2025 YEAR IN REVIEW & 2026 THREAT LANDSCAPE OUTLOOK

The Industrialization of Cybercrime: Identities are Under Attack

eSENTIRE
THREAT RESPONSE UNIT

Executive Summary

In 2025, one thing became clear: identities are under attack.

For $200-300 per month, any aspiring cybercriminal can now subscribe to a Phishing-as-a-Service (PhaaS) platform that bypasses multi-factor authentication, harvests session tokens in real-time, and hands off compromised accounts to operators who begin exploitation within 14 minutes of credential theft.

This is the operational reality that eSentire's Threat Response Unit (TRU) documented based on thousands of incidents across our global customer base throughout 2025. What was once a fragmented criminal underworld has consolidated into a sophisticated industrial complex, one where digital identities are harvested, packaged, and monetized with the efficiency of legitimate enterprise.

The defining characteristic of this year's threat landscape was not any single attack technique, but rather the wholesale industrialization of cybercrime itself, accelerated by "as-a-Service" models that have fundamentally altered who can attack, how quickly they can strike, and at what scale.

Identity has become the primary battleground. **Account compromise accounted for 50% of all threat observations TRU investigated, a 389% increase over 2024.** This shift reflects a strategic recalculation by threat actors: why exploit vulnerabilities or deploy malware when you can simply log in?

Social engineering has scaled beyond human-paced attacks. Email bombing combined with IT impersonation surged 14x year-over-year, which is the largest increase of any threat category. These attacks flood inboxes with spam, then arrive via phone or Teams chat posing as IT support to "resolve" the manufactured crisis. The victim, overwhelmed and grateful, grants remote access. From there, the path to ransomware deployment is measured in hours, not weeks.

The browser has become a primary malware delivery vector. Attacks involving the use of ClickFix as an initial access vector increased nearly 300%, now representing over 30% of all malware delivery cases. These attacks contain no malicious files; victims execute the payload themselves after being manipulated by fake error messages and CAPTCHA prompts.

Trusted relationships continue to be attack vectors. Supply chain and trusted relationship attacks demonstrated 85% intrusion ratios, which is the highest of any access category. Security controls designed to stop outsiders offer little resistance to what appears to be legitimate partner activity.

The threat trends converge on a single reality: the speed of modern attacks has outpaced the speed of traditional defense.

Organizations relying on next-day log reviews, weekly threat hunts, or business-hours-only security operations are structurally disadvantaged against adversaries who operate continuously and move from initial access to impact in minutes.

The strategic imperative for security leaders is clear: threat detection and response capabilities must operate at the speed the threat landscape now demands. This requires continuous monitoring with the authority to act immediately, AI-driven analysis that can identify threats across high-volume telemetry, and human expertise focused on complex investigations and strategic decisions rather than alert triage.

Organizations that build these capabilities will contain incidents before they become breaches. Organizations that do not will learn through costly experience what this report demonstrates through data.

The 2025 Threat Landscape Analysis

I. The Identity Crisis: Understanding 2025's Fundamental Shift

To understand the 2025 threat landscape, we must recognize that what was once a loose collection of hackers has evolved into a sophisticated marketplace where specialized services can be purchased, combined, and deployed at scale.

Identity-related threats surged to the forefront not because attackers suddenly discovered credentials were valuable, but because the economics shifted in favor of identity-based attacks. The emergence of turnkey PhaaS platforms lowered barriers to entry while simultaneously increasing attack sophistication.

A threat actor no longer needs to understand how to intercept session tokens or mechanisms to bypass authentication; they can simply subscribe to a service that handles the technical complexity for them.

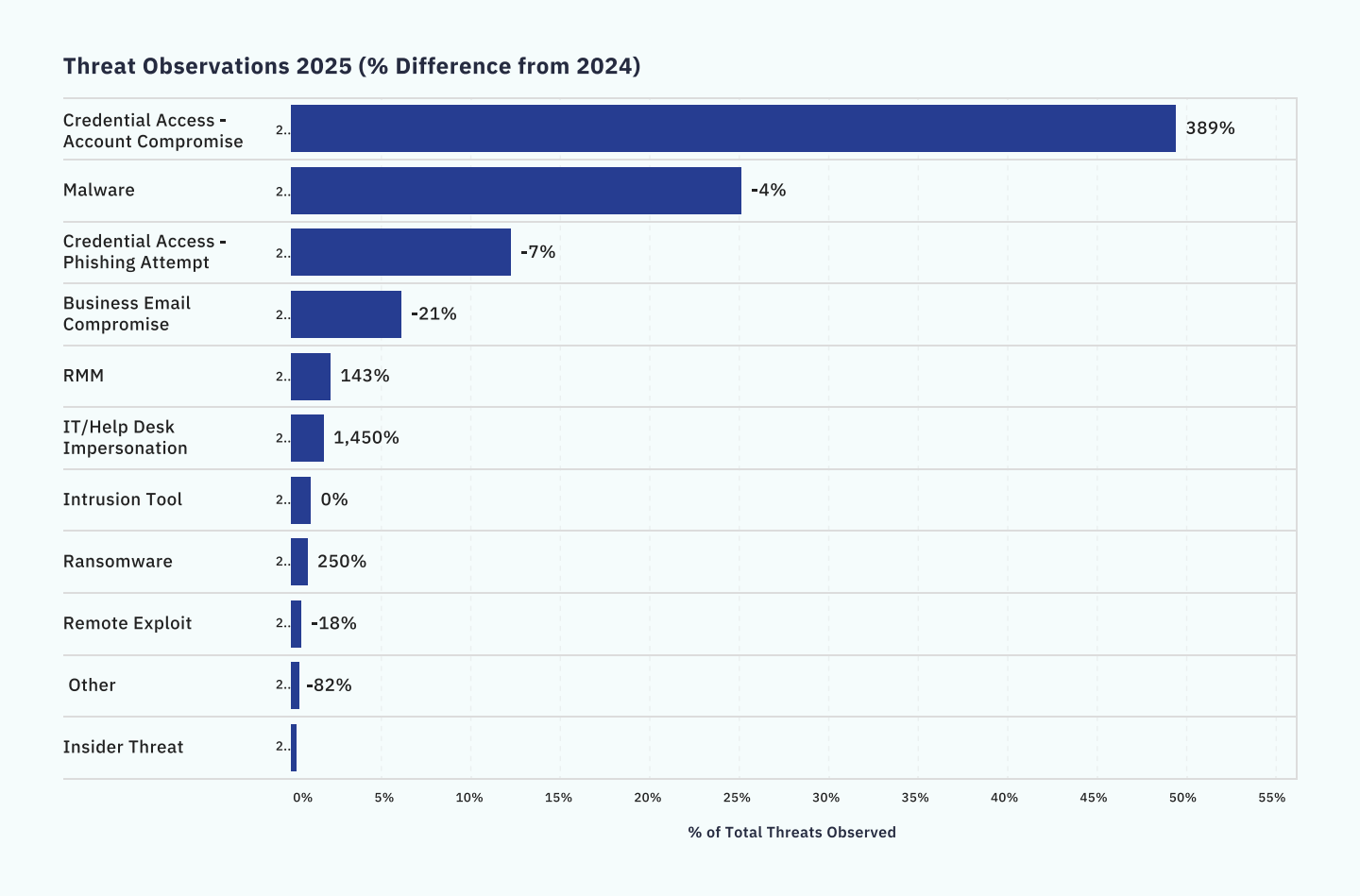


FIGURE 1: Year-over-Year Threat Type Observations

The distribution of threat observations in 2025 illustrates just how dramatically the landscape has reoriented around identity. After all, the new premise threat actors are relying on is simple: why break in when you can just log in?

Credential Access and Account Compromise threats dominated the threat landscape, representing over 50% of all observed threats with a staggering 389% year-over-year increase, dwarfing every other category in both volume and growth rate.

Other categories tell a supporting story: Remote Monitoring and Management (RMM) abuse surged 143% as attackers sought persistent access following initial compromise, while malware held steady at around 25% of cases, increasingly serving infostealers as a means to harvest credentials rather than an end in and of itself.

On the flip side, the cautious bright spot is that Business Email Compromise (BEC) attacks declined 21% despite the surge in account takeovers.

This suggests that improved threat detection and response to compromised accounts is disrupting the attacker's monetization pipeline.

However, account compromises are growing nearly 4x faster than BEC attacks are declining, meaning attackers are gaining ground on initial access even as defenders improve at limiting downstream impact.

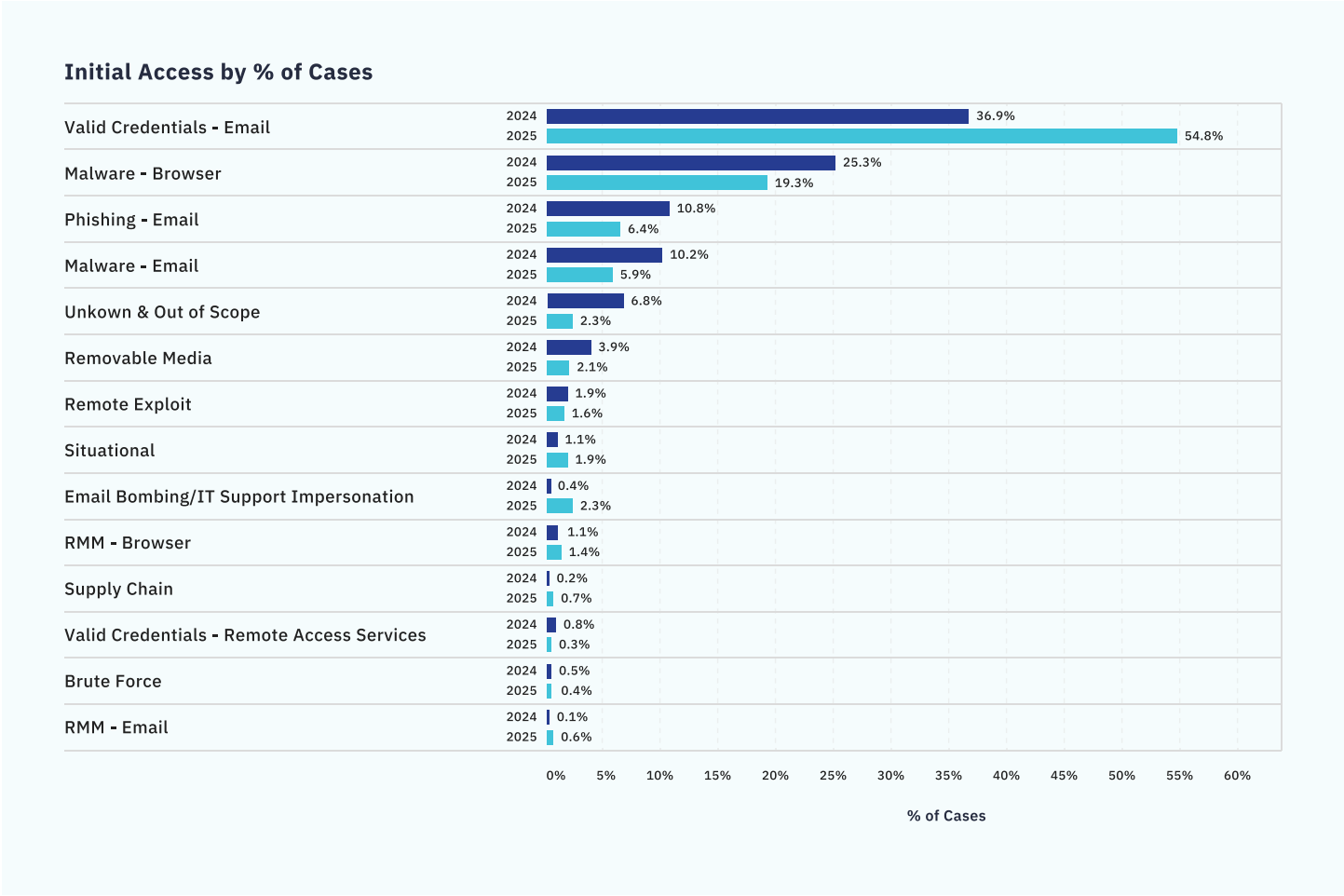


FIGURE 2: Initial Access Methods

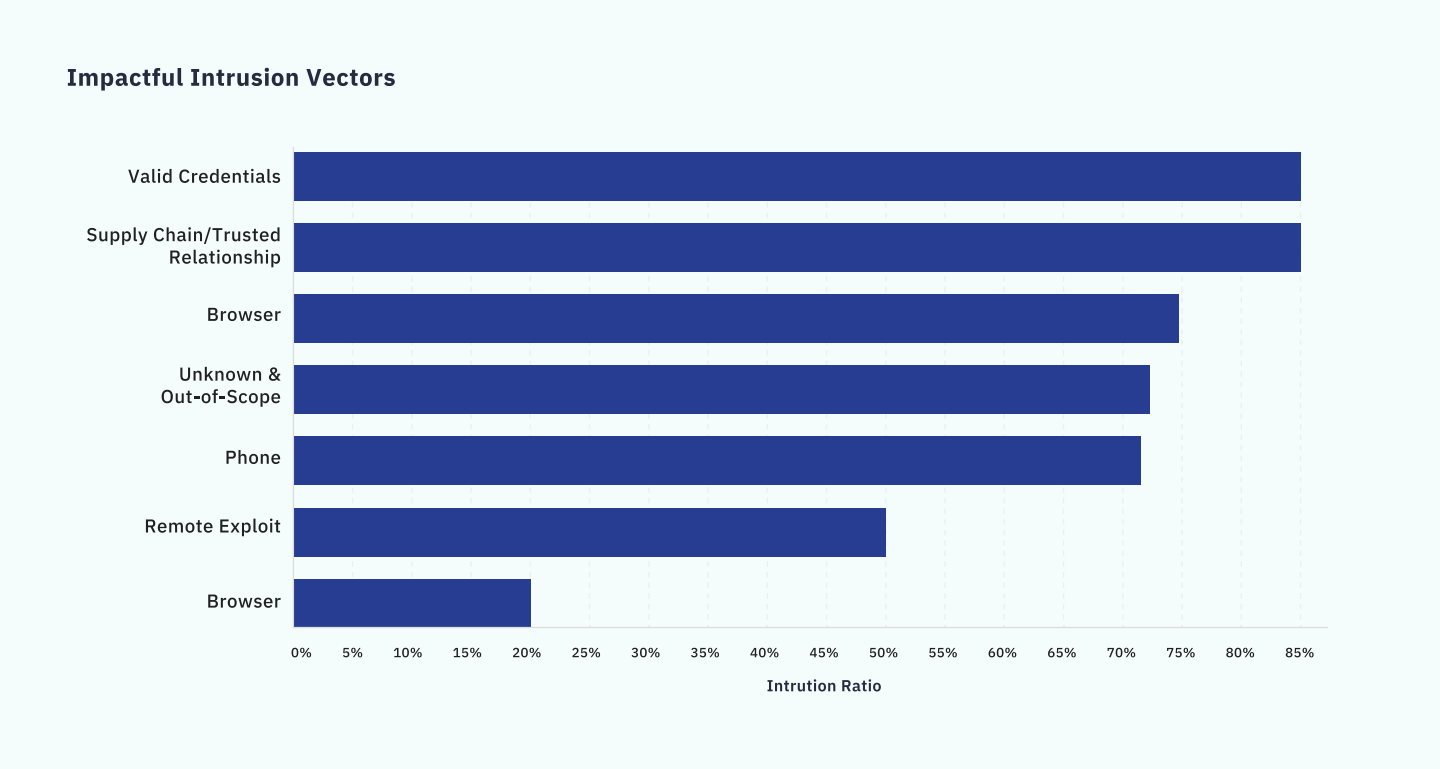


FIGURE 3: Intrusion Ratio by Access Vector

When looking at data around initial access vectors, the numbers tell a stark story. **Email-initiated account compromises rose from 36.9% in 2024 to 54.8% in 2025** of the total incidents investigated by the eSentire TRU team, a **110% year-over-year increase**. Most of these attacks stemmed from PhaaS operations, which accounted for **63% of all account compromise incidents**.

These platforms leverage Adversary-in-the-Middle (AitM) techniques to intercept credentials and session tokens in real-time, primarily targeting cloud services like Microsoft 365 where a single compromised identity can unlock a treasure trove of sensitive data.

This is not a gradual trend; it's a step-change with a very clear understanding: traditional security models built around perimeter defense and endpoint protection are fundamentally insufficient against adversaries armed with valid user credentials.

Raw numbers only tell part of the story; the intrusion ratio data reveals something equally important about the effectiveness of different access vectors.

Valid Credentials attacks demonstrated an 85% intrusion ratio, meaning that when threat actors obtained valid credentials, they successfully progressed beyond initial access in 85 out of 100 cases. This represents a decrease from nearly 100% in 2024, reflecting improved detection capabilities for credentials compromised through AitM phishing.

However, this improvement is offset entirely by the sheer volume increase in credential-based attacks. Although security teams are getting marginally better at catching compromised credentials in use, threat actors are stealing so many more credentials that the net outcome is significantly worse.

It's a treadmill that organizations cannot outrun through threat detection alone; reducing the success rate of credential theft itself must be part of the equation.

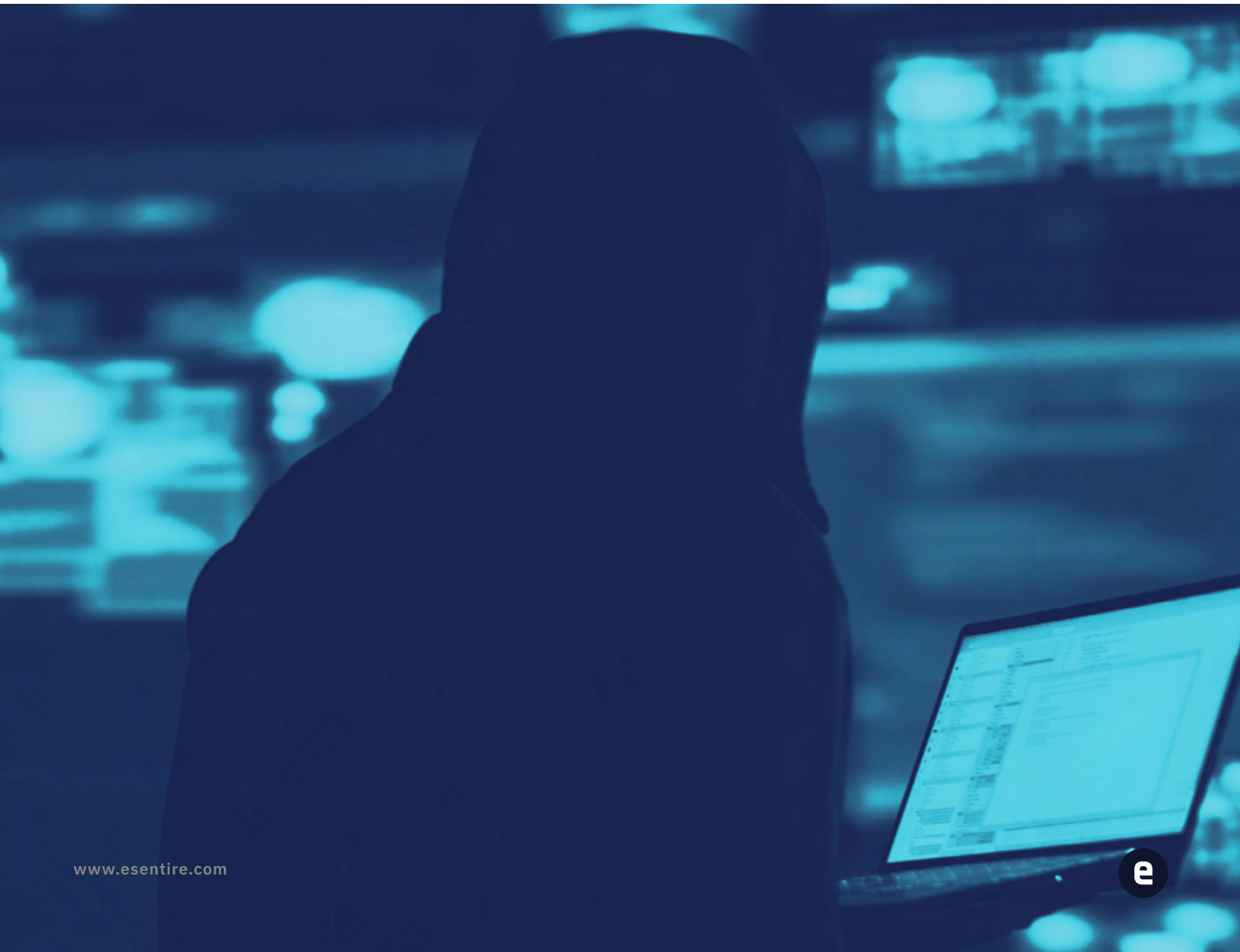
Cyberattacks that leveraged third-party supply chain and trusted relationships emerged as particularly concerning, showing an 85% intrusion ratio in 2025. What these types of attacks share is the exploitation of pre-established trust; attackers don't need to defeat security controls because they inherit the access rights of entities the victim already trusts.

When looking at supply chain compromises, TRU documented multiple cases involving compromised npm packages, including a large-scale attack involving a worm dubbed "Shai Hulud".

With trusted relationship attacks, TRU observed numerous cases involving ransomware operators abusing SonicWall SSL VPN credentials belonging to third-party MSPs. These credentials were mapped to over-privileged Active Directory accounts, providing threat actors with immediate privileged access to victim networks.

Vishing attacks (i.e., those that're initiated via phone calls) demonstrated a 72% intrusion ratio, driven by the email bombing and IT impersonation campaigns that defined 2025's social engineering landscape.

Additionally, out-of-scope (unmanaged) devices continue to present significant challenges for early-stage containment. In these scenarios, adversaries leverage compromised VPN credentials to connect their own unauthorized devices to target networks, bypassing traditional security controls designed for managed endpoints.



The Industry Lens: Who Is Being Targeted and Why

The distribution of threat cases across industries reveals patterns shaped by both attacker opportunism and deliberate targeting. The Software industry experienced the largest proportion of threat cases in 2025, showing nearly a 15% year-over-year increase. This is likely a reflection of the Software sector's high concentration of valuable intellectual property, cloud infrastructure access, and potential for supply chain leverage.

Manufacturing ranked second with a notable 33% increase, likely driven by operational technology vulnerabilities and the sector's acute sensitivity to downtime that makes ransomware extortion particularly effective. Business Services followed with an 8% increase, consistent with its role as a conduit to downstream client environments.

However, Construction presents an interesting counterpoint: while the overall case volume declined by 27%, the sector exhibited notably higher percentages of identity-related threats when targeted.

This suggests that when attackers do pursue construction firms, typically those involved in large financial transactions, they prioritize credential theft and BEC over malware-driven approaches, likely seeking to intercept payment flows rather than disrupt operations.

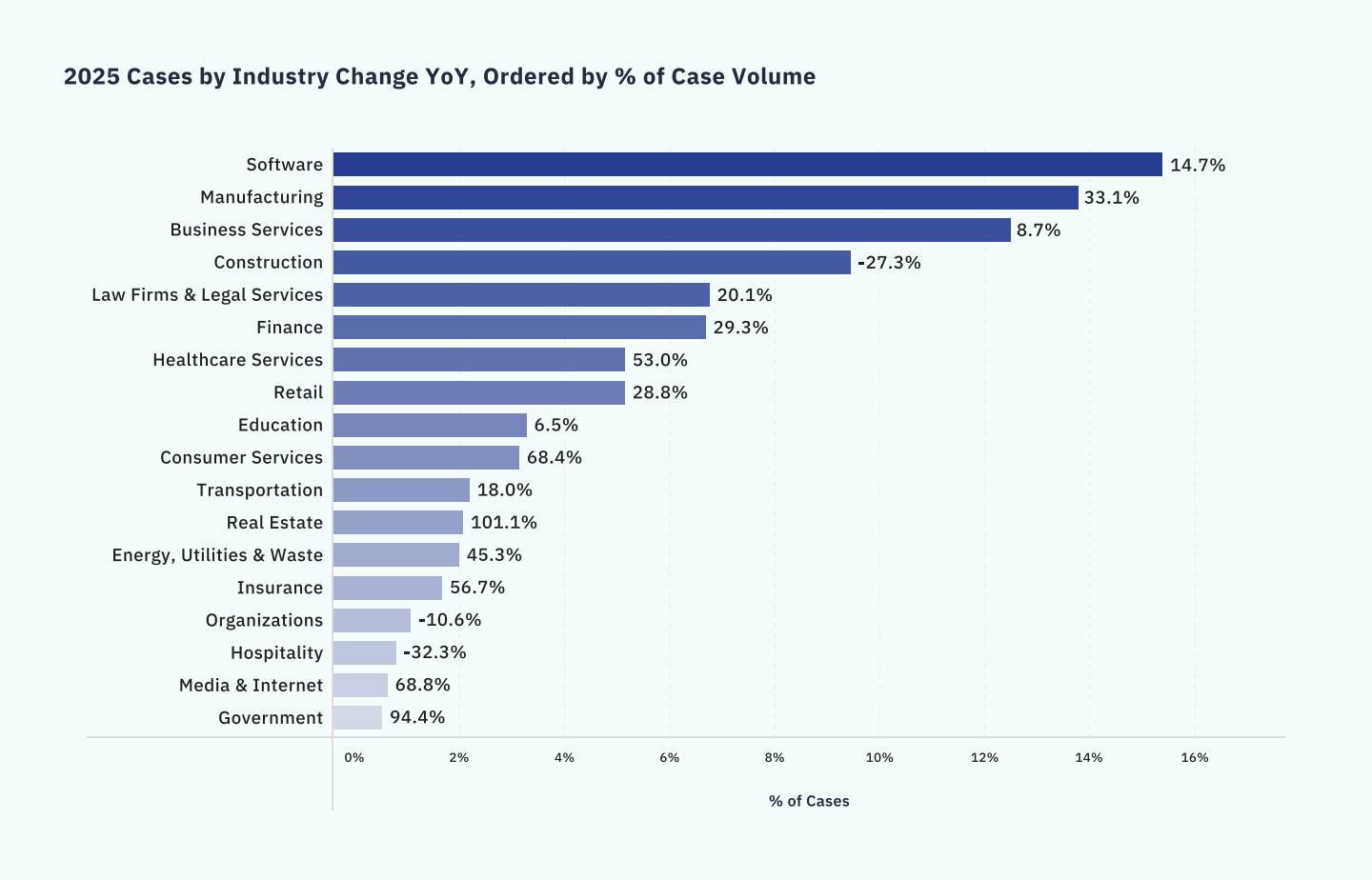


FIGURE 4: Year-over-Year Industry Threat Observations

When examining the distribution of all threat types across industries, most sectors contended primarily with identity-related threats including credential phishing, account compromise, and BEC attacks.

Industries such as Retail and Construction exhibited notably higher percentages of account compromise threats, indicating either increased vulnerability or deliberate targeting. On the other hand, the Legal industry experienced the highest proportion of IT/Helpdesk Impersonation attacks, suggesting particular susceptibility or deliberate targeting of this sector.

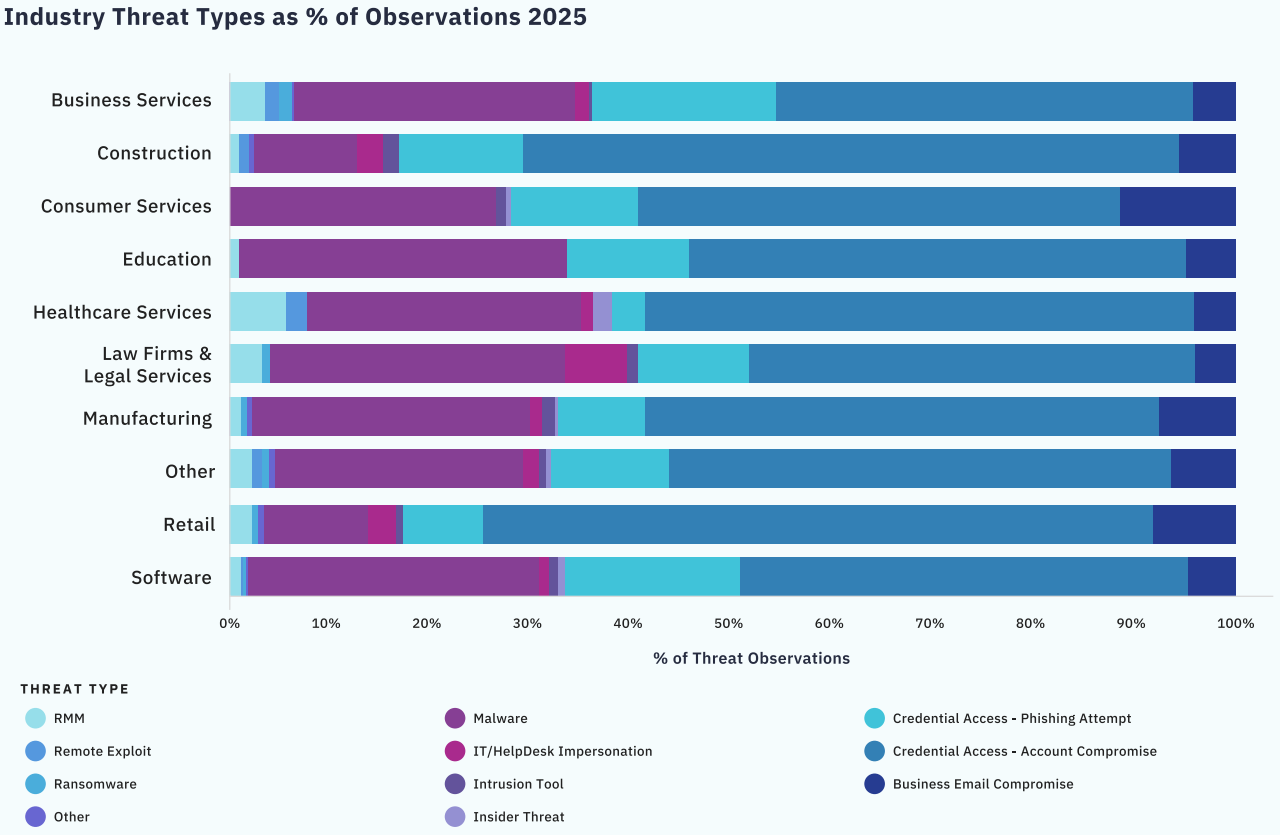


FIGURE 5: Observed Threat Types by Industry

What to Understand for an Effective Cyber Defense Strategy

When valid credentials provide an 85% intrusion ratio, perimeter defenses become insufficient; attackers aren't breaking in, they're logging in. The speed of modern identity attacks demands AI-powered threat response capabilities that can suspend sessions and trigger step-up authentication within minutes, not hours.

Organizations require continuous identity monitoring that establishes behavioral baselines and flags deviations in real-time: unusual login locations, impossible travel, access patterns inconsistent with role, and authentication from known anonymization infrastructure.

II. Phishing-as-a-Service: The $300/Month Enterprise Breach

The Phishing-as-a-Service model has become a dominant force in the threat landscape so understanding its mechanics is essential for developing an effective cyber defense strategy.

The strategic importance of PhaaS lies in how it packages advanced attack kits, infrastructure, and operational support into accessible subscription services. A substantial majority of observed account compromise cases belong to these ready-made platforms.

The PhaaS model dramatically lowers technical barriers to entry, enabling a broader range of threat actors to execute sophisticated campaigns that were once the exclusive domain of highly skilled groups.

The consequence is a massive global amplification in the scale and frequency of phishing attacks.

The Infrastructure Behind the Attacks

TRU's tracking of PhaaS infrastructure revealed consistent patterns that create threat detection opportunities for defenders. A critical finding concerns operational security patterns:

First, operators of AitM services invested heavily in the "front-end" of attacks, such as anti-bot captchas, HTML obfuscation, and traffic direction systems designed to bypass email gateways and security products. However, the backend infrastructure for relaying credentials and MFA tokens tended to be far less ephemeral.

Second, follow-on actions by PhaaS affiliates rarely used the same network infrastructure or even connection attributes (e.g., user-agent strings) as the initial phishing operation. In many cases, this activity occurred from known VPN providers or custom cloud-hosted proxies with moderately static footprints. For BEC actors this pattern held true, with over **50% of BEC cases involving access from a known consumer VPN provider**.

TRU also found that operators and affiliates generally faced minimal impedance from location-based access controls. While logins generally matched the country of the target business, they typically occurred from IP addresses tied to cities and states well beyond realistic travel limits for employees.

Credentials relayed by Tycoon2FA primarily used IP addresses geographically linked to five U.S. cities: Los Angeles, New York, Phoenix, Atlanta, and Chicago.

The re-use of infrastructure and VPN services suggests adversaries aren't facing strong headwinds accessing accounts. This likely reflects visibility gaps in identifying VPNs or high-risk network ranges in identity log data or alert fatigue from poorly tuned conditional access controls overwhelming defenders with high-volume alerts lacking sufficient context.

CASE STUDY

Inside Tycoon2FA: Anatomy of a PhaaS Campaign

Tycoon2FA emerged in August 2023 and rapidly evolved into the dominant PhaaS platform of 2025. Its sophistication rivals that of legitimate security tools, complete with user interfaces, customer support channels, and regular updates to counter defensive measures.

The attack chain begins with a phishing email, often containing a fake invoice attachment. Victims are directed to a phishing site protected by multiple layers: custom CAPTCHA implementations (the platform recently shifted from Cloudflare Turnstile to proprietary solutions), anti-debugging mechanisms, and traffic filtering designed to frustrate security researchers. Upon completing the CAPTCHA, victims encounter a convincing fake sign-in page for their target service.

What happens next is significant; rather than simply collecting static credentials, Tycoon2FA operates as a transparent proxy between the victim and the legitimate authentication service (e.g., Microsoft Entra ID, Gmail).

Credentials and session tokens are relayed in real-time through proxy infrastructure. Historically, this meant leveraging Global Connectivity Solutions LLP (a known bulletproof hosting provider) with a 2025 transition to Hivelocity Inc. for the final hop to Entra ID.

The image below shows an example timeline where Tycoon2FA successfully captured a session token and relayed it to the Tycoon2FA client, where in only minutes they made use of the token through Private Internet Access VPN and began creating inbox forwarding rules.

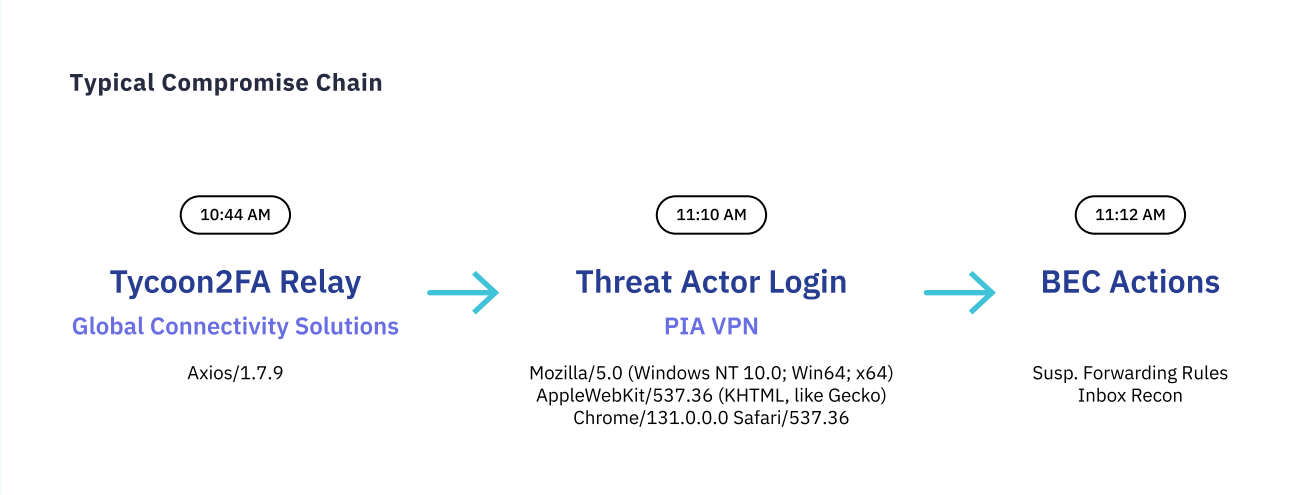


FIGURE 6: PhaaS to BEC Handoff Timeline

Phishing attacks rapidly escalate to Business Email Compromise in mere minutes.

In TRU's analysis of 100 Tycoon2FA incidents, threat actors began exploitation just 14 minutes on average after the initial compromise (i.e. "activation time").

This activation time was even more rapid in industries such as Real Estate, Finance, Retail, and Construction, sectors that regularly engage in large financial transactions, making them prime targets for payment redirection schemes.

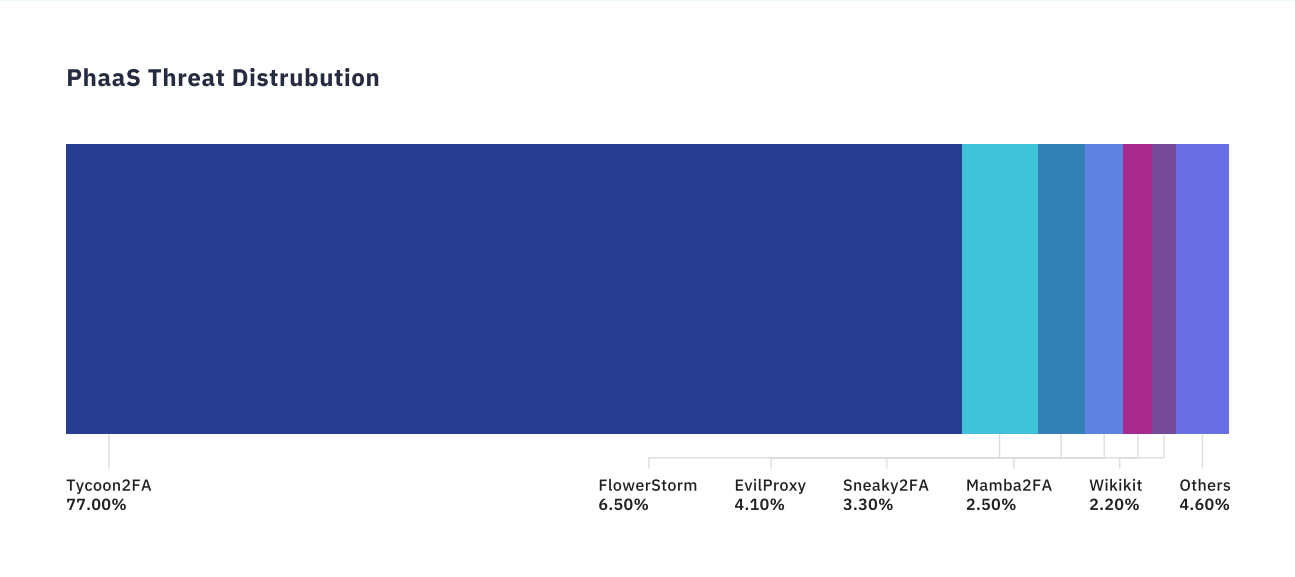


FIGURE 7: PhaaS Threat Distribution

These services are not simple templates; they are comprehensive, continuously updated offerings designed to bypass modern security controls, including MFA.

The widespread availability and continuous evolution of these PhaaS kits provide the fuel for the heightened number of account takeover cases TRU has seen. However, the tools are only the first step in a highly efficient monetization process.

The Business Email Compromise (BEC) Monetization Pipeline

The typical objective of an account takeover operation is financial gain. Compromised identities are either sold through underground marketplaces or used immediately to execute Business Email Compromise (BEC) attacks.

These attacks leverage compromised accounts to manipulate financial transactions and redirect funds. With reported losses measured in billions globally for several years running, BEC has created a thriving marketplace for PhaaS services.

In fact, **28% of BEC cases analyzed by TRU were traced back to PhaaS services**, with the majority linked to Tycoon2FA and FlowerStorm.

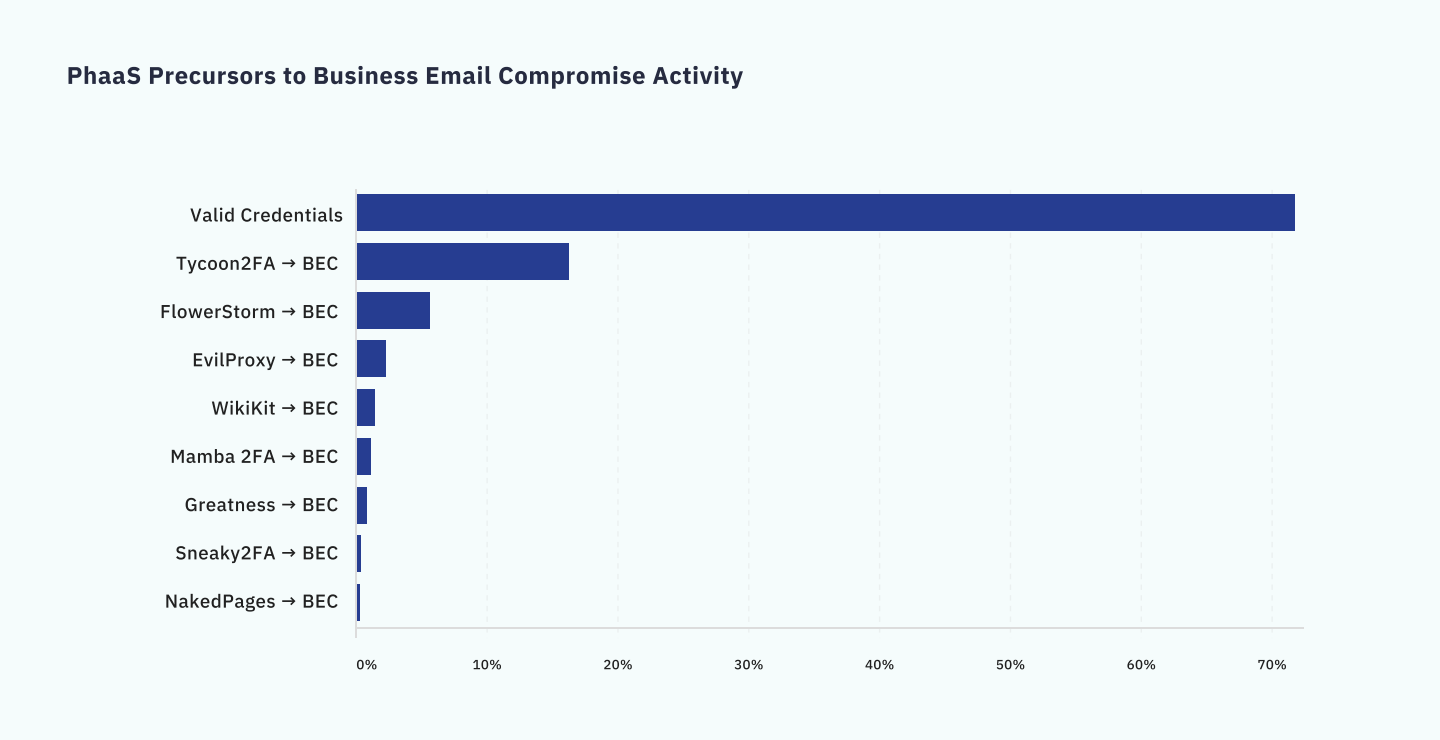
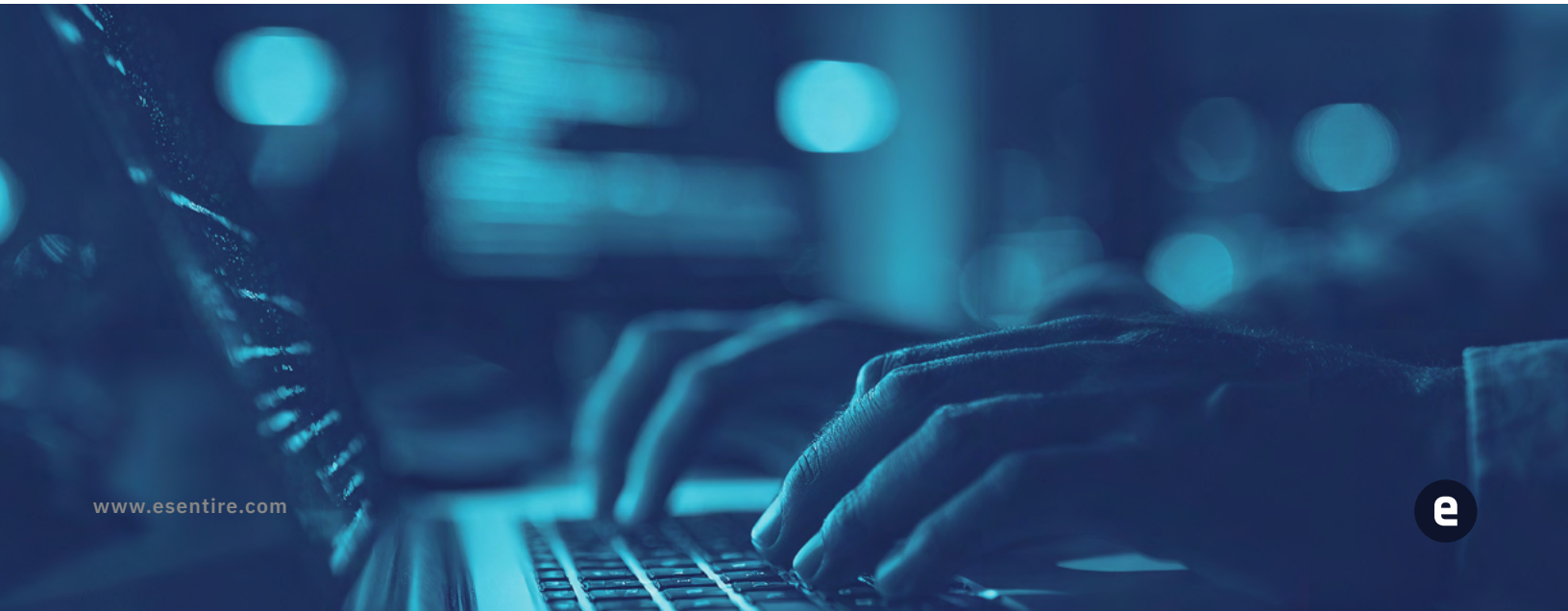


FIGURE 8: Precursors to Business Email Compromise



Moreover, TRU also observed a **30% increase in successful account takeovers** between the first and second half of 2025. This represents more than a quantitative increase; it signals a fundamental shift fueled by growing criminal demand for stolen identities and the widespread availability of sophisticated PhaaS platforms.

The figure below illustrates distinct phishing-related cases by impact, with cases categorized into three groups:

- **Purple** - Account compromise uncertain. Email bypassed spam filters, no evidence of account compromise.
- **Magenta** - Account was compromised by threat actor(s), no evidence of Business Email Compromise (BEC).
- **Teal** - Business Email Compromise (BEC), evidence of malicious activity post-account compromise.

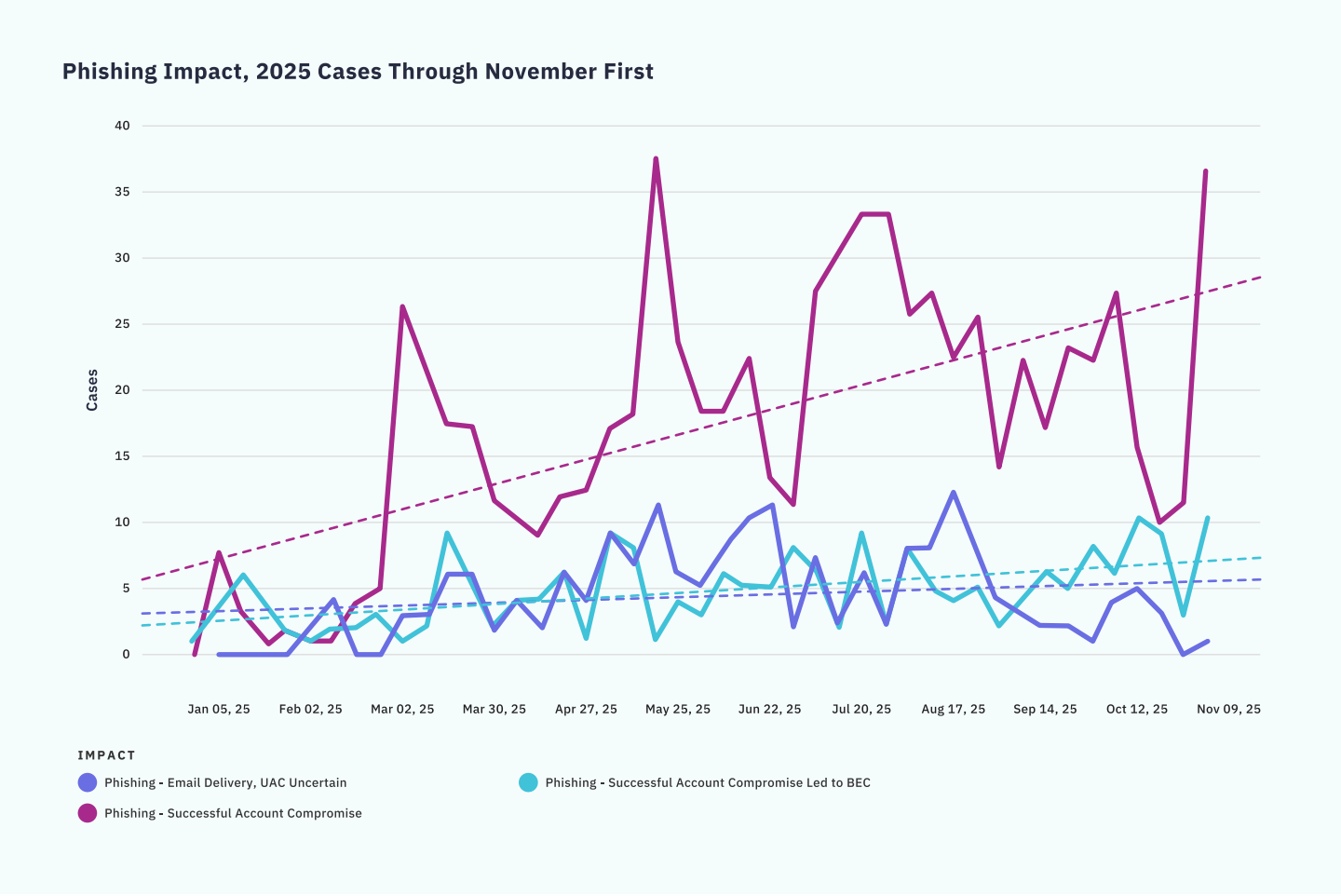


FIGURE 9: Weekly Phishing Cases by Impact

Exploiting Trusted Services

Threat actors proved to be quite creative in how they abused legitimate infrastructure throughout 2025. One prominent technique involved exploiting Microsoft 365 Exchange Online's Direct Send feature, which was originally designed to allow devices and applications (such as multifunction printers and scanners) to send email without authentication credentials.

Attackers exploited Direct Send to send phishing emails that appeared to originate from the victim's own domain without requiring any credentials or access to the target environment. In observed attacks, these spoofed emails originated from external IP addresses and failed SPF, DKIM, and DMARC authentication checks.

However, because Direct Send routes messages through Microsoft 365's infrastructure and prevents standard email security inspection, these emails were still delivered to recipients' inboxes.

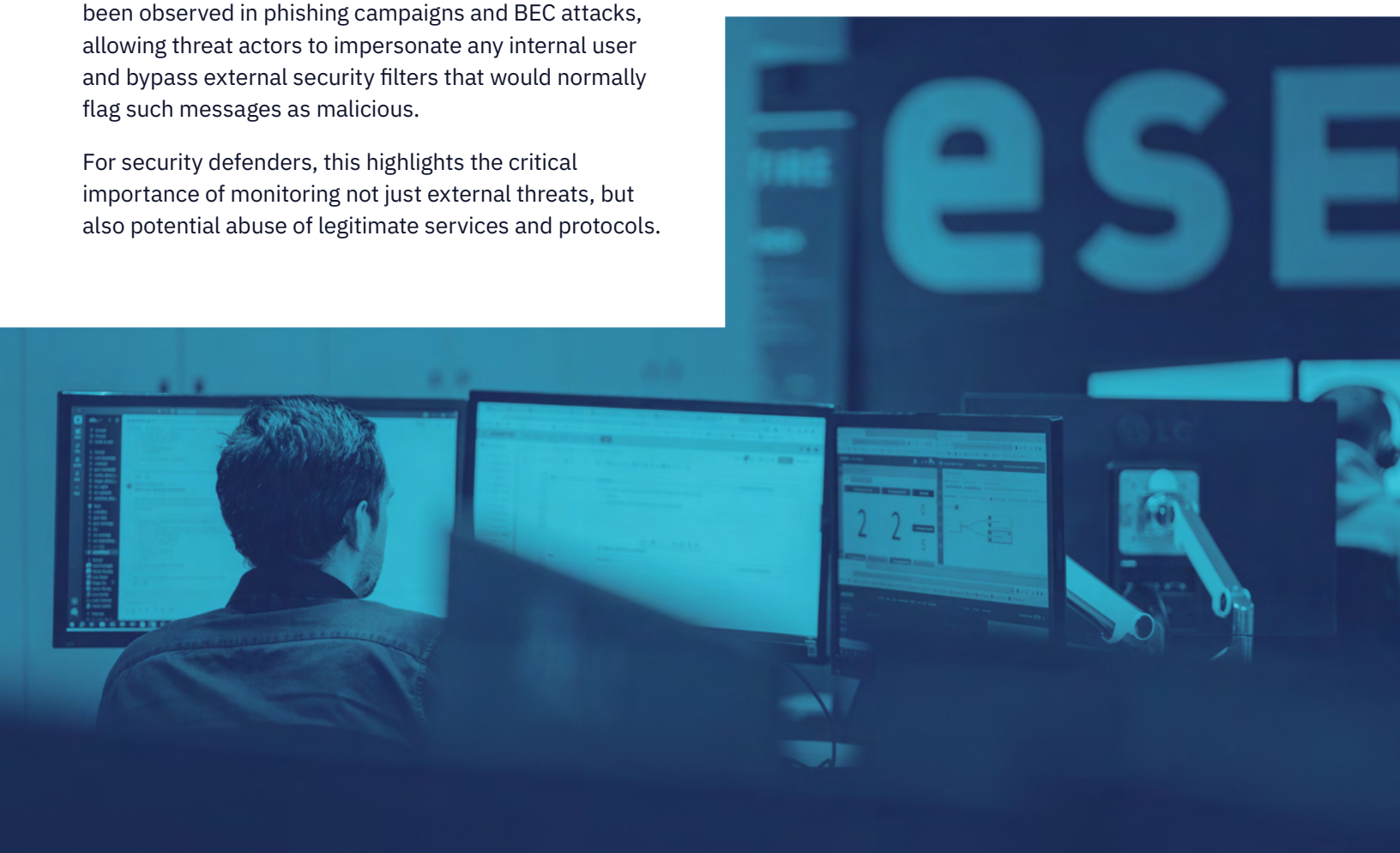
The attack's effectiveness is amplified when organizations have DMARC policies set to 'p=none' (monitoring only), as emails that fail authentication are delivered regardless of the failure. This technique has been observed in phishing campaigns and BEC attacks, allowing threat actors to impersonate any internal user and bypass external security filters that would normally flag such messages as malicious.

For security defenders, this highlights the critical importance of monitoring not just external threats, but also potential abuse of legitimate services and protocols.

What to Understand for an Effective Cyber Defense Strategy

Traditional MFA is no longer a reliable control against sophisticated PhaaS operations. However, the more significant finding is operational: PhaaS backend infrastructure proved far less ephemeral than front-end evasion techniques, and affiliates consistently reused VPN providers and network ranges. This creates detection opportunities for security operations teams with access to global threat intelligence.

Organizations should integrate ASN-based and IP reputation data into authentication monitoring, flag access from known anonymization services, and ensure 24/7 coverage to act on alerts before the 14-minute window closes. The compressed timeline between credential theft and exploitation means that detection without rapid response capability is effectively no detection at all.



III. Browser-Based Malware Delivery

Browsers emerged as the primary battlefield for malware delivery in 2025, with threat actors increasingly favoring techniques that manipulate human behavior.

TRU's analysis of incident case data shows malware was predominantly delivered using browser-based methods. The majority used deceptive tactics to trick users into executing payloads while software exploits initiated against browsers or plugins remained rare.

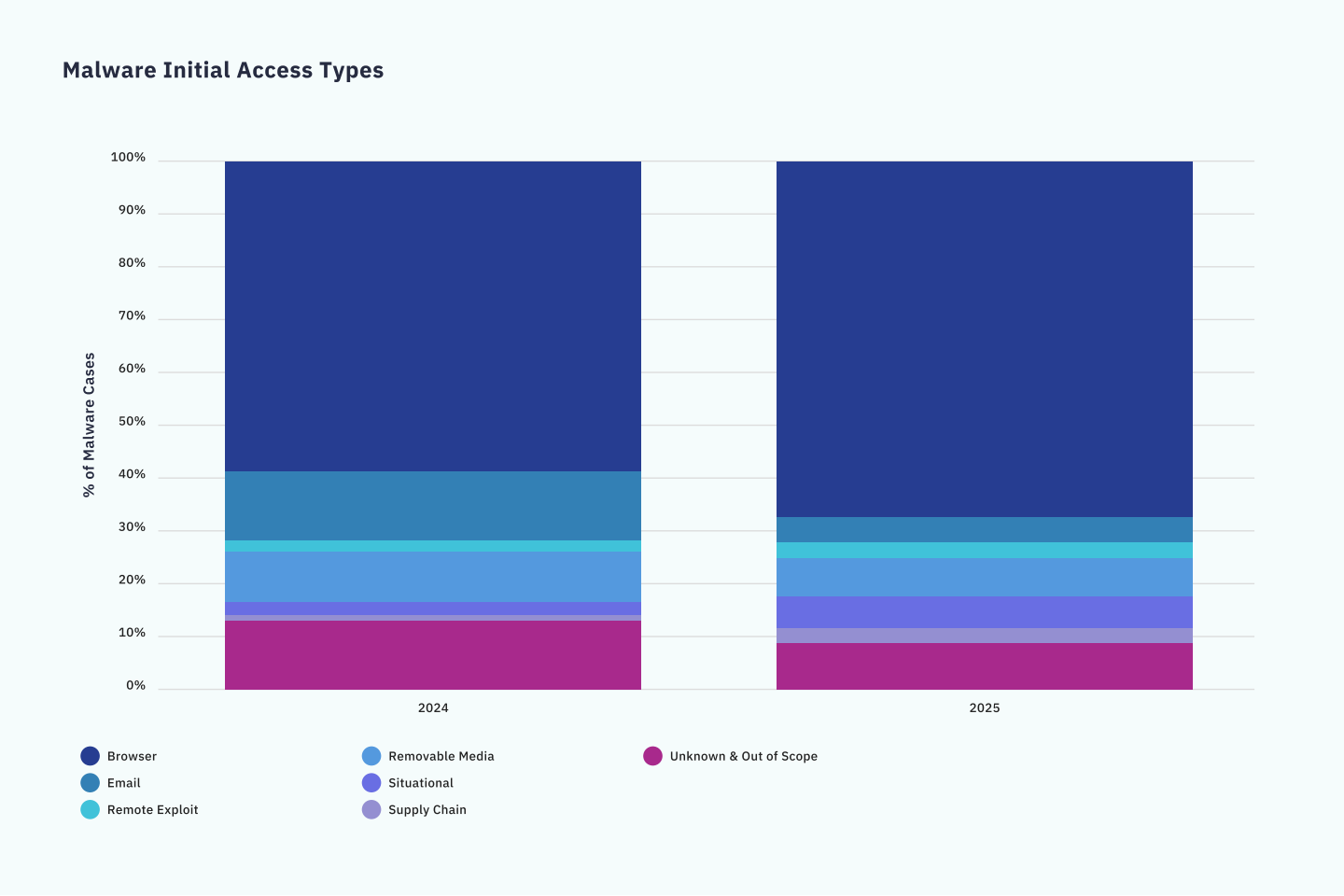


FIGURE 10: Year-over-Year Comparison of Malware Initial Access Vectors

Browser Delivery Subtypes: The Evolving Landscape

In Q4 2025, threat actors primarily relied on ClickFix and User Downloads for initial access, while other techniques rose and fell based on operational availability and organizations' cyber defense strategies.

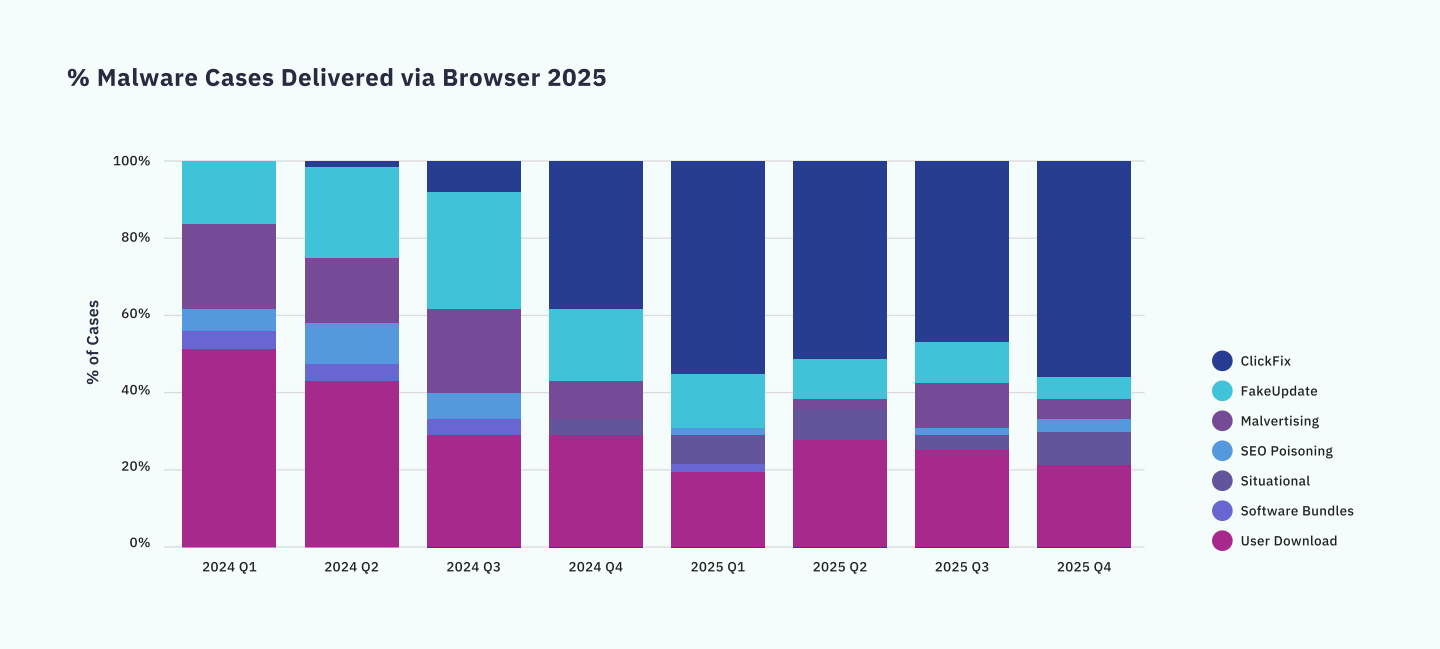


FIGURE 11: Quarter-over-Quarter Changes in Browser-Based Delivery

In addition to the rise of ClickFix and User Downloads as the primary delivery mechanisms, TRU also observed the use of fake updates and malvertising in 2025.

Fake Updates maintained steady momentum, averaging 10-11% of malware cases throughout the year. Led by SocGholish and NetSupport RAT installations, these schemes inject fake browser or software update prompts while users browse compromised websites.

Unlike ClickFix, which requires explicit user action to paste and execute commands, fake updates exploit the learned behavior of clicking through update prompts, a lower-friction social engineering approach that trades sophistication for volume.

Malvertising (i.e., malicious advertising impersonating popular applications) tells a story of adaptation. Heavily abused in 2024 before search platforms implemented countermeasures, threat actors responded with more sophisticated methods: pre-farmed or compromised advertising accounts that bypass new-account scrutiny, and TDS gateways that filter out security researchers before serving malicious content.

However, despite these adaptations, malvertising remained less common in 2025 than its 2024 peak, suggesting that platform-level defenses have provided at least partial friction.

The most notable shift was the significant decrease in **SEO Poisoning** compared to 2024. This decline traces directly to Gootloader, a JScript-based downloader that dominated SEO poisoning campaigns, going on hiatus from Q3 2024 through most of 2025 before resurfacing in Q4.

This pattern illustrates how the browser delivery landscape can shift dramatically based on the operational status of a single prolific malware family.

CASE STUDY

ClickFix: The Predominant Technique

ClickFix (also known as FakeCaptcha) was a prolific initial access technique used by threat actors throughout 2025, increasing from 7.8% to 30.7% of all malware cases—a nearly 300% year-over-year surge.

TRU identified over 65 distinct intrusion chains leveraging ClickFix throughout the year, demonstrating its widespread adoption across the threat landscape.

The technique's effectiveness lies in its psychological manipulation. ClickFix is primarily distributed through emails, malvertising, or compromised websites (often via fake WordPress plugins) that display deceptive pop-ups mimicking browser errors, CAPTCHA verifications (like fake reCAPTCHA or Cloudflare Turnstile), or service issues from brands such as Google Meet and Microsoft.

Users are prompted to click "Fix It," which copies a malicious command (often Base64-encoded) to the clipboard. They are then instructed to press Windows + R, paste it into the Run Prompt or PowerShell, and press enter, effectively executing malicious code while bypassing defenses that rely on files being written to disk.

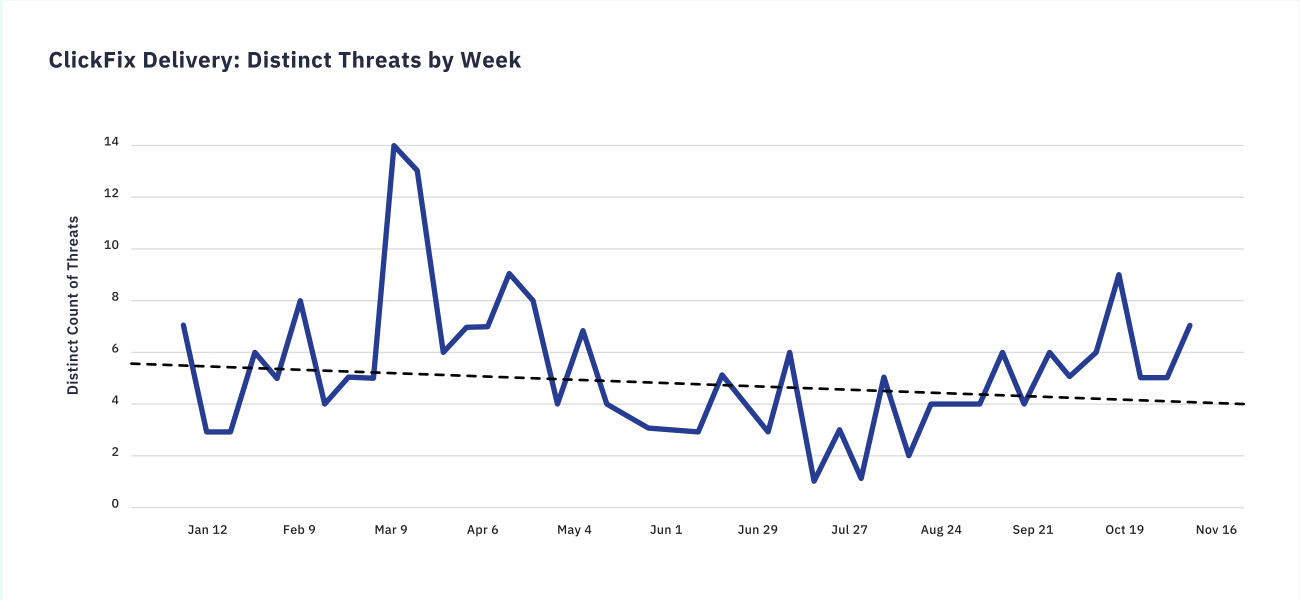


FIGURE 12: ClickFix Weekly Unique Threats

The top malware families delivered through ClickFix include Lumma Stealer, NetSupportManager RAT, and Rhadamanthys, a combination of information stealers and remote access tools that provides threat actors with both immediate credential monetization opportunities and persistent access for follow-on activities.

Traffic Distribution Systems: The Backbone Infrastructure

Running successful malware campaigns via browser-based methods requires more than just a malicious payload. It requires infrastructure that can filter out security researchers, route victims based on geography or browser fingerprint, and survive takedown attempts.

Traffic Distribution Systems (TDS) provide this backbone, acting as a gatekeeper for malware campaigns. It evaluates incoming traffic, blocks known security vendor IP ranges and analysis environments, and routes legitimate victims to the appropriate payload based on targeting criteria.

This layered architecture means that simply blocking a malicious domain often provides only temporary protection; the TDS operator can just rotate domains while maintaining campaign continuity.

In 2025, threat actors benefited greatly from an increasingly sophisticated market of TDS offerings with Kongtuke being the most common TDS observed by TRU to deliver a variety of top malware including Lumma Stealer.

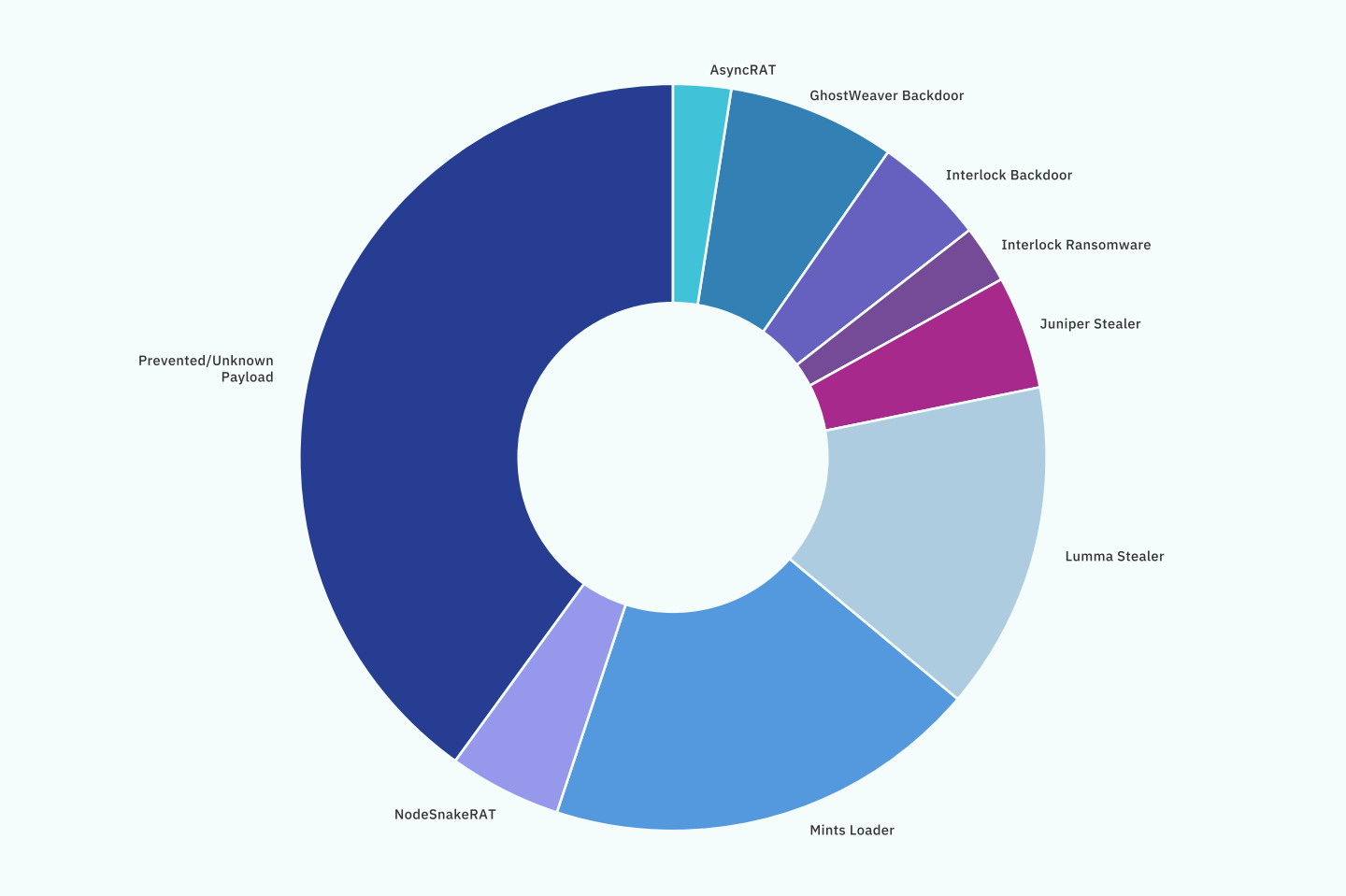


FIGURE 13: Kongtuke Payload Distribution

Notably, many IPs tied to Kongtuke were associated with **AS399629**, a **Wyoming-based entity** registered via agent proxy. This pattern of using legitimate-appearing shell entities for malicious infrastructure complicates attribution and legal takedown efforts, while providing attackers with the appearance of operating from reputable U.S.-based hosting.

What to Understand for an Effective Cyber Defense Strategy

ClickFix's effectiveness stems from bypassing file-based detection entirely, malicious commands execute directly from user input, leaving no traditional malware artifact to scan. Therefore, threat detection strategies must shift to behavioral indicators: clipboard-to-PowerShell execution patterns, Base64-encoded command strings, and process lineage anomalies where user-initiated Run prompts spawn network connections or child processes.

Endpoint detection and response (EDR) capabilities must be paired with analyst oversight to distinguish legitimate administrative activity from social engineering-induced execution. The 65+ distinct intrusion chains observed indicate this is not a single campaign but an ecosystem-wide technique requiring broad detection coverage.

IV. Email Bombing and IT Impersonation: Social Engineering at Scale

Over 2025, TRU observed a significant rise in the use of Email Bombing combined with IT impersonation attacks. What began as 4 observations of these social engineering tactics later increased to 60 observed threat cases by the end of 2025 – a **14x increase year-over-year** and the largest increase of any threat type.

Moreover, Email Bombing and IT Support Impersonation combines two significant trends in the 2025 threat landscape: increasingly sophisticated social engineering tactics and the growing use of Remote Monitoring and Management (RMM) tools for initial access.

This attack pattern represents a sophisticated fusion of technical capability and psychological manipulation. The two-stage approach exploits both email infrastructure and human trust in IT support.

Stage One: The Manufactured Crisis – Attackers flood target inboxes with overwhelming volumes of spam emails, creating confusion and service degradation. The victim's inbox becomes essentially unusable, a deliberately manufactured crisis to set up the second stage.

Stage Two: The "Rescue" – Immediately following the email flood, attackers establish contact with victims by posing as IT support and offering to resolve the deliberately created problem. During these "support" interactions, victims are manipulated into granting remote access to their devices. Once granted access, attackers can deploy various payloads, with several incidents escalating to the deployment of Black Basta ransomware in the most severe cases.

In examined cases, attackers contacted victims predominantly through Microsoft Teams calls or chats. **Over 80% involved attackers using Microsoft Teams accounts from suspected compromised organizations, while the remainder utilized temporary demo Microsoft accounts.**

This demonstrates threat actors' investment in acquiring compromised accounts specifically to bypass organizational trust filters.

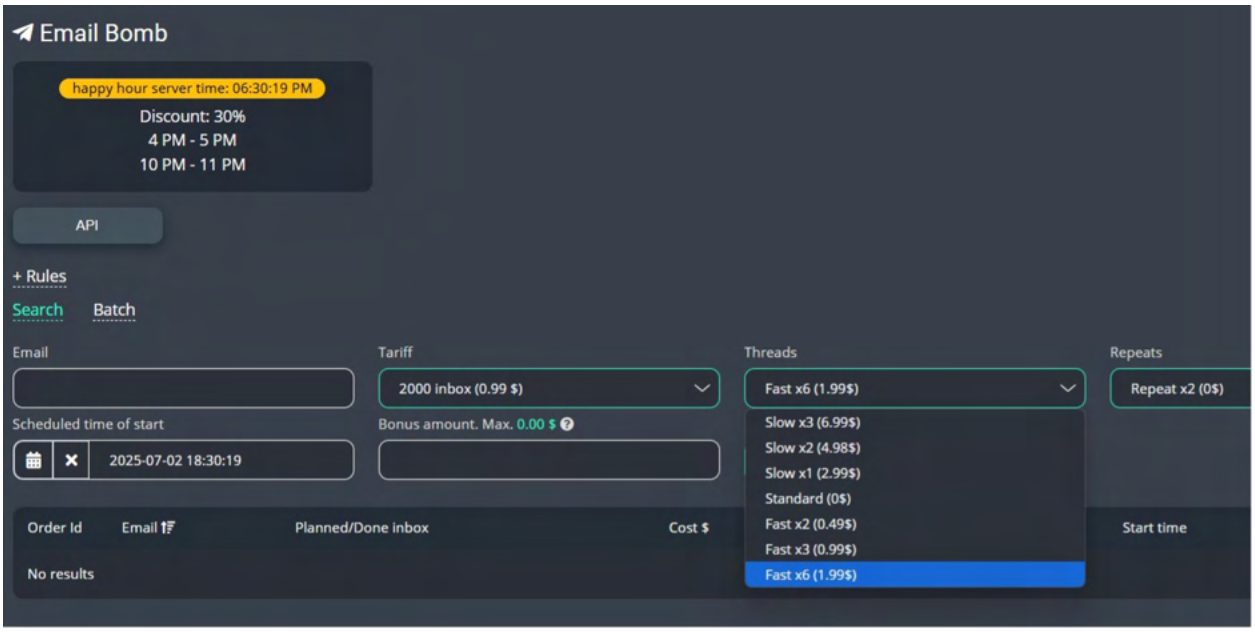


FIGURE 14: Email Bombing Service — Screenshot from July 2025 TRU Intelligence Briefing showing underground email bombing service offering.

The Email Bombing Intrusion Chain

After establishing contact, threat actors typically leveraged Microsoft Quick Assist for initial access, then promptly deployed secondary RMM tools and additional intrusion software.

In several cases, TRU observed adversaries utilizing the open-source Quick Emulator (QEMU) to create “rogue virtual machines”, conducting malicious activities within isolated virtual environments that effectively circumvent security monitoring and endpoint protection.

The Legal Services industry was particularly impacted, accounting for 28% of all email bombing cases. This concentration suggests either particular vulnerability or deliberate targeting; legal firms often handle sensitive transactions and may have less mature security operations than financial institutions.

To appear close to the target, threat actors used anonymization services (i.e., VPNs and proxies) for IP addresses tied to Microsoft Teams chat sessions. Top VPN services included MullVad, NordVPN, and BelkaVPN.

Other notable source infrastructure included US-based providers, AS399629 (BL Networks) and AS398343 (Baxet Group Inc.), UK-based AS215540 (GLOBAL CONNECTIVITY SOLUTIONS LLP), and Russian-based AS8359 (MTS PJSC).

Vishing attacks demonstrated a 72% intrusion ratio, reflecting the effectiveness of this human-centric approach. When attackers successfully reach a target on the phone and execute the IT support pretense, they succeed in gaining access nearly three-quarters of the time.

What to Understand for an Effective Cyber Defense Strategy

The 72% intrusion ratio for vishing attacks highlights a hard truth that when attackers reach employees directly and execute convincing social engineering, technical controls alone cannot prevent compromise.

However, the post-access phase offers detection opportunities. The deployment of unauthorized RMM tools, creation of rogue virtual machines via QEMU, and lateral movement following Quick Assist sessions all generate telemetry that a well-instrumented environment can capture.

The challenge is response speed; these intrusion chains progress rapidly from initial access to ransomware staging. Organizations need 24/7 monitoring with predefined response playbooks for unauthorized remote access tool deployment, enabling containment before attackers establish redundant persistence mechanisms.

V. Information Stealers: The Credential Harvesting Economy

Information stealers have become a cornerstone of the cybercrime economy, evolving from simple credential harvesters into sophisticated, multi-purpose platforms for data theft.

Threat cases involving infostealers increased by 30% in 2025, with 14% more distinct stealer variants detected compared to the prior year.

These tools are often the first malware deployed after initial access, providing threat actors with the sensitive data needed to facilitate lateral movement, financial fraud, or subsequent ransomware attacks. Their capabilities and widespread availability have made them a go-to choice for a broad spectrum of adversaries.

The top 3 infostealers of 2024 and 2025 include:

2024	2025
1. Lumma Stealer	1. Lumma Stealer
2. Vidar Stealer	2. Rhadamanthys
3. Redline Stealer	3. Vidar Stealer

Given its reliability, active development, and extensive feature set, Lumma Stealer maintained its dominant position throughout early 2025. The more interesting movement occurred in the second tier: Rhadamanthys displaced Vidar, while Redline, once a fixture in the top three, fell out entirely.

Rhadamanthys's rise reflects aggressive marketing in underground forums and a feature set that appeals to operators seeking capabilities beyond basic credential theft: cryptocurrency wallet targeting, browser session hijacking, and robust evasion techniques.

Vidar maintained its position among top stealers observed in 2025, showing resilience to countermeasures, while Redline's displacement likely reflects the law enforcement disruption of its infrastructure in 2024. These shifts underscore a competitive market where stealers rise, and fall based on operational security, feature development, and the attention of law enforcement.

CASE STUDY

Lumma Stealer: Other Stealers Fill the Void Post-Disruption

In 2025, law enforcement disrupted Lumma Stealer operations, and more recently Rhadamanthys as well. Lumma Stealer peaked in Q1 2025, then saw a 20% decrease in caseload across Q2, Q3, and Q4 combined. A reduction of incidents was observed following each disruption.

Unfortunately, demand for identity data in the crimeware ecosystem remains strong, and other stealers stepped in to fill the vacuum. Aside from mainstays such as Vidar, TRU analyzed several new or rising stealers in 2025:

Cyber Stealer

Cyber Stealer is a C#-based data theft malware operating on a Malware-as-a-Service (MaaS) subscription model. It targets web browsers, cryptocurrency wallets, communication platforms like Telegram and Discord, VPN clients, and password managers.

Beyond its primary function as a stealer, it includes integrated botnet capabilities, allowing operators to launch DDoS attacks, perform keylogging, and establish a remote shell on compromised systems.

LEARN MORE

Amatera Stealer

Identified as a rebrand of the former ACR Stealer, Amatera is an advanced infostealer that uses sophisticated evasion techniques, including the use of WoW64 SysCalls to bypass user-mode EDR hooks and an in-memory AMSI bypass to avoid detection by security products.

Its targeting is extensive, with capabilities to harvest data from over 149 different cryptocurrency wallets and more than 43 password managers.

LEARN MORE

AMOS (Atomic macOS) Stealer

Specifically targeting macOS, AMOS is often distributed via malvertising campaigns leading to fake software sites.

AMOS steals Keychain databases, Telegram session data, browser credentials, and files from Desktop, Downloads, and Documents directories.

LEARN MORE

DarkCloud

A VB6-based stealer targeting credentials from browsers, FTP clients, and email clients.

It's notable for sandbox evasion techniques using WMI queries to check hardware specifications and terminating its execution if it detects characteristics of analysis environments (e.g., low memory or processor count, small hard disk size, etc.).

LEARN MORE

The versatility of these stealers ensures that once a threat actor gains a foothold, they can quickly harvest valuable information, providing fuel for more disruptive, high-impact attacks.

The Cat-and-Mouse Game: EDR Evasion Techniques

Evasion is no longer an afterthought but a core component of modern cybercrime since successful evasion enables malware to execute its primary functions and establish persistence. As such, threat actors continuously integrate new techniques to bypass automated security solutions, such as: Anti-Virus, Endpoint Detection and Response, and sandboxes.

Key techniques observed in 2025 include: Anti-Malware Scan Interface (AMSI) Bypasses, Process and DLL Manipulation, Sandbox/Virtual Machine Detection, and asking users for consent via UAC to add exclusions in Microsoft Defender.

Anti-Malware Scan Interface (AMSI) Bypass: It is more common than ever for malware families, (e.g., Amatera Stealer) and especially loaders (e.g. Pure Crypter) to attempt to bypass Microsoft's AMSI through memory patching, preventing EDR/AV solutions from scanning malicious content, though some security solutions have already caught on.

TRU's Observations: Two common techniques seen involve patching the AmsiScanBuffer string in memory associated with clr.dll or directly patching usermode APIs like AmsiScanBuffer and EtwEventWrite in memory.

Process and DLL Manipulation: Process injection techniques such as "Process Hypnosis" (creating target processes in suspended and debug states), "Process Hollowing,", "Thread Execution Hijacking", and "DLL Sideloading" allow threat actors to inject malicious code into legitimate processes' address space, complicating the analysis process for security solutions.

TRU's Observations: The Process Hypnosis technique observed in the Ghost Crypt loader creates a target process in a suspended and debug state (DEBUG_ONLY_THIS_PROCESS flag), allowing the malware to inject its payload into the process's memory space before it fully initializes, thereby evading behavioral monitoring that triggers on other more common injection API sequences.

Sandbox and Virtual Machine Detection: Malware routinely performs checks to determine if it's running in an analysis environment.

TRU's Observations: Analysis of malware like DarkCloud, KoiLoader, and ChaosBot reveals diverse checks, including: searching for blacklisted process names (e.g., fiddler, wireshark); querying hardware properties (e.g., disk size less than 60GB); checking for specific default usernames (e.g., Joe Cage, bruno); identifying MAC address prefixes associated with virtualization vendors; and looking for the presence of VM-specific driver files (e.g., VBoxGuest.sys).

UAC Prompt Bombing: A technique during which victims are bombarded with User Account Control prompts until they click 'Yes', granting malware administrative privileges through persistent prompting.

TRU's Observations: TRU observed a MaaS loader delivering malware like **NightshadeC2** and Lumma Stealer that spawns a new PowerShell process as administrator to add an exclusion to Microsoft Defender for the malware payload. It verifies the exit code (0 indicates success) of the PowerShell process. If the process returns any exit code other than 0, the loop continues executing, forcing the user to approve the UAC prompt or face system usability issues. It was also discovered that this technique bypasses sandboxes that disable the Microsoft Defender service, "WinDefend".

What to Understand for an Effective Cyber Defense Strategy

Despite disruptions from law enforcement, the 30% increase in stealer cases indicates that market demand for harvested credentials remains robust. Therefore, security operations must extend beyond prevention to detect credential misuse by monitoring for authentication attempts using credentials appearing in underground marketplaces, alerting on access patterns inconsistent with legitimate user behavior, and correlating stealer infections on endpoints with subsequent identity-based attacks.

The increasing prevalence of evasion techniques (such as AMSI bypass, process injection, and sandbox detection) demonstrates that endpoint protection alone is inadequate; network-level visibility and behavioral analytics serve as essential complementary detection layers.

VI. The Loader Ecosystem: Infrastructure for Scale

The primary function of a loader is to deliver payload(s) successfully. Loaders serve as a critical element in modern cybercrime, obscuring original payloads while acting as an evasive stage against security solutions like AV and EDR in multi-stage infection chains.

The figure below shows the many-to-many relationships between loaders and final payloads in the cybercrime ecosystem. The width of each connecting flow visually quantifies how frequently a specific loader distributes a particular payload; thicker connections represent more common delivery pathways between loader X and payload Y.

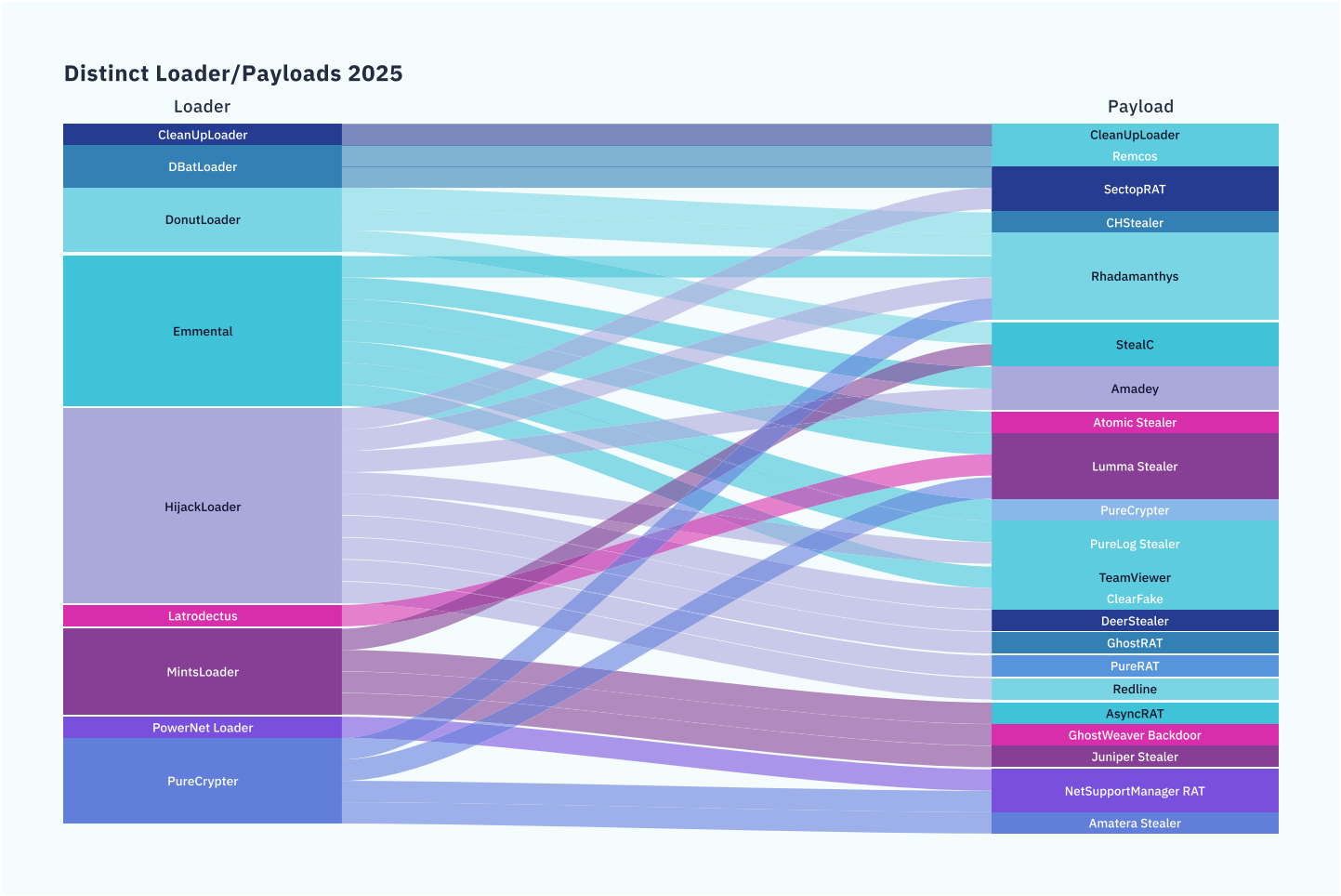


FIGURE 15: Loader to Payload Relationships

Several loaders deliver diverse final payloads, while individual payloads arrive via multiple loader families, which is a consequence of the MaaS market's modularity.

In most cases, 2-3 different loaders were responsible for delivering payloads ranging from stealers to RATs to RMMs, suggesting threat actors select MaaS products based on evasion effectiveness, compatibility with existing tooling, or simply availability and price.

For example, the HijackLoader-to-Lumma Stealer pipeline appeared consistently enough to indicate either deliberate bundling or strong market preference.

The market for loader-type malware is highly competitive because of ecosystem diversity and TRU assesses that threat actors are likely already using AI to assist with copying features from competitor MaaS products.

For security teams, this changeability and adaptability complicate attribution but clarifies threat detection strategy. Rather than chasing individual malware families, security operations should focus on behavioral patterns common across loader activity: process injection techniques, memory-only execution, AMSI bypass attempts, and anomalous parent-child process relationships.

The competitive MaaS market also means that successful evasion techniques propagate rapidly; what works for one loader will be copied by others within weeks. Moreover, AI is accelerating this distribution; security teams should expect novel capabilities to be commoditized faster than traditional threat intelligence cycles can track.

VII. Remote Monitoring and Management Tools: The 143% Increase

Following trends from recent years, threat actors increasingly deployed Remote Monitoring and Management (RMM) tools and Remote Access Trojans (RATs).

In 2025, TRU observed RMMs/RATs deployed alongside other malware or intrusion tools 30% of the time, highlighting their use for redundant remote access. The divergence between RAT and RMM trends in 2025 reveals a strategic shift in how threat actors approach remote access.

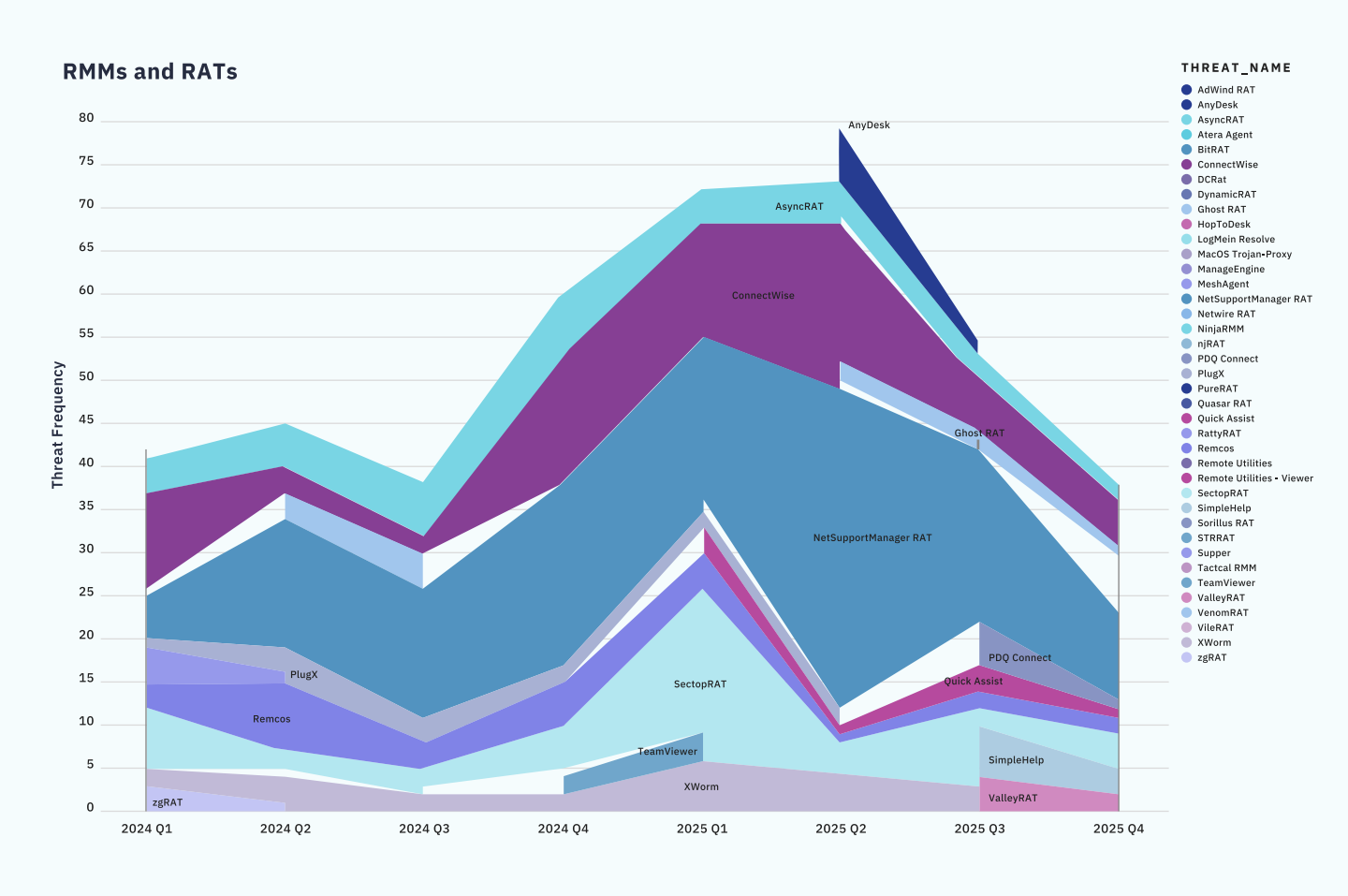


FIGURE 16: Frequency of RATs and RMMs Through 2024-2025

RAT cases increased 8%, but with 10% fewer distinct variants observed, suggesting consolidation around proven tools rather than proliferation of new ones. NetSupportManager RAT led these observations by a significant margin, with TRU tracking several distinct threat clusters leveraging NSM.

The diversity of these clusters, spanning different intrusion chains, targeting patterns, and apparent operators, indicates that NSM RAT has become a shared resource across the criminal ecosystem, valued for its stability and feature set rather than associated with any single threat actor.

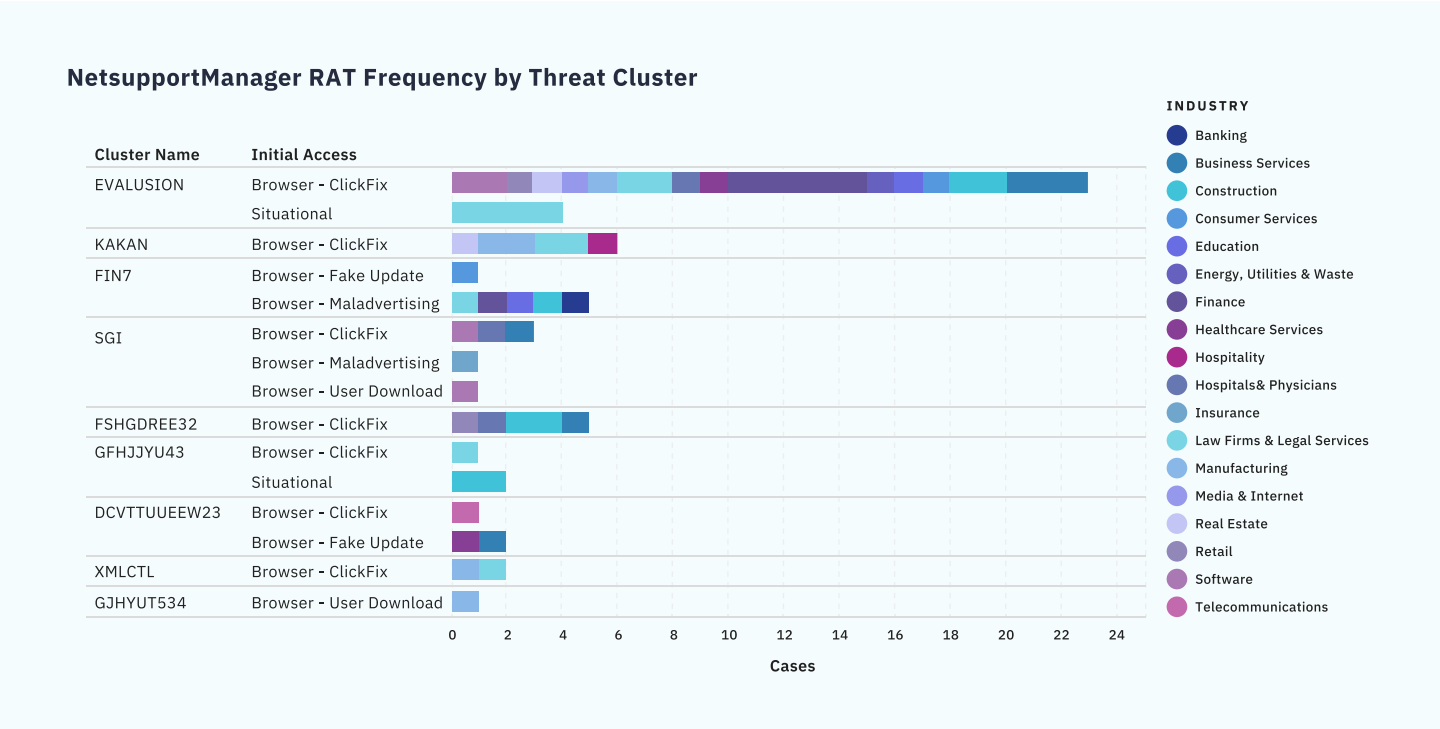


FIGURE 17: NetSupport Manager RAT Clusters 2025

On the other hand, the abuse of RMM tools for initial access/persistence tells a different story: **threat cases involving RMMs are up 143% year-over-year**, with distinct tool observations doubling. This explosive growth reflects a tactical preference shift.

Where RATs are purpose-built for malicious remote access and thus trigger security tool detections, RMMs are legitimate commercial software used daily by IT departments worldwide.

An AnyDesk or TeamViewer connection doesn't inherently signal compromise; it might be routine IT support. This ambiguity is precisely the point.

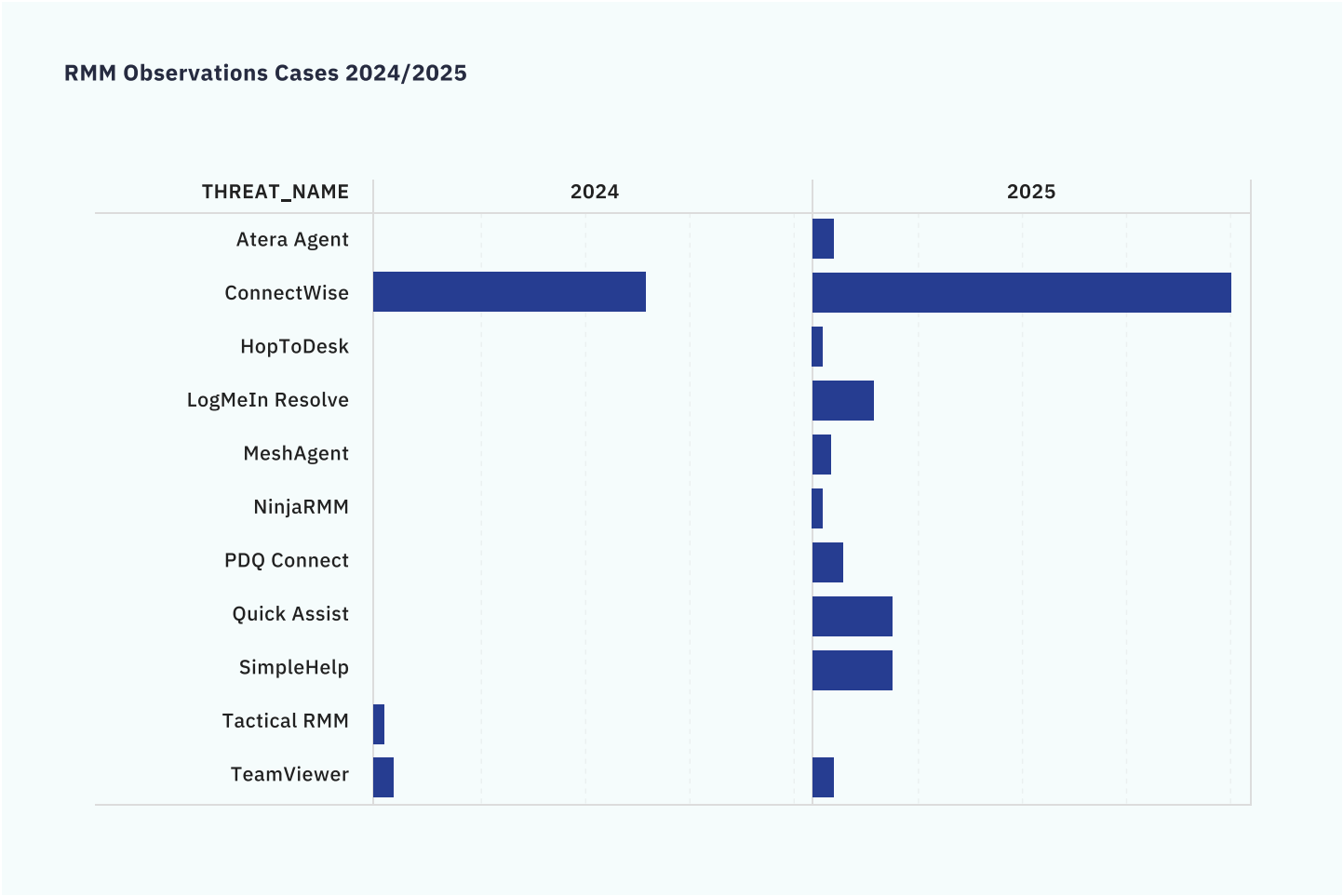


FIGURE 18: RMM Occurrences 2024/2025

Threat actors increasingly deploy RMMs not despite their legitimacy, but because of it, exploiting the detection gap between “unauthorized software” and “unauthorized use of authorized software”. However, using RMMs is not a new trend; ransomware groups have deployed RMMs for years to extend and maintain access.

What’s notable is the degree of cases where RMMs were deployed as the initial payload. Email bombing/helpdesk impersonation attacks were especially emblematic of this pattern.

The deployment of RMM tools as initial payloads appeared in browser-based attacks (1.4% of cases) and email-based attacks (0.6% of cases)—the latter representing a significant increase from virtually no observed cases in 2024.

For defenders, TRU recommends blocking all unapproved RMMs where possible, and monitor for violations. Unfortunately, threat actors may deploy or **even hijack** existing RMM deployments, thus approved services should be monitored as well.

What to Understand for an Effective Cyber Defense Strategy

The many-to-many relationships between loaders and payloads complicate traditional detection approaches that focus on specific malware families. Thus, the threat detection strategy must shift upstream to the behavioral patterns that loaders share regardless of their final payload: process injection techniques, memory-only execution, DLL unhooking to bypass EDR hooks, and AMSI bypass attempts.

The competitive MaaS market also creates a detection velocity challenge. Therefore, security operations require detection engineering capabilities that can adapt at similar speed, updating behavioral detection rules as new techniques emerge rather than waiting for annual detection content refreshes.

An AI-driven Security Operations Platform may provide advantage here: machine learning models can identify anomalous behavior patterns even when specific techniques haven't been explicitly signatured, and automated analysis can process the volume of samples necessary to track rapid ecosystem evolution.

VIII. Ransomware: Resilience Through Evolution

In 2025, the ransomware ecosystem demonstrated remarkable resilience and evolution, marked by continued attack volume, fragmentation among threat actors, and the integration of AI to enhance operational efficiency.

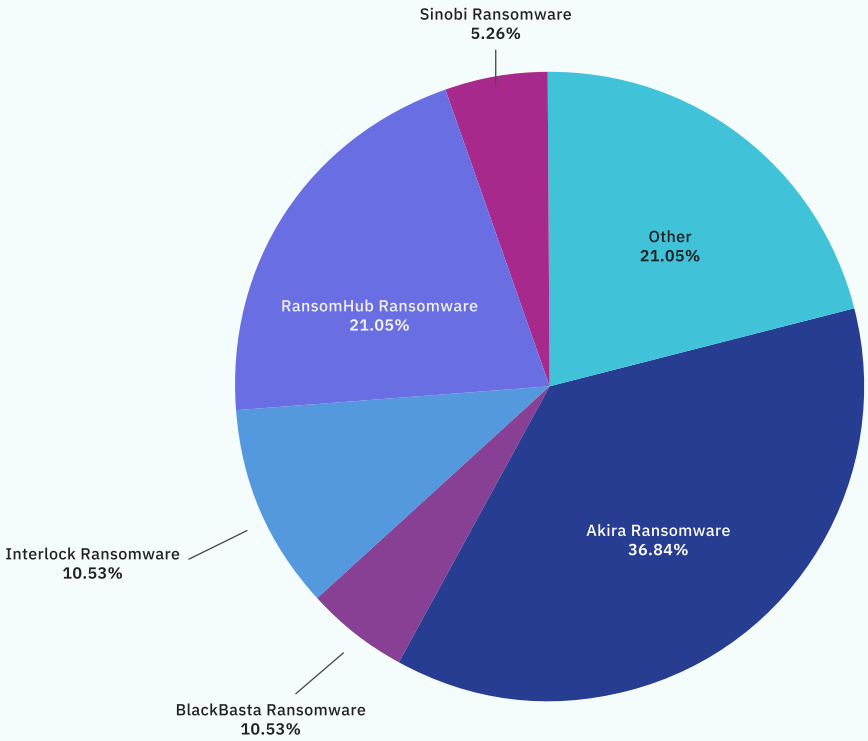


FIGURE 19: Ransomware by Cases 2025

The ransomware ecosystem in 2025 demonstrated remarkable resilience despite law enforcement pressure and internal fractures within major groups. Based on TRU's case data, the most active groups included Akira, RansomHub, Interlock, BlackBasta, and Sinobi.

Moreover, the top victim industries included Business Services, Construction, and Finance. This industry concentration is not coincidental; these sectors combine high-value data, operational sensitivity to downtime, and frequent large financial transactions, making them attractive targets for ransomware operations.

What's notable about 2025's ransomware activity is how closely initial access methods mirrored the broader identity-centric trends documented throughout this report. Social engineering coupled with remote access tooling emerged as the predominant entry point, displacing the exploit-driven access that characterized earlier ransomware eras.

eSentire's team of 24/7 Security Operations Center (SOC) Analysts responded to cases where Akira affiliates leveraged email bombing techniques for initial access, a direct adoption of the playbook that BlackBasta pioneered earlier in the year. Similarly, browser-based methods like ClickFix and fake update campaigns (with SocGholish serving as a known precursor to RansomHub deployments) provided another common pathway.

The implication is clear: ransomware operators are not developing novel access techniques; they are rapidly adopting whatever social engineering and identity compromise methods prove effective across the broader threat landscape.

The intrusion ratio is moderately consistent across industries, with some outliers. TRU's assessment is that ransomware operators/affiliates are generally industry-agnostic, emphasizing high-value footholds from an extortion perspective and focusing on businesses vulnerable to data leaks and downtime.

Moreover, TRU's analysis of BlackBasta's leaked internal communications revealed that certain countries and industries are politically sensitive to these groups but can be overruled by financial opportunity.

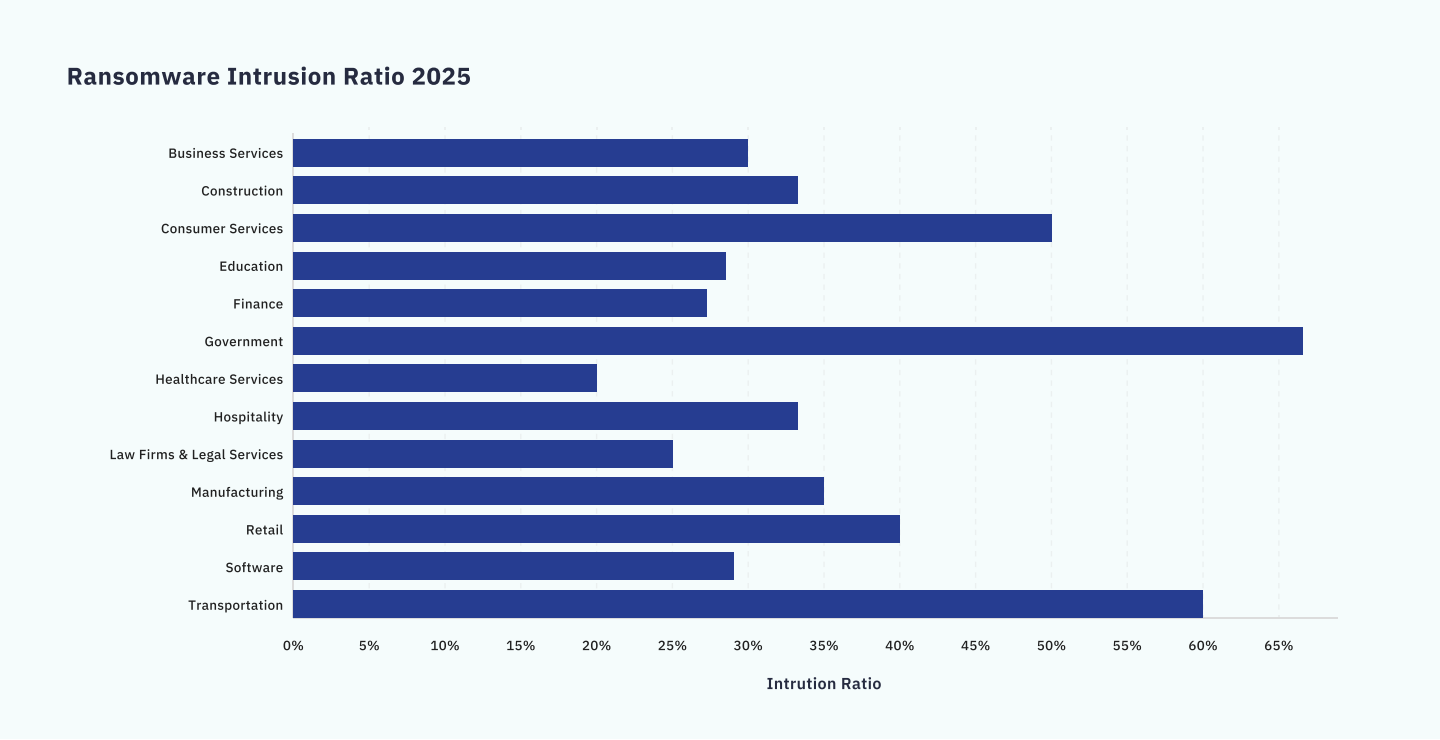


FIGURE 20: Ransomware Intrusion Ratio 2025

Exploiting Trusted Relationships and Monitoring Blind Spots

The use of privileged, compromised identities was a concerning through-line across several 2025 cases. In fact, eSentire's SOC and Incident Response (RI) teams engaged in multiple intrusions tied to Akira and Sinobi affiliates where privileged administrator accounts were used to access networks remotely, disable defenses, and exfiltrate data. In certain cases, these identities were traced to suspected Managed Service Provider (MSP) accounts in SonicWall VPN appliances.

These cases highlight a strategic shift where ransomware affiliates have perhaps taken a page from the APT playbook by exploiting third-party identities to gain access to edge devices, effectively circumventing endpoint security and operating in defenders' "blind spots".

Dedicated Infrastructure for Data Exfiltration

Another notable observation was the use of high-speed, geographically proximate infrastructure for data exfiltration. Affiliates historically used services like Mega.nz with tools like Rclone or Megasync to exfiltrate gigabytes of data.

In response to blocking and monitoring measures, TRU observed affiliates leveraging anonymization services to subvert location-based bandwidth monitoring.

Furthermore, TRU observed use of dedicated hosting services for increased bandwidth. One particular provider, Global Connectivity Solutions (aka 4VPS), was used by Termite, Sinobi, Akira, and RansomHub affiliates for data exfiltration throughout 2025.

AI Adoption by Ransomware Operators

The adoption of AI and LLMs by ransomware affiliates and Ransomware-as-a-Service (RaaS) groups is a strategic trend accelerating malware development, enhancing operational capabilities, and lowering technical barriers to entry.

Key instances observed:

- **AI-Driven Negotiations:** The emerging RaaS operation GLOBAL GROUP promotes its service by offering cross-platform payloads and AI-driven ransom negotiations as a service differentiator for affiliates.
- **AI-Powered Ransomware:** Researchers identified AI-powered strains like FunkLocker (used by FunkSec APT), with analysis revealing specific AI coding patterns in development.
- **Rapid Malware Creation:** The Ransomvibing VS Code extension showed signs of "vibe coding," suggesting AI-generated code enabling low-skill actors to rapidly produce semi-functional malware.

What to Understand for an Effective Cyber Defense Strategy

When ransomware affiliates access networks through MSP credentials mapped to over-privileged accounts, traditional endpoint detection may never trigger since the attacker is using legitimate administrative access paths. Therefore, threat detection must focus on behavioral anomalies: administrative accounts authenticating at unusual hours, mass file access patterns preceding exfiltration, and connections to known bulletproof hosting providers like Global Connectivity Solutions.

The use of dedicated exfiltration infrastructure by multiple ransomware groups (Termite, Sinobi, Akira, RansomHub) also creates threat intelligence opportunities given that known-bad infrastructure can be blocked or monitored proactively. Therefore, AI-driven analysis becomes essential for identifying subtle patterns across high volumes of legitimate administrative activity.

XI. Supply Chain and Trusted Relationship Attacks Lead to an 85% Intrusion Ratio

Threat actors increasingly leveraged trusted third-party relationships and software supply chains to bypass traditional security controls in 2025. These attacks rose to 0.7% of the overall caseload.

For supply chain compromises: TRU documented multiple cases involving compromised npm packages, including the "Shai Hulud" worm affecting 187 packages. The reach of this campaign extended to packages published by major organizations, including a well-known cybersecurity firm, demonstrating that even security-conscious organizations can become unwitting vectors.

For trusted relationship attacks: TRU observed numerous cases involving ransomware operators abusing SonicWall SSL VPN credentials belonging to third-party MSPs. These credentials were mapped to over-privileged Active Directory accounts, providing immediate privileged access to victim networks – no exploitation required, no malware to detect, just a legitimate login from a trusted partner.

Though relatively small in number, they represented high-severity compromises that leveraged privileged vendor or service provider access.

By infiltrating software packages, service providers, or browser extensions, attackers effectively inherited the established trust relationships of these entities, enabling them to deliver malicious payloads through channels that victims perceived as legitimate.

The 85% intrusion ratio reflects this dynamic: once attackers successfully leverage trusted access, traditional security controls offer little friction. The victim's defenses were designed to stop outsiders, not to scrutinize activity from partners and dependencies already inside the trust boundary.

What to Understand for an Effective Cyber Defense Strategy

The 85% intrusion ratio for supply chain and trusted relationship attacks represents the highest conversion rate of any access vector and the hardest to detect through traditional means. When attackers inherit legitimate trust relationships, they arrive with valid credentials and expected access patterns.

Cyber defense strategies require a fundamental shift toward zero-trust principles for third-party access: just-in-time provisioning rather than persistent credentials, continuous monitoring of vendor session activity, and immediate alerting on deviations from established behavioral baselines.

Continuous Threat Exposure Management (CTEM) also plays a critical role in understanding which vendors have access to which systems, and what the blast radius of a compromised vendor credential would be, enables prioritized monitoring and faster scoping during incidents.

Nation-State Intersection: DPRK Fraudulent IT Worker Schemes

Since mid-to-late 2024, TRU observed a significant increase in fraudulent remote worker schemes attributed to North Korean state-sponsored actors. These operations represent a sophisticated sanctions evasion strategy designed to generate foreign currency for the regime while potentially enabling future cyber operations.

The scheme involves deploying thousands of North Korean IT workers globally who masquerade as independent contractors or freelancers. These individuals meticulously obscure their identities and national origins using stolen/fabricated identification documents, false employment histories, and personas that make them appear to be citizens of non-sanctioned countries.

eSentire identified and investigated fake remote IT workers across several industry verticals in 2025, including technology services and finance.

TRU observed several campaigns aligned with the standard financial motivations associated with DPRK IT worker schemes: generating salary revenue for the regime while potentially positioning for data theft or extortion.

Persistent outreach using multiple personas was identified targeting research and technology firms, sectors where technical talent is in high demand and remote hiring is normalized.

Red Flags for HR & IT Teams

In response, TRU recommends paying special attention to the following red flags during the hiring process:

- **Inconsistencies with work and education history**
- **Use of VoIP numbers**
- **Unusual requests for corporate device shipment**

TRU also recommends that organizations should review and enhance hiring policies to prevent North Korean threat actors from being successfully hired. Since identity verification for all hires is critical, candidate interviews should be conducted in person; for virtual interviews, cameras should be on without any virtual background.

Looking Forward: The 2026 Threat Outlook

The threat patterns observed throughout 2025 establish clear trajectories for the coming year. These are not speculative forecasts; they are logical extensions of capabilities already demonstrated and trends already in motion.

Based on TRU's analysis of current threat actor behavior, emerging tooling, and the structural dynamics of the cybercrime ecosystem, security teams should prepare for the following developments.

Cybercrime Will Continue to Lean Into AI

The criminal utilization of Large Language Models (LLMs) will increase significantly in 2026, with threat actors harnessing these technologies to streamline operations. AI systems will function as dual-purpose assets in the criminal toolkit, facilitating rapid malware development while simultaneously serving as learning platforms for expanding technical expertise in programming and offensive security.

Emerging tradecraft will spread more rapidly than ever as criminals use LLMs to dissect, copy, and operationalize their competition's TTPs. Advanced tradecraft will be adopted more quickly by commodity threats, disrupting pre-AI threat models. As such, security teams will need to use AI and LLMs themselves to maintain an edge in this agile environment.

Moreover, you should also expect a persistent technical battle where cybercriminals continuously refine "jailbreak" strategies to bypass security constraints in commercial AI systems including ChatGPT, Copilot, Gemini, Grok, and Claude.

This escalating challenge will prompt platform developers to engineer increasingly sophisticated protections, ultimately driving some threat actors toward underground alternatives like WormGPT.

AI-Enabled Social Engineering at Scale

The use of AI by threat actors will transition from sporadic experimentation to standard operational procedure. The implications extend beyond faster malware development, though that alone is significant.

More consequential is the impact on social engineering: AI enables highly customized, context-aware phishing campaigns that adapt to target language, industry terminology, and organizational context in ways that template-based approaches never could.

Vishing operations represent a particularly concerning vector for AI augmentation. Voice synthesis technology has reached the point where convincing real-time voice cloning is accessible to non-experts.

Combined with the social engineering playbooks that proved effective in 2025 (e.g., IT impersonation, manufactured crises, urgency exploitation) AI-driven voice synthesis could enable adversaries to scale vishing operations that previously required human operators for each call.

The 1,450% increase in email bombing/IT impersonation attacks may represent the last generation of these campaigns that relied primarily on human callers.

Insider Access and Recruitment Will Accelerate

The economics of insider recruitment are becoming increasingly attractive to threat actors. When perimeter security improves, MFA adoption increases, endpoint detection catches more malware, the path of least resistance shifts toward acquiring legitimate access from the inside.

The Extortion-as-a-Service model provides a natural framework for this: rather than renting infrastructure or malware, affiliates invest in recruiting insiders who can bypass security measures entirely using their legitimate credentials.

The target profile is predictable; it's often employees in high-trust roles with access to sensitive systems and data, SaaS administrators who can create backdoor accounts or exfiltrate data, Telecom staff who can facilitate SIM swaps or access call records, or Finance personnel who can approve fraudulent transactions.

The pitch is straightforward: financial compensation in exchange for access and the operational security is favorable to attackers, as insider actions often blend with normal job functions.

The DPRK fraudulent IT worker schemes observed in 2025 represent a state-sponsored version of this approach, with operatives systematically infiltrating organizations through legitimate hiring processes.

While nation-state motivated, the playbook is transferable: if organizations struggle to detect fake employees with fabricated identities, they will struggle equally with real employees who have been recruited to act against organizational interests.

This shifts security focus heavily toward managing privileged trust, monitoring for behavioral anomalies among authorized users, and building insider threat programs that balance security with employee privacy.

A Fractured Stealer Market Creates New Opportunities

The information stealer landscape entering 2026 is defined by disruption, but disruption that creates opportunity. Law enforcement operations successfully targeted Lumma and Rhadamanthys infrastructure in 2025, forcing operators to rebuild and creating temporary gaps in availability.

Stealc and Vidar are positioned to absorb displaced demand, having undergone substantial development cycles that address previous functionality gaps. New entrants will also emerge, as the barrier to developing a functional stealer continues to drop with AI-assisted coding and readily available source code from leaked or deprecated projects.

The underlying demand signal remains strong: a 30% increase in stealer cases throughout 2025 despite mid-year disruptions indicates that the market for harvested credentials, session tokens, and cryptocurrency wallets is robust enough to sustain multiple competing products.

Security teams should expect the stealer ecosystem to reconstitute quickly, likely with improved operational security informed by lessons learned from 2025's takedowns.

Targeting of Operational Technology and Critical Infrastructure

Attacks against Industrial Control Systems (ICS), like those observed in Canadian water and energy facilities, are assessed to continue increasing. These represent strategic targets for espionage (by APTs) and high-impact disruption (by hacktivists or financially motivated groups) due to severe physical and safety consequences.

Organizations operating critical infrastructure must prioritize OT security assessments and implement network segmentation between IT and OT environments.

Strategic Recommendations to Stay Ahead of the Threat Curve

The 2025 threat landscape demands fundamental changes to security architecture and operational practices. The threat trends documented in this report share a common characteristic: they exploit the gap between the speed at which attackers operate and the speed at which defenders can detect and respond.

Closing this gap requires not just better tools, but a structural shift toward security operations that can match the tempo of industrialized cybercrime. Before diving into tactical recommendations, it's critical to understand the three cyber defense imperatives that should form the foundation of the greater cybersecurity strategy:

Long-Term Cyber Defense Strategy

24/7 Threat Detection and Response

The threat trends documented in this report also make clear that threat detection without rapid response capability is effectively no detection at all. When ransomware affiliates access networks through compromised MSP credentials at 2 AM, business-hours-only monitoring means attackers operate unimpeded during their most critical staging activities.

Organizations should partner with a trusted AI-driven **Managed Detection and Response (MDR) provider** with the authority and capability to take containment actions immediately, such as suspending compromised sessions, isolating affected endpoints, blocking malicious infrastructure, without waiting for business hours or approval chains. This is the fundamental value proposition of MDR: not just visibility, but action at the speed the threat landscape now demands.

Continuous Threat Exposure Management (CTEM)

The concentration of exploitation activity in network applications and surge of third-party supply chain attacks reflects a broader truth about attack surface risk. Organizations cannot defend what they cannot see. Internet-exposed management interfaces, forgotten VPN concentrators, over-privileged vendor accounts, unmanaged devices connecting via compromised credentials: these represent the exposure gaps that sophisticated attackers exploit.

Effective defense requires continuous visibility into external attack surface, prioritization based on actual exploitability and threat intelligence, and integration with security operations to ensure that critical exposures receive immediate attention. The mass scanning observed within days of vulnerability disclosure means that point-in-time assessments are insufficient; exposure management must be continuous to match the tempo of exploitation.

AI-Driven Security Operations

The influx and industrialization of cybercrime means that human-only security operations programs simply cannot keep up. When PhaaS platforms enable thousands of simultaneous credential harvesting campaigns and AI accelerates malware development and enables hyper-personalized social engineering, security teams must match that leverage or fall behind.

AI-driven security operations provide the analytical horsepower to identify subtle attack patterns across massive data volumes, correlate signals across identity, endpoint, and network telemetry, and surface high-confidence alerts from noise that would overwhelm human analysts.

But AI alone is insufficient. The sophisticated attacks documented in this report (e.g., trusted relationship abuse, supply chain compromise, insider threats) require human judgment to investigate, contextualize, and respond appropriately.

The answer is not AI or human expertise, but AI-first security with human-backed trust: machine-speed detection and triage, with human analysts providing the expertise for complex investigations, threat hunting, and strategic response decisions.

Tactical Cyber Defense Recommendations

The following recommendations address both immediate tactical actions and connect specific threat trends to defensive capabilities, with emphasis on how AI-driven security operations and continuous threat detection can provide organizations with meaningful advantage.

1 Strengthen Identity Security

Identity has become the primary attack surface; with 55% of threat cases in 2025 involving account compromise and 63% of those attributable to PhaaS platforms, the volume alone demands attention. But the more critical finding is the speed of exploitation: **TRU's analysis of Tycoon2FA incidents revealed an average of just 14 minutes between credential capture and active exploitation.**

Traditional identity security approaches (i.e., periodic access reviews, next-day log analysis, weekly threat hunts) operate on the assumption that attackers move slowly. A compromised credential that isn't detected within minutes will be used within minutes. By the time a SOC Analyst reviews overnight authentication logs in the morning, the attacker has already established inbox forwarding rules, conducted reconnaissance, and potentially initiated BEC activity.

The challenge is further compounded by the ineffectiveness of traditional MFA against AitM techniques. Organizations that invested in MFA as a primary identity control now face a threat ecosystem specifically designed to circumvent it. Platforms like Tycoon2FA, FlowerStorm, EvilProxy exist because traditional MFA works well enough that attackers needed industrialized solutions to bypass it.

What to Implement:

- Deploy phishing-resistant MFA (FIDO2/WebAuthn, passkeys) prioritizing privileged accounts and critical business applications. Phishing-resistant authentication eliminates the token interception vector entirely.
- Implement conditional access policies tuned to detect VPN/proxy anomalies, impossible travel patterns, and authentication from high-risk network ranges.
- Deploy continuous session monitoring with automated revocation capabilities. The ability to terminate suspicious sessions within minutes, not hours, is critical given compressed attack timelines.
- Integrate ASN-based threat intelligence into authentication monitoring. TRU's research found that PhaaS backend infrastructure was far less short-lived than front-end evasion techniques, creating detection opportunities that maintain current intelligence on known-bad network ranges.

2 Enhance Email and Browser Threat Controls

Email and browser-based attacks accounted for most of the initial access in 2025, but the nature of these attacks has evolved beyond what traditional controls were designed to address. What makes these attack vectors particularly challenging is their exploitation of legitimate functionality and human behavior rather than technical vulnerabilities:

- QR code phishing embeds malicious links in images that bypass text-based URL scanning.
- Threat actors are **spoofing an organization's domains** to deliver phishing emails that appear internally sent by exploiting complex routing and misconfigured spoof controls.
- ClickFix attacks contain no malicious files; rather, victims execute commands themselves after being socially engineered by fake error messages and CAPTCHA prompts.

Traditional email gateways and browser security tools were designed for a different threat model: malicious attachments, known-bad URLs, and exploit kits targeting browser vulnerabilities. These controls remain necessary but are increasingly insufficient against attacks designed specifically to evade them.

What to Implement:

- Deploy advanced email filtering capable of detecting QR code phishing (quishing) and Direct Send abuse. Traditional text and link-based analysis is insufficient for image-embedded threats.
- Block execution of clipboard-based commands and monitor PowerShell activity for obfuscation patterns.
- Implement browser isolation for high-risk web categories and monitor for unauthorized browser extensions.

3 Monitor and Restrict Remote Access Tools

RMM applications are used daily by IT departments for remote support, so an RMM connection doesn't inherently signal compromise. This ambiguity is exactly what threat actors exploit. It's no surprise that the surge of email bombing and IT impersonation attacks relied heavily on RMM tools for initial access.

The defensive challenge is distinguishing unauthorized RMM usage from legitimate IT operations at speed, and at scale. Blocking all RMM tools is rarely feasible; IT operations depend on them. But permitting them without monitoring creates blind spots that sophisticated attackers specifically target.

What to Implement:

- Maintain an allowlist for approved RMM tools and alert on unauthorized installations.
- Monitor approved RMM usage for contextual anomalies: connections initiated without corresponding IT tickets, RMM sessions immediately following external Teams calls, or RMM activity on systems with no prior remote support history.
- Audit legitimate RMM deployments for hijacking attempts since threat actors may compromise existing installations.
- Implement network-level visibility into RMM traffic patterns. Baseline normal usage volumes and flag significant deviations that might indicate unauthorized access or data staging.

4 Supply Chain and Vendor Risk Management

When supply chain and trusted relationship attacks succeed in gaining initial access, they almost invariably progress to full compromise. The reason is structural: attackers who leverage trusted relationships inherit the access rights of entities the victim already trusts. Security controls designed to stop outsiders offer little friction against what appears to be legitimate partner activity.

The challenge is that modern organizations cannot operate without third-party relationships. From software dependencies and MSPs to the use of cloud platforms and SaaS applications, the attack surface extends far beyond organizational boundaries. Therefore, eliminating third-party access isn't feasible; managing its risk is essential.

What to Implement:

- Validate integrity of third-party software packages and enforce SBOM checks.
- Monitor privileged vendor accounts for anomalous access patterns. Implement just-in-time access for MSP connections.
- Require phish-resistant authentication and activity logging from vendors with internal system access.
- Implement just-in-time access, especially that's time-bound and purpose-specific, for vendor connections rather than persistent credentials to reduce exposure.

5 Insider Threat Mitigation

The DPRK fraudulent IT worker schemes documented throughout 2025 represent a threat category that bypasses traditional security controls entirely. These aren't 'normal' threat actors; they are operatives who successfully navigate legitimate hiring processes, pass background checks, and receive authorized access to organizational systems as employees.

While DPRK schemes represent the state-sponsored manifestation, the underlying vulnerability extends beyond nation-state threats. If organizations struggle to detect fake employees operating under fabricated identities, they will struggle equally with real employees who have been recruited, through financial inducement or coercion, to act against organizational interests. The Extortion-as-a-Service model creates economic incentive for exactly this type of insider recruitment.

What to Implement:

- Screen remote hires rigorously for identity inconsistencies: verify educational credentials against alumni rosters, investigate employment history gaps, flag use of VOIP numbers and VPNs during interviews.
- Monitor for abnormal equipment requests, particularly corporate device shipments to addresses different from stated residences.
- Train HR and IT teams to recognize red flags and implement high-alert protocols following suspicious candidate identification.

6 Prepare for AI-Driven Threats

AI adoption by threat actors is not a future concern, but a reality in 2025 that will only accelerate into 2026. The implications extend beyond faster malware development, though that alone is significant when defenders rely on signature-based detection. More consequential is the impact on social engineering.

AI enables phishing campaigns that adapt to target language, industry terminology, and organizational context in ways that template-based approaches never could. AI-driven voice synthesis is reaching the point where real-time vishing at scale becomes feasible.

Industrialized cybercrime now has access to the same AI capabilities that enterprises are adopting, but with fewer constraints on deployment and experimentation. Threat actors are not bound by change management processes, risk committees, or concerns about model governance so they will integrate AI into their operations at whatever pace proves operationally effective.

What to Implement:

- Simulate AI-enabled phishing scenarios in security awareness programs. Train users to recognize highly customized social engineering.
- Invest in behavioral analytics and anomaly detection to counter rapid, automated attack chains.
- Deploy AI-enabled security solutions that leverage machine learning for detection and response at machine speed, backed by human expertise for complex decision-making.
- Monitor for AI-specific attack patterns as they emerge: synthetic voice in vishing calls, AI-generated code patterns in malware samples, and signs of automated attack chain orchestration.

Conclusion

The 2025 threat landscape tells a story of industrialized cybercrime operating at unprecedented speed and scale.

Identity compromise is not an emerging concern to monitor; it is the dominant threat vector, accounting for 50% of all cases with a 389% year-over-year increase.

When attackers possess valid credentials, they bypass perimeter defenses entirely, achieve 85% intrusion ratios, and progress from initial access to active exploitation in minutes rather than days.

The data points throughout this report converge on a single operational reality: **the window for detection and response has collapsed.**

The 14-minute average activation time from PhaaS credential capture to business email compromise. The compressed timelines from email bombing to ransomware staging. The same-day exploitation of newly disclosed network appliance vulnerabilities. These are not statistics to be monitored, but rather deadlines that security teams must beat.

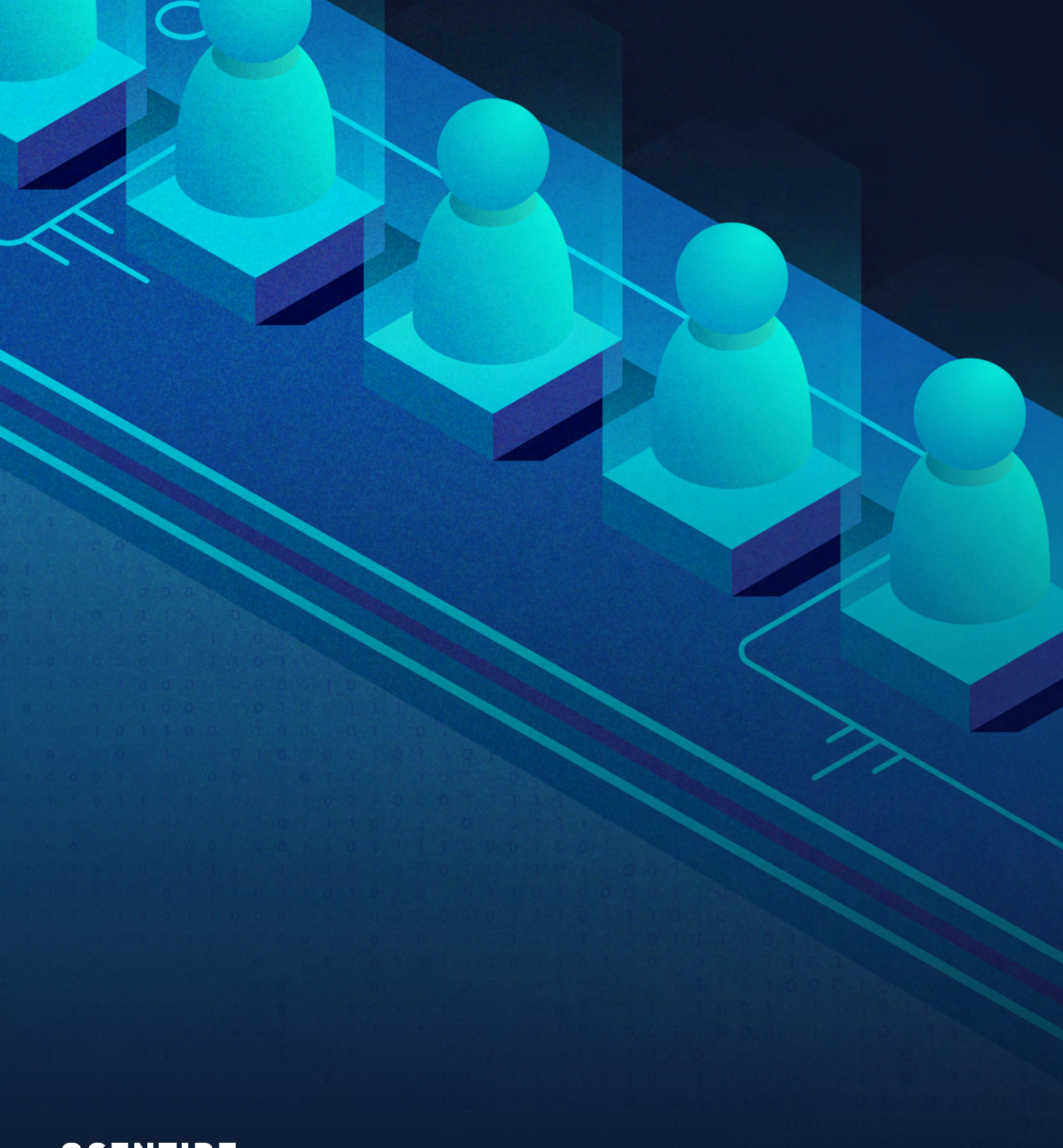
What will not change is the fundamental dynamic that defines modern cybersecurity: attackers operate continuously, at machine speed, with industrialized efficiency.

Organizations that match this tempo through 24/7 detection and response, continuous exposure management, and AI-driven security operations will contain incidents before they become breaches.

Moving into 2026, the strategic priorities are clear: security architectures must be rebuilt around the assumption that identities will be compromised, with AI-enabled threat detection and response capabilities that identify threats at machine speed, backed by human expertise for complex decision-making, threat hunting, and incident response.

The organizations that continue operating with legacy security models will face increasing exposure until a successful attack forces reactive changes under crisis conditions.

The threat landscape will continue to evolve. The fundamental shift toward identity-centric attacks will not. The only remaining question is whether organizations will adapt proactively or wait until a successful attack forces the issue.



eSentire

eSentire, Inc., the Authority in Managed Detection and Response (MDR), protects the critical data and applications of 2000+ organizations in 80+ countries, across 35 industries from known and unknown cyber threats by providing Continuous Threat Exposure Management, Managed Detection and Response, and Incident Response services designed to build an organization's cyber resilience & prevent business disruption. Founded in 2001, eSentire protects the world's most targeted organizations with 65% of its global base recognized as critical infrastructure, vital to economic health and stability. By combining open XDR platform technology, 24/7 threat hunting, and proven security operations leadership, eSentire's award-winning MDR services and team of experts help organizations anticipate, withstand and recover from cyberattacks. For more information, visit **www.esentire.com** and follow **@eSentire**.