
HUNTRESS
2026 CYBER THREAT REPORT
STATE OF RANSOMWARE

Table of Contents

Why Ransomware Is Actually Your Fiercest Competitor

When you think about competition, who comes to mind? Probably the company across town trying to poach your best clients. Or the industry giant that's squeezing your margins with lower prices.

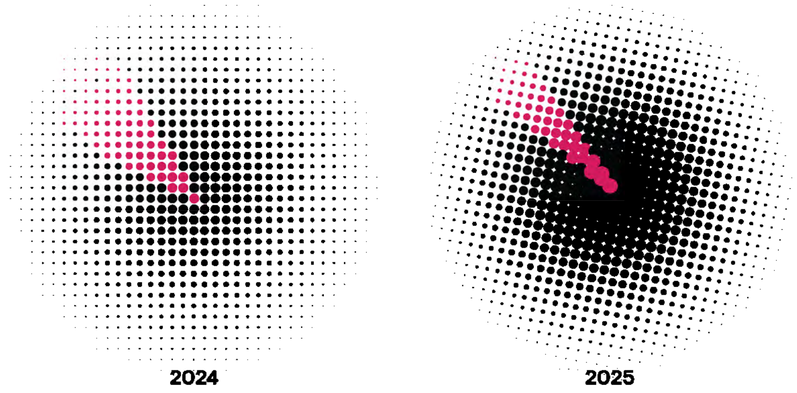
But the landscape has shifted right under our feet. Your biggest threat isn't just the business rival trying to beat you to market. It's the invisible, highly organized, and surprisingly corporate-like ecosystem of ransomware. It's a full-blown business model with customer support, R&D departments, and profit margins. And right now, it's vying for your revenue just as hard as any legitimate competitor.

These cybercriminals don't want to build a better product than you. They want to steal the value you've already worked so hard for. When a ransomware attack hits, it freezes your operations, damages your reputation, and drains your bank account. That creates a massive opening for your traditional competitors to swoop in. If your systems are down for a week, where do your customers go? Will they wait for you to reopen, or will they go to a competitor? This is how security gaps directly translate to lost business.

This ebook unpacks the top ransomware trends from the Huntress 2026 Cyber Threat Report. Understand the ransomware threats you're facing today, so you can shut down this unwanted competition with confidence and secure your future.

Ransomware in 2025

The State of Ransomware



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

Even with law enforcement crackdowns on major cybercrime groups, ransomware remained a menacing force in 2025. It accounted for 5% of incidents in 2025, and the total volume of attacks actually went up.

Four major players were linked to over half of all ransomware incidents: Akira, Medusa, Qilin, and RansomHub. To outpace one another, they standardized their operations into a "common playbook" that looks like this:

- External payload retrieval through PowerShell-based downloaders
- Active Directory enumeration for reconnaissance
- Bring your own vulnerable driver (BYOVD) techniques to block endpoint detection and response (EDR) solutions
- Running standard commands to wipe shadow copies and disable Windows Defender
- Living off the land with legitimate remote monitoring and management (RMM) tools to hide in plain sight
- Using encrypted tunnels to stage attacks
- Stealing data for extortion before deploying ransomware

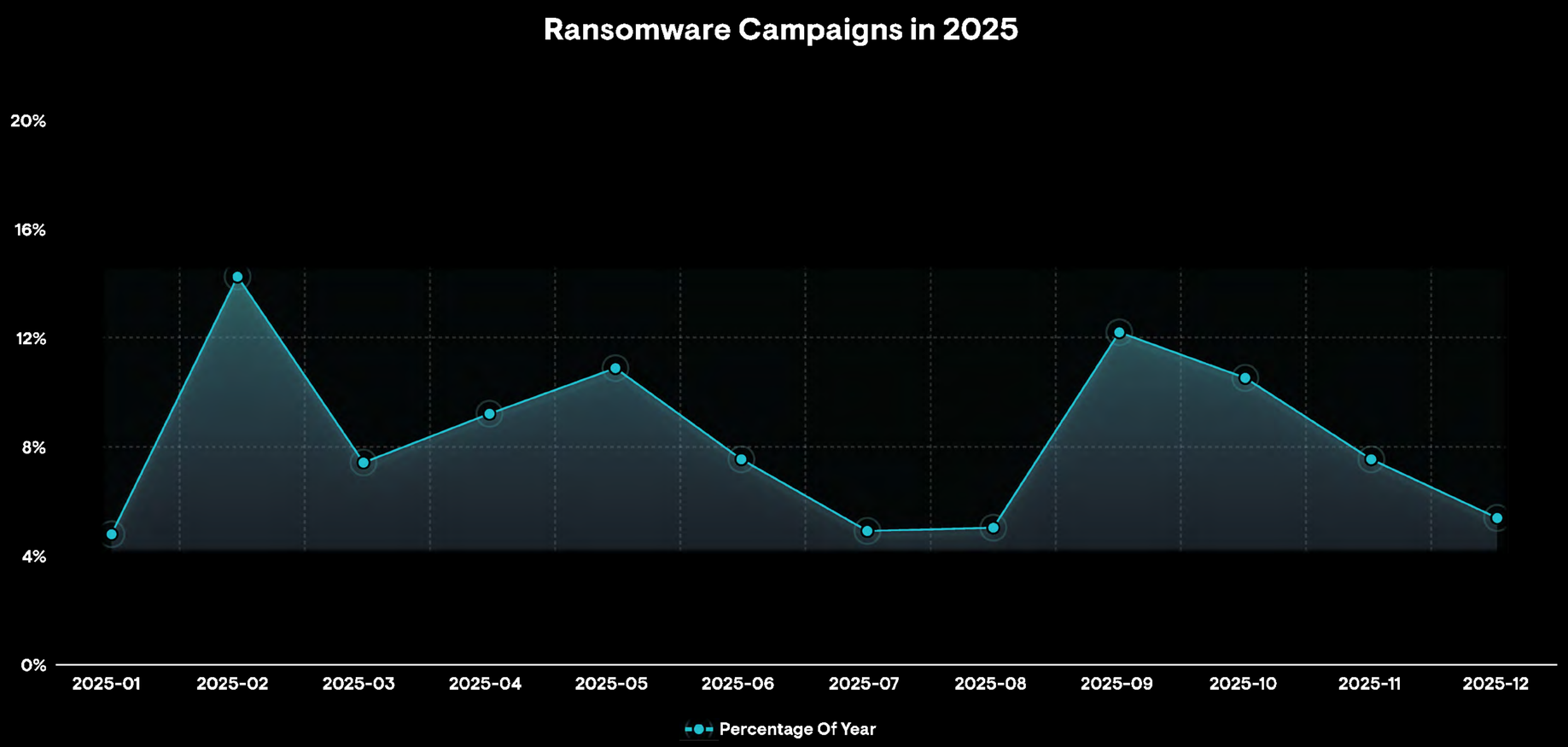


Figure 1: Monthly distribution of global ransomware campaigns

Time-to-Ransom Increases

Criminals are taking their time. The average time-to-ransom (TTR) crept up from 17 to 20 hours in 2025.

This wasn't because they got slower. It was a strategic choice. Attackers are prioritizing stealth and data exfiltration over speed. They're spending that extra time ensuring they have your data before they lock your systems.

The Shift Away from Exploits

Hackers often follow the path of least resistance. With fewer server-side vulnerabilities to abuse, most groups moved away from complex exploits. Instead, they relied on stolen or reused credentials, disabled multi-factor authentication (MFA), and exposed RDP, VPN, and access logs.

There are exceptions, of course. Groups like Cl0p and Akira still use an "exploit once, compromise many" strategy, as seen in the campaign targeting SonicWall, Ivanti, and Fortinet devices. But for the average ransomware gang, developing custom exploits is a luxury they can't afford when stolen passwords work just as well.

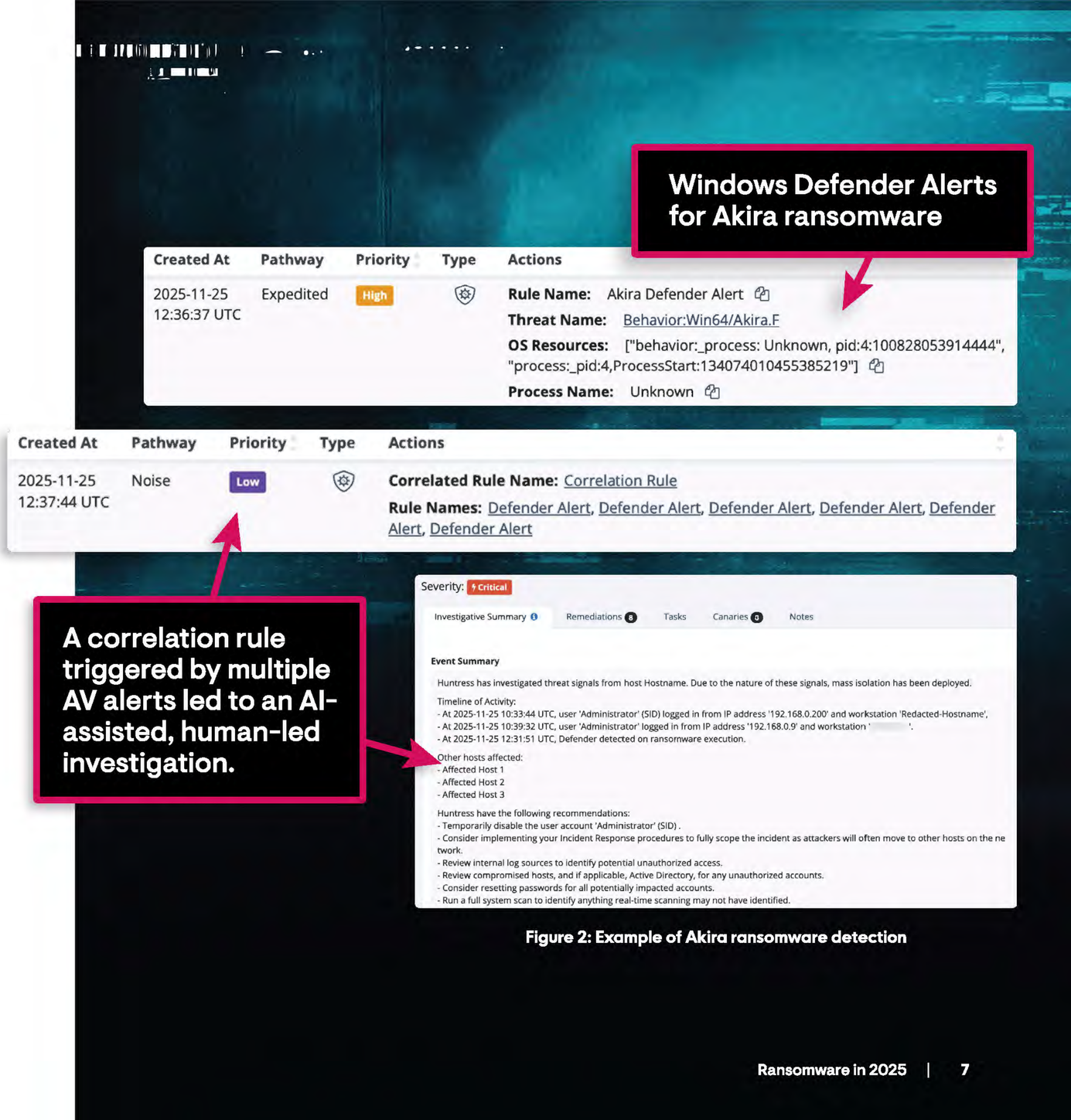


Figure 2: Example of Akira ransomware detection

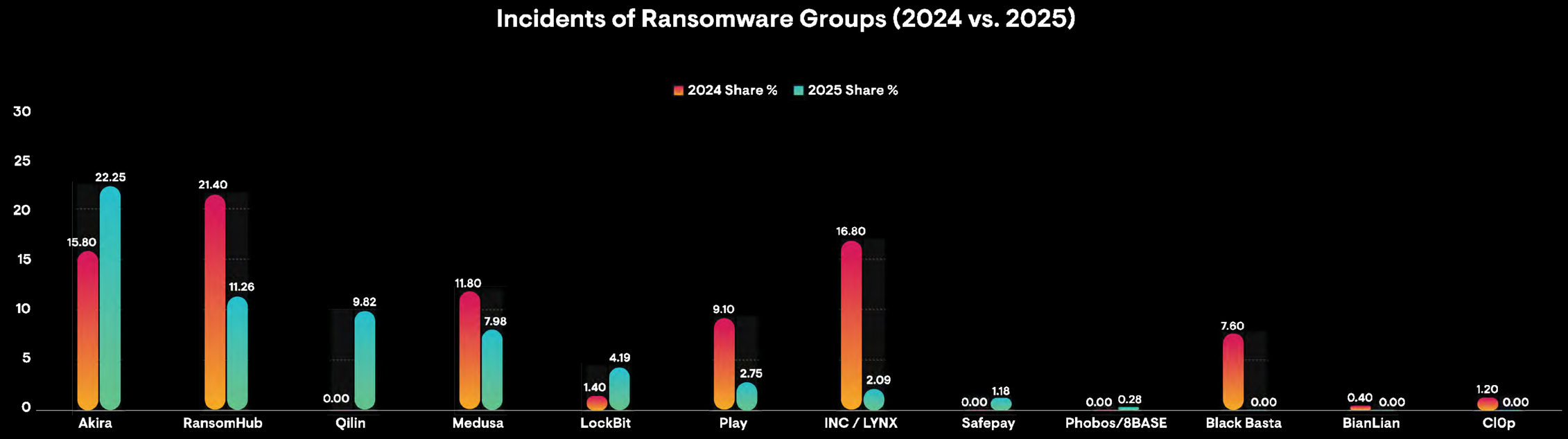


Figure 3: Ransomware groups incident frequency from 2024 to 2025

Ransomware Groups

Ransomware activity in 2025 felt eerily similar across different sectors. Attackers streamlined their playbooks, and major cybercrime partnerships ramped up operations. Longtime groups stuck to tradecraft that worked, rather than inventing new tricks. Most relied on the existing ecosystem: initial access brokers, remote-management abuse, and commodity malware loaders.

We saw the merger of Shiny Hunters, Scattered Spider, and Lapsus$ into "ShinySp1d3r," while DragonForce attempted to build a cartel alongside Qilin and LockBit (which resurfaced as LockBit 5.0). Akira dominated the playing field, accounting for nearly 25% of all incidents. This persisted even as competitors fell: Black Basta suffered a massive leak of internal chats, and law enforcement dismantled BlackSuit. While new variants like Cephalus and Obscura emerged, the data shows that four groups—Akira, Medusa, Qilin, and Ransomhub—drove over half of all ransomware incidents.

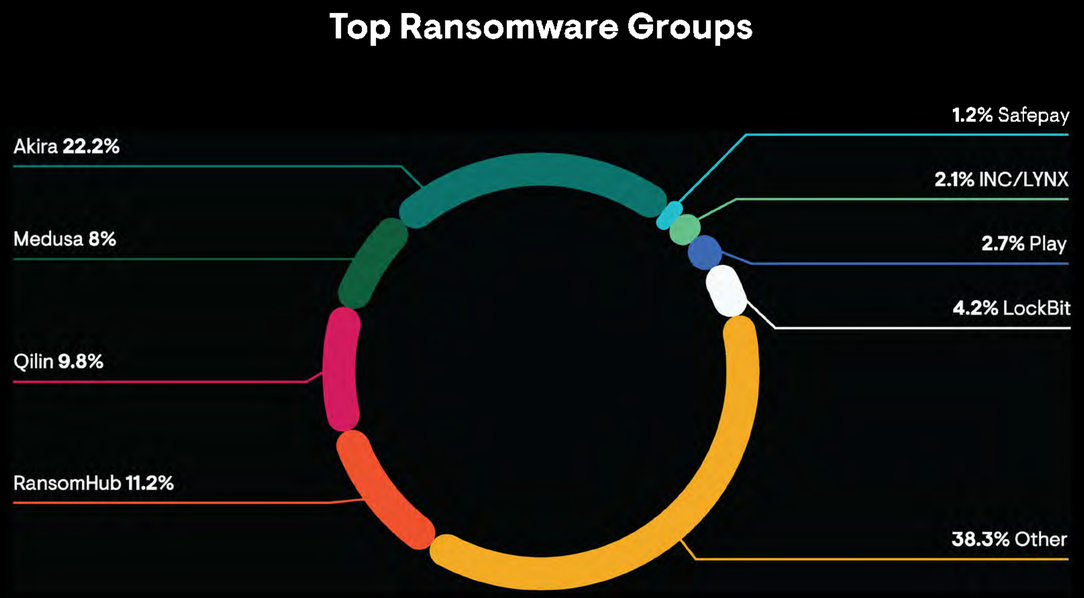


Figure 4: Most prevalent ransomware groups in 2025

Ransomware Groups Gains and Losses

Ransomware Family	2024 Frequency	2025 Frequency	Gain or Loss
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 5: Table of ransomware gains and losses 2024 vs. 2025

Common Ransomware Tradecraft

Inside Ransomware Toolkits

Ransomware operators relied on the classics in 2025. They doubled down on approaches, like stealing credentials, establishing SYSTEM-level persistence, and wiping shadow copies.

Active Directory Data Theft Via Shadow Copy and Symlink Abuse

`NTDS.DIT` is the main database file for Microsoft Active Directory Domain Services (AD DS). It stores everything related to your domain, including user accounts, group memberships, and hashed passwords. It's essentially a playground for ransomware operators.

We consistently saw attackers grab credential material from `NTDS.DIT` without ever touching the live database. Instead, they went for offline copies via Volume Shadow Copies. This keeps things quiet, avoiding service disruptions or the kind of domain controller instability that sets off alarms.

To pull this off, operators frequently abused legitimate Windows utilities. They modified Windows symlink behavior to weaken the default file system trust boundaries. This trick let them access shadow copy devices in ways Windows security controls normally block.

Once those protections were down, attackers mapped internal shadow copy paths to locations they could access. This exposed protected system files to their tools without needing direct access to the live NTDS database. It bridges the gap between system-level resources and user tools, allowing criminals to copy, parse, and exfiltrate credentials under the radar.

After they grabbed the file, `NTDS.DIT` helped expand the attackers' reach through credential-driven attacks. While this is a known strategy, we saw it adopted by several smaller ransomware groups this year, who previously relied on noisier, easily detected methods like ntsdutil or impacket.

Operators extracted password hashes offline, used Kerberoasting against service accounts, and reused credentials via pass-the-hash and pass-the-ticket techniques. This workflow drastically cut the time needed to take over a domain and dodged many traditional detection methods.

Clearing Security Obstacles

The defense evasion tactics we saw in 2025 weren't accidental. Groups like Akira, Medusa, and DragonForce routinely scoped out security products from the start of an attack, guiding their tampering efforts to blind defenders.

Operators tweaked security configurations, added process or path exclusions, suppressed logging, and wiped event data to cover their tracks. In sophisticated attacks, we even saw them abuse or deploy kernel drivers to bypass user-mode protections entirely. The goal wasn't always to kill the security tools immediately, but to blind them long enough to stage the attack, harvest credentials, and prep for encryption without interruption.

Figure 6: Encrypted file sample from Obscura ransomware

Hiding Behind Encrypted Tunnels

Ransomware operators upped their game in 2025, choosing legitimate tunneling and exfiltration tools over custom malware.

Cloudflared became the go-to tunneling mechanism, with spikes in activity in July and August matching surges in hands-on-keyboard attacks. For stealing data, Rclone remained the heavy lifter, especially in the autumn, as campaigns shifted toward bulk theft and extortion.

While SSH is still a staple, we saw tools like FRP and Chisel pop up for specific jobs. We also observed brief spikes in WinSCP and Mega Cloud Sync, suggesting opportunistic file theft after attackers gained privileged access.

These trends highlight a shift among ransomware groups to hide in legitimate network traffic, move data fast, and steal it at scale before the ransom note ever lands.

Tunneling and Exfiltration Tools Used for Ransomware

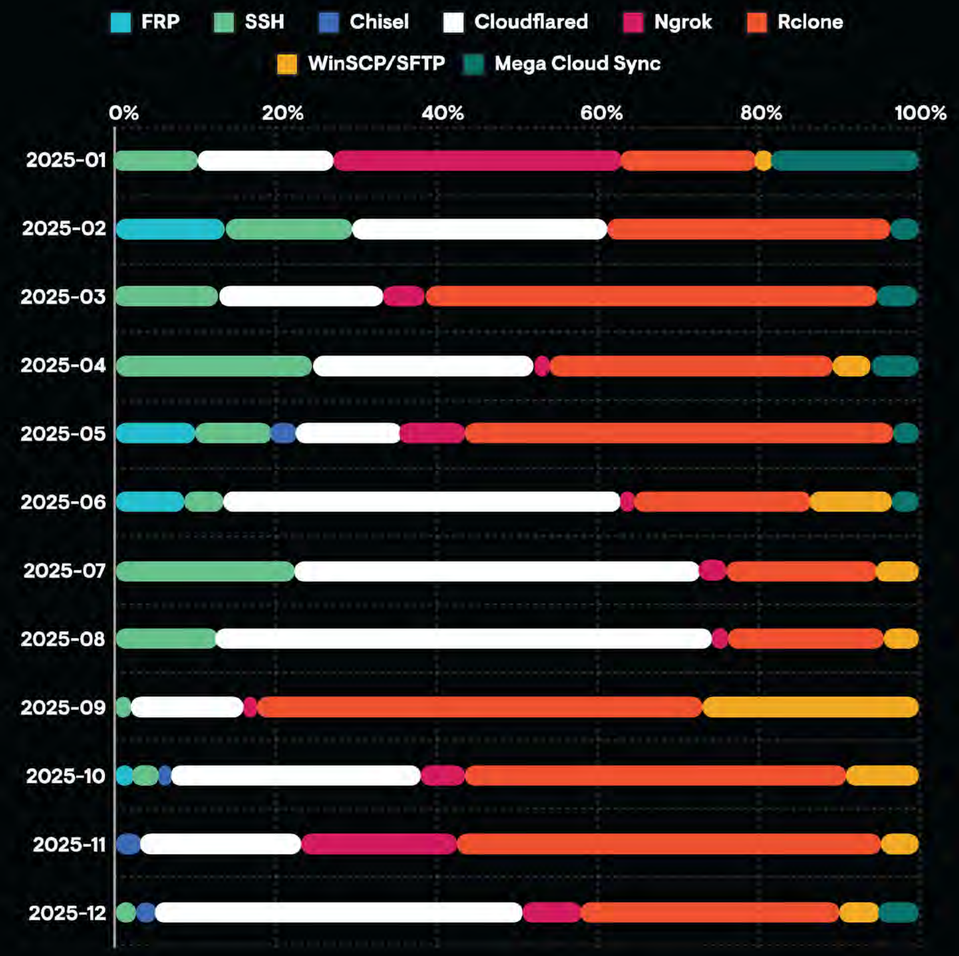


Figure 7: Monthly breakdown of tunneling and exfiltration methods linked to ransomware activity

Time-to-Ransom (TTR) Measurement

Tracking Compromise Windows

Average Time-to-Ransom in 2024 and 2025

TTR isn't just a number. It reveals operator maturity, attack complexity, and the operational workload behind successful breaches. We use this metric to track the average time it takes ransomware operators to go from initial access to full deployment.

Our 2025 data showed attackers are changing their behavior in three key ways, reflecting a longer TTR of 20 hours...

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.

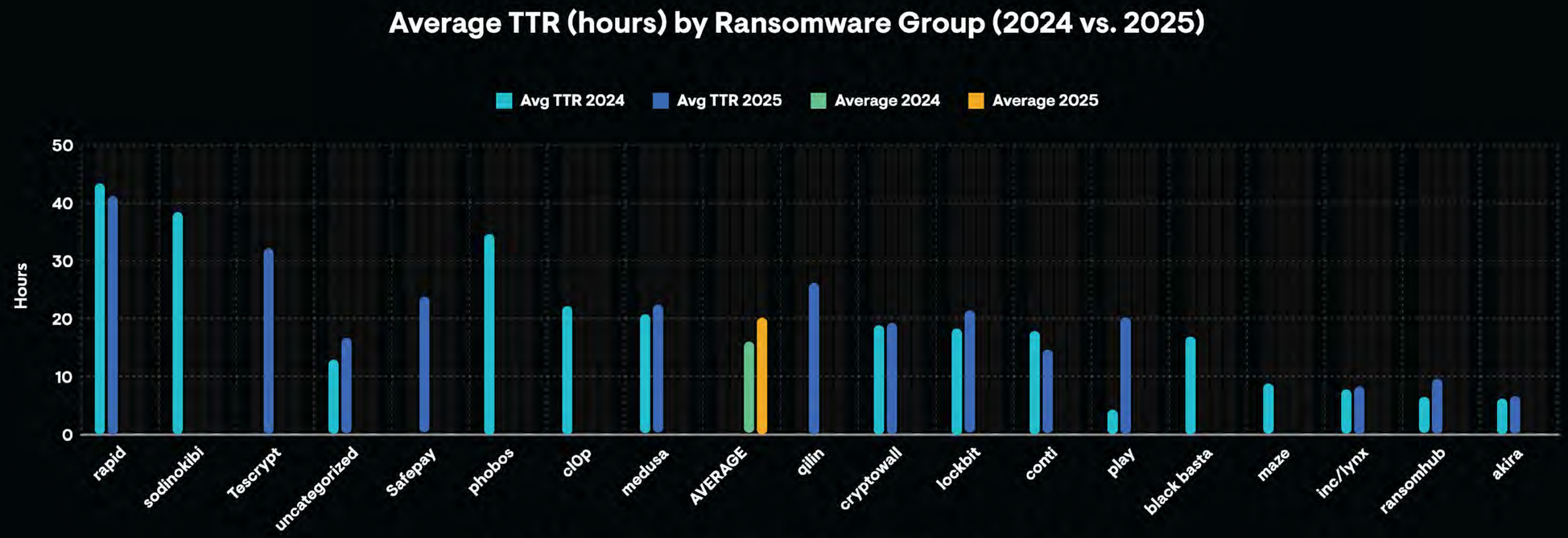
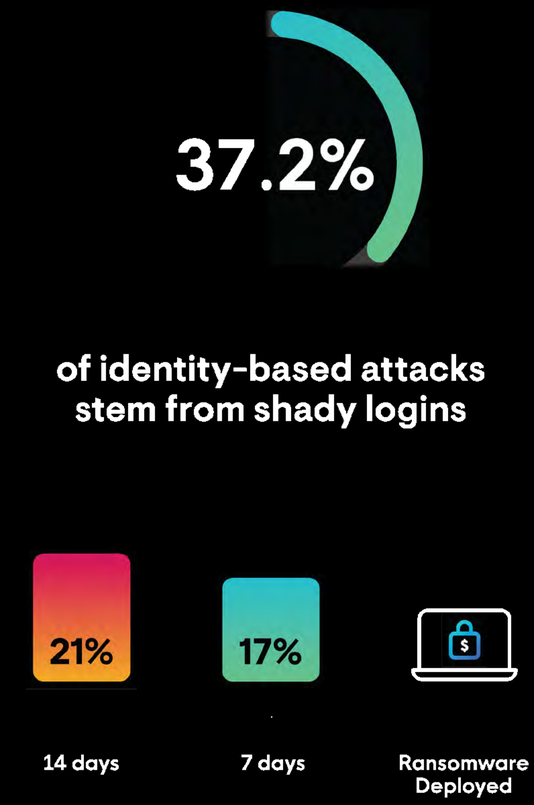


Figure 8: Average time-to-ransom (TTR) by ransomware group in 2024 vs. 2025

A Ransomware Early Warning System

Our Identity Threat Detection and Response (ITDR) telemetry flagged a critical "pre-access" ransomware window. We often see precursor activity, like account verification using stolen credentials, days or weeks before the ransomware event.

In fact, around 17% of incidents showed ITDR-related activity at least seven days before ransomware. That number climbs to nearly 21% over a 14-day window. This suggests initial access brokers (IAB) are validating credentials early to ensure they work when it is time to strike.



Mapping Ransomware Attack Paths

Decoding Attack Vectors

Whether it's a remote access trojan (RAT), a RMM tool, or a clever social engineering scam, the window for disruption is narrow. Here's what defenders need to know about three of the most common paths to ransomware attacks to shut them down early.

ClickFix Scams: Hacking the Human

ClickFix scams succeed because they exploit human trust, the biggest vulnerability out there. These attacks trick users into executing arbitrary commands, usually under the guise of fixing a fake error. FakeCAPTCHA, a variant of ClickFix, takes victims through manual steps to "verify" they're human.

Most ClickFix operations are optimized for speed, with immediate handoffs to ransomware teams. However, fake CAPTCHA variants often have a 6-16 hour delay. This suggests a broker model where system info is harvested and validated before being sold for ransomware attacks.

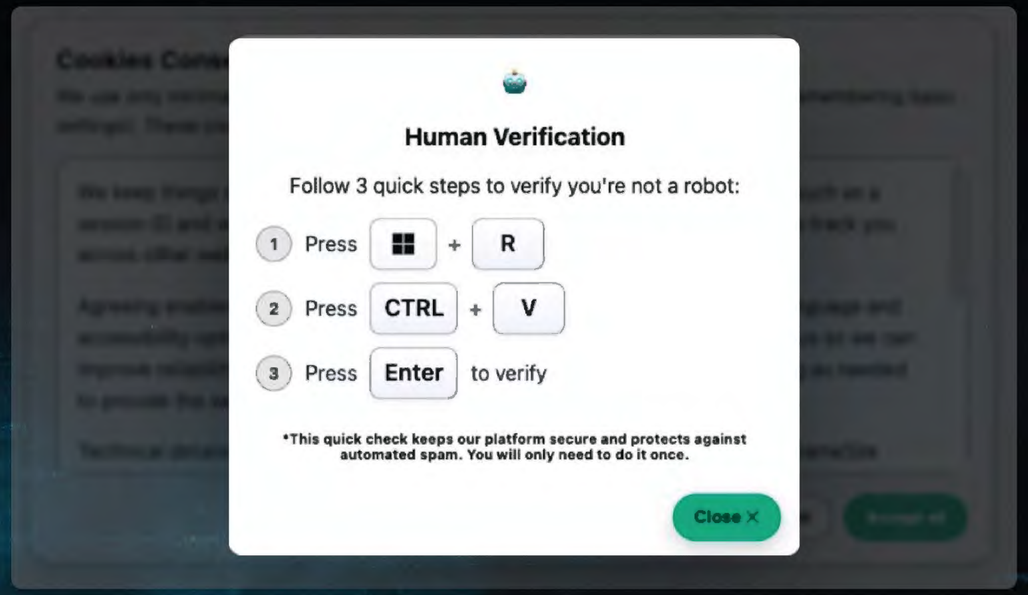


Figure 9: Example of a ClickFix human verification lure

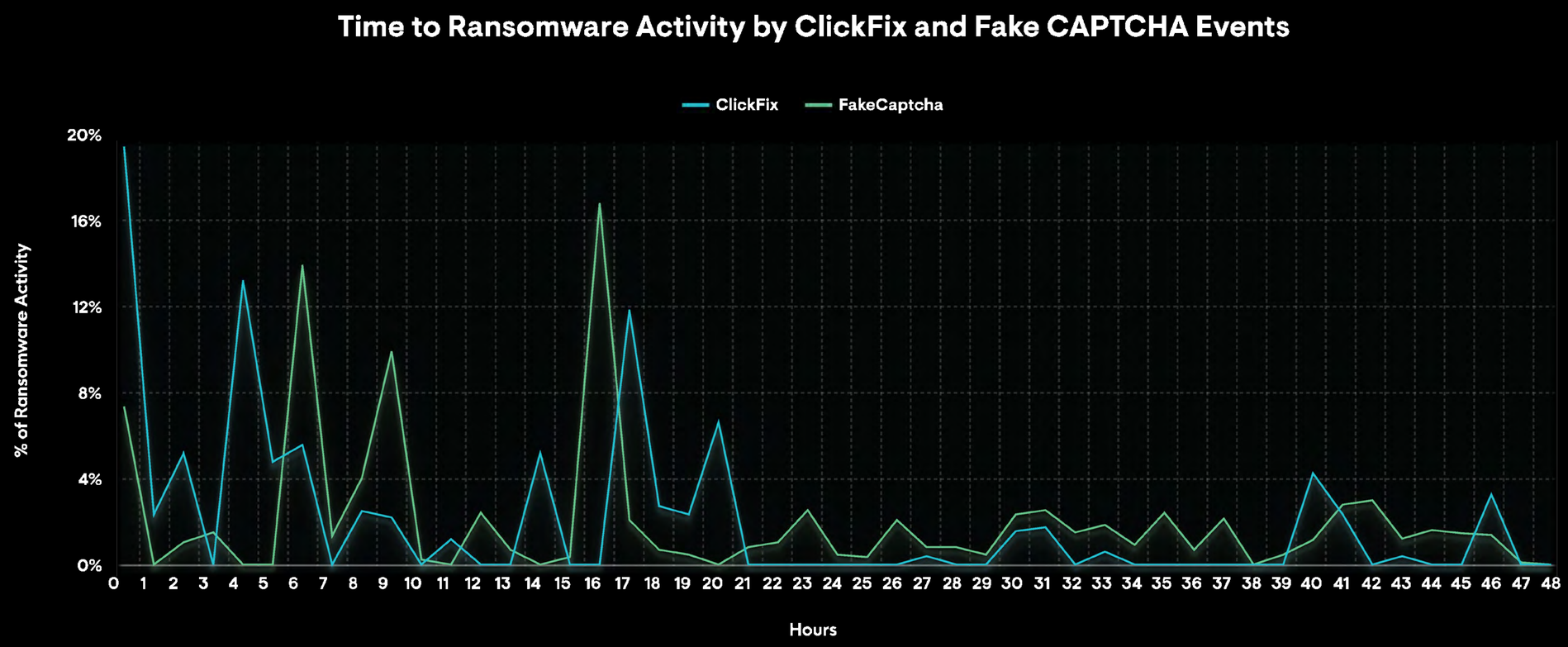
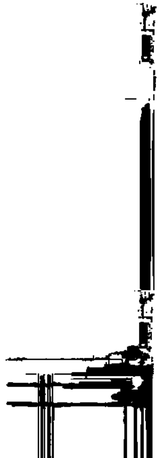


Figure 10: Time to ransomware activity within 48 hours of ClickFix and fake CAPTCHA events

RMMs: Legitimate Tools, Malicious Intent

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 12 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 divided 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.

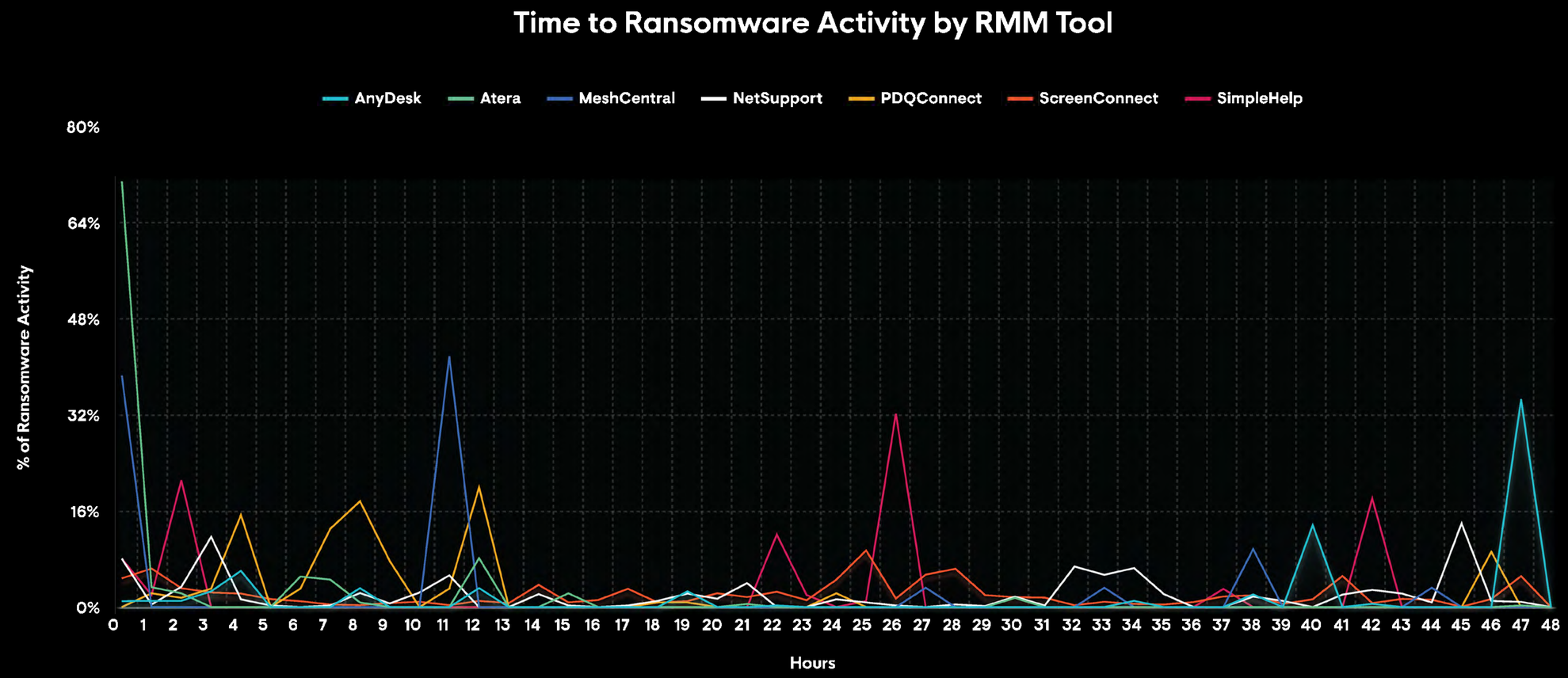


Figure 11: Time to ransomware activity within 48 hours of RMM execution

RATs: The 12-Hour Warning

If you detect a RAT, you're already in the danger zone. RATs follow a highly compressed attack path timeline. In 25% of incidents, ransomware activity begins within one hour of RAT installation.

Families like AsyncRAT are built for immediate cashing in, with about one-third of activity often starting within minutes. Other families, like RevengeRAT, STRRAT, and XWorm, are serious red flags that require immediate attention to keep your systems out of trouble.

Think of a RAT detection as a late-stage warning. The attackers are already inside, preparing to cause damage.

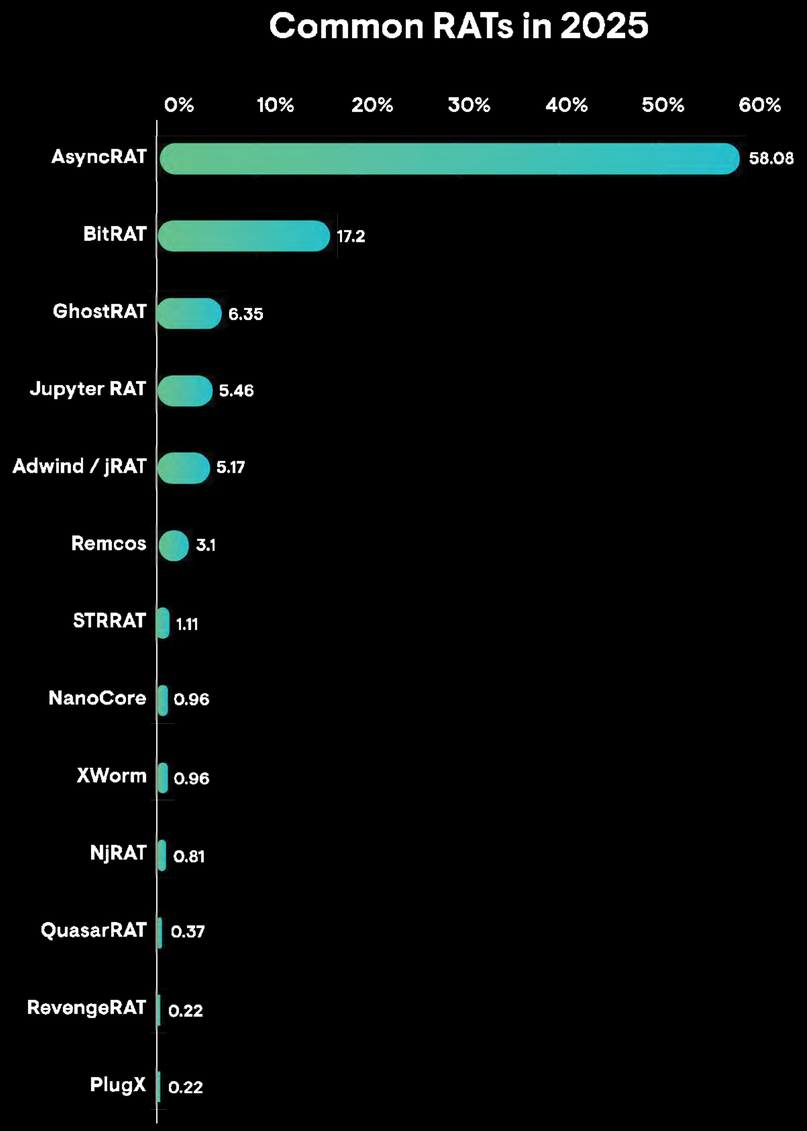


Figure 11: Distribution of RATs

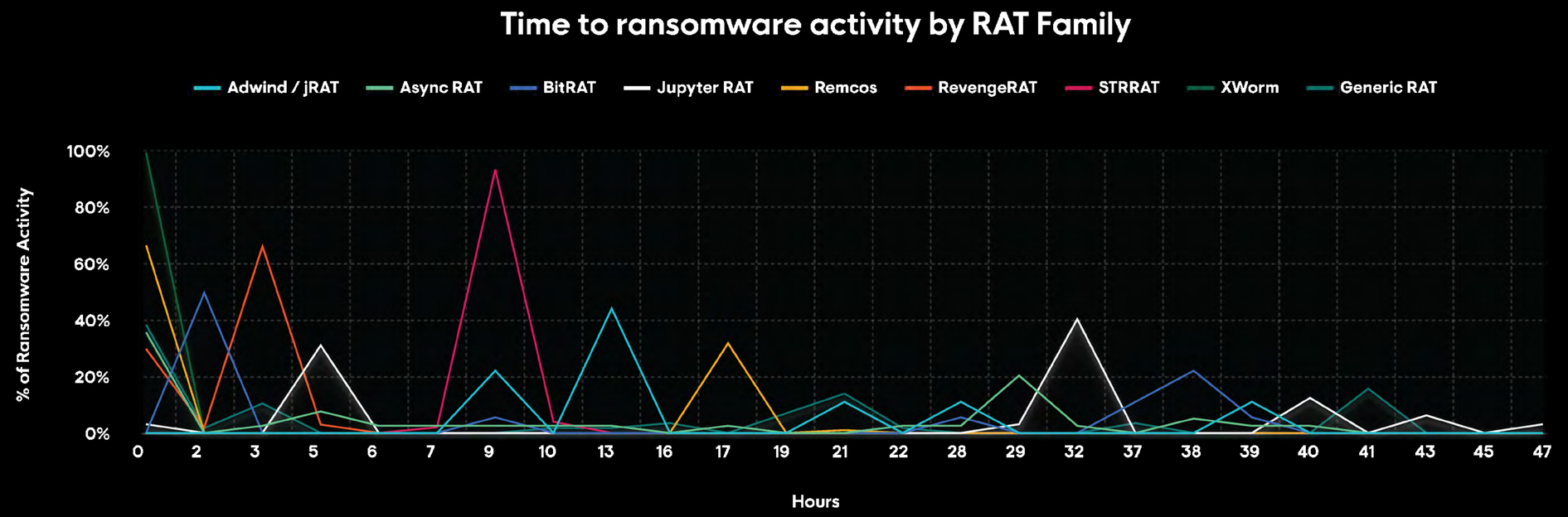


Figure 12: Time to ransomware activity within 48 hours of RAT install


How to Stay Ahead of Ransomware
HUNTRESS | 2026 CYBER THREAT REPORT

Outpacing Hidden Competition

Addressing security gaps isn't just about staying ahead of threats—it's about gaining a strategic competitive advantage. When you invest in strong security and spot ransomware threats early, you protect your business, build credibility, and scale with confidence. Make security a priority now with these tips, because it's what keeps you competitive and secure for what's next tomorrow and beyond.

- ✓ Turn on MFA on network perimeter devices. If you've got VPNs in your environment, we're talking to you.
- ✓ Strong passwords only. Always.
- ✓ Don't slack on access inventory reviews and audits to spot unnecessary exposure gaps. Know your organization's baseline profile for authorized software.
- ✓ Consider disabling accounts that haven't been used for 30 days or more.
- ✓ Use RMM allow/deny listing. If you don't want it, block it.
- ✓ Friends don't let friends expose RDP. Close the gap on port 3389 by putting it behind a VPN with MFA enabled or a firewall.
- ✓ Don't use local administrator accounts for daily operations.

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.

Contact us to learn more.

8 Phone Number

f8l sales@itispivotal.com

D www.itispivotal.com

pivotal IT
Strategy. Solutions. Support.

In partnership with

HUNTREss