EXECUTIVE SUMMARY

CROWDSTRIKE

2026 GLOBAL THREAT REPORT

YEAR OF THE EVASIVE ADVERSARY

The Year of the Evasive Adversary

Each year, the Global Threat Report provides the cybersecurity industry with a comprehensive analysis of the previous year's threat landscape and the adversary behavior and tradecraft that shaped it. 2025 was the year of the evasive adversary.

Last year, adversaries responded to increasingly sophisticated defenses by exploiting inherent trust in supply chain partners, legitimate software, internal systems, and employees to gain initial access and move across environments undetected. And as organizations adopted AI, the adversaries targeting them did the same. Adversaries spanning all motivations exploited AI technology throughout 2025 to accelerate, optimize, and troubleshoot existing techniques.

To stop adversaries, we must know how they operate. Learning their behaviors, motivations, and techniques can inform a stronger understanding of their activity — and ultimately, a stronger defense.

The CrowdStrike 2026 Global Threat Report takes a look back at 2025 so readers can gain a fuller picture of the threats they face. This report consists of observations from the elite CrowdStrike Counter Adversary Operations team, which combines the power of threat intelligence with the speed of dedicated threat hunting teams and trillions of telemetry events from the AI-native CrowdStrike Falcon® platform.

This is an overview of the report's key findings, which detail critical information on what security teams need to know, and do, in an increasingly complex threat landscape.

Key Takeaways

Adversaries continue to accelerate:

The average eCrime breakout time — the time it takes for an adversary to move from an initially compromised host to another within the target organization — dropped to **29 minutes** in 2025, with the fastest breakout time recorded at **27 seconds**.

AI is in the adversary toolbox:

Adversaries explored the use of AI in attack types such as social engineering and information operations (IO), demonstrating growing proficiency with AI tools. Most threat actors that integrated AI increased their attack volume: CrowdStrike observed an **89%** increase in the number of attacks by AI-enabled adversaries compared to 2024.

AI has become a target:

As AI is embedded into development pipelines, SaaS platforms, and operational workflows, AI systems are becoming part of the attack surface. In 2025, adversaries exploited legitimate generative AI (GenAI) tools at more than **90 organizations** by injecting malicious prompts to generate commands for stealing credentials and cryptocurrency.

Trust is in the crosshairs:

Adversaries operated using 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, where they blended into normal activity.

Nation-state activity evolves:

China-nexus activity increased by **38%** across all sectors, with an **85%** increase in logistics targeting, and Democratic People's Republic of Korea (DPRK)-nexus incidents increased **130%** as FAMOUS CHOLLIMA's activity doubled year-over-year and STARDUST CHOLLIMA increased their operational tempo.

Zero-days are under siege:

CrowdStrike observed a **42% year-over-year** increase in zero-days exploited prior to public disclosure as adversaries weaponized dozens of them for initial access, remote code execution (RCE), and privilege escalation.

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

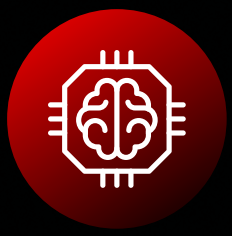
SPIDER
eCRIME

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

Interactive Intrusions by Region

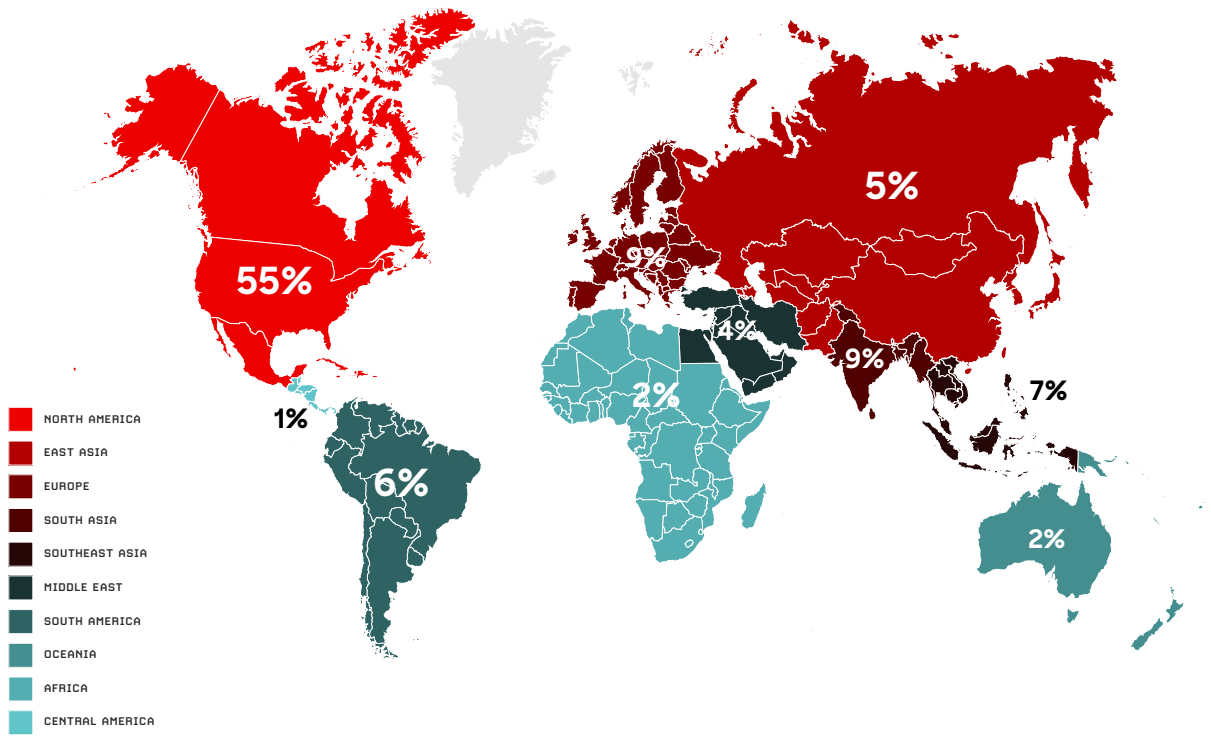


Figure 1. Interactive intrusions by region, January-December 2025

Top 10 Industries Targeted by Interactive Intrusions

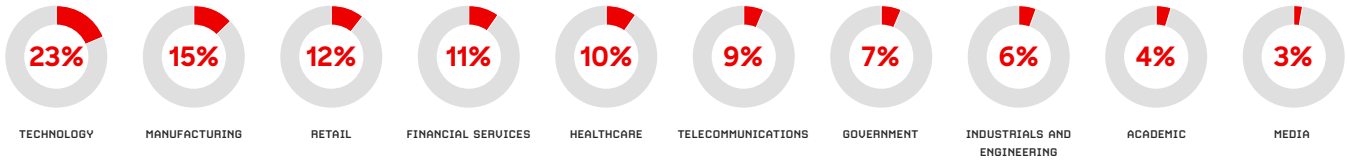


Figure 2. Top 10 industries targeted by interactive intrusions, January-December 2025

Key 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.

AI-ENHANCED THREATS

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

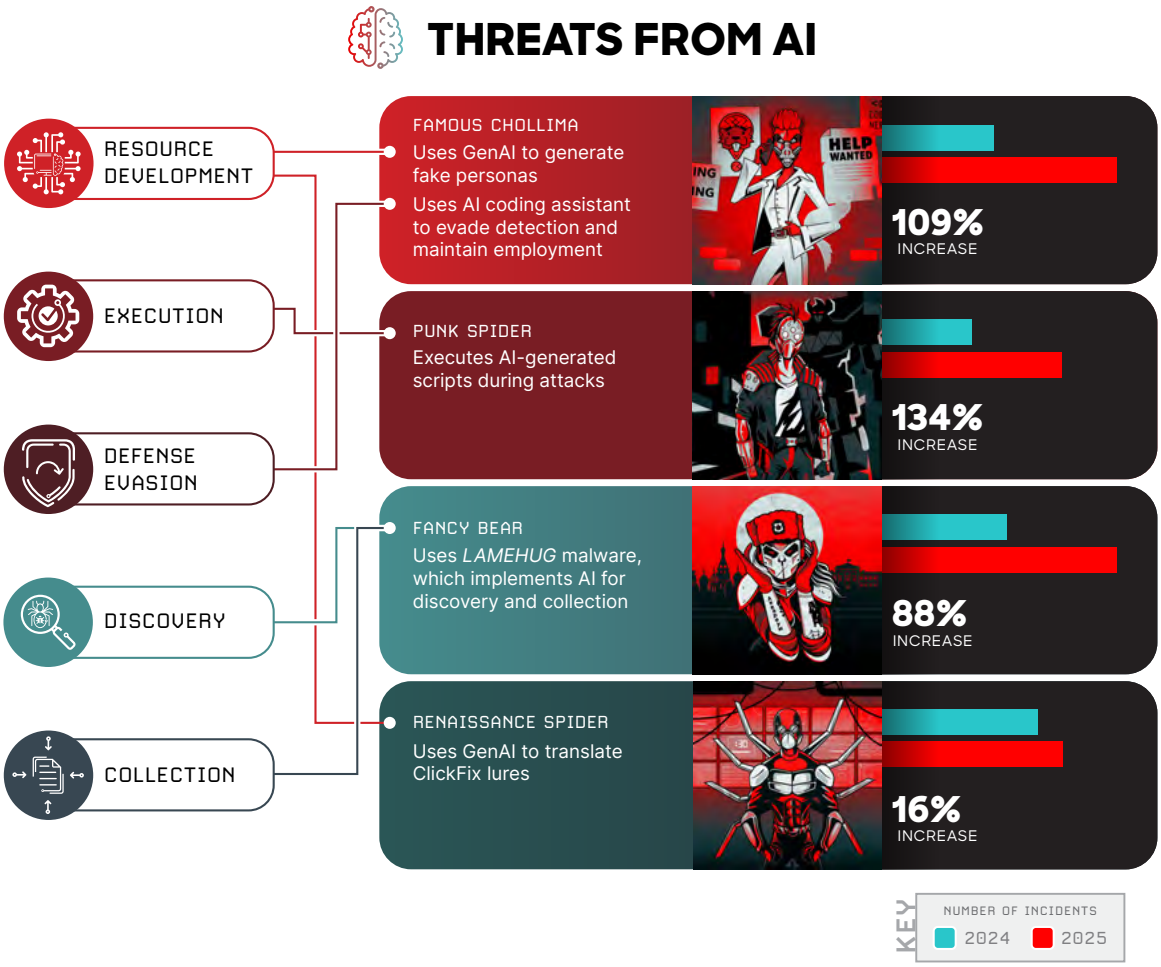


Figure 3. AI threats across the kill chain, 2024 vs. 2025

Threat actors are using AI to increase 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. Multiple AI-related tools have assisted threat actors with developing, organizing, and scaling phishing operations. These tools allow adversaries 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.

Adversaries are also using 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 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.

THREATS TO AI SYSTEMS

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

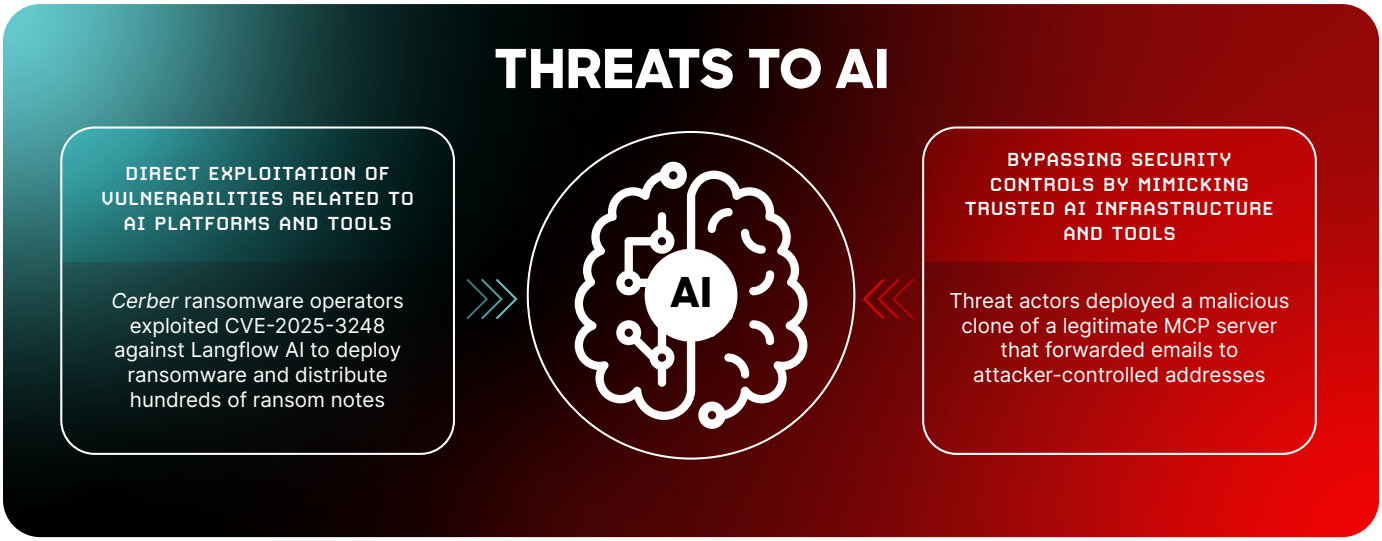


Figure 4. Threats to AI systems

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 an adversary-controlled address.

Ransomware Adversaries Expand Cross-Domain Tradecraft

In 2025, ransomware disrupted organizations' operations, inflicted financial losses, and caused reputational damage. In response to stronger defenses, adversaries have curated tradecraft that minimizes their need to interact with heavily monitored endpoints. The methods included gaining initial access via voice phishing (vishing), targeting cloud-based SaaS applications for data discovery and exfiltration, and in many cases, deploying ransomware solely on VMware ESXi infrastructure.

Modern enterprise networks are complex, with edge devices, identity solutions, endpoints, cloud environments, and virtualization infrastructure. This complexity is heightened by unmanaged assets such as VPNs and firewalls, employees' personal accounts and devices, unauthorized applications, and third-party contractor systems.

In cross-domain intrusions, sophisticated big game hunting (BGH) adversaries such as BLOCKADE SPIDER, PUNK SPIDER, and SCATTERED SPIDER move across these surfaces to evade detection. They consistently reach their goals by targeting unmanaged or poorly secured assets in victim environments.

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

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

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.

- In 2025, China-nexus adversaries demonstrated they can consistently operationalize publicly disclosed exploits within days of an exploit's release.
- Edge devices were targeted in 40% of cases in which a China-nexus adversary exploited a vulnerability during an intrusion in 2025.
- In 67% of the vulnerabilities China-nexus adversaries exploited, the flaw provided immediate system access.
- The sophistication and operational tempo of China-nexus threat actors' 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.
- China-nexus adversary targeting reflected intelligence collection priorities aligned with Chinese Communist Party strategic objectives, including telecommunications surveillance, economic espionage, and technology transfer.

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.

- Adversaries continued compromising software providers to enable supply chain attacks throughout 2025, typically in highly targeted operations with significant impacts.
- In 2025, CrowdStrike 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.
- Throughout 2025, threat actors frequently used supply chain attack methods to target Node Package Manager (npm) repositories that offer JavaScript-based libraries for the Node.js runtime environment.
- CrowdStrike anticipates supply chain attacks will continue to pose a significant threat to organizations throughout 2026; attackers value this method because it offers wide potential scope and allows them to hijack trusted update mechanisms.

Adversary Objectives Shape Zero-Day Exploit Selection

Throughout 2025, threat actors used dozens of zero-day exploits to enable initial access, RCE, and privilege escalation. CrowdStrike 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.[1]

- In 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.
- eCrime adversary GRACEFUL SPIDER differentiates themselves from other BGH adversaries by repeatedly exploiting zero-day vulnerabilities; this adversary targets vulnerabilities in internet-facing enterprise products in widespread campaigns.
- Some targeted intrusion adversaries, often driven by mandates to gain persistent access and collect intelligence, prioritize zero-days in internet-exposed endpoints; they frequently use them to gain initial access to unmanaged assets in high-value networks.

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

Adversaries Subvert Trust in Cloud Platforms and Services

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 assesses 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.
- Both eCrime and targeted intrusion threat actors have used adversary-in-the-middle (AiTM) phishing pages to enable credential collection and to access Microsoft 365 SaaS services for data collection.
- Both eCrime and targeted intrusion adversaries continued to target cloud-based SaaS applications throughout 2025; adversaries also continued targeting document management and storage suites, data warehousing platforms, and payroll and expense reimbursement applications.

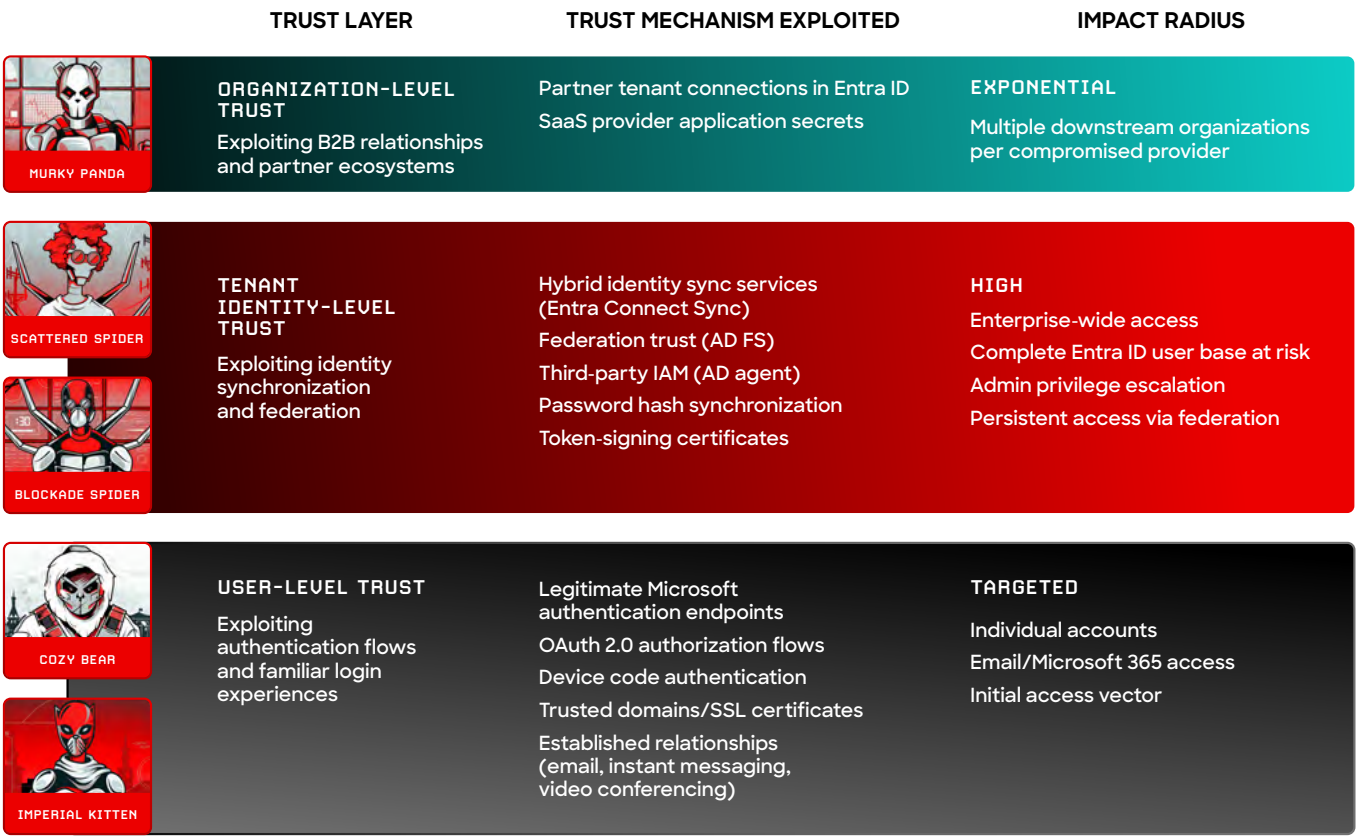


Figure 5. Layers of trust targeted by cloud-conscious threat actors

Conclusion

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

AI became a key adversary tool. Threat actors of all skill levels will continue adopting AI for social engineering, IO, and technical activity. 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.

BGH adversaries were the primary eCrime threat of 2025. These adversaries caused significant business disruptions in 2025, leading to substantial recovery costs and lost revenue for victims.

Targeted intrusion adversaries were persistent and adaptive in 2025. China-nexus adversaries are expected to maintain their high operational tempo while increasingly incorporating stealth tactics and targeting edge devices and internet-facing applications. DPRK-nexus adversaries will highly likely continue to prioritize operations focused on military intelligence collection, cryptocurrency theft, and revenue generation. Russia-nexus adversaries are expected to continue conducting aggressive operations, primarily to collect intelligence from Ukrainian targets and NATO member states.

In the vulnerability exploitation landscape, threat actors will continue to use evasion capabilities and 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 proof-of-concept (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. 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 to evolve in 2026, the CrowdStrike Counter Adversary Operations team remains committed to identifying, tracking, and disrupting threat actors while providing organizations with the intelligence and capabilities necessary to defend themselves in an increasingly sophisticated and persistent threat landscape.

Recommendations

CrowdStrike offers the following recommendations to help organizations defend against ever-evolving cyberattacks:

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 multifactor authentication (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 continuous integration and continuous delivery (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 endpoint detection and response (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 virtual machines, 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.

Download the Full Report

The CrowdStrike 2026 Global Threat Report presents a comprehensive analysis of the most significant trends and events in cyber threat activity in 2025. Download a free copy of the report at https://www.crowdstrike.com/global-threat-report/.

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