
HUNTRESS
2026 CYBER
THREAT REPORT

Table of Contents

Inside the Business of Cybercrime 3
2025 Threat Landscape 4
Attack Breakdown By Industry 7
Ransomware 12
Attacker Tools and Techniques 30
RMM Abuse 40
Exploit-Driven Campaigns 47
Defense Evasion 55
Breaking Down Hacker Activity 64
Identity-Based Attacks 71
Phishing Activity 86
AI Abuse 91
Conclusion 94

Inside the Business of Cybercrime

As adversaries heavily abused legitimate tools, processes, and software at scale, and locked in on stealth and speed in 2025, the lines between normal activity and unauthorized intrusions blurred.

Attackers have realized they don't need to break in anymore when they can just log in as you. As a result, identity-based attacks surged as attackers relied on multi-factor authentication (MFA) fatigue, token theft, OAuth abuse, and misconfigured SaaS applications to infiltrate and persist in target environments.

Legitimate tools and processes quietly morphed into dangerous attack vectors. Bad actors continued to abuse trusted infrastructure, like remote monitoring and management (RMM) tools, and living off the land binaries (LOLBins), to avoid detection before launching payloads.

Social engineering sharpened its deceptive edge. ClickFix and fake CAPTCHA schemes were abundant, tricking users into installing infostealers, ransomware, or remote access trojans (RATs).

Right now, the good guys are losing way too often. Malicious hackers are the real competition you have in your business. We don't say that to scare you, but to wake you up.

Your traditional business competitors aren't the only ones you have to worry about, because cybercriminals are actively trying to steal your livelihood. They're organized, efficient, and relentlessly profit-driven, running operations that rival legitimate corporations in scale and strategy. They silently scope out your digital footprint and online identities while targeting your people.

All too often, the biggest vulnerability isn't a zero-day exploit: it's humans. We get tired, we get distracted, and we click things we shouldn't. These seemingly innocent mishaps turn a normal Tuesday into an unwanted interruption at 3am.

One thing is crystal clear—you can't hire or innovate fast enough to fight these threats alone. Security isn't just an IT ticket anymore: it's a finance issue, an HR issue, a leadership issue, and a business survival issue.

The Huntress 2026 Cyber Threat Report looks back at 2025 to show you where threat actors moved the needle and what that means for your business to safely scale today and beyond. The report draws on analysis gleaned from over 4.6 million endpoints and 9.4 million identities protected by the Huntress Security Platform and backed by a 24/7 AI-assisted Security Operations Center (SOC).

Let's get to work. It's time to wreck hackers together.

2025 Threat Landscape

2025 Threat Landscape at a Glance

Throughout 2025, cybercriminals leveled up their attack playbooks, prioritizing stealthy access and persistence in targeted environments. They did it by abusing legitimate tools, launching sophisticated identity attacks, and executing clever social engineering scams.

We successfully shut down attackers using these exact methods every day in 2025. And in 2026, it's crucial to understand the most common threats competing with your business...

RMM Abuse

Businesses use RMMs to work smarter, but attackers abuse these trusted tools to gain persistence, execute commands, and deploy malware while evading detection, leading to a 277% year-over-year increase in RMM abuse. By abusing the inherent legitimacy of these platforms, threat actors blend in with normal admin activity, significantly complicating defense efforts.

ClickFix and Fake CAPTCHA Variants

ClickFix accounted for 53.2% of all malware loader activity, showing that abuse of end-user trust rather than traditional vulnerabilities is an effective tactic. Threat actors also invested in new ClickFix techniques and post-attack patterns. Fake CAPTCHA lures showed up across different types of campaigns, blurring the lines between normal and malicious activity. This reflects a broader shift towards scaling stealthier operations, away from more easily detected exploit-driven campaigns focused on CVEs.

Ransomware

This ruthless threat accounted for 5% of all incidents in 2025, contributing to a year-over-year volume increase. The average time-to-ransom (TTR) went up from 17 to 20 hours, as ransomware attackers focused on stealth, data theft, and extortion. We saw four major groups—Akira, Medusa, Qilin, and Ransomhub—dominate over half of all ransomware incidents. Intense competition drove these actors toward a standardized playbook, tapping into tactics like Active Directory mapping, disabling security tools, and deploying encrypted tunnels.

Identity-Based Attacks

These ghostlike threats have evolved from isolated incidents into structured intrusion chains, making the unsuspecting user the main attack vector. Attackers now bypass traditional perimeter defenses by logging in with valid credentials, using tactics like adversary-in-the-middle (AiTM) schemes and shadow workflows to launch more damaging attacks like business email compromise (BEC). In 2025, this shift solidified identity as the new endpoint, with access policy and trust boundary violations (37.2%), mailbox manipulation and persistence (19.0%), and AiTM dominating identity-based threat activity.

Frequency of Threats Overall (2024 vs. 2025)

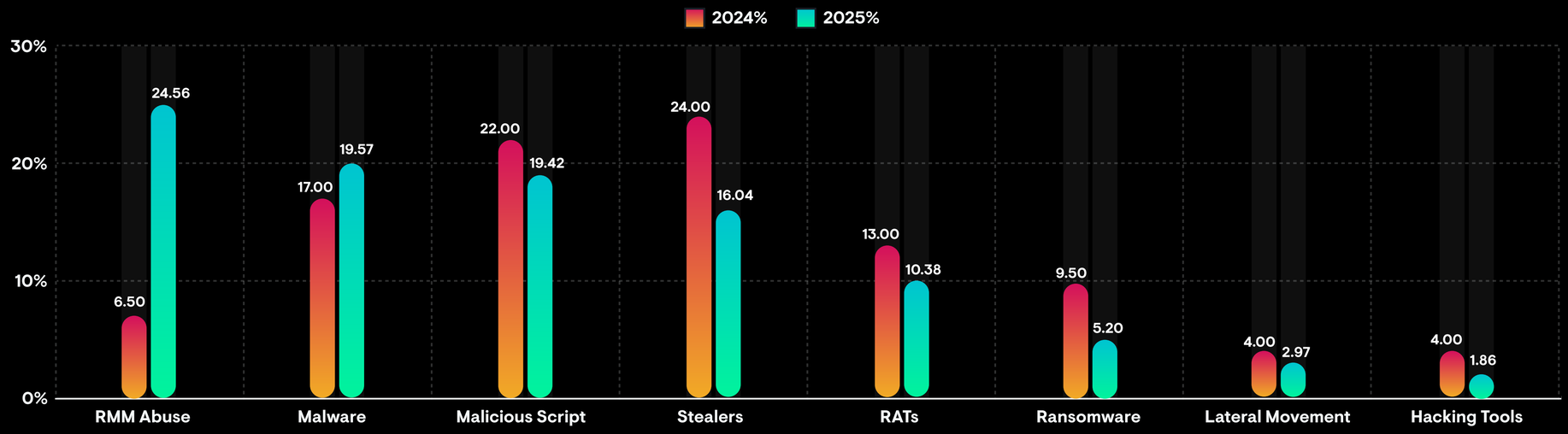


Figure 1: Most common threat categories in 2024 vs. 2025

Attack Breakdown By Industry

Industries Under Fire

Throughout 2024, attackers targeted a wide range of industries, with a focus on education and healthcare. This trend continued in 2025, with these two industries accounting for 37% of all observed incidents. Notably, healthcare overtook education as the most targeted industry, representing 21% of all attacks. This shift reflects attackers' focus on the high resale value of sensitive patient data and the critical nature of medical services, which they exploit to demand higher ransom payments.

At the same time, t**he manufacturing industry became a new focus for attackers, accounting for 17% of observed incidents in 2025.** Manufacturing's "zero-downtime" requirements make it especially vulnerable to extortion. Brief production interruptions can result in millions of dollars in losses, as seen when a breach at Jaguar Land Rover forced a complete shutdown of global manufacturing.

Beyond these industries, the technology and government sectors also saw major cyber incidents.

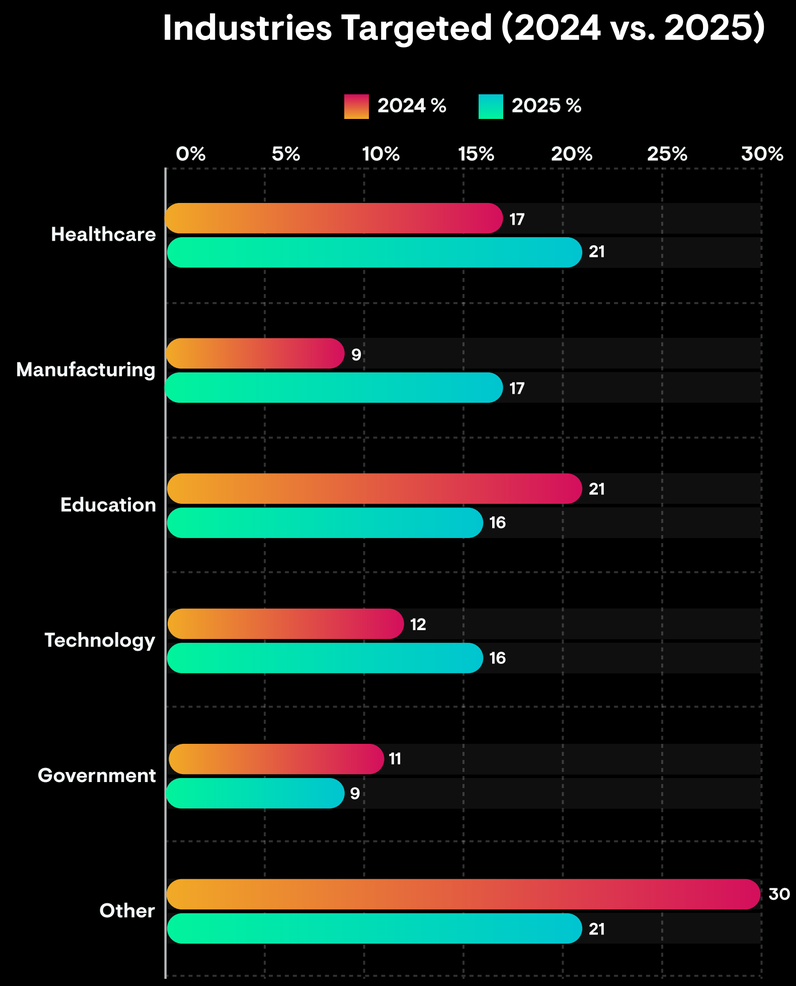


Figure 2: Industries targeted by percentage in 2024 vs. 2025

Threats by Industry (2024 vs. 2025)

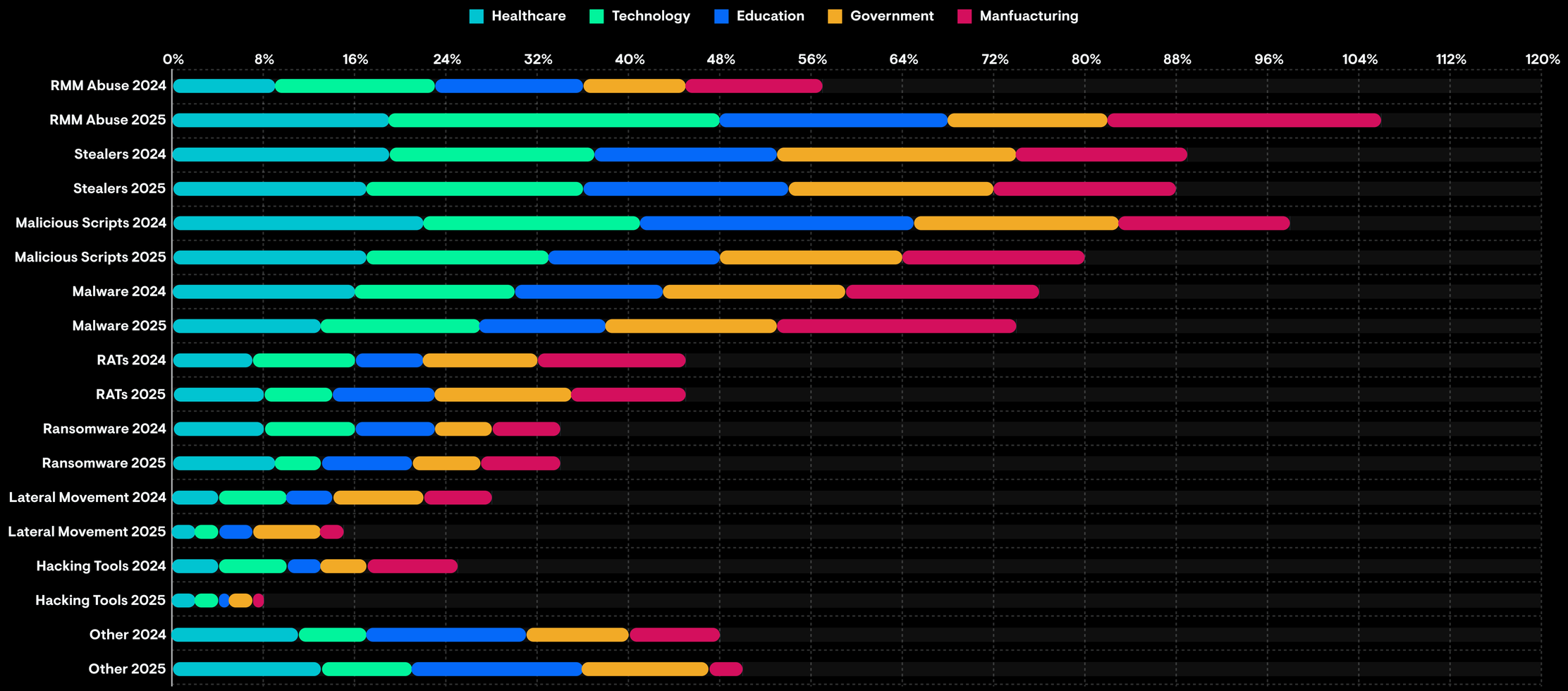


Figure 3: Threat frequency by industry in 2024 vs. 2025

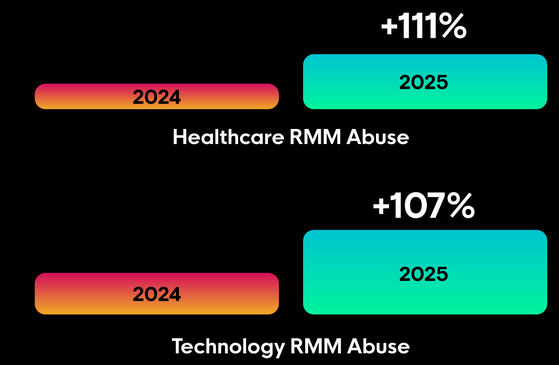
In 2025, we noticed a shift toward more operationally efficient and stealth-focused attacker behavior across all major industries. Attackers were forced to adapt or risk getting left in the dust, with many malware and ransomware groups either pivoting to new tactics or losing ground.

Malicious RMM use surged across most sectors. Healthcare and technology experienced the largest increases in attacks leveraging RMM abuse, letting attackers stay undetected for longer periods, giving them more time to operate in targeted environments. This extended dwell time makes it easier to steal credentials, access additional systems, and move laterally before detection occurs.

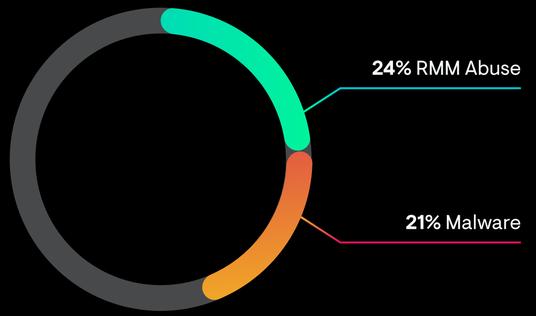
Government environments, on the other hand, continue to be targeted by infostealers and malicious scripts. This suggests that specific controls focusing on RMM attack vectors work, but attacks using traditional tradecraft are still slipping through the cracks.

Attackers heavily targeted the manufacturing sector with traditional malware loaders and RMMs to gain access. We saw a drop in hacking tools and malicious scripts, meaning attackers are moving toward abusing trusted services and platforms versus heavy payload intrusions. Why? Because security tools often catch them when they use malicious scripts to download other components or deliver payloads.

> **Cybercrime isn't underground anymore; it's the world's third-largest economy. There are pricing models, support, and even refunds. It's organized crime operating like a business.**
>
> **Kyle Hanslovan**
> CEO and Cofounder of Huntress



Healthcare and technology experienced the largest increases in attacks leveraging RMM abuse



Attackers heavily targeted the manufacturing sector with traditional malware loaders and RMMs to gain access

Ransomware persists, but threat actors are targeting more selectively. They often look for large payouts or environments they can easily manipulate. Similar to what we saw in 2023, this could open the door for smaller ransomware groups to claim their stake in the threat landscape as others shift their focus to extortion-only operations and specific targeting patterns, like specific industries or companies. Successful takedowns caused a few of these groups to shut down, but many moved on to bigger targets.

Malicious scripts are still popular, but many operators have replaced them with RMM installers or RAT components. Additionally, endpoint detection and response (EDR) solutions are getting better at spotting these scripts. This often disrupts attacks earlier in the attack path, killing longer chains of script executions or similar payloads.

Finally, attackers seem to be standardizing playbooks tested against technology and MSP-adjacent environments and reusing them on other industries. 2025 data indicates that risk will be defined by low-noise abuse of legitimate access mechanisms, combined with faster credential theft to pivot to other resources, rather than typical malware families.

Looking ahead, RMM abuse will continue to outpace traditional RAT deployments across all industries. This is especially true where distributed or outsourced IT operations are part of the security stack. Attackers have caught on that exploiting these trusted relationships gives them access to multiple victims simultaneously.

Out (Traditional & Noisy)	In (Stealth & Trusted)
Malicious Scripts	RMM Installers
Generic RATs	Legitimate RMM Components
Mass Phishing	Credential Theft

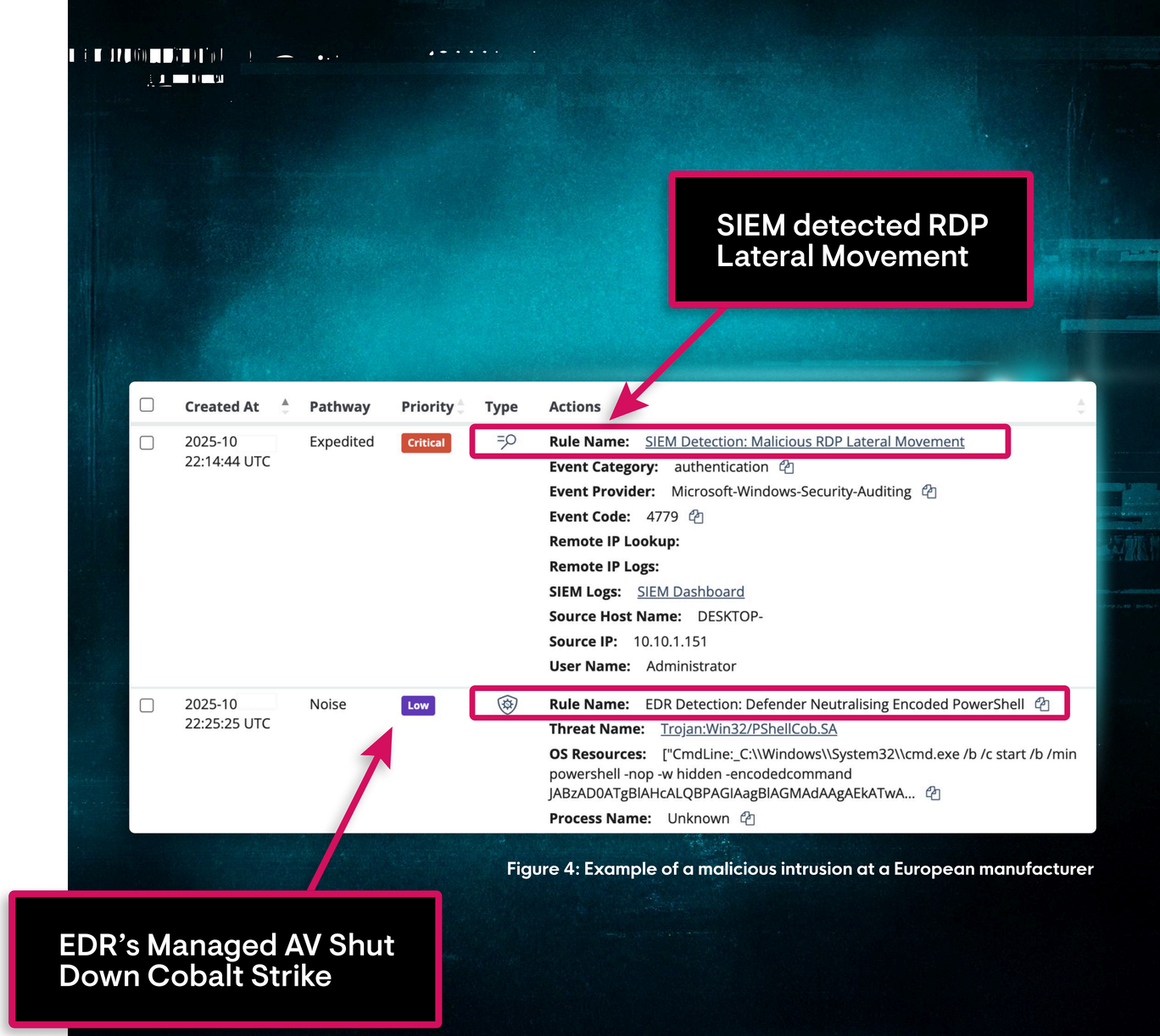
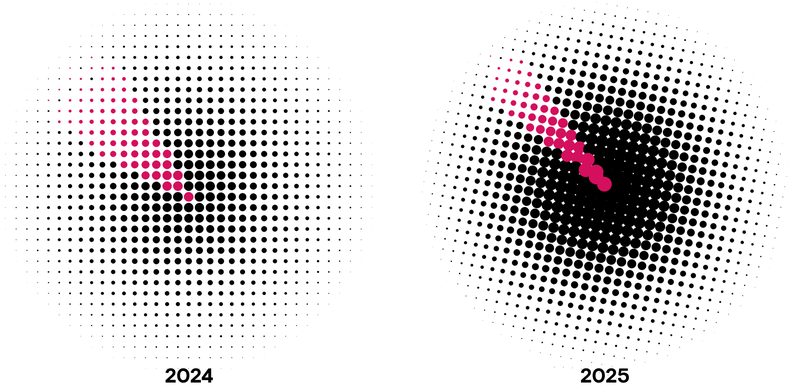


Figure 4: Example of a malicious intrusion at a European manufacturer

Ransomware

The State of Ransomware



Ransomware is a smaller share of overall incidents in 2025, even though its volume went up YoY.

Despite a year of aggressive law enforcement takedowns and high-profile disruptions, ransomware activity was steady, accounting for 5% of all observed incidents in 2025. While ransomware made up a smaller share of total incidents, the overall volume increased year-over-year.

This increased volume was paired with a noticeable drop in the variety of tactics, techniques, and procedures (TTPs) used across ransomware groups. **Power became concentrated among four major players: Akira, Medusa, Qilin, and Ransomhub,** who collectively accounted for over half of all ransomware incidents. Driven by intense competition to outdo each other, these groups and their rivals standardized their operations to create a "common playbook," defined by:

- External payload retrieval through PowerShell-based downloaders
- Active Directory enumeration for internal mapping and target identification
- Use of Bring Your Own Vulnerable Driver (BYOVD) techniques to systematically disable EDR solutions
- Standardized commands to remove shadow copies and modify Windows Defender settings
- Strategic implementation of RMMs to blend in with legitimate IT tooling and aid in specific parts of the attack chain.
- Mass adoption of encrypted tunnels such as cloudflared, ngrok, FRP, and Chisel to conduct staging and steal files, especially in more professional groups
- Increased evidence of data theft happening before ransomware delivery for extortion or additional sources of financial gain, or might even have been the primary goal in some circumstances

Average Time-to-Ransom in 2024 and 2025



What also stands out is that the time-to-ransom (TTR) in 2025 went up from 17 to 20 hours. Here's why this likely happened:

- Increased focus on extortion and data theft
- A strategic shift to stealth over speed
- Extended time between initial access and follow-up activity

With fewer server-side vulnerabilities, most ransomware activity in 2025 shifted away from exploit-driven attacks. While the number of ransomware campaigns fluctuated in part due to spikes attributed to known ransomware families, most groups pivoted to alternative methods: using stolen or brute-forced credentials, remote access tools (VPN/RMM), and data bought from infostealers.

Specific surges were occasionally tied to exploits, like Akira's August campaign targeting SonicWall SSLVPN devices, but these became the exception and not the norm. Groups specializing in exploitation—like Cl0p and Akira—doubled down on their niche expertise for "exploit once, compromise many" strategies that effectively balance hands-on intrusion efforts with exploit development, a luxury that most ransomware groups can't afford.

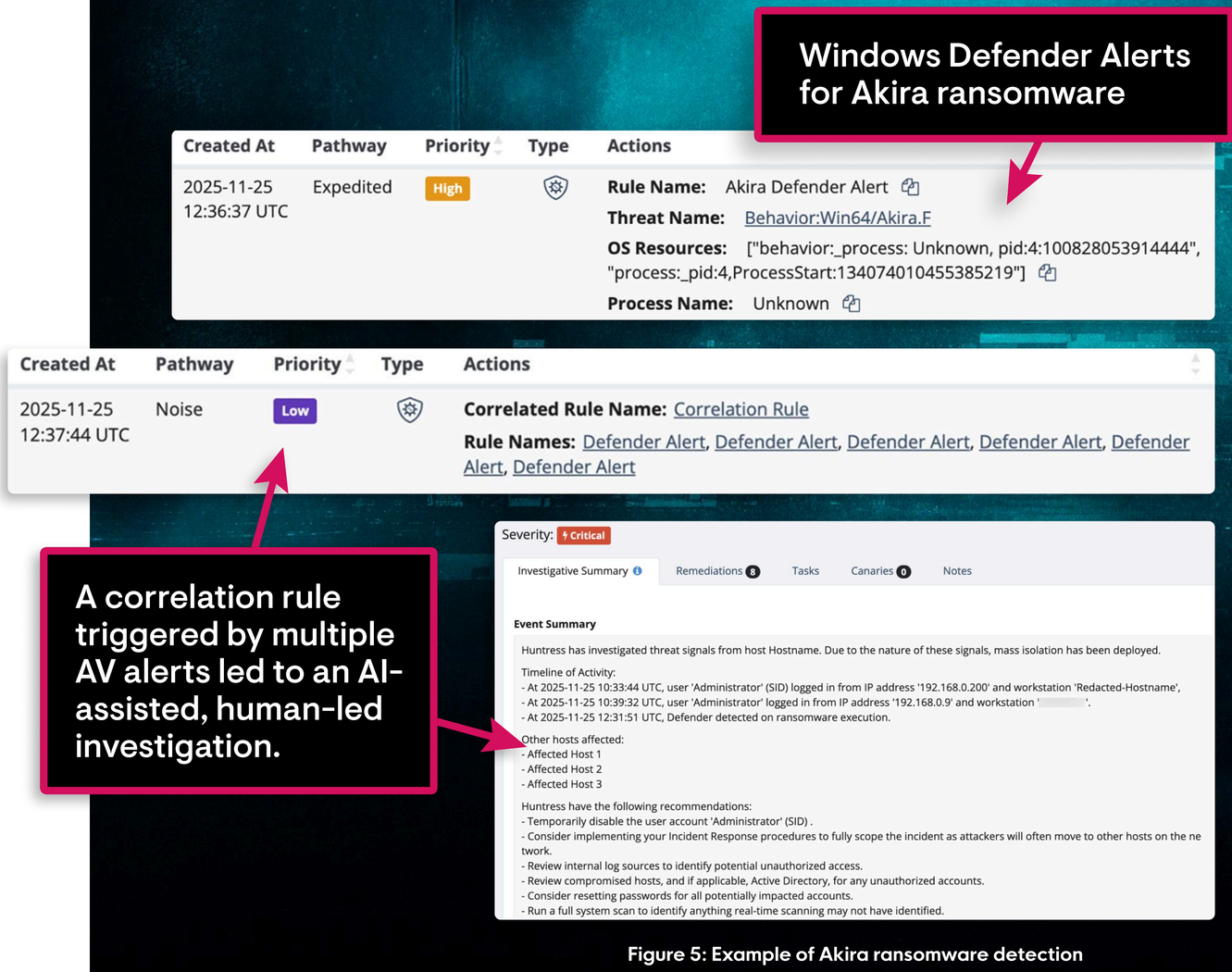


Figure 5: Example of Akira ransomware detection

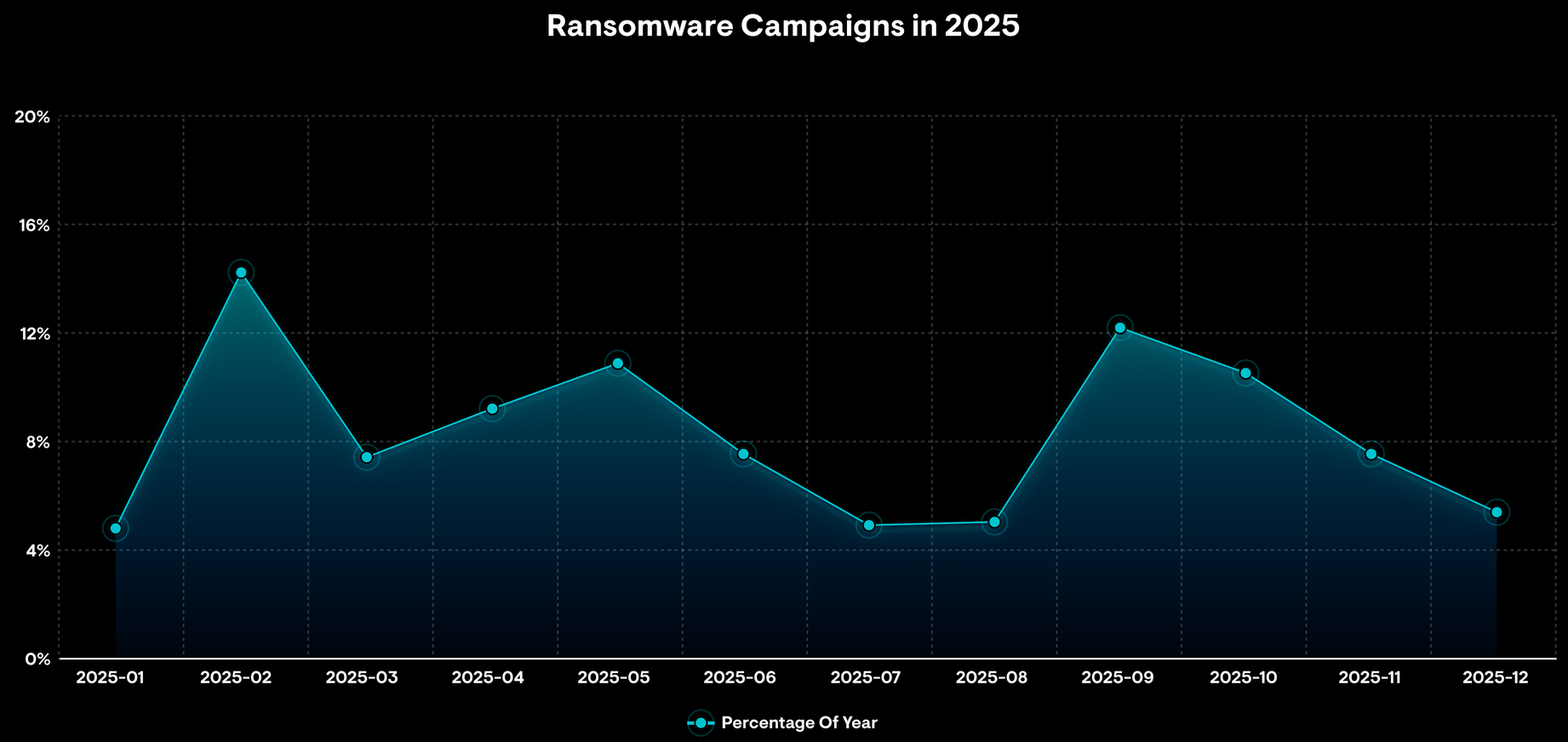


Figure 6: Monthly distribution of global ransomware campaigns

Ransomware Groups

Ransomware is increasingly concentrated in the hands of a few groups (Akira, Medusa, Qilin, and RansomHub) that run organized and efficient operations with streamlined playbooks.

Ransomware activity in 2025 looked surprisingly similar across sectors, as attackers streamlined their playbooks. Major cybercrime partnerships ramped things up through coordinated efforts, as we saw with the merger of Shiny Hunters, Scattered Spider, and Lapsus$ to develop "ShinySp1d3r." Similarly, DragonForce (formed by ex-members of RansomHub) attempted to build a "ransomware cartel" alongside Qilin and LockBit, which resurfaced with LockBit 5.0 despite repeated law enforcement disruptions.

While newer families like Shinobi and Play popped up, a few key groups controlled most of the market. Akira solidified its position as the year's top operator, accounting for nearly a quarter of all observed incidents. Their dominance persisted even as other giants faltered: Black Basta was rocked by a massive leak of over 200,000 internal chat messages that exposed its infrastructure and operations, while BlackSuit (formerly Royal) was dismantled in July following a successful global law enforcement takedown.

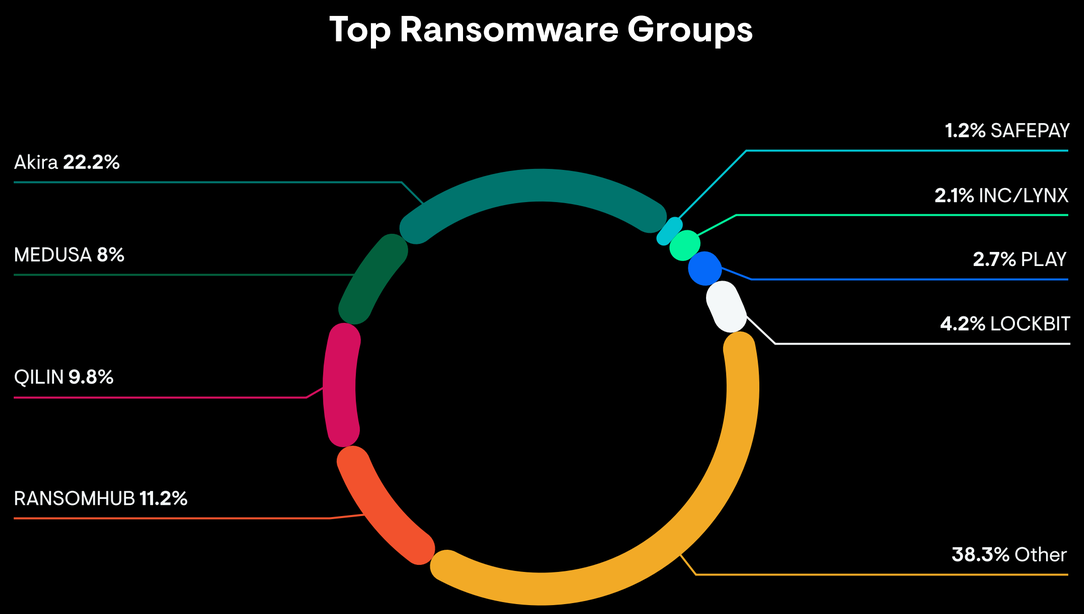


Figure 7: Most prevalent ransomware groups in 2025

Longtime groups had a clear preference for proven attack chains, not novel techniques. In 2025, most relied on the existing and available ransomware ecosystem: initial access brokers for infostealers or credential-theft tools, remote-management abuse, commodity malware loaders, and hands-on-keyboard actions prior to deployment. While brand-new variants like Cephalus, Obscura, and Kawalocker showed up, most incidents were driven by Akira, Medusa, Qilin, and Ransomhub, who accounted for 51% of all ransomware incidents we observed.

Ransomware groups have largely abandoned novel methods, instead favoring a 'common playbook' of proven attack chains.

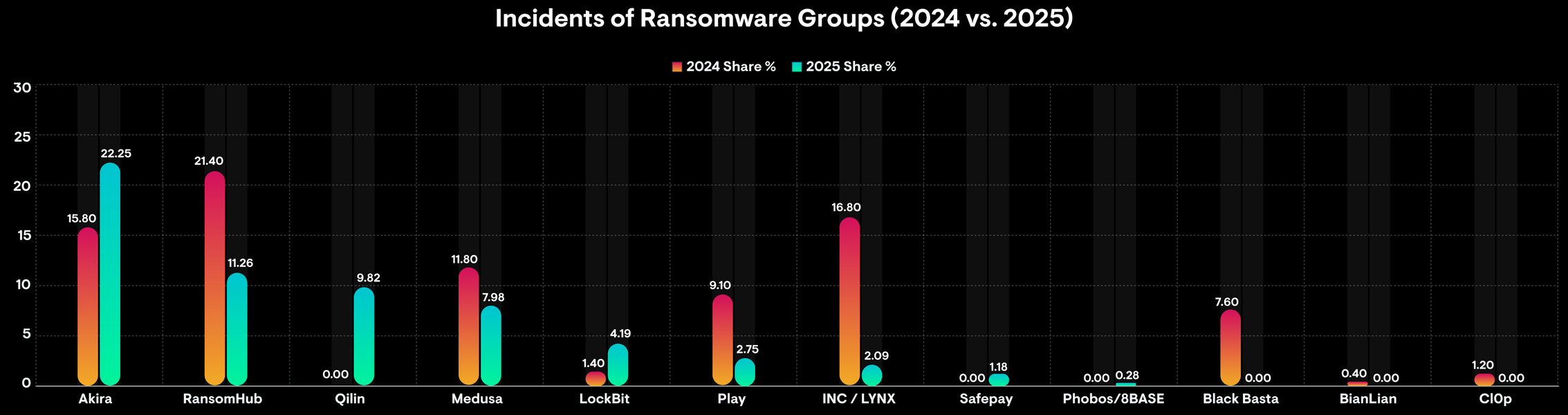


Figure 8: Ransomware groups incident frequency from 2024 to 2025

Ransomware Groups Gains and Losses

Ransomware Family	2024 Frequency	2025 Frequency	Gains and Losses
Qilin	0.00%	9.82%	+9.82%
Akira	15.80%	22.25%	+6.45%
LockBit	1.40%	4.19%	+2.79%
Safepay	0.00%	1.18%	+1.18%
Phobos	0.00%	0.28%	+0.28%
BianLian	0.40%	0.00%	-0.40%
Cl0p	1.20%	0.00%	-1.20%
Medusa	11.80%	7.98%	-3.82%
BlackSuit	5.70%	0.00%	-5.70%
Play	9.10%	2.75%	-6.35%
Black Basta	7.60%	0.00%	-7.60%
RansomHub	21.40%	11.26%	-10.14%
INC / LYNX	16.80%	2.09%	-14.71%

Figure 9: Table of ransomware gains and losses 2024 vs. 2025

Common Ransomware Tradecraft in 2025

Proven, Reliable, and Profitable



Ransomware campaigns across different families used the same core techniques to move through the attack path, from initial access to domain-wide control. Ransomware operators stuck to what worked in 2025, and experimentation wasn't on the agenda. Instead, they consistently rolled out vetted ransomware approaches focused on credential extraction, SYSTEM-level persistence, and deletion of shadow copies. These behaviors showed up over and over in the pre-encryption phase, and should be considered standard components of modern ransomware tradecraft.

NTDS.dit Access via Shadow Copy and Symlink Abuse

For those unfamiliar with `NTDS.dit`, it's the main database file for Microsoft Active Directory Domain Services (AD DS). It stores all domain information, including user accounts, group memberships, and hashed passwords. In other words, a playground for ransomware operators.

We consistently saw operators take Active Directory credential material from `NTDS.dit` without interacting with the live directory database. Attackers routinely accessed offline copies of `NTDS.dit` through Volume Shadow Copies, avoiding service disruption and reducing the likelihood of detection tied to domain controller instability.

To make this happen, operators frequently abused legitimate Windows utilities that copied files from snapshot contexts, bypassing file locks that normally protect `NTDS.dit` during runtime. To do this, attackers modified Windows symlink evaluation behavior to weaken default filesystem trust boundaries. These changes allowed paths associated with shadow copy devices to be resolved in contexts normally restricted by Windows security controls and file-system limitation.

The 2025 Pre-Encryption Workflow



Once symlink protections were relaxed, attackers mapped internal shadow copy device paths into attacker-accessible locations. This exposed protected system files to post-exploitation tooling without needing direct access to the live NTDS database. The technique bridges privilege boundaries between system-level resources and userland tooling, enabling credential material to be copied, parsed, and exfiltrated with minimal operational noise.

After acquisition, `NTDS.dit` was used as the foundation for credential-driven expansion. It's a known strategy, but this year, we saw it used by several small ransomware groups who had been using ntsdutil, impacket, reg save, or similar easily detected methods to carry out these attacks.

Operators extracted domain password hashes offline, performed Kerberoasting against service accounts, and reused credentials via pass-the-hash and pass-the-ticket techniques. These credentials were then used to escalate privileges and move laterally across the environment. In practice, this workflow cuts down the time needed to achieve domain-wide access and eliminated many traditional detection opportunities tied to interactive credential dumping.

Security Control Tampering as a Preparatory Phase

Defense evasion activity observed in 2025 was deliberate, not incidental. Ransomware operators like Akira, Medusa, and DragonForce routinely used installed security products early in the intrusion to inform follow-on actions. This reconnaissance guided attackers' targeted tampering efforts to reduce visibility and response effectiveness.

Operators frequently changed security configurations, introduced process or path exclusions, suppressed logging, and cleared event data to limit forensic traceability. In more advanced cases, we saw attackers abuse or deploye kernel drivers to bypass user-mode protections entirely. These actions weren't used to immediately disable security tooling, but to degrade detection long enough to allow staging, credential harvesting, and encryption preparation to proceed uninterrupted.

Expanded Use of Encrypted Tunnels

In 2025, ransomware operators used more mature tradecraft by favoring resilient, legitimate tunneling and exfiltration tools over custom malware. Cloudflared emerged as the main tunneling mechanism, seeing big spikes in July and August that aligned with surges in "hands-on-keyboard" activity. For data theft, Rclone was still the most consistent and scalable exfiltration utility, especially during late summer and fall as campaigns shifted toward bulk data theft and extortion.

While SSH remains a staple with attackers, tools like FRP and Chisel appeared selectively, suggesting specialized use by specific threat actors. At the same time, brief upticks in WinSCP and Mega Cloud Sync suggest opportunistic, operator-driven file theft once privileged access was established. All together, these trends highlight a growing use of encrypted tunnels among ransomware groups, most notably Akira, Medusa, and LockBit, to blend into legitimate network traffic, maximize throughput, and quietly exfiltrate data at scale before extortion.

Ransomware crews stepped up their game by leaning on legit, resilient tools for tunneling and data theft. Groups like Akira, Medusa, and LockBit increasingly hid inside encrypted, normal-looking traffic to quietly steal data before making their demands.

Tunneling and Exfiltration Tools Used for Ransomware

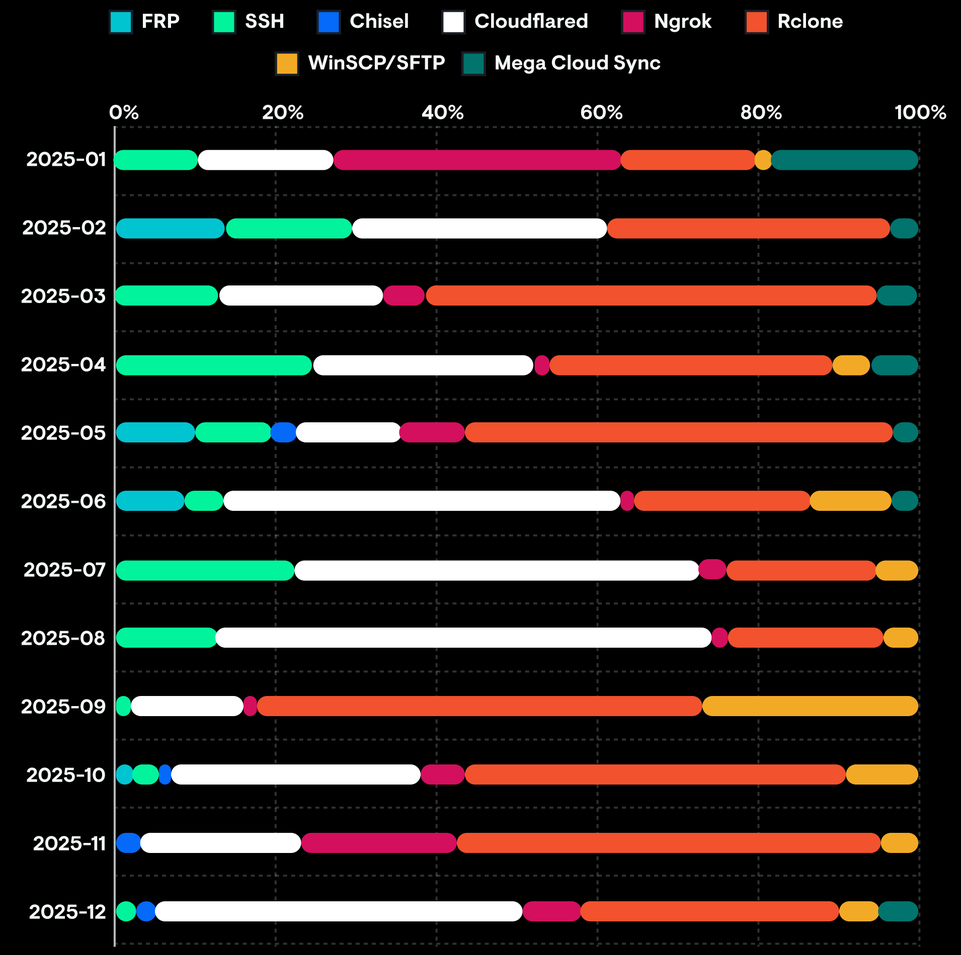
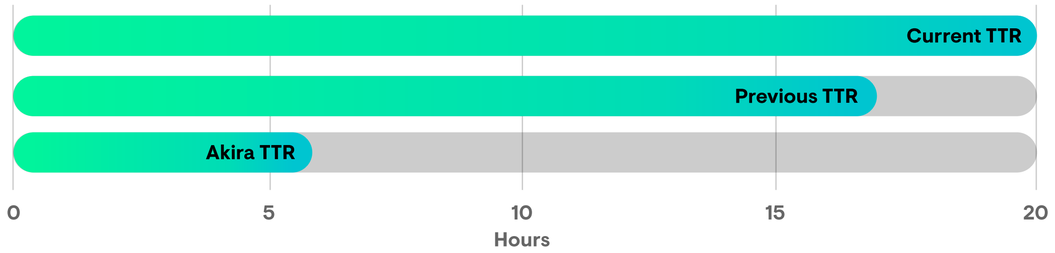


Figure 10: Monthly breakdown of tunneling and exfiltration methods linked to ransomware activity

Time-to-Ransom (TTR) Measurement



Last year, we introduced TTR, a specialized metric for the average time it takes ransomware operators to move from initial access to ransomware deployment. By investigating incidents where ransomware is deployed and analyzing activity logs, we determine the initial access time and attribute it to specific groups based on the attempted delivery of a ransomware note. This calculation is influenced by several critical variables, including where and how a ransomware operator gains initial access, level of network isolation in the environment, value of victim data and need for exfiltration, and more.

TTR helps shape our knowledge of operator maturity, intrusion complexity, and the operational workload required for successful attacks. For businesses, this metric also helps build knowledge for the average time to spot and mitigate ransomware threats based on real-world trends.

In 2024, our findings revealed an average TTR of approximately 17 hours, with "smash-and-grab" groups like Play, RansomHub, and Akira often deploying ransomware in less than seven hours.

By contrast, this year's data shows the average TTR increased to approximately 20 hours. We believe this trend is driven by several critical shifts and factors in attacker behavior:

Prioritizing Extortion and Data Theft

Attackers are shifting toward extortion operations, with more time spent on spotting and exfiltrating data. We often see exfiltration as the final step, happening within the last six hours of a ransomware incident. The three most common exfiltration methods are Archive tools (Zip/Rar), Encrypted Tunnel Relays (Cloudflared, SSH, Ngrok, and FRP), and FTP/Secure FTP (Filezilla, FTP.exe, WinSCP).

Operational Handoffs and Workloads

We're seeing longer "pauses" in activity that likely signal slower handoffs from initial access brokers and affiliates to ransomware operators. As groups take on larger workloads, the time between initial access and follow-up activity is longer.

Stealth Over Speed

Attackers prioritize "low and slow" methods over the high-velocity "smash-and-grab" tactics of previous years. Manual, multi-step techniques—like the `NTDS.dit` exploit—show how operators do more prep work to stay under the radar.

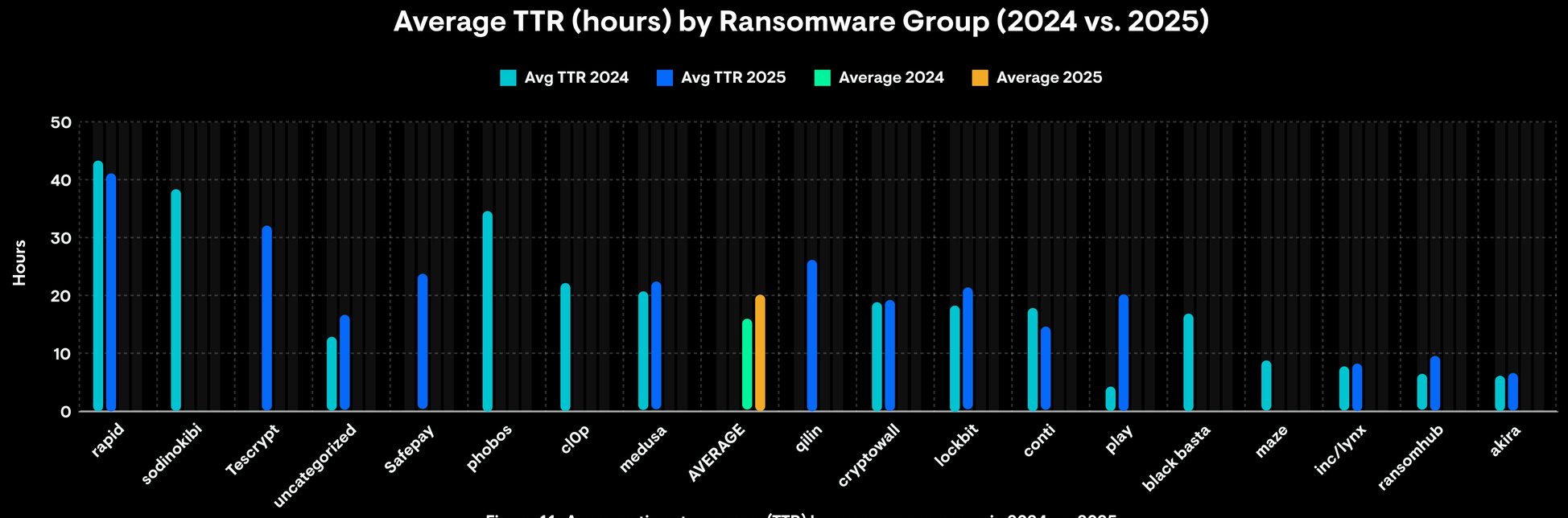


Figure 11: Average time-to-ransom (TTR) by ransomware group in 2024 vs. 2025

Notably, telemetry from our Identity Threat Detection and Response (ITDR) solution flagged a critical "pre-access" window, where precursor activity like account verification via stolen credentials from VPNs or data centers happens days or weeks before ransomware. Around 17% of ransomware incidents showed ITDR-related precursor activity at least seven days prior to deployment, a figure that climbed to nearly 21% when expanded to a 14-day window. This pattern suggests that infostealer operators or initial access brokers validate credentials so they don't go inactive/cold before high-velocity ransomware events go down.

The increase in average TTR reflects a strategic tactical move in how ransomware operators manage their intrusion timelines that suggests many groups are now prioritizing thorough data exfiltration and stealthy, manual techniques over the sheer velocity of "smash-and-grab" attacks. While the window for detection has widened, it's defined by "low and slow" activity and deliberate operational pauses.

For defenders, these findings highlight how important it is to spot late-stage indicators like encrypted tunnels or archive tools before the final deployment.

Mapping Ransomware Attack Paths With Initial Access Data



Figure 12: Encrypted file sample from Obscura ransomware

One of the biggest variables impacting TTR is initial access. This vector largely sets the stage for how efficiently ransomware operators execute attacks. Depending on how an operator compromises a system, they'll have a shorter TTR in the targeted environment, significantly decreasing detection time for defenders.

To understand these timelines, it is important to distinguish between two metrics:

Time-to-ransom (TTR)

measures the duration from initial access to the final deployment (or attempted deployment) of the ransomware payload

Time to ransomware activity

tracks the window from initial access to the first sign of malicious behavior, like lateral movement or credential harvesting

By focusing on the time to first activity versus just the final deployment, we can more accurately convey the true agility of these operators, and the narrow intervention window before an attack reaches its destructive final stage.

To illustrate how these timelines vary, we analyzed three common initial access methods: RATs, RMM tools, and ClickFix scams. We then measured the time from the initial compromise to ransomware activity, or attempted activity, within a 48-hour window.

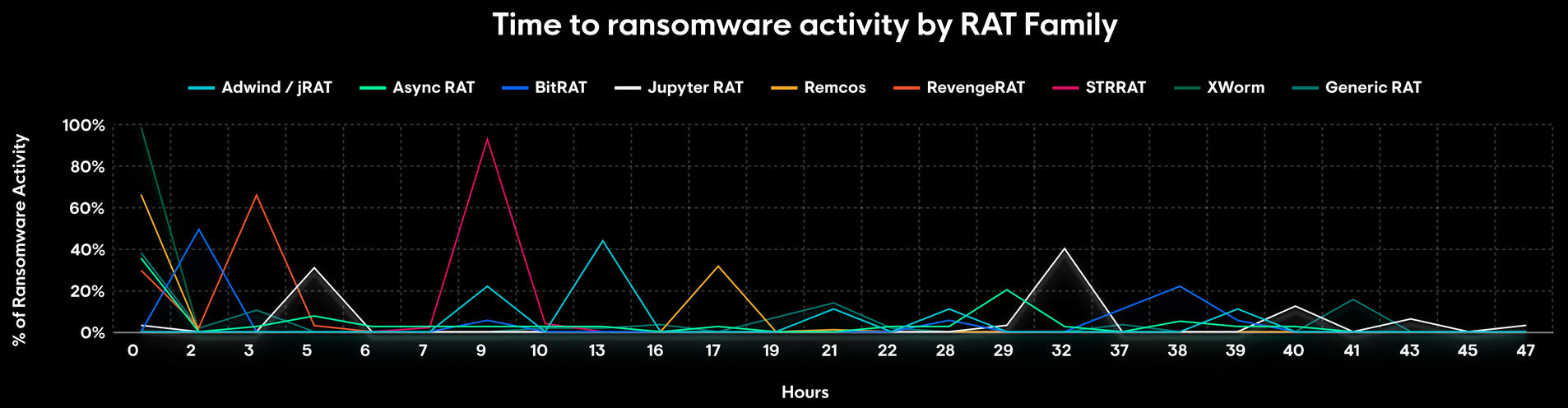


Figure 13: Time to ransomware activity within 48 hours of RAT install

RATs

The time between RAT installation and ransomware activity follows a highly compressed timeline. In cases where a RAT was the initial access vector, 25% escalated to ransomware activity within the same hour, and more than 50% did so within 12 hours. AsyncRAT is the most prominent catalyst for these handoffs, with one-third of ransomware activity happening within minutes of installation, a clear sign of immediate monetization. Depending on the family, these tools signal different behaviors: Jupyter RAT often indicates methodical "hands-on-keyboard" activity, while Remcose is typically deployed after gaining elevated privileges near the end of an operation.

These deployments frequently serve as a final hand-off point, a redundant communication channel, or a tool for data exfiltration, particularly for groups without other specialized exfiltration methods. Regardless of the variant, a RAT suggests an attacker has already completed extensive environmental prep, leaving a narrow window for defensive intervention. Here are three key things defenders should know:

RAT Detection as a "Late-Stage" Warning

Because most ransomware activity starts within 12 hours of a RAT install, these detections are emergency signals that an environment is already compromised and prepared for impact.

Variant-Specific Urgency

Certain families—specifically RevengeRAT, STRRAT, and XWorm—are precursors to imminent ransomware activity and require the same immediate response as the ransomware itself.

Strategic Redundancy & Exfiltration

Attackers often deploy RATs late in an operation so they have a persistent backup if ransomware deployment is interrupted, or for final data exfiltration before "going loud."

RMM Execution

Unlike the highly compressed and uniform timelines we saw with RATs, the transition from RMM execution to ransomware activity is notably varied. We identified three distinct operator workflows categorized by their timing and tool choice, and these strategies suggest that choosing an RMM for initial access is rarely random. It's a tactical reflection of the attacker's immediate goals, ranging from immediate execution to methodical multi-stage operations.

0–8 Hours

Near-Immediate Conversions

Ransomware activity that occurs within eight hours of RMM execution tends to be attackers who already have credentials, reconnaissance intelligence, and pre-staged executions planned. RMMs like RustDesk and various VNC iterations show the highest urgency, with 50% of ransomware activity happening within the first hour of RustDesk abuse. Atera follows a similar high-velocity pattern, with 75% of ransomware activity in under two hours, with a secondary peak of activity (~10%) between the six and eight hour marks. In these scenarios, the RMM is likely used as a safety net to ensure encryption delivery or as a specialized channel for late-stage data exfiltration.

8–12 Hours

Mid-Window Execution

This group aligns with human-operated cadences, where the RMM is used for "hands-on-keyboard" lateral movement or near-endgame staging. This timing is consistent with fast-operating ransomware groups, who migrate to their ransomware toolkits only after confirming they've landed on high-value targets. Tools like MeshCentral and PDQConnect typically see ransomware deployment between eight and twelve hours post-installation, suggesting the RMM is being used mid-operation to broaden environmental control and perform final defense evasions before "going loud."

12+ Hours

Initial Access & Reseller Gaps

The longest lead times are associated with larger, traditional RMM platforms, suggesting a multi-stage operation or a change in ownership. ScreenConnect and SimpleHelp have the longest dwell times, ranging from 18 to 32 hours, with SimpleHelp showing unique activity spikes at the 24-hour mark. AnyDesk displays a bifurcated strategy, where activity happens either immediately or after a distinct 48-hour delay. These extended gaps are hallmarks of Initial Access Broker (IAB) activity, where the ransomware group is the purchaser or the secondary phase of the operation. Furthermore, immediate deployments following these specific RMMs can be an indicator of successful bribing or insider threats, where the attacker bypasses the reconnaissance phase due to pre-existing knowledge or access.

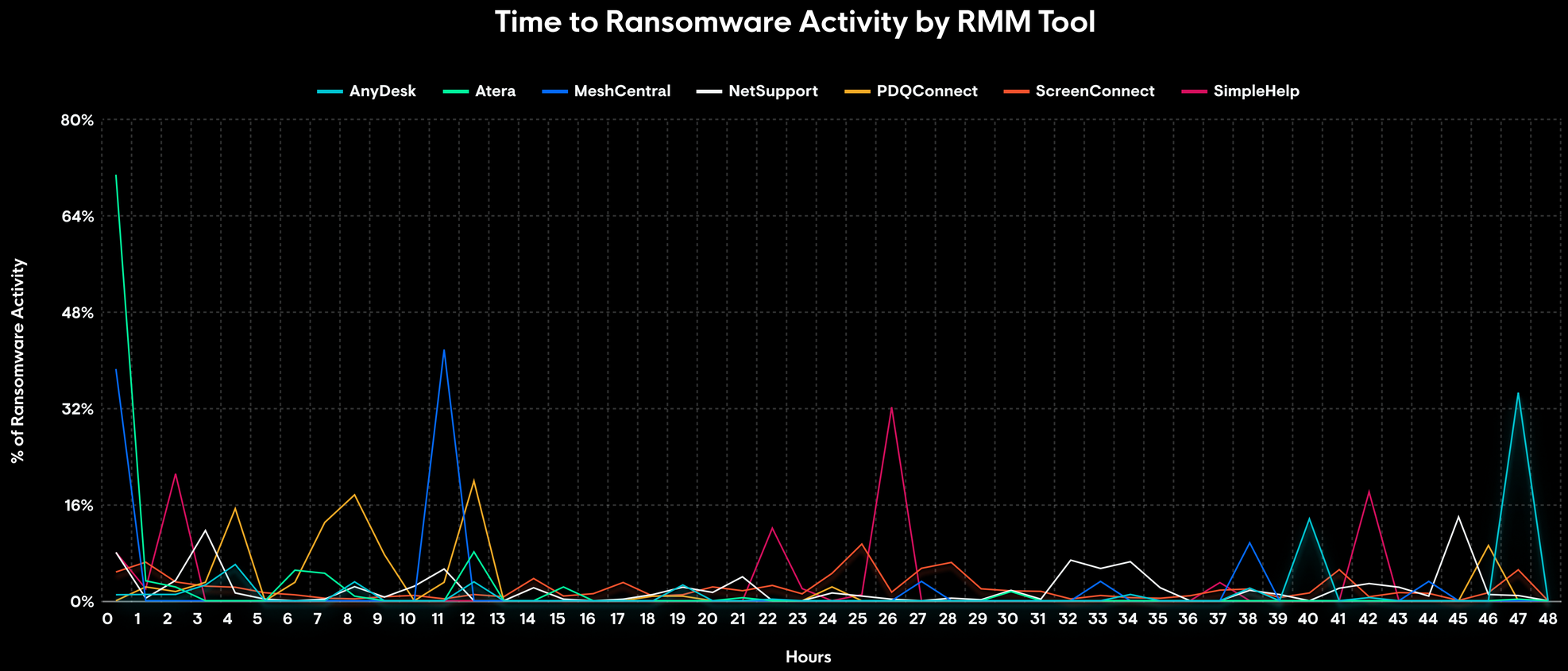


Figure 14: Time to ransomware activity within 48 hours of RMM execution

ClickFix Scams

ClickFix scams have become an initial access vector of choice for threat actors looking to exploit the human psyche, evade defenses, and target multiple platforms. These attacks trick users into unknowingly executing arbitrary commands, like PowerShell scripts or terminal instructions, under the guise of a legit authentication or troubleshooting process. The fake CAPTCHA lure, which makes users go through manual steps to "verify" they're human, has emerged as a common variation of this technique. Notably, our analysis found that fake CAPTCHA lures exhibit a markedly different time to ransomware activity compared to general ClickFix attacks, revealing two distinct operational strategies:

ClickFix (Rapid Deployment)

Timing data shows ClickFix campaigns are built for speed, with ransomware activity kicking off almost immediately after infection. Smaller spikes 16–20 hours later suggest some access is handed off or sold to specialized ransomware operators rather than used right away.

Fake CAPTCHA (Broker Model)

Shows a more distributed timeline with only 7% of ransomware activity starting within the first hour. The majority of handoffs happen between 6 and 16 hours, consistent with a model where system information is harvested and validated before being resold on the dark web.

While both methods had limited direct involvement in ransomware activities, with only 4% of ClickFix events and 6% of fake CAPTCHA events leading to ransomware, the sheer volume of these attacks makes them a serious threat. Even if ransomware isn't the immediate goal, if left unchecked, these threats can lead to the installation of infostealers, credential theft, or other malicious activity. Both should be treated with fast responses and threat hunting teams should look for signs of credential theft, secondary payloads, and lateral movement that typically happen with these attacks.

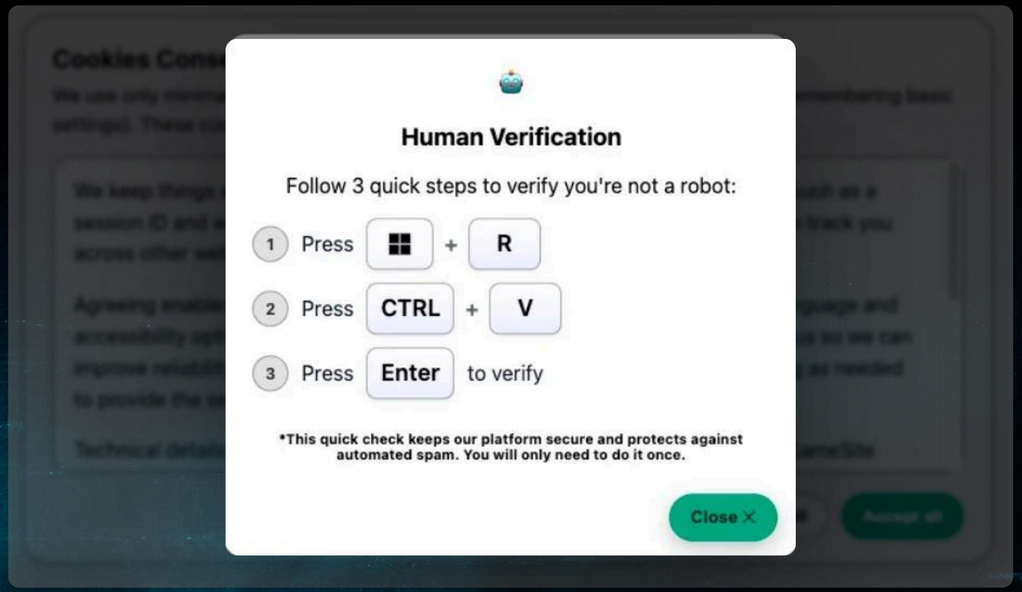


Figure 15: Example of a ClickFix human verification lure

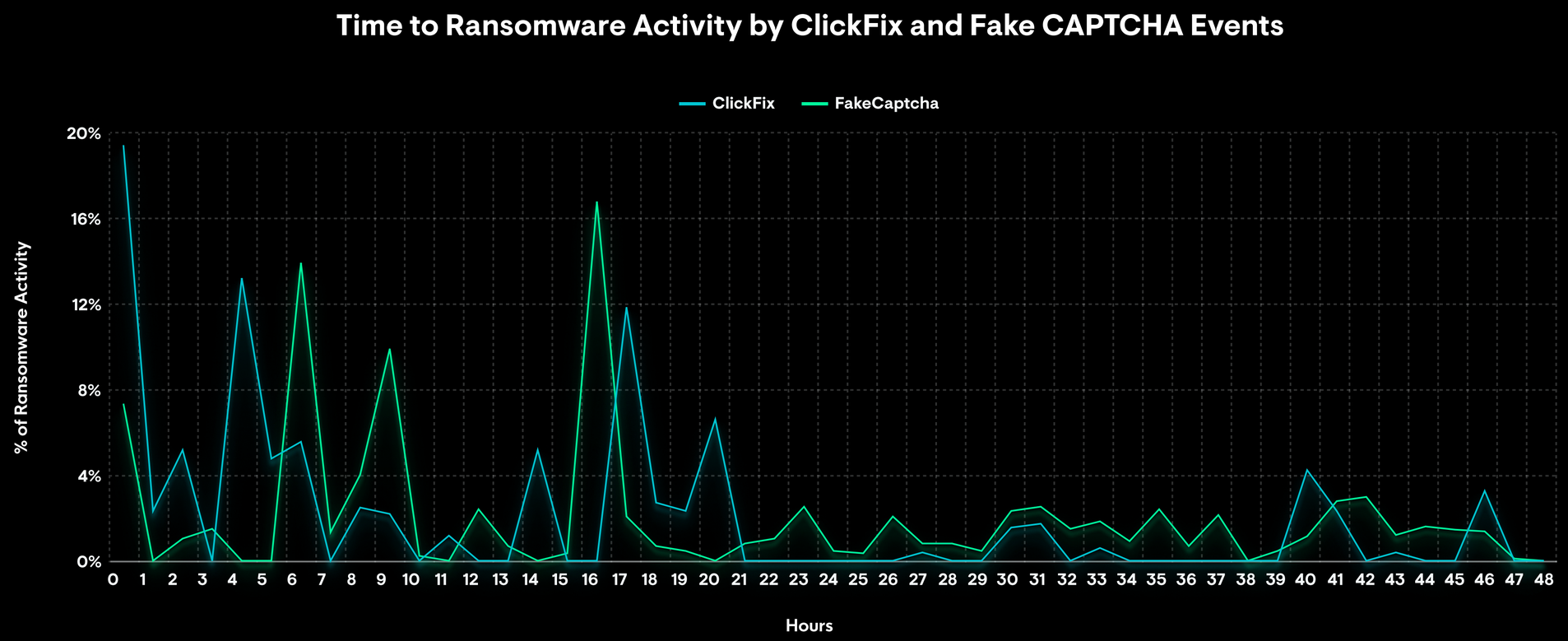


Figure 16: Time to ransomware activity within 48 hours of ClickFix and fake CAPTCHA events

Attacker Tools and Techniques

Hacking Tools

Attackers are ditching traditional hacking tools for trusted RMMs, which are tougher to spot and better for persistence. Speed and automation still matter, but blending in with legit admin software is now the bigger advantage.

When attackers compromise systems at scale, speed and automation are key. Threat actors use hacking tools to carry out fast, complex actions within a short window of intrusion opportunity. These tools bundle advanced capabilities like credential harvesting, memory dumping, password cracking, network discovery, lateral movement, persistence, installation, and remote C2 into streamlined workflows without a lot of effort.

Modern attackers often combine purpose-built offensive tooling with legitimate administrative and diagnostic software, abusing trusted binaries to blend into normal system activity. Common examples include the Sysinternals Suite, network scanners, and PowerShell-based frameworks.

A noticeable trend in 2025 is the growing replacement of traditional hacking frameworks with abused RMM tools for command-and-control, persistence, and lateral movement. With detection of traditional hacking tools improving, RMM abuse is becoming popular for maintaining access and control in post-compromise environments, since these platforms are already trusted.

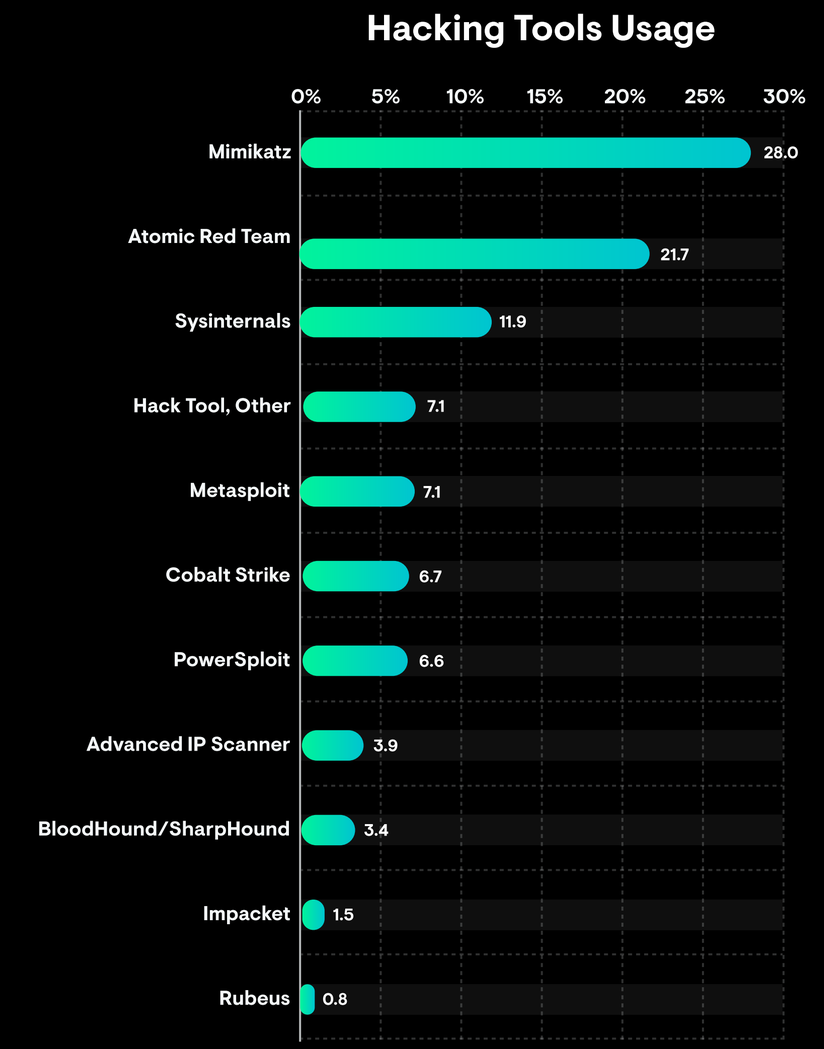


Figure 17: Distribution of hacking tools used in 2025

In 2025, Mimikatz, a well-known, open-source post-exploitation tool used to extract credentials from Windows systems, was the most frequently observed hacking tool by event volume, accounting for 28% of all hacking-tool detections. Originally created as a proof-of-concept to show weak spots in Windows authentication, Mimikatz has become a popular dual-use tool that can pull plaintext passwords, hashes, Kerberos tickets, and other sensitive credentials from system memory.

Despite being more than a decade old, Mimikatz remains central to credential-theft operations. It's commonly executed via direct payloads, through PowerShell scripts, or embedded within larger malware frameworks. The continued prevalence of Mimikatz highlights the lasting value of credential access in post-compromise activity and its deep integration into modern intrusion and ransomware campaigns from groups like Akira and Play.

Atomic Red Team, an open-source framework that does small, focused tests to emulate adversary behavior, accounted for 21.7% of hacking-tool detections in 2025. Repeated test executions drove this volume and automated emulation workflows. Although Atomic Red Team is most commonly used for defensive testing and purple-team activities, its activity is indistinguishable from real adversary behavior at the telemetry level. Because of this, its frequent appearance in detection data reinforces how important context and analyst validation is when interpreting its presence in an environment.

Sysinternals tools, a collection of free monitoring and troubleshooting utilities from Microsoft, accounted for 11.9% of detections, underscoring continued abuse of legitimate administrative tools for malicious purposes. We saw threat actors using tools like `ProcDump`, `PsExec`, and related binaries for credential dumping, remote execution, and reconnaissance, letting attackers operate under the guise of normal system administration.

Mimikatz Attack Techniques	
Pass the Hash	Attackers steal NTLM hashes to authenticate to systems without needing plaintext passwords, gaining access even if credentials are encrypted.
Pass the Ticket	This technique uses captured Kerberos tickets to impersonate legitimate users and authenticate to other systems across the network.
Kerberos Golden Ticket	One of the most critical attacks where an operator forges a Ticket Granting Ticket (TGT) for a Domain Admin, granting unrestricted and persistent control over the entire network.
Overpass the Hash	An advanced method that converts stolen NTLM hashes into Kerberos tickets, allowing attackers to bypass standard authentication mechanisms.
DC Sync Attack	A stealthy method where Mimikatz mimics a Domain Controller to trick the environment into replicating sensitive data, including admin password hashes.

Hacking Tools Usage (2024 vs. 2025)

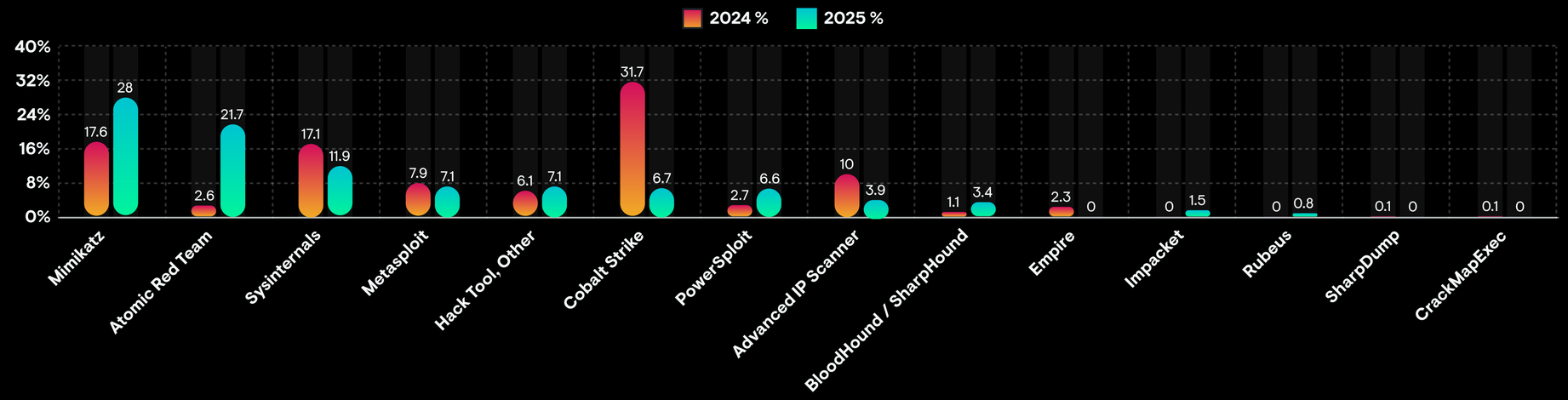


Figure 18: Distribution of hacking tools used in 2024 vs. 2025

Cobalt Strike, while still an important tool in adversary tradecraft, represented a smaller share of total events in 2025 (6.7%) compared to previous years. It appears Cobalt Strike users shifted toward tools like Atomic Red Team, PowerSploit, BloodHound, or, in some cases, legitimate RMM tools.

Despite this decline in event volume, Cobalt Strike is still one of the most operationally significant frameworks, widely used by both cybercriminals and advanced threat groups because of its mature command-and-control (C2) capabilities and flexibility. Known APT groups, including Ocean Lotus, APT31, Cinnamon Tempest, and Wizard Spider, use Cobalt Strike to blend malicious activity with legitimate red-team behavior for plausible deniability.

Other notable tools observed in 2025 include Metasploit (7.1%), PowerSploit (6.6%), Advanced IP Scanner (3.9%), and BloodHound / SharpHound (3.4%), each playing specific roles in exploitation, credential access, and Active Directory reconnaissance. Frameworks like Empire, Impacket, Rubeus, and CrackMapExec appeared less frequently by volume, but are still impactful due to their targeted use in lateral movement and domain compromise operations.

Malware Loader Activity

Thanks to international law enforcement, the malware ecosystem took a few solid hits this year. Operation Endgame targeted major loader families like Qakbot, Bumblebee, and Trickbot. But malware loaders didn't disappear in 2025.

Malware loaders are usually small components—often PowerShell, JavaScript, or other natively supported scripting languages—that send back environmental information to the attacker, set a specific flag or key, and then download additional malware components onto the victim's computer. While all malware loaders are designed to gain initial access and drop secondary payloads, our telemetry shows that some are also used as a stealthy way to launch additional tooling at later stages throughout the attack path, often going unnoticed by victims. In some cases, threat actors remove loaders once they've done their job to minimize their attack footprint in the targeted environment.

Loaders can be diverse in terms of operational functionality. Some are rented or purchased by one group to give access to another group. We've also seen loaders get delivered pre-infected by another group's malware, and then hijack existing infections with their own malware later in the compromise phase.

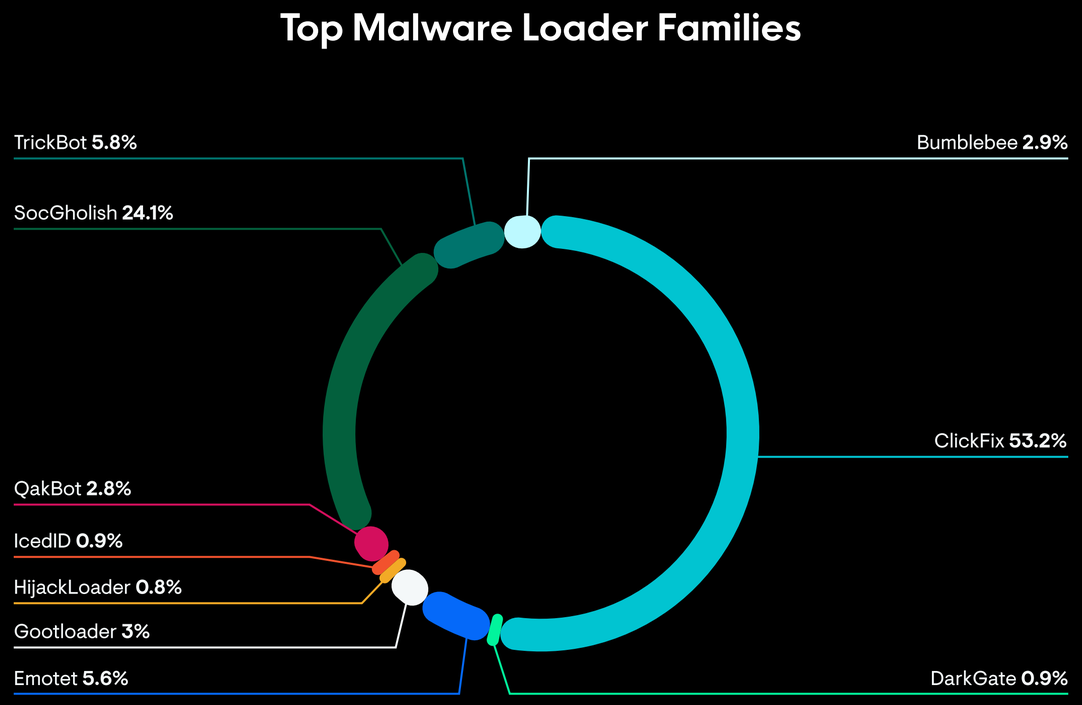


Figure 19: Distribution of malware loader families

ClickFix

The 'Human-Operated' Attack Chain



In 2025, malware authors doubled down on adding more innovative defense evasion, stealth techniques, and obfuscation into their malware variants, like Gootloader using custom WOFF2 fonts with glyph substitution for filenames.

Most malicious loader activity centers around user interaction abuse, deceptive execution chains, and staged payload delivery. This reflects a continued shift by threat actors toward techniques that reduce reliance on exploits and instead leverage trust, familiarity, and built-in operating system capabilities.

ClickFix emerged as the main malware loader delivery mechanism, representing over half (53.2%) of all observed loader executions. ClickFix campaigns are characterized by highly repeatable social-engineering workflows that instruct users to manually copy and execute commands, most often through PowerShell, MSHTA, or LOLBins. These campaigns are particularly effective because they rely on exploiting user trust (rather than vulnerabilities) and look like normal administrative or user activity.

Like we saw in 2024, SocGholish, a malware framework that uses social engineering to trick users into downloading infected updates, is a major initial access vector. This year, it accounted for 24.1% of all malware loader and initial access behavior. It's typically associated with fake update themes and drive-by delivery mechanisms, often executed through JavaScript or browser-assisted execution chains. Its persistence highlights the ongoing effectiveness of compromised web infrastructure and malicious advertising as a scalable infection vector, particularly against environments with permissive browser execution policies.

QakBot (2.8%), Emotet (5.6%), and Gootloader (3%) loaders might be lower in volume this year, but they're clear red flags for fast moving secondary malware payloads, including RATs, credential stealers, and ransomware precursors. Compared to SocGholish, for example, these loader families are a clear sign of a more deliberate attack path following initial access: staged execution, discovery, and lateral movement.

Think of loaders as a prime opportunity to interrupt an attack. By proactively identifying and neutralizing them, defenders can stop an intrusion in its tracks. It's a vital step for securing your environment.

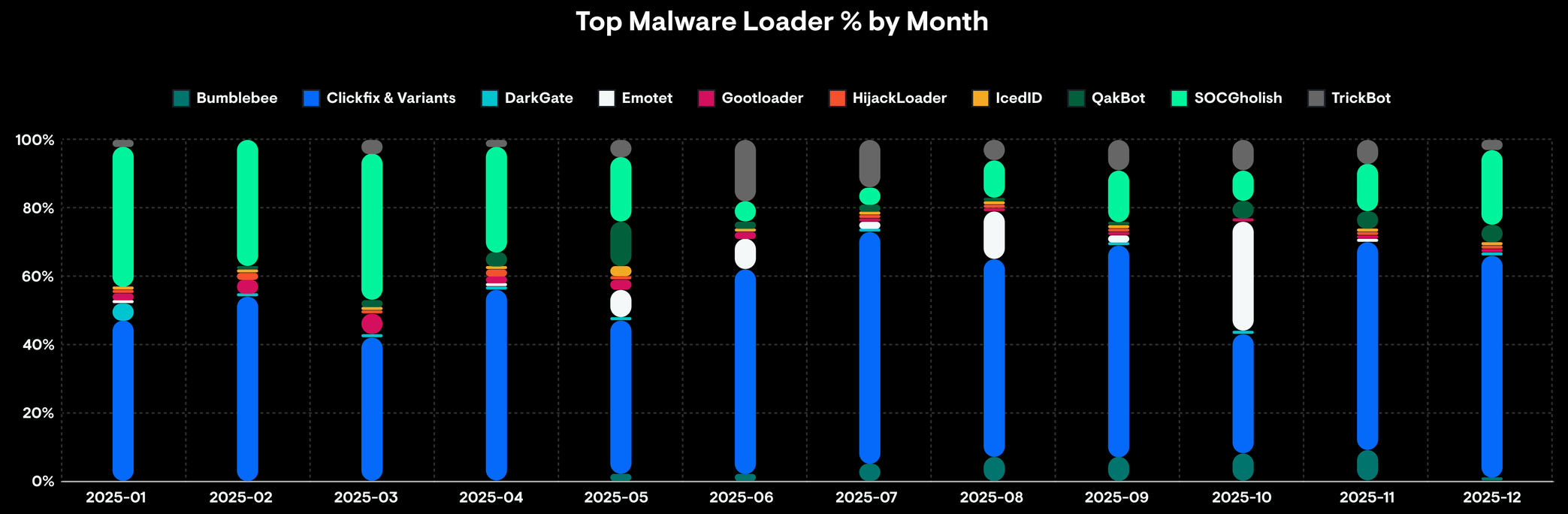


Figure 20: Monthly distribution of malware loader families in 2025

Remote Access Trojans (RATs)

RATs disguise themselves as legitimate or harmless files or applications to trick a user into installing and downloading them, giving the attacker control over the infected device. RAT activity in our 2025 telemetry data reflects a post-initial access phase of compromise, where attackers transition from delivery and staging into persistent control, reconnaissance, credential access, and lateral movement. Unlike malware loaders, RATs represent an explicit intent to maintain interactive access to endpoints, and often serve as the operational backbone for longer-lived intrusions.

With over 50% of RAT activity, AsyncRAT led the pack in 2025. It frequently sets the stage for ransomware and has become a staple in enterprise intrusion playbooks.

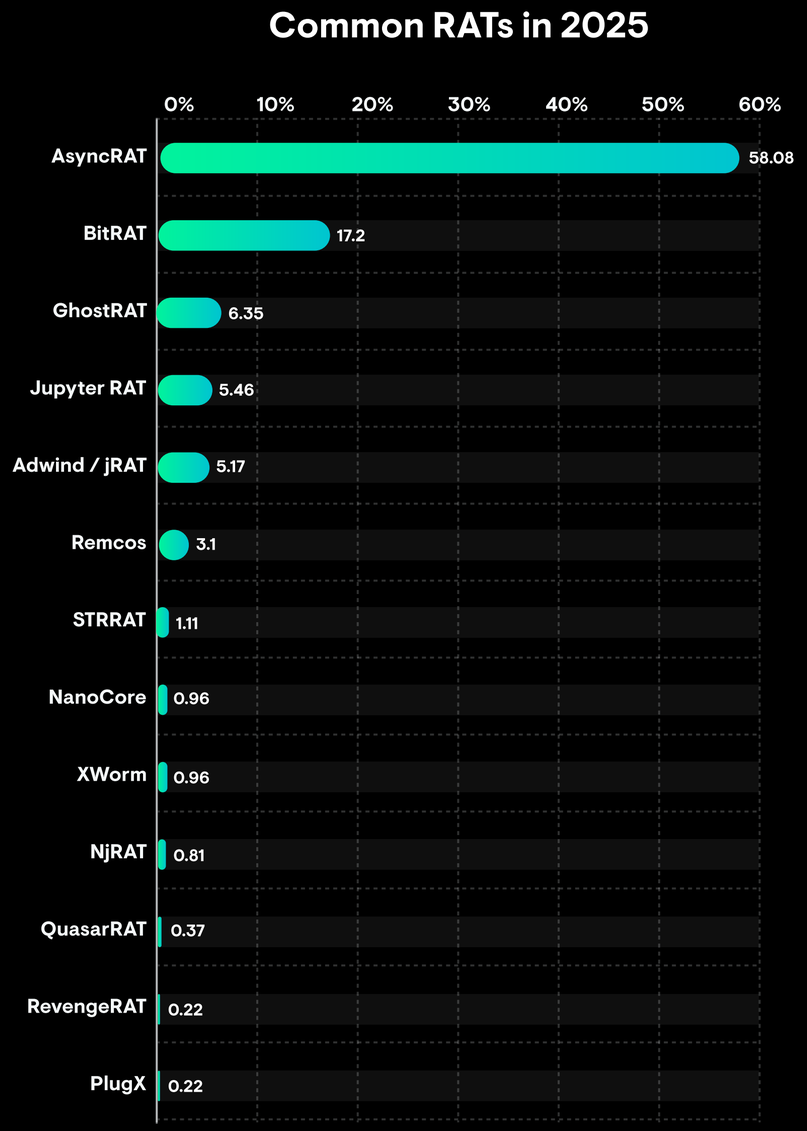


Figure 21: Distribution of RATs

In 2025, cybercriminals relied on less than 10 malware families for most RAT deployments, with execution patterns strongly aligned to loader activity observed elsewhere in the telemetry. In many cases, RAT execution happens shortly after initial access loaders like ClickFix, SocGholish, or similar delivery mechanisms, reinforcing the modular attack life cycle we saw throughout 2025.

RAT execution is rarely isolated. Instead, it's most often observed:

- Following loader execution, sometimes within minutes or hours
- As part of a multi-stage execution chain
- On systems that subsequently exhibit discovery, credential access, or privilege escalation behavior

This attack sequencing shows that RATs aren't the entry point—they're the control mechanism used after initial access is secured.

RAT(s)	Primary Role	Key Activity
AsyncRAT	Foundational Access Enabler	Most prevalent RAT family of 2025, thanks to its accessibility, extensibility, and wide adoption. It's typically executed as managed .NET binaries staged from user-writable directories and used to establish a persistent foothold, execute interactive commands, transfer files for payload staging, and conduct initial credential harvesting and reconnaissance. It frequently precedes ransomware activity in structured intrusion playbooks and has become a foundational access tool in enterprise ransomware operations.
BitRAT & GhostRAT	Stealth and Persistence	Used less than AsyncRAT but is operationally significant due to its focus on stealth and persistence. Technical activity is characterized by obfuscated execution parameters, non-standard parent/child process relationships, and deliberate attempts to blend into legitimate application execution paths. Their presence typically indicates a more deliberate intrusion phase rather than mass commodity activity.
Jupyter & Python-Based RATs	Evasive Scripting Framework Targeting Browser Info	This year, a variant of Jupyter was notable for using Python runtimes or embedded interpreters to move across networks where Python exists. This can evade detection due to their script-based nature and quickly introduce functionality and modular capabilities. Activity often overlaps with generic RAT and infostealer heuristics, as they target browser credentials and cryptowallets. This particular variant was frequently deployed in environments where scripting execution is common to reduce the operational footprint.
Remcos, STRRAT, & NjRAT	Ransomware Affiliate Workflow	Used in targeted or semi-targeted campaigns, these families are typically used in affiliate-driven ransomware ecosystems where operators prioritize rapid deployment and broad compatibility. Remcos occupies a niche between commodity RATs and advanced frameworks, used to establish persistence, conduct reconnaissance, and stage payloads before moving to ransomware execution. Activity is followed by delivery/staging and impact-oriented behavior, aligning with ransomware workflows rather than espionage.

Figure 22: Breakdown of most common RAT activity observed in 2025

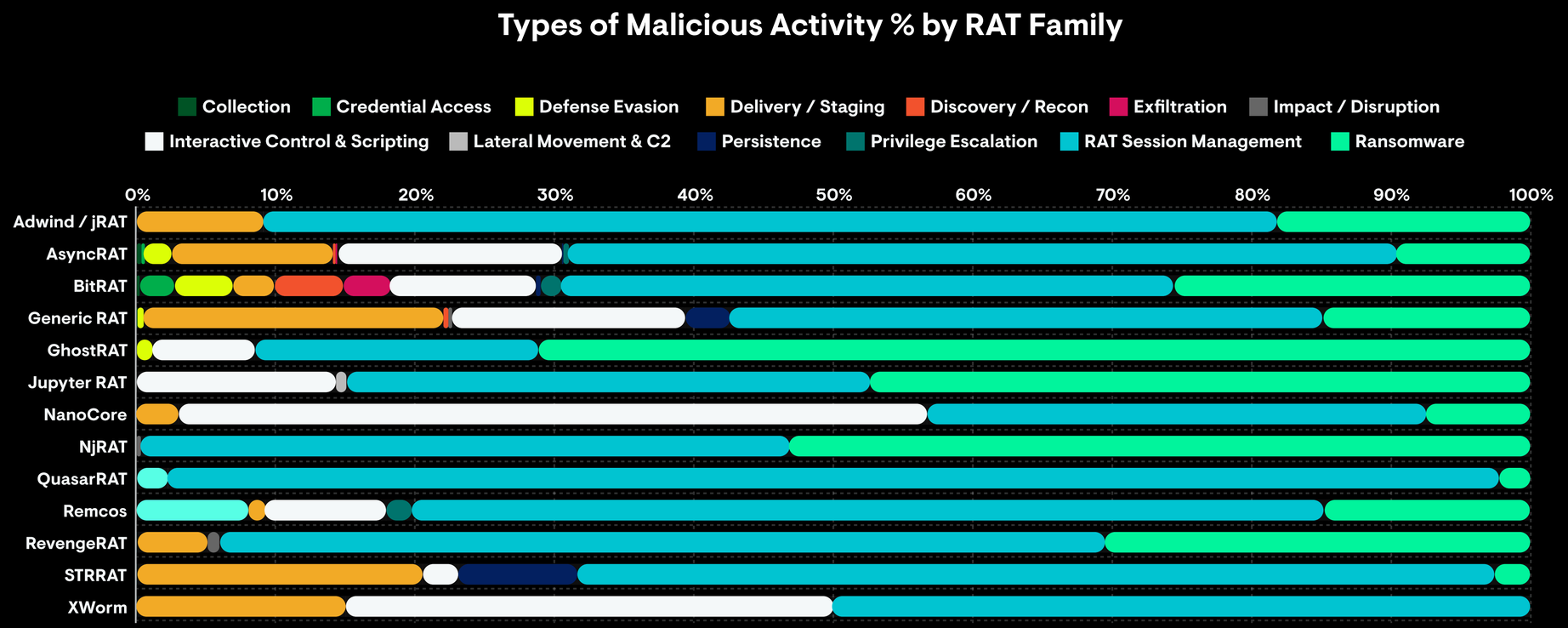
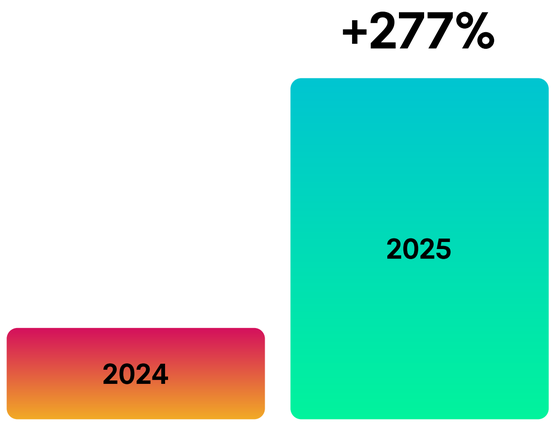


Figure 23: Distribution of malicious activity following RAT installation

RMM Abuse

RMMs are Hackers' New Favorite Weapon



Attackers are ditching traditional hacking tools and abusing trusted software that blends into normal business workflows—RMM abuse alone is up 277% year over year.

RMM solutions have emerged as hackers' new favorite weapon, offering stealth, persistence, and operational efficiency. Because they're legitimate tools, their activity can look completely normal, making malicious use harder to spot. As a result, we've seen a surge in RMM abuse over the past year, with the threat now accounting for 24% of all incidents observed at Huntress.

RMM abuse has evolved beyond opportunistic usage into a deliberate, standardized intrusion strategy. As cybercriminals built entire playbooks around these tools to drop malware, steal credentials, and execute commands, the use of traditional hacking tools plummeted by 53%, while RATs and malicious scripts dropped by 20% and 11.7%, respectively.

This shift reflects a broader pivot in the threat landscape, where attackers are increasingly "living off the land" and weaponizing the same applications, tools, and solutions businesses use for day-to-day operations.

> "Instead of running their own malware to conduct C2 functions, attackers have moved to using legitimate RMM solutions that offer an interactive console, HOK access, and all the features and functionality they could want."
>
> **Robert Knapp**
> Director, Security Operations Center

RMM Techniques and Tool Analysis

In 2025, RMM tools transitioned from simple initial access points to dominant post-access channels. Our analysis throughout the year consistently showed that once an RMM agent is established, the use of traditional malware becomes notably rare. This highlights a deliberate shift in which adversaries swap short-lived implants for legitimate management tooling to sustain access and reduce their footprint.

Rather than deploying custom backdoors, attackers now leverage RMMs as a unified control hub for the following:

Consolidated C2

Once deployed, RMM tooling often became the only interactive access method, with outbound network noise decreasing, as operators used RMMs to issue commands, transfer tooling, and orchestrate follow-on actions.

Execution via LOLBins

There is a high correlation between RMM sessions and the execution of native Windows utilities (e.g., `PowerShell`, `msiexec`, `rundll32`, `certutil`). This indicates hackers mainly used RMMs to "live off the land" and execute native tooling rather than introduce new binaries.

Attack Path Redundancy

Attackers often installed two or more RMM agents during a single intrusion. This gave them a "fail-safe" persistence method, ensuring that if one tool was detected and removed, persistent access was maintained through the second.

Throughout the year, malicious tradecraft consistently followed suspicious RMM executions, with each major RMM platform highlighting a unique blend of attacker behaviors. Attackers strategically chose specific RMM platforms based on their operational objectives and the stage of their intrusion. A detailed analysis of non-RMM activity within a 24-hour window of suspicious RMM execution revealed distinct behavioral patterns from each major tool.

These findings highlight how hackers strategically weaponize specific RMM tools during certain phases of the attack lifecycle:

- ScreenConnect sets up orchestration and credential harvesting
- NetSupport speeds up staging
- AnyDesk and Atera align with ransomware execution
- Splashtop supports credential-driven lateral expansion
- PDQConnect is an initial delivery bridge

When correlated with 24 hour post-infection tradecraft, RMM telemetry shows a high-confidence signal of where an intrusion is headed in the attack path, not just the one in progress.

Over 50% of activity following suspicious Atera instances ties to ransomware, highlighting its role in late-stage abuse. It usually shows up during active ransomware and extortion efforts.

Adjacent Malicious Activity by RMM Tool (24 Hours Post-Compromise)

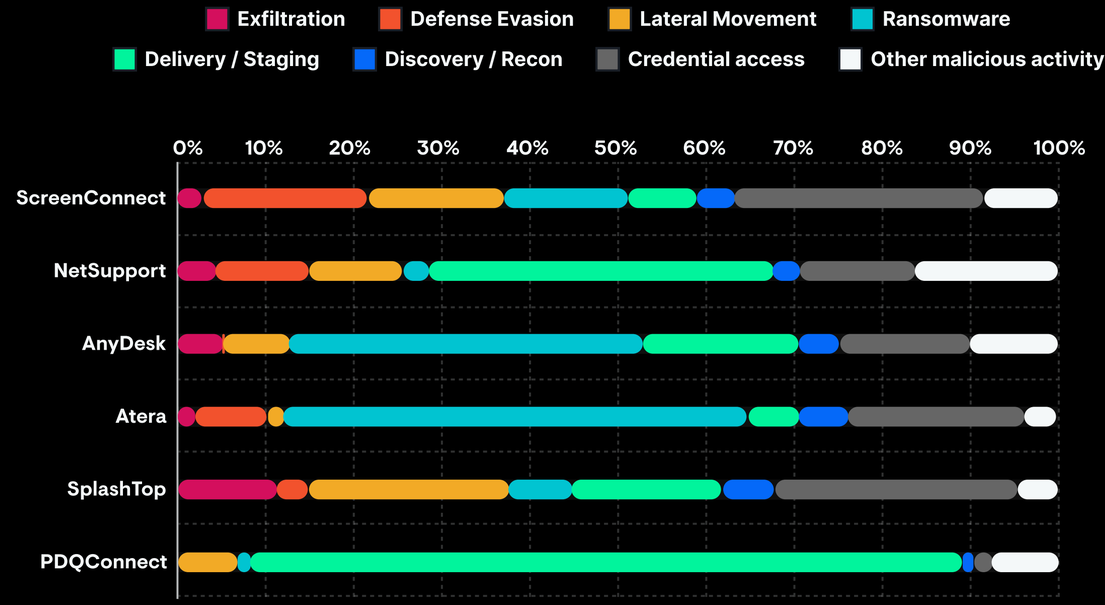


Figure 24: Adjacent malicious activity by RMM tool within 24 hours of RMM execution

Tool	Primary Operational Role During Attack	Key Activity
ScreenConnect	General Purpose Post-Access	Most often used to stabilize access, contain defenses, harvest credentials, and coordinate movement before or alongside impact versus trigger encryption right away.
NetSupport	Early Operationalization	Mainly used for delivery and staging, far exceeding any other RMM observed in this category. Frequently abused during the early operationalization phase, where attackers move from initial access into active execution and tool deployment. Rarely the final control mechanism during impact.
AnyDesk and smaller DWAgent, Chrome Remote, and ZohoAssist	Stabilization & Pre-Encryption	Commonly introduced during stabilization and pre-encryption phases, where attackers reinforce access, validate credentials, and prep the environment for extortion.
Atera	Late-Stage Impact	More than half of activity following a suspicious Atera execution is ransomware-related, with the RMM exhibiting the clearest late-stage abuse profile. Rarely used for initial access or staging and instead appears once attackers are actively executing ransomware and extortion operations.
Splashtop	Lateral Expansion	Often used to harvest credentials and pivot internally, rather than to directly facilitate encryption events.
PDQConnect	Initial Delivery Bridge	Majority of activity is tied to delivery and staging. Frequently used as a transitional mechanism to introduce other RMM tooling before attackers pivot to RMM platforms better suited for sustained control and impact.

Figure 25: Breakdown of adjacent malicious activity within 24 hours of RMM activity by tool

While RMM abuse patterns vary by tool, we observed three core techniques that remain consistent across all platforms. These methods exploit the inherent trust granted to administrative tools, letting attackers execute commands and move files under the guise of authorized maintenance. By focusing on these shared behaviors, rather than specific tool techniques, defenders can more accurately distinguish malicious activity from routine system management.

Direct File Drop and Execution

RMM sessions were used to transfer and execute payloads directly on endpoints, often via built-in file transfer mechanisms or native Windows utilities. Payloads included secondary tools, scripts, and persistence components.

Remote PowerShell Sessions

PowerShell execution over RMM channels was common, enabling script-based discovery, defense evasion, and follow-on tooling deployment. These sessions frequently leveraged encoded or obfuscated commands to blend with legitimate administrative activity.

Lateral Movement Through Internal RMM Consoles

In environments where RMM platforms were already deployed internally, adversaries abused existing consoles to pivot laterally. This included using trusted RMM infrastructure to access additional hosts without introducing new external connections, significantly reducing detection opportunities.

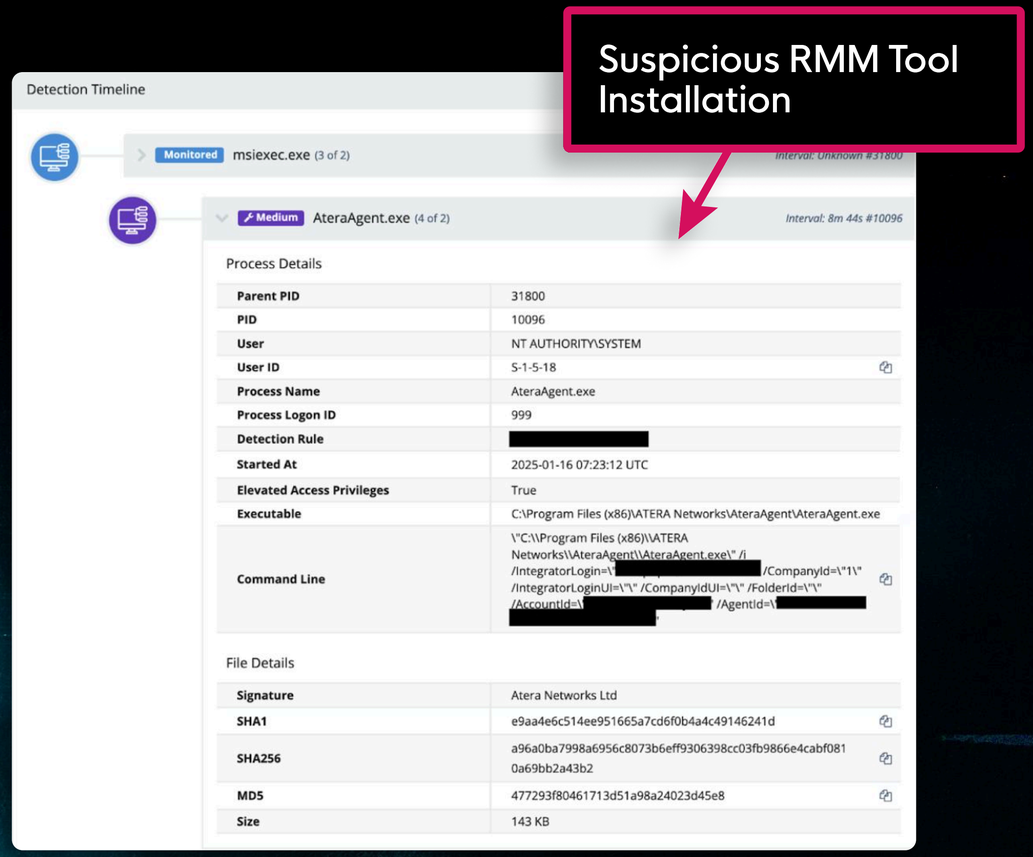


Figure 26: An attacker gained persistence with RMM installation

Redefining Defense in the Era of RMM Abuse

The evolution of RMM abuse in 2025 highlights a critical challenge for defenders: adversaries are increasingly aligning their operations with legitimate administrative behavior. By mimicking routine IT workflows, leveraging trusted management tools, and minimizing the use of distinct malware artifacts, attackers are blurring the lines between malicious and authorized activity. Defenders should expect this pattern to continue.

As long as RMMs are easy to deploy and tough to differentiate from authorized activity, they will be an attractive vector for both initial access brokers and financially motivated threat groups. Attackers are also tailoring their use of specific RMM platforms to align with distinct operational goals. This deliberate selection of RMM tools based on their unique capabilities and the stage of an intrusion highlights the sophistication of modern attacker tradecraft.

Detection strategies that rely solely on malware signatures or traditional indicators of compromise are no longer sufficient. Effective defense requires a shift toward behavioral detection, focusing on anomalous RMM usage, execution patterns, and deviations from established administrative baselines. Organizations must treat RMM telemetry as a high-confidence signal of potential compromise, especially when correlated with adjacent suspicious activity.

Organizations can stay ahead of this threat by:

- ✓ Treating unexpected RMM installations as high-confidence signs of compromise
- ✓ Applying the latest security patches to close the gap on vulnerabilities
- ✓ Reviewing logs regularly to detect suspicious or unauthorized RMM activity
- ✓ Using security awareness training to teach employees to quickly spot and report shady lures
- ✓ Enforcing MFA on all RMM platforms and accounts
- ✓ Restricting external connections from atypical geographies or infrastructure. Enforce IP allow lists where supported.
- ✓ Routinely auditing and monitoring remote access tools to maintain an up-to-date inventory of approved RMM solutions
- ✓ Locking down new RMM agent enrollment with approval workflows and device validation

Exploit-Driven Campaigns

SonicWall Exploitation

(CVE-2024-40766)

A huge wave of exploit-driven incidents we saw this year was threat actors targeting an improper access control flaw (CVE-2024-40766) in SonicWall SSLVPN devices. SonicWall noted this 2024 vulnerability stemmed from firewall migrations from sixth to seventh generation, where local user passwords were carried over without being reset. In the activity that spiked between July and August, attackers exploited flaws in SonicWall to gain administrative access, move laterally, steal credentials, disable security defenses, and deploy Akira ransomware. With no evidence of password spraying or invalid login tactics, attackers had authentication bypass, stolen credentials, or previously undetected systems access.

Our analysis of SonicWall post-exploitation activity since August shows attackers create interactive access, not fully automated follow up payload deployment. About 51% of behavior we looked at immediately following compromise consisted of profile and interactive user initialization artifacts. Beyond these actions, roughly 20% of follow-up events pointed to clear hands-on-keyboard activity, including manual command execution, system domain discovery, privilege elevation, and direct inspection of logs, security settings, and file contents.

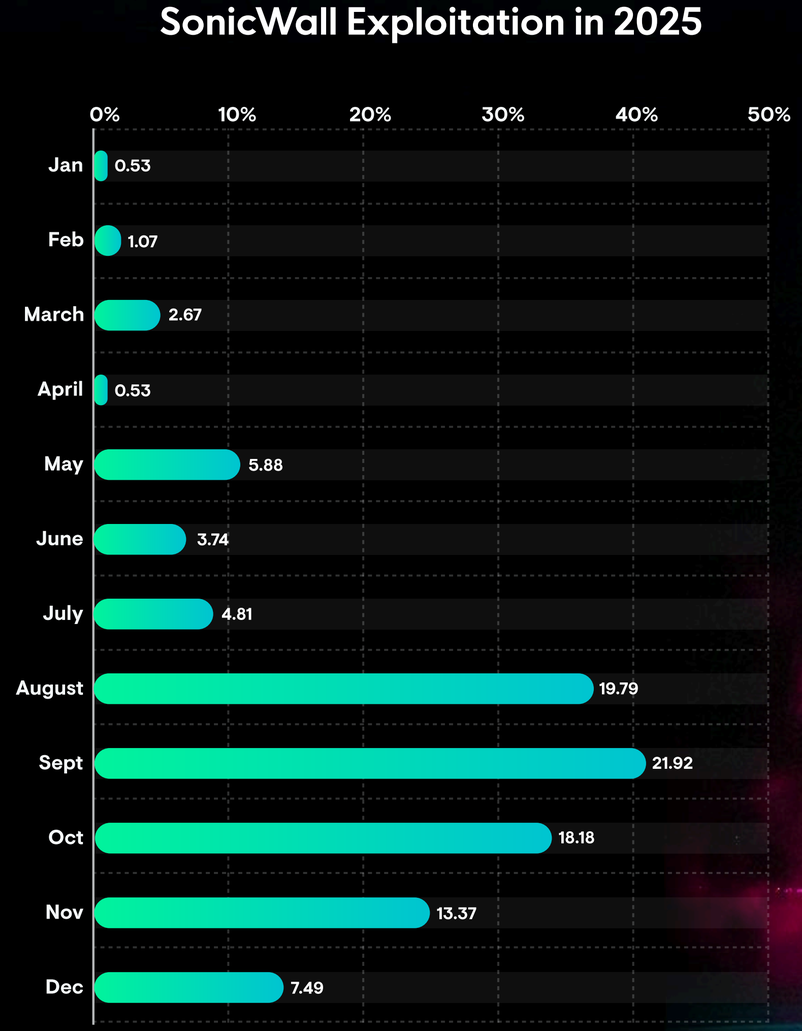
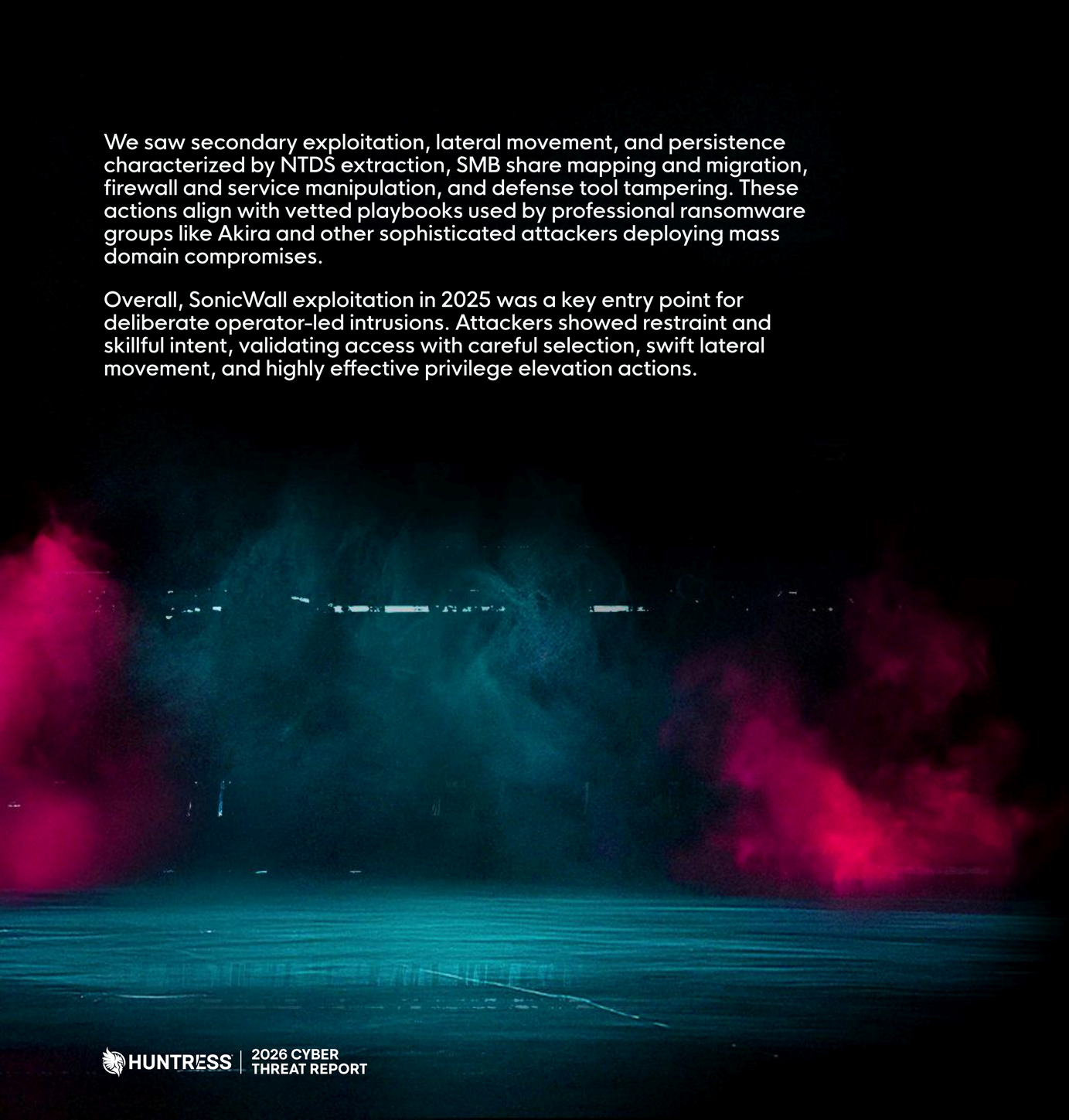


Figure 27: Monthly breakdown of SonicWall Exploitation

We saw secondary exploitation, lateral movement, and persistence characterized by NTDS extraction, SMB share mapping and migration, firewall and service manipulation, and defense tool tampering. These actions align with vetted playbooks used by professional ransomware groups like Akira and other sophisticated attackers deploying mass domain compromises.

Overall, SonicWall exploitation in 2025 was a key entry point for deliberate operator-led intrusions. Attackers showed restraint and skillful intent, validating access with careful selection, swift lateral movement, and highly effective privilege elevation actions.



Types of SonicWall Post-Exploitation Activity

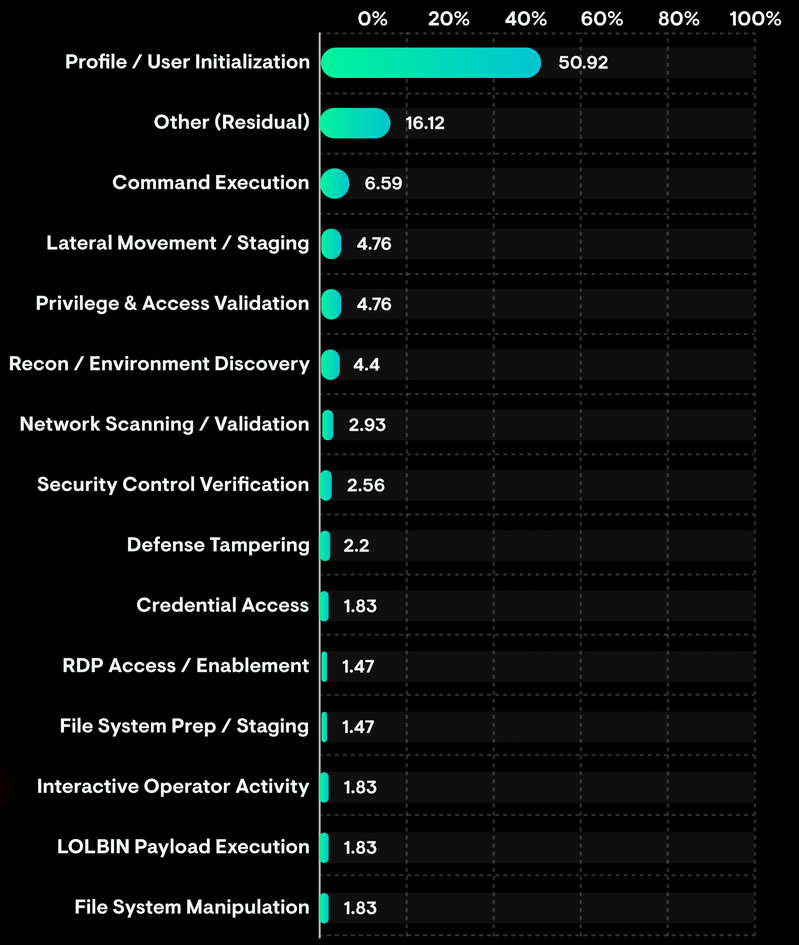


Figure 28: Distribution of SonicWall post-exploitation activity

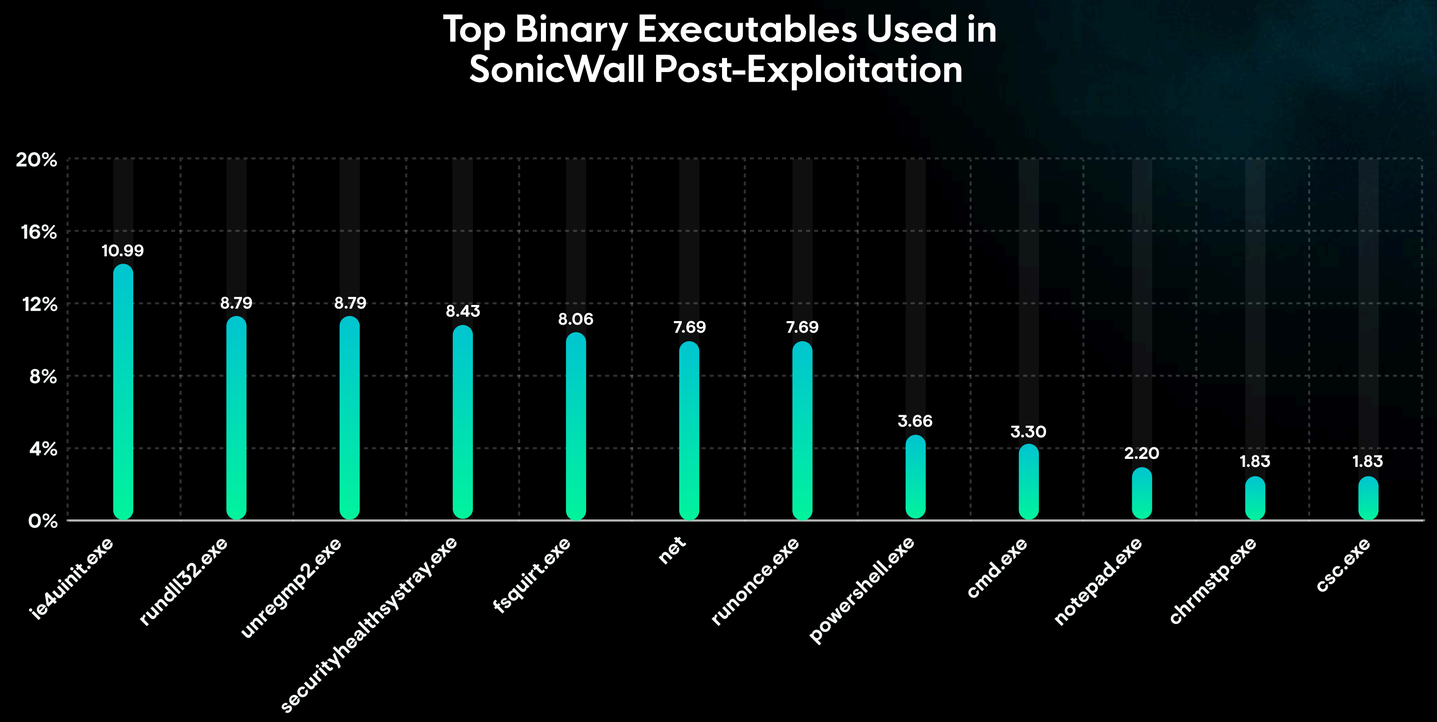


Figure 29: Most common binary executables used in SonicWall post-exploitation activities

CrushFTP Exploitation

(CVE-2025-31161)

In April, we saw in-the-wild exploitation of an authentication bypass flaw (CVE-2025-31161) in CrushFTP software. This vulnerability impacted how the file transfer application handles user authentication and gave attackers access to the application's administrator user account, which led to new backdoor accounts, unauthorized file access (upload and download), malicious code execution, and full control of the vulnerable server. Across several incidents, we saw threat actors exploit the flaw to deploy MeshAgent, install malicious AnyDesk RMM instances, and more.

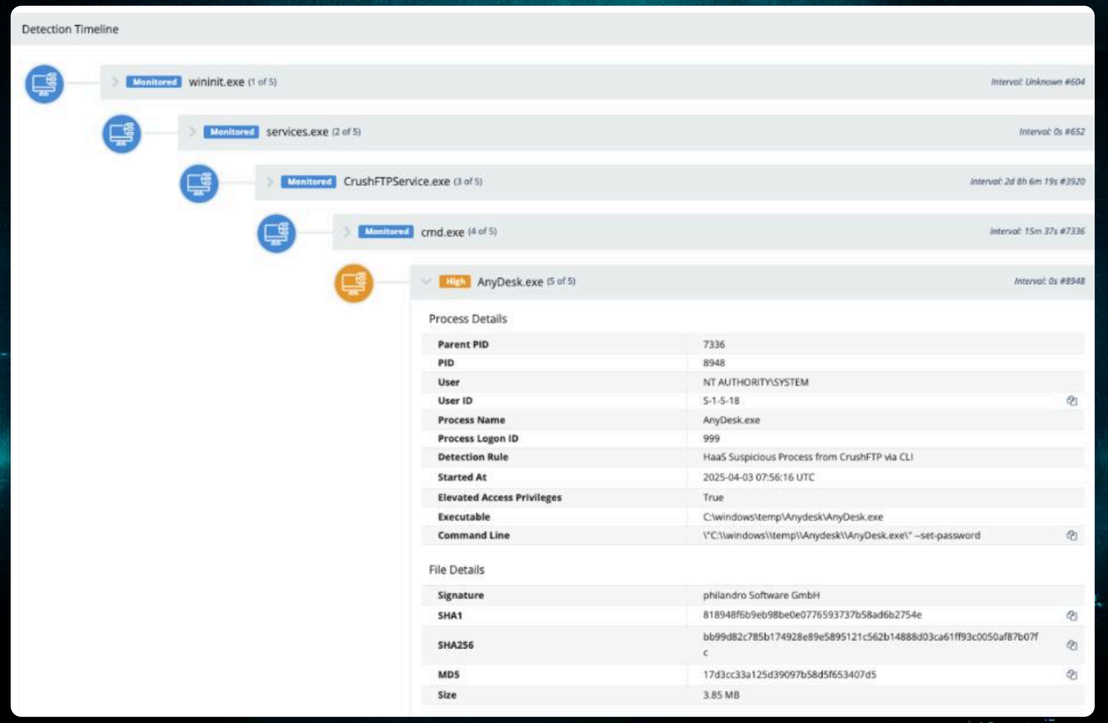


Figure 30: AnyDesk process spawning from CrushFTPService.exe

Gladinet Exploitation

(CVE-2025-30406, CVE-2025-11371, CVE-2025-14611)

Gladinet had a spicy security year. We responded to multiple exploited vulnerabilities, including a critical severity flaw, in Gladinet's CentreStack and Triofox products, its enterprise file access, sharing, and content management solutions.

It started with a Rapid Response in April for CVE-2025-30406, a critical severity vulnerability stemming from a hard coded machine key, which would allow a threat actor to achieve remote code execution via a ViewState deserialization flaw.

In October, we spotted adjacent Gladinet in-the-wild exploitation, with an unauthenticated CentreStack and Triofox Local File Inclusion flaw (CVE-2025-11371). After a deep dive, we found this flaw impacted several customers and allowed threat actors to retrieve the machine key from the Web.config file to perform remote code execution via the same ViewState deserialization vulnerability in CVE-2025-30406.

In December, the security community uncovered another round of Gladinet exploitation. This time, it was linked to CI0p ransomware gang and tracked under CVE-2025-14611. Because the AES implementation in Gladinet's CentreStack and Triofox products has hardcoded cryptographic keys, threat actors could potentially abuse this to access the web.config file, opening the door for deserialization and remote code execution.



Figure 31: Screenshot of CISA's Notification of CVE-2025-30406

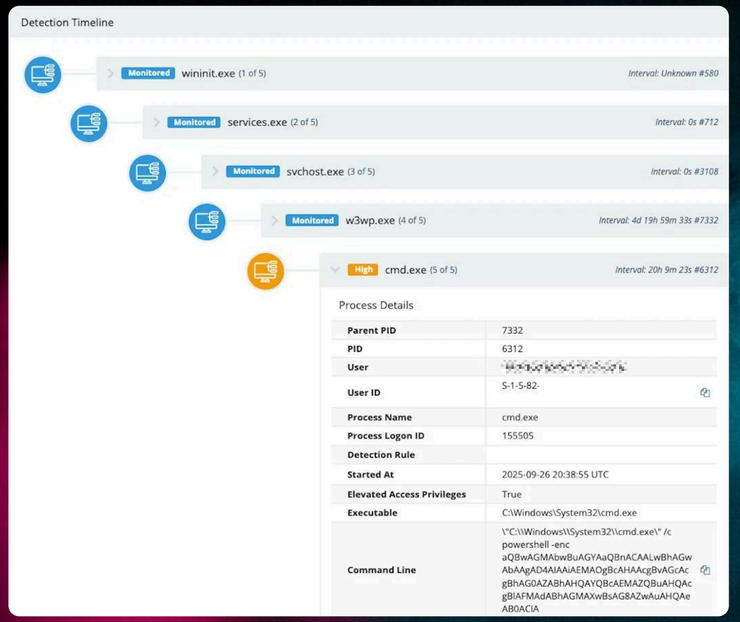


Figure 32: Detection timeline for observed exploitation of CVE-2025-30406

React2Shell Exploitation

(CVE-2025-55182)

In December, a threat advisory was released for another deserialization flaw with five words nobody wants to hear: critical unauthenticated remote code vulnerability. This exploit, dubbed React2Shell, abused React Server Components' processing of the React Flight protocol. Threat actors broadly targeted CVE-2025-55182 due to its widespread nature (the components are used in React.js, Next.js, and more) and the ease of exploitation. CVE-2025-55182 is caused by insecure deserialization of React Server Components' payload logic, and can be exploited with an unauthenticated attacker and one HTTP request.

During these incidents, we saw attackers move fast from initial access to post-exploitation payloads, including cryptominers, a Linux backdoor called 'PeerBlight', a reverse-proxy tunneling tool nicknamed CowTunnel, and a Go-based implant dubbed ZinFoq. We also watched a Kaiji botnet variant get dropped.

Feature	Primary Role	Key Activity
SPivoting	`socket_quick_start`	Starts a SOCKS5 proxy to move laterally through the network.
Stealth	`change_file_time`	Timestomping — Modifies timestamps (defaults to 2016-01-15) to evade forensic detection.
Execution	`interactive_shell`	Spawns a reverse PTY bash shell and immediately wipes the command history.
Exfiltration	`explorer_download`	Reads, hex-encodes, and exfiltrates files to the attacker's C2.

Figure 33: Post-exploitation stage of React2Shell attack path



Figure 34: Example of React2Shell exploitation

Veeam Backup Exploitation

(CVE-2025-48983)

Exploitation of Veeam backup servers didn't skip a beat in 2025, with attacks on the Mount Service (CVE-2025-48983), the SVC_VEEAM service account, and the Veeam database components that interface with backup systems. This malicious activity happened after attackers gained access to internal networks, suggesting that patching and hardening of these systems is still a tricky issue.

Attackers targeted the Mount Service for elevated privileges to disable defenses, get access to backup jobs, access mounted backup content, and extract files for credential access. Attackers also targeted the SVC_VEEAM account, taking advantage of the account's elevated privileges, or creating accounts disguised as this account to blend in with normal service operations. They would then give this account RDP access to move laterally under the guise of the legitimate backup system.

Most of this activity happened after attackers exploited the local VeeamBackup SQL database, which stores service credentials. The most common command execution was via the sqlcmd or similar SQL database clients.

```
""$DBProduct = (Get-ItemProperty -Path \"HKLM:\\SOFTWARE\\Veeam\\Veeam Backup and
Replication\\DatabaseConfigurations\").SqlActiveConfiguration

# Add EncryptionSalt value from registry HKLM\\SOFTWARE\\Veeam\\Veeam Backup and Replication\\Data

$saltbase = (Get-ItemProperty -Path \"HKLM:\\SOFTWARE\\Veeam\\Veeam Backup and
Replication\\Data\").EncryptionSalt
if ($DBProduct -eq \"Mssql\")
{
    #Get SQL configuration
    $SQLConfiguration = Get-ItemProperty -Path \"HKLM:\\SOFTWARE\\Veeam\\Veeam Backup and
Replication\\DatabaseConfigurations\\MsSql\"
    $SQLServer        = $SQLConfiguration.SqlServerName
    $SQLInstance      = $SQLConfiguration.SqlInstanceName
    $SQLDB            = $SQLConfiguration.SqlDatabaseName
    $SQLConnection    = $SQLServer + \"\\\" + $SQLInstance
    $sqlquery=\"SELECT user_name,password from dbo.Credentials\"
    $Connection                 = New-Object System.Data.SQLClient.SQLConnection
    $Connection.ConnectionString = \"server='$SQLConnection';database='$SQLDB';trusted_connection=false;
integrated security='true'\"
    $Connection.Open()
    $command                    = $Connection.CreateCommand()
    $command.CommandText        = $sqlquery
    $Datatable                  = New-Object \"System.Data.Datatable\"
    $result                     = $command.ExecuteReader()
    $Datatable.Load($result)
    $Result=$Datatable
}
```

Figure 35: PowerShell script exploiting Veeam Backup and Replication Service

C:\Windows\system32\net1 localgroup "Remote Desktop Users" /add	net.exe	cmd.exe
net localgroup "Remote Desktop Users" /add	cmd.exe	Veeam.Backup.MountService.exe
C:\Windows\system32\net1 localgroup Administrators /add	net.exe	cmd.exe
net localgroup Administrators /add	cmd.exe	Veeam.Backup.MountService.exe

Figure 36: Suspicious parent process of Veeam.Backup.MountService.exe



Defense Evasion

Driver Abuse and EDR Tampering in 2025

Attackers began acting earlier in the attack chain and deliberately targeting endpoint visibility. They increasingly sought kernel-level control to improve their chances of success, particularly in ransomware and multi-stage campaigns. Instead of relying only on user-mode evasion or short-lived process termination, adversaries invested in techniques for persistent, system-wide control over security tools.

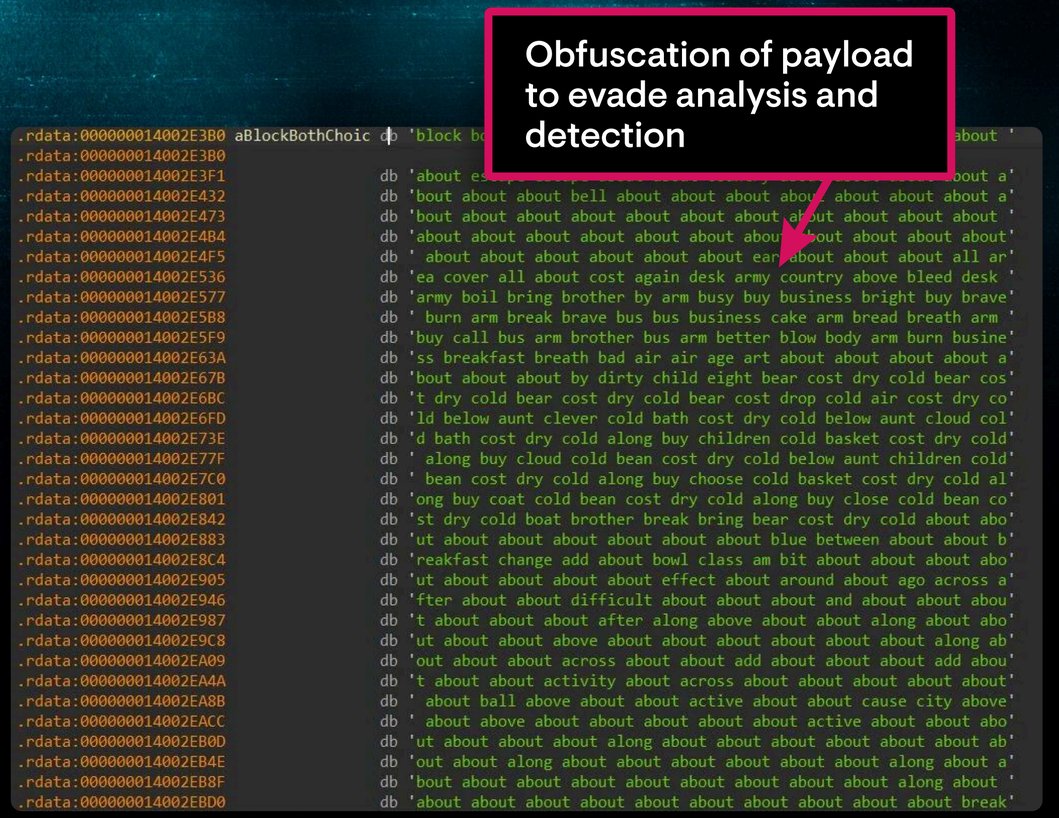


Figure 37: Wordlist-encoded BYOVD payload

Bring Your Own Vulnerable Driver (BYOVD)

In 2025, BYOVD techniques were a reliable and repeatable method for attackers to gain privileged Ring 0 execution without exploiting zero day kernel vulnerabilities. Instead of chasing novel kernel exploits, malware operators favored a stable inventory of well-documented, signed but vulnerable drivers that provide predictable input/output control (IOCTL) abuse paths.

Drivers like `Throttlestop`, `SSPort`, Dell's `DBUtilDrv2`, `RTCore64`, `Asus AsIO series`, and `WinRing0` appeared across unrelated incidents, reinforcing that attackers keep curated "driver toolkits" to reuse across campaigns. The presence of ransomware-linked vulnerable driver telemetry, especially `inpoutx64.sys` and `gdrv.sys`, further shows that these drivers are commonly used during pre-encryption staging workflows, not just for post-exploitation persistence.

Over time, the execution flow became consistent:

1. Establish execution via initial access or lateral movement
2. Load or map a vulnerable driver using a kernel loader
3. Leverage kernel primitives to squash defenses or stabilize access

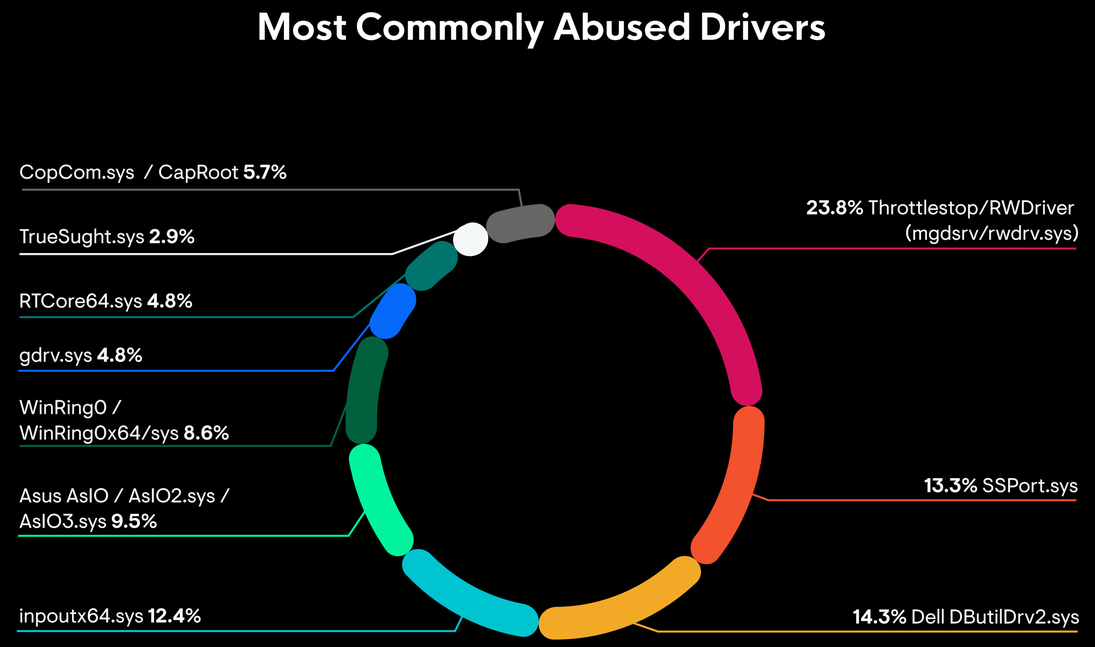


Figure 38: Most commonly abused drivers in 2025

Kernel Loader Tooling and Signature Enforcement Bypass

Kernel loader utilities like driver mappers were popular in attacker toolkits. These tools let attackers load unsigned or modified drivers without directly exploiting kernel vulnerabilities, often by temporarily weakening code integrity through boot configuration changes.

The recurring combo of kernel loader usage, explicit kernel service creation, and code integrity enforcement modification means attackers are designing workflows that assume driver loading may initially fail, and include fallback paths to ensure kernel code execution regardless of system posture. This layered approach mirrors the redundancy seen in lateral movement tooling and shows a mature understanding of modern Windows protections.

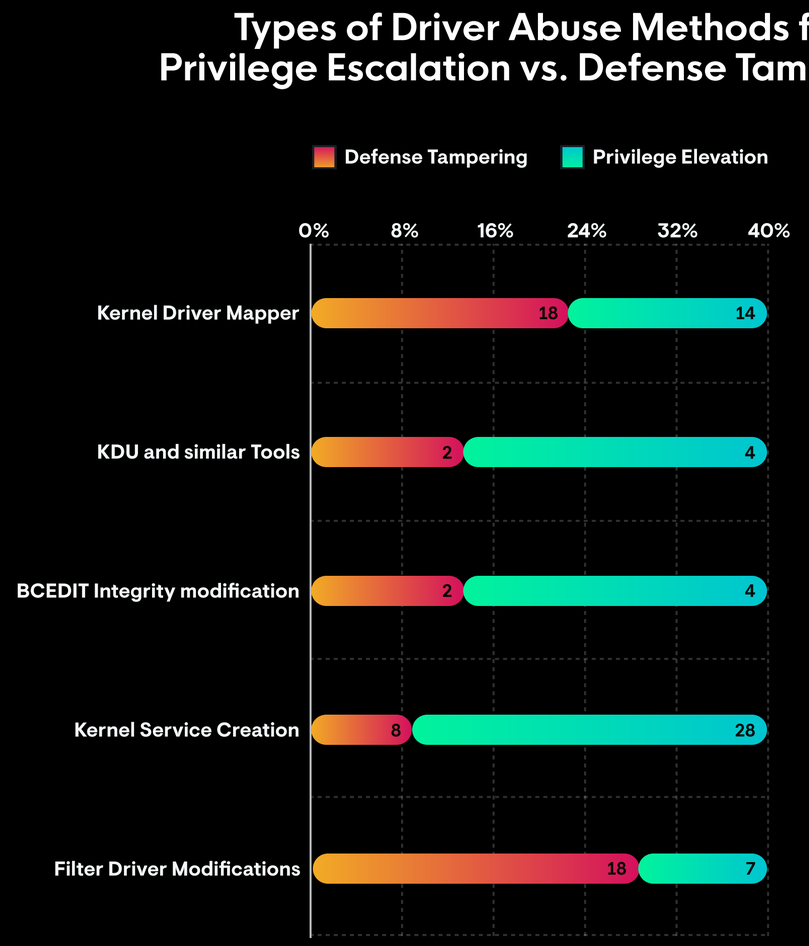


Figure 39: Distribution of driver abuse methods used for privilege escalation vs. defense tampering

Driver-Enabled Credential and Privilege Consolidation

Driver-assisted credential and privilege access was a persistent attacker strategy throughout 2025. The continued appearance of Mimikatz's `mimidrv.sys` highlights a reliance on kernel components to bypass user-mode protections around credentials and protected processes. This approach acts as a force multiplier, letting attackers extract credentials shielded by the OS, access memory protected by Protected Process Light (PPL), and expand privileges before disabling security controls.

Attackers applied these techniques in different ways. Some tried to load kernel components early to keep full control over the environment, while others delayed kernel access until later stages of an intrusion. In several cases, attackers were convinced that failure to gain kernel access would often lead to their discovery, and decided to only try it as a last resort.

Another notable trend was more use of filter driver manipulation to suppress security visibility at the kernel level. Unloading monitoring filter drivers represents a decisive escalation beyond user-mode tampering, as it removes telemetry at the source, rather than racing against agent self-defense logic.

This technique popped up right before:

22%
Lateral movement bursts

31%
Payload staging

39%
Ransomware execution windows

Its use means attackers know that disabling configuration settings alone isn't enough in environments with layered monitoring. Filter driver tampering offers a more durable suppression mechanism and reflects growing attacker confidence operating in kernel space.

Escalation to Service and Process Termination

When configuration-level tampering wasn't enough or was blocked, attackers escalated to direct service and process termination. This pattern underscores attacker adaptability and highlights that EDR resistance is treated as an obstacle to be iteratively overcome and not a single control to bypass.

Kernel-level suppression consistently represented the final and most effective stage of this progression.



Figure 40: Example of KillProc implementation

Microsoft Defender Degradation as a Repeatable Workflow

Attackers didn't just shut down Defender last year—they quietly weakened it. By tweaking settings, they lowered detection rates while keeping the service running. This keeps the lights on but the alarms off, so cybercriminals can lurk in your system unnoticed.

Based on activity we saw, Defender tampering wasn't a single action, but a multi-stage process repeated across hosts within the same intrusion.

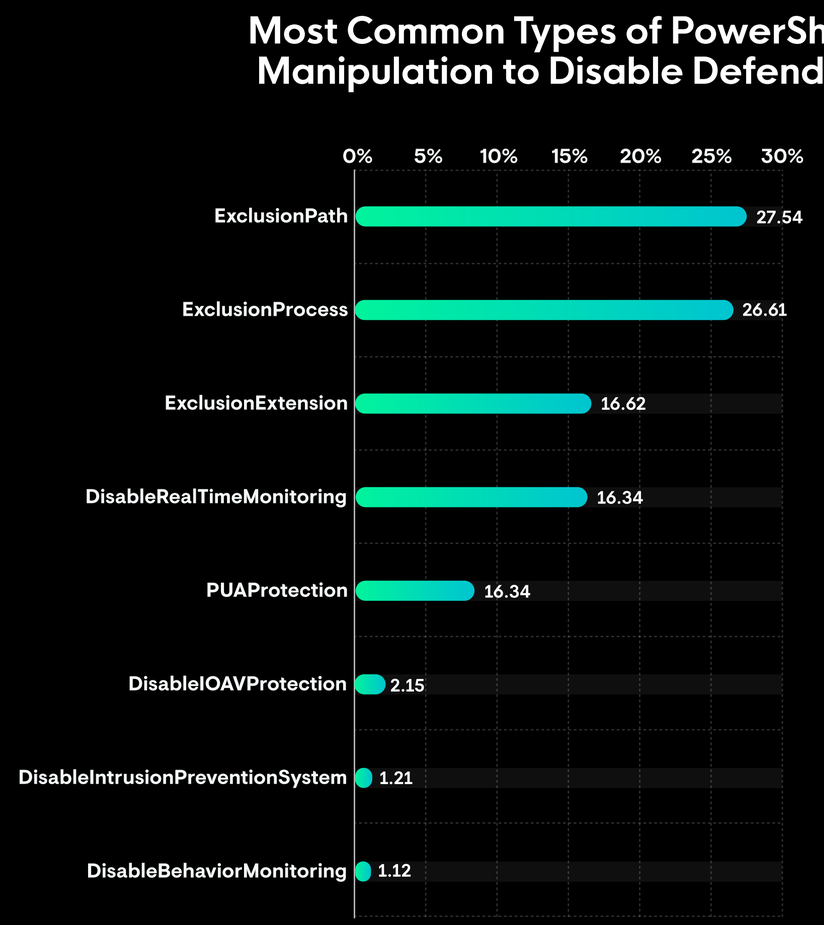


Figure 41: Most common types of PowerShell manipulation attackers used to tamper with or disable Microsoft Defender

PowerShell-Based Manipulation

PowerShell-based manipulation of Defender accounted for ~81% of all Defender-related tampering activity, making it the number-one defense evasion technique in 2025.

Attackers consistently used Defender's native management interface, enabling protection changes without exploiting vulnerabilities and often without triggering tamper-protection safeguards. This reflects a preference for legitimate administrative tooling over noisy or brittle bypass techniques.

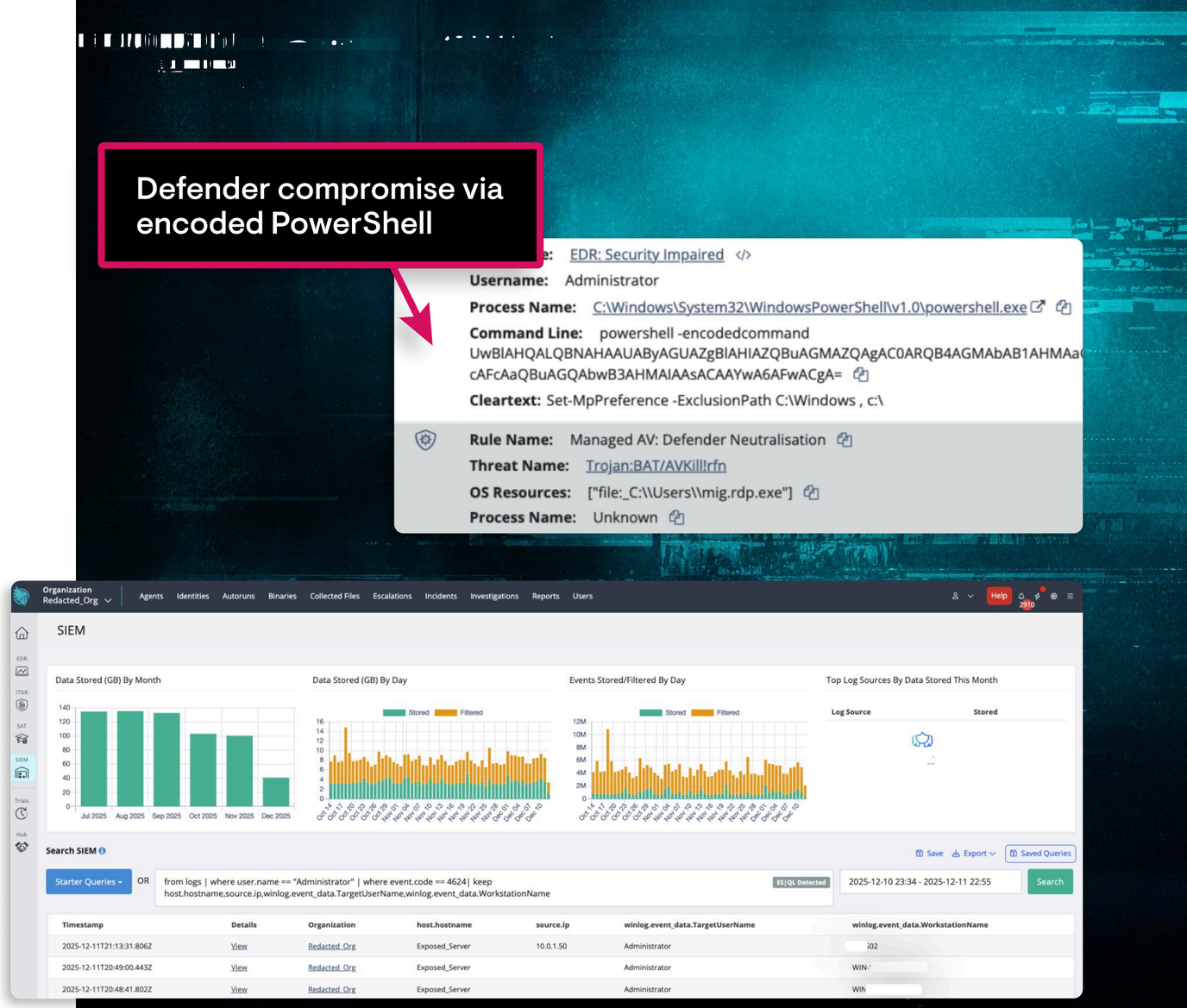


Figure 42: Security Information and Event Management (SIEM) detection events for compromised host

Real-Time Protection Tampering

Attackers usually tampered with Defender by explicitly disabling real-time protections, accounting for roughly 9% of all Defender tampering. This action was treated as a high-risk situational step and not a default move, happening after exclusions were already configured and before high-risk activity like payload deployment, encryption, or mass credential access, or once stealth was no longer a priority, signaling a shift from evasion to execution.

Registry-based policy tampering was rampant, representing about 14% of Defender tampering activity. Adversaries modified core policy and service enforcement keys to weaken real-time monitoring, behavioral protections, and IOAV scanning. In a smaller but notable subset of cases, several threat actors fully disabled cloud reporting and sample submission, suggesting deliberate attempts to reduce telemetry and detection feedback rather than fully dismantle local protections.

A smaller but operationally significant portion of Defender tampering activity involved direct command-line utilities, third-party suppression tools, and service-level control, collectively accounting for ~4.5% of all Defender degradation observed.

This included use of Defender's native CLI, purpose-built disabling scripts or tools designed to repeatedly enforce suppression, and explicit stopping or disabling of Defender-related services.

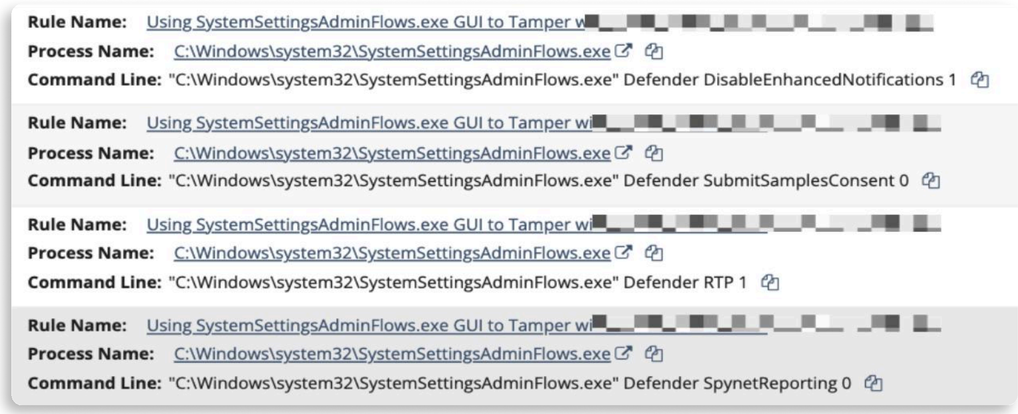


Figure 43: Commands modifying Defender security settings

Breaking Down Hacker Activity

Hands-On-Keyboard (HOK) and Evasive Activity

Let's unpack attacker behaviors that highlight direct human interaction during different stages of the attack path. We're talking about things like network reconnaissance commands, manual command execution, or lateral movement, not fully automated tools or scripts. Tracking hands-on-keyboard (HOK) activity shapes defenses by revealing operational timeframes and default attacker behaviors and strategies across attack phases. It also gives us an inside perspective on how threat actors respond to roadblocks, whether that's failed execution events or unexpected security defenses.

Our findings reinforce that most intrusions move beyond automation into active human control. This drives actionable insights for detection timing, response prioritization, and dwell time reduction.

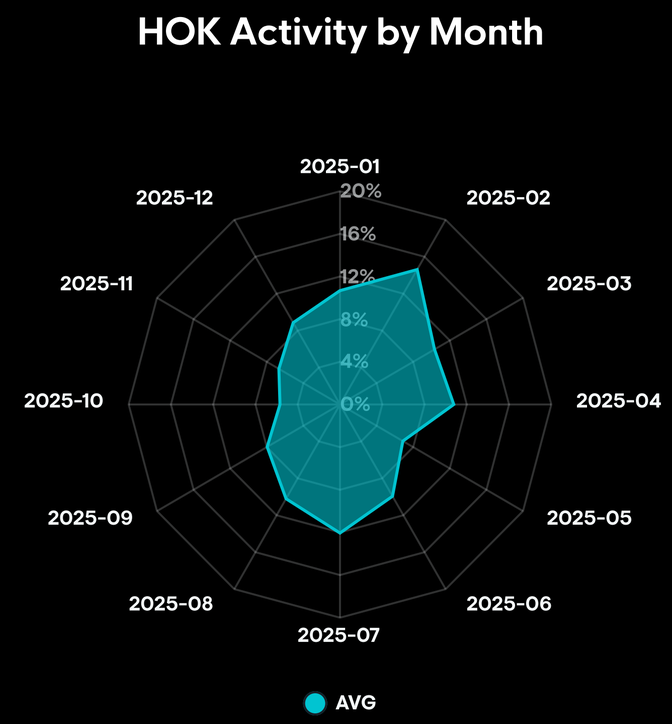


Figure 44: HOK activity by month

Operational Timeframes

Mapping HOK activity by hour within a 24-hour period shows clear activity clusters within late-day and early-evening UTC windows, with peak activity between 15:00 and 19:00 UTC. These windows align with reduced security staffing in many regions, while still overlapping with standard business hours in North America. These also correlate to heightened obfuscation activity, when attackers alter scripts or commands to hide malware or their HOK activities from detection.

Compared to automated execution, interactive activity demonstrates tighter hourly clustering and longer session durations. Manual reconnaissance, obfuscated command attempts, and defense tampering disproportionately happen within these windows, indicating active operator oversight rather than scheduled or scripted execution.

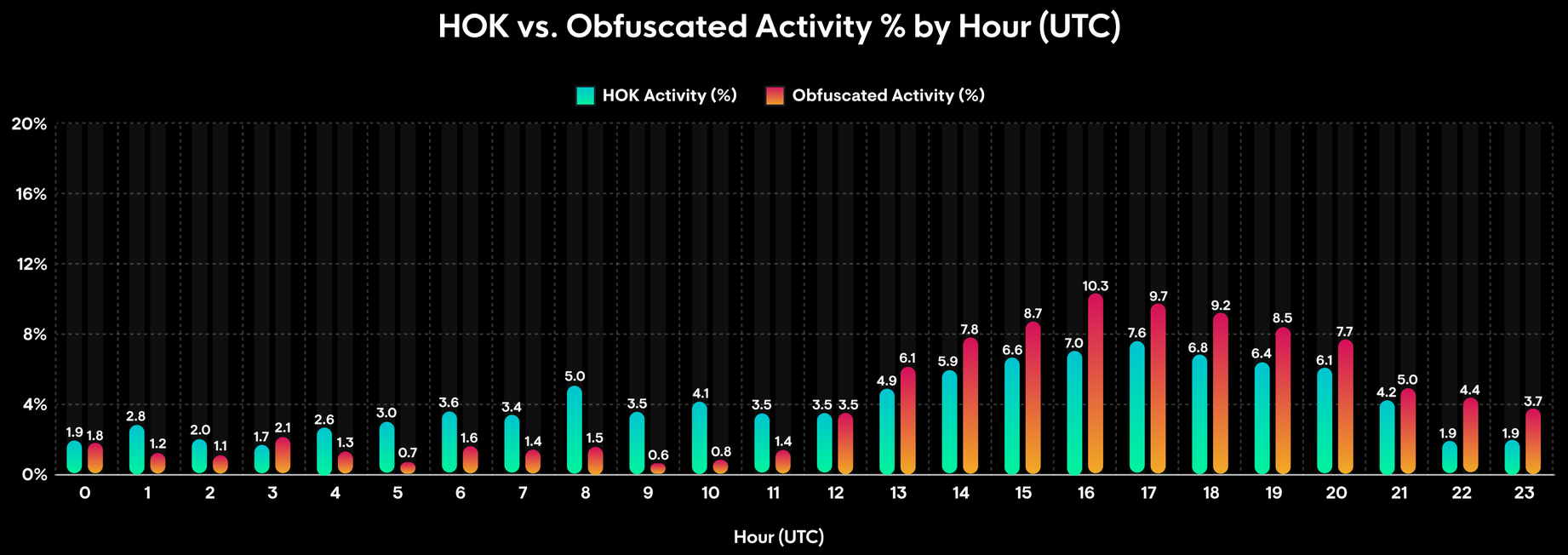


Figure 45: Percentages of HOK vs. obfuscated activity by hour (UTC)

HOK Activity Breakdown

Reconnaissance (26.1%), lateral movement (23.8%), and manual tool execution (19.8%) topped the list of HOK activity in 2025.

Over the last year, we spotted multiple manual reconnaissance sequences where attackers executed three or more distinct actions in a short timeframe. These sequences can include identity validation, domain enumeration, network discovery, and privilege assessment. Threat actors extensively used low-frequency, environment-specific commands, with direct references to local domains, user contexts, network paths, and service names that reflected situational awareness of the target environment.

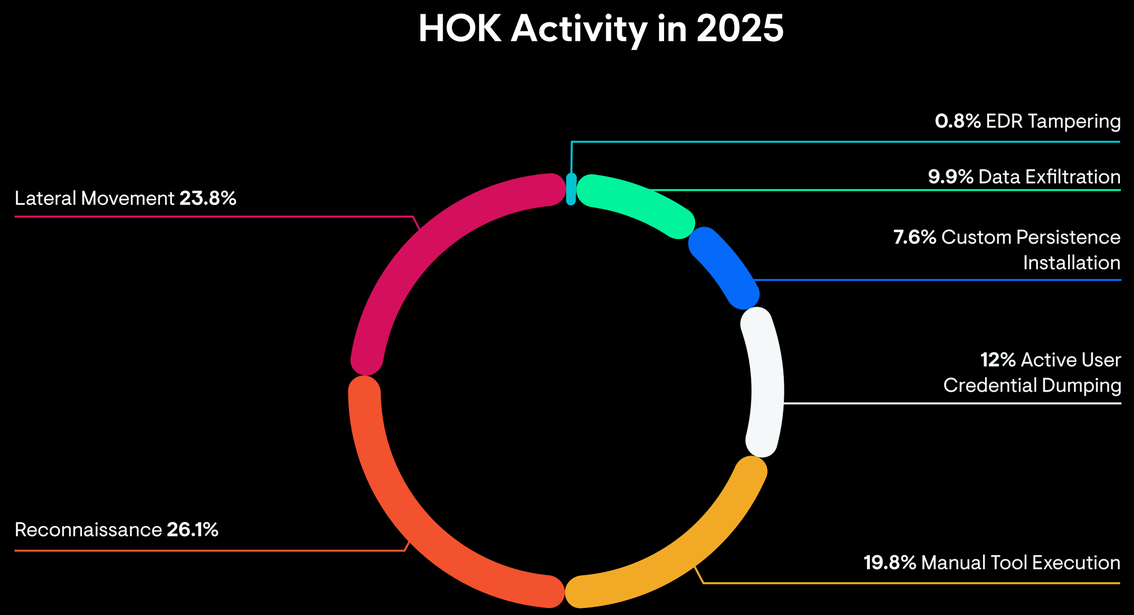


Figure 46: Type of HOK activity

Interaction Type Breakdown by Month

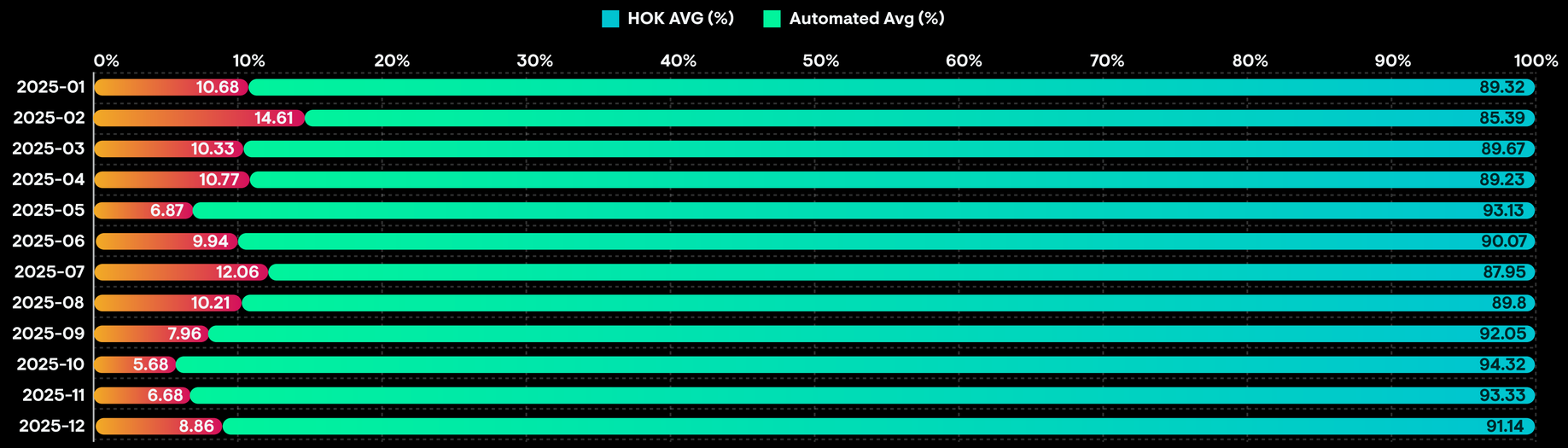


Figure 47: HOK vs. automated activity in 2025

User-driven execution surged this year, especially ClickFix, leading us to dig into the associated HOK data. Following the success of ClickFix attacks, we noticed a measurable rate of follow-on HOK activity shortly after successful fake CAPTCHA scams. In these cases, initial user execution was followed by interactive command execution, obfuscation attempts, or reconnaissance. Analyzing HOK activity post-infection, we saw that roughly 7% of ClickFix attacks leads to HOK activity within two hours.

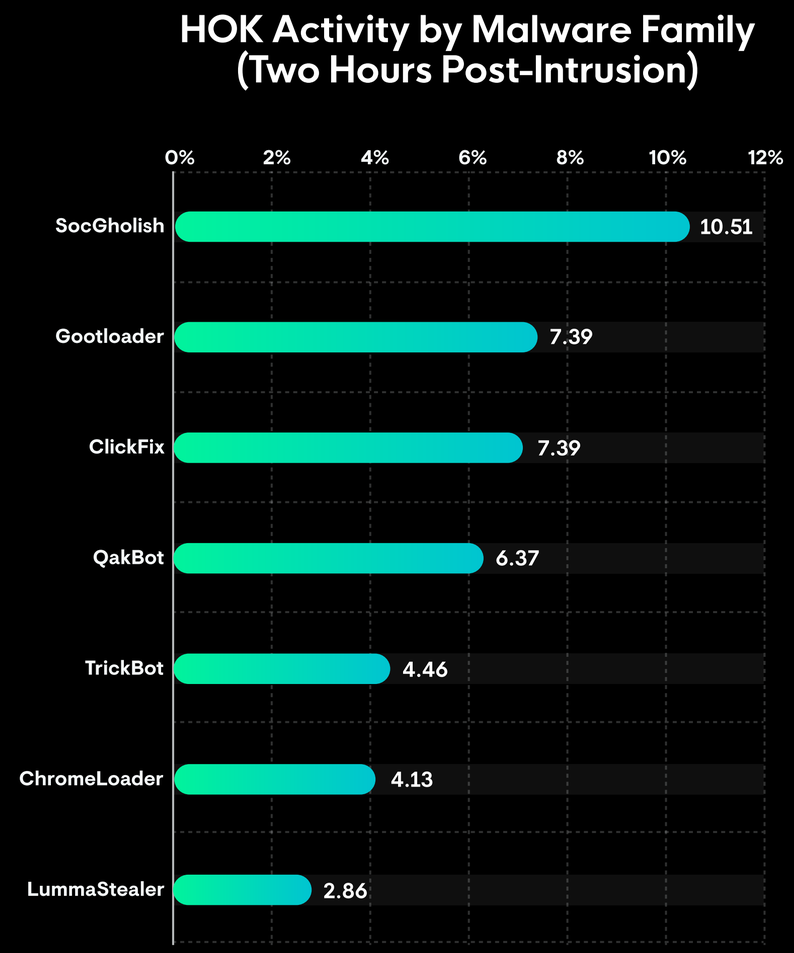


Figure 48: Percentages of follow-on HOK activity by malware family two hours post-intrusion

HOK Obfuscation Techniques

Threat actors use obfuscation to hide their tracks and confuse detection analysis. They often use techniques like the Invoke-Expression cmdlet or string concatenation to sneak past defenses, and if their initial attempts get blocked, these human operators react. They switch to complex methods like split keywords or delayed string resolution to evade detection.

We also see them use adaptive decoding chains. Instead of a set pattern, they shift strategies during interactive sessions. If an execution fails, they refine their approach with trickier, indirect commands.

Finally, watch for PowerShell activity with nested scriptblocks. These multi-layered executions vary wildly between incidents, which confirms you're dealing with a human operator manually tweaking the payload rather than a standard malware tool.

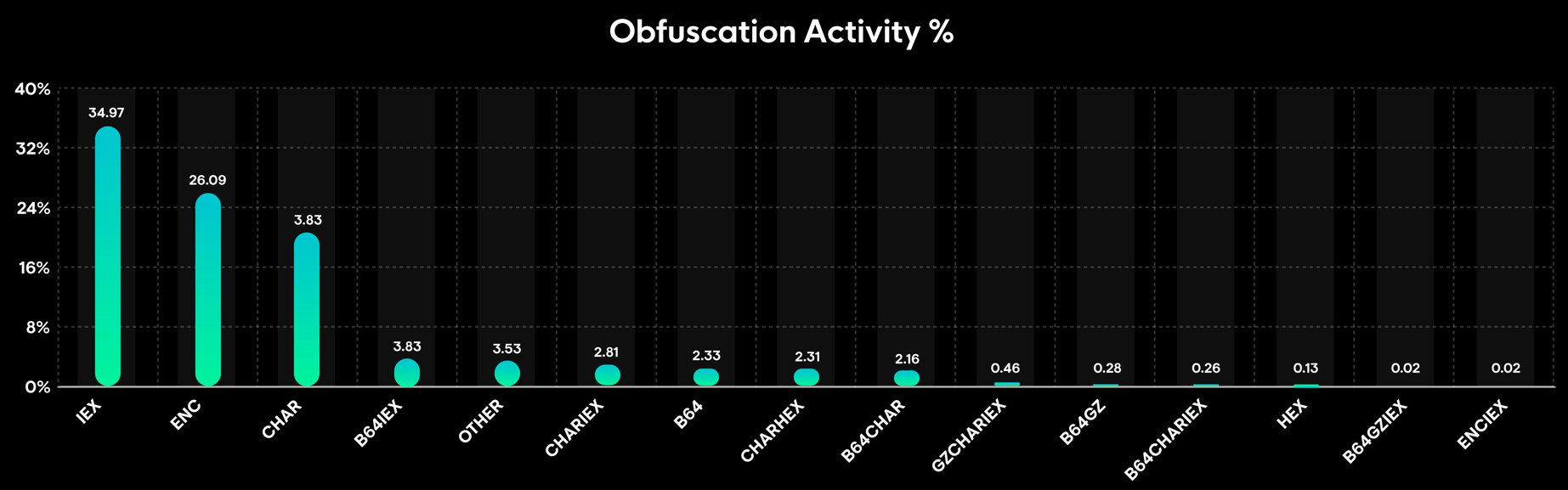


Figure 49: Types of obfuscation methods in 2025

Identity-Based Attacks

Legit Credentials. Malicious Users.



Identity threats were everywhere in 2025. While organizations have spent years hardening devices and securing network perimeters, attackers have shifted their focus to the path of least resistance: the user. Threat actors don't just get unauthorized access to victims' accounts anymore—they're using infostealers, rogue apps, and shadow workflows (malicious rules attackers use to hide activity by auto-forwarding or deleting messages) to expand their reach into your business.

Compromising an identity lets threat actors bypass traditional defenses by logging in with valid user credentials. Attackers weaponize these identities to quietly work in your environment, turning a single compromised user into a launchpad for major operations like ransomware and BEC attacks.

Identity-based threat activity in 2025 reflected a continued shift away from isolated authentication abuse toward structured, goal-driven intrusion chains. Attackers treated identity as the primary attack vector, using access anomalies, phishing-as-a-service platforms, session hijacking, OAuth abuse, and mailbox manipulation as interconnected steps, rather than independent tactics.

This past year, we also saw threat actors respond more confidently to security measures like MFA, by launching AiTM attacks or abusing legitimate authentication workflows.

While identity alert volume fluctuated throughout the year, the underlying tradecraft showed consistency, suggesting a smaller number of mature campaigns rather than broad, opportunistic abuse.

We saw a sharp increase in identity threat activity in February, with daily event volume rising noticeably in the middle of the month. This surge coincided with the public disclosure of CVE-2025-0108 on February 12, an authentication bypass in the management web interface of Palo Alto Networks PAN-OS software. The timing aligns with increased malicious OAuth abuse, anomalous session behavior, and post-authentication activity spotted across multiple organizations, peaking on February 14th. These give strong evidence that threat actors focused on campaign deployment, accelerated access, and prioritized exploitation activity during that week.

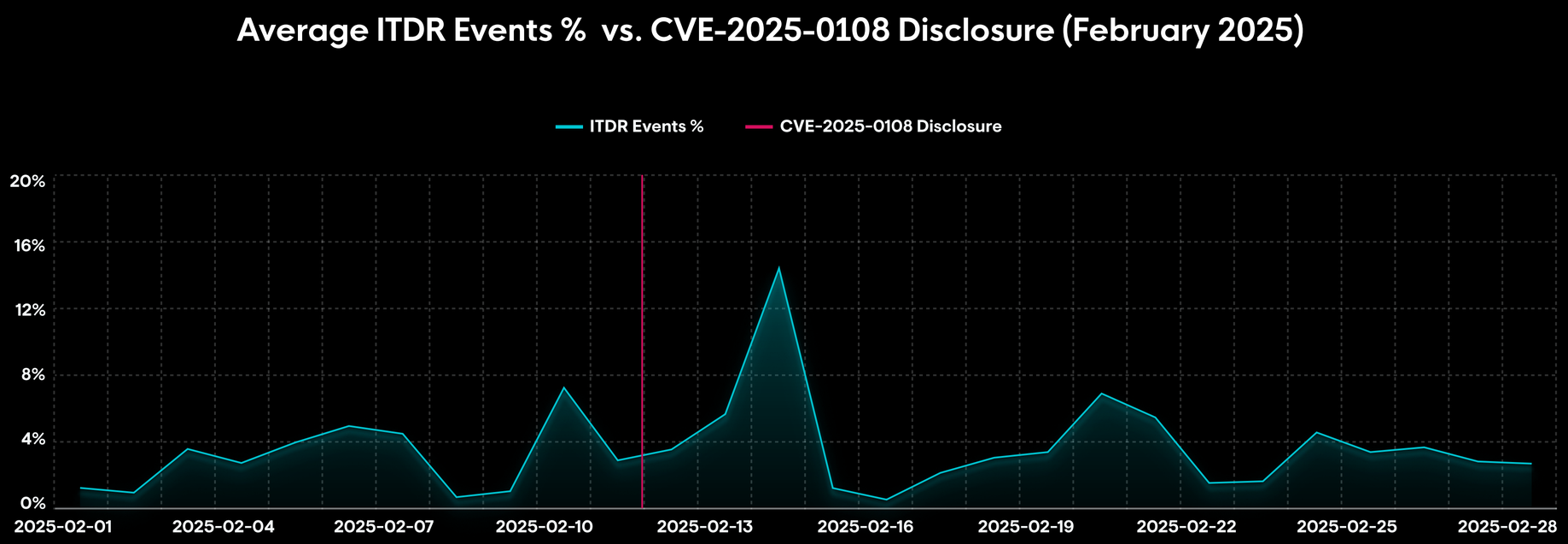


Figure 50: Average ITDR events in February 2025 compared to spike related to CVE-2025-0108 disclosure date

Shady Logins

Threat actors continued to exploit Microsoft 365 environments, but in 2025, we saw attackers get better at breaking in quietly and staying there.

Access policy and trust boundary violations (37.2%) emerged as a top attack category for ITDR. This means attackers are trying to log in from suspicious places—like unauthorized countries or known bad networks—often using stolen credentials bought from the dark web. In fact, these types of shady login attempts made up over a third of all detections this year.

This can also be a signal that attackers hide behind legitimate VPN services. Throughout 2025, we saw cybercriminals use VPNs and proxies to mask their malicious activities and behaviors. A small group of consumer VPN services—specifically NordVPN, ExpressVPN, TunnelBear, SurfEasy, and ProtonVPN—accounted for most of this activity, while a long tail of providers supported short-term, opportunistic access attempts.

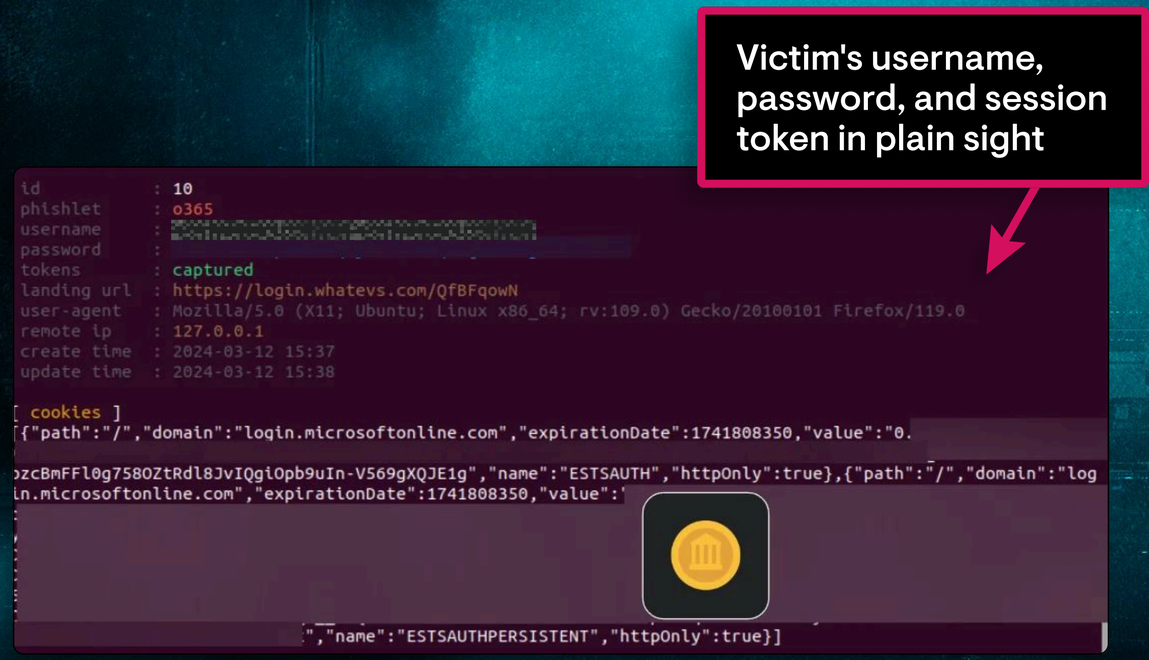


Figure 51: An example of an AiTM attack with Evilginx

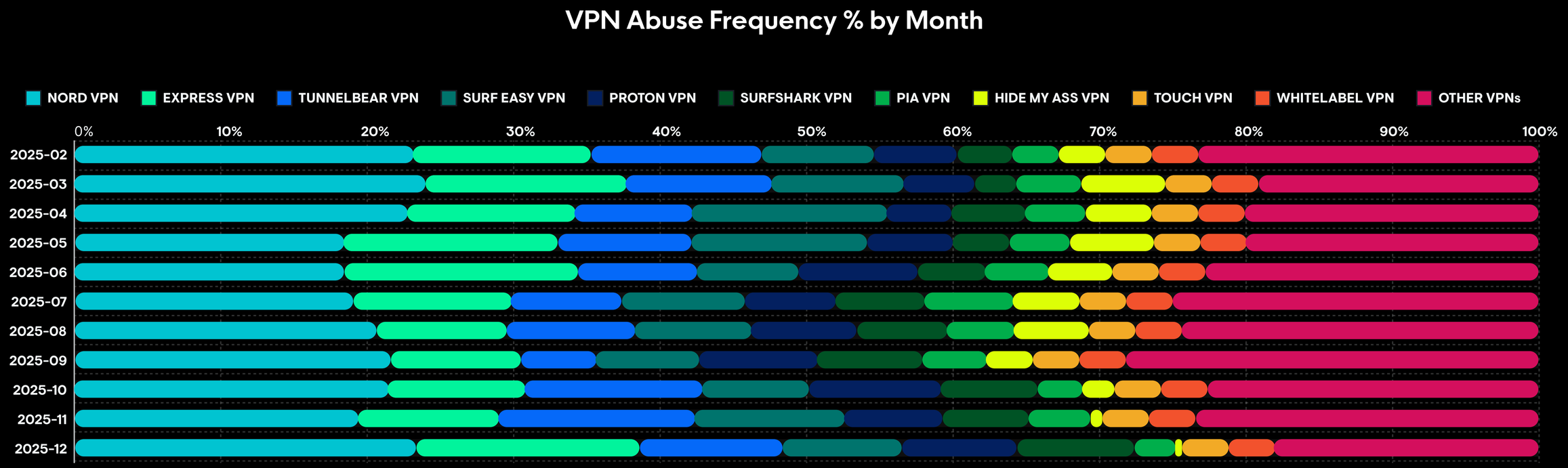


Figure 52: VPN abuse in 2025

NordVPN was the most consistently abused provider, accounting for 18–24% of tunnel-related activity in any given month, and averaging just over 21% across the year. Its steady use in 2025 suggests repeated reuse rather than opportunistic testing, especially during months that also showed higher post-authentication behavior. ExpressVPN followed a similar pattern, averaging roughly 12% of monthly activity, with noticeable increases during several campaign windows, including late Q2 and early Q4.

Other providers showed more fleeting behavior. TunnelBear and SurfEasy each showed sharp, short-lived spikes, often exceeding 10% of monthly tunnel usage during specific periods, followed by fast decline. These bursts aligned closely with access-stage activity and didn't always come before mailbox manipulation or OAuth persistence, indicating likely use during credential validation or access brokerage rather than sustained intrusion operations. ProtonVPN had moderate but recurring usage, ranging between five to nine percent and suggesting a hybrid role spanning both exploratory and follow-on activity.

In our month-over-month analysis of malicious VPN activity, we spotted these operational patterns:

- Initial access phases: Attackers deliberately rotated providers across multiple VPN services to minimize detection
- Persistence or BEC: Attackers returned to the same VPN providers across multiple weeks or months, signaling operational success against tenant-specific controls

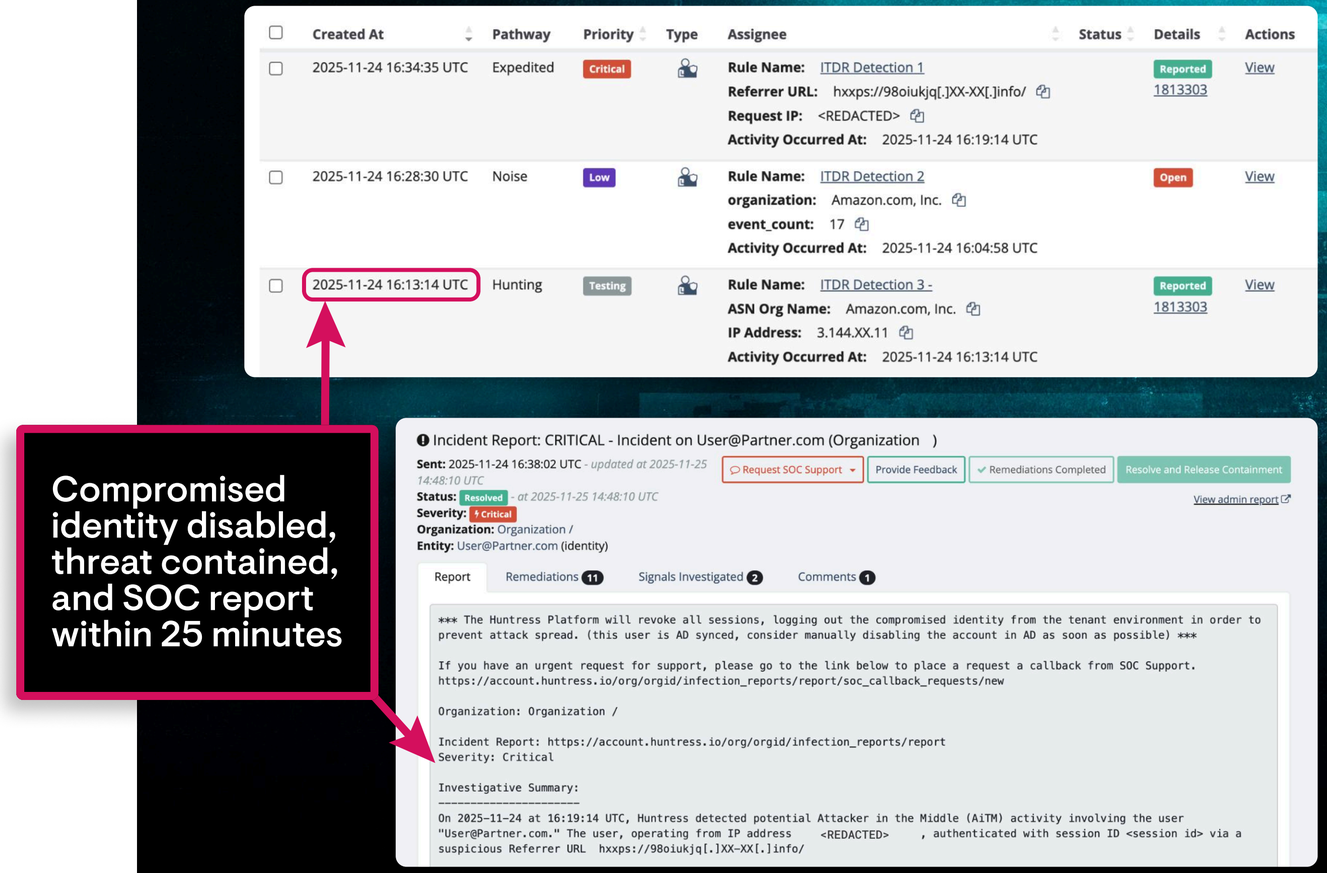


Figure 53: ITDR telemetry revealing adversary abuse of legitimate hosting environments

Malicious Identity Activity by Month

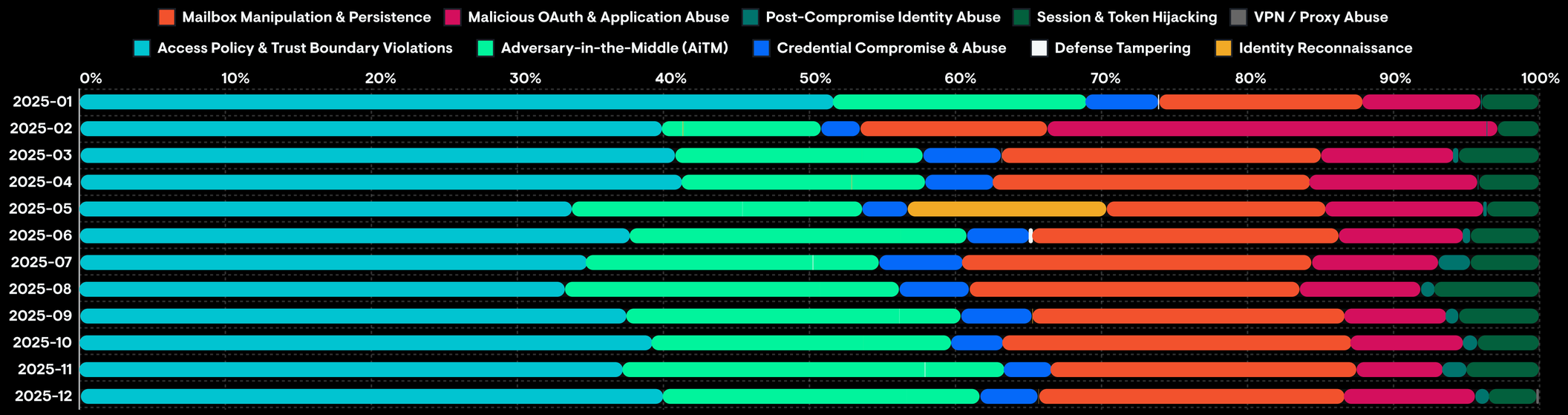


Figure 54: Malicious identity activity breakdown by month in 2025

Other key identity threat trends in 2025 include:

Mailbox Manipulation and Persistence

Attackers love to hide their tracks. In about 19% of cases, they set up automated rules to hide or forward sensitive emails. This helps them stay undetected during BEC attacks or quietly steal data.

Anomalous behavior after valid logins

While the initial login might look legitimate, the subsequent session activity will have unusual characteristics.

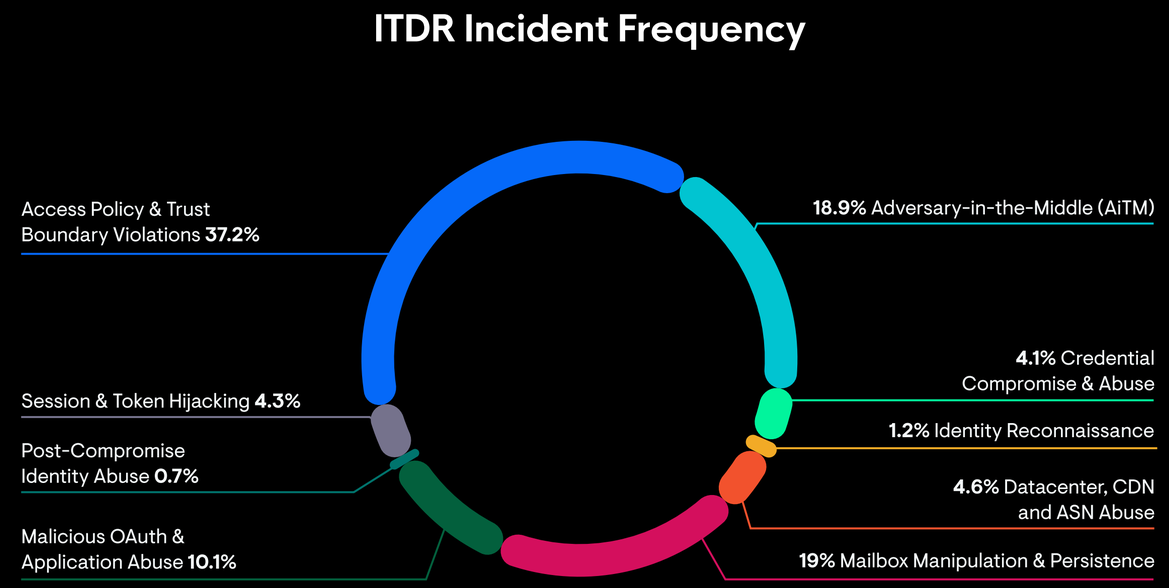
AiTM Attacks

Nearly 19% of attacks involved AiTM tools like Evilproxy or Evilginx. These tools help criminals steal credentials and bypass 2FA and MFA.

Quality Over Quantity

Attackers moved away from volume-based attacks to stealthier tactics like valid authentication abuse, session persistence, and post-authentication manipulation.

Attackers are becoming more efficient. They're turning unauthorized access into reliable footholds within your network, often validating stolen data quickly (looking over large sets of stolen data to see if there's valuable data in it) to sell it to other cybercriminals. They're running a profitable business, and this scaling of the identity theft ecosystem means organizations need to be more vigilant about monitoring post-login activity, not just the initial break-in.



Figurer 55: Identity Threat Detection and Response (ITDR) incidents in 2025

Mailbox Manipulation

Mailbox manipulation (19.0%) and persistence followed access policy and trust boundary violations, as the second most common identity threat flagged by ITDR. Cybercriminals know that obvious moves like forwarding emails immediately set off alarms, especially as precursors to BEC attacks. So, they favor subtle concealment tactics, like:

- Marking messages as read
- Deleting inbound mail
- Redirecting emails to obscure folders

We typically see external forwarding and outbound spam only after the attacker establishes a foothold. It's a deliberate choice: they stage their attacks carefully, because they know that immediate exploitation will get them busted.

Old inbox rules and hidden artifacts make it tough to spot these intruders once they take control. These techniques keep you in the dark and allow attackers to maintain access, particularly if you don't perform routine mailbox audits.

Step	PowerShell Command	Purpose
1	Connect-ExchangeOnline	Establish authenticated session
2	Get-Mailbox -ResultSize Unlimited	Retrieve all mailboxes
3	Get-InboxRule -Mailbox user@company.com -IncludeHidden	Surface all rules including hidden ones
4	Export-Csv -Path "InboxRules.csv"	Document findings for analysis

Figurer 56: How to manually uncover hidden inbox rules with PowerShell

Adversary-in-the-Middle (AiTM)

AiTM (18.9%) attacks were the third most frequent identity threat in 2025. Whether ITDR flagged sketchy session reuse or token mismatches from suspicious networks, the goal was the same for attackers: bypass MFA to access a vulnerable network.

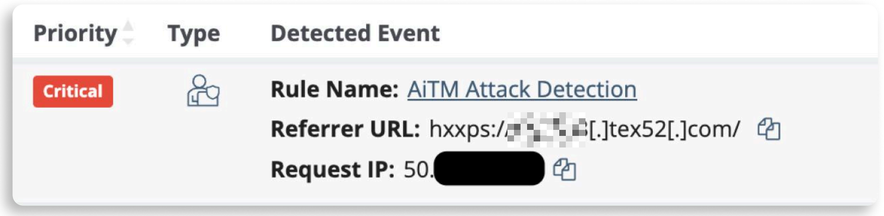
While an AiTM attack might not look like a full-blown breach, it's often just the beginning. It's the open door for criminals to steal authentication tokens and abuse OAuth, paving the way for more severe incidents.

Rather than a steady stream of background noise, these attacks hit in short, intense bursts. Think of it like a series of coordinated raids. We saw recurring technical clues—like specific login patterns and reused tools—that tell us organized groups are managing these campaigns centrally.

Our data explicitly identified multiple AiTM platforms, with EvilProxy appearing most frequently, followed by Sneaky 2FA and FlowerStorm. These platforms often used malicious subdomains and spoofed login panels, though we also saw fake document signing requests and deceptive error messages designed to trick users into giving their credentials.

AiTM activity didn't grow in a straight line this year. Instead, we saw clear ups and downs, which tells us that these events are specific campaign indicators rather than general risk signals.

In many cases, the lack of follow-up activity shows that defensive controls at the access stage are working. But don't let your guard down, because instances where attackers did succeed prove that phishing attacks designed to bypass MFA are highly effective, especially when cybercriminals strike fast.



Figurer 57: AiTM detection alert

OAuth Abuse and Malicious Application Activity

While not an ITDR frontrunner in 2025, OAuth abuse and malicious application (10.1%) activity are high impact tradecraft, up from 4.8% in 2024. Attackers use malicious web apps and sneaky consent requests to get permanent access to your accounts, all without ever changing your password.

This shift in our data shows that criminals now prefer to hide within the application layer itself. It lets them quietly raid mailboxes and data for months without setting off security alarms.

This stealthy approach is perfect for BEC attacks and corporate espionage. Even as other attack methods dropped off throughout the year, OAuth abuse was steady. It proves that if your defenses aren't configured tightly, this is a low-risk, high-reward way for attackers to slip past your controls.

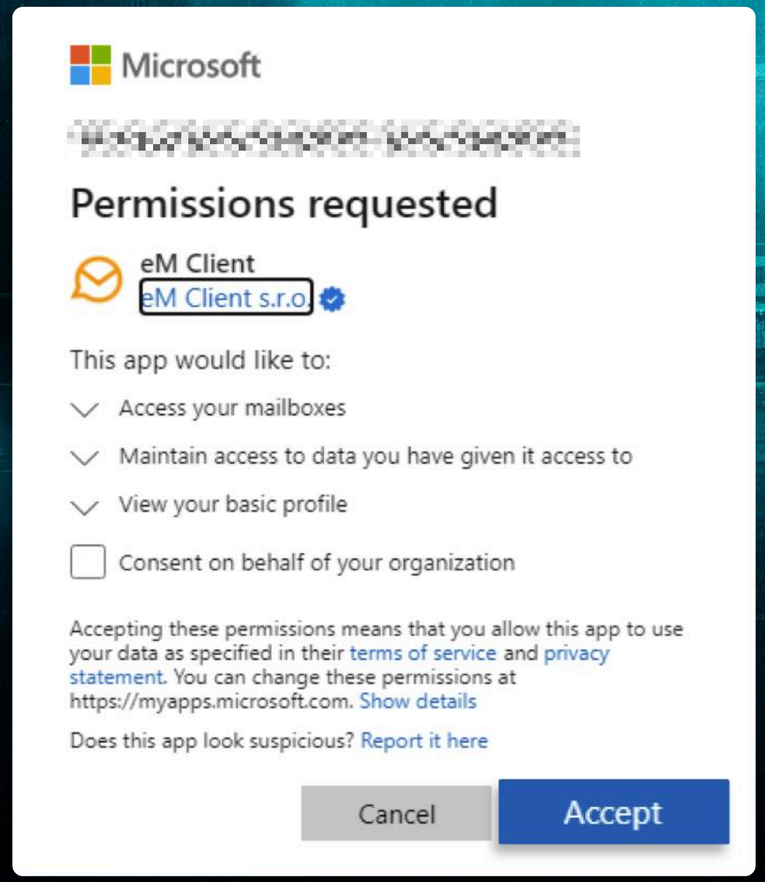


Figure 58: Attackers exploit OAuth permissions for access and persistence

Session and Token Hijacking

Token theft (4.3%) happened consistently throughout the year, but many attackers got caught because they failed to match their victims' location, browser, operating system, and tunnel characteristics.

Think of it like a burglar trying to use a stolen key, but wearing a neon sign that says "I don't live here!" These victories highlight why we need to proactively monitor for strange behavior. If successful, these techniques let adversaries bypass MFA entirely. This reduces their reliance on credentials and drastically speeds up their activity after gaining access, leading to further compromises.

In the past, attackers often compromised session tokens and waited a long time to sell them to the highest bidder to maximize profits. But now, with ITDR becoming more effective at spotting these intrusions and cutting off access, the game has changed. Would-be bidders now pay a premium for quick access to maximize their cybercrime profits before their window closes.

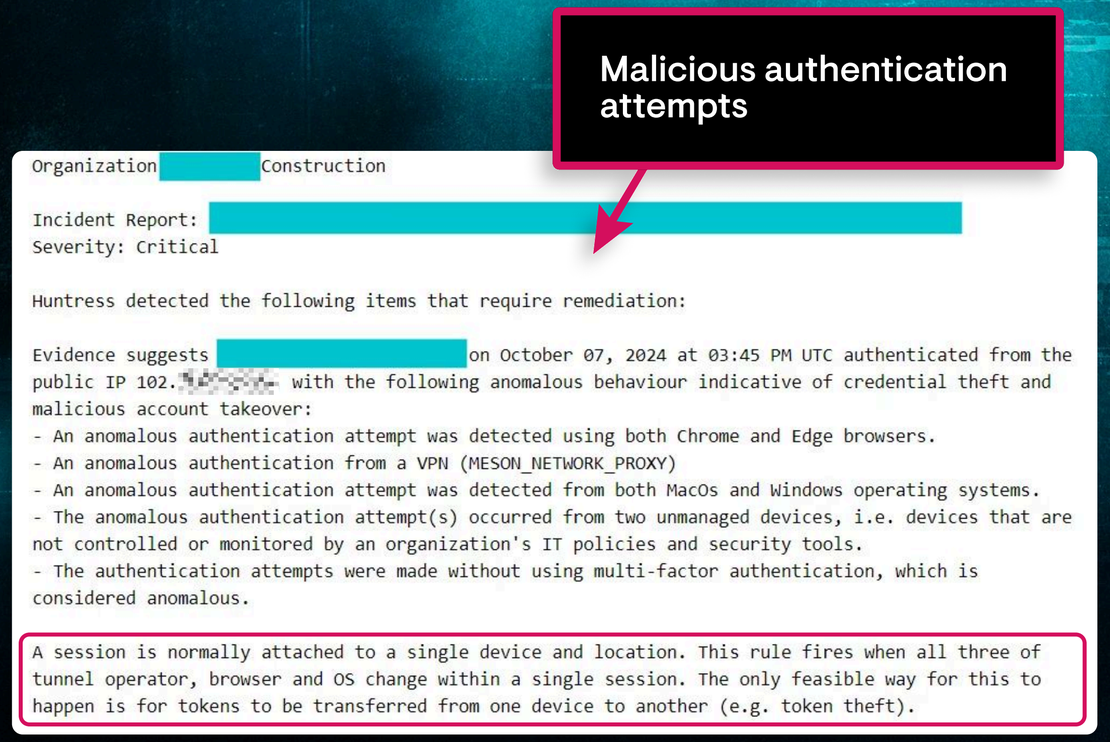


Figure 59: A Huntress report flags a session hijacking attack

BEC: Trends, Conversion, and Campaign Activity

BEC was one of the most dangerous identity threat trends of 2025. Mailbox manipulation, external forwarding, outbound spam abuse, or OAuth-based mailbox persistence was a smaller proportion of total identity telemetry compared to prior years, but showed higher confidence and tighter sequencing in 2025 leading to financial fraud. A notable spike in February aligns with the previously noted CVE-2025-0108 disclosure.

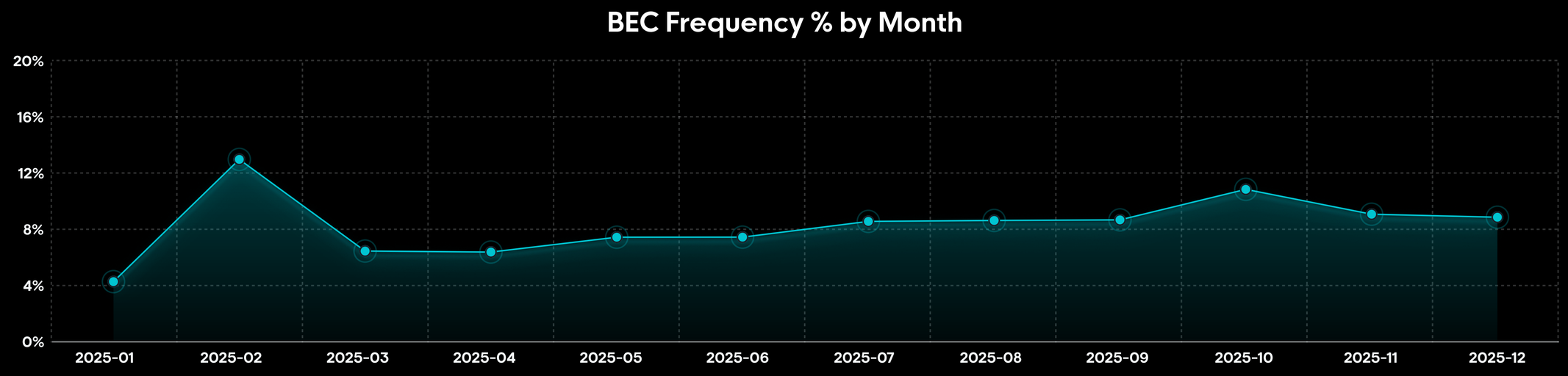


Figure 60: Frequency of BEC attacks in 2025

In our analysis of ITDR data, a BEC conversion is marked by detection of inbox rules manipulation to hide emails or suspicious outbound email activity. We analyzed two types of BEC pre-compromise activity to establish BEC conversion events:

BEC Precursors

Suspicious activities that set the stage for potential BEC attacks. Sketchy password activity, suspicious sign-in attempts, attempts to manipulate tokens/sessions, suspicious activity related to mailboxes, or identity reconnaissance methods.

BEC Enabler

Actions that give an attacker control over email or identity workflows, like session hijacking, OAuth consent abuse, and role or permission escalations.

Not every BEC red flag turns into a full-blown financial fraud email-based attack. This was evident in November in the chart below, with a spike of BEC enabler activity characterized by increased AiTM activity followed by shady credential theft (sessions/tokens/passwords). But instead of moving to sketchy mailbox activity, the attackers installed malicious apps and turned to traditional exploitation.

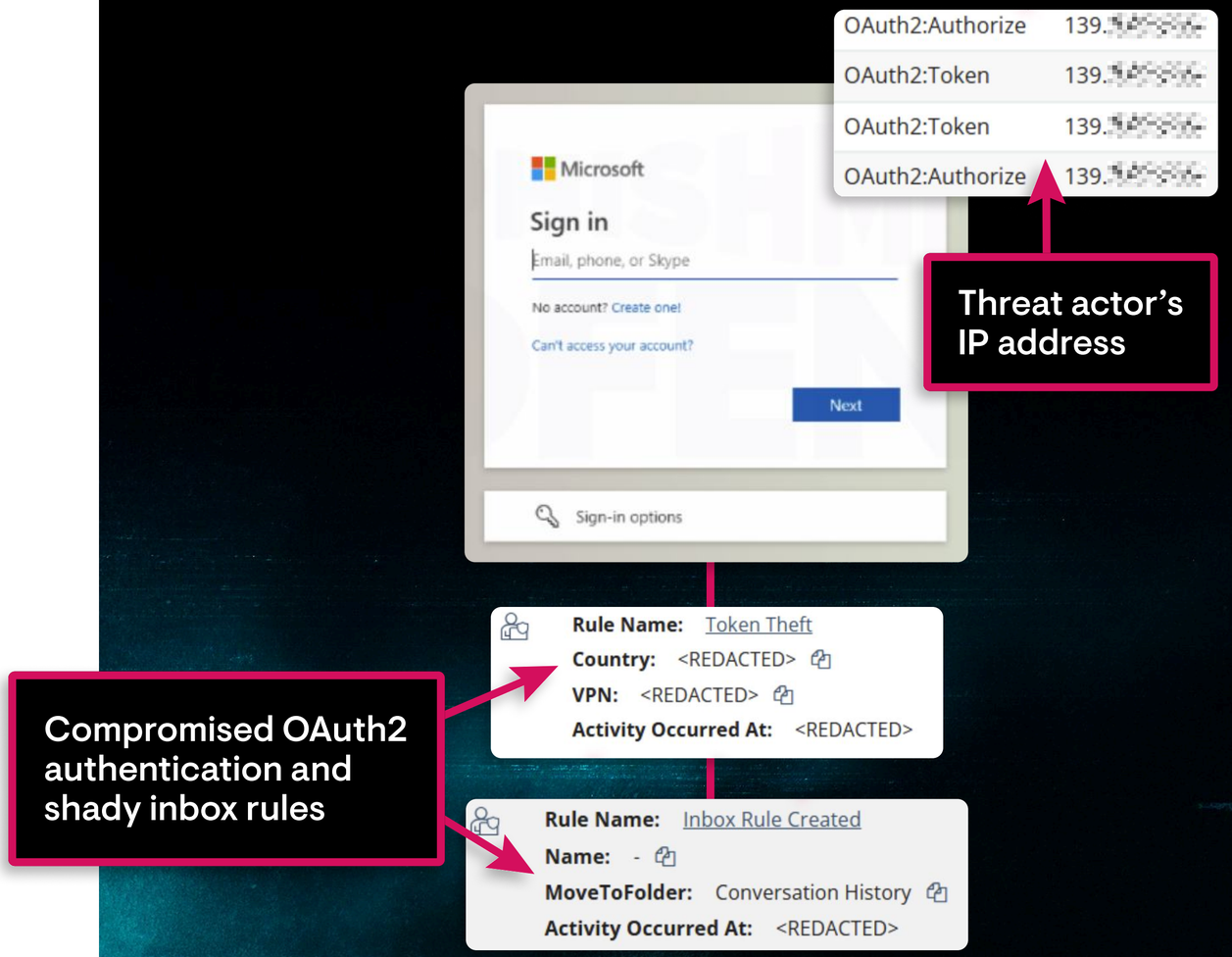


Figure 61: Example of BEC activity flagged by ITDR

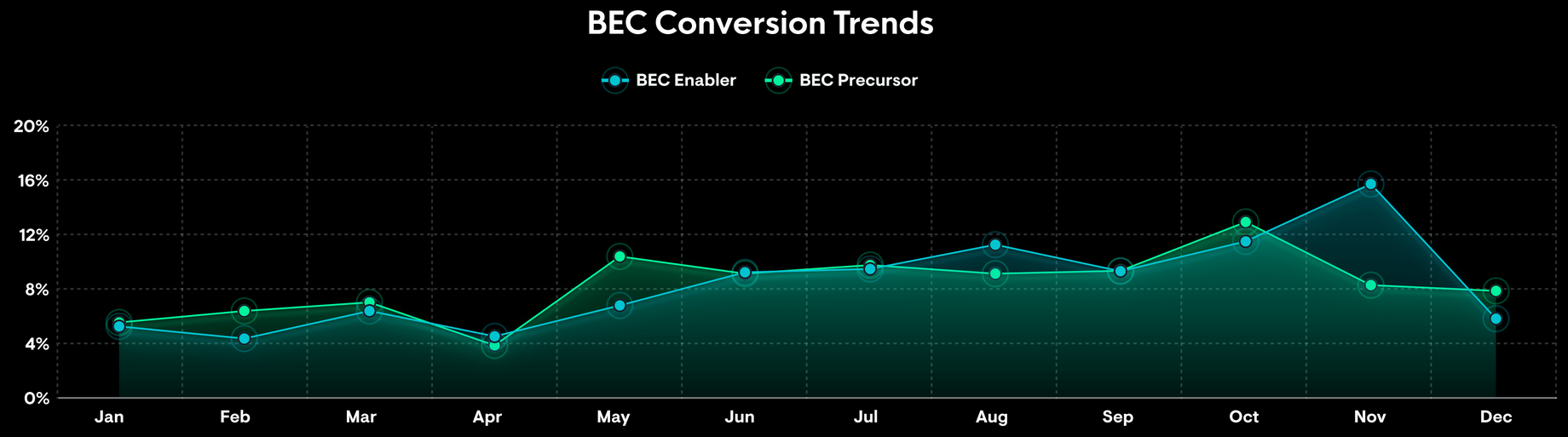


Figure 62: Distribution of BEC enabler vs. BEC precursor activity

> **BEC attacks don't always involve malware, so attackers use AiTM to steal credentials and bypass MFA for persistent access to compromised accounts. Organizations can improve resilience by setting known login locations. Block or challenge anything outside of the allow lists.**
>
> **Casey Smith**
> Staff Threat Intelligence Analyst

In BEC attacks, we see cybercriminals rely on session and token hijacking because it gives them a quick path from compromising a token to manipulating a mailbox. Once inside, attackers stay hidden before they try to cash out. They abuse inbox rules to conceal their presence, setting the stage for external forwarding or spam activity. This trend shows that cybercriminals are playing the long game. They prioritize long-term access and operational flexibility over rapid, high-volume fraud.

As the year closed out, BEC conversion and activity spiked. This surge happened because attackers ramped up campaigns focused on mail spamming, reselling email accounts, and gaining enterprise access during the holiday season.

Phishing Activity

Hacking Human Nature

In 2025, phishing was a major entry point for threat actors to gain initial access and do reconnaissance work. Despite vendor disruptions to phishing kits like Raccoon0365 and Lighthouse, these kits kept developing to give attackers advanced capabilities for scalable credential theft like MFA bypass tactics, unique subdomains for victims, or anti-analysis scripts.

To track phishing trends throughout the year, we gathered potential phishing emails reported by Huntress Managed Security Awareness Training (SAT) learners. These emails were then studied using a vision-based identification process to catalog, organize, and do in-depth analysis to categorize the most prevalent threats into unique groups of attacks targeting customers. While these groups don't represent all potential attacks, they present clear recurring themes and techniques consistently abused.

As seen on the next page, the most common phishing themes revolved around requests for e-signatures, voicemail notifications, invoice payments, and file shares. Alongside these lures, we most frequently saw file attachments that included .pdf, .png, and .html.

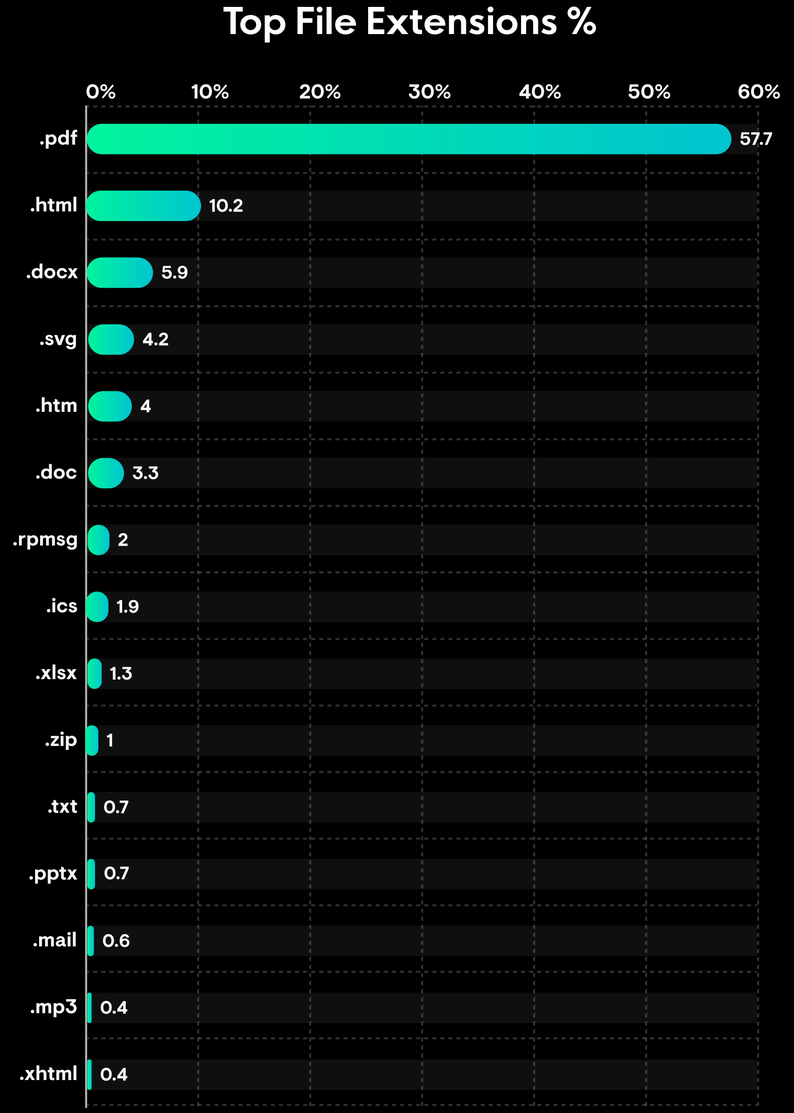


Figure 63: Most prevalent phishing attachment file extensions in 2025

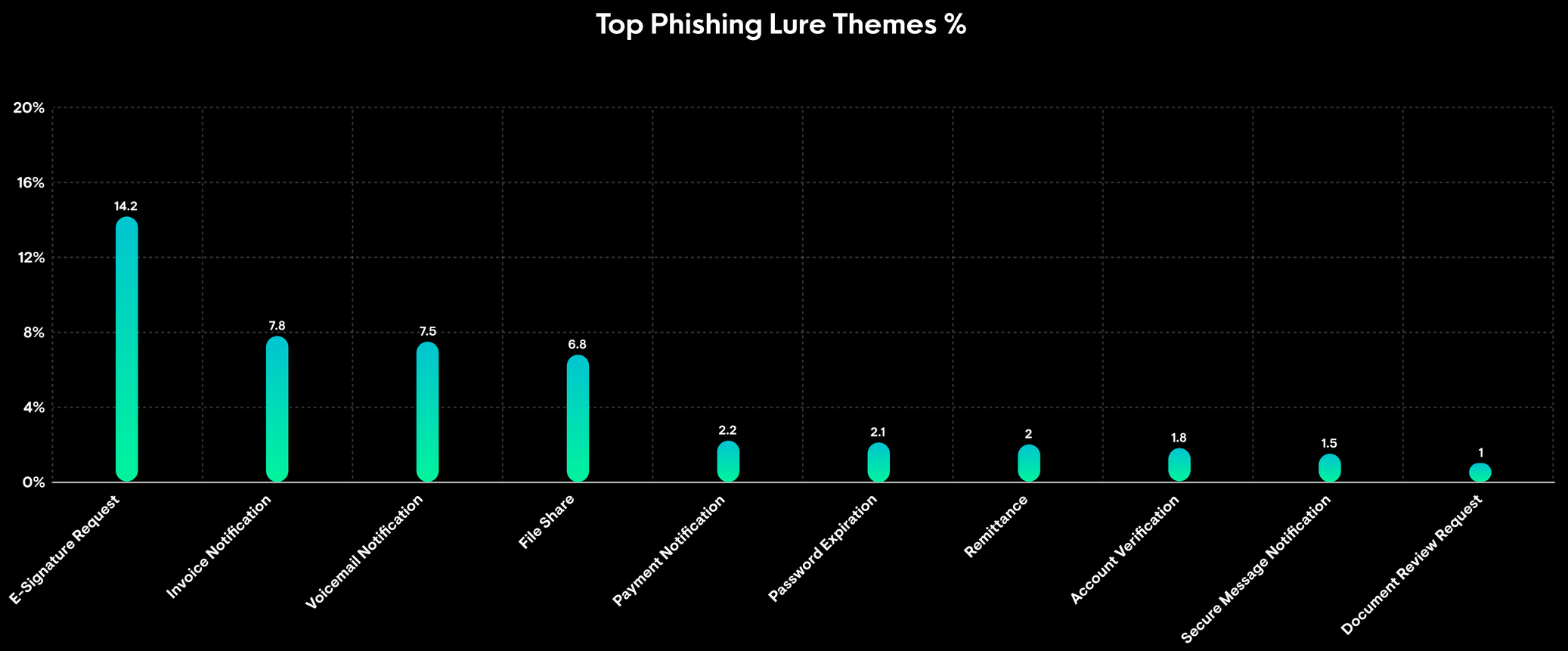


Figure 64: Most common phishing lure themes in 2025

Impersonated Brands

Microsoft was still the top impersonated brand, accounting for 31% of phishing emails we analyzed. Microsoft's widespread adoption and role as a cornerstone of productivity tools make it an attractive target. Attackers used phishing lures that mimicked everything from Teams to Microsoft Office 365 to compromise these accounts, giving attackers access to emails, files, internal communications, and more.

While mainstays like Docusign, Intuit, and Google were frequently impersonated, RingCentral is a notable new addition to our coverage this year. The cloud communications company was mimicked for voicemail lures prompting targets to "listen to the voice message" or "view the transcript" to facilitate AiTM attacks. Callback phishing, where emails use mistaken invoices or charges and provide a phone number for victims to call to "fix" a problem, was a popular method in 2025, and PayPal was a top brand attackers impersonated to carry out these attacks.

Attackers also exploited the inherent trust placed in these brands in "Living off Trusted Sites" (LoTS) attacks. Unlike standard phishing emails that link directly to a malicious page, LoTS attacks guide victims to legitimate platforms, such as file-sharing and collaboration sites, where attackers either host malicious files directly or embed deceptive links within documents stored on the trusted site. This approach is particularly effective, as users tend to lower their guard for content on "trusted" sites and outside the perceived risks of their inbox.

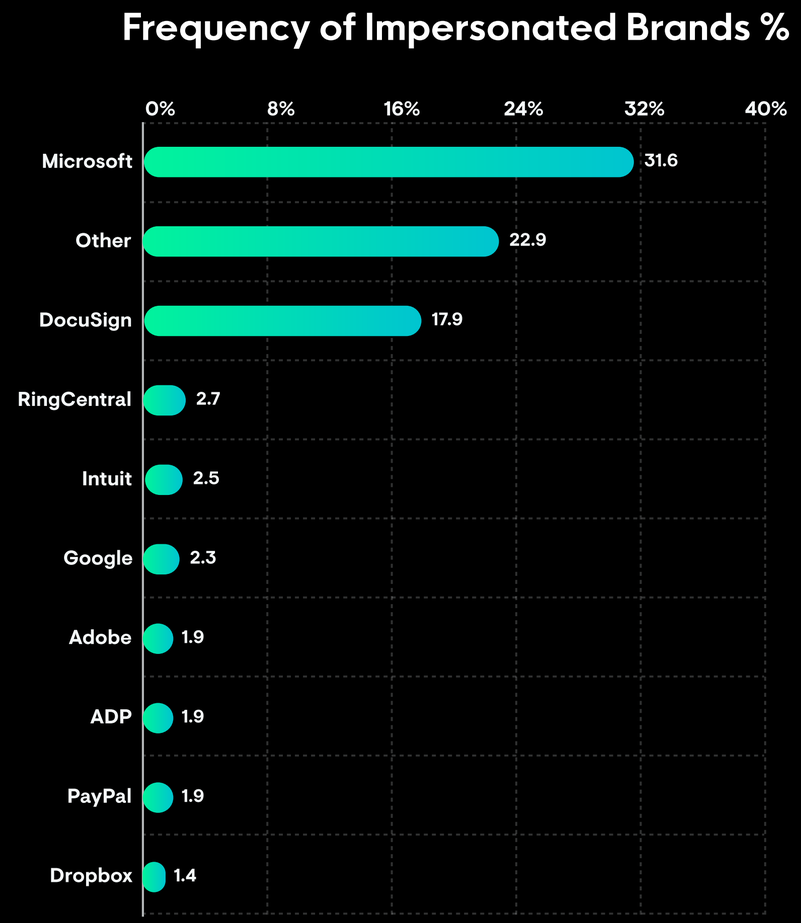


Figure 65: Brands most commonly impersonated in phishing emails in 2025

Phishing: Lures and Defense Evasion

It isn't surprising that threat actors still rely on well-known lures like those nagging shipping notifications claiming you have incorrect delivery details or that text message saying you have unpaid toll road charges. After all, why change a winning formula?

These lures are often paired with defense evasion tactics like QR codes with ASCII characters that won't be picked up by security tools, or manipulating legitimate URLs vulnerable to open URL redirects to push victims to a malicious site.

These phishing lures continue to work for threat actors because they prey on human emotion, manipulating users into opening a link or clicking on an attachment by using psychological hooks. Across the phishing lures used in 2025, urgency and trust were the most common psychological hooks used by attackers, with 56% of all phishing emails we analyzed leveraging these emotions.

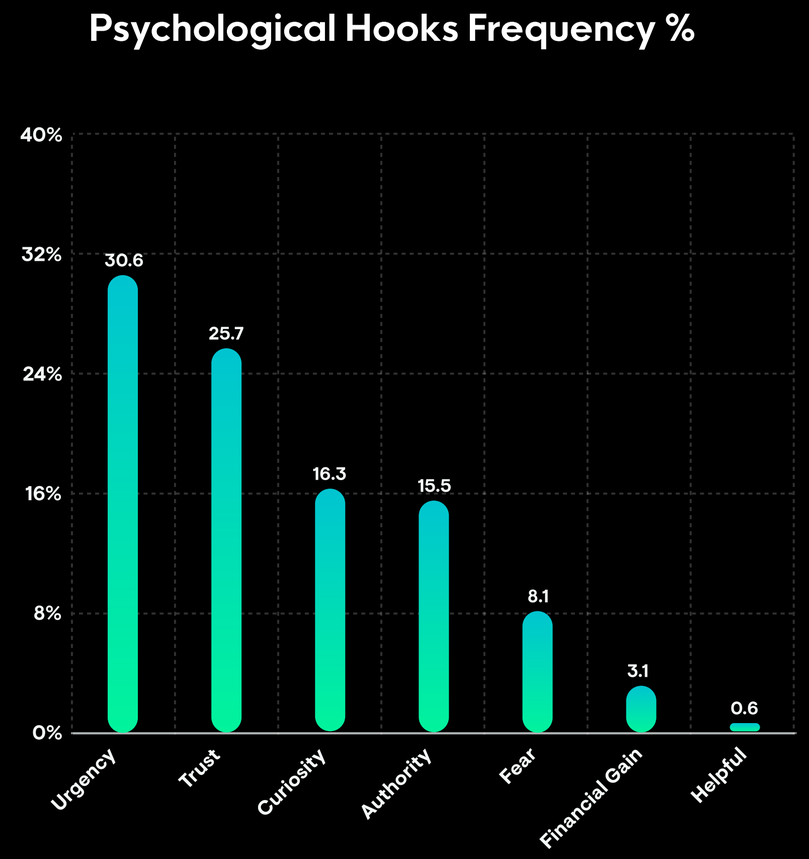


Figure 66: Most common psychological hooks used in phishing emails throughout 2025

AI Abuse

Friend, Foe, or Both?

While AI-powered cybercrime might seem like a scene from a sci-fi blockbuster, the reality behind defender lines isn't film-worthy stuff. AI abuse in 2024 was mostly about threat actors crafting phishing emails, but in 2025, experimentation evolved into more sophisticated, tangible applications.

One of the most alarming advancements is in deepfake technology. A chilling example involves BlueNoroff, a North Korean APT group, which used deepfakes of a company's leadership during a Zoom call to deceive an employee into downloading malware. Deepfakes have also infiltrated HR and recruitment processes, with companies unknowingly "interviewing" candidates who were, in reality, North Korean-linked actors using deepfake personas. Their goal is to secure employment, infiltrate organizations, and steal sensitive data.

In December, we saw a particularly novel tactic in an AMOS stealer campaign where threat actors used the 'shared chat' features of ChatGPT and Grok. By pre-generating conversations giving malicious Terminal commands—disguised as helpful instructions for queries like 'Clear disk space on macOS'—attackers bypassed user suspicion. These shared links were then promoted via sponsored Google ads to dominate search results, tricking users into executing malware directly on their systems.



Figure 67: An attacker's attempt to use an AI-generated script for credential dumping

Cybercrime is, at its core, a business, and like any business, cybercriminals are constantly seeking ways to scale. AI has become their ultimate productivity tool, helping them automate and accelerate operations at breakneck pace. But this rush to scale often comes at a cost: In their haste, attackers leave behind telltale signs like scripts riddled with Russian comments or Cyrillic characters, malicious browser extensions with emojis buried in the source code, or even scripts that claim to steal data, but don't have the functionality to exfiltrate it.

Malicious groups are adopting AI to speed up tooling and development. They use AI-assisted OSINT to pinpoint target details and deploy dark web tools to find high-value data. Attackers also rely on AI to generate code, clone phishing websites, and modify malware signatures to evade detection. While this technology raises the baseline skill level for lower-level hackers, its biggest advantage is speed. AI cuts down the time needed to stage and launch attacks, forcing defenders to identify and react to threats faster than ever.

What does 2026 hold for us as AI-powered cybercrime evolves? If 2025 taught us anything, it's that AI will keep lowering the barrier to entry for cybercriminals, so even novice threat actors can launch sophisticated attacks while helping seasoned operators scale their operations. But we're also seeing a shift in AI abuse tactics. Threat actors will exploit user trust in AI tools, creating even more convincing social engineering schemes and using automation to supercharge reconnaissance efforts.

To prepare for these threats and build stronger defenses against AI abuse, organizations should take these steps in 2026:

- Invest in managed security solutions that connect the dots through the entire attack path, from telemetry retention through security awareness training
- Use MFA for all VPN, admin interfaces, RMM, and backup consoles
- Restrict lateral movement paths by hardening the network with segmentation and least privilege deployment, and monitoring WinRM, RDP, and service account usage
- Log and alert on suspicious interpreter activity with command-line capture and script block logging, and/or deploy appropriate security solutions that facilitate full visibility across the network
- Maintain and tune detection for early stage tradecraft behaviours like anomalous enumeration, lateral movement, credential dumping, and privilege escalation

> **We're seeing adversaries use AI much like engineers do: for coding, tool development, and workflow automation. They're using it to find software vulnerabilities, craft more convincing phishing emails, clone voices for deepfakes, and optimize operations across the board. We even caught an attacker installing our own EDR agent, which let us see how they used AI to streamline workflows and sharpen phishing campaigns.**
>
> **Jamie Levy**
> Senior Director, Adversary Tactics



Conclusion

Resilience Wins

> **Most teams think resilience comes from seeing more. In reality, it comes from knowing what matters and acting quickly when it does.**
>
> **Eric Stride**
> Chief Information Security Officer, Huntress

2025 was defined by shifting tactics and blurred lines across the threat landscape. Attackers don't need to break down your digital doors when they can just log in with stolen credentials or trick an employee into giving them access. By weaponizing legitimate tools like RMMs and exploiting everyday behaviors through stealthy tactics like ClickFix and fake CAPTCHAs, cybercriminals have turned identity into the new perimeter. The line between normal activity and an incident is thinner than ever, proving that traditional defenses alone aren't enough to stop these organized, profit-driven cybercriminal operations.

To stay ahead in 2026, we have to treat security as a business-wide responsibility, not just another IT ticket piled up in the queue. This means building a defense strategy that prioritizes identity protection, monitors the abuse of trusted processes, and empowers every employee to spot attacker tradecraft. Trust us—you can't hire or innovate fast enough to fight this competition alone. But by curating a culture where humans are the first line of defense, we can turn our biggest vulnerability into our greatest strength and lead the threat landscape, not react to it.

About Huntress

Huntress is a global cybersecurity company on a mission to make enterprise-grade products accessible to all businesses. Purpose-built from the ground up, Huntress' technology is specifically designed to continuously address the unique needs of security and IT teams of all sizes. From Endpoint Detection and Response (EDR) and Identity Threat Detection and Response (ITDR) to Security Information and Event Management (SIEM) tools and Security Awareness Training (SAT), the platform provides targeted protection for endpoints, identities, data, and employees, delivering trusted outcomes and valuable peace of mind.

Its 24/7, AI-assisted Security Operations Center (SOC) is powered by a team of world-renowned engineers, researchers, and security analysts, dedicated to stopping cyber threats before they can cause harm. Huntress is often the first to respond to major hacks and incidents, with its expert security team sharing real-time tradecraft analysis and actionable advisories with the community. Currently safeguarding over 4.5 million endpoints and 10 million identities, Huntress empowers security teams, IT departments, and Managed Service Providers (MSPs) worldwide to protect their businesses with enterprise-grade security accessible to everyone.

As long as hackers keep hacking, Huntress keeps hunting. Join the hunt at www.huntress.com and follow us on X, Instagram, Facebook, and LinkedIn.

HUNTRESS