EXECUTIVE SUMMARY

CROWDSTRIKE

2025 GLOBAL THREAT REPORT

The Year of the Enterprising Adversary

Each year, the CrowdStrike 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. In its pages are the trends and events that defined 2024, the methods adversaries are using, and the steps organizations must take to protect themselves as threats evolve.

Throughout 2024, adversaries adopted a business-like approach, refining and scaling their successful strategies while exploring new technologies to fuel their speed and efficiency. Modern adversaries are determined and professional. They are quick to learn and adapt to changing defenses while staying laser-focused on their goals.

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

The CrowdStrike 2025 Global Threat Report takes a look back at 2024 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 executive summary 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.

» FOR MORE INFORMATION ON ANY OF THE ADVERSARIES MENTIONED IN THIS EXECUTIVE SUMMARY AND THOSE TARGETING YOUR INDUSTRY OR REGION, CHECK OUT THE CROWDSTRIKE ADVERSARY UNIVERSE.

Threat Landscape Overview

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 **48 minutes** in 2024, with the fastest breakout time recorded at **51 seconds**.

Access methods are evolving: Adversaries adopted voice phishing (vishing), callback phishing, and help desk social engineering to enter target networks. They also relied on compromised credentials: Access broker advertisements, which sell valid stolen credentials, surged **50% year-over-year**. **More than half (52%) of vulnerabilities** CrowdStrike observed in 2024 were related to initial access.

Stealth remains a priority: Modern threats are dominated by interactive intrusion techniques, where adversaries use hands-on-keyboard actions to achieve their goals. In 2024, **79% of detections were malware-free**, and CrowdStrike observed a **35% year-over-year increase** in interactive intrusion campaigns.

Generative AI is in the adversary toolbox: Adversaries increasingly used generative AI (genAI) in 2024 to improve social engineering, accelerate misinformation operations, and support malicious network activity.

China's cyber enterprise grows: China-nexus activity increased by **150% across all sectors**, with a staggering **200-300%** surge in key targeted industries such as financial services, media, manufacturing, and industrials/engineering.

Cloud environments are under siege: Cloud continues to be a prime target due to its vast data, scalability, and exploitable misconfigurations. In 2024, CrowdStrike saw a **26% increase** in new and unattributed cloud intrusions, indicating more adversaries are targeting cloud services.

NAMING CONVENTIONS

ADVERSARY	NATION-STATE OR CATEGORY
BEAR	RUSSIA
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	TURKEY

Interactive Intrusions by Region

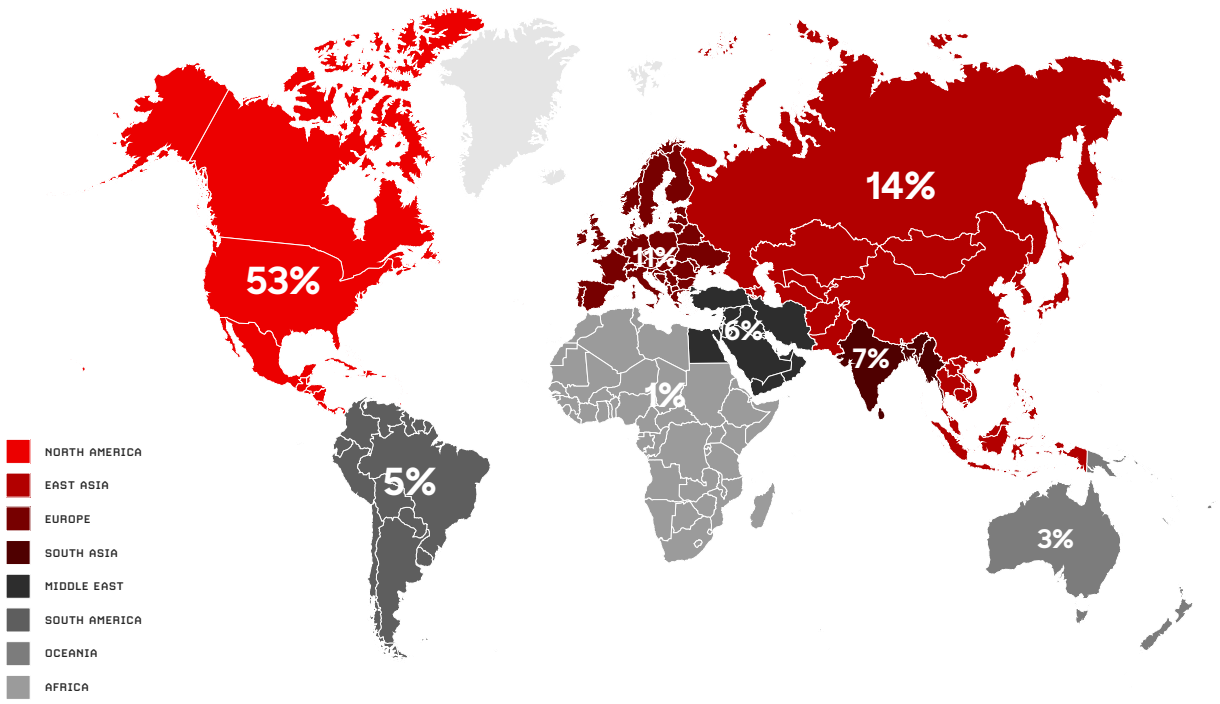

Figure 1. Interactive intrusions by region, January-December 2024

Top 10 Industries Targeted by Interactive Intrusions

Figure 2. Top 10 industries targeted by interactive intrusions, January-December 2024

These statistics highlight the global reach of adversary operations and the necessity for cross-domain security strategies that account for identity compromise, lateral movement, and cloud-based attack vectors.

The shift toward malware-free attack techniques has been a defining trend over the past five years. In 2024, malware-free activity accounted for 79% of detections, a significant rise from 40% in 2019.

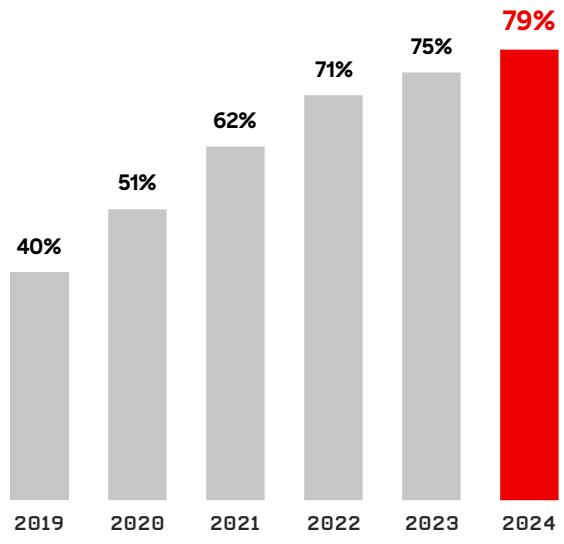

Figure 3. Percentage of detections that were malware-free, 2019-2024

Key Adversary Themes

THE BUSINESS OF SOCIAL ENGINEERING

Initial access techniques shifted in 2024 as adversaries targeted human weaknesses, using compromised credentials and social engineering to gain access and move laterally within organizations. CrowdStrike observed a surge in telephone-oriented social engineering campaigns and help desk manipulation, signaling an evolution in eCrime tactics.

- Vishing operations grew 442% between the first and second half of 2024.
- Sophisticated eCrime groups such as CURLY SPIDER, CHATTY SPIDER, and PLUMP SPIDER used these tactics to steal credentials, establish remote sessions, and evade detection.
- Throughout 2024, CrowdStrike tracked at least six similar but likely distinct campaigns in which threat actors posing as IT staff called targets and tried to persuade them to establish remote support sessions.

CASE STUDY

CURLY SPIDER

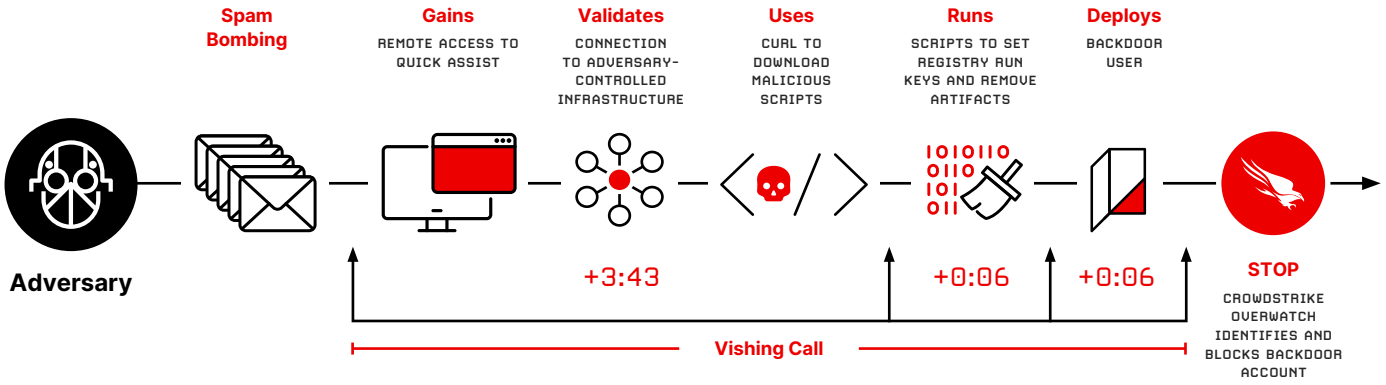

Figure 4. Timeline of CrowdStrike OverWatch moving faster than CURLY SPIDER to stop a social engineering attack in less than four minutes

In 2024, CURLY SPIDER emerged as one of the fastest and most adaptive eCrime adversaries. In this case, they attempted to achieve their goals without needing to break out to another device. The entire attack chain — from initial user interaction and social engineering to introducing a backdoor account to establish persistence — took under four minutes.

Once CURLY SPIDER gains initial access, their window of opportunity is limited; access will only last as long as the victim is on the call. To extend control, the adversary's immediate objective is to establish persistent access before the session ends.

With remote access secured, CURLY SPIDER moves quickly — often while still actively engaging with the victim — to deploy their payloads and establish persistence. Most of the intrusion time is spent ensuring connectivity and troubleshooting access issues to reach their cloud-hosted malicious scripts.

Generative AI and the Enterprising Adversary

Despite the relative novelty of genAI, CrowdStrike has identified several examples of adversaries using it. GenAI's low barrier to entry and powerful capabilities make it an appealing tool. It enables threat actors to craft convincing phishing emails, conduct deception campaigns, and develop malicious scripts, a trend expected to continue in 2025.

- Large language models (LLMs) and genAI models that create photorealistic imagery can generate convincing content at scale with minimal expertise. They can support social engineering efforts or information operations.
- CrowdStrike responded to FAMOUS CHOLLIMA activity in **304 incidents throughout the year**, with **40% representing insider threat operations**. In some cases, the adversary used genAI to create fake LinkedIn profiles.
- NITRO SPIDER used AI-generated websites in malvertising campaigns, filtering victims through malicious ads before redirecting others to AI-created fake pages.

China's Growing Cyber Enterprise

In 2024, China's cyber espionage capabilities reached a critical inflection point marked by increasingly bold targeting, stealthier tactics, and expanded operational capacity. These advancements reflect China's strategic intelligence priorities, including regional influence, technology acquisition, and suppression of perceived threats to regime stability.

- Throughout 2024, China-nexus adversaries continued to operate in every sector and region across the globe, maintaining the scope of their operations while increasing their scale.
- CrowdStrike identified seven new China-nexus adversaries in 2024, highlighting a shift toward more targeted and mission-specific intrusions. Five of these groups are unique in their specialization and sophistication.
- LIMINAL PANDA, LOCKSMITH PANDA, and OPERATOR PANDA are high-capability adversaries with unique telecom network targeting remits and toolsets; VAULT PANDA focuses on the financial services sector worldwide; and ENVOY PANDA is a previously low-capability adversary who has markedly increased their operations security (OPSEC) posture.

Cloud-Conscious Actors Continue to Innovate

Cloud-focused adversaries exploit misconfigurations, stolen credentials, and cloud management tools to infiltrate systems, move laterally, and maintain persistent access for activities like data theft and ransomware deployment. China- and North Korea-nexus actors expanded their targeting of cloud platforms, and eCrime groups adopted advanced tactics such as abusing trust relationships and insider threats to compromise cloud resources.

- Valid account abuse has become the primary initial access tactic, accounting for **35% of cloud incidents** in the first half of 2024. Attackers are increasingly using stealth-oriented tactics and trying to access credentials to target valid accounts.
- In 2023, eCrime adversary SCATTERED SPIDER accounted for **30% of all cloud intrusions**. This number fell to **13% in 2024**, partly because many nation-state and opportunistic threat actors are increasingly targeting the cloud control plane.
- In **75% of observed cases**, cloud-conscious actors removed indicators from log files in an attempt to evade detection.

Enterprising Vulnerability Exploitation

Adversaries are increasingly targeting internet-exposed network appliances, exploiting their inherent security weaknesses to gain initial access where endpoint detection and response (EDR) visibility is limited. They achieve remote code execution (RCE) with techniques such as chaining exploits or abusing legitimate product features, and they often repurpose known vulnerabilities to repeatedly compromise the same devices. Adversaries continue to target end-of-life appliances, as outdated systems with unpatched vulnerabilities provide footholds into target environments.

- Threat actors are targeting vulnerabilities within the network appliance's proprietary operating system (OS). These vulnerabilities are appealing targets because they potentially allow attackers to use one flaw to target multiple products running the same OS.
- Chaining multiple vulnerabilities offers attackers more advantages. First, it allows them to achieve unauthenticated RCE by combining multiple exploits in one attack. Second, exploit chaining undermines the severity score-based patching process that many enterprises follow.
- To discover new vulnerabilities or abuse legitimate product features, adversaries will likely use technical blogs and operationalize public proof-of-concept (POC) exploits faster than in previous years.

SaaS Exploitation Expected to Continue

Throughout 2024, CrowdStrike Intelligence observed several eCrime and targeted intrusion adversaries use access to cloud-based software as a service (SaaS) applications to obtain data to facilitate lateral movement, extortion, and third-party targeting. Threat actors often accessed these applications by compromising single sign-on (SSO) identities. As cloud adoption grows, we expect adversaries to refine their tradecraft in 2025, making SaaS exploitation a critical and evolving threat.

- In the first half of 2024, cloud-conscious threat actors frequently targeted Microsoft 365, with **SharePoint accessed in 22% of intrusions and Outlook in 17%**.
- SCATTERED SPIDER has leveraged compromised SSO accounts to access a wide range of integrated SaaS applications, including chat, customer relationship management, credential management, document storage, productivity, and security tools.
- In many intrusions, adversaries searched SaaS applications for the following information: 1) account credentials and network architecture documentation to conduct lateral movement and 2) cyber insurance and revenue data to inform extortion demands.

Conclusion

As 2025 begins, the cybersecurity landscape continues to rapidly evolve, presenting significant challenges for organizations in all sectors and geographies. Adversaries' resilience, innovation, and adaptability underscore the critical need for a comprehensive understanding of today's threats across every aspect of the landscape.

Social engineering proliferated throughout 2024 as adversaries explored new initial access methods to bypass security defenses. GenAI became a key adversary tool, especially in support of social engineering campaigns and high-tempo intelligence operations (IO) campaigns. CrowdStrike anticipates it will be employed in 2025 adversary operations.

Targeted eCrime adversaries remain a persistent threat to specific sectors. Throughout 2024, they demonstrated tenacity in their targeting, often compensating for lower sophistication by gaining in-depth knowledge about victims' sectors, geographies, and associated technologies.

Targeted intrusion adversaries were active and innovative in 2024, adapting their tactics to achieve geopolitical and strategic goals while evading improved defenses. Russia-nexus adversaries are expected to continue their aggressive pursuit of victory in Ukraine, focusing on intelligence collection operations targeting Ukraine and NATO members. China-nexus adversaries will likely benefit from long-term investments in cyber programs, manifesting in increased OPSEC practices, a sustained high operational tempo, and prolific global intrusion activity.

The vulnerability exploitation landscape remains a critical concern. Threat actors are expected to continue aggressively targeting devices at the network periphery, particularly network appliances. SaaS applications are also in the crosshairs. After observing eCrime and targeted intrusion adversaries use access to cloud-based SaaS applications to obtain data for lateral movement, extortion, and third-party targeting in 2024, CrowdStrike anticipates SaaS exploitation will be a threat to watch in 2025.

Throughout 2024, the enterprising adversary expanded the maturity and sophistication of their operations across sectors and geographies. As these threats evolve in 2025, the CrowdStrike Counter Adversary Operations team remains committed to identifying, tracking, and disrupting threat actors whenever and wherever possible.

Recommendations

1 Secure the entire identity ecosystem

Adversaries increasingly target identities using credential theft, multifactor authentication (MFA) bypass, and social engineering while covertly moving laterally between on-premises, cloud, and SaaS environments via trusted relationships. This allows them to impersonate legitimate users, escalate access, and evade detection.

Organizations should adopt phishing-resistant MFA solutions, such as hardware security keys, to prevent unauthorized access. Strong identity and access policies are essential, including just-in-time access, regular account reviews, and conditional access controls. Identity threat detection tools must monitor behavior across endpoints and on-premises, cloud, and SaaS environments to flag privilege escalation, unauthorized access, or backdoor account creation. Integrating these tools with extended detection and response (XDR) platforms ensures comprehensive visibility and a unified defense against adversaries.

Additionally, organizations should educate users to recognize vishing and phishing attempts while maintaining proactive monitoring to detect and respond to identity-based threats.

2 Eliminate cross-domain visibility gaps

Adversaries' growing use of hands-on-keyboard techniques and legitimate tools makes detection and response more difficult. Unlike traditional malware, these methods allow attackers to bypass traditional security measures by executing commands and using legitimate software to mimic normal operations.

To counter this, organizations must modernize their detection and response strategies. XDR and next-generation security information and event management (SIEM) solutions provide unified visibility across endpoints, networks, cloud environments, and identity systems, enabling analysts to correlate suspicious behaviors and see the full attack path.

Proactive threat hunting and threat intelligence further enhance detection by identifying potential attack patterns and providing insights into adversary tactics, techniques, and procedures. With real-time intelligence, organizations can stay informed about emerging threats, anticipate attacks, and prioritize critical security efforts.

3 Defend the cloud as core infrastructure

Cloud-focused adversaries are exploiting misconfigurations, stolen credentials, and cloud management tools to infiltrate systems, move laterally, and maintain persistent access for malicious activities like data theft and ransomware deployment.

Cloud-native application protection platforms (CNAPPs) with cloud detection and response (CDR) capabilities are critical to counter these threats.

These solutions provide operators with a unified view of their cloud security posture, helping them rapidly detect, prioritize, and remediate misconfigurations, vulnerabilities, and adversary threats. Additionally, enforcing strict access controls — such as role-based access and conditional policies — limits exposure to critical systems and ensures continuous monitoring for anomalies, including logins from unexpected locations.

Regular audits are also critical to maintaining security. Automated tools can uncover overly permissive storage settings, exposed APIs, and unpatched vulnerabilities. Frequent reviews of cloud environments ensure unused permissions and outdated configurations are addressed promptly.

4 Prioritize vulnerabilities with an adversary-centric approach

Adversaries are increasingly exploiting publicly disclosed vulnerabilities and using exploit chaining, combining multiple vulnerabilities to gain rapid access, escalate privileges, and bypass defenses. These multi-stage attacks often rely on public resources like POC exploits and technical blogs, enabling adversaries to craft effective and hard-to-detect payloads.

To counter these threats, organizations must prioritize regular patching or upgrading of critical systems, especially frequently targeted internet-facing services like web servers and VPN gateways. Monitoring for subtle signs of exploit chaining, such as unexpected crashes or privilege escalation attempts, can help detect attacks before they progress.

Tools like CrowdStrike Falcon® Exposure Management, built with native AI prioritization, enable teams to reduce noise and focus on the vulnerabilities that matter most, specifically those affecting critical and high-risk systems. By adopting proactive security approaches, discovering exposures across the attack surface, and leveraging automation, organizations can mitigate sophisticated threats and limit adversary opportunities.

5 Know your adversary and be prepared

When a cyberattack unfolds in minutes — or even seconds — being prepared can be the difference between containment and catastrophe. An intelligence-driven approach enables security teams to move beyond reactive defense by understanding which adversary is targeting them, how they operate, and what their objectives are. With threat intelligence, adversary profiling, and tradecraft analysis, security teams can prioritize resources, adapt defenses, and actively hunt for threats before they escalate. CrowdStrike's threat intelligence doesn't just detect known threats — it anticipates new and evolving tradecraft, ensuring defenders are always one step ahead. By seamlessly integrating intelligence into security workflows, organizations can accelerate response times, disrupt adversaries, and turn intelligence into action.

Though technology is critical to detect and stop intrusions, the end user remains a crucial link in the chain to stop breaches. Organizations should initiate user awareness programs to combat the continued threat of phishing and related social engineering techniques. For security teams, practice makes perfect. Encourage an environment that routinely performs tabletop exercises and red/blue teaming to identify gaps and eliminate weaknesses in your cybersecurity practices and response.

Download the Full Report

The CrowdStrike 2025 Global Threat Report presents a comprehensive analysis of the most significant trends and events in cyber threat activity in 2024. Download a free copy of the report at https://www.crowdstrike.com/global-threat-report/.

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: www.crowdstrike.com/free-trial-guide