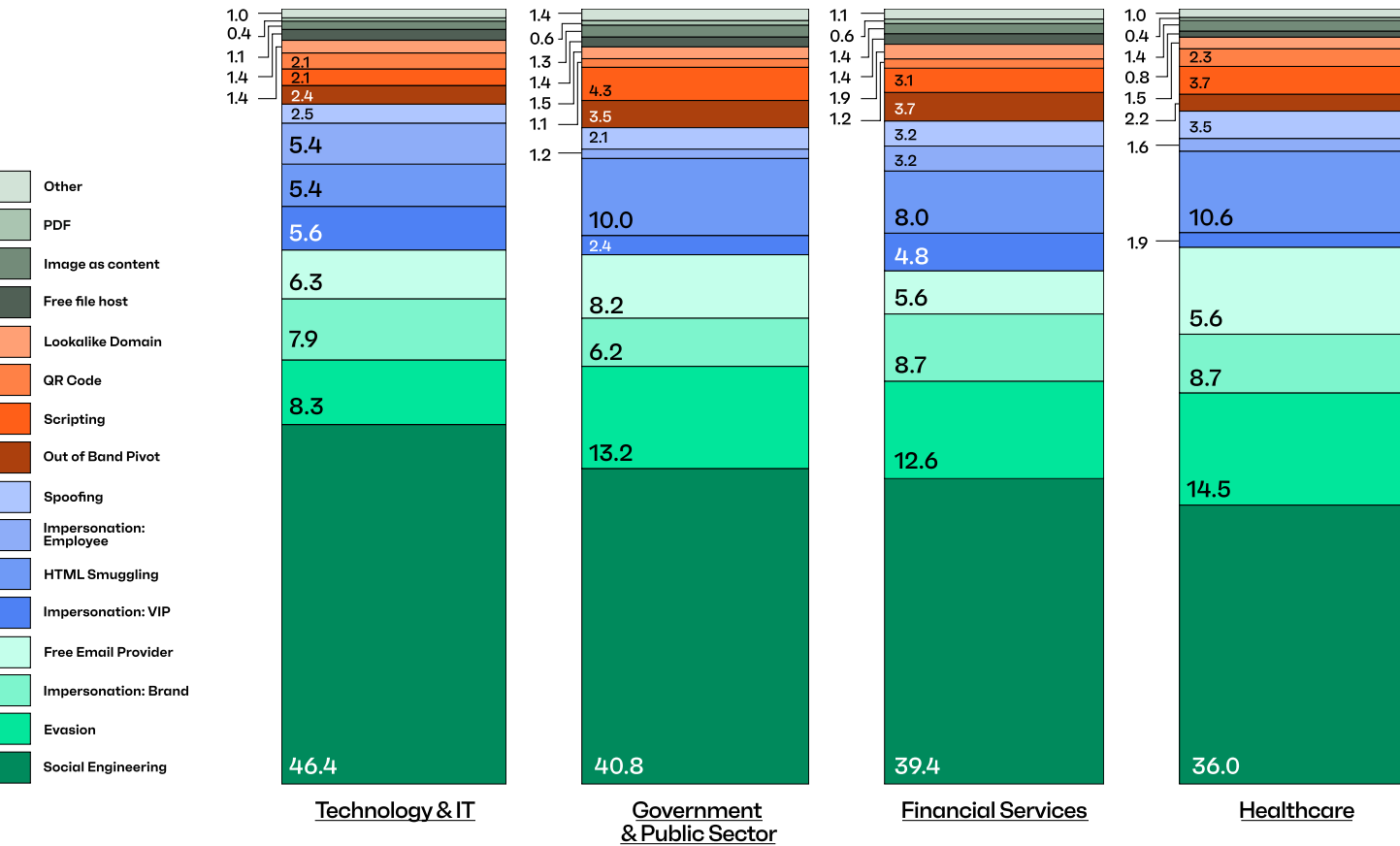


FIGURE 20 Breakdown of TTPs per Industry

Our analysis shows distinct patterns in the distribution of attack techniques across different industries, as illustrated in Figure 20.

These patterns reveal how attackers customize their approaches based on industry-specific characteristics:

- Volume-based targeting

Large employee bases and frequent business transactions make Financial Services organizations ideal for lower-effort, high-volume scams.
- Operational urgency

The Healthcare industry's reliance on time-sensitive communication (e.g., scheduling, billing) increases the likelihood of success for impersonation tactics.

- Brand trust

Logos and domains carry inherent authority, making them attractive for brand impersonation and abuse across industries.
- Building trust

Attacks that use social engineering to engage a target before delivering a payload—like BEC and callback phishing—are harder to detect and often bypass traditional filters by avoiding links or payloads.

TREND 4

Evasion techniques by attack type

KEY INSIGHTS

- Evasion techniques vary significantly by attack type, reflecting tailored strategies to bypass specific detection layers.
- Credential phishing remains the most varied, with attackers constantly adapting and testing new techniques.
- Attackers shift tactics within days of detection innovations, underscoring the need for adaptive and layered defenses.

43%

BEHAVIORAL  
EVASION

53%

HEADER-BASED  
EVASION

71%

FILE-BASED  
EVASION

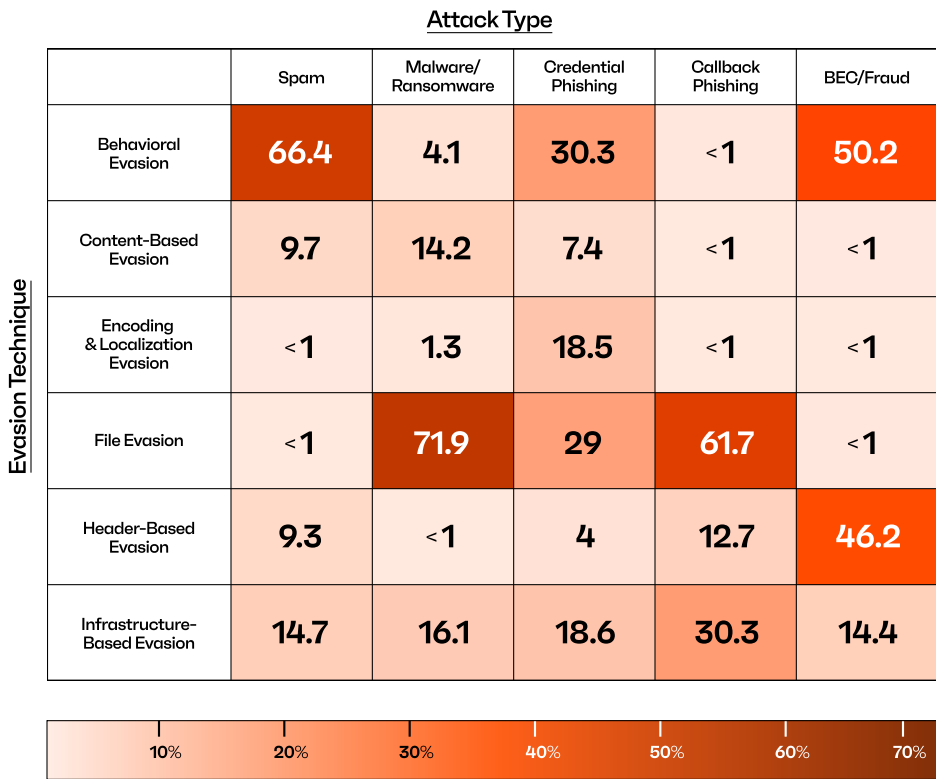
- BEC/Fraud campaigns rely heavily on header-based (53%) and behavioral evasion (43%), often exploiting trust in known senders.
- Callback phishing exploits file evasion (71%), typically using PDFs or images to lure victims into phone-based social engineering.

Which evasion techniques are most prevalent across different attack types?

We looked at seven types of evasion techniques across five different attack types. The evasion types we used were:

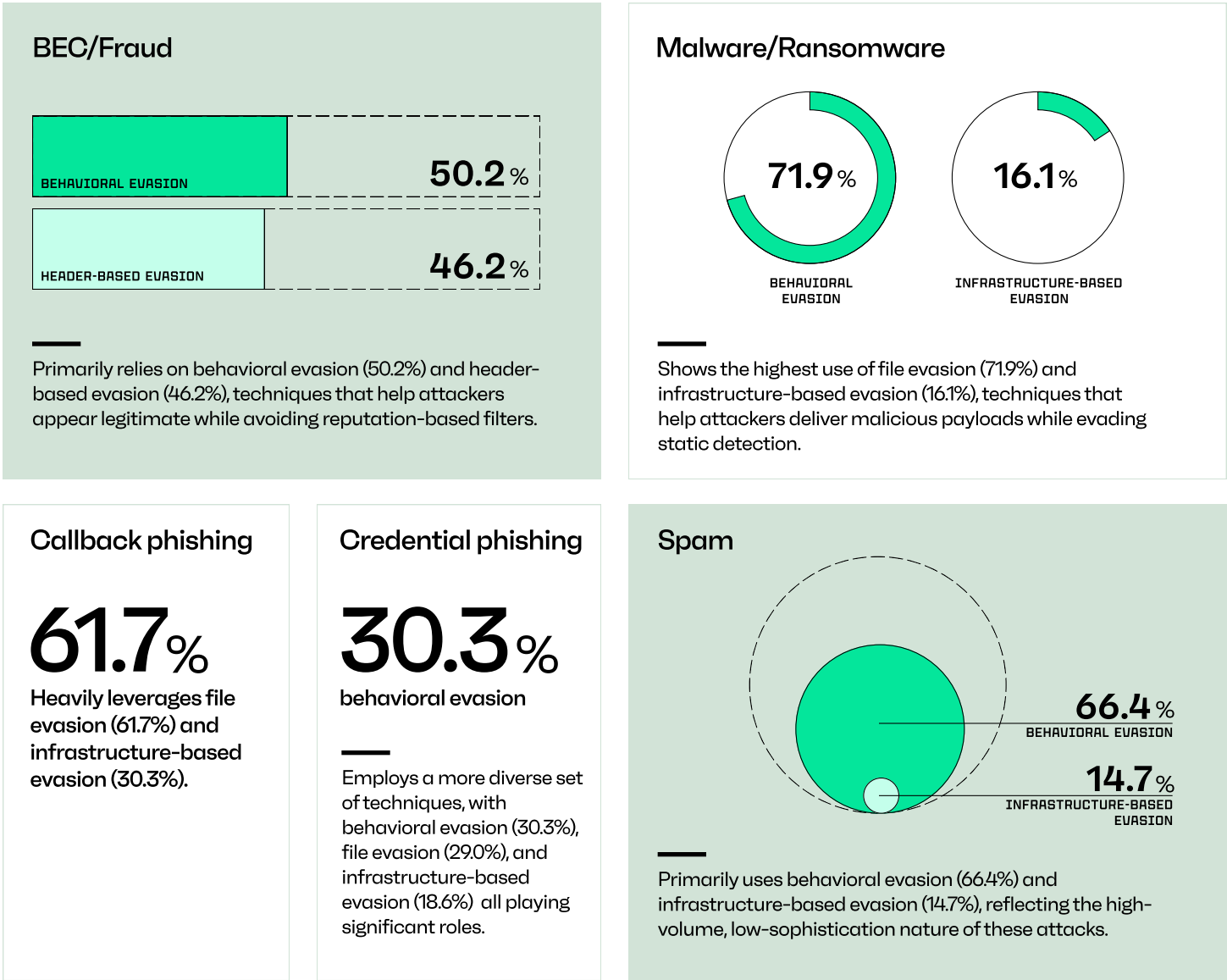
- **File-based:** Embeds the payload in a file to avoid detection or delay execution.
- **Behavioral:** Evades detection by manipulating timing, patterns, or social context to appear legitimate.
- **Content-based:** Techniques that manipulate the visible body content to obscure intent or evade keyword/signature detection.
- **Encoding and localization:** Uses alternative languages, character sets, or encodings to bypass traditional filters.
- **Header-based:** Manipulations in email headers that obscure sender, recipient, or subject intent.
- **Infrastructure-based:** Tactics that manipulate sender infrastructure or the delivery path.

FIGURE 6 Evasion techniques prevalence across attack types



TREND 4 Evasion techniques by attack type

Our analysis reveals distinct patterns in how attackers employ evasion techniques across different attack types:



These patterns evolved significantly over the past quarter:



Callback phishing has seen a notable shift toward header-based and infrastructure evasion techniques, with respective increases of 12% and 5% compared to Q4 2024.



BEC campaigns show increased use of infrastructure-based evasion, growing from 8% to 13% of attacks, suggesting attackers are investing in more sophisticated delivery mechanisms.



Malware/Ransomware delivery has recently reverted to higher use of file evasion, increasing from 63% to 69% in Q1 2025.





TREND 5

Evasion Stacking

KEY INSIGHTS

■ Complex attacks like malware/ ransomware and credential phishing now combine multiple evasion techniques to bypass traditional defenses.



■ Rise of evasion stacking observed across all major attack types.

↑ 160 %

■ Callback phishing shows the largest increase (+160%) in multi-evasion attacks.

The complexity of email-based attacks continues to increase as threat actors combine multiple evasion techniques in a single campaign. This "evasion stacking" significantly reduces traditional detection rates.

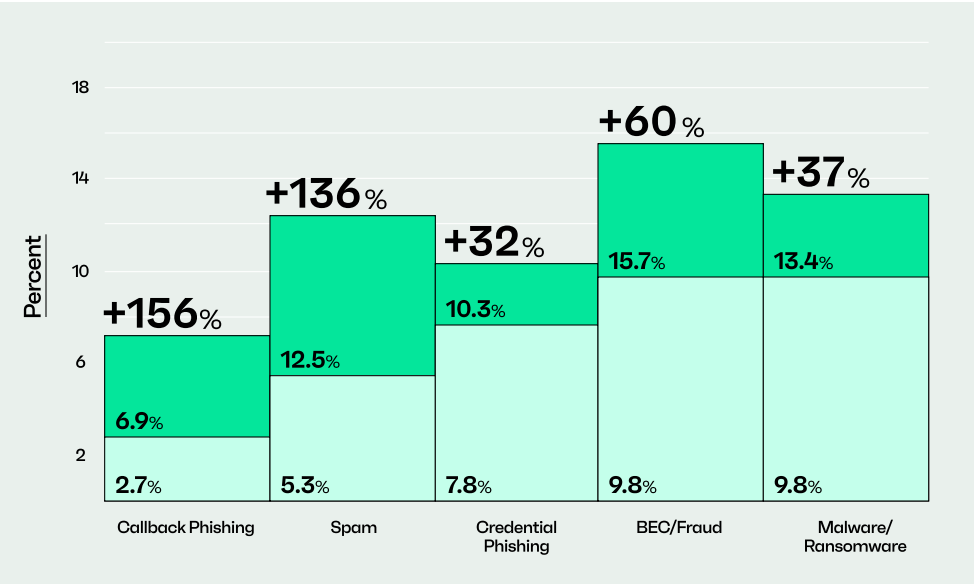
What percentage of attacks use evasion stacking?

Our analysis reveals a trend toward increased evasion complexity across most attack types.

This can likely be attributed to the fact that as defenders increase their detection capabilities, attackers are investing more in multi-layered evasion to stay effective:

Q4 2024

Q1 2025



↑ 156%

relative increase for callback phishing from Q1 to Q2

■ Credential phishing

Shows moderate growth in complexity, with multi-evasion attacks increasing from 7.8% to 10.3%, a 32% relative increase.

■ Spam

Demonstrates the second-largest increase, with multi-evasion attacks growing from 5.3% to 12.5%, a 136% relative increase.

■ Callback phishing

Shows the most dramatic increase, with multi-evasion attacks growing from 2.7% to 6.9% between Q4 2024 and Q1 2025, representing a 156% relative increase.



# Conclusion

The email threat landscape in Q1 2025 is characterized by increasing sophistication, customization, and evasion complexity.

Traditional security approaches that rely on slow to update models, static signatures, reputation, or known indicators of compromise are increasingly ineffective against these evolving threats.

As attackers continue to evolve their techniques at an accelerating pace, as defenders we must embrace adaptive defensive approaches that can respond quickly to emerging threats and anticipate future developments.

## CUSTOMIZED ATTACKS

Attackers have tools (GenAI, Phishing as a Service, etc.) that let them quickly customize their attacks to their target. This has led to the proliferation of tailored attacks.

## INDUSTRY-SPECIFIC

Attackers understand the need for industry-specific attacks to maximize campaign success.

## NOVEL APPROACHES

Attackers are developing novel approaches to bypass traditional security detection. QR code phishing, malicious SVGs, and LOTS techniques are evolving, and new tactics are always on the horizon.

## INCREASED SPEED

Attackers shift tactics within days of detection innovations, amping up the game of cat and mouse between attackers and defenders.

## STACKING TACTICS

Attackers are increasingly stacking their evasion tactics, reducing traditional detection rates.



# Recommendations

## REC 1

### Secure the email environment

The email threat landscape is characterized by increasing sophistication, customization, and evasion complexity.

Organizations should adopt an email security solution that can adapt to changing tactics and techniques as well as organization needs, with the ability to detect the full-spectrum of email attacks using a multi-layered approach that includes AI/ machine learning, behavioral analysis, rules, and threat intelligence.

## REC 2

### Adopt phishing-resistant MFA solutions

Stop credential phishing in its tracks through hardware security keys such as Yubikeys.

## REC 3

### Implement additional controls for high-risk transactions

Add friction to high-risk and high-value actions like payroll changes and invoicing payments by adding multi-modal and multi-person verification.

## REC 4

### Train and educate users on the increasing sophistication of attacks

Many threats look familiar on purpose. Run data-driven training that shows users real-world attacks they're likely to receive.

## REC 5

### Stay current with the latest attacker tactics and techniques

Verify that your email security solution can detect emerging attacks. SVGs, QR codes, and trusted services are now common payload carriers. Make sure your tools can parse and inspect them properly, and red/blue team your email security solution to verify and identify gaps.

Dive deep in the Sublime Thoughts blog:

- [Threat Detection](#)
- [Machine Learning](#)
- [Attack Spotlights](#)

Get a live demo of Sublime:

<https://sublime.security/demo/>



# Methodology

This report was compiled by the Sublime Machine Learning and Detection teams from anonymized customer telemetry and analyzed under strict adherence to our internal Data Privacy Framework.

## Data

Our analysis draws from multiple complementary and anonymized data sources:

- **Detection telemetry:** Analysis over messages processed by Sublime Security's detection engine across enterprise customer environments in Q1 2025.
- **External research:** Correlation with findings from leading security researchers, vendors, and government agencies.

## Data Privacy Framework

Our commitment to preserving privacy extends throughout our intelligence collection, analysis, and disclosure processes. All data presented in this report adheres to our stringent privacy principles:

- **Data minimization:** We employ advanced anonymization techniques to strip all personally identifiable information (PII) from our telemetry before analysis. This includes a multi-stage sanitization pipeline to ensure that no individual or specific organization can be identified through the presented data patterns.
- **Explicit consent boundaries:** We analyze only data explicitly authorized through our service agreements, with clearly delineated boundaries that respect both regulatory requirements and ethical considerations regarding customer privacy.

This multi-layered privacy architecture ensures that organizations can benefit from collective threat intelligence without compromising individual privacy or exposing sensitive operational details. By implementing these measures, we maintain a responsible balance between security intelligence sharing and privacy preservation.

## Questions? Feedback?

Reach out at [research@sublime.security](mailto:research@sublime.security) or [@sublime\\_sec](https://twitter.com/sublime_sec) on X.

## Analysis

Our analytical approach combines automated pattern detection with expert human analysis:

- **Machine learning classification:** Initial categorization of threats using our supervised ML models trained on verified malicious and benign content.
- **Behavioral analysis:** Examination of attacker TTPs, including delivery mechanisms, social engineering techniques, and technical indicators.
- **Temporal analysis:** Tracking of threat evolution over time to identify emerging trends and anticipate future developments.
- **Cross-industry comparison:** Identification of industry-specific targeting patterns and customization techniques.

## Limitations

We acknowledge several limitations in our analysis that may affect the generalizability of our findings:

- **Customer composition:** Our customer base skews toward enterprise, potentially underrepresenting threats targeted at SMBs.
- **Detection bias:** Our visibility is limited to attacks that reach our customers' email environments and does not capture threats blocked upstream by gateways or other security controls.
- **Geographic concentration:** While we have global coverage, our customer base is primarily in North America and Western Europe, potentially underrepresenting regional threats in other parts of the world.
- **Temporal window:** This report focuses on Q1 2025, and may not capture seasonal variations or longer-term trends.

## References

- 1 <https://cloud.google.com/blog/topics/threat-intelligence/adversarial-misuse-generative-ai>
- 2 [https://www.ic3.gov/AnnualReport/Reports/2023\\_ic3report.pdf](https://www.ic3.gov/AnnualReport/Reports/2023_ic3report.pdf)
- 3 <https://sublime.security/blog/b2b-freight-forwarding-scams-on-the-rise-to-evade-financial-fraud-crackdowns/>
- 4 <https://www.verizon.com/business/resources/T620/reports/2024-dbir-data-breach-investigations-report.pdf>
- 5 <https://sublime.security/blog/qr-code-phishing-decoding-hidden-threats/>
- 6 <https://sublime.security/blog/callback-phishing-via-invoice-abuse-and-distribution-list-relays/>