CROWDSTRIKE

2025 GLOBAL THREAT REPORT

Foreword

Don't Underestimate Today's Enterprising Adversaries

Watch any nature program, and you'll quickly discover what happens to animals that underestimate their adversaries. They become prey. The same principle applies in cybersecurity — the adversary is advancing so fast that you can't afford to underestimate them.

Our latest research demonstrates that adversaries are becoming more efficient, focused, and business-like in their approach — in many ways, more like the enterprise organizations they prey upon. That's why our team of security analysts, experts, and authors chose "the enterprising adversary" as the theme for this year's CrowdStrike Global Threat Report.

Take generative artificial intelligence (genAI), for instance. Highly effective adversaries across all major categories — nation-state, eCrime, and hacktivist — have become early and avid adopters. The "force multiplier" impact of off-the-shelf chatbots has made genAI a popular addition to the global hacker toolbox.

Along with legitimate organizations, easy access to commercial large language models (LLMs) is making adversaries more productive, too. It's shortening their learning curve and development cycles, and it's allowing them to increase the scale and pace of their activities. Though this report indicates that malicious use of AI is growing, it remains largely iterative and evolutionary at this point in time. Only occasionally does it manifest as an entirely novel use case. **But it is still early days.**

At CrowdStrike, we aren't waiting for threat actors to experience their next "aha" moment. We are accelerating our own use of AI techniques — from our foundational machine learning capabilities to our leading-edge generative and agentic AI models — to help our customers anticipate the next zero-day attacks in advance and proactively inoculate themselves against them. This is the essence of an AI-native approach to cyber defense. Unlike legacy systems — which are still relied upon by organizations globally — we don't sit idle until an attack occurs before we can identify and stop it.

Adversarial Enterprise Takes Its Toll

The job of protecting your organizations continues to get harder by the day. You'll find ample evidence of this fact in the data that follows. The number of new "named adversaries" tracked by the elite CrowdStrike Counter Adversary Operations team continues to expand, and established adversaries are constantly adding new targets and more sophisticated techniques to their evasion, intrusion, and exfiltration arsenals.

The purpose of this report is to arm you, the world's security professionals and dedicated cyber defenders, with the knowledge you need to keep a step ahead of these threat actors — and to never, ever underestimate them.

Here are a few key facts you should know about the shifting threat landscape:

- Breakout time — how long it takes for an adversary to start moving laterally across your network — reached an all-time low in the past year: The average fell to **48 minutes**, and the fastest breakout time we observed dropped to a mere **51 seconds**.
- Voice phishing (vishing) attacks, where adversaries call victims to amplify their activities with persuasive social engineering techniques, saw explosive growth — up **442%** between the first and second half of 2024.
- Attacks related to initial access boomed, accounting for **52%** of vulnerabilities observed by CrowdStrike in 2024. Providing access as a service became a thriving business, as advertisements for access brokers increased **50% year-over-year**.
- Among nation-states, China-nexus activity surged **150%** overall, with some targeted industries suffering **200% to 300%** more attacks than the previous year.
- GenAI played a pivotal role in sophisticated cyberattack campaigns in 2024. It enabled **FAMOUS CHOLLIMA** to create highly convincing fake IT job candidates that infiltrated victim organizations, and it helped China-, Russia-, and Iran-affiliated threat actors conduct AI-driven disinformation and influence operations to disrupt elections.

As with every product and service we provide, we hope this year's Global Threat Report makes you more aware, more attuned to the threats you may be facing now or in the near future, and better equipped overall to defend your organization.

CrowdStrike remains at your service and wholly dedicated to the single-minded vision and mission on which the company was founded more than a decade ago. Our company, our platform, and our people are focused on one thing: **working together in close partnership with our customers to stop breaches.**

George Kurtz

CrowdStrike CEO and Founder

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

Table of Contents

Introduction

The CrowdStrike 2025 Global Threat Report is the industry's preeminent source on adversary intelligence, examining the emerging adversary trends of the past year. During 2024, adversaries matured faster than ever, innovating techniques and tools as well as finding creative solutions to circumvent modern defenses, all while staying laser-focused on their targets. Adversaries are streamlining their tactics, refining and scaling successful strategies, and learning from both their own and their colleagues' mistakes and successes to conduct attacks with a business-oriented approach. 2024 was the year of the enterprising adversary.

eCrime adversaries exemplified such enterprising cyberattacks, constantly adapting to shifting environments and quickly scaling effective operations. Throughout 2024, initial access techniques began to shift — eCrime adversaries began moving away from phishing to alternative access methods. This shift suggests that commodity malware operators are likely finding more effective and successful infections with innovative techniques as they face hardened security defenses. One such technique that proliferated in 2024 is social engineering leveraging telephony-based exploitation: Various eCrime adversaries are increasingly adopting vishing, callback phishing, and help desk social engineering attacks to gain a foothold into networks.

These shifting initial access methods are consistent with a larger trend identified in the CrowdStrike 2024 Threat Hunting Report: Rather than delivering malware, eCrime adversaries are increasingly leveraging legitimate remote monitoring and management (RMM) tools to access a victim's system — and therefore making malware non-essential for successful operations. Throughout 2024, eCrime actors frequently leveraged RMM tools in their campaigns.

In 2024, China's cyber espionage operations reached new levels of maturity, with adversaries maintaining a higher operational tempo than observed in 2023 and engaging in prolific targeting. Decades of government investment into China's cyber workforce and programs have yielded matured capabilities and efficiencies as well as an increasing number of new, specialized China-nexus adversaries. In 2024, CrowdStrike graduated seven new China-nexus adversaries and observed a 150% increase in China-nexus activity across all sectors on average compared to 2023. Additionally, China-nexus adversaries increasingly prioritized operations security (OPSEC) and at-scale infrastructure management by obfuscating their activities via operational relay box (ORB) networks.

Democratic People's Republic of Korea (DPRK)-nexus adversaries LABYRINTH CHOLLIMA, VELVET CHOLLIMA, and SILENT CHOLLIMA consistently targeted defense and aerospace entities in various countries. However, similar to previous years, most of these adversaries' cyber operations focused on generating currency, which has become a lifeline for the regime. Notably, FAMOUS CHOLLIMA innovated their currency generation operations in 2024 by leveraging their IT worker schemes at scale across the globe. During 2024, CrowdStrike Falcon® Adversary OverWatch™ threat hunters responded to 304 FAMOUS CHOLLIMA incidents, with nearly 40% of these representing insider threat operations.

While DPRK adversaries have skillfully shifted their operations to support large-scale currency generation over the years, the specific tactics deployed in their 2024 operations — such as leveraging virtual interviews, allocating significant resources and staffing, and using laptop farms at scale — highlight the DPRK's enterprising approach to computer network operations (CNO).

Across the 2024 vulnerability threat landscape, threat actors continued to target devices in the network periphery and regularly leveraged publicly available vulnerability research — such as disclosures, technical blogs, and proof-of-concept (POC) exploits — to aid their malicious activity. Within the cloud landscape, an increasing number of new adversaries effectively exploited cloud environments, often employing previously tested techniques and adapting them for their own goals.

Adversaries also leveraged genAI when conducting intelligence operations (IO) targeting election processes. Throughout 2024, adversaries increasingly adopted genAI, especially as a part of social engineering efforts.

Staying one step ahead of the enterprising adversary is difficult — but not impossible. As the adversary matures, so do your defenses. As the adversary innovates, so does CrowdStrike. CrowdStrike Counter Adversary Operations raises the operational cost of conducting malicious cyber operations by combining the power of threat intelligence with the speed of dedicated hunting teams and trillions of cutting-edge telemetry events from the AI-native CrowdStrike Falcon® platform to detect, disrupt, and stop today's sophisticated adversaries.

Counter Adversary Operations comprises two closely integrated teams. The CrowdStrike Intelligence team provides actionable reporting that identifies new adversaries, monitors their activities, and captures emerging cyber threat developments in real time. The CrowdStrike OverWatch team uses this intelligence to conduct proactive threat hunting across customer telemetry to detect and address malicious activity.

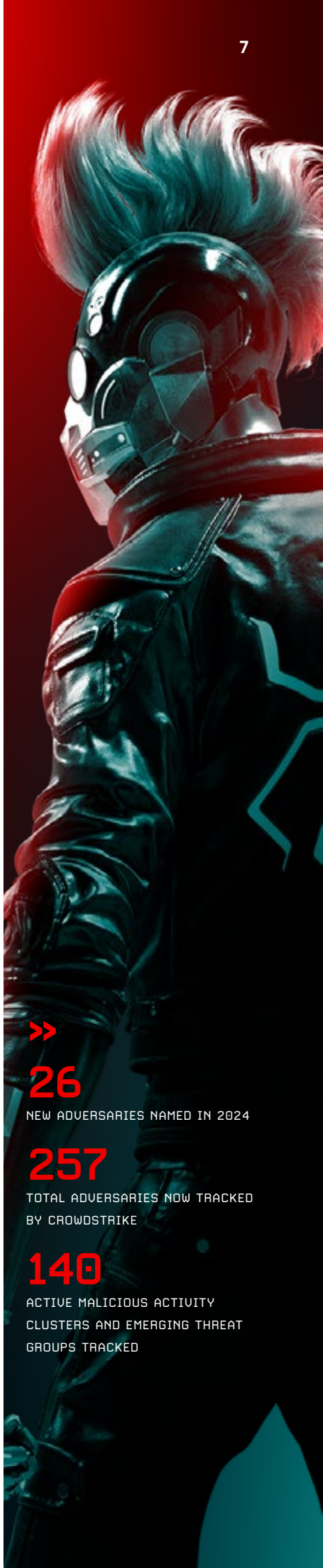
» DURING 2024, CROWDSTRIKE FALCON ADVERSARY OVERWATCH THREAT HUNTERS RESPONDED TO 304 FAMOUS CHOLLIMA INCIDENTS, WITH NEARLY 40% OF THESE REPRESENTING INSIDER THREAT OPERATIONS.

During 2024, CrowdStrike Intelligence introduced 26 newly named adversaries — including the new Kazakhstan-based adversary COMRADE SAIGA — raising the total number of named adversaries tracked across all motivations to 257. In addition to named adversaries, CrowdStrike Intelligence tracks more than 140 active malicious activity clusters and emerging threat groups.

In the past year, CrowdStrike has been working to enrich the in-platform Falcon experience by providing further insights from CrowdStrike's broad view into the changing threat landscape in different industries and regions. CrowdStrike ties these insights to activity occurring outside the customer perimeter by monitoring the criminal underground and emerging threats.

New dashboards provide insight into Falcon Adversary OverWatch threat hunting findings across CrowdStrike's customer ecosystem, while click-to-hunt capabilities enable seamless transition from new threat hunting query feeds to real-time investigations in CrowdStrike Falcon® Next-Gen SIEM. Additionally, new Counter Adversary Playbooks make it easy to build comprehensive intelligence monitoring programs customized for any organization.

The CrowdStrike 2025 Global Threat Report summarizes the CrowdStrike Intelligence team's analysis performed throughout 2024 and describes notable themes, trends, and events across the cyber threat landscape. This annual report also includes anticipatory threat assessments to help prepare and protect organizations throughout the coming year.



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

Threat Landscape Overview

Cyberattacks are escalating in speed, volume, and sophistication. As organizations work to strengthen their defenses, adversaries target their weaknesses: employees susceptible to social engineering and systems lacking modern security controls. Once inside, they act within seconds, stealthily moving across networks to execute attacks. In 2024, 79% of the detections CrowdStrike observed were malware-free, indicating adversaries are instead using hands-on-keyboard techniques that blend in with legitimate user activity and impede detection.

China-nexus activity surged **150%** across all sectors, with a staggering **200-300%** increase in key targeted industries

Vishing attacks skyrocketed **442%** between the first and second half of 2024

Average eCrime breakout time dropped to **48 minutes**, with the fastest breakout observed at just **51 seconds**

79% of detections in 2024 were malware-free, up from **40%** in 2019

Access broker advertisements increased **50%** year-over-year

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

52% of vulnerabilities observed by CrowdStrike in 2024 were related to initial access

26 new adversaries tracked by CrowdStrike, raising the total to **257**

The Growing Reliance on Identity Attacks and Vulnerability Exploits

Every breach starts with initial access, and identity-based attacks are among the most effective entry methods. Instead of traditional malware, adversaries favor faster and stealthier methods such as vishing, social engineering, access broker services, and trusted relationship abuse.

A major driver behind this shift is the rise of access brokers: specialists who acquire access to organizations and sell it to other threat actors, including ransomware operators. Access broker activity surged in 2024, with advertised accesses increasing by nearly 50% over 2023. Meanwhile, valid account abuse was responsible for 35% of cloud-related incidents, reflecting attackers' growing focus on identity compromise as a gateway to broader enterprise environments.

But identity isn't the only target — adversaries are also exploiting vulnerabilities to gain initial access. In 2024, 52% of observed vulnerabilities were linked to initial access, reinforcing the need to secure exposed systems before attackers establish a foothold.

As adversaries scale identity-based attacks and vulnerability exploitation, organizations must adopt proactive defense strategies, including identity verification, risk-based patching, and early detection of credential abuse, to disrupt adversary operations before they escalate.

MONTH	2024
JANUARY	590
FEBRUARY	306
MARCH	242
APRIL	186
MAY	813
JUNE	201
JULY	177
AUGUST	151
SEPTEMBER	253
OCTOBER	386
NOVEMBER	328
DECEMBER	853
TOTAL	**4,486**

Figure 1. Access broker advertisements by month, 2024

The Continued Rise of Interactive Intrusions

Modern cyber threats are increasingly dominated by "interactive intrusion" techniques, where adversaries execute hands-on-keyboard actions to achieve objectives. Unlike traditional malware attacks, these intrusions rely on human adversaries mimicking legitimate user or administrator behavior, making them exceptionally difficult to detect.

In 2024, CrowdStrike observed a 35% year-over-year increase in interactive intrusion campaigns. For the seventh consecutive year, the technology sector remained the most targeted industry, with high attack volumes also observed in consulting, manufacturing, and retail. The charts on the following page reflect the relative frequency of intrusions in the top geographical regions and industry verticals.

Interactive Intrusions by Region

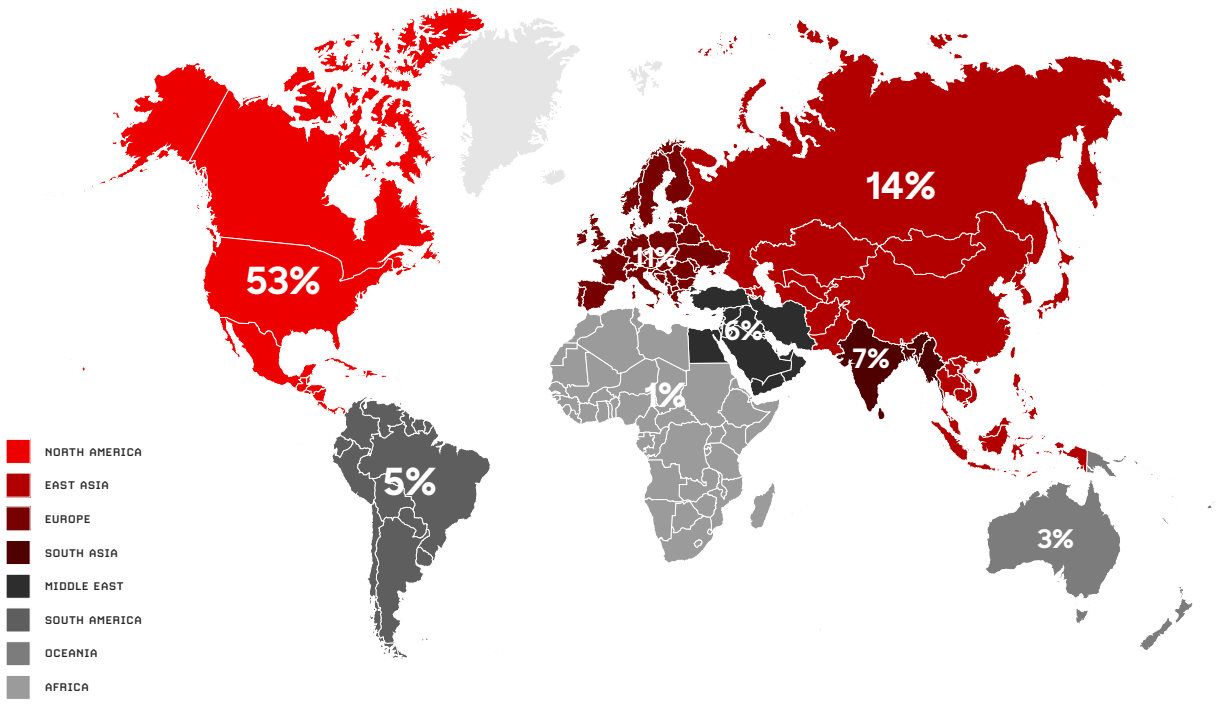


Figure 2. Interactive intrusions by region, January-December 2024

Top 10 Industries Targeted by Interactive Intrusions

Figure 3. 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.

This 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.

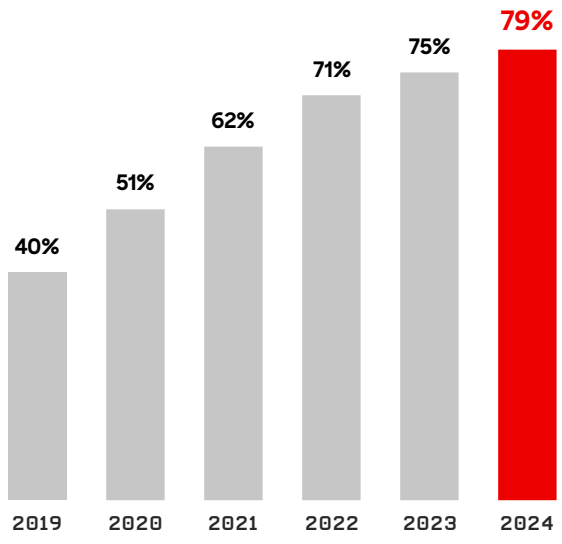


Figure 4. Percentage of detections that were malware-free, 2019-2024

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.

In 2024, the average breakout time for interactive eCrime intrusions fell to 48 minutes, down from 62 minutes in 2023. Alarmingly, the fastest breakout was recorded at just 51 seconds — meaning defenders may have less than a minute to detect and respond before attackers establish deeper control.

This rapid escalation in breakout time reinforces the need for:

- **Real-time threat detection** to identify and halt intrusions before they spread
- **Identity and access controls** to prevent adversaries from leveraging valid credentials
- **Proactive threat hunting** to identify pre-attack behaviors and block adversary movements early

CASE STUDY

CURLY SPIDER's Social Engineering Attack

In 2024, CURLY SPIDER emerged as one of the fastest and most adaptive eCrime adversaries, executing high-speed, hands-on intrusions. In this case, the adversary attempted to achieve their objectives without even 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.

This incident would have been prevented by the CrowdStrike Falcon sensor with proper prevention policies. Regardless, within minutes, CrowdStrike OverWatch threat hunters saw the suspicious activity, notified the customer, and eliminated the threat.

How CURLY SPIDER Operates

This adversary relies heavily on social engineering for initial access. In some cases, the following will occur:

- A user will receive a large volume of spam emails impersonating charities, newsletters, or financial offers
- Shortly after, a caller posing as help desk or IT support claims the spam is caused by malware or outdated spam filters
- The user is instructed to join a remote session using an RMM tool, such as Microsoft Quick Assist or TeamViewer, with the attacker guiding them through the installation if the tool is not already present; in this case, the adversary chose Quick Assist to establish control

CURLY SPIDER

CrowdStrike OverWatch in Action:
Stopping a Social Engineering Attack in Under 4 Minutes

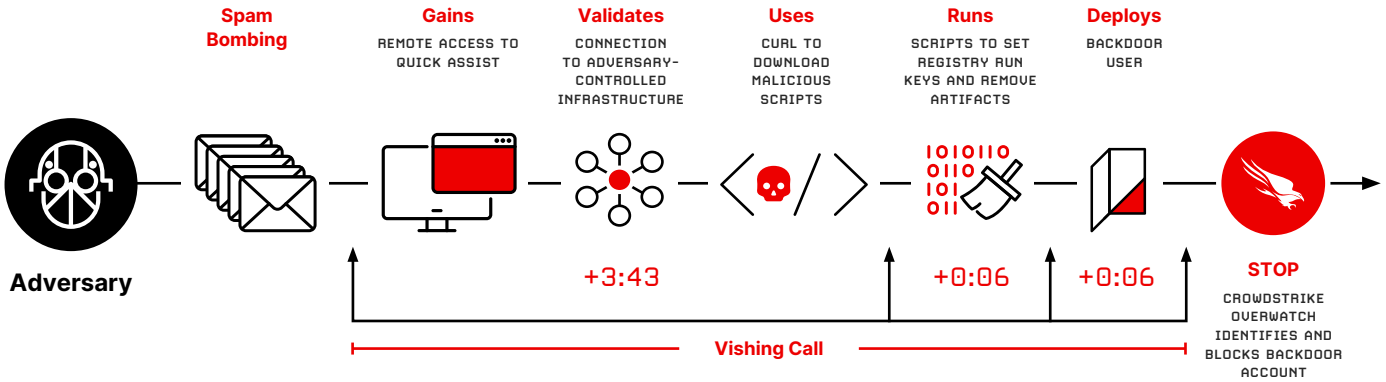


Figure 5. Timeline of CrowdStrike OverWatch moving faster than CURLY SPIDER to stop a social engineering attack in less than four minutes

Once CURLY SPIDER gains initial access, its window of opportunity is limited — access will only last as long as the victim remains 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. The bulk of the intrusion time is spent ensuring connectivity and troubleshooting any access issues to reach their cloud-hosted malicious scripts.

1. Validating Connectivity (3:43)

- Posing as IT support offering assistance, the adversary requests access to Quick Assist.
- The adversary ensures a connection to pre-configured cloud storage, where they host malicious scripts and work through any access barriers. Once access is confirmed, CULRY SPIDER downloads malicious scripts.

2. Deploying Payload (0:06)

- CURLY SPIDER executes the scripts via `curl` or PowerShell. These scripts:
  - Modify registry run keys, creating a user to ensure execution at startup
  - Remove forensic artifacts to erase traces of the intrusion

3. Establishing Persistent Access (0:06)

- The adversary creates a backdoor user, embedding persistence directly into the system.
- The final payload is executed under a legitimate binary, allowing CURLY SPIDER to blend into normal activity and evade detection.

In this example, CURLY SPIDER does not rely on traditional "breakout" techniques to move laterally. Instead, the adversary compromises the network in seconds by securing long-term access before the victim even realizes what's happening.

Impact and Connection to Ransomware

In this case, CURLY SPIDER was stopped by CrowdStrike OverWatch before they could proceed with the rest of their attack. However, CrowdStrike Intelligence has seen these tactics directly support ransomware operations, and this adversary frequently collaborates with WANDERING SPIDER, the group behind *Black Basta* ransomware. By combining high-tempo social engineering, legitimate remote tools, and cloud-hosted payloads, CURLY SPIDER exemplifies how modern adversaries bypass traditional defenses and achieve rapid operational success.

Proactive Defense Is Essential

Adversaries are refining their tactics to move faster and exploiting trusted access to bypass traditional defenses. The explosive growth in access broker activity, valid credential abuse, and interactive intrusions highlights the urgent need for organizations to adopt proactive security strategies that prevent, detect, and respond to these threats in real time.

Security teams must:

- Prioritize identity protection to prevent unauthorized access
- Harden cloud environments against credential abuse and address misconfigurations
- Accelerate response times to counter rapid breakout events
- Leverage AI-driven threat hunting to detect stealthy adversary movements

In 2025, attackers will only move faster. Will defenders keep up?

Key Adversary Themes

THE BUSINESS OF SOCIAL ENGINEERING

Since 2023, eCrime and targeted intrusion adversaries have increasingly used identity compromise and other human-centric tradecraft to gain initial access and perform lateral movement. The emergence of this tactic is partly driven by the growing efficacy and abundance of modern host-based security tools such as endpoint detection and response (EDR) solutions. These factors have driven social engineering activity in which threat actors attempt to access targeted accounts or persuade legitimate employees to provide remote access to targeted systems.

In 2024, CrowdStrike Intelligence observed a massive increase in the number of distinct campaigns using telephone-oriented social engineering techniques to gain initial access, including vishing and help desk social engineering, marking a potential shift in the eCrime ecosystem.

2024 Vishing Trends

Several eCrime adversaries incorporated vishing into their intrusions in 2024, amounting to a 40% compounded monthly growth rate in observed vishing operations for the year. The latter half of 2024 saw a significant increase in the use of this tactic (Figure 6).

WHY VISHING IS SO EFFECTIVE

Similar to other social engineering techniques, vishing is effective because it targets human weakness or error rather than a flaw in software or an operating system (OS). Malicious activity may not be detected until later in an intrusion, such as during malicious binary execution or hands-on-keyboard activity, which can delay an effective response. This gives the threat actor an advantage and puts the onus on users to recognize potentially malicious behavior.

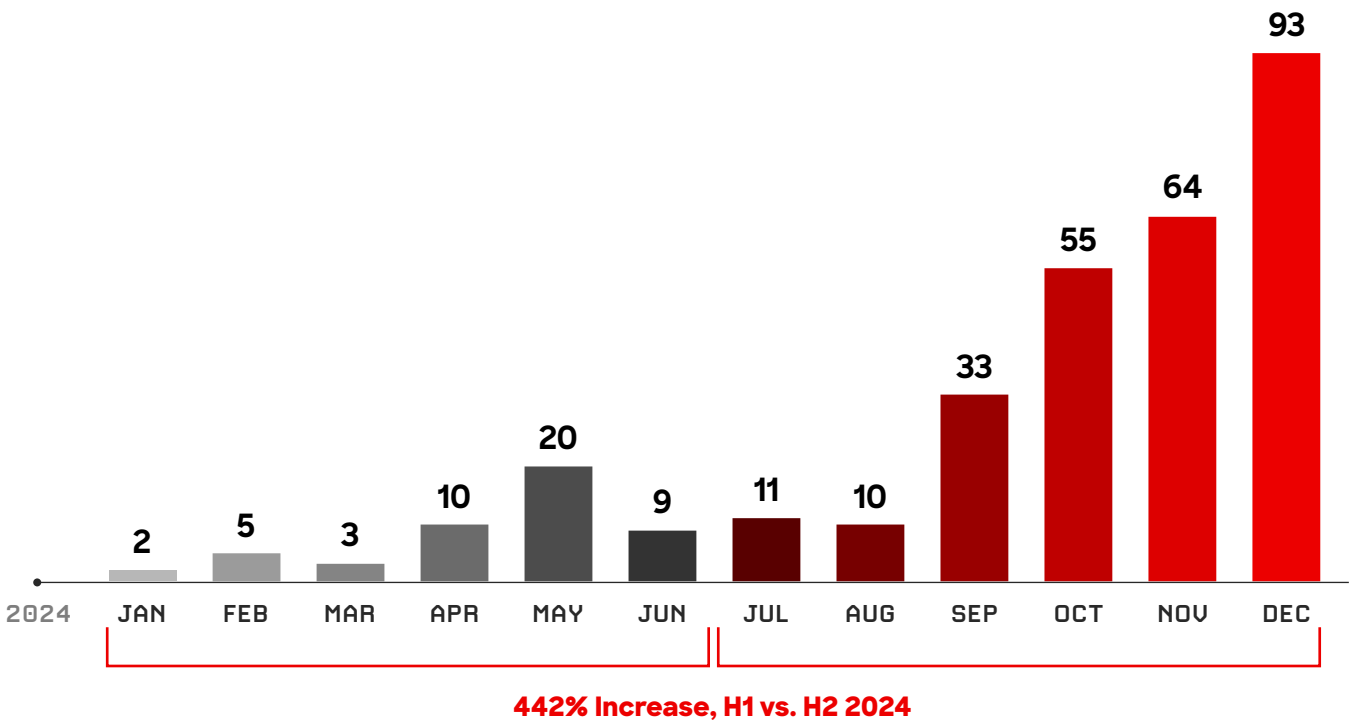


Figure 6. Vishing intrusions detected by CrowdStrike OverWatch per month, 2024

In vishing campaigns, threat actors call targeted users and attempt to persuade them to download malicious payloads, establish remote support sessions, or enter their credentials to adversary-in-the-middle (AITM) phishing pages. In most 2024 vishing campaigns, threat actors impersonated IT support staff, calling targeted users under the pretext of resolving connectivity or security issues.

Throughout 2024, CrowdStrike Intelligence tracked at least six similar but likely distinct campaigns in which threat actors posing as IT staff called their targets and attempted to persuade them into establishing remote support sessions, often using Microsoft Quick Assist. In many cases, calls were made via Microsoft Teams from external tenants.

At least four of these campaigns leveraged spam bombing — sending thousands of spam emails to targeted users' email addresses — as a pretext for the vishing call. The CrowdStrike Falcon® Complete Next-Gen MDR and CrowdStrike OverWatch teams observed a significant increase in these campaigns in the second half of 2024, detecting several relevant intrusions each day. eCrime adversary CURLY SPIDER is behind one of these campaigns, with relevant intrusions culminating in *Black Basta* ransomware deployment.

The long-standing Russia-based eCrime adversary CHATTY SPIDER continued to employ callback phishing as an initial access vector in data theft and extortion campaigns. In callback phishing, threat actors typically begin by sending a lure email to targeted users, often regarding an imminent charge or overdue payment. This prompts users to initiate a phone interaction. CHATTY SPIDER primarily targets the legal and insurance sectors and has demanded ransoms up to 8 million USD. Several eCrime actors used callback phishing to gain initial access in 2024, including one campaign that used it to install a remote support tool.

Brazil-based eCrime adversary PLUMP SPIDER exclusively targeted Brazil-based organizations throughout 2024 with attempts to conduct wire fraud. PLUMP SPIDER uses vishing calls to direct targeted users to sites hosting remote support and RMM tools such as RustDesk and Supremo. After gaining access, they compromise the victim's payment systems to perform fraudulent financial transfers. In addition to targeting unwitting users, the adversary has reportedly attempted to recruit insiders at targeted organizations.

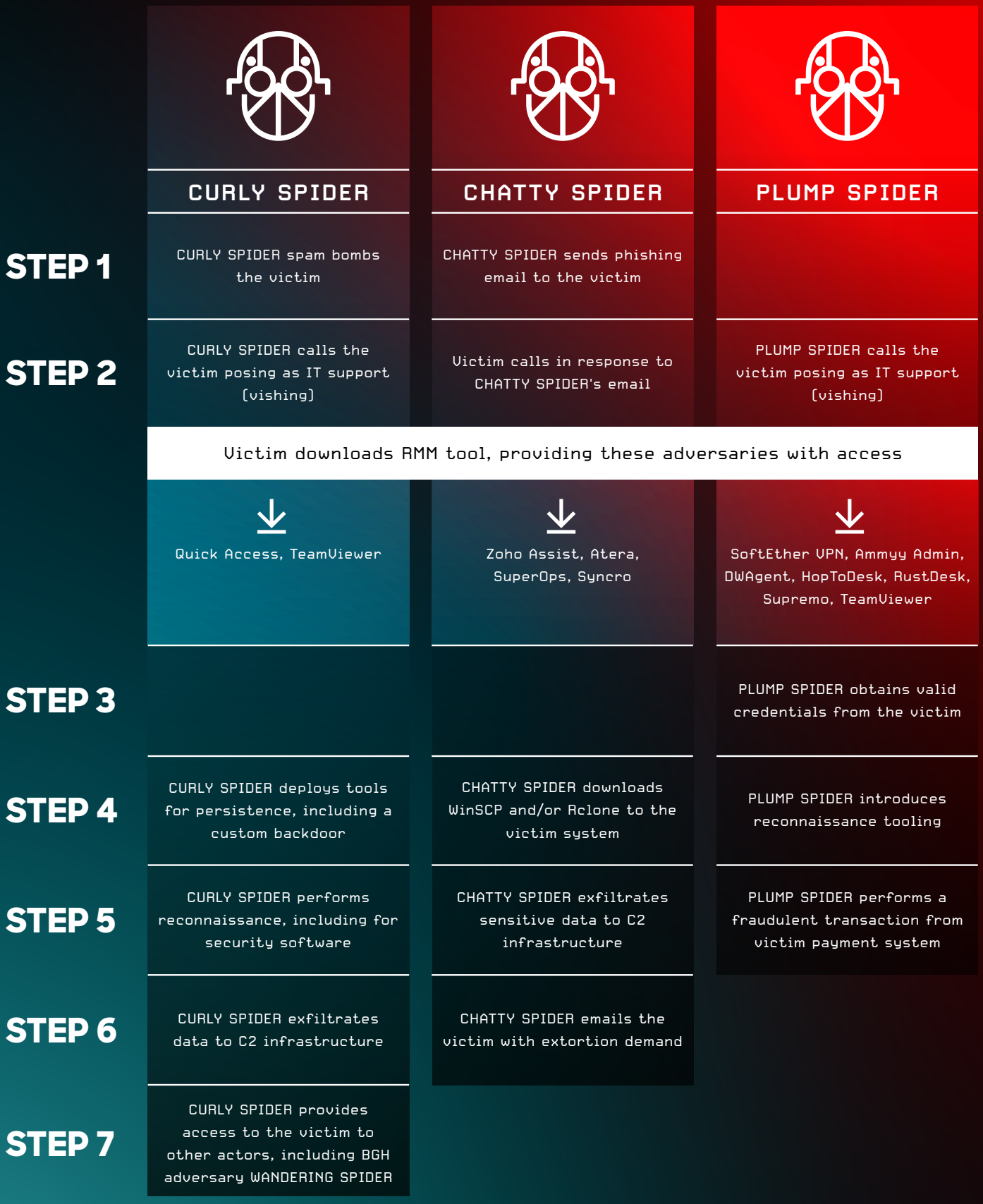


Figure 7. CURLY SPIDER, CHATTY SPIDER, and PLUMP SPIDER use vishing for initial access

Help Desk Social Engineering

In addition to vishing, multiple eCrime threat actors are increasingly adopting help desk social engineering tactics. In these campaigns, threat actors call a targeted organization's IT help desk and impersonate a legitimate employee, attempting to persuade a help desk agent to reset passwords and/or multifactor authentication (MFA) for the relevant account.

Since early 2023, SCATTERED SPIDER has used this technique to gain access to single sign-on (SSO) accounts and cloud-based application suites. Multiple eCrime actors adopted this technique in 2024. Several relevant cases targeted academic and healthcare entities; in these incidents, threat actors subsequently used the compromised identity to exfiltrate data from cloud-based software as a service (SaaS) applications or modify employee payroll data.

IT help desks often require employees seeking password and MFA resets to provide their full name, date of birth, employee ID, and manager name or answer a previously determined security question. However, eCrime actors attempting to socially engineer help desk personnel often accurately respond to these questions. Much of this information is not necessarily privileged and can be found in public resources and social media sites. Identity data that is typically confidential, such as a Social Security number, is often advertised in underground markets.

In most help desk social engineering incidents, calls were made outside the victim's local business hours. This is likely because it enables the threat actor to maintain longer access to the compromised account before the legitimate owner reports suspicious activity.

Threat actors using this technique often register their own device for MFA to enable persistent access to compromised accounts. They also often manually delete emails from compromised mailboxes related to suspicious account activity or configure mail transport rules to redirect relevant emails to a folder other than the main inbox.

Over the past year, several eCrime actors have openly recruited callers on popular eCrime forums. The advertisements are usually for English-speaking callers with knowledge of RMM tooling and experience conducting remote sessions. Some eCrime actors have also sought effective methods for spoofing phone numbers or encrypting calls to ensure caller IDs can be edited and appear more legitimate. This activity suggests phone-oriented social engineering will be a credible threat in 2025 as demand for these capabilities increases.

HOW TO MITIGATE HELP DESK SOCIAL ENGINEERING

- Require video authentication with government identification for employees who call to request self-service password resets
- Train help desk employees to exercise caution when taking password and MFA reset request phone calls made outside of business hours, particularly if an unusually high number of requests is made in a short time frame or if the caller purports to be calling on behalf of a colleague
- Use additional, non-push-based authentication factors such as FIDO2 to prevent account compromise
- Monitor for more than one user registering the same device or phone number for MFA

GENERATIVE ARTIFICIAL INTELLIGENCE AND THE ENTERPRISING ADVERSARY

GenAI has emerged as an attractive tool for adversaries with a low barrier to entry that makes it widely accessible. Recent advancements in genAI have enhanced the efficacy of certain cyber operations, particularly those using social engineering. It will almost certainly be employed in 2025 cyber operations.

Adversaries increasingly adopted genAI throughout 2024, particularly in support of social engineering efforts and high-tempo IO campaigns. Both were supported by genAI tools that can create highly convincing outputs without precise prompting, custom model training, or fine-tuning. Some threat actors are employing genAI, specifically LLMs, to support CNO efforts.

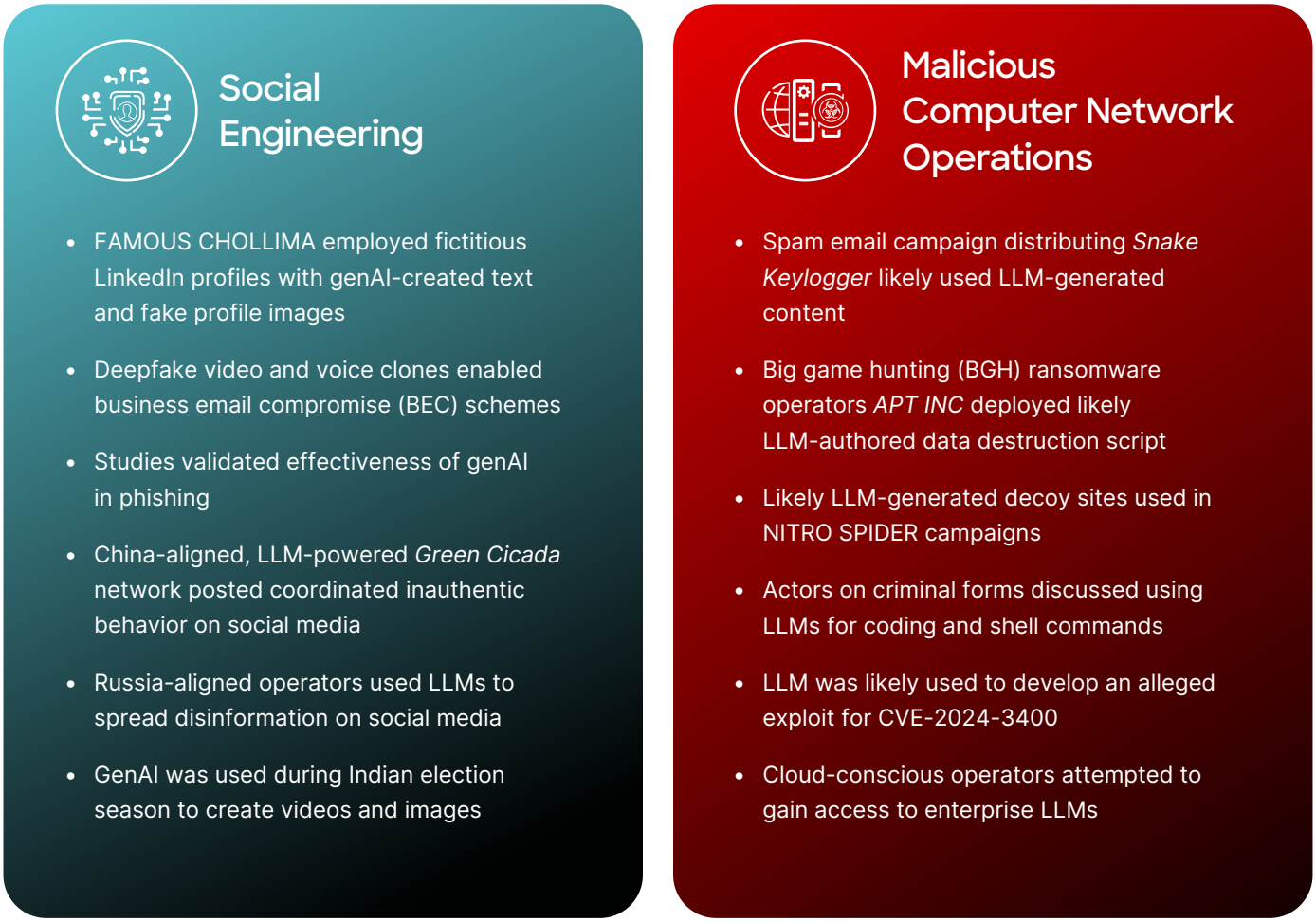


Figure 8. Adversaries leveraging LLMs for social engineering and malicious CNO

GenAI Supports Social Engineering

LLMs and genAI models that create photorealistic imagery can generate convincing content at scale with minimal expertise. These tools can support social engineering efforts or IO. Despite the relative novelty of genAI, CrowdStrike has identified several examples of adversaries using it.

Social Engineering

Operators associated with DPRK-nexus adversary FAMOUS CHOLLIMA obtain positions at companies worldwide under fake personas, occasionally using genAI tools to socially engineer recruiters during the job application process. They also create fictitious LinkedIn profiles with genAI-created text and fake profile images. During interviews, many FAMOUS CHOLLIMA candidates provide answers likely derived from external sources. LLMs likely support these interviews by rapidly generating plausible responses.

GenAI is also used for BEC and fraud. In February 2024, unidentified threat actor(s) used public footage of a target company's chief financial officer and other employees to create credible deepfake video clones and socially engineer the victim into transferring 25.6 million USD to the threat actor(s). In May 2024, industry reporting indicated threat actors had impersonated the CEO of an international professional services entity and attempted to solicit fraudulent payments. The threat actor also appeared to have used genAI to clone the CEO's voice and attempted to persuade the call recipient to transfer funds.

The relationship between genAI and social engineering is also evidenced by the evolving focus of mobile malware. Since late 2023, the *GoldPickaxe* malware has been employed to steal biometric facial data from iOS and Android devices throughout the Asia Pacific (APAC) region. The malware, which cannot bypass authentication, captures images and videos to generate deepfake videos or perform face-swap operations.

Academic research further highlights the appeal of LLMs for social engineering. LLMs can generate phishing email content or credential harvesting websites at least as well as humans. A 2024 study of phishing email click-through rates indicated LLM-generated phishing messages had a significantly higher click-through rate (54%) than likely human-written phishing messages (12%).[1] A separate 2024 study found detection rates for LLM-generated phishing pages were comparable to those for human-created phishing pages.[2]

» A 2024 STUDY OF PHISHING EMAIL CLICK-THROUGH RATES INDICATED LLM-GENERATED PHISHING MESSAGES HAD A SIGNIFICANTLY HIGHER CLICK-THROUGH RATE (54%) THAN LIKELY HUMAN-WRITTEN PHISHING MESSAGES (12%).[1]

1 https://arxiv.org/pdf/2412.00586

2 https://arxiv.org/pdf/2310.19181v2

ADVERSARY SPOTLIGHT: FAMOUS CHOLLIMA

In 2024, FAMOUS CHOLLIMA quickly entered the spotlight due to their broad-scale operations, high operational tempo, and unique malicious insider tactics. The adversary regularly conducted financially motivated cyber operations across the globe, deploying their characteristic *BeaverTail* and *InvisibleFerret* malware families.

The adversary also oversaw a larger malicious insider campaign, using a network of personas to obtain fraudulent employment as software developers at large companies across North America, Western Europe, and East Asia (Figure 9). CrowdStrike OverWatch responded to FAMOUS CHOLLIMA activity in 304 incidents throughout the year, with nearly 40% representing insider threat operations.

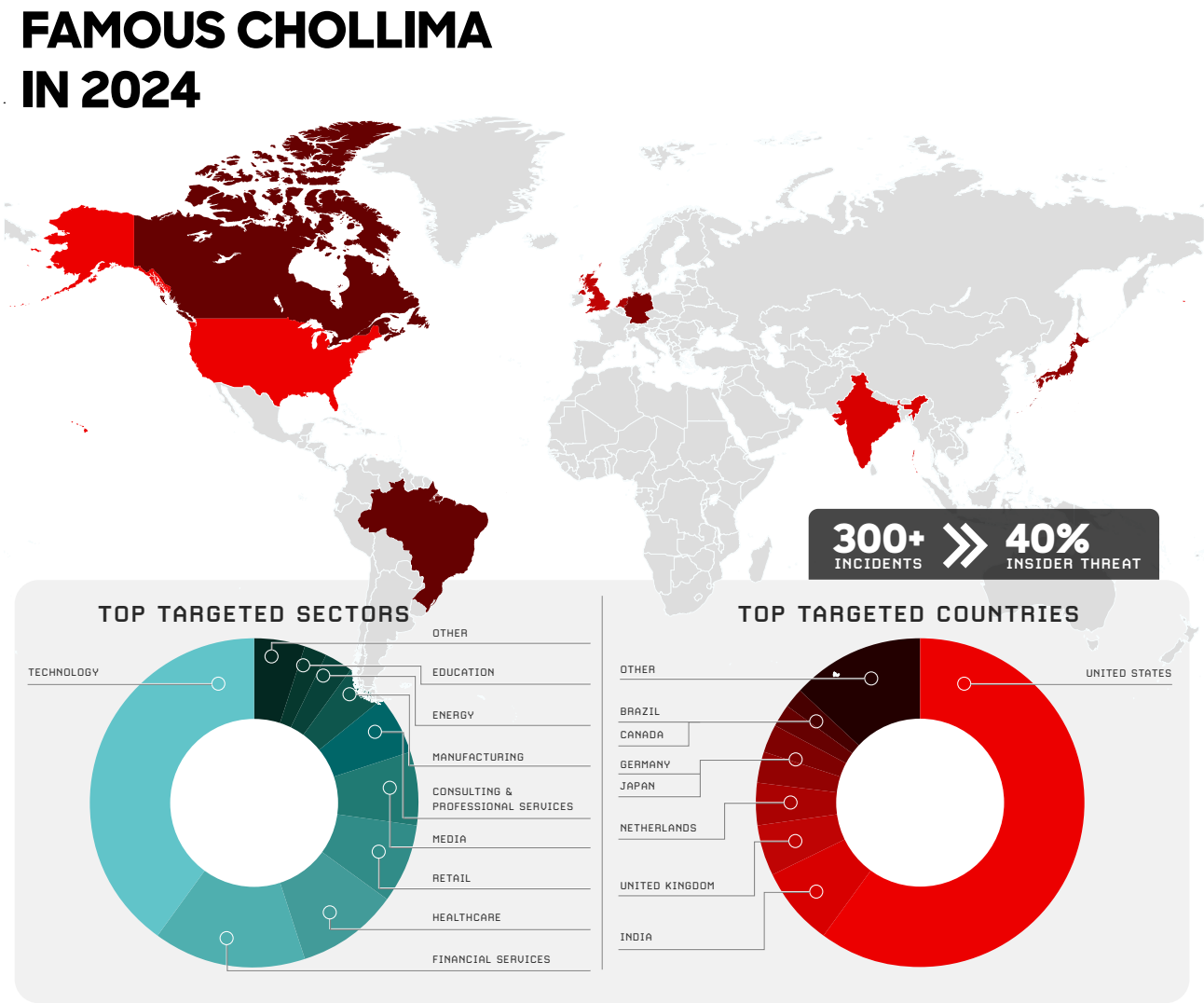


Figure 9. FAMOUS CHOLLIMA's target sectors and regions, 2024

FAMOUS CHOLLIMA's cyber operations remained remarkably consistent throughout 2024, relying on delivery of a first-stage implant via a trojanized Node.js application. This application was disguised as a coding challenge for blockchain developers and delivered to victims under the guise of an employment interview. FAMOUS CHOLLIMA deployed seven distinct malware families in 2024, evading detection by slightly refining how the files were downloaded and executed.

FAMOUS CHOLLIMA's malicious insiders appear to opportunistically pursue insider access across multiple sectors. The adversary's activity is likely driven by available employment opportunities rather than specific targeting requirements.

Operatives use stolen or fraudulent identities to obtain software development jobs and then send their company-provided laptop to a third-party facilitator running a laptop farm. CrowdStrike OverWatch identified several laptop farms in Illinois, New York, Texas, and Florida. FAMOUS CHOLLIMA installs remote management tools and several browser extensions on the laptops. While CrowdStrike Intelligence has observed code or intellectual property exfiltration in some cases, most insider threats appear motivated by the job's salary.

FAMOUS CHOLLIMA was one of the most active adversaries in 2024, significantly surpassing other state-nexus adversaries' operational tempos. Notably, activity increased in the second half of 2024. This adversary will very likely continue conducting parallel cyber and insider threat campaigns well into 2025. This assessment is based on the adversary's success, their ongoing high operational tempo, and the minimal impact of government indictments and actions against the adversary throughout 2024.

Information Operations

Adversaries can easily employ genAI tools to conduct IO campaigns and primarily use them to create tailored content at scale. Unlike other social engineering techniques, IO campaigns using AI-generated content are typically not checked for accuracy by most consumers. Adversaries may achieve their goals even if the target knows the content is fabricated.

In August 2024, industry sources reported on *Green Cicada*, an IO network likely enabled by a Chinese-language LLM system comprising more than 5,000 inauthentic accounts on the social media platform X. This network amplified politically divisive issues to exacerbate social divisions in the lead-up to the 2024 U.S. presidential election. Industry sources have linked the operation to China-based entities using LLMs.

Russia-aligned operators also used genAI to spread disinformation. In 2024, a propagandist likely used LLMs to generate tailored content and workflow automation tools that supported a vast IO campaign targeting U.S. audiences. Multiple Russia-nexus IO campaigns — including those targeting Israel, the U.S., and various European countries — employed genAI to generate text and images throughout 2024.

Threat Actors Leverage GenAI to Support CNO

Some adversaries are exploring the use of genAI to directly support CNO, likely using it to assist in writing utility scripts and developing tools or malware. Limited direct visibility into adversary use of LLMs often inhibits analysis of these campaigns. Nonetheless, many adversaries using LLMs are likely still familiarizing themselves with these tools.

In March 2024, a criminal actor distributed a spam email campaign that used a likely LLM-generated `.txt` template. The emails delivered an archive file containing the commodity malware *Snake Keylogger*. This campaign marks CrowdStrike's first confirmed instance of a criminal actor using likely LLM-generated content in a malicious spam campaign.

BGH ransomware operators *APT INC* used an uncommon, destructive PowerShell script to destroy data on a physical host. Based on the comment formatting, the similarity to results produced by other LLMs, and the lack of public sources resembling the script, it was likely generated using an LLM. Adversaries have used LLMs to generate scripts in the past; for example, SCATTERED SPIDER used a likely LLM-generated script in 2023.

eCrime actors have also employed genAI to produce content. NITRO SPIDER, who employs malvertising to deliver *Nitrogen*, used LLM-generated decoy websites in 2024. The adversary lures prospective targets by purchasing advertisements for particular search terms via Google or Bing. They filter out requests not originating from a malicious advertisement to ensure only legitimate victims receive the malware; other requests are rerouted to decoy websites created with LLM-generated text and imagery.

In another campaign, an eCrime actor used similar techniques while distributing tooling crypted with the *Davey* crypter to targets who searched for two-factor authentication (2FA) software. Clicking on the advertisement exposes the malicious download site, while direct accesses are forwarded to an LLM-generated decoy site.

Throughout 2024, several malicious actors discussed using genAI in criminal marketplaces and forums. For example, one Latin America (LATAM)-based threat actor discussed using generative pre-trained transformers (GPTs) and genAI to learn how to build malware with C and C++. As of December 2024, a Yemen-based cyber operator related to the *Dragon* and *Stormous* ransomware families maintains a GitHub repository for a command line interface tool that allegedly leverages a GPT model for various tasks, including executing shell commands.

Vulnerability Research and Exploitation

GenAI models are both a target and enabler of exploit-related activity. As with CNO, LLMs can accelerate vulnerability research and testing by potentially speeding up development timelines. However, confirmed evidence of LLM-aided vulnerability exploit development, and exploitation of LLMs in the wild, remains rare.

In 2024, Iran-nexus actors were among the most notable groups seeking genAI support in the vulnerability landscape. Iranian government initiatives aspire to leverage AI to develop assistants and enable patching systems for domestic networks. Moreover, Iran's government aims to use LLMs in vulnerability research and exploit development.

Threat actors' interest in genAI-enabled exploit development is further evidenced by observed activity in April 2024. An unattributed threat actor likely used genAI to develop an alleged exploit for a command injection vulnerability in GlobalProtect PAN-OS Gateway (CVE-2024-3400). While the exploit was ultimately ineffective, CrowdStrike Intelligence observed exploitation attempts as threat actors attempted to rapidly repurpose LLM-generated exploits in the wild.

Alternatively, threat actors and researchers are exploring potential attack vectors associated with vulnerabilities within genAI models. Techniques such as prompt injection may potentially circumvent access controls, achieve code execution, or raise the potential for unintentional disclosure of sensitive information. Further, genAI platforms with external resources can introduce vulnerabilities typically associated with many web applications, such as server-side request forgery and SQL injection.

Cloud-Conscious Threat Actors

Cloud-conscious adversaries are beginning to explore genAI and LLMs for their operations. As cloud adoption expands and genAI becomes more integrated into services such as Azure AI Foundry (formerly Azure AI Studio),[3] threat actors will likely begin exploiting genAI services for data theft, model manipulation, unauthorized access, and other malicious purposes.

CrowdStrike Intelligence expects cloud-conscious threat actors with varied skill levels will increasingly exploit technical vulnerabilities and misconfigurations in the growing genAI-driven cloud ecosystem. They will seek to abuse AI services, and services that customers integrate using AI, to acquire data of strategic interest.

CASE HIGHLIGHT: LLMJACKING

LLMJacking involves threat actors exploiting stolen cloud credentials to access AI services to fuel an expanding criminal market for unauthorized LLM queries. In Q2 2024, an unknown threat actor compromised a North American consulting victim. In this operation, the threat actor prepared for LLMJacking by listing available foundational machine learning (ML) models for a cloud-based AI service. For unavailable models, the threat actor attempted to gain access by leveraging an API that enables users to request permission for restricted machine learning models by submitting a justification.

In a separate Q4 2024 campaign, a threat actor compromised a North America-based technology company and similarly attempted to use the same API to obtain access to models hosted on the cloud platform. In both cases, the threat actors likely intended to resell ML model access to other threat actors seeking to use the models for malicious purposes.

3 https://azure.microsoft.com/en-us/blog/build-your-own-copilot-with-microsoft-azure-ai-studio/

GenAI Outlook

More adversaries will likely use genAI to augment social engineering and CNO campaigns in 2025. This assessment is made with moderate confidence based on the growing availability and capability of genAI tools and adversaries' increased experience with integrating them. CrowdStrike Intelligence assesses more technically capable threat actors will be best equipped to employ genAI tools, while less sophisticated threat actors will likely not fully exploit their capabilities.

CHINA'S CYBER ENTERPRISE

China's Maturing Cyber Capabilities

China's cyber espionage and intelligence collection capabilities reached an inflection point in 2024 relative to previous years. In addition to prolific and high-profile cyber espionage activities — which continued to increase across almost every sector that CrowdStrike Intelligence tracks — China-nexus adversaries and the larger ecosystem supporting their operations have matured in capability and capacity.

Throughout 2024, China-nexus adversaries' advancements manifested through increasingly bold targeting, stealthier tactics, and specialized operations. The underlying motivation is likely China's desire for regional influence in the nation's near abroad. This includes a desire for the eventual reunification of Taiwan, which may ultimately bring China into conflict with the United States.

In addition to facilitating intelligence collection against foreign political and military entities, these operations likely fulfill general intelligence requirements in the Chinese Communist Party (CCP)'s strategic plans. This includes the 14th Five-Year Plan, which highlights key sector and technology priorities. China-nexus adversaries also conduct intelligence collection against social and political movements perceived as domestic security threats in China. The CCP collectively refers to Falun Gong practitioners, Chinese democracy activists, Uyghur separatists, Tibetan separatists, and Taiwanese separatists as the "Five Poisons" and views these groups as a threat to its legitimacy and China's overall stability.

Figure 10. Role of cyber operations in China's grand strategy

General Secretary Xi Jinping's 2014 call for China to become a cyber power (网络强国) and the CCP's grand strategy of national rejuvenation (伟大复兴) have accelerated the sophistication of China's cyber capabilities throughout the first quarter of the 21st century. The CCP's decades of cyber program investments include:

- Expanding CCP oversight of information networks in China through a broad cybersecurity legal framework
- CCP investment in university systems that produce a highly trained and readily available cyber workforce
- Private sector contracting pipelines that provide skilled support and infrastructure to the People's Liberation Army (PLA), Ministry of Public Security (MPS), and Ministry of State Security (MSS) cyber units
- Vulnerability discovery, bug hunt, and domestic capture-the-flag competitions that foster Chinese cyber talent and feed CCP-controlled exploit development programs
- Industry networking through which MSS and PLA cyber operators increasingly share unique closed-access tooling and tradecraft

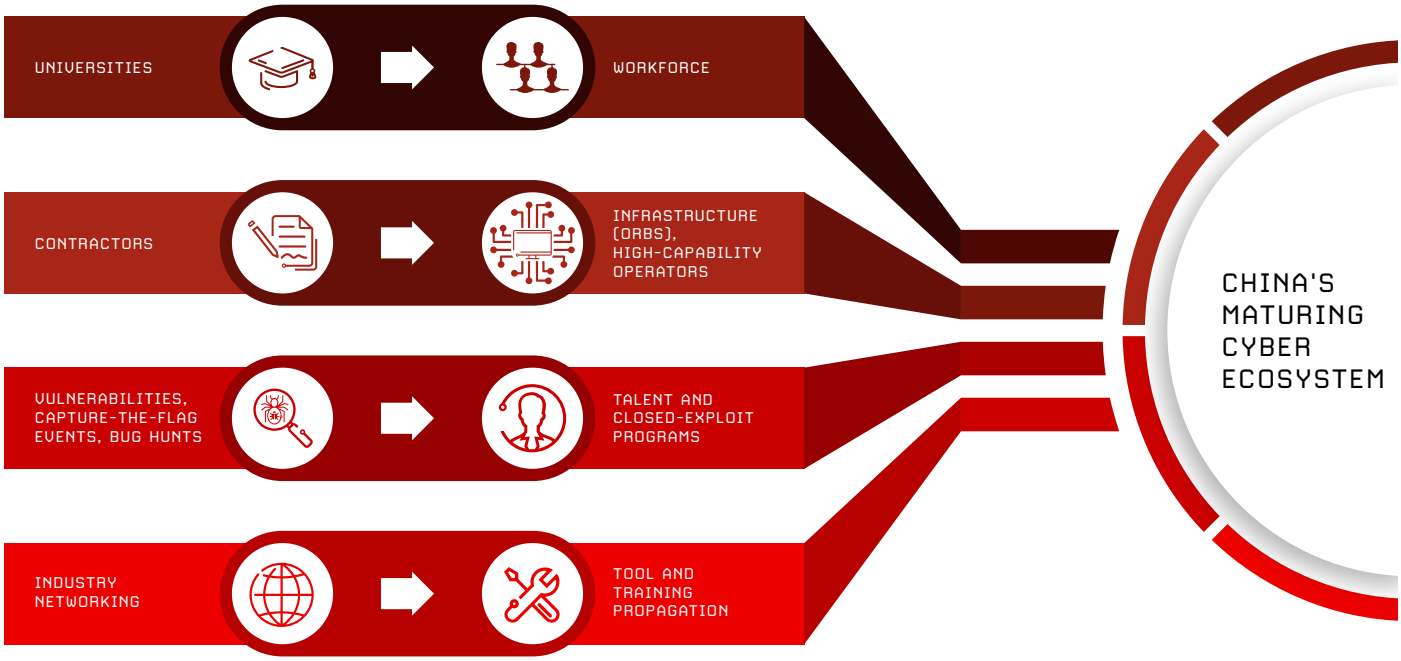


Figure 11. China's maturing cyber ecosystem

Highly likely as a result of these investments, China-nexus targeted intrusion operations are marked by increased OPSEC and specialization. Adversaries are pre-positioning themselves into critical networks and are supported by industry networking and larger ecosystems, which include shared tooling and training pipelines supplying them with sophisticated malware and tradecraft.

China-Nexus Adversaries Dominate the Global Threat Landscape

China-nexus intrusions increased 150% across all sectors on average compared to 2023 and represent the most active targeted intrusion threats CrowdStrike Intelligence tracks. Throughout 2024, China-nexus adversaries continued to operate in every sector and region across the globe, maintaining the scope of these operations while increasing their scale.

These increases were most significant in the financial services, media, manufacturing, and industrials and engineering sectors, which all experienced 200-300% increases in observed China-nexus intrusions compared to previous years. Even among the top three sectors China-nexus adversaries most commonly target — government, technology, and telecommunications — China-nexus activity increased 50% in 2024 compared to 2023.

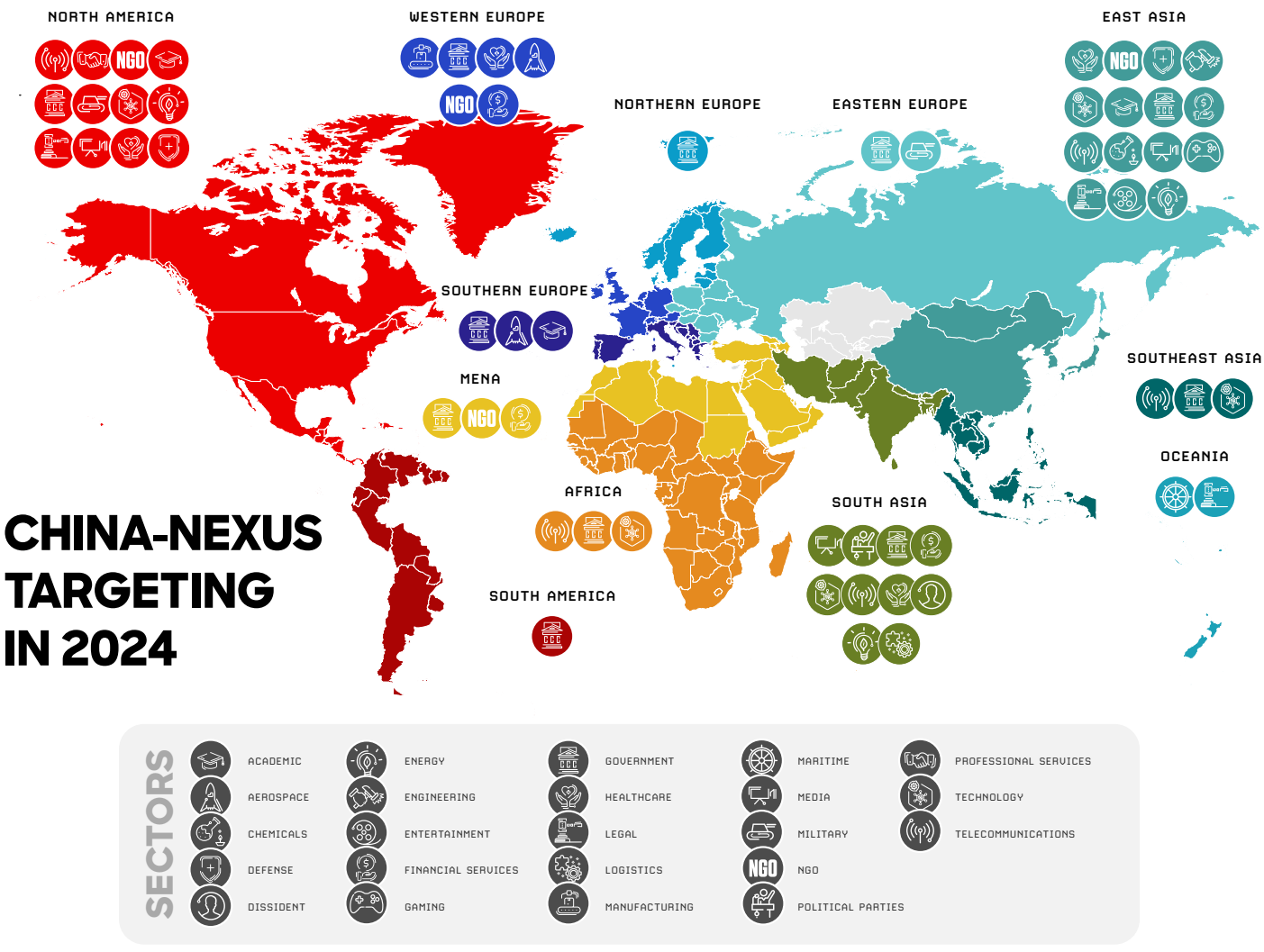


Figure 12. China-nexus targeting in 2024

Specialized China-Nexus Adversaries

CrowdStrike Intelligence identified seven new targeted intrusion adversaries originating from China in 2024, five of which 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 OPSEC posture. The emergence of adversaries with unique tactics, tradecraft, and target scopes represents an ongoing shift in China-nexus intrusions from so-called smash-and-grab operations to increasingly focused and mission-specific intrusions.

LIMINAL PANDA

Demonstrates extensive knowledge of telecommunications networks and uses compromised telecom infrastructure to move across regions

LOCKSMITH PANDA

Has targeted technology, gaming, energy, and telecommunications entities in Taiwan and Indonesia as well as Hong Kong democracy activists in operations likely intended to facilitate intelligence collection

OPERATOR PANDA

Has targeted telecom and professional services entities and relies heavily on exploiting internet-facing appliances (such as Cisco switches) for initial access

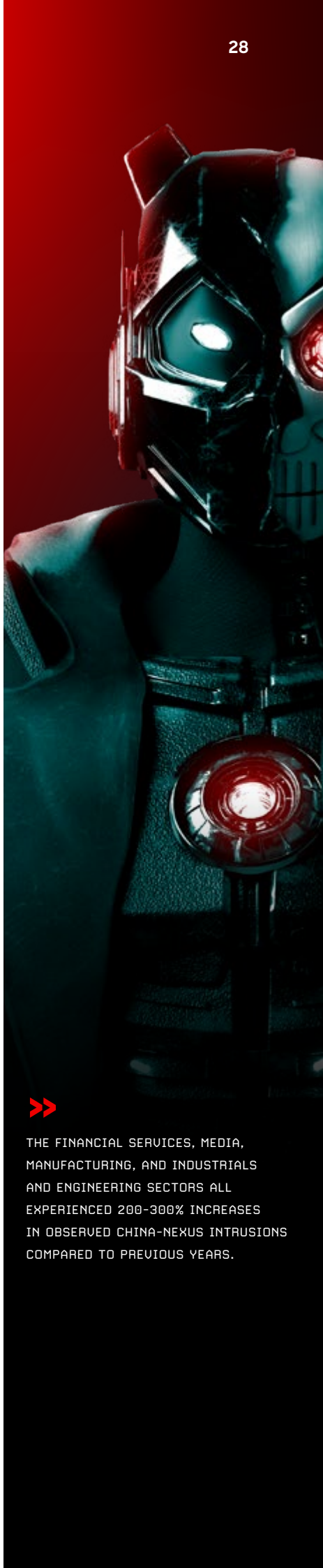
VAULT PANDA

Exploits web-facing applications to achieve initial access to victim networks and uses a combination of unique, shared, and publicly available tools in their intrusions; targets financial services, gambling, technology, academic, defense, and government entities likely to facilitate intelligence collection operations

ENVOY PANDA

Targets Africa- and Middle East-based government entities — particularly in the diplomatic space — and increasingly uses anonymization attempts in the operations

Figure 13. Newly named specialized China-nexus adversaries



» THE FINANCIAL SERVICES, MEDIA, MANUFACTURING, AND INDUSTRIALS AND ENGINEERING SECTORS ALL EXPERIENCED 200-300% INCREASES IN OBSERVED CHINA-NEXUS INTRUSIONS COMPARED TO PREVIOUS YEARS.

Adversaries Respond to Tracking and Disruption

Throughout 2024, China-nexus adversaries increasingly responded to ongoing government, law enforcement, and security researcher tracking and disruption efforts by redoubling their attempts to obfuscate operations. Multiple adversaries employed ORB networks consisting of hundreds or thousands of compromised devices to proxy and route their traffic during intrusion operations in an attempt to maintain anonymity. Despite law enforcement attempts to disrupt the ORB networks, China-nexus adversaries continue to use these resources as a key part of their operations. They also continue to share tools; for example, at least five distinct China-nexus adversaries are now using the once-unique malware *KEYPLUG*.

CLOUD-CONSCIOUS THREAT ACTORS CONTINUE TO INNOVATE

In 2024, new and unattributed cloud intrusions increased 26% compared to 2023, indicating more threat actors seek to exploit cloud services. CrowdStrike observed more intrusions in which attackers gained initial access via valid accounts, leveraged cloud environment management tools for lateral movement, and abused cloud provider command line tools. Other cloud-conscious tactics — such as enumerating cloud infrastructure and identities and maintaining persistence via alternate authentication mechanisms — were consistent throughout 2024.

New Cloud-Conscious Threat Actors Emerge in 2024

In 2023, prolific eCrime adversary SCATTERED SPIDER accounted for 30% of all cloud-based intrusions. This number fell to 13% in 2024, partly because numerous nation-state and opportunistic threat actors are increasingly targeting the cloud control plane. Many of these threat actors have adopted and employed techniques similar to those previously used by SCATTERED SPIDER, including moving laterally to cloud-hosted virtual machines (VMs) via management tools. The tactics observed in these intrusions varied significantly; some threat actors opportunistically queried the cloud control plane after host-based exploitation, and others specifically targeted cloud environments via access keys with little or no host-based interaction.

Cloud-Conscious China-Nexus Actors

China-nexus actors developed cloud-conscious techniques throughout 2024 and are increasingly targeting and abusing cloud environments for data collection. The increase in unattributed cloud intrusions corresponds with an incremental increase in suspected China-nexus incidents overall. Suspected China-nexus cloud intrusions increased 6% in 2024 across multiple cloud services, including Alibaba and Azure.

Cloud-Conscious DPRK-Nexus Actors

DPRK-nexus adversary LABYRINTH CHOLLIMA consistently targeted cloud environments, compromising developer workstations via backdoored GitHub projects before pivoting to the cloud by using cached credentials. FAMOUS CHOLLIMA also emerged as a cloud-conscious adversary in 2024, frequently gaining access to cloud environments as an insider threat and then establishing persistence via a backdoor administrator user.

Access to Valid Accounts Facilitates Initial Access Techniques

Abusing valid accounts has become the primary initial access vector to the cloud, accounting for 35% of cloud incidents in the first half of 2024. Attackers are increasingly using stealth-oriented tactics and attempting to access credentials to target valid accounts. They do not change the credentials, which would notify the user of illicit access. Emerging threat actors are likely to continue exploring similar methods to access valid cloud accounts, as this allows for more reliable access to cloud environments with a lower detection risk.

In 2023, threat actors commonly obtained cloud credentials via unsecured sources such as the cloud VM Instance Metadata Service, IT development services, or secured password storage solutions. Though this trend continued into 2024, threat actors also began to explore other mechanisms to access valid accounts via credentials and trust relationships.

One likely initial access mechanism is leveraging information stealers; during 2024, threat actors updated *Stealc* and *Vidar* to target cloud accounts. These stealers provide attackers with instant access to cloud credentials and email lists that can be leveraged for password spraying and phishing.

Another method for credential collection involves abusing trust relationships to gain access to cloud accounts. More adversaries used connections between business partners and their cloud tenants to access environments without needing to obtain credentials in the victim tenant. FAMOUS CHOLLIMA capitalized on another form of trusted relationships as an insider threat to deploy a backdoor in a cloud tenant after one of their operators was hired at the target organization. This adversary is a particularly concerning insider threat, as their operators are often hired in developer positions and given access to cloud accounts.

ABUSING VALID ACCOUNTS HAS BECOME THE PRIMARY INITIAL ACCESS VECTOR TO THE CLOUD, ACCOUNTING FOR 35% OF CLOUD INCIDENTS IN THE FIRST HALF OF 2024.

Password spraying techniques evolved significantly in 2024. For example, the China-nexus ORB07 network targeted Entra ID accounts, leveraging a bug in the Resource Owner Password Credentials authentication flow to validate credentials without logging a successful sign-in event. The threat actor then performed automated exfiltration of all SharePoint documents (Figure 14).

Figure 14. ORB07 breakout time

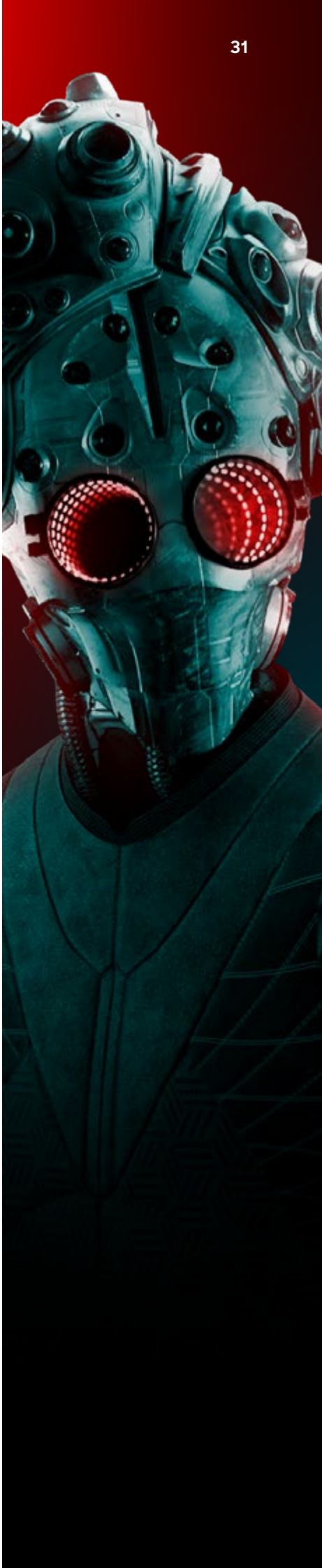
SCATERED SPIDER's diminished operational tempo in 2024 likely accounts for the reduced number of phishing-related cloud intrusions throughout the year. However, some threat actors are using AITM-based phishing, which proxies the phished user's authentication requests to the cloud authentication service being targeted. This allows the threat actor to prompt the user for an MFA token as well, circumventing one of the primary cloud account security controls.

Defense Evasion Trends

Similar to other security domains, cloud-conscious threat actors are consistently attempting to evade defender detections and security controls. Indicator removal continues to be the most common defense evasion tactic. This tactic is primarily driven by SCATTERED SPIDER and other adversaries hampering email-based detection of malicious activity, a method used in approximately 75% of cases in which indicators were removed in the first half of 2024 and in 78% of these cases in the second half of 2023.

Threat actors are also consistently attempting to evade policy-based security controls implemented by defenders. This is primarily done by implementing alternate MFA methods on compromised identities and bypassing cloud firewall segmentation.

In addition to these ongoing tactics, 2024 saw the emergence and continued development of more stealthy initial access and credential collection techniques, which enable further defense evasion in cloud intrusions.



COMMON ATTACK PATHS AND TACTICS IN CLOUD INTRUSIONS

Figure 15 shows the attack paths and tactics that most threat actors employ during a cloud intrusion. Though threat actors may not use all of the displayed techniques in a given intrusion, multiple threat actors with varying motivations have used each technique across various cloud attacks.

Although threat actors have numerous methods to gain initial access, this illustrates the value of valid accounts in a successful cloud intrusion. These allow the threat actor to access the cloud control plane and use several other techniques for persistence, privilege escalation, defense evasion, discovery, collection, and impact.

Once the threat actor has access to a valid account, they often use it to collect more credentials from secured and unsecured sources so that they can access more accounts and further their activity. A valid account also allows them to access and execute commands on cloud-hosted VM infrastructure using tools such as a cloud VM management service, thus enabling them to collect files or deploy malware or ransomware.

Each adversary's path depends on their goals and the hosting location of their target data. eCrime actors abuse cloud services to efficiently deploy ransomware and increase the deployment's impact. Cloud-conscious state-nexus actors employ stealthier cloud tactics to gain long-term access to data with a lower risk of detection and meet their collection requirements.

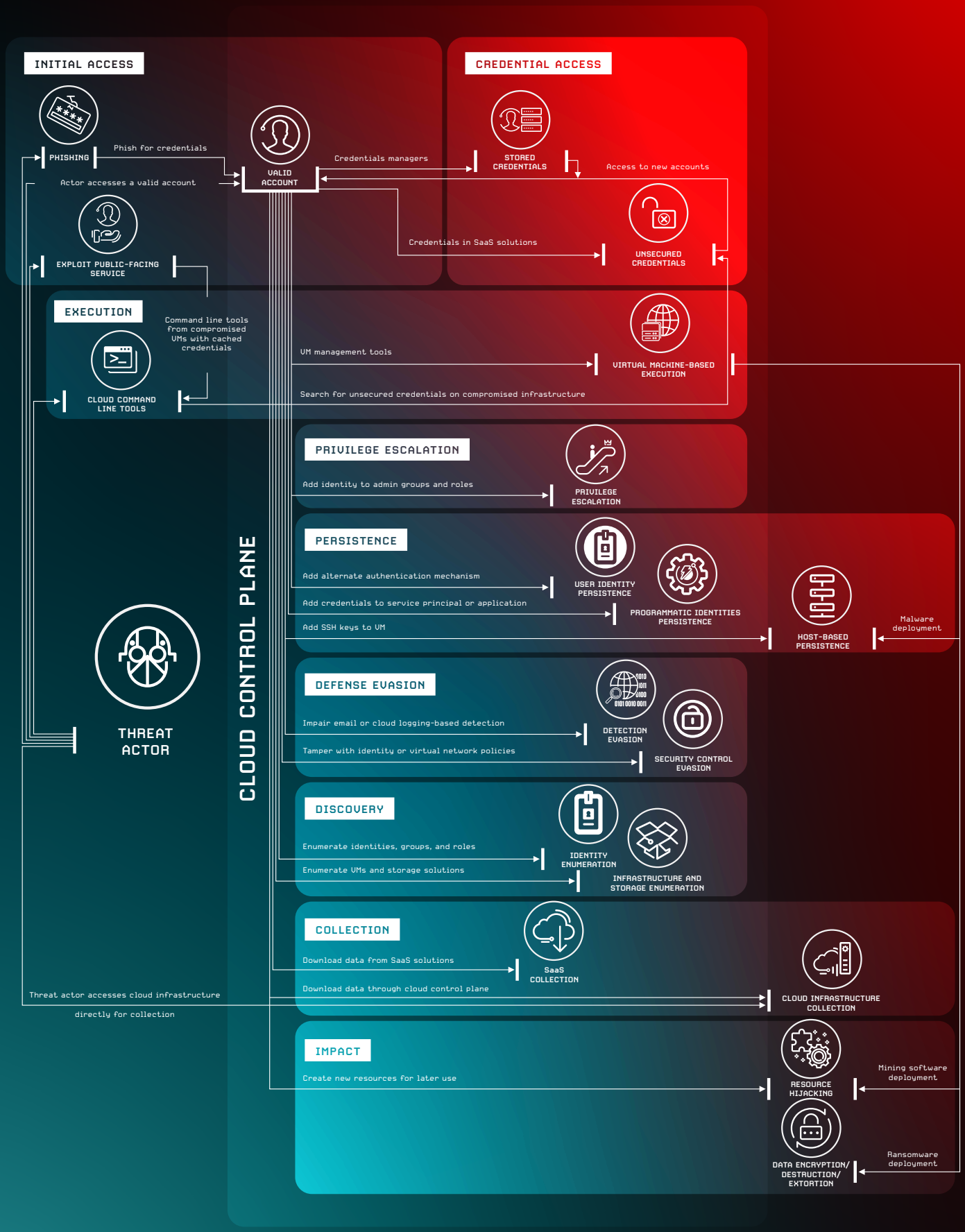


Figure 15. Common cloud intrusion attack paths and tactics

ENTERPRISING VULNERABILITY EXPLOITATION

In 2024, threat actors continued to target devices in the network periphery, where traditional EDR visibility is often limited. Exploiting unmanaged internet-exposed hosts, particularly network appliances, remained a popular initial access vector throughout 2024. Network appliances are attractive targets for many threat actors due to their many unresolved security shortcomings and often deliberate exposure. Many exploits observed in 2024 demonstrate that threat actors are leveraging previously established attack vectors and components to repeatedly exploit the same products.

Attackers almost certainly prefer to target vulnerabilities that directly allow for unauthenticated remote code execution (RCE) and seek to improve their chances for success with creative and resourceful approaches. In 2024, attackers increasingly achieved RCE using two layered approaches:

- **Chaining exploits:** Combining two or more exploits to compose an attack sequence, which increases their capabilities and impact on the target systems
- **Abusing legitimate features:** While exploits often enable initial access, attackers sometimes rely on product features, such as integrated command shells, to enable RCE

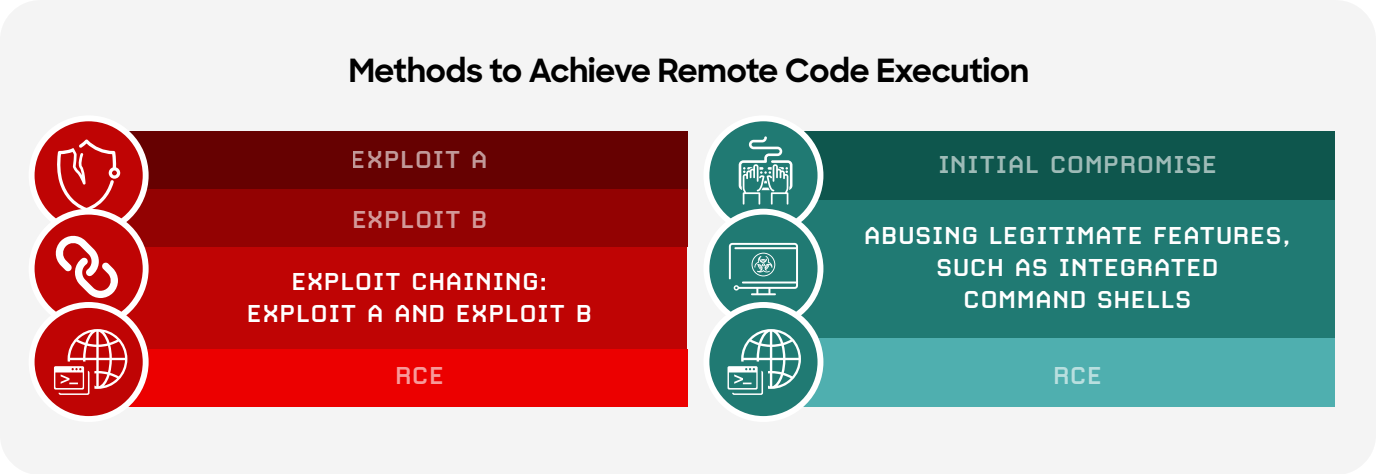


Figure 16. Layered approach to achieving RCE

Exploit Chaining

In November 2024, two notable incidents exemplified the effectiveness of exploit chains. Multiple unattributed threat actors chained a bypass vulnerability (CVE-2024-0012) and privilege escalation vulnerability (CVE-2024-9474) in the Management Web Interface of Palo Alto Networks PAN-OS software. The same month, CrowdStrike Services investigated a separate campaign in which China-nexus adversary OPERATOR PANDA likely chained two Cisco IOS vulnerabilities — a privilege escalation vulnerability (CVE-2023-20198) and a command injection vulnerability (CVE-2023-20273) — to target U.S. telecom and professional services entities.

These examples also highlight another theme observed throughout 2024: Threat actors are leveraging vulnerabilities within the network appliance's proprietary OS. Vulnerabilities in these OSs are appealing targets because they potentially allow attackers to leverage one vulnerability to target multiple products running the same OS. These proprietary OSs are often reachable via internet-exposed management interfaces and provide an easily identifiable attack vector, making them increasingly attractive targets.

Chaining two or more vulnerabilities offers attackers additional advantages. First, it allows attackers to achieve their primary objective, unauthenticated RCE, by combining multiple exploits into one seamless attack. These vulnerabilities can often be packaged into a single request or exploit payload with minimal complexity.

Second, exploit chaining undermines the severity score-based patching process that many enterprises follow. While the pre-authentication vulnerabilities receive out-of-band patches and are typically prioritized for deployment, associated post-authentication exploits receive less attention and may be ignored, potentially allowing the exploit to be chained with a different vulnerability at a later date to again achieve RCE. Over time, this approach potentially increases the efficiency of RCE exploit chain development. Unless the vendor addresses the root cause of multiple vulnerabilities, threat actors can repurpose similar techniques and quickly develop alternatives that bypass initial mitigations.

Chaining exploits can complicate efforts to efficiently remediate vulnerabilities. Understanding the combined effects of exploit chaining often requires more analysis in addition to patching vulnerabilities ahead of traditional timelines, potentially resulting in patching fatigue. Security teams typically prioritize patching internet-facing services before other internal processes. However, depending on the specific exploit chain, certain internal-facing vulnerabilities (such as post-authentication flaws) may need to be prioritized, which may strain security teams.

Abusing Legitimate Features Enables Effective Exploitation

Throughout 2024, threat actors combined vulnerability exploitation with legitimate feature abuse to achieve unauthenticated RCE. Microsoft SQL Server's built-in `xp_cmdshell` was abused in various products to achieve RCE; these included CVE-2023-48788 and CVE-2023-27532. Abusing the legitimate `xp_cmdshell` feature, which is disabled by default because of its known security shortcomings, likely indicates threat actors are attempting to employ living-off-the-land techniques.

Continuing the Discovery, Rediscovery, and Circumvention Trend

Threat actors continued to focus on previously established attack vectors and targeted similar components to achieve exploitation in 2024, continuing a trend first observed in the CrowdStrike 2023 Global Threat Report. In several 2024 incidents, threat actors leveraged their expertise in particular products to exploit those devices via one or more zero-day vulnerabilities.

For example, in September 2024, an unknown threat actor exploited and chained a zero-day file disclosure vulnerability (CVE-2024-21287) to obtain plaintext credentials. This allowed them to target a deserialization vulnerability (CVE-2024-20953) to compromise and execute code. Though CVE-2024-20953 had been disclosed prior to this incident, neither an exploit nor substantive technical details were publicly available. Despite this, an unknown threat actor successfully reproduced a functional n-day exploit for CVE-2024-20953 and chained it with a zero-day vulnerability (CVE-2024-21287). This incident indicates the threat actor had specialized product knowledge, which allowed them to identify a new vulnerability and ultimately compromise these devices and conduct follow-on malicious activity.

Another example of threat actors using previously established attack vectors involves the Windows local privilege escalation vulnerabilities in the `mskssrv` driver. During the Pwn2Own Vancouver event in March 2023, the offensive security company Synacktiv exploited a logical vulnerability in the `mskssrv` driver (CVE-2023-29360) to escalate privileges to SYSTEM. Since then, this previously overlooked attack surface has drawn the attention of security researchers and threat actors, resulting in at least 16 vulnerability disclosures since August 2023.

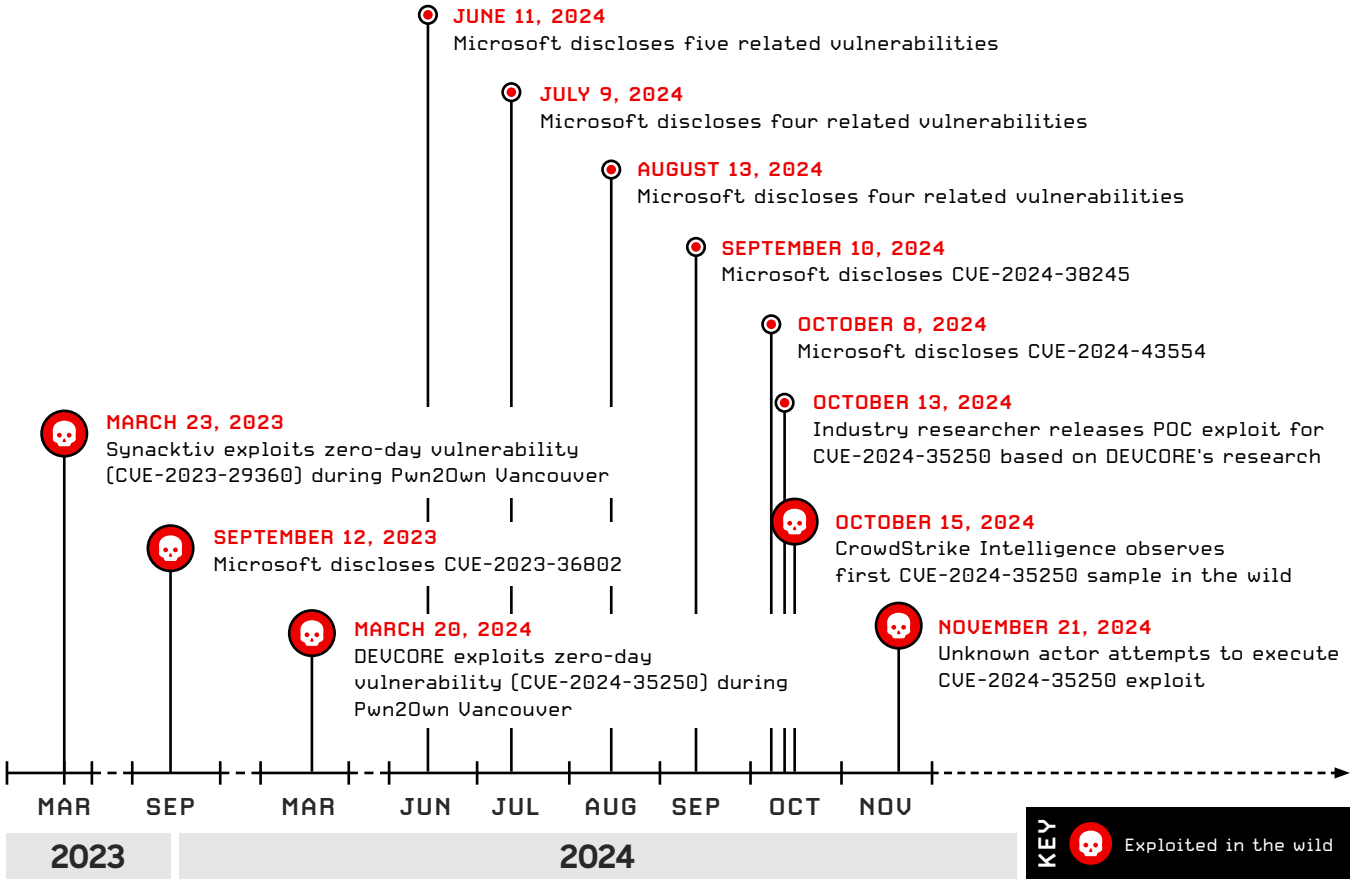


Figure 17. `mskssrv` vulnerabilities discovery timeline

Disclosing a vulnerability, particularly one acknowledged as exploited in the wild, highlights potentially viable mechanisms for future exploitation. For example, in September 2024, CrowdStrike Intelligence observed multiple `POST` requests consistent with exploiting a direct request vulnerability in Apache OFBiz (CVE-2024-45195). These `POST` requests mirrored CVE-2024-45195 exploitation guidance that a well-known industry source had published two weeks earlier. CVE-2024-45195 results from the option to desynchronize the `requestUri` and `overrideViewUri` variables in the `RequestHandler` component of the OFBiz Java application logic.

CVE-2024-45195 is similar to earlier vulnerabilities (CVE-2024-32113, CVE-2024-36104, and CVE-2024-38856) that also exploited desynchronization capabilities to allow unauthorized users to bypass authentication mechanisms. Though the vendor has provided multiple patches and several industry sources have publicly discussed these vulnerabilities, the core flaw persists and allows attackers to manipulate the controller-view state.

Separately, in January 2024, CrowdStrike Intelligence assessed threat actors had almost certainly leveraged CVE-2023-29324 in recent spear-phishing operations. CVE-2023-29324 bypasses Microsoft's mitigations for a previously disclosed Microsoft Outlook vulnerability (CVE-2023-23397), which FANCY BEAR has very likely exploited since at least March 2022 to target organizations in multiple regions and sectors. The same researcher that discovered the initial bypass (CVE-2023-29324) later found another bypass (CVE-2023-35384).

An attacker can trigger both bypasses by inserting a Universal Naming Convention path into either a Server Message Block (TCP 445) or WebDAV share on an attacker-controlled server into the MAPI property named `PidLidReminderFileParameter` (Figure 18).

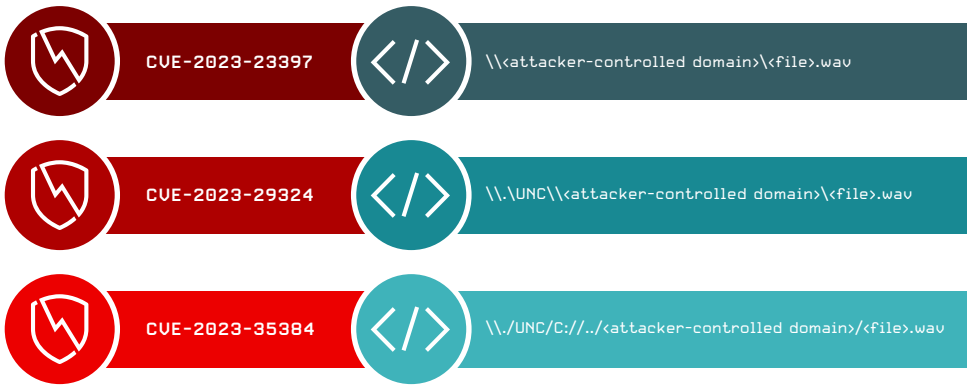


Figure 18. `PidLidReminderFileParameter` examples showing CVE-2023-23397, CVE-2023-29324, and CVE-2023-35384 exploitation

Whether threat actors have used either bypass in 2024 is unknown. However, these vulnerabilities underscore that circumventing mitigations from earlier patches to target the same vulnerable components is often trivial.

These trends highlight threat actors' evolving tactics and the challenges involved in effectively addressing vulnerabilities. Much of the exploitation activity discussed in this report occurred after the vulnerabilities were publicly disclosed and patches became available.

REDUCING THE RISK OF VULNERABILITY EXPLOITATION

Diligently applying vendor patches and other applicable mitigations/workarounds against known vulnerabilities will reduce the risk of exploitation. CrowdStrike Falcon® Exposure Management can help customers gain complete attack surface visibility and prioritize vulnerability management to reduce intrusion risk and patching fatigue.

To prevent zero-day vulnerability exploitation, security teams can implement a defense-in-depth approach to detect and remediate malicious activity before an attacker can reach their objectives. For example, applying network-level access controls to limit server exposure to trusted remote hosts can help reduce potential threats, and periodically ensuring applicable logs are correctly collected and stored for later analysis can help facilitate incident response.

Other best practices — such as server/application isolation and sandboxing, network segmentation, and adherence to least-privilege principles — can help prevent or limit the impact of malicious activity as well as protect against zero-day and n-day exploitation. Using extended detection and response (XDR) technology, such as CrowdStrike Falcon® Insight XDR, as an additional layer of detection and protection on servers hosting public-facing applications can also reduce response times.[4]

Network Perimeter Device Targeting

In 2024, threat actors continued to target devices on the network periphery, frequently leveraging industry vulnerability research — including disclosures, technical blogs, and POC exploits — to support their malicious activities. This focus on perimeter devices, both opportunistic and targeted, highlighted their appeal to adversaries and underscored the urgent need for enhanced defender visibility and protection.

The breadth and scope of compromised Palo Alto Networks perimeter devices exemplify threat actors' persistence, objectives, and imagination in perimeter device exploitation.

Since November 14, 2024, or earlier, at least one unidentified threat actor has chained an authentication bypass vulnerability (CVE-2024-0012) with a privilege escalation vulnerability (CVE-2024-9474) in the Management Web Interface of Palo Alto Networks' PAN-OS software. The vulnerabilities' public disclosure and subsequent industry reporting almost certainly prompted additional threat actors to adopt the CVE-2024-0012 and CVE-2024-9474 exploit chain.

4 https://www.crowdstrike.com/platform/endpoint-security/

On October 9, 2024, Palo Alto Networks disclosed five vulnerabilities (CVE-2024-9463, CVE-2024-9464, CVE-2024-9465, CVE-2024-9466, and CVE-2024-9467) affecting Expedition versions prior to 1.296. Expedition, which runs under the Linux OS, hosts and primarily facilitates a customer's transition from a supported vendor (Check Point, Cisco, and Juniper) to Palo Alto Networks firewalls. The vendor's disclosure statement acknowledged an attacker could exploit these vulnerabilities to read Expedition database contents and/or write arbitrary files to temporary storage locations.

On the same day, the industry source that discovered CVE-2024-9464, CVE-2024-9465, and CVE-2024-9466 released a technical blog providing exploitation guidance for all three vulnerabilities as well as CVE-2024-5910, which was previously disclosed by Palo Alto Networks in July 2024.

Within 24 hours of disclosure, CrowdStrike Intelligence captured HTTP requests consistent with CVE-2024-5910, CVE-2024-9463, and CVE-2024-9465 exploitation. Threat actors' initial post-exploitation activities — including cryptomining, malware deployment, and basic reconnaissance — were common for opportunistic exploitation activity. However, on October 18, 2024, CrowdStrike Intelligence observed CVE-2024-5910 exploitation that likely originated from two IP addresses connected to a China-nexus ORB network (Figure 19).

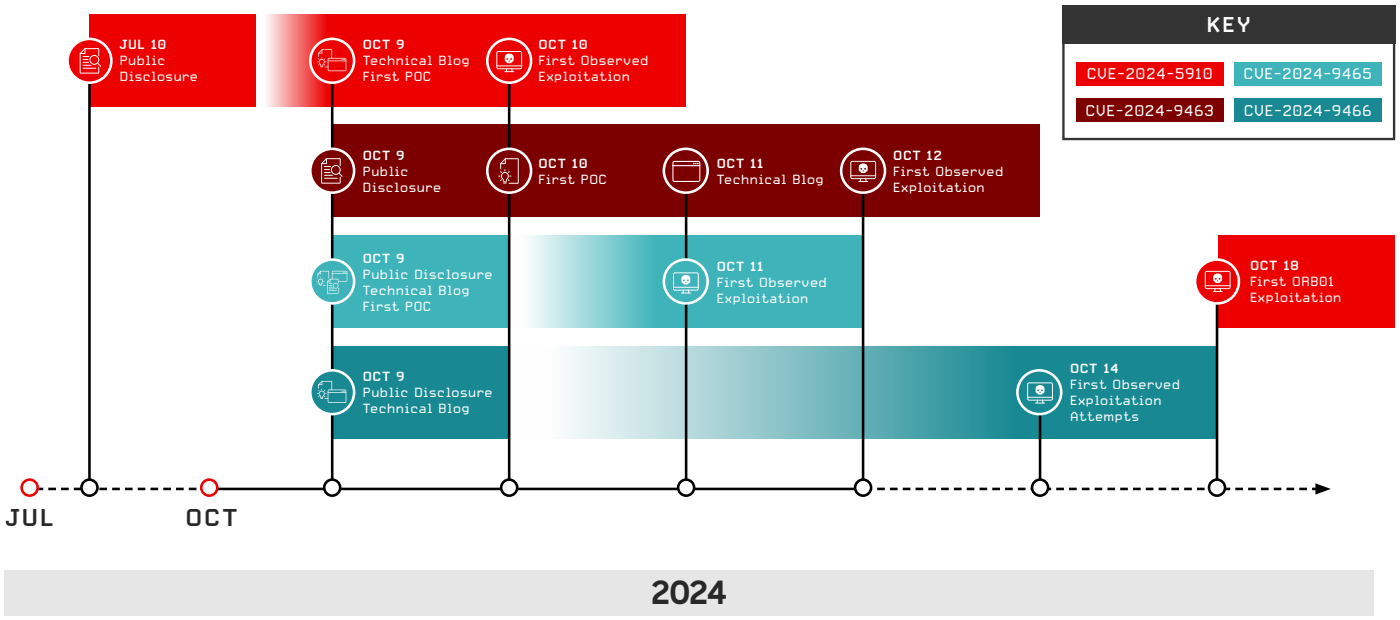


Figure 19. 2024 Palo Alto CVE exploitation timeline

Each of the Palo Alto Networks vulnerabilities described in this section provides the necessary information and/or privileges to facilitate malicious activity on victim networks. In particular, threat actors almost certainly leveraged these vulnerabilities with the intent to eventually compromise Palo Alto Networks firewalls, which are attractive targets because they are often placed in front of the demilitarized zone (DMZ) or local area networks (LANs). Compromising such devices can allow attackers to achieve the following objectives:

- Easily conduct lateral movement across the victim's network
- Monitor, divert, or detect network traffic
- Accept or drop specific network traffic

SAAS EXPLOITATION LIKELY TO CONTINUE

In 2025, enterprising adversaries will undoubtedly continue to seek advanced exploitation opportunities across multiple domains, specifically cloud-based SaaS applications, to access sensitive data and conduct lateral movement. With many organizations migrating data from on-premises systems to cloud-based services, adversaries are expected to continue to adapt their tradecraft accordingly. Throughout 2024, CrowdStrike Intelligence observed several eCrime and targeted intrusion adversaries leverage access to cloud-based SaaS applications to obtain data to facilitate lateral movement, extortion, and downstream targeting of third parties. SaaS exploitation will therefore be a threat to watch in 2025.

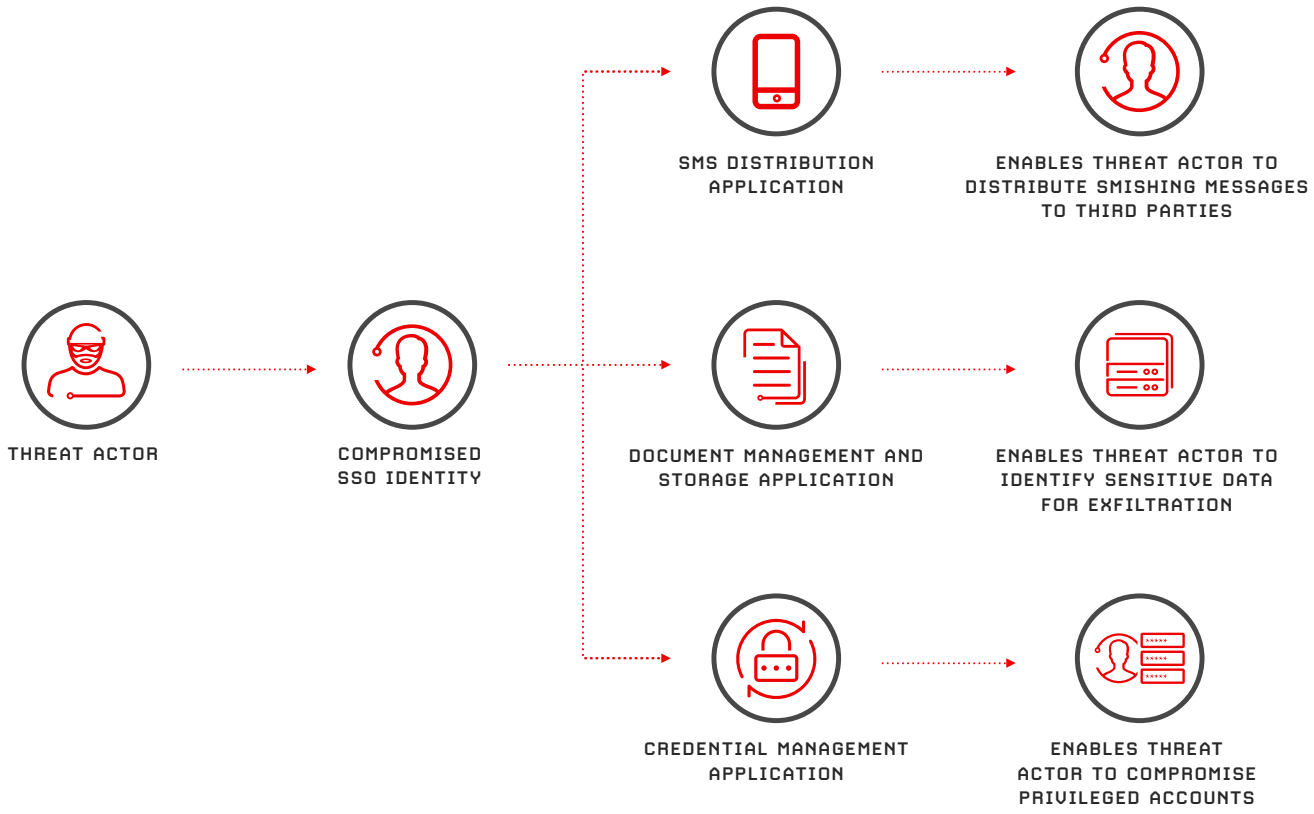


Figure 20. SaaS exploitation techniques

In most relevant cases, threat actors accessed SaaS applications after compromising an SSO identity. eCrime adversary SCATTERED SPIDER has employed this tactic since at least 2022. After gaining access to an SSO account, SCATTERED SPIDER often tests access to all available SSO-integrated applications, particularly those used for chat and video conferencing, credential management, customer relationship management, document management and storage, productivity and ticketing, and security.

In many intrusions, the adversary searched these applications for the following information:

- Account credentials and network architecture documentation to conduct lateral movement
- Cyber insurance and revenue information to inform extortion demands

Microsoft 365 has also become a popular target for cloud-conscious threat actors: SharePoint and Outlook were accessed in 22% and 17%, respectively, of relevant intrusions in the first half of 2024. SCATTERED SPIDER often uses strings such as `password manager`, `server inventory`, and `vpn instructions` to search compromised SharePoint tenants and mailboxes for data that will aid further account compromise and lateral movement to on-premises systems. Many organizations do not audit the data that employees upload to cloud-based storage repositories (such as SharePoint) or transmit internally via email, making these resources valuable targets for adversaries seeking to pivot within victim environments.

Threat actors can also leverage access to SaaS tooling to facilitate downstream targeting of third parties. In 2024, SCATTERED SPIDER obtained API keys to a commercial SMS distribution application from a compromised email inbox. The adversary subsequently used the application to send more than 700,000 SMS messages containing links to AITM phishing and cryptocurrency drainer pages.

The eCrime threat actor tracked in industry reporting as *Atlas Lion* adeptly abuses SaaS applications in their gift card fraud campaigns. Similar to SCATTERED SPIDER, *Atlas Lion* often gains initial access via SMS phishing (smishing), typically obtaining Microsoft 365 credentials. They use their access to compromised mailboxes to perform internal phishing in support of lateral movement. *Atlas Lion* uses access to HR-related SaaS applications to identify employees who have direct access to gift card resources and then searches for gift card-related strings across SSO-enabled applications, including Microsoft 365, chat platforms, and code repositories.

Customer Database Compromise Campaign

Malicious access to SaaS applications does not always follow a broader network compromise. In April 2024 and May 2024, a threat actor conducted a widely reported data theft and extortion campaign targeting customers of a data warehousing platform. To access customer database instances that did not require MFA or other controls such as network access policies, the threat actor leveraged compromised credentials obtained from information stealer logs that were widely available in eCrime channels and marketplaces.

This campaign targeted only the organizations' database instances, and no lateral movement or malicious activity impacting other applications or systems was observed. Threat actors could apply this tradecraft to steal data from other public-facing databases or cloud storage platforms not secured by MFA.

Adversaries will highly likely continue to target SaaS applications in 2025. This assessment is made with moderate confidence based on the proliferation of eCrime activity targeting SSO accounts and other relevant identities throughout 2024.

MANY ORGANIZATIONS DO NOT AUDIT THE DATA THAT EMPLOYEES UPLOAD TO CLOUD-BASED STORAGE REPOSITORIES (SUCH AS SHAREPOINT) OR TRANSMIT INTERNALLY VIA EMAIL, MAKING THESE RESOURCES VALUABLE TARGETS FOR ADVERSARIES SEEKING TO PIVOT WITHIN VICTIM ENVIRONMENTS.

Given that malicious access to SaaS applications typically begins with an identity compromise, relevant campaigns are best mitigated by hardening accounts with MFA. To minimize the risk of adversaries such as SCATTERED SPIDER manipulating MFA, organizations should consider using number matching or hardware-based FIDO2 devices, such as YubiKeys. Moreover, organizations should enforce MFA policies with secure verification methods across all accounts and regularly review any trusted zones or restriction exceptions to avoid unfettered access scenarios.

MITIGATION RECOMMENDATIONS

Organizations can further strengthen their defenses against SaaS compromise by implementing the following mitigation strategies:

Implement strong identity and access management (IAM)

- Use MFA for all user accounts
- Enforce strong password policies
- Implement least-privilege access principles
- Regularly review and audit user permissions

Enhance data protection

- Encrypt data at rest and in transit
- Implement data loss prevention (DLP) solutions
- Regularly back up critical data and test restoration processes

Conduct regular security assessments

- Audit SaaS providers to ensure compliance with relevant security frameworks

Improve monitoring and incident response

- Implement user behavior-based monitoring
- Develop and regularly test incident response plans

Educate users

- Provide regular security awareness training
- Teach employees to recognize phishing attempts and social engineering tactics

Implement secure configuration management

- Regularly review and update SaaS application settings
- Disable unnecessary features and integrations

Develop a robust vendor management program

- Assess a SaaS provider's security posture before adopting the software
- Regularly review provider security practices and certifications

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. Vishing was particularly popular, with eCrime adversaries more heavily relying on vishing, callback phishing, and help desk attacks to enter target networks. This trend is expected to continue and expand in 2025.

GenAI became a key adversary tool in 2024, especially in support of social engineering campaigns and high-tempo IO campaigns. Its low barrier to entry enables adversaries to create convincing content at scale without precise prompting or model training. Though genAI is still relatively novel, CrowdStrike has identified several examples of its use and anticipates it will be employed in 2025 adversary operations.

Though they are less impactful to victims than BGH adversaries, targeted eCrime adversaries remain a persistent threat to specific sectors. Throughout 2024, these threat actors demonstrated tenacity in their targeting, often compensating for lower sophistication by gaining in-depth knowledge about their victims' sectors, geographies, and associated technologies. Targeted eCrime adversaries demonstrated a growing interest in Latin American targets in 2024, realizing more lucrative profits through cryptocurrency theft in that region.

Targeted intrusion adversaries were also exceptionally active and innovative in 2024, adapting their tactics to achieve geopolitical and strategic objectives while evading improved defensive measures. Russia-nexus adversaries are expected to continue their aggressive pursuit of victory in Ukraine, focusing primarily 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. These adversaries will likely focus on entities operating in key sectors aligning with the CCP's strategic priorities.

The vulnerability exploitation landscape remains a critical concern. Threat actors are expected to continue aggressively targeting devices at the network periphery, particularly network appliances. End-of-life (EOL) product exploitation is almost certain to continue or grow in 2025. In their continued pursuit to discover new vulnerabilities or abuse legitimate product features, adversaries will likely leverage technical blogs and operationalize public POC exploits faster than in previous years.

SaaS applications are also an area of concern. After observing several 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 also anticipates SaaS exploitation will be a threat to watch in 2025.

Additionally, 2024 brought the emergence of threat actors who exclusively target cloud environments with unique, cloud-specific skill sets. Adversaries strengthened their emphasis on defense evasion in cloud environments, adopting stealth-oriented tactics and tools for initial access and credential access. This focus is expected to intensify 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, 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 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 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.

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 Agent

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

Charlotte AI

Powers the CrowdStrike portfolio of generative AI capabilities across the Falcon platform, 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 allow you to collect contextually enriched data and automate security operations, threat intelligence, and incident response — all in a single platform and through the same console — to mitigate cyber threats and vulnerabilities

CrowdStrike 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 (IoT), and more — and connecting them together in a graph form

CrowdStrike 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

CrowdStrike 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, no-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 | EXTENDED DETECTION AND RESPONSE

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 DATA PROTECTION | UNIFIED DATA PROTECTION

Provides deep real-time visibility into what is happening with sensitive data and stops data theft with policy enforcement that automatically follows content, not files

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 XDR/EDR 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 GO | SMB CYBER PROTECTION

Gives small businesses peace of mind against cyber threats with easy-to-install next-gen antivirus, device control, and mobile device protection

Counter Adversary Operations

FALCON ADVERSARY OVERWATCH | INTELLIGENCE-LED THREAT HUNTING

Provides 24/7 protection across endpoints, identities, and cloud workloads delivered by AI-powered threat hunting experts and includes built-in threat intelligence to expose adversary tradecraft, vulnerabilities, and stolen credentials

FALCON ADVERSARY INTELLIGENCE | SOC AUTOMATION

Cuts response time from days to minutes across the entire SOC with end-to-end intelligence automation, enabling you to instantly submit potential threats to an advanced malware sandbox, extract indicators of compromise, and deploy countermeasures — all while continuously monitoring for fraud and safeguarding your brand, employees, and sensitive data

FALCON ADVERSARY INTELLIGENCE PREMIUM | ADVERSARY INTELLIGENCE

Delivers industry-leading intelligence reporting at your fingertips, along with prebuilt detections and one-click hunting, to cut the time and cost required to understand and defend against sophisticated nation-state, eCrime, and hacktivist adversaries

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 APPLICATION SECURITY

Enables security teams to secure their entire SaaS stack through threat prevention, detection, and response; proactively find and fix weaknesses across their SaaS stack; and maintain continuous security for all configurations, human and non-human users, data, and SaaS genAI

Identity Protection

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 behavioral analytics, leveraging the unified Falcon platform to stop identity-based attacks in real time

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 streamline your SOC by unifying industry-best detection, world-class threat intelligence, blazing-fast search, and AI-led investigation in one platform

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 FILEVANTAGE | FILE INTEGRITY MONITORING

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

FALCON FOR IT | AUTOMATED WORKFLOWS

Extends the Falcon platform to automate IT and security workflows with an end-to-end, visibility-to-action life cycle

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 data — combining elite security expertise, AI-powered technology, and proactive threat hunting to detect, disrupt, and remediate sophisticated threats in minutes

CrowdStrike Services

INCIDENT RESPONSE

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

Incident Response Services | Provides comprehensive response and recovery in the event of a cyber breach — spanning investigation, remediation, and recovery — backed by world-class threat intelligence and delivered by a highly experienced IR team

Active Defense Services | Provides cross-domain response to recover from a breach with speed and precision

Services Retainer | Provides on-demand access to CrowdStrike expertise, from rapid response to long-term resilience

STRATEGIC ADVISORY SERVICES

Develops and matures the security program to improve defenses

Tabletop Exercises | 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

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

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

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

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

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