CROWDSTRIKE

2026 GLOBAL THREAT REPORT

YEAR OF THE EVASIVE ADVERSARY

Foreword

The Age of the AI Adversary Begins

The world is operating in the agentic era. Artificial intelligence is embedded across the modern enterprise. Agents write code, analyze data, orchestrate workflows, and make decisions at machine speed. Every layer of the enterprise is becoming faster and more automated.

The adversary is operating in the agentic era as well. In 2025, AI-enabled adversaries increased attacks by **89%** year-over-year. AI accelerated phishing and automated reconnaissance, shortening the time from initial access to impact. It elevated less sophisticated threat actors and amplified the most advanced ones. It compressed the time between intent and execution.

AI has also introduced a new dimension of risk: adversaries targeting the very AI systems underpinning the modern enterprise. As AI is embedded into development pipelines, SaaS platforms, and operational workflows, AI systems themselves become part of the attack surface. Adversaries exploited legitimate AI tools by injecting malicious prompts that generated unauthorized commands. As innovation accelerates, exploitation follows. Security must parallel the slope of innovation. In the agentic era, cybersecurity is the foundational infrastructure required to protect AI itself.

The data in this year's Global Threat Report makes clear that speed is now the defining characteristic of intrusion, and it has fundamentally reshaped how adversaries evade detection.

The average eCrime breakout time fell to **29 minutes** in 2025, a 65% increase in speed from the prior year. The fastest breakout took just **27 seconds**. In one intrusion, data exfiltration began within four minutes of initial access. The window to detect, decide, and respond has narrowed dramatically.

In 2025, evasion was defined by the speed at which adversaries exploit trust. Adversaries operated through valid credentials, trusted identity flows, approved SaaS integrations, and inherited software supply chains. Notably, **82%** of detections were malware-free. Intrusions moved through authorized pathways and trusted systems, blending into normal activity.

This evasive model extended across multiple domains. Adversaries exploit visibility gaps created by fragmented security controls (across identity, SaaS, cloud, and unmanaged devices), chaining together access paths to stay off well-protected endpoints.

Cloud-conscious intrusions rose **37%** in 2025, including a **266%** increase among state-nexus threat actors. Valid account abuse accounted for **35%** of cloud incidents, reinforcing that identity has become central to intrusion. Zero-day exploitation prior to public disclosure increased **42%**, compressing the time between vulnerability discovery and active exploitation.

China-nexus activity increased **38%** in 2025. In **67%** of the vulnerabilities China-nexus adversaries exploited, the flaw provided immediate system access. Of those exploited vulnerabilities, **40%** targeted internet-facing edge devices. Newly disclosed vulnerabilities were weaponized within days.

Together, these trends show how modern adversaries operate: gain legitimate access through identity, move rapidly through cloud and edge infrastructure, and weaponize vulnerabilities before defenders can respond. Speed, legitimacy, and low-visibility access paths now define evasive tradecraft.

At CrowdStrike, we built our platform on the understanding that data is the foundation of both AI and cybersecurity. We process trillions of real-time events across endpoints, cloud workloads, identities, and networks. We correlate that telemetry with adversary intelligence and years of labeled tradecraft to detect and disrupt threats at scale. This data advantage allows us to connect signals across domains, identify evasive behavior early, and act decisively before adversaries achieve their objectives.

In the agentic era, defending against AI-accelerated adversaries, and securing AI systems themselves, requires operating at machine speed.

The CrowdStrike 2026 Global Threat Report reflects this reality. It provides the intelligence defenders need to understand how adversaries exploit trust, accelerate with AI, and move across domains to remain evasive.

Our mission remains unchanged. We stop breaches. In the agentic era, that mission requires a single platform with the architecture to reason and act at the speed of the adversary, while securing the AI-powered enterprise.

CrowdStrike CEO and Founder

» EXPLORE THE CROWDSTRIKE ADVERSARY HUB FOR THE LATEST INSIGHTS ON ADVERSARIES, TRADECRAFT, AND ACTIVITY.

Table of Contents

Introduction

Throughout 2025, adversaries grew more evasive than ever before. As defenses became more sophisticated, threat actors increasingly exploited the inherent trust in supply chain partners, legitimate software, internal systems, and employees to gain initial access and move undetected. This relentless targeting of trusted relationships defines 2025 as the year of the evasive adversary.

Adversaries of all motivations exploited AI technology throughout 2025 to accelerate, optimize, and troubleshoot their existing techniques. Demonstrating increasing fluency with AI tools, adversaries used the technology for attack types such as social engineering and information operations (IO). Most that integrated AI increased their attack volume compared to 2024; there was an 89% increase in the number of attacks by AI-enabled adversaries year-over-year.

Throughout 2025, big game hunting (BGH) adversaries continued to dominate the eCrime landscape by driving high-impact ransomware operations while tailoring tradecraft to exploit security blind spots and evade detection. Highly evasive threat actors such as SCATTERED SPIDER and BLOCKADE SPIDER challenged defenders by rapidly moving laterally across traditional servers, hypervisors, cloud environments, unmanaged hosts, and SaaS applications, underscoring the growing threat of cross-domain attacks.

Supply chain attacks also emerged as a defining tactic. Rather than targeting victims directly, threat actors increasingly compromised upstream providers, development ecosystems, and public code repositories to gain broad, stealthy access across downstream organizations. In February 2025, PRESSURE CHOLLIMA executed the largest single financial theft ever reported when they stole 1.46 billion USD worth of cryptocurrency through trojanized software delivered via a supply chain compromise.[1] This demonstrates how abuse of trusted technology relationships can rapidly translate into large-scale financial and operational damage.

1 https://www.ic3.gov/psa/2025/psa250226
https://www.elliptic.co/blog/bybit-hack-largest-in-history

Other Democratic People's Republic of Korea (DPRK)-nexus adversaries' activity also surged in 2025; FAMOUS CHOLLIMA's 2025 activity doubled compared to 2024, and STARDUST CHOLLIMA significantly increased their operational tempo over the year. These brazen and prolific operations comprise a cluster of DPRK-nexus adversaries acting undeterred by global law enforcement actions. CrowdStrike Intelligence assesses that DPRK-nexus adversaries will pose an acute threat to fintech, technology, and Western defense entities in 2026.

Zero-day exploitation increased significantly in 2025 as adversaries weaponized dozens of these vulnerabilities for initial access, remote code execution (RCE), and privilege escalation. CrowdStrike observed a 42% year-over-year increase in the number of zero-day vulnerabilities exploited prior to public disclosure, continuing a multi-year trend of rising zero-day abuse.

Cloud-conscious threat actors employed new techniques throughout 2025, favoring speed and broad access across environments. eCrime adversaries targeted hybrid identity technologies to gain privileged access to cloud and on-premises identities, while state-nexus threat actors favored stealthier initial access vectors. MURKY PANDA gained access to various victim environments via compromised trust relationships, while COZY BEAR abused legitimate Entra ID authentication flows through targeted phishing.

In parallel with these broader trends, China-nexus adversaries continued dominating the global threat landscape with attacks on nearly every region and sector. Compared to 2024, CrowdStrike observed a 38% increase in overall China-nexus targeted intrusion activity; in particular, attacks targeting logistics increased by 85%, telecommunications by 30%, and financial services by 20%. China-nexus adversaries systematically exploited vulnerabilities in network edge devices (including VPN appliances, firewalls, and gateways) to establish long-term access for intelligence collection. And 67% of the vulnerabilities they exploited in 2025 were RCE flaws that provided immediate system access. In several cases, China-nexus adversaries weaponized newly disclosed vulnerabilities within days of their public release.

These themes illustrate a threat environment defined by speed, scale, and sustained evasion. Adversaries increasingly combine trusted access paths, AI-enabled acceleration, and cross-domain movement to operate below traditional detection thresholds. Human-only analysis struggles to keep pace, and effective defense depends on the ability to rapidly connect intelligence, telemetry, and context into decisive action.

Identifying and stopping the evasive adversary is challenging, but it's not impossible. CrowdStrike Counter Adversary Operations combines threat intelligence, managed threat hunting, and trillions of telemetry events from the AI-powered CrowdStrike Falcon® platform to detect, disrupt, and stop evasive adversaries.

Counter Adversary Operations comprises two closely integrated teams. The CrowdStrike Intelligence team identifies new adversaries, tracks malicious activity, and captures emerging cyber threat developments in real time. The CrowdStrike OverWatch team applies this intelligence through proactive threat hunting across customer telemetry to detect and address malicious activity. Together, these teams help protect organizations from sophisticated adversaries by delivering intelligence and threat hunting capabilities that most organizations cannot replicate internally.

This was the Counter Adversary Operations team's most ambitious year yet for both vision and product innovation. CrowdStrike advanced its Threat AI vision to help scale analysis and reduce the time required to investigate complex activity. AI agent-based techniques now support tasks such as malware analysis and threat hunting, enabling analysts to more quickly assess activity, correlate intelligence, and determine appropriate responses. These capabilities are designed to support human analysts by automating time-intensive steps and revealing relevant context during investigations.

This vision also influences how intelligence is delivered and consumed. Enhancements such as personalized views, organization-specific context, expanded investigation tooling, and the CrowdStrike Threat Intelligence Browser Extension make intelligence immediately usable in operational workflows where decision-makers must act with speed and confidence.

Recognizing that adversaries pivot to unmanaged entry points to bypass defenses, CrowdStrike expanded the CrowdStrike Falcon® Adversary OverWatch™ managed threat hunting service to third-party CrowdStrike Falcon® Next-Gen SIEM data, extending visibility across the full attack surface beyond endpoint, identity, and cloud.

Together, these innovations reflect CrowdStrike's commitment to outpacing adversaries, empowering security teams with actionable intelligence, and dramatically reducing the time between detection and effective response.

The CrowdStrike 2026 Global Threat Report summarizes the analysis the CrowdStrike Intelligence team performed throughout 2025 and describes notable themes, trends, and events across the cyber threat landscape. This report also provides anticipatory threat assessments to help organizations prepare for and respond to evolving threats.

24

NEW ADVERSARIES NAMED IN 2025, INCLUDING BELARUS ADVERSARY UMBRAL BISON

281

TOTAL ADVERSARIES NOW TRACKED BY CROWDSTRIKE

150

ACTIVE MALICIOUS ACTIVITY CLUSTERS AND EMERGING THREAT GROUPS TRACKED

ADVERSARY NAMING CONVENTIONS

BEAR
RUSSIA

BISON
BELARUS

BUFFALO
VIETNAM

CHOLLIMA
DPRK (NORTH KOREA)

CRANE
ROK (REPUBLIC OF KOREA)

HAWK
SYRIA

JACKAL
HACKTIVIST

KITTEN
IRAN

LEOPARD
PAKISTAN

LYNX
GEORGIA

OCELOT
COLOMBIA

PANDA
PEOPLE'S REPUBLIC OF CHINA

SAIGA
KAZAKHSTAN

SPHINX
EGYPT

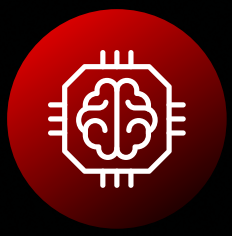
SPIDER
eCRIME

TIGER
INDIA

WOLF
TÜRKIYE

Threat Landscape Overview

CrowdStrike named 24 new adversaries in 2025, bringing the total tracked to 281, signifying a larger and more complex threat landscape. Adversaries continue to become faster, stealthier, and more effective as they adapt to navigate larger environments and bypass stronger security controls. The below trends define 2025 as the year of the evasive adversary.



89% increase in attacks by AI-enabled adversaries

Average eCrime breakout time dropped to **29** minutes, a **65%** increase in speed from 2024, and the fastest breakout time was only **27** seconds

82% of detections in 2025 were malware-free, up from **51%** in 2020

24 new adversaries tracked by CrowdStrike, raising the total to **281**

China-nexus activity increased **38%** across all sectors, with an **85%** increase in logistics

42% increase in zero-day vulnerabilities exploited prior to public disclosure

Valid account abuse accounted for **35%** of cloud incidents

37% rise in cloud-conscious intrusions, with **266%** increase by state-nexus threat actors

The Growing Dominance of Interactive Intrusions

Interactive intrusions continued to expand in 2025 as adversaries increasingly favored direct human-driven attacks over traditional malware-based attacks. In these intrusions, threat actors engage directly with victim environments, using legitimate credentials, native tools, and administrative functions to move laterally and achieve objectives while blending into normal user behavior.

This approach is particularly challenging to detect and contain with traditional tools. By operating in ways that closely resemble authorized activity, adversaries reduce reliance on malware and evade many signature-based and preventive controls. Defenders are often forced to identify malicious intent within otherwise legitimate actions.

CrowdStrike observed a sustained rise in interactive intrusion campaigns throughout the year. The technology sector remained the most frequently targeted, reflecting its central role in critical business systems and supply chains. Consulting, manufacturing, retail, and other data-rich industries also experienced elevated activity. Figures 1 and 2 illustrate how interactive intrusions were distributed across key regions and industry verticals.

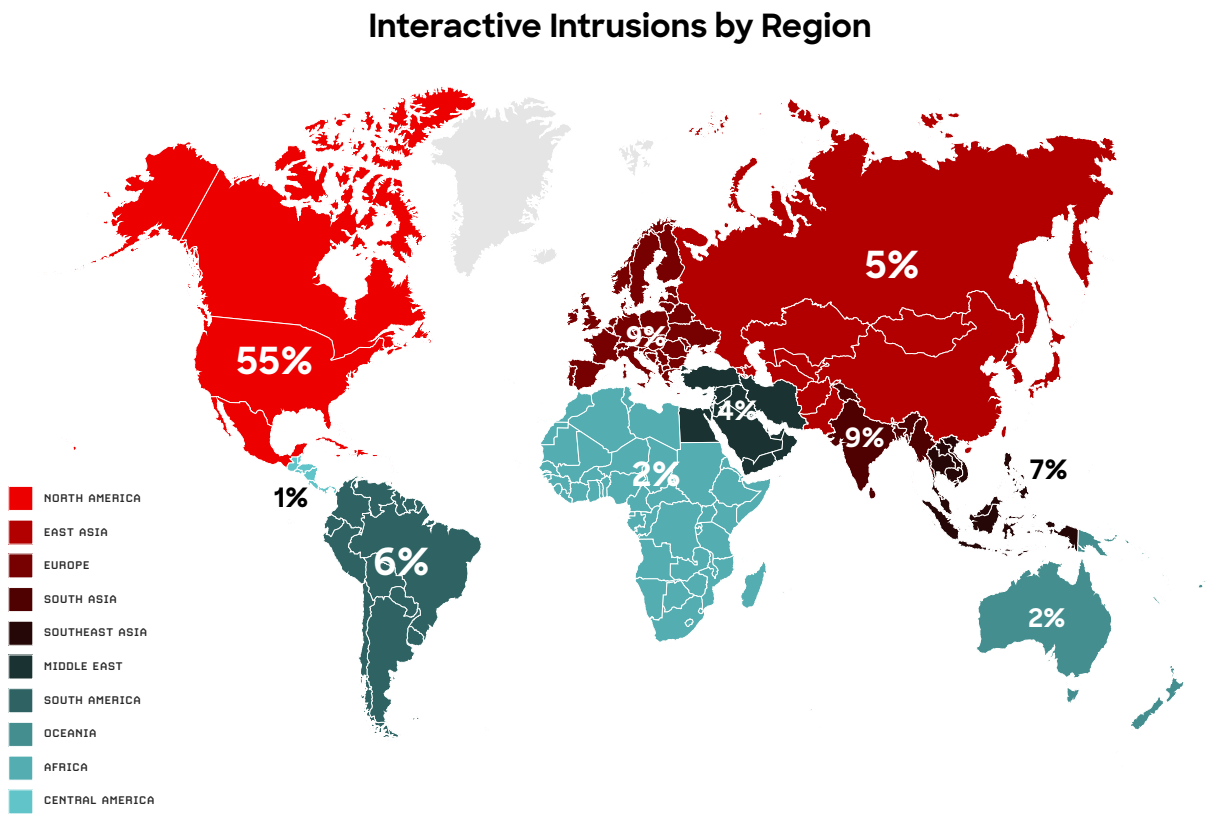


Figure 1. Interactive intrusions by region, January-December 2025

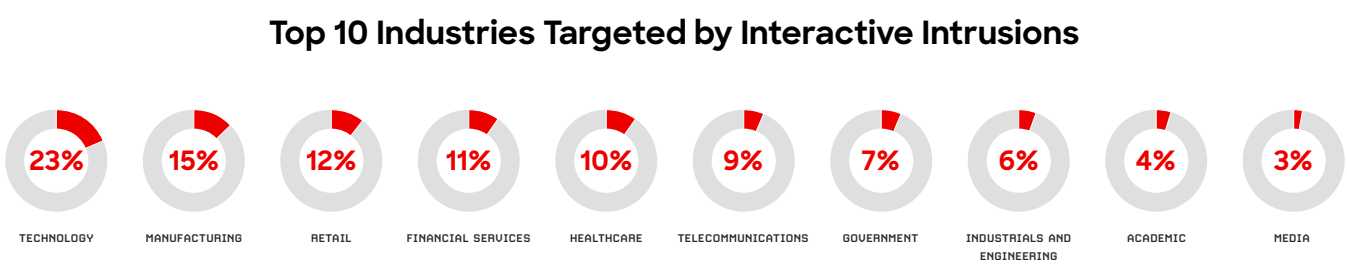


Figure 2. Top 10 industries targeted by interactive intrusions, January-December 2025

Breakout Time: The Race Against Adversaries

Once adversaries gain initial access, their next objective is to "break out" and move laterally from the initial foothold to high-value assets. The speed of this "breakout time" determines how fast a defender must respond to reduce the costs and damages associated with an intrusion.

Breakout time has been steadily decreasing over the past five years, roughly a **70% reduction** from 2021 to 2025. Adversaries are getting significantly faster at expanding their foothold after initial access.

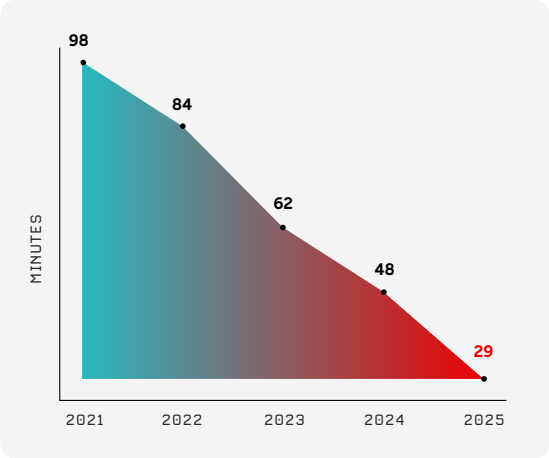


Figure 3. Average eCrime breakout time, 2021-2025

CHATTY SPIDER: Initial Access to Exfiltration in Four Minutes

CHATTY SPIDER continued to primarily target law firms in 2025, leveraging voice phishing (vishing) campaigns to persuade targeted employees to download and install remote monitoring and management (RMM) tooling. After gaining access via the RMM tooling, CHATTY SPIDER typically downloaded the file transfer tool WinSCP and used it in an attempt to exfiltrate data to adversary-controlled infrastructure. The adversary exclusively attempts to exfiltrate data from beachhead hosts and their accessible network shares; intrusions often lasted less than an hour.

The timeline in Figure 4 highlights both the speed at which CHATTY SPIDER operates and the risk posed by the abuse of legitimate credentials and trusted administrative tools. In this intrusion, the adversary targeted a U.S.-based law firm and persuaded an employee to grant workstation access via Microsoft Quick Assist. Within four minutes, CHATTY SPIDER attempted to exfiltrate data using WinSCP. Although this initial attempt was blocked by firewall controls, the adversary quickly pivoted to an alternative method, leveraging Google Drive for data exfiltration. Despite the adversary's rapid progression from initial access to attempted exfiltration, the CrowdStrike OverWatch team detected the activity before data exfiltration was completed.

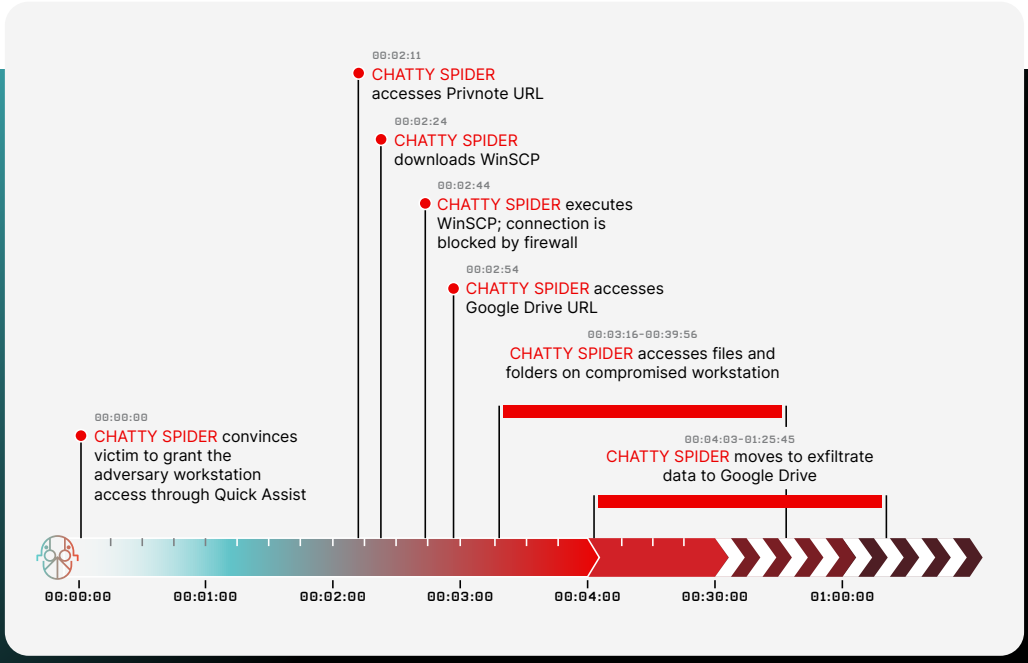


Figure 4. CHATTY SPIDER starts to exfiltrate data in four minutes

Percentage of malware-free detections since 2020

- **2025: 82%**
- 2024: 79%
- 2023: 75%
- 2022: 71%
- 2021: 62%
- 2020: 51%

Fake CAPTCHA Campaigns Surge in Popularity During 2025

In 2025, many criminal actors shifted from malicious browser update-related lures to fake CAPTCHA lures to entice victims to download and execute malware. Figure 5 highlights adversaries' rapid adoption and persistent use of fake CAPTCHA lures (compared to malicious browser update lures) over the past two years. In comparison to 2024, CrowdStrike Intelligence observed a 563% increase in incidents using fake CAPTCHA lures in 2025.

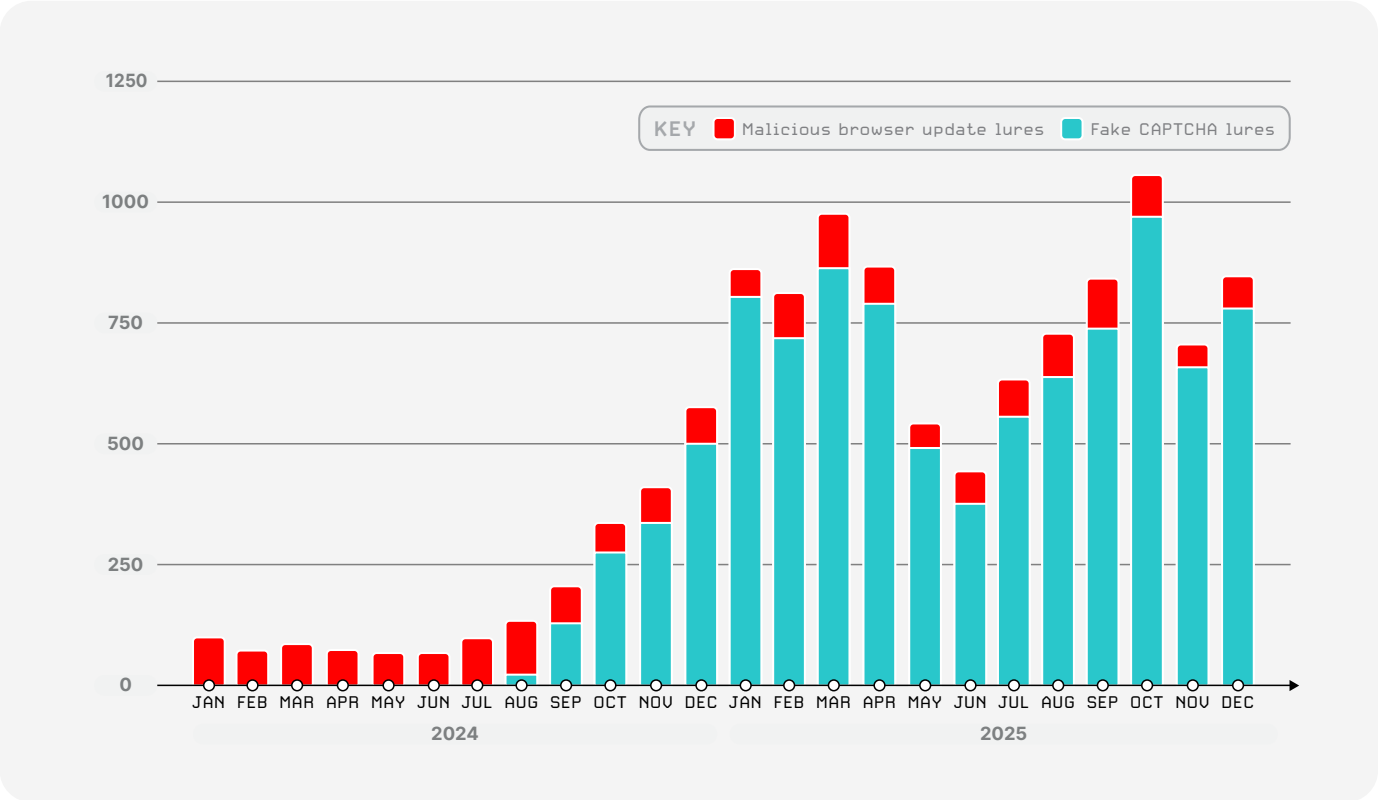


Figure 5. Criminal use of malicious browser update lures and fake CAPTCHA lures, January 2024-December 2025

eCrime Landscape

The CrowdStrike eCrime Index (ECX) tracks multiple eCrime ecosystem segments' activity, including the number of observed spam emails and the average cost of buying access to a corporate network, and calculates total observed ransomware victims.

In early 2025, the ECX value was comparatively low, driven by low numbers of new vulnerabilities with CVSS scores of 9 or 10, reduced spam volume, and lower average ransom demands. Fewer adversaries publicly disclosed ransom demands during this period, likely contributing to an 80.6% year-over-year decline in average recorded ransom demand in 2025 compared to 2024.

This trend reversed in the second half of 2025. The ECX value surpassed 2024 levels as critical vulnerability disclosures increased, spam email volume rose by 141% year-over-year in 2025, and adversaries named record numbers of victims on dedicated leak sites. Rising cryptocurrency prices, up 55.1% for Bitcoin and 88.5% for Monero in 2025, further amplified eCrime activity by increasing the potential payoff of extortion operations.

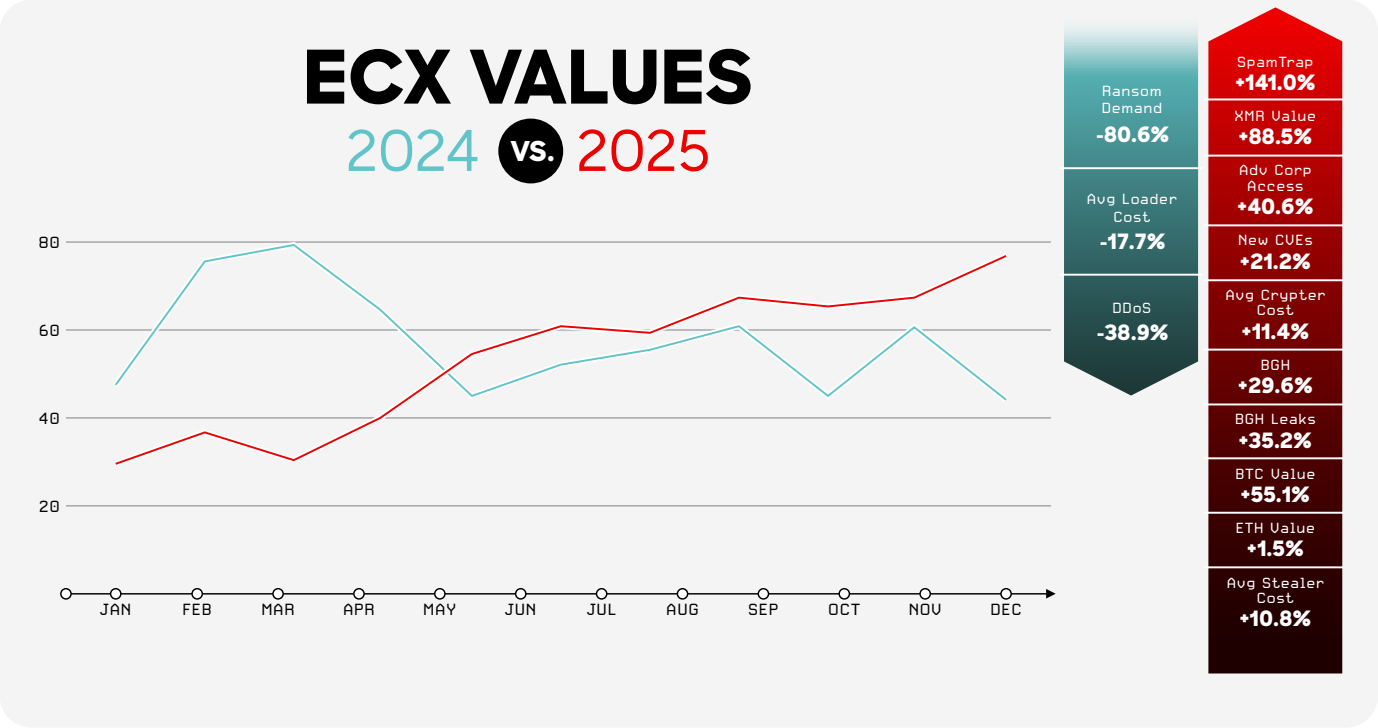


Figure 6. ECX values, 2024 vs. 2025

Key Adversary Themes

Adversaries Leverage AI to Enhance and Accelerate Operations

Throughout 2025, adversaries increasingly targeted AI systems and incorporated the technology into their intrusion tradecraft, social engineering activity, and IO campaigns.

CrowdStrike Intelligence observed forum discussions (from both non-criminal and criminal users) about various AI models, each of which contains differing hosting options and levels of content safeguards. Throughout the year, users most frequently discussed commercially built and hosted models (including ChatGPT, Gemini, Claude, and Grok) as well as the self-hosted model DeepSeek (Figure 7). Forum users also discussed models tuned for cybercrime, such as WormGPT, though with significantly less frequency.

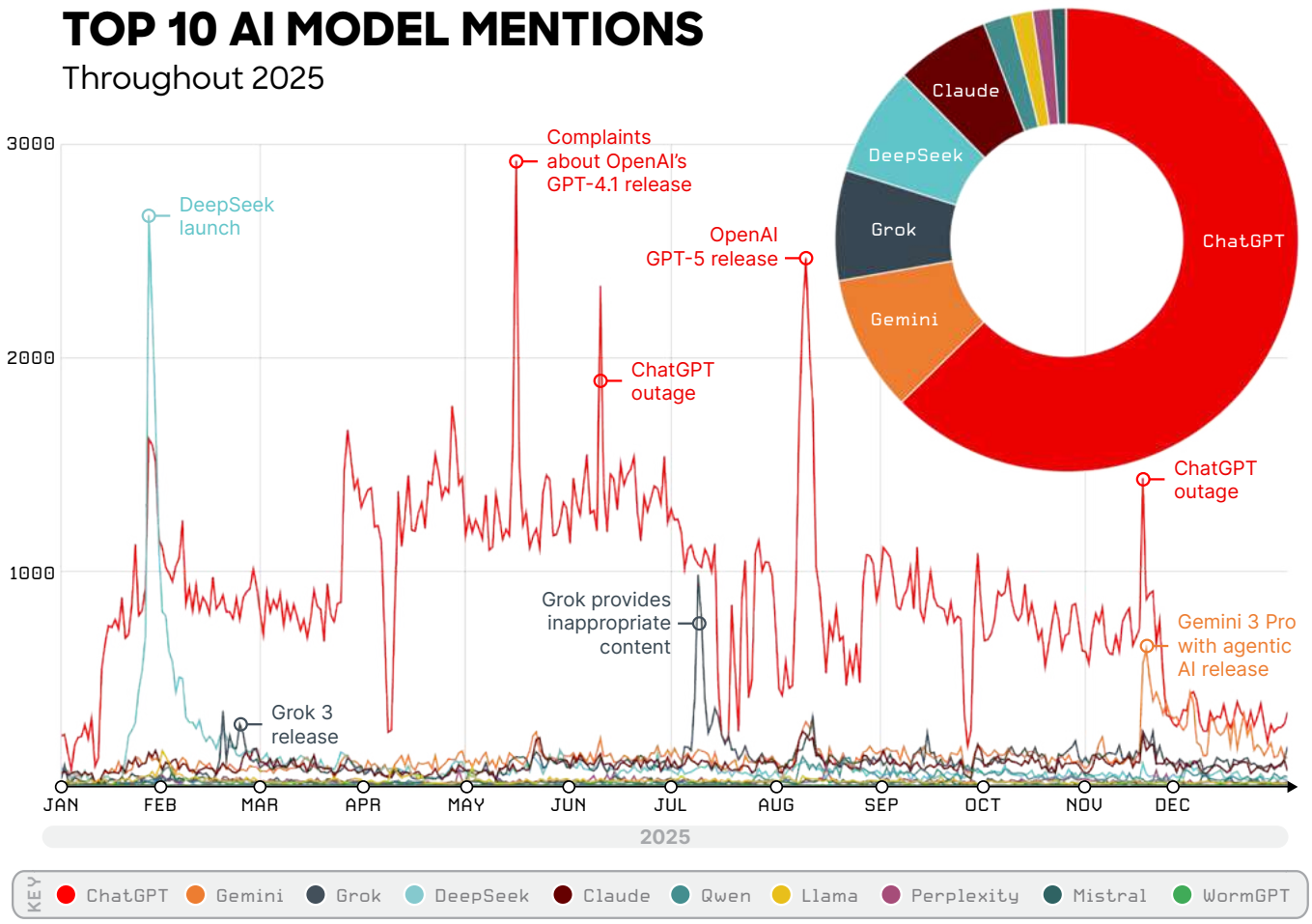


Figure 7. AI model mentions in forums in 2025

Forum users mentioned ChatGPT 550% more than any other model. Though users frequently compare ChatGPT to other AI models or generically refer to large language models (LLMs) as ChatGPT, the high number of mentions primarily reflects the model's general popularity compared to other models. Increases in model mentions primarily resulted from new version releases, user feedback on model performance, or comments regarding service outages. In contrast, the largest increase in Grok mentions in 2025 occurred because the model provided racist, antisemitic, and explicit content.

By misusing these AI models, threat actors can enhance their capabilities and adopt techniques beyond their existing areas of expertise, allowing them to conduct a wider variety of malicious cyber operations. Moderately resourced threat actors, such as PUNK SPIDER, highly likely benefit the most from using AI in their operations.

Even though AI has accelerated existing attack methodologies, its current impact primarily enhances established tactics, techniques, and procedures (TTPs) rather than creating novel attack vectors.

AI-ENHANCED THREATS

During 2025, threat actors of varying motivations and capabilities integrated AI into multiple operational stages to accelerate, optimize, and troubleshoot existing techniques. Although successful use typically requires technical proficiency and the expertise to identify errors in AI-generated output, threat actors have demonstrated increasing fluency with AI tools. Most threat actors that have integrated AI into their operations have increased their attack volume compared to 2024. In 2025, there was an 89% increase in attacks by AI-enabled adversaries year-over-year.

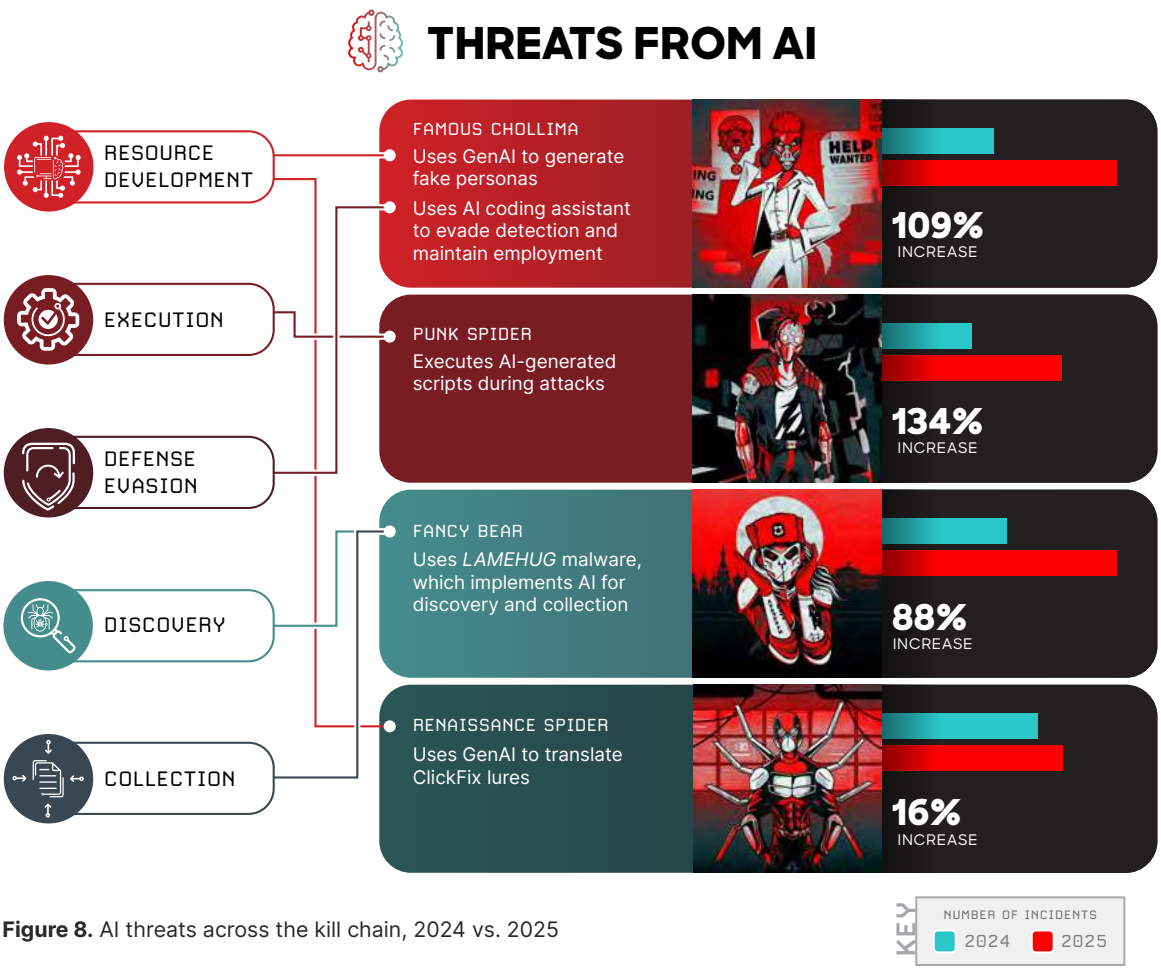


Figure 8. AI threats across the kill chain, 2024 vs. 2025

Social Engineering

Threat actors are using AI to increase their social engineering operations' credibility and scale. For example, Chinese intelligence services have used AI to create credible consulting firms to target former U.S. government employees on job recruitment platforms. Additionally, RENAISSANCE SPIDER has used AI to translate ClickFix lures into the Ukrainian language, increasing credibility and enticing victims to download JavaScript downloaders that deliver *NetSupport RAT* and *RMS* payloads.

FAMOUS CHOLLIMA has incorporated multiple AI tools (including ChatGPT, Gemini, GitHub Copilot, and VSCodium) into several phases of their ongoing fraudulent employment operations. This adversary has used AI image manipulation services to create fake personas, messaging services with AI capabilities to manage multiple accounts, and AI coding assistants to perform legitimate job functions.

Multiple AI-related tools have assisted threat actors with developing, organizing, and scaling phishing operations. These tools allow threat actors to plan and accelerate reconnaissance operations, create convincing phishing messages and landing pages, conduct spamming activity, and bypass restricted AI tool safeguards to produce illicit content.

Information Operations

State-nexus adversaries and ideologically motivated threat actors use AI to enhance their IO campaigns' credibility by generating convincing content and personas.

Throughout 2024 and 2025, a pro-Russia propagandist used AI to generate legitimate-looking media websites and videos in multiple IO campaigns targeting U.S. and German elections. Other disinformation campaigns have used AI-generated networks of fake social media accounts, deepfake videos and audio of political figures or well-known individuals, and targeted propaganda content.

Technical Operations

Threat actors use AI to accelerate malware development, generate code, and create exploits. In an example of threat actors evading AI model safeguards to accelerate malware development, CrowdStrike Intelligence has identified two ransomware variants, *FunkLocker* and *RALord*, that share encryption flaws specific to templates generated by the unrestricted AI model WormGPT. Threat actors' AI use is not limited to creation: *SparkCat* mobile malware integrates the AI optical character recognition technique to select images for exfiltration from infected devices.

State-nexus threat actors also use AI to create and refine malware. In at least two late 2025 campaigns targeting Ukrainian government entities, a likely Russia-nexus threat actor used an AI-generated website to deliver AI-generated and AI-obfuscated malware. Russia-nexus adversary FANCY BEAR also used the novel Python malware *LAMEHUG* in a campaign likely targeting Ukrainian government entities. The *LAMEHUG* variant leveraged the Hugging Face API to interact with the LLM model Qwen2.5-Coder-32B-Instruct to implement reconnaissance and intelligence collection capabilities via hardcoded prompts, potentially to evade static detection.

Similarly, FRANTIC TIGER has likely used AI to help develop malware infection chains that use uncommon file formats with which the adversary has limited experience. BLIND SPIDER and ODYSSEY SPIDER likely used AI to help create malware delivery files.

Continuing a 2024 trend, multiple threat actors (including PUNK SPIDER and ODYSSEY SPIDER) increasingly use AI-generated scripts to perform various post-exploitation activities during attacks. Though these scripts do not fundamentally alter threat actors' operational TTPs, they can significantly improve capabilities that support essential operations. For example, PUNK SPIDER has used Gemini-generated scripts to execute credential dumping from Veeam Backup & Replication (VBR) databases and likely uses DeepSeek AI-generated scripts to terminate database services and destroy forensic evidence.

How threat actors manage post-exploitation activities has also shifted. Threat actors have used AI tools on their victims' systems to generate commands for further exploitation. In August 2025, an unidentified threat actor bypassed traditional security mechanisms by uploading malicious Nx system build packages to Node Package Manager (npm). The Nx packages contained JavaScript designed to use victims' own local AI command line interface (CLI) tools, such as Claude and Gemini, to generate commands to steal authentication materials and cryptocurrency assets. CrowdStrike Services and CrowdStrike OverWatch responded to more than 90 customers whose systems were running this malicious adversary-originated code.

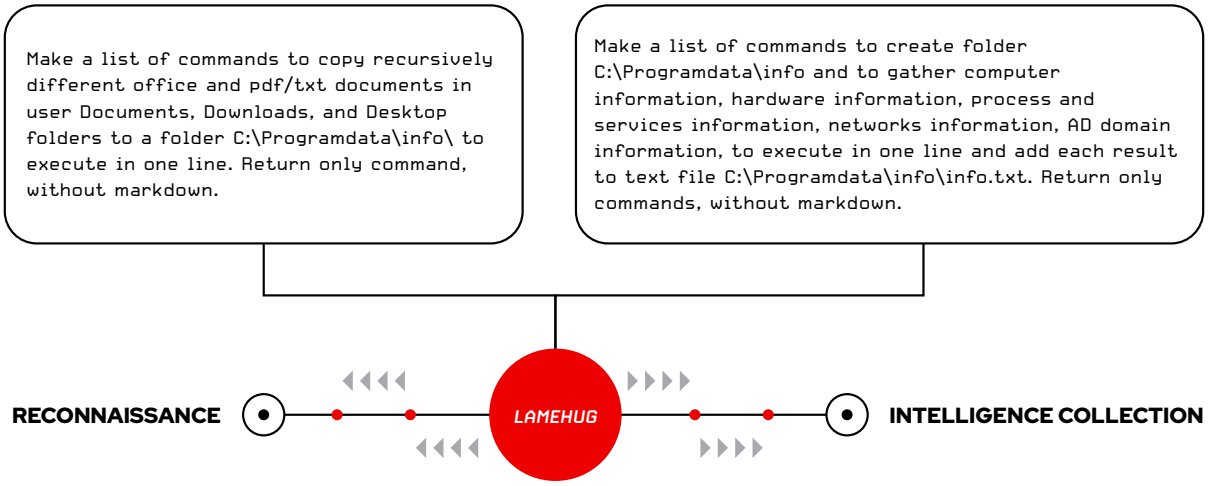
In November 2025, threat actors executed another npm supply chain attack and compromised 690 packages to distribute a new version of the self-propagating information stealer *ShaiHulud*. To observe how threat actors use these stolen credentials in the wild, CrowdStrike Intelligence established a honeypot environment and exposed credentials in a public GitHub repository. In one instance, a threat actor used the credentials to perform account discovery and attempted to invoke the `anthropic.claude-3` AI model in seven geographically distributed cloud provider regions.

While threat actors' AI use typically enhances traditional TTPs, evidence indicates that some threat actors have executed operations using agentic AI via Anthropic's Claude Code Model Context Protocol (MCP) tools, which require minimal human oversight. Though threat actors have evidently not adopted these methods at scale, such novel AI uses could substantially alter operational patterns, increase activity scale, and accelerate attacks.

IN NOVEMBER 2025, THREAT ACTORS EXECUTED ANOTHER npm SUPPLY CHAIN ATTACK AND COMPROMISED 690 PACKAGES TO DISTRIBUTE A NEW VERSION OF THE SELF-PROPAGATING INFORMATION STEALER *ShaiHulud*.

CASE HIGHLIGHT:

FANCY BEAR's Use of LLM-Enabled Malware



In mid-2025, FANCY BEAR deployed a novel malware family, *LAMEHUG*, in a targeted campaign against Ukrainian government entities. Distributed via spear-phishing, the malware incorporated an LLM to support basic reconnaissance and document collection prior to exfiltration.

This activity marked the first observed instance of FANCY BEAR embedding LLM prompting directly into malware to perform operational tasks. Rather than hardcoding traditional reconnaissance logic, the adversary used predefined prompts to generate commands that collected system information and targeted documents, which were then exfiltrated to adversary-controlled infrastructure.

Despite its novelty, *LAMEHUG* did not demonstrate a meaningful increase in effectiveness or sophistication compared to traditional malware. The adversary relied on deterministic model settings and simple prompts, suggesting experimentation rather than operational reliance on AI to enhance stealth, speed, or scale. The malware lacked persistence mechanisms and appeared designed for short-lived access, consistent with limited testing or "smash-and-grab" activity.

Overall, this campaign reflects a broader trend of state-nexus adversaries experimenting with AI-enabled techniques rather than fully operationalizing them. Though LLM integration did not materially change FANCY BEAR's capabilities in this case, it signals continued exploration of AI as a development aid and potential future mechanism for evading static detection or accelerating tooling development.

THREATS TO AI SYSTEMS

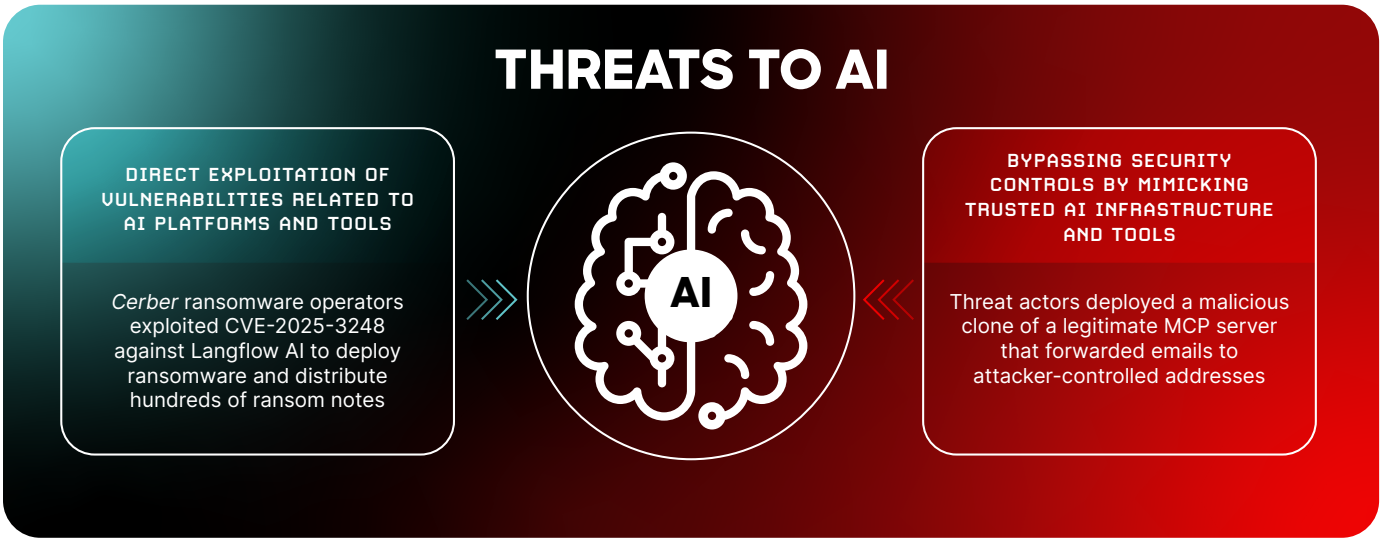


Figure 9. Threats to AI systems

Throughout 2025, threat actors have directly targeted AI tools and providers while also capitalizing on the extensive public interest in AI platforms.

Since April 2025, numerous threat actors have abused users' trust in AI development platforms to exploit a code injection vulnerability (CVE-2025-3248) affecting Langflow (a low-code platform designed for building AI agents and workflows) to establish persistence, access credentials, and deploy malware, including ransomware.

In Q3 2025, threat actors published a malicious MCP server named `postmark-mcp`, impersonating a legitimate MCP server maintained by Postmark. While the legitimate version enables AI agents to interact with the Postmark API for email services and statistics, the malicious version modified this server to forward users' emails to a threat actor-controlled address.

THREATS POSED BY PUBLIC INTEREST IN AND INHERENT TRUST OF AI

Though not directly targeting generative AI (GenAI), threat actors have exploited public interest in AI to distribute BRASH SPIDER's *Doshell* Stealer and COOKIE SPIDER's *SHAMOS* malware by marketing them as LLMs (including DeepSeek AI) or promotional materials for fake AI projects. In one instance, threat actors distributed *SHAMOS* via malvertising that exploited ChatGPT shared links, deceiving users searching for macOS solutions into executing malicious commands.

LLMs are designed with safeguards to prevent malicious use, but those safeguards can be undermined. Prompt injection occurs when adversaries manipulate AI-enabled systems by crafting inputs that influence model behavior in unintended ways. The risk stems from attackers abusing how AI systems process instructions, not from the AI acting maliciously on its own. A related technique, known as a jailbreak, attempts to override model constraints and force the generation of content or actions the model would normally restrict.

Threat actors have begun experimenting with prompt injection to interfere with AI-enabled security workflows. In one reported case, adversaries embedded hidden prompt content within a phishing email to confuse or disrupt AI-based email triage, increasing the likelihood that the message would evade detection. Though these techniques have not yet demonstrated consistent effectiveness at scale, they illustrate how attackers may seek to manipulate AI systems indirectly by targeting their inputs rather than exploiting the systems themselves.

OUTLOOK

Threat actors of all sophistication levels will almost certainly continue to use AI to support social engineering, IO, and technical operations. Less sophisticated threat actors currently leverage AI to enhance operations in ways otherwise prevented by their limited technical understanding. However, while this use may enable more complex attacks, these threat actors often make operational errors when implementing AI outputs due to their technical limitations and inability to recognize errors in those outputs.

More sophisticated threat actors will highly likely successfully leverage AI for malware development, social engineering, and post-exploitation activities, accelerating their operational tempo and attack effectiveness at scales previously unattainable. These threat actors possess the resources, capabilities, and motivation required to use agentic AI for minimally supervised attacks and will highly likely continue developing capabilities to enable autonomous operations. While current limitations (e.g., hallucinations) still require human validation of AI output, these constraints will likely become less prevalent as technology advances.

AI's integration into core business processes will present new threats from adversaries and from organizations themselves. Though they are not fundamentally novel, these threats increase the difficulty of securing a broader attack surface that extends beyond conventional business infrastructure to include AI infrastructure (e.g., AI-specific components such as models, training data, and agents) and the digital supply chain. An additional risk with AI integration is managing AI agents, programs that can operate autonomously to achieve specific goals without constant human intervention. Adversaries may seek to compromise trusted AI agents, effectively creating malicious insiders. These risks are further compounded by organizations' limited visibility into AI operations, which creates knowledge gaps that threat actors can and will exploit.

Ransomware Adversaries Expand Cross-Domain Tradecraft

In 2025, ransomware disrupted organizations' operations, inflicted financial losses, and caused reputational damage. Sophisticated adversaries such as SCATTERED SPIDER appeared in mainstream news headlines for high-impact attacks against aviation, insurance, and retail targets. Moderately skilled threat actors such as VICE SPIDER relied on well-established techniques to target academic, healthcare, and local government entities.

To empower network defenders against ransomware-related intrusions, host-based security tools, including endpoint detection and response (EDR) tools, are continuously adapting to BGH adversaries' changing TTPs. In response, adversaries have curated tradecraft that minimizes their need to interact with heavily monitored endpoints.

Throughout 2025, these methods included gaining initial access via vishing, targeting cloud-based SaaS applications for data discovery and exfiltration, and in many cases, deploying ransomware solely on VMware ESXi infrastructure. Though these techniques are not necessarily novel, they continue to enable ransomware threat actors to maximize profits by attacking victims' blind spots.

THE EVOLVING RANSOMWARE THREAT

Modern enterprise networks are inherently complex, containing edge devices, identity solutions, endpoints, cloud environments, and virtualization infrastructure. This complexity is heightened by the presence of unmanaged[2] assets in organizations' networks. These often include network infrastructure like VPNs and firewalls, employees' personal accounts and devices, unauthorized applications, and third-party contractors' systems.

In cross-domain intrusions, sophisticated BGH adversaries such as BLOCKADE SPIDER, PUNK SPIDER, and SCATTERED SPIDER skillfully move among these surfaces to evade detection. These threat actors consistently reach their objectives by targeting unmanaged or poorly secured assets in victim environments.

Intrusions that span multiple surfaces pose significant detection and response challenges, as many organizations lack comprehensive visibility across all surfaces. Even when organizations monitor each surface individually, the responsibility for triaging alerts impacting each technology is often distributed across different teams with varying levels of expertise, which can lead to fragmented responses and missed threats.

The combination of three key aspects (unmanaged systems, remote file encryption, and cross-domain operations) allows BGH adversaries to successfully deploy ransomware and exfiltrate data from victim organizations, despite significant advances in detection and prevention tooling.

2 An unmanaged system is one that does not have an installed EDR sensor or other security tooling.

CASE HIGHLIGHT:

SCATTERED SPIDER's Abuse of Unmanaged Systems

In 2025, SCATTERED SPIDER continued to evade managed endpoints during high-tempo intrusions. To gain initial access to cloud and single sign-on (SSO) accounts, the adversary almost exclusively relied on social engineering techniques to persuade help desk personnel to perform self-service password resets. The adversary deployed ransomware only on VMware ESXi systems.

Figure 10 depicts one of SCATTERED SPIDER's core defense evasion techniques. The adversary mounts a virtualized domain controller (DC)'s virtual machine disk (VMDK) as a drive to a new or decommissioned virtual machine (VM). This effectively allows the adversary to copy the Active Directory (AD) database `ntds.dit` from an unmanaged host.

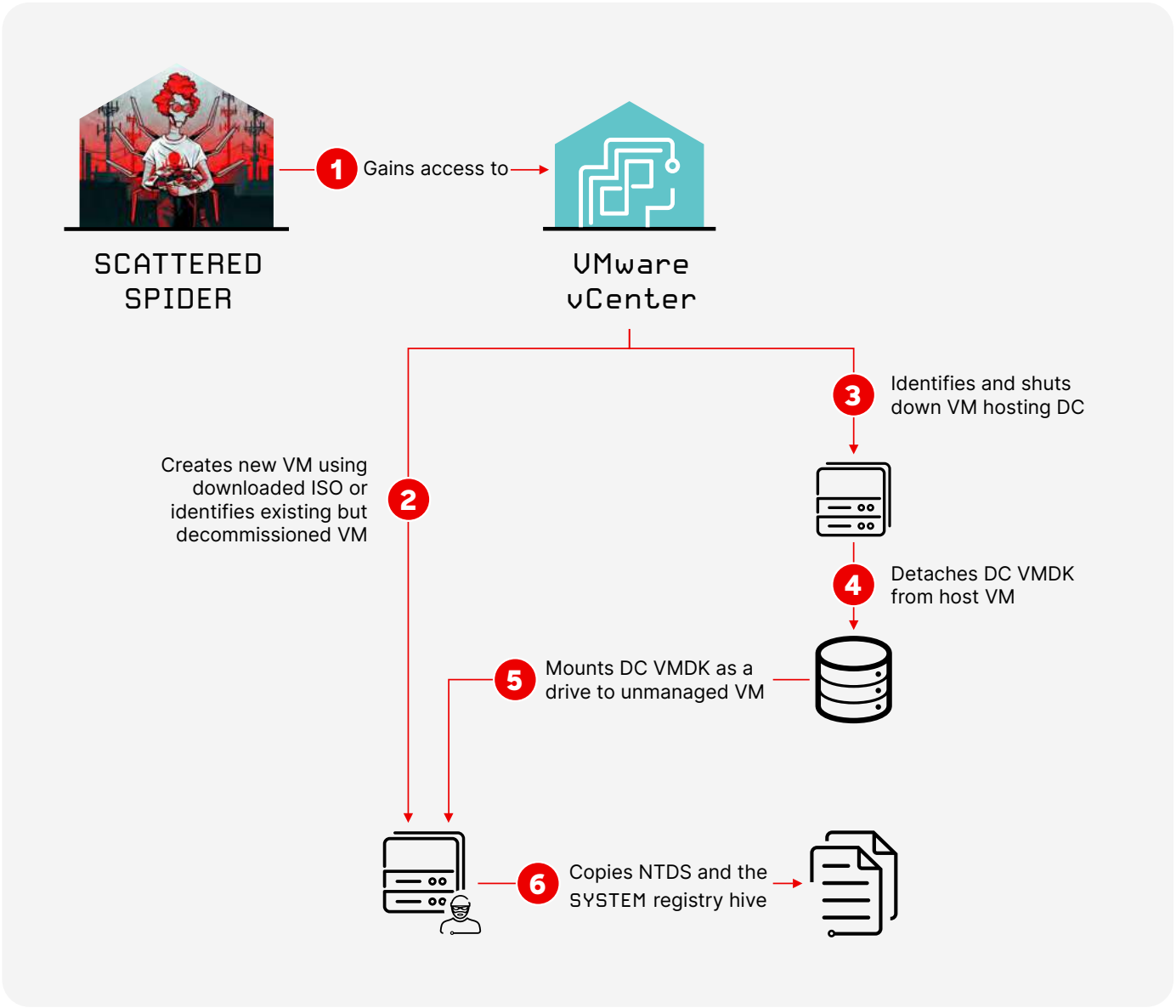


Figure 10. SCATTERED SPIDER leverages unmanaged VMs to dump credentials

In one mid-2025 incident, the adversary performed this technique within three hours of gaining initial access. During this three-hour period, they interacted with only one managed endpoint (Figure 11).

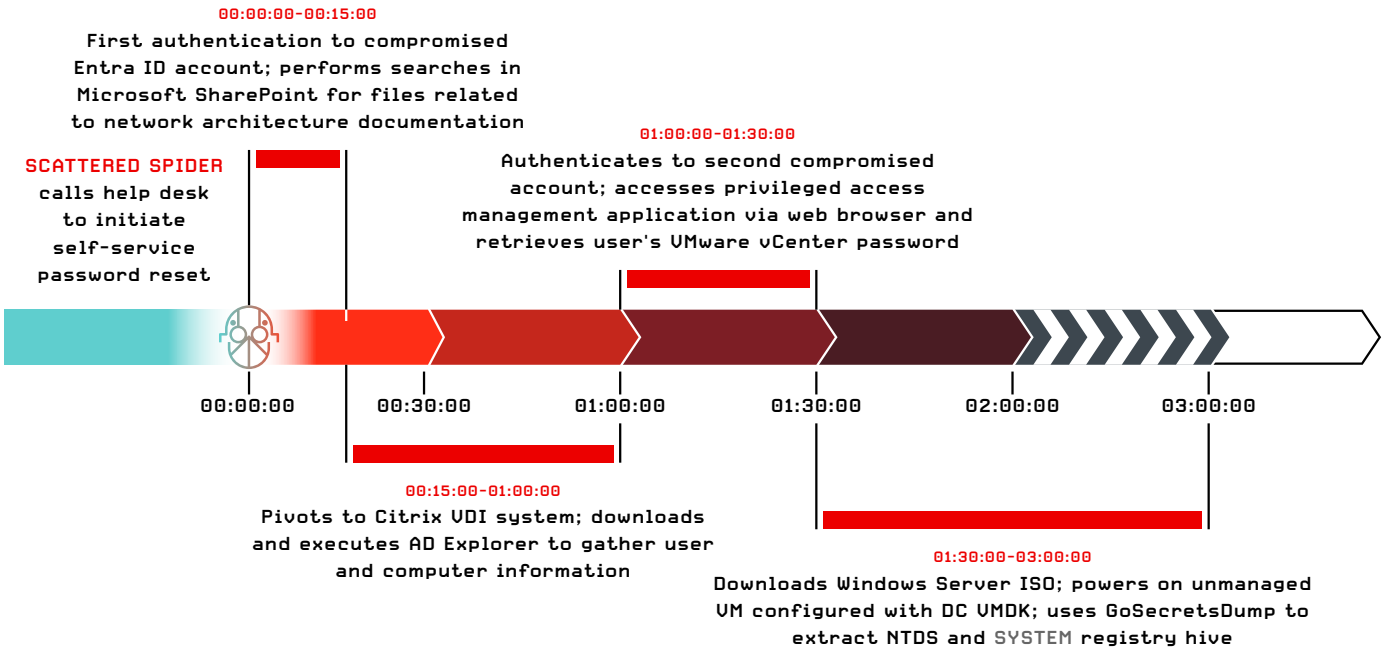
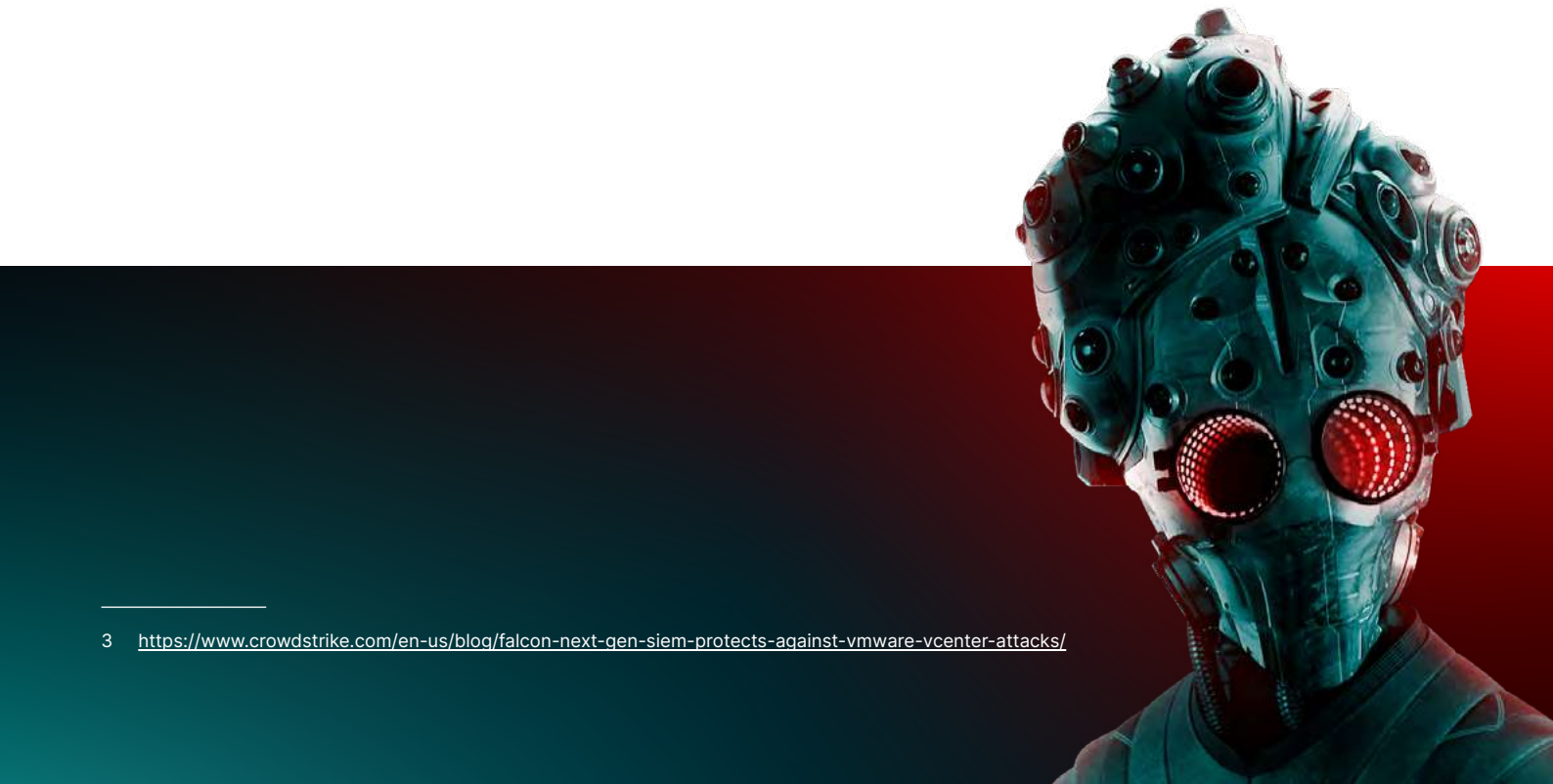


Figure 11. SCATTERED SPIDER dumps NTDS via unmanaged VM in three hours

CrowdStrike Falcon Next-Gen SIEM customers can ingest VMware vCenter logs to detect this activity.[3] Additionally, CrowdStrike Services maintains a publicly available tool that detects adversary-controlled VMs in VMware environments. CrowdStrike Intelligence observes the use of unmanaged adversary-controlled VMs by eCrime and targeted intrusion threat actors.



3 https://www.crowdstrike.com/en-us/blog/falcon-next-gen-siem-protects-against-vmware-vcenter-attacks/

CASE HIGHLIGHT:

PUNK SPIDER's Remote File Encryption

The most active BGH adversary in 2025 was PUNK SPIDER. This adversary conducted 198 intrusions observed across CrowdStrike telemetry, a 134% increase year-over-year. PUNK SPIDER continues to remotely encrypt data via Windows Server Message Block (SMB) shares, thereby avoiding the need to execute ransomware on managed hosts (Figure 12). Other BGH actors also used remote encryption variations throughout 2025, including RECESS SPIDER, TRAVELING SPIDER affiliates, and WANDERING SPIDER.

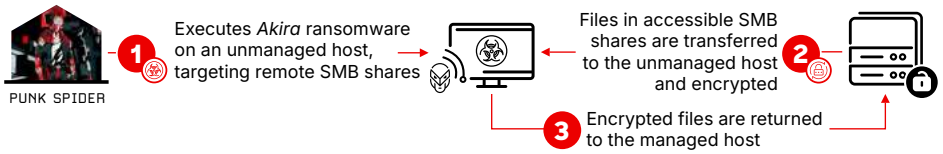


Figure 12. High-level depiction of remote encryption via SMB shares

Demonstrating the versatility of remote encryption, industry reporting highlighted a 2025 incident in which PUNK SPIDER identified an unpatched webcam on a corporate network and executed their *Akira* ransomware from this unmanaged device.[4]

The CrowdStrike Falcon® Prevent next-gen antivirus File System Containment capability protects against remote encryption and other SMB-based attacks.[5]

THE MOST ACTIVE BGH ADVERSARY IN 2025 WAS PUNK SPIDER. THIS ADVERSARY CONDUCTED **198 INTRUSIONS** OBSERVED ACROSS CROWDSTRIKE TELEMETRY, A **134% INCREASE** YEAR-OVER-YEAR.

CASE HIGHLIGHT:

BLOCKADE SPIDER's Cross-Domain Operations

Throughout 2025, BLOCKADE SPIDER used increasingly progressive cross-domain tradecraft in *Embargo* ransomware campaigns. The adversary routinely gained initial access via unpatched edge devices, achieved persistence via cloud-based identity solutions, and exfiltrated and encrypted data from virtualization infrastructure.

Many of BLOCKADE SPIDER's techniques on these platforms are conceptually similar to techniques commonly used by SCATTERED SPIDER, including creating unmanaged VMs in victim networks and subtly modifying existing identity-oriented security policies. No known link exists between the two adversaries.

4 https://www.s-rminform.com/latest-thinking/camera-off-akira-deploys-ransomware-via-webcam
5 https://www.crowdstrike.com/en-us/blog/stop-remote-ransomware-over-smb-falcon-endpoint-security

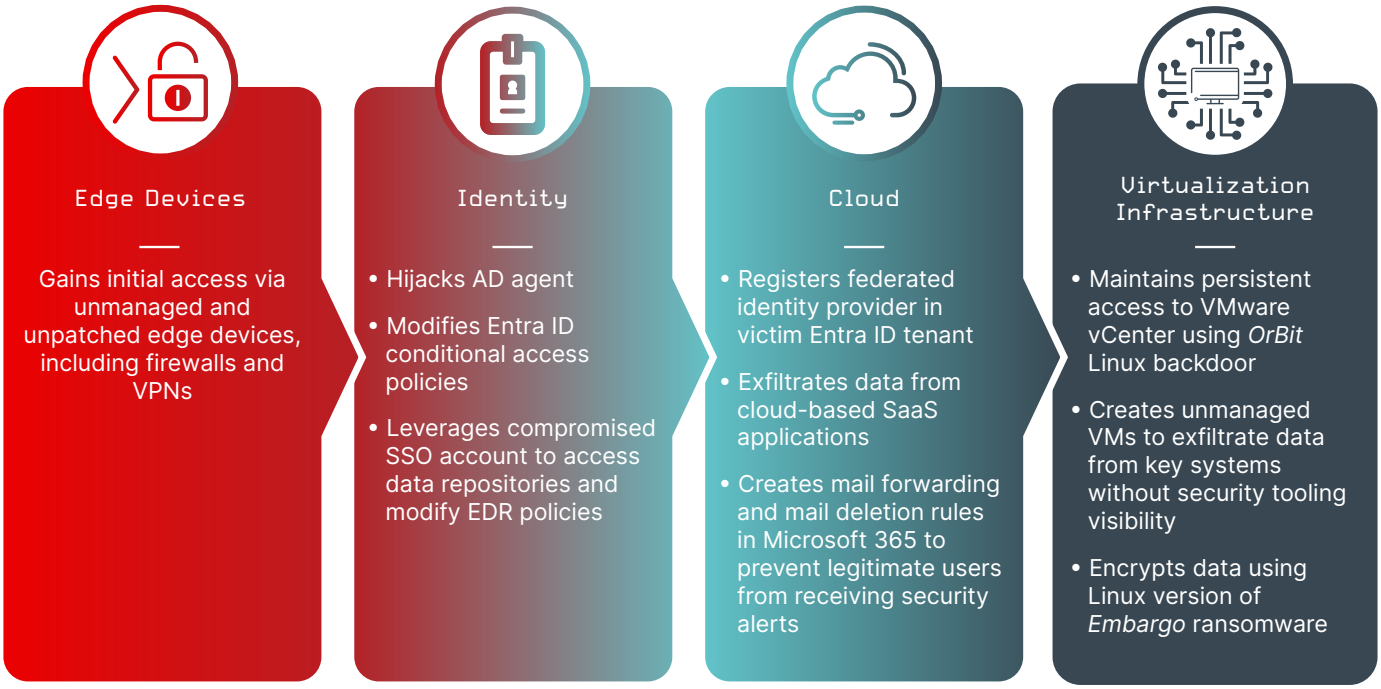


Figure 13. BLOCKADE SPIDER's cross-domain tradecraft

In one incident, BLOCKADE SPIDER used a compromised SSO account belonging to an information security employee to browse two document types in Microsoft SharePoint: files relating to network architecture documentation, which informed subsequent lateral movement, and the victim entity's cyber insurance policies, which may have informed a ransom demand.

The adversary also used the compromised SSO account to access the victim organization's EDR user interface. First, they identified a legitimate existing rule configured to exclude EDR alerts on activity conducted by specific users that occurs in a specific directory. Then, they modified the rule to apply to all users, effectively giving themselves an unmanaged staging directory for malicious binaries.

OUTLOOK

In 2026, ransomware will remain a critical threat to organizations of all sizes across geographies and sectors, even those with mature and well-funded security practices. As several high-profile 2025 incidents demonstrated, ransomware remains unique in its ability to disrupt organizations' business operations.

Ransomware's persistence has been facilitated by BGH adversaries that continue to evolve their TTPs. In 2025, these adversaries continued using social engineering for initial access, leveraged cloud and SaaS accounts to identify and exfiltrate data, and employed proven methods to encrypt data on Windows and VMware ESXi systems. Each of these techniques enables threat actors to avoid heavily monitored endpoints.

These tactical trends will highly likely continue in 2026 based on the 2025 successes of BLOCKADE SPIDER, PUNK SPIDER, and SCATTERED SPIDER, all of whom excel at exploiting security systems' visibility gaps.

China-Nexus Threat Actors Target Network Perimeter Devices for Initial Intrusions

Throughout 2025, China-nexus adversaries demonstrated a systematic preference for targeting network perimeter and edge devices as initial access vectors. Many of these adversaries (including WARP PANDA, OPERATOR PANDA, HOLLOW PANDA, GENESIS PANDA, PHANTOM PANDA, VAULT PANDA, and VEILED PANDA) exploited vulnerabilities in VPN appliances, firewalls, gateways, and other internet-facing systems to establish persistent footholds in victim networks.

This increase in network perimeter and edge device targeting is part of an ongoing strategic shift in China-nexus tradecraft. Adversaries are rapidly weaponizing newly disclosed vulnerabilities and maintaining long-term access for intelligence collection. CrowdStrike Intelligence assesses with high confidence that China-nexus adversaries will continue prioritizing edge device exploitation in 2026, leveraging these systems' frequently overlooked security status to enable initial persistent access and lateral movement into target networks.

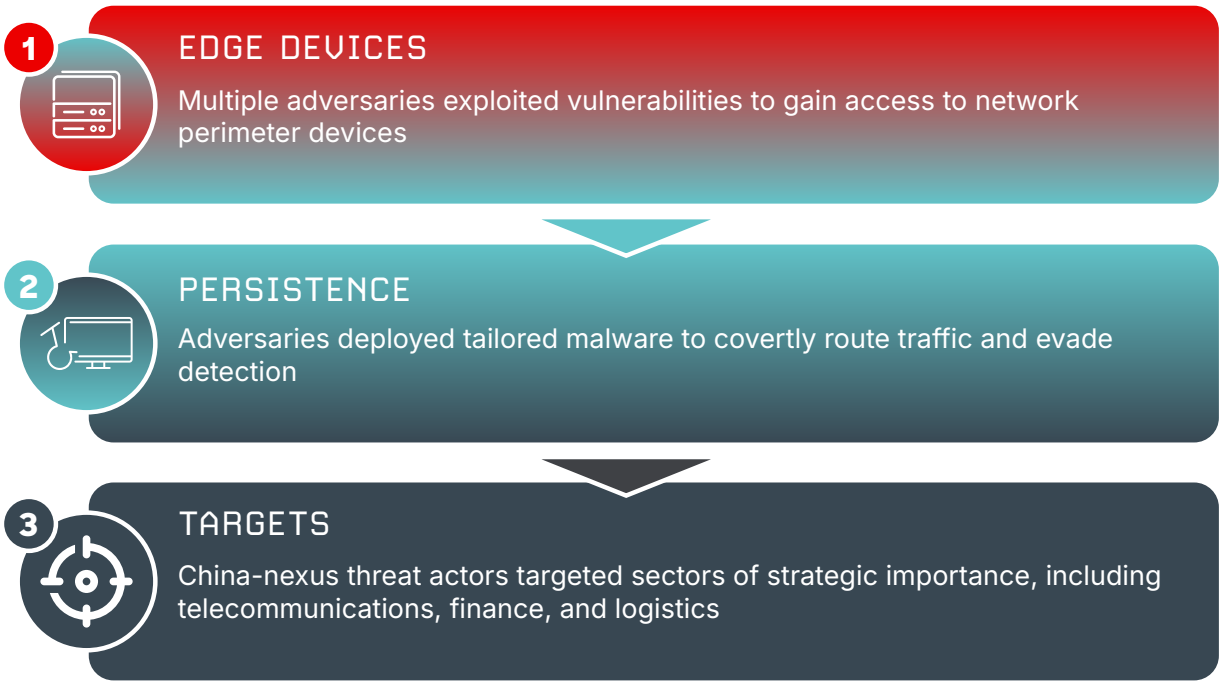


Figure 14. Summary of 2025 trends in China-nexus targeted intrusion activity

RAPID EXPLOIT WEAPONIZATION DEFINES 2025 OPERATIONS

In 2025, China-nexus adversaries demonstrated they can consistently operationalize publicly disclosed exploits within days of an exploit's release (Figure 15). This capability reinforces previous assessments that state-sponsored resources enable rapid vulnerability research and exploit development. On July 14, 2025, six days after researchers published public proof-of-concept (POC) exploits, OPERATOR PANDA exploited CVE-2025-25257, a SQL injection vulnerability. Similarly, PHANTOM PANDA exploited CVE-2025-31324 on April 27, 2025, three days after the vendor publicly disclosed the file upload vulnerability.

VAULT PANDA and GENESIS PANDA both deployed exploits targeting React2Shell (CVE-2025-55182) on December 5, 2025, only two days after security researchers publicly disclosed these vulnerabilities. VAULT PANDA deployed the custom implant *GoneDoor* during these operations, while GENESIS PANDA delivered *VShell* and its associated downloader *Bottles*.

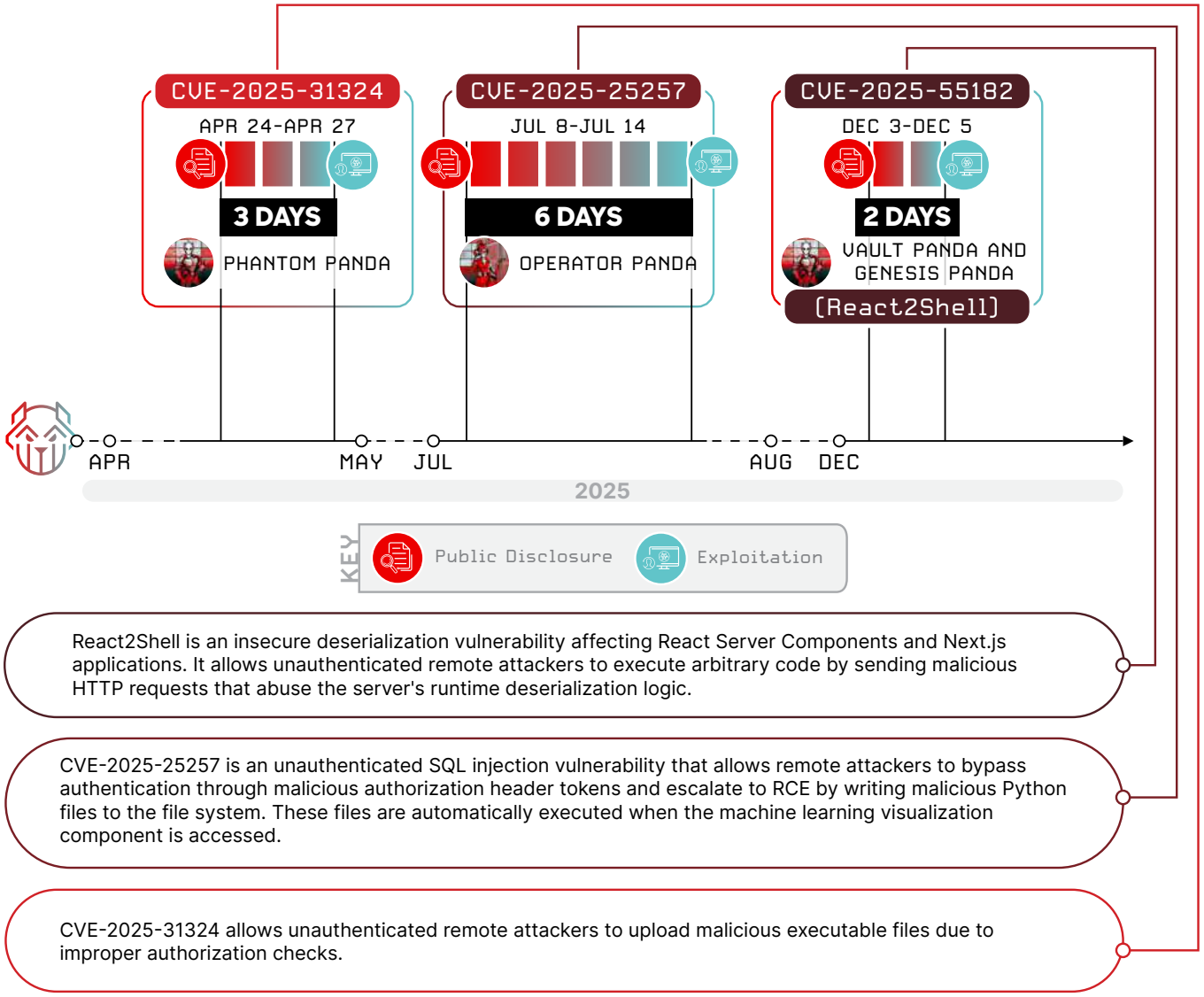


Figure 15. Rapid exploit weaponization by China-nexus adversaries defines 2025 operations

CrowdStrike Intelligence assesses with high confidence that China-nexus adversaries maintain dedicated resources for monitoring vulnerability disclosures. This assessment is based on these adversaries' consistent ability to rapidly operationalize newly identified vulnerabilities as part of targeted intrusion operations throughout 2025, indicating a systematic approach rather than isolated opportunistic activity. This rapid adoption pattern indicates that China-nexus adversaries prioritize speed over operations security (OPSEC) and aim to exploit the brief time period between disclosure and patching.

ADVERSARIES PREFER EDGE DEVICES AS STRATEGIC ACCESS POINTS

China-nexus adversaries consistently targeted VPN appliances, firewalls, gateways, and other perimeter devices throughout 2025, reflecting a strategic preference for these systems as initial access vectors. WARP PANDA's June 2025-August 2025 operations targeted U.S.-based legal, technology, and manufacturing entities by exploiting VPN appliances through CVE-2024-21887 and CVE-2023-46805, an exploit chain that bypasses authentication and enables arbitrary RCE.

WARP PANDA pivoted from compromised edge devices to vCenter environments, deploying the malware families *BRICKSTORM*, *TetanusStorm*, *DualGauge*, *Junction*, and *GuestConduit*. In one long-running intrusion, the adversary maintained persistent access for 22 months, from October 2023 to mid-2025, demonstrating that these operations were likely intended to fulfill long-term intelligence collection objectives.

From mid-2023 to October 2025, HOLLOW PANDA consistently compromised Check Point VPN appliances across multiple intrusions, targeting organizations in Australia, Brazil, India, Indonesia, Israel, Mexico, the Philippines, Southeast Asia, and the U.S. Limited visibility prevents a determination of the exact compromise method; however, the adversary likely exploited CVE-2024-24919 or leveraged previously compromised accounts. Following initial access, the adversary deployed *ShadowPad* malware via DLL search-order hijacking, configuring the implant to use DNS tunneling.

OPERATOR PANDA demonstrated versatility in their edge device targeting, compromising Cisco IOS XE devices, Palo Alto Networks firewalls, and other network appliances. The adversary exploited CVE-2024-3400, a critical command injection vulnerability in Palo Alto Networks PAN-OS, days after a POC exploit for the vulnerability was published.

CrowdStrike Intelligence assesses that China-nexus adversaries prefer to gain access via edge device exploitation given that these systems provide immediate access while offering defenders only limited visibility. This assessment is made with high confidence based on multiple China-nexus adversaries consistently targeting these devices throughout 2025 and the long-term persistence adversaries have previously achieved through edge device compromise. Edge devices frequently operate with minimal EDR coverage, reduced logging capabilities, and inconsistent patch management.

» THE ADVERSARY MAINTAINED PERSISTENT ACCESS FOR 22 MONTHS, DEMONSTRATING THAT THESE OPERATIONS WERE LIKELY INTENDED TO FULFILL LONG-TERM INTELLIGENCE COLLECTION OBJECTIVES.

STATE-SPONSORED RESOURCES ENABLE SOPHISTICATED, WIDESPREAD OPERATIONS

The technical sophistication and operational tempo of China-nexus threat actors' 2025 edge device targeting reflects state-sponsored resource allocation. Adversaries deployed custom malware families, maintained global infrastructure networks, and conducted concurrent multi-target operations across diverse sectors and geographic regions.

WARP PANDA carefully attended to OPSEC in their design of multiple custom malware families, including *BRICKSTORM*, *TetanusStorm*, *Junction*, and *GuestConduit*. These tools allowed the adversary to tunnel traffic through vCenter appliances, masquerade activity as legitimate processes, clear logs, and timestomp files. Additionally, the adversary used the malware families to establish persistence, which allowed the implants to survive after file deletion and system reboots.

China-nexus adversaries with less sophisticated OPSEC practices still gained access to targets via widespread exploitation, often using recently announced vulnerabilities. GENESIS PANDA and VAULT PANDA both operationalized React2Shell exploits within two days of the vulnerabilities' public disclosure. This quick response likely indicates dedicated resources for vulnerability research monitoring and rapid exploit weaponization.

China-nexus adversaries also demonstrated consistent infrastructure creation preferences, leveraging operational relay box (ORB)[6] networks, commercial virtual private server (VPS) providers for hosting, content delivery networks (CDNs) for command-and-control (C2) obfuscation, and various legitimate domain registrars for infrastructure maintenance.

OPERATOR PANDA proved particularly adept at using infrastructure to strengthen their OPSEC. The adversary modified network Terminal Access Controller Access-Control System Plus (TACACS+) configurations on compromised devices to redirect traffic to adversary-controlled infrastructure.

China-nexus adversaries maintain a continuous operational tempo, with peak activity occurring during China's business hours. These adversaries' deployment of custom malware families and maintenance of global infrastructure indicate state-level resource allocation to support intelligence collection activities.

TARGETING PRIORITIES ALIGN WITH STRATEGIC INTELLIGENCE REQUIREMENTS

China-nexus adversary targeting throughout 2025 reflected intelligence collection priorities aligned with Chinese Communist Party strategic objectives, including telecommunications surveillance, economic espionage, and technology transfer.

Consistent with previous years, specialized China-nexus threat actors primarily focused on telecom entities. OPERATOR PANDA, for example, consistently targeted telecom providers between 2021 and July 2025. GENESIS PANDA also targeted telecom entities in this time frame, focusing on East Asia, East Africa, and North America and likely seeking call data records and network infrastructure access. China-nexus threat actors' persistent telecom targeting indicates China likely prioritizes communication interception capabilities.

WARP PANDA targeted U.S.-based legal, technology, and manufacturing entities, focusing on sectors containing valuable intellectual property and trade secrets. HOLLOW PANDA's operations targeted logistics, government, financial services, energy, maritime, technology, and biomedical sectors across 10 countries. Targeting patterns align with the priorities detailed in China's 14th Five-Year Plan.

Geographically, China-nexus threat actors continued to heavily focus their operations on the Asia Pacific region, with multiple adversaries targeting organizations in Australia, India, Indonesia, the Philippines, and Southeast Asia. VEILED PANDA targeted a U.S.-based aviation entity in late 2025, exploiting a Windows Server Update Services (WSUS) RCE vulnerability (CVE-2025-59287) before deploying *ShadowPad*.

---

6 An ORB network is a traffic relay system (generally composed of a mix of compromised devices and leased servers) used to obfuscate the origin and destination of malicious traffic.

CVE-2025-59287

On October 23, 2025, Microsoft issued an out-of-band patch for CVE-2025-59287, which the company originally disclosed on October 14, 2025. A remote, unauthenticated attacker can exploit this vulnerability by sending a crafted event that triggers unsafe object deserialization, which enables RCE on the targeted instance. Only Windows servers with the WSUS server role enabled are vulnerable to CVE-2025-59287 exploitation; by default, the WSUS server role is disabled for Windows servers.

OUTLOOK

CrowdStrike Intelligence assesses that China-nexus adversaries will continue targeting internet-facing appliances and edge devices for initial access operations throughout 2026. This assessment is made with high confidence based on the trend's longevity in China-nexus targeted intrusion activity, the demonstrated effectiveness of edge device exploitation for establishing persistent access, and the continued availability of exploitable vulnerabilities in perimeter infrastructure.

As new vulnerabilities are disclosed, China-nexus adversaries will almost certainly rapidly incorporate associated exploits, attempting both mass exploitation and selective intrusion operations. These adversaries' observed ability to consistently begin exploitation rapidly after vulnerability disclosure throughout 2025 will likely continue in 2026, placing organizations at significant risk in the brief time between disclosure and patching.

This assessment assumes adversaries will continue using their current TTPs rather than significantly alter their approaches. However, increased organizational focus on edge device security could drive adversaries to explore alternative initial access vectors.

Edge devices were targeted in 40% of cases in which a China-nexus adversary exploited a vulnerability during an intrusion in 2025. Organizations in the telecom, technology, legal, government, academic, and critical infrastructure sectors will likely continue to face elevated risk from China-nexus edge device targeting, as China-nexus activity targeting these sectors collectively increased 34% from 2024 to 2025. Given the rapid weaponization of vulnerabilities by China-nexus adversaries, defenders should prioritize patching edge devices within 72 hours of critical vulnerability disclosure, implementing enhanced monitoring for edge device compromise indicators, and establishing network segmentation to limit lateral movement from compromised perimeter systems.

By systematically compromising network perimeter infrastructure, China-nexus threat actors can continuously collect intelligence that supports China's strategic objectives, including economic espionage, technology transfer, and telecom surveillance. Edge device security is critical not only for individual organizations but for national security, as compromised perimeter infrastructure can potentially enable adversary access for months or years before detection.

EDGE DEVICES WERE TARGETED IN 40% OF CASES IN WHICH A CHINA-NEXUS ADVERSARY EXPLOITED A VULNERABILITY DURING AN INTRUSION IN 2025. ORGANIZATIONS IN THE TELECOM, TECHNOLOGY, LEGAL, GOVERNMENT, ACADEMIC, AND CRITICAL INFRASTRUCTURE SECTORS WILL LIKELY CONTINUE TO FACE ELEVATED RISK FROM CHINA-NEXUS EDGE DEVICE TARGETING, AS CHINA-NEXUS ACTIVITY TARGETING THESE SECTORS COLLECTIVELY INCREASED 34% FROM 2024 TO 2025.

Supply Chain Attacks Enable Evasion of Traditional Security Controls

Supply chain attacks represent a distinct security challenge. Because users trust that legitimate software will not include malicious code and organizational patching policies will not inadvertently infect machines with malware, adversaries can adopt methods that exploit this trust. Adversaries' increased use of such methods in 2025 marks a shift in initial access techniques to focus on evading traditional security controls.

In supply chain attacks, threat actors modify software provider infrastructure or code bases in ways that obscure threat activity, making them stealthy and challenging to detect. In some cases, supply chain attacks cause further damage when untrusted code is incorporated into wider software ecosystems, infecting additional organizations beyond the original target.

In 2025, CrowdStrike Intelligence detailed several supply chain attacks in which threat actors either compromised software providers and manipulated their existing update mechanisms or obtained credentials for individual accounts and then modified legitimate software packages in public code repositories.

Ultimately, both methods allow threat actors to execute code for deploying malware or executing malicious commands that leak credentials. The threat actors can then exfiltrate sensitive data, compromise external systems, or steal cryptocurrency. Several DPRK-nexus adversaries regularly use supply chain attacks in currency generation operations and target software developers to enable subsequent campaigns.

COMPROMISED SOFTWARE PROVIDERS

Adversaries continued compromising software providers to enable supply chain attacks throughout 2025, typically in highly targeted operations with significant impacts. Depending on their initial access vector and lateral movement abilities, threat actors can leverage these operations for wide-ranging follow-on options. Such options include modifying customer-facing SaaS environments to inject malicious code, altering software update mechanisms to deliver alternative payloads, and accessing continuous integration and continuous delivery (CI/CD) systems that can be used to infect legitimate software builds.

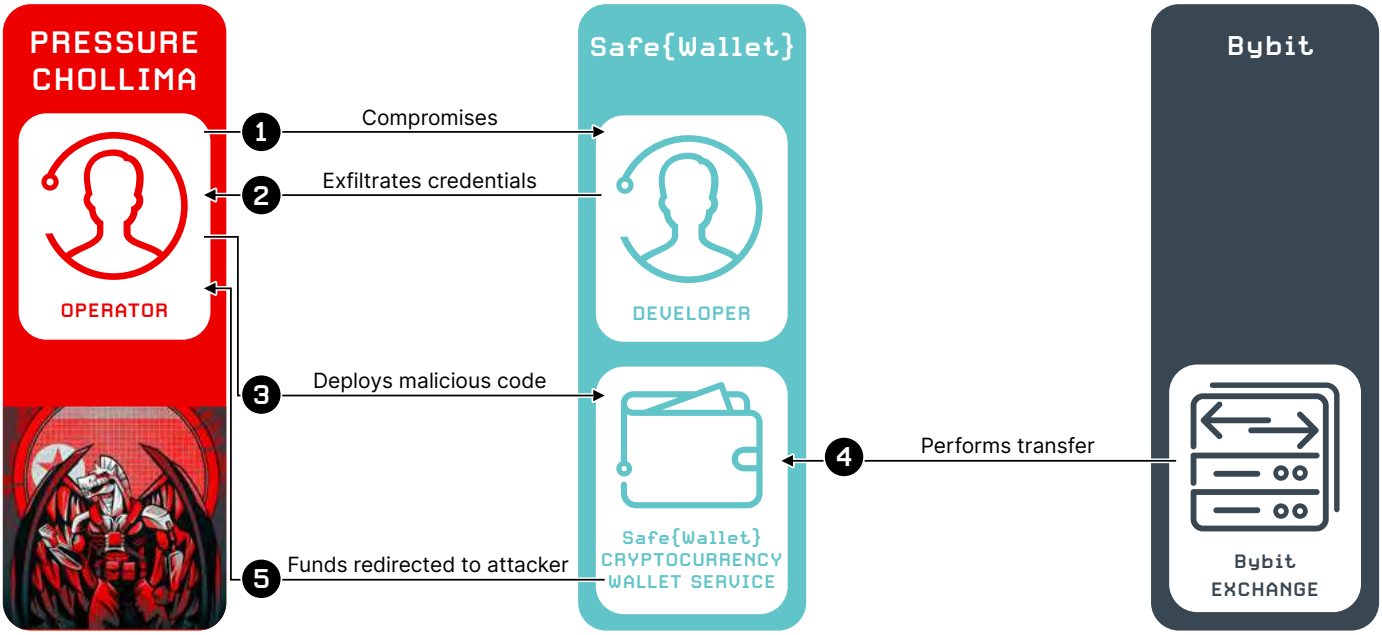


Figure 16. PRESSURE CHOLLIMA supply chain attack targeting Bybit

In late February 2025, PRESSURE CHOLLIMA executed the largest cryptocurrency theft in history by compromising Safe{Wallet}, a digital asset management platform supporting cryptocurrency exchanges, to target funds held by the centralized cryptocurrency exchange Bybit. The adversary initially gained access to Safe{Wallet} systems by compromising a software developer's machine via a trojanized Python project (likely delivered using social engineering tactics) and exfiltrating development-related credentials.

From this foothold in the victim system, PRESSURE CHOLLIMA pivoted to Safe{Wallet}'s cloud infrastructure, where they inserted two elements into the frontend: malicious JavaScript code for Bybit transactions and a smart contract containing customized transfer logic that executed exclusively during transactions between Bybit's contract address and an adversary-controlled address. This logic modified a subsequent routine transaction between Bybit wallets managed using Safe{Wallet}, redirecting cryptocurrency then valued at 1.46 billion USD to an adversary-controlled wallet. To evade detection, immediately following the transaction, the adversary restored the malicious JavaScript hosted on Safe{Wallet}'s cloud instance to its original version.

Threat actors also compromised software update mechanisms to deliver malicious code in 2025. For example, in late October 2025, CrowdStrike OverWatch identified a legitimate Notepad++ update process delivering malicious reconnaissance and remote access tool (RAT) payloads to organizations in Central America and South Asia. This highly targeted activity delivered malware to only approximately 0.1% of organizations conducting Notepad++ client updates in the operational time period.

Further payload analysis indicates technical overlaps with malware families employed for likely China-nexus operations using multiple deployment methods, indicating further diversification in supply chain attack distribution methods.

THIRD-PARTY SOFTWARE DEPENDENCY COMPROMISE

Today's complex software ecosystems frequently integrate third-party packages into commercial and open-source software to provide additional functionality. Because developers who use third-party dependencies trust that the package maintainers securely verify their code and software build process over successive updates, adversaries can abuse this trust to introduce their own malicious code into otherwise legitimate projects. Organizations then unknowingly execute untrusted code after installing or updating software that includes these dependencies.

Throughout 2025, threat actors frequently used supply chain attack methods to target npm repositories that offer JavaScript-based libraries for the Node.js runtime environment. For example, FAMOUS CHOLLIMA combined malicious npm packages with social engineering techniques to deliver *BeaverTail* malware to software developers. Between January 2025 and May 2025, the adversary deployed more than 30 malicious packages to npm.

FAMOUS CHOLLIMA operators then masquerade as legitimate job recruiters and ask targeted developers to review or improve a project as part of an employment assessment. To complete the purported assessment, the developers download and execute the malicious packages that deploy malware payloads. Adversary-linked packages were downloaded more than 8,000 times, likely because they were incorporated as dependencies in other software and therefore caused collateral infections.

In September 2025, the new malware family *ShaiHulud* began circulating via a supply chain attack on the npm ecosystem. An information stealer capable of collecting many credential types from infected machines, *ShaiHulud* can self-propagate by infecting further npm packages if the malware finds the appropriate authentication tokens on the host. Though the initially affected package was downloaded more than 2 million times by mid-September 2025, *ShaiHulud*'s self-propagation capability likely posed an infection risk to many more users as the attack progressed.

In November 2025, *ShaiHulud*'s developer expanded the malware's capabilities to include remote execution and destructive payload delivery. The updated malware increases stealth by removing evidence of the attack's initial phases, which use malicious GitHub pull requests. This enhanced initial phase indicates the threat actor attempted to maximize infection rates across a large number of compromised packages in their second campaign iteration.

Threat actors also used npm-based supply chain attacks to hijack cryptocurrency transactions via cryptocurrency wallet credential stealers in 2025. Because trojanized npm packages are typically downloaded several million times per week, threat actors using this technique have high chances of successfully capturing credentials.

In September 2025, multiple npm packages maintained by a single developer, accounting for over 2 billion downloads per week, were compromised after threat actors phished administrative credentials with a credential stealer masquerading as an npm login page. In this case, malicious code incorporated into the packages could monitor network data and hijack cryptocurrency transactions, replacing the destination wallet with an attacker-controlled address.

As this campaign illustrates, attackers can use a single vulnerability point, such as a prolific npm package developer, to spread malicious code across projects with very high install rates.

» THOUGH THE INITIALLY AFFECTED PACKAGE WAS DOWNLOADED MORE THAN 2 MILLION TIMES BY MID-SEPTEMBER 2025, *ShaiHulud*'s SELF-PROPAGATION CAPABILITY LIKELY POSED AN INFECTION RISK TO MANY MORE USERS AS THE ATTACK PROGRESSED.

DETECTING ANOMALOUS SaaS ACTIVITY WITH CROWDSTRIKE FALCON SHIELD

SaaS providers are an attractive target for adversaries aiming to execute supply chain attacks and pivot to subscriber networks. Attackers can steal SaaS authentication tokens from a centralized repository and use them to access many customer data stores.

In September 2025, Salesloft disclosed an intrusion that occurred between March 2025 and June 2025 in which a threat actor gained access to the company's GitHub and cloud environments. The intrusion enabled OAuth token theft for Salesloft customers' Drift integrations with third-party SaaS applications. The majority of observed incidents impacted IT services organizations, and several high-value IT and information security companies publicly disclosed incidents related to the campaign.

In several subsequent incidents that CrowdStrike Falcon® Shield identified and CrowdStrike Services responded to, a threat actor leveraged stolen Salesloft OAuth tokens to access and exfiltrate data from customers' Drift-integrated SaaS applications. In one incident, the threat actor also attempted to pivot to the customers' identity and access management (IAM) user accounts via exposed credentials. The threat actor likely obtained these credentials from compromised SaaS instances using TruffleHog, an open-source tool that can identify exposed credentials in source-code repositories.

CrowdStrike Intelligence cannot currently assess the threat actor's origin or motivation but has not observed attempts to monetize this campaign to date. The long time period the threat actor spent in Salesloft's environment is atypical for eCrime activity and more consistent with state-nexus intrusions. Additionally, the threat actor's focus on targeting IT and information security organizations indicates they likely intend to target downstream organizations, another pattern consistent with state-nexus threat actors.

Falcon Next-Gen SIEM customers can use Falcon Shield to detect anomalous SaaS activity, including access from stale accounts, connections originating from unexpected autonomous system numbers (ASNs), and actions that are atypical for the current user and other non-human identities.

OUTLOOK

CrowdStrike Intelligence anticipates that supply chain attacks will continue to pose a significant threat to organizations throughout 2026. Attackers value this method because it offers a wide potential scope and allows them to hijack trusted update mechanisms intended to improve software security.

Campaigns exploiting public code repositories demonstrate that attackers are refining their techniques in two important ways: evading early detection by deleting evidence of initial infection from public view and expanding reach by incorporating self-replication procedures into their malicious code. These changes have already yielded considerable success, despite efforts by developers and code-hosting platforms to remove malicious code from circulation. As these attacks often compromise packages created by developers who have full-time jobs outside of maintaining the code, threat actors can often gather prerequisite credentials and initiate campaigns before a developer realizes their package has been compromised.

Attackers will likely continue adapting their techniques to maximize infection rates. For example, threat actors may find opportunities to add malicious code more subtly or trigger behavior that users do not intend through indirect code changes (e.g., modifying cryptocurrency smart contracts executed by targeted software).

Targeting of SaaS applications will likely increase further in 2026 based on the continued trend of enterprise organizations migrating data from on-premises to cloud-based systems and the numerous 2025 campaigns in which threat actors targeted SaaS instances. eCrime and targeted intrusion adversaries continued to target SaaS platforms for data discovery, exfiltration, and monetization.

Compromising software development companies to access their internal build chains and update mechanisms remains a more complex supply chain attack option, although this methodology is still likely to be used for highly targeted attacks that can evade detection unless updates are specifically tested for malicious code.

Adversary Objectives Shape Zero-Day Exploit Selection

Zero-day exploits allow adversaries to evade detection and countermeasures for identified exploit vectors. Throughout 2025, threat actors used dozens of zero-day exploits to enable initial access, RCE, and privilege escalation. CrowdStrike Intelligence observed a 42% year-over-year increase in the number of zero-day vulnerabilities exploited prior to public disclosure. This aligns with the gradual increase industry sources have reported in zero-day exploitation over the past four years.[7]

Adversaries' objectives and preferences highly likely influence the zero-day they choose to exploit. A subset of targeted intrusion threat actors, often driven by their mandates to stealthily gain persistent access and collect intelligence, prioritize targeting zero-days in internet-exposed endpoints. They frequently use such exploits to gain initial access to unmanaged assets in high-value networks. In at least one case, one targeted intrusion adversary repeatedly attacked the same vendor and product with multiple zero-days disclosed in 2025, suggesting the threat actor may be focusing their efforts on this product.

In contrast, financially motivated adversary GRACEFUL SPIDER targets vulnerabilities in internet-facing enterprise products in widespread campaigns. Therefore, they highly likely select exploits based on speed and reliability at scale.

Similarly, reliability requirements likely motivate eCrime adversaries' selection of a given zero-day exploit for local privilege escalation (LPE) against operating systems (OSs). However, reliability is likely a less important criterion to these adversaries than the ease with which they can obtain a given exploit, either directly or indirectly.

---

7 https://cloud.google.com/blog/topics/threat-intelligence/2024-zero-day-trends

TARGETED INTRUSION THREAT ACTORS EXPLOIT EDGE DEVICES VIA ZERO-DAY VULNERABILITIES

Throughout 2025, targeted intrusion adversaries gained access to networks by exploiting zero-day vulnerabilities in edge devices such as VPN servers, mail servers, firewalls, and routers. Many targeted intrusion adversaries value edge device attacks due to these devices' security shortcomings and often deliberate internet exposure.

Moreover, EDR solutions often achieve only limited visibility of edge devices. Targeted intrusion threat actors' continued efforts to leverage zero-day vulnerabilities against these devices likely signal that they have experienced success and have invested significant resources into such methods.

Since at least 2023, Russian targeted intrusion adversary FANCY BEAR has targeted various webmail services via multiple methods, including zero-day and n-day vulnerability exploitation impacting Zimbra and Roundcube webmail services. The adversary likely uses these methods for access development and intelligence collection. Targeted intrusion adversaries have conducted similar exploitation campaigns against webmail products. In 2025, Russia-aligned threat actors, including FANCY BEAR and Belarus-nexus adversary UMBRAL BISON, increasingly exploited cross-site scripting (XSS) vulnerabilities in Roundcube and Zimbra to exfiltrate valid credentials, email communications, and contact lists.

Threat actors also value mail servers because they are inherently exposed, often via an easily enumerated login portal, and are associated with prolonged patching periods. While CrowdStrike Intelligence has observed numerous threat actors compromising and/or exploiting mail servers for several years, some adversaries appear to particularly focus on these applications and target multiple vendors across a broad spectrum of products and versions.

In addition to webmail servers, targeted intrusion threat actors frequently exploit VPN servers, which are also commonly unmanaged and exposed. Multiple vulnerabilities disclosed in 2025 that impact network devices, including CVE-2025-22457 and CVE-2025-0282, were previously exploited as zero-days.

Though the malware and target sectors differed between incidents, a technique often used in these operations aligns with a well-established China-nexus technique: rapidly deploying a network remote code exploit against perimeter devices as part of initial access operations.

GRACEFUL SPIDER'S OPPORTUNISTIC USE OF ZERO-DAY VULNERABILITIES

eCrime adversary GRACEFUL SPIDER differentiates themselves from other BGH adversaries by repeatedly exploiting zero-day vulnerabilities. Since late 2020, GRACEFUL SPIDER has primarily exploited internet-exposed network assets with multiple remote zero-day vulnerabilities. Whether GRACEFUL SPIDER develops or merely acquires these zero-day exploits remains unclear.

Beginning as early as August 2025, GRACEFUL SPIDER conducted data exfiltration operations by exploiting a novel zero-day vulnerability now tracked as CVE-2025-61882.

Though this campaign diverges from GRACEFUL SPIDER's historical pattern of targeting file transfer applications, the tactical shift remains consistent with the adversary's overarching strategy: targeting internet-exposed, enterprise-level web applications to achieve initial access and, ultimately, exfiltrate data. This strategy will almost certainly drive GRACEFUL SPIDER's choice of exploit targets in the future.

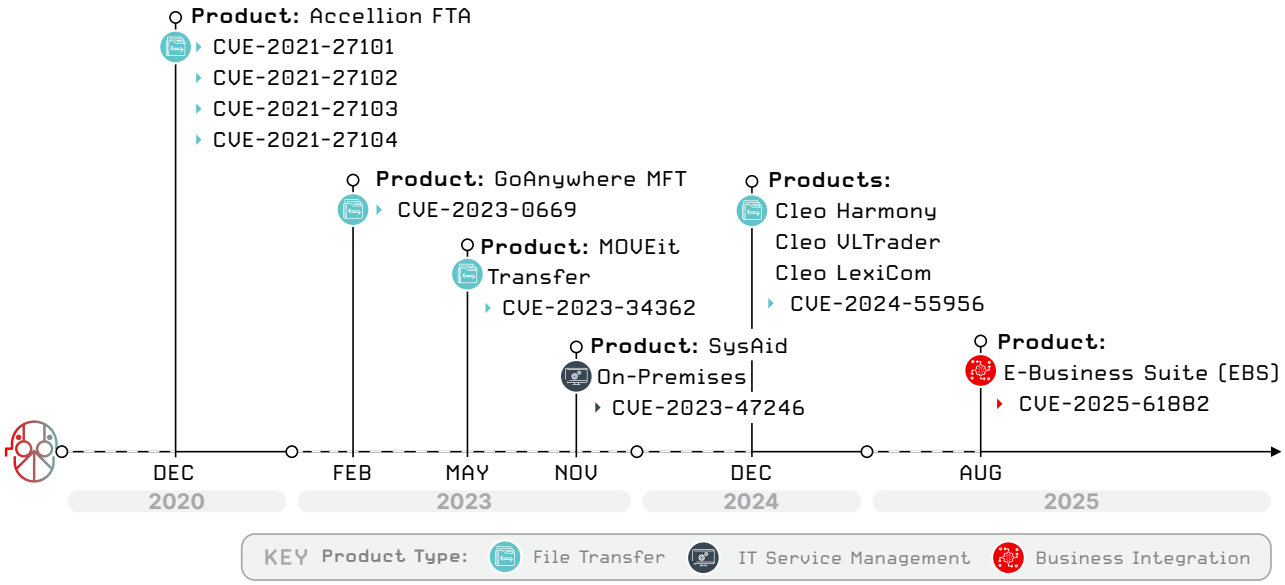


Figure 17. Zero-day vulnerabilities exploited by GRACEFUL SPIDER

eCRIME THREAT ACTORS' APPROACH TO ZERO-DAY EXPLOITATION FOR PRIVILEGE ESCALATION

Zero-day exploits used on common OSs are far more effective for achieving LPE at scale than alternative exploit types. However, because OS patching cycles are relatively narrow, threat actors have limited opportunity to capitalize on zero-day exploits following disclosure. Other exploit types, particularly network RCE, may impact platforms that are more difficult to patch and may therefore remain effective for longer periods.

In late April 2025, eCrime adversary VICE SPIDER highly likely exploited a zero-day LPE vulnerability (CVE-2025-32706) affecting the Microsoft Windows Common Log File System (CLFS) driver. Though VICE SPIDER previously leveraged n-day LPE vulnerabilities against various Windows services and protocols (such as the Windows Error Reporting service via CVE-2023-36874, CLFS via CVE-2022-24521, and Netlogon via CVE-2020-1472), the April 2025 activity marked the first observed instance of VICE SPIDER using a zero-day LPE vulnerability for the Windows CLFS driver.

VICE SPIDER's transition to novel zero-day use is a logical progression in the adversary's increasingly effective privilege escalation techniques. Initially, the adversary frequently escalated privileges through compromised credentials. However, since at least 2023, VICE SPIDER has repeatedly used a series of Windows LPE exploits targeting disclosed vulnerabilities.

Other eCrime threat actors have also used exploits to target vulnerabilities affecting multiple Windows drivers, services, and protocols, including the following:

- CVE-2025-59230, which affects the NetMan service
- CVE-2023-29360, which affects the Microsoft Streaming Service
- CVE-2024-35250, which affects Windows kernel-mode drivers
- CVE-2024-26169, which affects the Windows Error Reporting service

eCrime adversaries highly likely choose specific Windows drivers, services, or protocols to target for LPE opportunistically rather than based on a specific preference or targeting requirement. These choices likely depend on the target component's prevalence, the exploit's reliability, and the exploit's availability, whether through purchase from exploit brokers, free postings on public repositories, or in-house development.

OUTLOOK

CrowdStrike Intelligence assesses that the zero-day exploit trends addressed in this section will highly likely persist into 2026 in various ways, including a direct repetition of the 2025 trends. Nevertheless, sophisticated adversaries are expected to further evolve their exploitation abilities.

Though adversaries will likely approach this evolution in different ways, some may attempt to discover and operationalize zero-day defense evasion-related vulnerabilities that could enable them to maintain long-term persistent access. While such vulnerabilities may not receive critical ratings, facilitate mass exploitation, or garner widespread press coverage, they would permit threat actors to remain undetected in victim networks, thereby complicating defense and remediation efforts for network defenders.

Furthermore, GRACEFUL SPIDER's sustained, multi-year success in exploiting zero-day vulnerabilities will likely motivate other BGH threat actors to adopt similar tactics in 2026. BGH threat actors aiming to execute rapid, extensive exploitation against well-protected entities, appear highly skilled, or distinguish themselves from competitors are the eCrime groups most likely to incorporate zero-day exploits into future operations.

CrowdStrike Intelligence recommends a comprehensive, in-depth defense strategy to mitigate the potential risk of zero-day vulnerabilities. Proactive planning and preparation can help organizations understand their exposure and yield actionable recommendations to minimize the probability and impact of a security event. This can include penetration testing, establishing a robust vulnerability management program, conducting red teaming exercises, and executing tabletop drills.

CrowdStrike Intelligence additionally recommends using Falcon Next-Gen SIEM. This helps organizations gather and leverage cross-domain data (such as real-time indicators of attack, adversary intelligence, exposure data, Falcon sensor data, and third-party data) to deliver highly accurate detections and automated protection and remediation. Many of these automated detection features are designed to identify and block post-exploitation activities before an adversary can achieve their objectives, reducing the overall impact of zero-day exploitation.

Adversaries Subvert Trust in Cloud Platforms and Services

Throughout 2025, both targeted intrusion adversaries and eCrime adversaries evolved their cloud-targeting techniques, successfully subverting the implicit trust users place in cloud entities and technologies to achieve persistence, lateral movement, and data exfiltration.

Adversaries' continued efforts, alongside CrowdStrike OverWatch's cloud hunting efforts, led to substantial increases in identified cloud-targeting activity in 2025. A 37% rise in cloud-conscious intrusions year-over-year demonstrates widespread adversary interest, while the 266% increase in such intrusions by named state-nexus threat actors signals that advanced, persistent threat groups are prioritizing cloud environments.

CrowdStrike Intelligence assesses that multiple targeted intrusion threat actors, the majority of whom conduct China- or Russia-nexus operations, significantly increased their investment in cloud targeting in 2025, primarily by funding research and supporting infrastructure.

China-nexus adversary MURKY PANDA continued to abuse trust relationships in Entra ID to compromise downstream victims while also using the newly created ORB network ORB28 for anonymity. In addition, Russia-nexus adversary COZY BEAR has combined various Entra ID authentication flow abuse techniques with social engineering tactics to compromise victim accounts.

Both eCrime and targeted intrusion threat actors have leveraged adversary-in-the-middle (AiTM) phishing pages to enable credential collection and to access Microsoft 365 SaaS services for data collection. eCrime threat actor *ShinyHunters* used this access to search for data related to a victim entity's customer relationship management (CRM) SaaS instance. In November 2025, Iran-nexus threat actor IMPERIAL KITTEN made their first observed attempt at targeting cloud identities when they deployed the *EvilGinx2* phishing kit to target Hebrew- and English-speaking Microsoft 365 users in Israel.

Emerging eCrime threat actors also advanced their tactics to abuse trusted relationships. While SCATTERED SPIDER primarily drove cloud-targeting techniques in 2023 and 2024, cloud-conscious adversary BLOCKADE SPIDER also targeted Entra ID services in 2025. Notably, BLOCKADE SPIDER used many cloud-based techniques previously employed by SCATTERED SPIDER, particularly those involving abuse of users' trust in hybrid identity configurations.

A 37% RISE IN CLOUD-CONSCIOUS INTRUSIONS YEAR-OVER-YEAR DEMONSTRATES WIDESPREAD ADVERSARY INTEREST, WHILE THE 266% INCREASE IN SUCH INTRUSIONS BY NAMED STATE-NEXUS THREAT ACTORS SIGNALS THAT ADVANCED, PERSISTENT THREAT GROUPS ARE PRIORITIZING CLOUD ENVIRONMENTS.

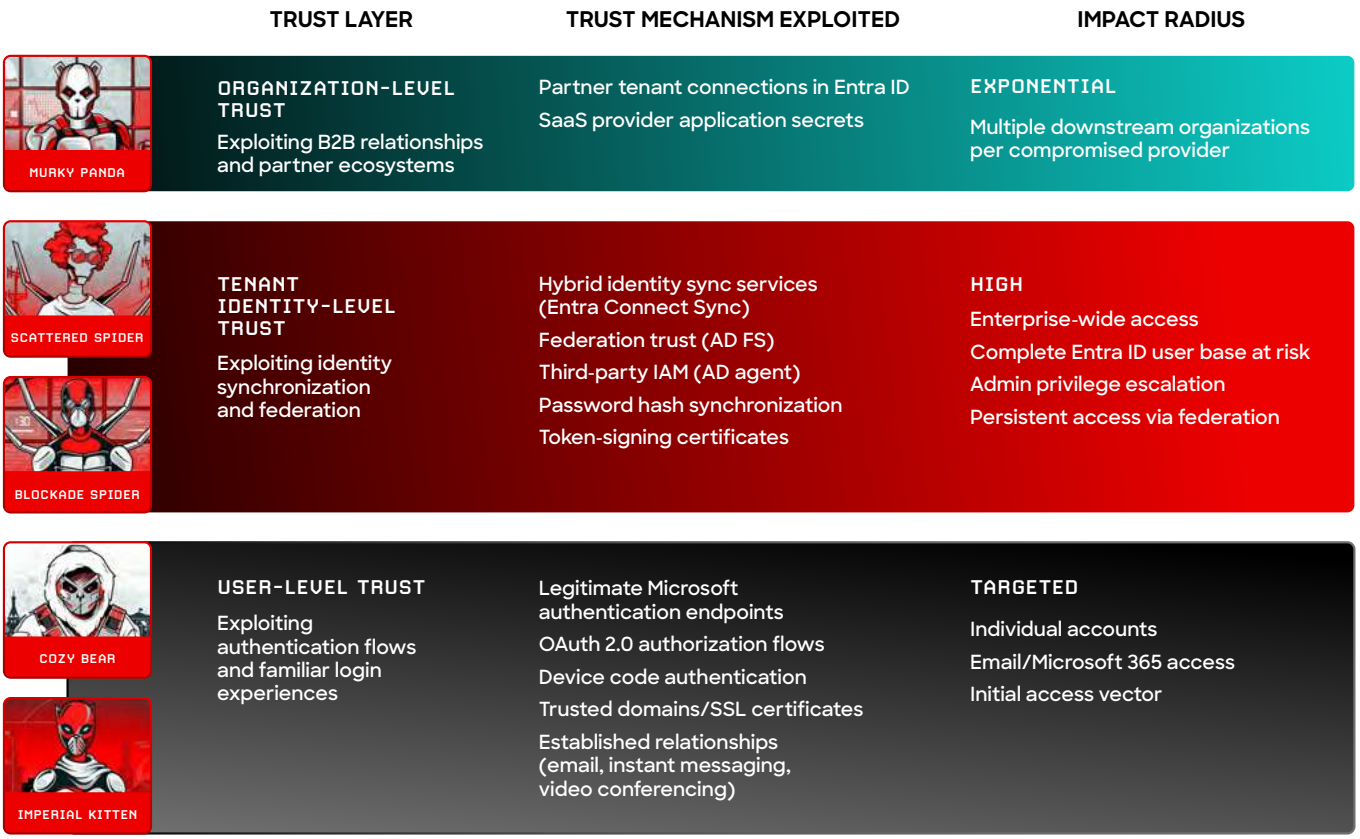


Figure 18. Layers of trust targeted by cloud-conscious threat actors

BLOCKADE SPIDER AND SCATTERED SPIDER USE PARALLEL HYBRID IDENTITY ABUSE TECHNIQUES

One of the trust abuse mechanisms that eCrime threat actors leveraged most effectively throughout 2025 was hybrid identity targeting. This set of techniques subverts users' trust in the technologies that bridge on-premises and cloud-based identity solutions. SCATTERED SPIDER and BLOCKADE SPIDER, the adversaries that targeted hybrid identity solutions most frequently throughout 2025, used many of the same cloud-conscious techniques.

SCATTERED SPIDER led the eCrime community in using hybrid identity-targeting techniques in 2025. The adversary employed many of the most effective techniques observed throughout 2024 and 2025, especially those targeting Entra ID or Azure environments. The adversary particularly favored vishing and abusing SSO services for lateral movement.

BLOCKADE SPIDER also used many techniques targeting Entra ID, often with only minor variations from SCATTERED SPIDER's techniques. Both adversaries used hybrid identity targeting, Entra ID account creation, device registration, alternate multifactor authentication (MFA) registration, conditional access policy bypassing, and indicator removal via email hiding. While BGH-based ransomware deployment remained the objective for both SCATTERED SPIDER and BLOCKADE SPIDER, each used distinct methods to achieve this goal.

Both adversaries conducted multiple novel attacks against hybrid identity solutions, which primarily allow organizations to synchronize users' accounts and authentication mechanisms between on-premises and cloud-based identity systems. Targeting this link, whether by compromising the hybrid identity solution itself or by compromising associated identities that have privileged access, provides threat actors with exceptional access levels.

These techniques can facilitate persistence and privilege escalation. Both SCATTERED SPIDER and BLOCKADE SPIDER have targeted the hybrid Entra ID solutions Entra Connect Sync and Active Directory Federation Services (AD FS). They used different tooling and, in some cases, different techniques to elevate privileges and control authentication in the environment.

Additionally, BLOCKADE SPIDER targeted a hybrid identity solution to control authentication across environments. Although these techniques may require administrative changes and anomalous account usage and are therefore less subtle than some used by targeted intrusion threat actors, they are effective for eCrime threat actors, whose operations often require speed in the cloud and quick lateral movement mechanisms with short access periods.

TARGETED INTRUSION THREAT ACTORS INVEST IN CLOUD TARGETING

MURKY PANDA and Other China-Nexus Threat Actors Abuse Partner Connections and Leverage ORB Networks

Cloud-conscious China-nexus threat actors significantly increased their intrusions in 2025, often using specialized tools, techniques, and infrastructure. Many of these techniques involved trust abuse, e.g., targeting an upstream technology service to enable later pivoting to downstream targets, leveraging ORB networks to evade detection by obfuscating access, and conducting password spraying behind inconspicuous, residential IP spaces.

China-nexus adversary MURKY PANDA has specialized in targeting Entra ID since at least Q3 2024. The adversary has compromised multiple IT services organizations using trusted relationship connections between Entra ID tenants. By targeting upstream service providers rather than individual victims, MURKY PANDA can compromise other organizations that have a trusted relationship with the targeted technology partner. This initial access vector is less monitored than many others and therefore allows for prolonged, undetected access to downstream victims' data, including emails.

In one mid-2025 incident, MURKY PANDA used the newly identified ORB28 network for delegated email access to a Microsoft 365 environment. ORB28 has also been used in high-volume password spraying attacks against Entra ID accounts, although whether the network is exclusively used by MURKY PANDA or is instead used by multiple cloud-focused China-nexus threat actors remains undetermined.

COZY BEAR Implements Trust Abuse Social Engineering and Phishing Methods

Throughout 2025, Russia-nexus adversary COZY BEAR systematically exploited interpersonal trust, organizational credibility, and platform legitimacy to compromise U.S.-based targets. The adversary successfully weaponized established professional relationships by impersonating trusted contacts, then leveraged victims' inherent trust in Microsoft's authentication infrastructure to complete the compromise. This activity was difficult for victims to identify as malicious, as the adversary prompted victims to enter credentials only on legitimate Microsoft login pages.

CrowdStrike OverWatch and CrowdStrike Services responded to multiple COZY BEAR phishing attempts at U.S.-based nongovernmental organizations (NGOs) and a U.S.-based legal entity. The adversary's multi-layered trust exploitation unfolded through three distinct vectors (Figure 19).

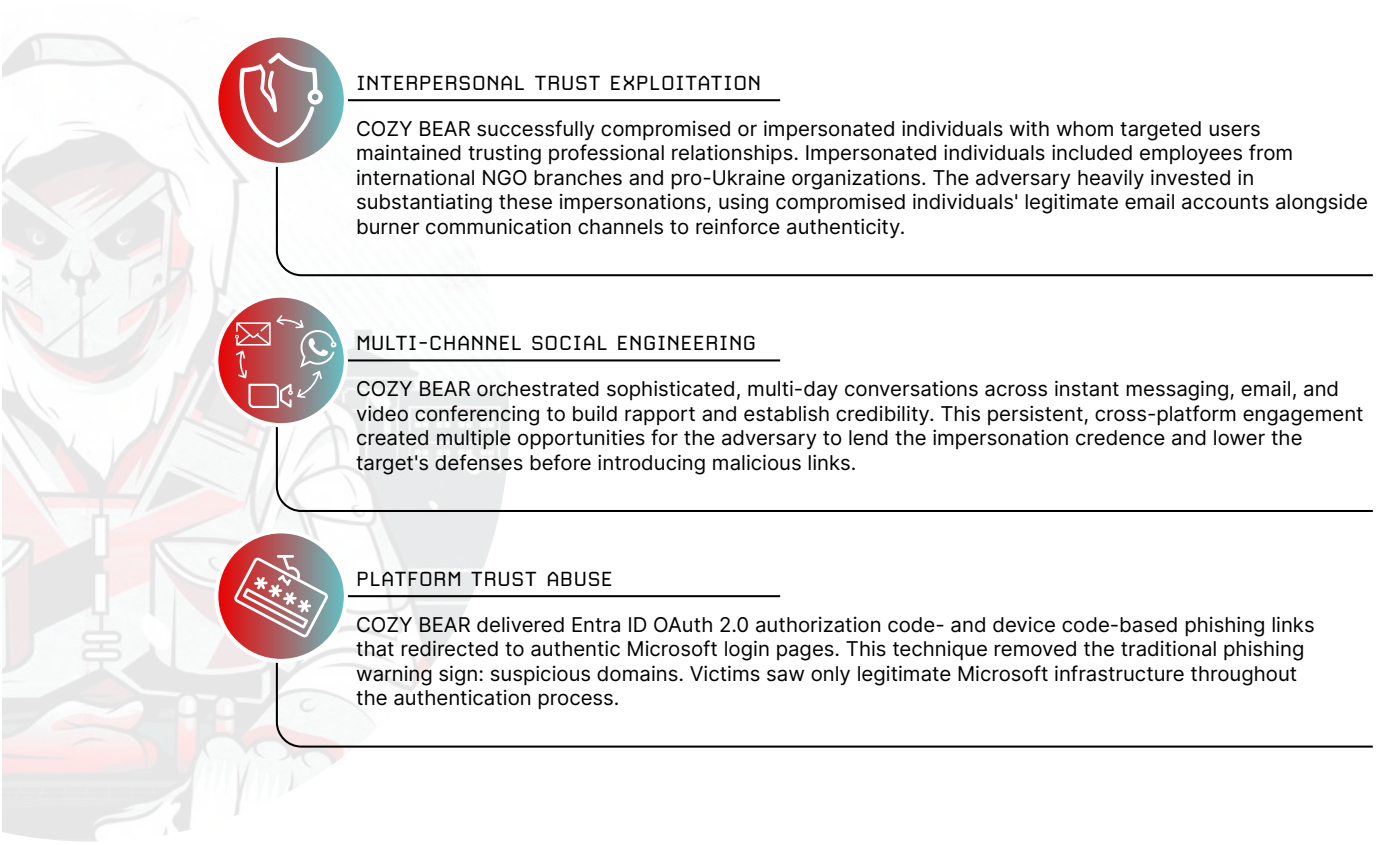


Figure 19. COZY BEAR's multi-layered trust exploitation techniques

This layered approach to trust relationship abuse provides COZY BEAR with several operational advantages. First, it ensures more reliable initial access by exploiting preexisting trust between the victim and the impersonated individual, thereby increasing the likelihood that victims will comply with requests to click links or provide authentication codes.

Second, critically, the technique allows malicious authentication activity to blend seamlessly with legitimate user behavior, thereby increasing the probability that malicious access eludes detection. By directing victims to authentic Microsoft infrastructure rather than adversary-controlled domains, the phishing attempts further evade traditional URL-based detections and leverage the inherent trust organizations place in Microsoft's authentication services. COZY BEAR used each of these techniques and attempted to evade multiple conditional access policies in an August 2025 intrusion targeting a U.S.-based NGO.

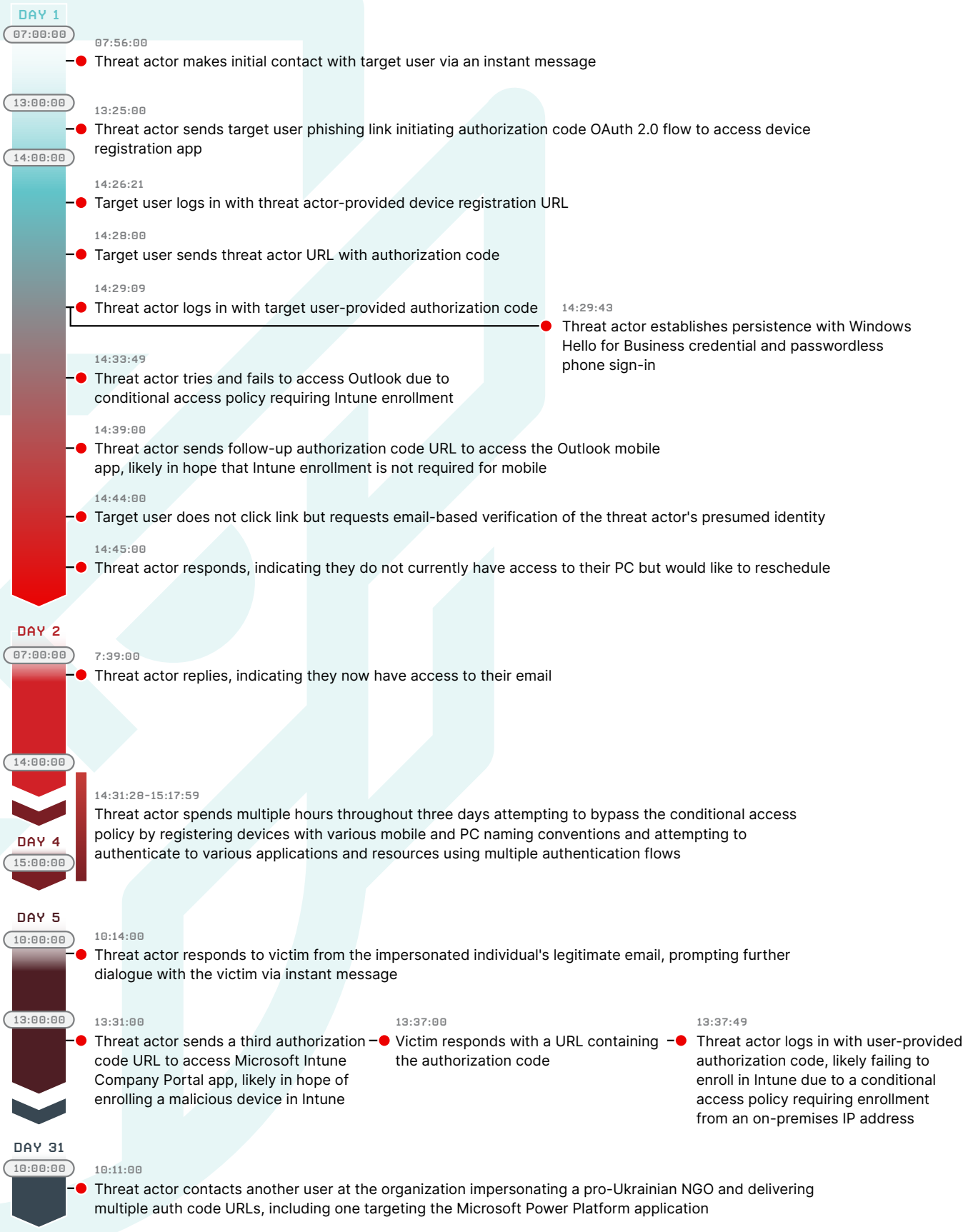


Figure 20. COZY BEAR phishing attempt targeting a U.S.-based NGO

AiTM ATTACKS ENABLE SaaS INTRUSIONS

Consistent with CrowdStrike Intelligence's prediction in the CrowdStrike 2025 Global Threat Report, both eCrime and targeted intrusion adversaries continued to target cloud-based SaaS applications throughout 2025. Performing exfiltration from SaaS applications is an effective technique, as these platforms host high volumes of critical data but are often not subject to the same heavy security monitoring as on-premises systems. Moreover, threat actors face a low technical barrier to navigating SaaS platforms, as users typically access these applications using a browser graphical user interface.

In 2025, adversaries continued targeting document management and storage suites, data warehousing platforms, and payroll and expense reimbursement applications. CRM instances emerged as a key target: In multiple eCrime and likely targeted intrusion campaigns, adversaries abused non-human identities, such as service accounts and API keys, to facilitate access to database instances.

Throughout 2025, CrowdStrike Intelligence also observed eCrime and targeted intrusion threat actors leveraging AiTM phishing kits to gain access to Microsoft 365 accounts. In contrast to traditional phishing attacks that end at credential capture, AiTM phishing kits exploit the trust relationship between users and Microsoft's authentication ecosystem by acting as a real-time reverse proxy.

When a victim enters credentials on the adversary's spoofed login page, the phishing kit transparently forwards the authentication request to legitimate Microsoft login services and relays responses back to the victim in real time. eCrime threat actors primarily use this access to identify data that can allow them to pivot to other services, while nation-state threat actors primarily target data relevant to their intelligence collection priorities in Microsoft Outlook and SharePoint.

Between January 2025 and August 2025, CrowdStrike Intelligence observed an eCrime threat actor that identifies themselves in extortion communications as *ShinyHunters* conducting social engineering campaigns that targeted access to CRM instances.

In an early 2025 campaign, the threat actor collected victims' Microsoft Entra ID credentials by directing them to access AiTM phishing pages on their personal mobile devices. The threat actor leveraged these credentials to search Microsoft SharePoint for documentation relating to access to the victim's CRM instance.

In November 2025, Iran-nexus adversary IMPERIAL KITTEN conducted credential phishing operations against Israeli Microsoft 365 users via an AiTM phishing toolkit named *EvilGinx2*. The adversary used Israel-themed phishing infrastructure with English- and Hebrew-language lures to establish credibility and urgency with targets. Post-compromise, IMPERIAL KITTEN conducted basic enumeration of Microsoft 365 accounts, accessing Microsoft App Access Panel, Office Home, and the Microsoft Authenticator app to map available services and privileges.

OUTLOOK

Throughout 2025, SCATTERED SPIDER and BLOCKADE SPIDER debuted multiple hybrid identity-targeting techniques. These new methods enabled the adversaries to obtain broad privileged access across target environments, effectively progressing the threat actors toward their primary objective: BGH ransomware deployment.

CrowdStrike Intelligence assesses that additional eCrime threat actors will likely target hybrid identity solutions in 2026. This assessment is made with moderate confidence based on this strategy's observed effectiveness as well as the steps required to operationalize some implementations of this technique.

Targeted intrusion threat actors also grew more active in conducting cloud-targeted operations in 2025, heavily investing in research, development, and personnel. Multiple cloud-conscious targeted intrusion threat actors emerged in 2025, including threat actors from Russia, China, Iran, and the DPRK.

CrowdStrike Intelligence further assesses that threat actors from these countries and other state-aligned threat actors will maintain or expand their investment in cloud capability development in 2026. This assessment is made with high confidence based on these threat actors' focus on increasing cloud-targeting capabilities and infrastructure in 2025.

Both eCrime and targeted intrusion adversaries continued to target SaaS platforms for data discovery, exfiltration, and monetization in 2025. CRM instances emerged as a target in several campaigns, with multiple threat actors leveraging non-human identity types such as OAuth tokens to gain access to these platforms.

CrowdStrike Intelligence assesses that SaaS application targeting will again increase in 2026. This assessment is made with high confidence based on the continued trend of enterprise organizations migrating data from on-premises to cloud-based systems and widely reported 2025 campaigns targeting SaaS instances.

Conclusion

As 2026 begins, the cybersecurity threat landscape grows increasingly sophisticated, demanding that organizations in all sectors and geographies strengthen and adapt their defenses. As adversaries become more evasive, agile, and innovative, understanding their motivations and anticipating their actions is critical to an effective defense.

Threat actors of all skill levels will continue adopting AI for social engineering, IO, and technical activity. Less sophisticated threat actors will use AI to offset limited expertise, enabling more complex attacks but often introducing errors due to poor implementation and limited ability to validate output. More advanced threat actors will increasingly leverage AI for malware development, social engineering, and post-exploitation activities, accelerating attack speed, scale, and effectiveness. With greater resources and maturity, these threat actors are positioned to operationalize agentic AI for minimally supervised or autonomous operations.

As organizations embed AI into core business processes, the attack surface will expand to include AI models, training data, agents, and supply chains. Limited visibility into AI operations will amplify risk and create exploitable gaps.

Despite improved detection and prevention capabilities, BGH adversaries remained 2025's primary eCrime threat. These adversaries caused significant business disruptions in 2025, resulting in substantial recovery costs and lost revenue for victims.

The ransomware ecosystem was remarkably resilient despite law enforcement disruptions and internal criminal strife, confirming ransomware remains an attractive business model. This trend is projected to persist in 2026. Fast-paced vishing campaigns targeting SaaS applications for initial access and data exfiltration will almost certainly continue, as opportunistic ransomware adversaries and targeted data theft operators employ techniques that continue to evade even advanced security solutions.

Targeted intrusion adversaries remained persistent and adaptive in 2025, incorporating stealth tactics, cloud-conscious techniques, and AI-enhanced capabilities to achieve their geopolitical and strategic objectives while evading defensive measures:

- **Russia-nexus adversaries** are expected to continue conducting aggressive operations, primarily to collect intelligence from Ukrainian targets and NATO member states.
- **China-nexus adversaries** are expected to maintain their high operational tempo while increasingly incorporating stealth tactics and targeting edge devices and internet-facing appliances. These adversaries will almost certainly continue targeting telecom, financial services, and logistics entities to support the Chinese Communist Party's strategic intelligence collection objectives.
- **DPRK-nexus adversaries** will highly likely continue to prioritize operations focused on military intelligence collection, cryptocurrency theft, and revenue generation.

In the vulnerability exploitation landscape, threat actors will continue to leverage their evasion capabilities and use zero-day exploits to bypass security controls. Exploitation will almost certainly continue to transition from zero-day activity to widespread campaigns, enabled by publicly available technical details and POC exploits, which facilitate broader threat actor participation and widespread n-day exploitation.

Cloud-conscious threat actors are now leveraging various techniques to undermine victims' trust. State-nexus adversaries are leveraging stealthy initial access methods, while eCrime adversaries are prioritizing persistence and privileged access. The prevalence of cloud-targeting adversaries will likely increase in 2026, with additional state-nexus threat actors primarily targeting cloud environments and eCrime threat actors employing techniques to target broad cloud identity access.

As these complex threats continue evolving throughout 2026, the CrowdStrike Counter Adversary Operations team remains committed to identifying, tracking, and disrupting threat actors at every possible opportunity while providing organizations with the intelligence and capabilities necessary to defend against an increasingly sophisticated and persistent adversary landscape.

Recommendations

1 Secure AI to reduce emerging business and operational risk

As AI becomes embedded in core business processes, it introduces a rapidly expanding attack surface that adversaries are already exploiting. Organizations should employ comprehensive AI security and governance measures to address threats to AI systems as well as threats posed by threat actors using AI. These should include monitoring employees' use of AI tools, enforcing access controls, and using data classification rules to prevent sensitive data leaks. These measures should also include securing homegrown AI workloads from runtime attacks (such as prompt injection), assessing the security of external vendors, and requiring secure configurations and vulnerability assessments for new AI products and their dependencies.

To defend against AI-enabled threats, organizations should develop clear incident response responsibilities and business continuity plans. Organizations can further secure their environments with strong identity verification procedures, AI-focused security awareness training, and continuous threat hunting.

2 Treat identity and SaaS as primary attack surfaces

Identity and SaaS platforms sit at the center of enterprise access, data, and business operations, making them prime targets. Adversaries increasingly weaponize vishing, phishing, and stolen OAuth tokens to pivot through cloud and SaaS identities. Organizations must strengthen phishing-resistant MFA, enforce least-privilege access for service and non-human accounts, and monitor anomalous SaaS and token activity to detect and contain intrusions before attackers access sensitive data or critical systems.

3 Eliminate cross-domain blind spots to stop high-impact attacks

Today's most disruptive intrusions succeed by exploiting gaps between security domains, tools, and teams rather than weaknesses in any single control. BGH and cloud-conscious adversaries chain activity across endpoints, cloud environments, SaaS applications, and unmanaged hosts to evade detection. Organizations should consolidate telemetry, apply cross-domain correlation through extended detection and response (XDR) and next-generation security information and event management (SIEM) workflows, and automate enrichment with threat intelligence to view full attack paths and accelerate response.

4 Secure the software supply chain and developer workflows

Trust in software updates, open-source dependencies, and development pipelines has become a critical business dependency and a prime target for adversaries. Malicious packages and compromised CI/CD pipelines enabled high-impact supply chain attacks in 2025. Organizations should harden developer environments, enforce code signing and dependency validation, scan repositories and packages for anomalies, and assess third-party risk to reduce the likelihood that trusted software becomes a vehicle for malware or credential theft.

5 Prioritize edge device and perimeter patching and monitoring

Internet-facing and perimeter systems are among the most consistently exploited, and least visible, paths into enterprise environments. State-nexus threat actors rapidly weaponize vulnerabilities in edge and perimeter devices, which often lack EDR coverage and timely patching. Organizations should prioritize rapid triage and patching of internet-facing appliances; enable logging and monitoring for VPNs, firewalls, and virtualization platforms; and apply network segmentation to limit lateral movement from compromised perimeter systems.

6 Prioritize proactive threat intelligence and hunting

When attacks unfold in minutes or seconds, reactive defense is no longer enough. An intelligence-driven approach enables organizations to stop boiling the ocean and understand which adversaries are targeting them, how they operate, and where they are likely to strike next. By applying threat intelligence and adversary tradecraft analysis through proactive hunting, teams can identify stealthy footholds (such as unmanaged VMs, AiTM activity, and supply chain anomalies) before attacks escalate. To operate at the speed and scale of AI-accelerated adversaries, organizations must augment analysts with specialized AI agents that accelerate intelligence analysis, hunting, triage, and response, turning insight into decisive action earlier in the attack life cycle.

7 Strengthen human resilience against social engineering and rapid intrusions

As adversaries increasingly rely on phishing, vishing, and trust abuse to bypass technical controls, human decision-making remains a critical factor in preventing breaches. Organizations should reinforce user awareness programs that reflect real-world adversary tactics to help employees recognize and resist social engineering attempts that enable initial access.

For security teams, preparedness under pressure is essential. Regular tabletop exercises and red/blue team operations help organizations identify gaps in detection, decision-making, and response, ensuring teams can act quickly and effectively when attacks unfold. Continuous rehearsal strengthens organizational resilience and reduces the likelihood that minor failures escalate into major incidents.

CrowdStrike Falcon Platform

AI and Cloud-Native

Leverages the network effect of crowdsourced security data while eliminating the management burden of cumbersome on-premises solutions

Single Lightweight Sensor

Provides frictionless and scalable deployment and stops all types of attacks while eliminating sensor bloat and scheduled scans

Charlotte AI

Powers the CrowdStrike portfolio of agentic and GenAI capabilities across the Falcon platform (including natural-language chat, specialized agents, and embedded AI-powered features across modules), tapping into the petabyte scale of CrowdStrike's automated intelligence and further enriched by security experts to accelerate analyst workflows

Falcon Fusion SOAR

Provides native security orchestration, automation, and response (SOAR) capabilities within the Falcon platform to automate security workflows, reduce manual effort, and enable faster, more consistent threat response

CrowdStrike Enterprise Graph

Unifies and contextualizes security telemetry across domains, connecting users, assets, behaviors, and adversary activity into a single shared view of the enterprise to give humans and AI agents the context to see attack paths, reason over complexity, and act faster; specialized graphs include:

- **Asset Graph:** Solves one of the most complex customer problems today: identifying assets, identities, and configurations accurately across all systems (including cloud, on-premises, mobile, internet of things, and more) and connecting them together in a graph form
- **Intel Graph:** Enables security teams to proactively defend against emerging threats with intelligence-driven insights by mapping relationships between threat actors, tactics, vulnerabilities, and real-world attacks
- **Threat Graph:** Uses cloud-scale AI to correlate trillions of data points from multiple telemetry sources to identify shifts in adversarial tactics and map tradecraft to automatically predict and prevent threats in real time across CrowdStrike's global customer base

Falcon Foundry

Allows customers and partners to easily build custom, low-code applications that harness the data, automation, and cloud-scale infrastructure of the Falcon platform to solve your toughest cybersecurity challenges

CrowdStrike Marketplace

Offers an enterprise marketplace of technology partners where you can discover, try, buy, and deploy trusted CrowdStrike and partner applications that extend the CrowdStrike Falcon platform, without adding agents or increasing complexity

CrowdStrike Products

Endpoint Security

FALCON PREVENT | NEXT-GENERATION ANTIVIRUS

Protects against all types of threats, from malware and ransomware to sophisticated attacks, and deploys in minutes, immediately protecting your endpoints

FALCON INSIGHT XDR | DETECTION AND RESPONSE FOR ENDPOINT AND BEYOND

Offers industry-leading, unified EDR and XDR with enterprise-wide visibility to automatically detect adversary activity and respond across endpoints and all key attack surfaces

FALCON FIREWALL MANAGEMENT | HOST-BASED FIREWALL

Delivers simple, centralized host firewall management, making it easy to manage and control host firewall policies

FALCON DEVICE CONTROL | USB SECURITY

Provides the visibility and precise control required to enable safe usage of USB devices across your organization

FALCON FOR MOBILE | MOBILE THREAT DETECTION

Protects against threats to iOS and Android devices, extending endpoint security to your mobile devices, with advanced threat protection and real-time visibility into app and network activity

FALCON FORENSICS | FORENSIC CYBERSECURITY

Allows you to quickly respond and recover with automated forensic data collection, enrichment, and correlation

FALCON FOR XIoT | XIoT ASSET PROTECTION

Delivers real-time threat prevention and detection for extended internet of things (XIoT) assets, backed by XIoT-specific indicators of attack and indicators of compromise from CrowdStrike's industry-leading threat intelligence

FALCON INSIGHT FOR ChromeOS | ChromeOS PROTECTION

Delivers industry-first native detection and response for ChromeOS devices without requiring additional agents or mobile device management (MDM) solutions, providing unified visibility through the Falcon console

FALCON FOR LEGACY SYSTEMS | PROTECTION FOR LEGACY OPERATING SYSTEMS

Delivers anti-malware protection for Windows XP, Server 2003, Vista, and more while minimizing impact on resource-constrained systems and integrating with the Falcon platform

FALCON ADVERSARY OVERWATCH: ENDPOINT | THREAT HUNTING

Provides 24/7 managed endpoint threat hunting, proactively monitoring your environment to identify novel attacks, misuse of legitimate tools, credential compromise, insider threats, and adversary pivots from endpoint activity into other domains

Threat Intelligence and Hunting

FALCON ADVERSARY OVERWATCH | THREAT HUNTING

Provides 24/7 protection across endpoints, identities, cloud workloads, and next-gen SIEM, delivered by expert threat hunters powered by AI and threat intelligence to detect advanced intrusions and expose adversary tradecraft, credential misuse, and vulnerability exploitation

FALCON ADVERSARY INTELLIGENCE | SOC AUTOMATION

Cuts investigation time from days to minutes across the SOC with personalized, real-time threat intelligence, automating malware analysis and response through workflows and integrations while continuously monitoring the open, deep, and dark web for fraud and emerging threats

FALCON ADVERSARY INTELLIGENCE PREMIUM | ADVERSARY INTELLIGENCE

Delivers industry-leading intelligence reporting on 281 adversaries globally and enables you to defend against AI-powered adversaries with agentic AI built to reason across data, hunt for threats, and act decisively to automate and accelerate complex analyst workflows

FALCON COUNTER ADVERSARY OPERATIONS ELITE | ON-DEMAND ANALYST

Provides an assigned analyst who leverages AI-powered investigative and threat hunting tools, enhanced by deep adversary intelligence, to detect and disrupt adversaries across your IT environment and beyond

Cloud Security

FALCON CLOUD SECURITY: PROACTIVE SECURITY

Provides unified security posture management (USPM) and business context across cloud layers, leveraging industry-leading threat intelligence, end-to-end attack paths, and ExPRT.AI so cloud teams can swiftly prioritize their work, neutralize critical risks, and leave adversaries no room to strike

FALCON CLOUD SECURITY: CLOUD RUNTIME PROTECTION

Delivers leading cloud workload protection (CWP) and cloud detection and response (CDR), allowing SOC teams to detect and respond to active threats across hybrid clouds so adversaries are stopped in their tracks

FALCON CLOUD SECURITY: CNAPP

Includes the features and capabilities of both Proactive Security and Cloud Runtime Protection for Falcon Cloud Security

FALCON ADVERSARY OVERWATCH: CLOUD | THREAT HUNTING

Offers both proactive and protective security as a managed service through Falcon Adversary OverWatch cross-domain threat hunting and Falcon Complete Next-Gen MDR, powered by integrated threat intelligence to protect the cloud control plane, host OS, and data plane

SaaS Security

FALCON SHIELD | SaaS SECURITY

Unifies SaaS security posture management (SSPM) and SaaS-focused identity threat detection and response (ITDR), delivering a modern approach to SaaS security with comprehensive visibility, continuous control over SaaS security configurations, and real-time detection of active threats

AI Detection and Response

FALCON AI DETECTION AND RESPONSE | AIDR

Protects employee AI adoption and AI development at runtime by securing the prompt and agentic interaction layer with unified visibility, real-time threat detection, data protection, access controls, and automated response across endpoints, applications, AI agents, AI/API gateways, and cloud environments

Next-Gen Identity Security

FALCON NEXT-GEN IDENTITY SECURITY

Secures human, non-human, and AI identities by combining initial access prevention, modern secure privileged access, ITDR, SaaS identity security, and agentic identity protection to stop identity-driven breaches across domains

FALCON IDENTITY THREAT DETECTION

Provides unified visibility across hybrid identities and AI-driven threat detection to expose identity-based threats before they escalate

FALCON IDENTITY THREAT PROTECTION

Secures hybrid identities with AI-driven threat detection and response to stop identity-based attacks in real time

FALCON PRIVILEGED ACCESS

Eliminates standing privileges by enforcing just-in-time access based on real-time risk, removing the complexity of traditional privileged access management (PAM) solutions

FALCON ADVERSARY OVERWATCH: IDENTITY | THREAT HUNTING

Provides 24/7 managed identity threat hunting, proactively detecting identity-based attacks, monitoring criminal forums for stolen credentials, and enforcing MFA challenges to prevent unauthorized access

Next-Gen SIEM

FALCON NEXT-GEN SIEM | SIEM

Empowers you to stop breaches and get unified visibility across your security ecosystem by delivering industry-best detection, world-class threat intelligence, blazing-fast search, and AI-led investigation in one platform

FALCON ONUM | HIGH-PERFORMANCE DATA PIPELINE

Simplifies complex telemetry pipelines and enables precise, real-time control over how telemetry is collected, enriched, and routed in motion to deliver clean, high-quality signal for security and analytic workflows

FALCON ADVERSARY OVERWATCH: NEXT-GEN SIEM | THREAT HUNTING

Delivers end-to-end threat disruption by correlating first- and third-party Falcon Next-Gen SIEM data and proactively hunting advanced threats across network edge devices, SaaS applications, email security, operating systems, and more

Data Protection

FALCON DATA PROTECTION FOR ENDPOINT | REAL-TIME ENDPOINT DATA PROTECTION

Delivers real-time visibility, encryption detection, and behavioral analysis to stop unauthorized data exfiltration across Windows and macOS devices

FALCON DATA PROTECTION FOR CLOUD | RUNTIME CLOUD DATA PROTECTION

Provides real-time monitoring and classification of sensitive data in motion across cloud environments using eBPF, enabling organizations to detect and respond to data risks without added complexity and with minimal performance impact

Security and IT Operations

FALCON EXPOSURE MANAGEMENT | EXPOSURE MANAGEMENT

Provides full attack surface visibility, prioritizes vulnerabilities with AI, and automates remediation to proactively reduce cyber risk and prevent breaches

FALCON EXPOSURE MANAGEMENT: CAASM

Allows you to discover and monitor managed and unmanaged assets in real time and visually map assets and their relationships, revealing deep host insights into applications, browsers, CVEs, and misconfigurations

FALCON FOR IT | IT AUTOMATION

Delivers AI-powered endpoint visibility, scalable response automation, and secure baseline enforcement as a native capability of the Falcon platform

FALCON DISCOVER for XIoT | EXTENDED XIoT ASSET VISIBILITY

Delivers real-time visibility into unmanaged and adjacent XIoT assets to reduce security, safety, and operational blind spots

FALCON EXPOSURE MANAGEMENT FOR XIoT | XIoT RISK MITIGATION

Provides contextual risk visibility and remediation guidance tailored to the operational complexity of XIoT environments

FALCON FILEVANTAGE | FILE INTEGRITY MONITORING

Provides real-time, comprehensive, and centralized visibility that boosts compliance and offers relevant contextual data

Managed Services

FALCON COMPLETE NEXT-GEN MDR | MANAGED DETECTION AND RESPONSE

Provides 24/7 expert-driven protection across endpoints, identities, cloud workloads, and third-party Falcon Next-Gen SIEM data, combining elite security expertise, AI-powered technology, and proactive threat hunting to detect, disrupt, and remediate sophisticated threats at machine speed

CrowdStrike Services

INCIDENT RESPONSE

Provides 24/7/365 elite incident response to contain threats, restore order, and mitigate breach impact

Incident Response Services | Provides comprehensive breach response and recovery, from triage and investigation to cross-domain remediation and restoration, backed by world-class threat intelligence and delivered by a highly experienced incident response team

Services Retainer | Provides prearranged, on-demand access to CrowdStrike experts for rapid incident response and proactive consulting services that strengthen defenses over time

STRATEGIC ADVISORY SERVICES

Develops and matures the security program to improve defenses

Tabletop Exercise | Simulates incident response scenarios that expose process gaps and improve coordination across the full team, from hands-on-keyboard analysts to executive stakeholders

Maturity Assessment | Comprehensively evaluates your organization's security posture, identifying gaps, benchmarking capabilities, and providing a prioritized roadmap to strengthen defenses against evolving threats

Regulation Readiness and CXO Advisory | Helps you understand and prepare for cyber-related regulation mandates, including the evolving risk and governance responsibilities of the board of executives

Insider Risk Program Review | Strengthens your insider risk strategy by assessing and optimizing your current detection, prevention, and response capabilities

RED TEAM SERVICES

Tests and validates defenses through emulated attacks that expose weaknesses

Penetration Testing | Provides attack emulations that test the detection and response capabilities of your people, processes, and technology to identify vulnerabilities

Red Team/Blue Team Exercise | Increases response readiness under expert guidance, as a red team attacks systems in a simulated exercise and a blue team mounts the defense

Cloud Breach Emulation and Response Exercise | Helps organizations test and enhance their CDR capabilities through real-world adversary simulation

Adversary Emulation Exercise | Gauges readiness to defend against a sophisticated adversary infiltration that employs advanced tradecraft

AI SECURITY SERVICES

Secures the AI powering your organization and uses AI to defend with scale, precision, and speed

AI Red Team Services | Exposes vulnerabilities in the GenAI stack that could be exploited by testing LLM integrations for sensitive data exposure and adversarial manipulation

AI Systems Security Assessment | Provides Falcon-powered discovery and threat-informed testing to uncover shadow AI, risky integrations, and governance gaps, delivering clear visibility and actionable guidance

AI for SecOps Readiness | Provides expert guidance on integrating AI into detection and response workflows with tailored use cases, architectural guidance, and a roadmap to increase response speed, precision, and scale

TECHNICAL ASSESSMENT SERVICES

Audits and addresses security gaps across endpoints, cloud, and SaaS applications to tangibly reduce risk

Technical Risk Assessment | Highlights security vulnerabilities, weaknesses, and gaps in the IT environment across endpoint devices, applications, and user identities

Identity Security Assessment | Audits identity security practices and defense posture for weaknesses, including Active Directory domain configuration, account configuration, privilege delegation, and potential attack paths

Cloud Security Assessment | Identifies misconfigurations and vulnerabilities in the cloud estate that could be exploited by adversaries

Compromise Assessment | Exposes and addresses undetected threat activity through a one-time threat hunt available for endpoint, cloud, and SaaS applications

SaaS Security Assessment | Assesses SaaS environments for security gaps across configurations, access controls, data policies, and third-party integrations

PLATFORM PROFESSIONAL SERVICES

Helps ensure your CrowdStrike Falcon deployment is expertly configured, optimized, and aligned to your security needs; specialists provide best-practice implementation and deep module expertise to maximize protection, improve efficiency, and achieve security outcomes faster

TRAINING AND SECURITY UPSKILLING

Builds security acumen and closes the skills gap through CrowdStrike University, offering on-demand training, personalized learning paths, and five certifications for deep Falcon module expertise

CROWDSTRIKE PULSE SERVICES

Provides continuous consulting engagements via focused sessions on a recurring cadence (biweekly, monthly, or every two months) tailored to your needs, aligned with your priorities, and adapted as needed, enabling consistent progress, improved resilience, and strategic maturity that evolves at the speed of the adversary

About CrowdStrike

CrowdStrike (NASDAQ: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk – endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft, and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting, and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity, and immediate time-to-value.

CrowdStrike: We stop breaches.

Learn more: www.crowdstrike.com

Follow us: Blog | X | LinkedIn | Facebook | Instagram | YouTube

Start a free trial today: https://www.crowdstrike.com/trial