HUNTRESS | 2026 CYBER THREAT REPORT

The TL;DR

The business of cybercrime is booming, and it's never been more efficient.

In 2025, we analyzed hacker activity across more than 4.6 million endpoints and 9.4 million identities. One theme was clear: cybercrime is running better than most businesses. What was once a chaotic patchwork of isolated attacks and disorganized groups has transformed into a sophisticated, global supply chain. Cybercriminals are exploiting the same tools we depend on every day, and they're competing against your business with a standardized playbook.

Our 24/7 human-led, AI-assisted Security Operations Center (SOC) shuts down these threats, giving us a front-row seat to the shifting threat landscape. In the Huntress 2026 Cyber Threat Report, we break down how cybercriminals are abusing legitimate tools, launching complex identity attacks, and pulling off clever social engineering scams to bypass traditional defenses and avoid noisy exploits.

To scale your business securely in the year ahead, here's the TL;DR on the most critical threats.

Industry

Attacks against the manufacturing industry were up by 88%

Malware

ClickFix accounted for 53.2% of all malware loader activity

Identity

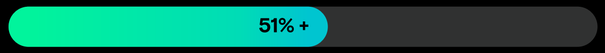
18.9% of all identity-based threats were linked to adversary-in-the-middle (AiTM) attacks (a tactic that bypasses MFA controls)

Phishing

57.7% of phishing attacks used malicious PDF attachments

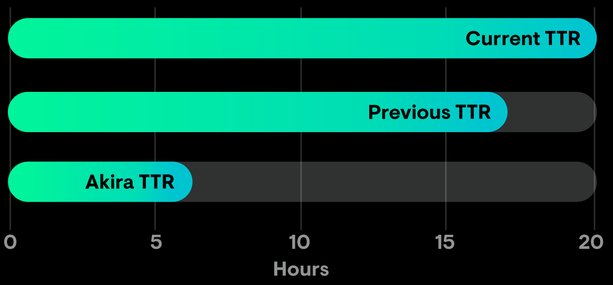
Ransomware

Over 51% of all ransomware incidents were linked to Akira, Medusa, Qilin, and Ransomhub



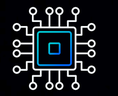
Average time-to-ransom (TTR) jumped from 17 to 20 hours because attackers:

- Focused more on extortion and data theft
- Prioritized staying hidden over moving fast
- Took their time between initial access and the next steps in the attack path



Akira, the top ransomware group, had a TTR of 6.58 hours and was linked to 22% of all ransomware incidents

Threat Landscape at a Glance



AI

AI-powered cybercrime isn't just about smarter phishing scams anymore. It's an illicit business built on the abuse of trust. Attackers use deepfakes to impersonate executives on video calls, fake job interviews to sneak into HR departments, and even manipulate shared chat features in tools like ChatGPT to trick users into running malicious commands. The real danger here is AI puts powerful cyberattack tactics and tools in anyone's hands.

Identity Attacks

Microsoft 365 stayed in attackers' crosshairs throughout 2025. Over 35% of identity threats came from shady logins: risky locations, malicious networks, or sketchy VPNs, followed by 19% from mailbox manipulation and persistence, a telltale sign of business email compromise (BEC) attacks. Digital identities are the new security gate, letting attackers slip by defenses unnoticed to persist, move laterally, and run BEC attacks from the inside.

Ransomware

Despite aggressive law enforcement takedowns and high-profile disruptions, ransomware was a ruthless threat in 2025. While its share of total incidents fell, the overall volume increased year over year. Groups streamlined their playbooks, favoring proven attack chains over novel techniques and shifting away from exploit-based attacks toward other methods like RMM abuse and commodity malware loaders. This shift in tradecraft was accompanied by a rise in the average TTR to 20 hours, as groups prioritized stealth and focused on data theft and exfiltration.

RMM Abuse

Abuse of remote monitoring and management (RMM) tools shot up 277% in 2025. Cybercriminals built entire playbooks around these legitimate, trusted tools to drop malware, steal credentials, and execute commands. Because RMM activity often blends into expected admin workflows, spotting malicious activity can be tough.

ClickFix

ClickFix surged in 2025 as the most frequent malware loader, tricking users into installing infostealers, ransomware, or remote access trojans (RATs). This sneaky tradecraft speaks volumes about attackers' strategies: abusing user trust beats exploiting vulnerabilities. It's a move toward quieter, more scalable operations, not noisy, exploit-heavy attacks.

Cyberthreats are leveling up—here's how.

Get the Full Report

HUNTRESS | 2026 CYBER THREAT REPORT