CROWDSTRIKE

2025 THREAT HUNTING REPORT

Table of Contents

Introduction

A new era of cyber threats has emerged with the rise of the “enterprising adversary,” as highlighted in the CrowdStrike 2025 Global Threat Report. This new breed of threat actor distinguishes itself through sophisticated and scalable tactics designed to execute attacks with calculated, business-like efficiency. These adversaries operate with strategic precision to maximize impact and quickly achieve their goals.

Innovation is a critical cornerstone to outmaneuver and disrupt the enterprising adversary. Novel technologies and threat hunting are required to anticipate the adversary's next moves, understand their evolving methodologies, and adapt defenses to stay ahead.

Today's enterprising adversary is adept at bypassing traditional cybersecurity defenses. They understand the limitations of conventional safeguards and seek to exploit security weaknesses and vulnerabilities that established systems and processes often overlook. This includes exploiting human factors through sophisticated social engineering techniques — now often enhanced by AI — and moving to unmanaged devices, which are often significant blind spots in an organization's security posture. By targeting devices outside the direct purview of IT departments, they can establish footholds, exfiltrate data, or launch further attacks without immediate detection.

The CrowdStrike Counter Adversary Operations team brings together industry-leading threat intelligence and best-in-class managed threat hunting with the AI-powered CrowdStrike Falcon® platform to detect, disrupt, and stop enterprising 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. Together, these teams protect thousands of customers from the most sophisticated adversaries by providing the intelligence and threat hunting skills and resources that most organizations lack.

Enterprising adversaries are using generative AI (GenAI) to enhance their operations, underscoring the critical need for innovative defensive strategies. The integration of GenAI into insider threat operations by Democratic People’s Republic of Korea (DPRK)-nexus adversary FAMOUS CHOLLIMA rapidly made them the most GenAI-proficient adversary. FAMOUS CHOLLIMA IT workers use GenAI to create attractive résumés for companies, reportedly use real-time deepfake technology to mask their true identities in video interviews, and leverage AI code tools to assist in their job duties, all of which pose a substantial challenge to traditional security defenses.

Adversaries continually seek to stay undetected by moving to unmanaged networks and expanding their reach. Cross-domain threat hunting is critical, as adversaries increasingly operate across multiple domains — such as identity, endpoint, and cloud — in their efforts to evade detection. These cross-domain threats often generate fewer detections in a single domain or product, making the activity difficult to recognize as malicious. To stay ahead of sophisticated cross-domain adversaries such as BLOCKADE SPIDER and OPERATOR PANDA, CrowdStrike OverWatch hunters are expanding their hunting grounds with innovative next-gen security information and event management (SIEM) technology to capture adversaries' every move.

Though adversaries that prioritize rapid execution have the most visible and immediate impact, those that emphasize stealth, prolonged presence, and the meticulous execution of a "long game" approach present an equally potent threat. These operations often include sustained access, covert data harvesting, and — in some cases — preparing a victim's environment for future, more impactful operations. China-nexus adversaries such as GLACIAL PANDA have increasingly excelled at this approach. GLACIAL PANDA primarily targets the global telecommunications sector through patient and methodical infiltration, established persistence, and deep, quiet reconnaissance of target networks, systems, and data. The challenge in detecting these stealthy adversaries is amplified by their minimal digital footprint, allowing them to easily blend into legitimate network traffic. CrowdStrike OverWatch successfully disrupts them by conducting customized hunts that uncover trojanized software and malicious code and focusing on repeated attempts to access sensitive data sources.

In the first half of 2025, CrowdStrike OverWatch identified a 136% increase in cloud intrusions compared to all of 2024, highlighting the fact that more threat actors are becoming versed in exploiting cloud environments. China-nexus adversaries in particular have quickly gained proficiency in cloud exploitation techniques; GENESIS PANDA and MURKY PANDA, for example, have become adept at navigating cloud environments. Over the past 12 months, CrowdStrike OverWatch observed a 40% increase in cloud intrusions attributed to China-nexus adversaries. CrowdStrike OverWatch keeps pace by developing innovative hunting techniques for cloud services, workloads, and control planes as well as leveraging advances in identity protection.

In the CrowdStrike 2025 Global Threat Report, CrowdStrike reported that voice phishing (vishing) attacks increased by 442% from the first to the second half of 2024, marking a significant and effective evolution in eCrime tactics. This trend has not slowed down in the first half of 2025, where vishing attacks have already surpassed the total number seen in 2024. These attacks are successful because they exploit human vulnerabilities and leverage compromised credentials and social engineering to bypass traditional security measures, gain initial access, and move laterally within organizations at speed. One of the earliest adopters of this tactic is SCATTERED SPIDER, an eCrime adversary well known for their sophisticated social engineering and credential theft techniques. In 2025, this adversary exploded back into the eCrime landscape, and though they showcased some new techniques, help desk attacks have remained a prominent tool in SCATTERED SPIDER's arsenal.

» IN THE FIRST HALF OF 2025, CROWDSTRIKE OVERWATCH IDENTIFIED A 136% INCREASE IN CLOUD INTRUSIONS COMPARED TO ALL OF 2024.

» IN THE CROWDSTRIKE 2025 GLOBAL THREAT REPORT, CROWDSTRIKE REPORTED THAT VOICE PHISHING (VISHING) ATTACKS INCREASED BY 442% FROM THE FIRST TO THE SECOND HALF OF 2024, MARKING A SIGNIFICANT AND EFFECTIVE EVOLUTION IN eCRIME TACTICS. THIS TREND HAS NOT SLOWED DOWN IN THE FIRST HALF OF 2025, WHERE VISHING ATTACKS HAVE ALREADY SURPASSED THE TOTAL NUMBER SEEN IN 2024.

Also noted in the CrowdStrike 2025 Global Threat Report, 52% of vulnerabilities observed by CrowdStrike in 2024 were related to initial access. Adversaries continue to exploit internet-exposed applications for initial access. When adversaries like GRACEFUL SPIDER develop zero-day exploits, CrowdStrike OverWatch's ability to identify and hunt for post-exploitation malicious behaviors becomes a critical fail-safe, ensuring rapid and effective coverage against widespread exploitation.

The CrowdStrike 2025 Threat Hunting Report highlights key trends and shifts the CrowdStrike OverWatch team observed over the past 12 months and details how CrowdStrike Falcon® Adversary OverWatch™ leverages innovation and proactive, intelligence-informed threat hunting to track, detect, and disrupt the adversary. This year's report presents trends the team identified from July 1, 2024, to June 30, 2025. In this time frame, CrowdStrike OverWatch observed the following:

- **81% of interactive intrusions were malware-free.**
- **Interactive (hands-on-keyboard) intrusions increased 27% year-over-year**, highlighting that adversaries are innovating their operations to bypass legacy detection methods.
- **eCrime activity represented 73% of total interactive intrusions.**
- **Cloud intrusions increased 136% in the first half of 2025** compared to all of 2024.
- CrowdStrike OverWatch observed a **40% year-over-year increase in intrusions** by suspected cloud-conscious China-nexus actors.
- In the first half of 2025, **vishing attacks already surpassed the total number seen in 2024.**
- The government sector was affected by a **71% year-over-year increase** in overall interactive intrusions and a **185% year-over-year increase** in targeted intrusion activity.
- **FAMOUS CHOLLIMA insiders infiltrated over 320 companies in the last 12 months — a 220% year-over-year increase** — by leveraging GenAI at every stage of the hiring and employment process.
- SCATTERED SPIDER accelerated their operations — in one incident, **the adversary moved from account takeover to ransomware deployment in just 24 hours, 32% faster than they were able to accomplish this in 2024.**

This report showcases the Counter Adversary Operations team's relentless pursuit to disrupt the adversary. In CrowdStrike customer environments, adversaries face a unified security solution that empowers every CrowdStrike threat hunter with extensive security telemetry — spanning endpoint, identity, cloud, and next-gen SIEM, along with integrated intelligence — to detect and disrupt threats quickly and effectively.

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	TÜRKIYE

Front-Line Snapshot

The statistics provided in this report specifically focus on interactive intrusions — attacks where adversaries establish an active presence within a target network, often engaging in hands-on-keyboard activities to achieve their objectives. Unlike automated attacks, interactive intrusions involve human operators who interact with systems in real time, adapting their tactics as needed. They are typically more sophisticated and difficult to detect than automated attacks, and they require advanced threat hunting and incident response capabilities to identify and mitigate.

ANATOMY OF AN INTERACTIVE INTRUSION

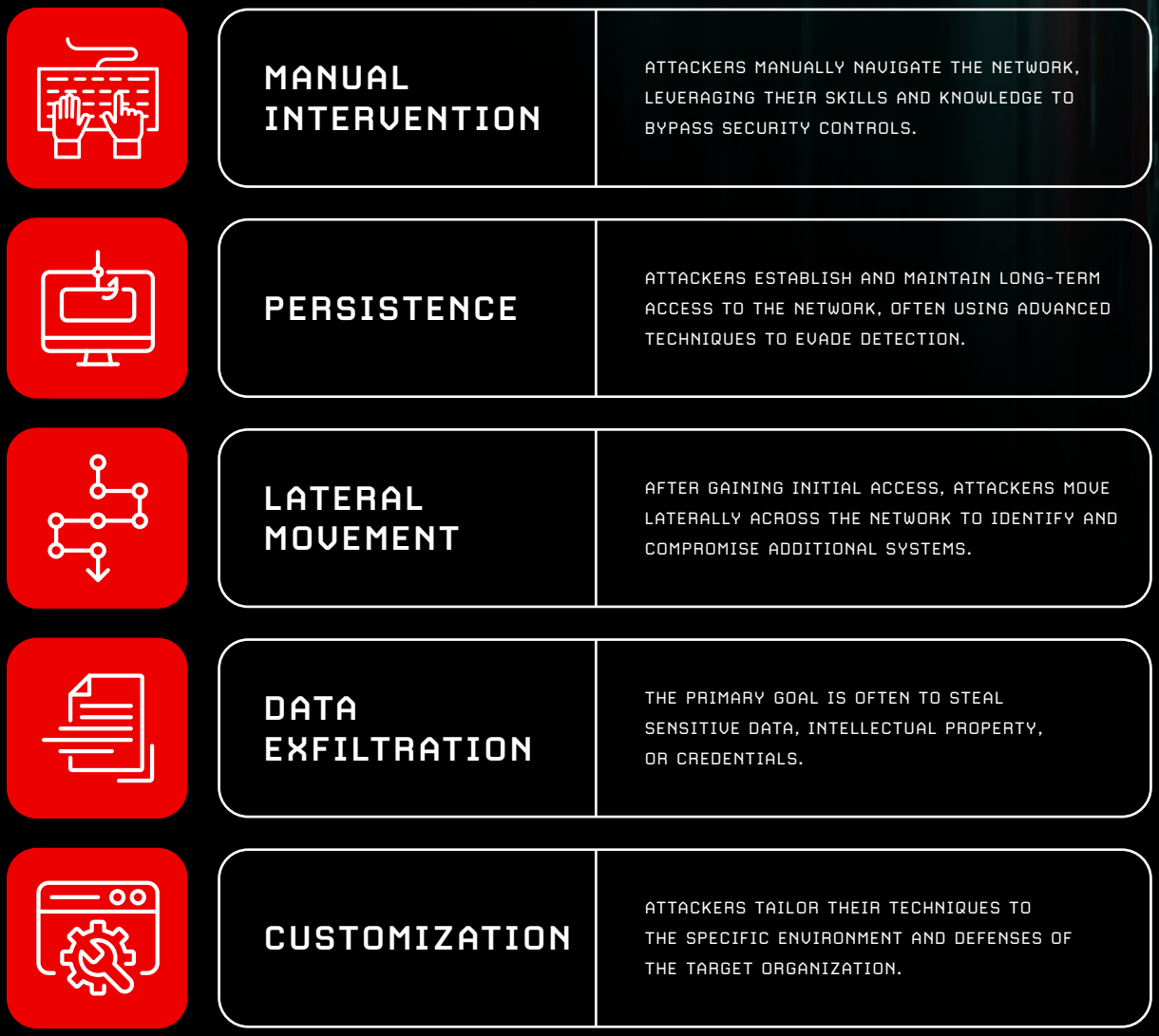


Figure 1. Description of a typical interactive intrusion observed by CrowdStrike OverWatch

Over the past 12 months, CrowdStrike OverWatch observed interactive intrusions continue to climb, increasing 27% year-over-year. The overall distribution of interactive intrusion activity by threat type saw a noted increase in eCrime: 73% of the total 2025 reporting period volume was associated with eCrime activity, highlighting the persistent and pervasive threat of adversaries seeking financial gain.

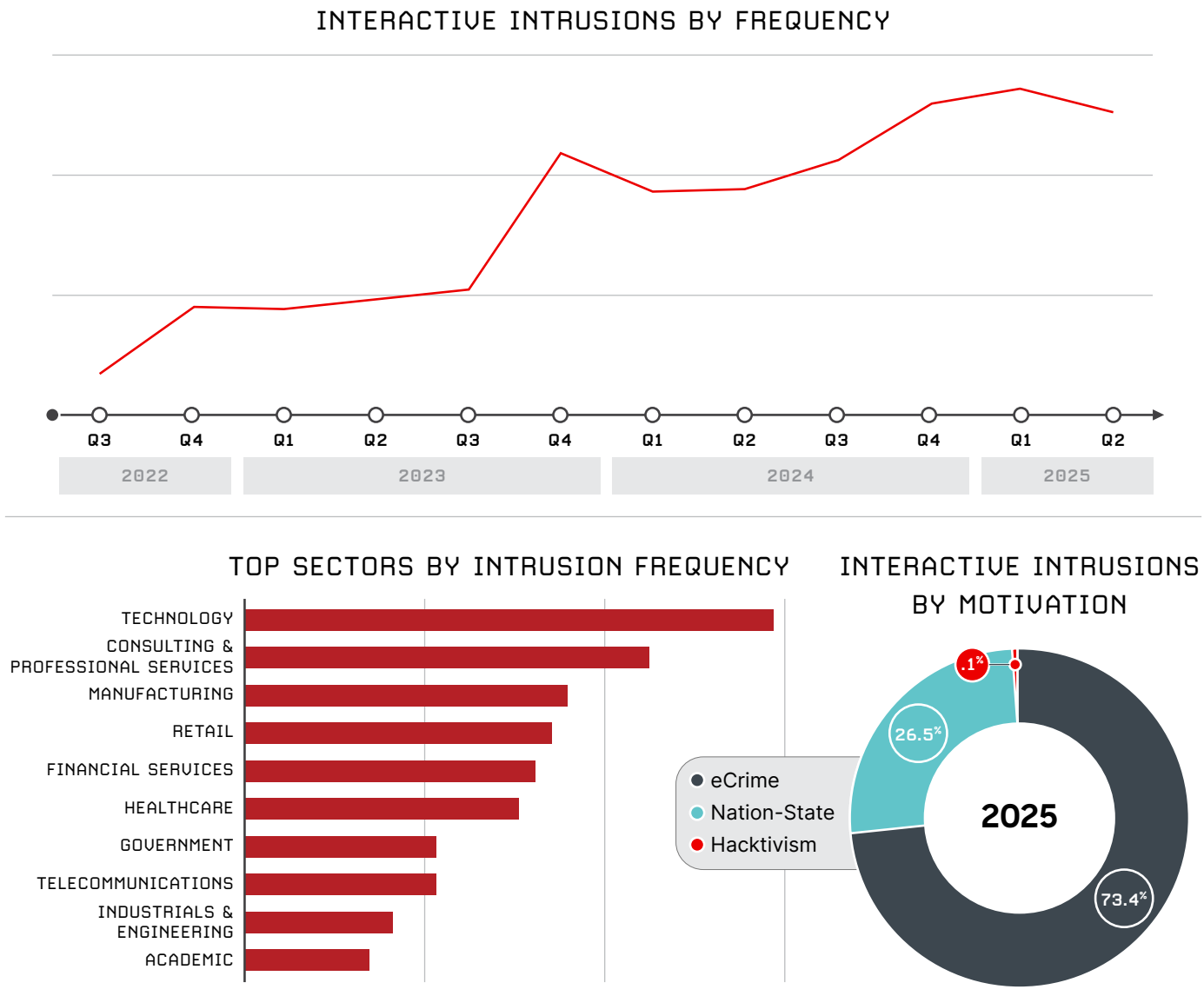


Figure 2. Interactive intrusion breakdown

SECTOR TARGETING

The technology sector remained at the top of the list for the reporting period, making technology the most frequently targeted industry for the eighth consecutive year. This sector encompasses a broad range of organizations that develop computer software and hardware or provide IT services or technology. Due to its relationship to many other sectors, the technology sector is a high-value target for both nation-state and eCrime adversaries.

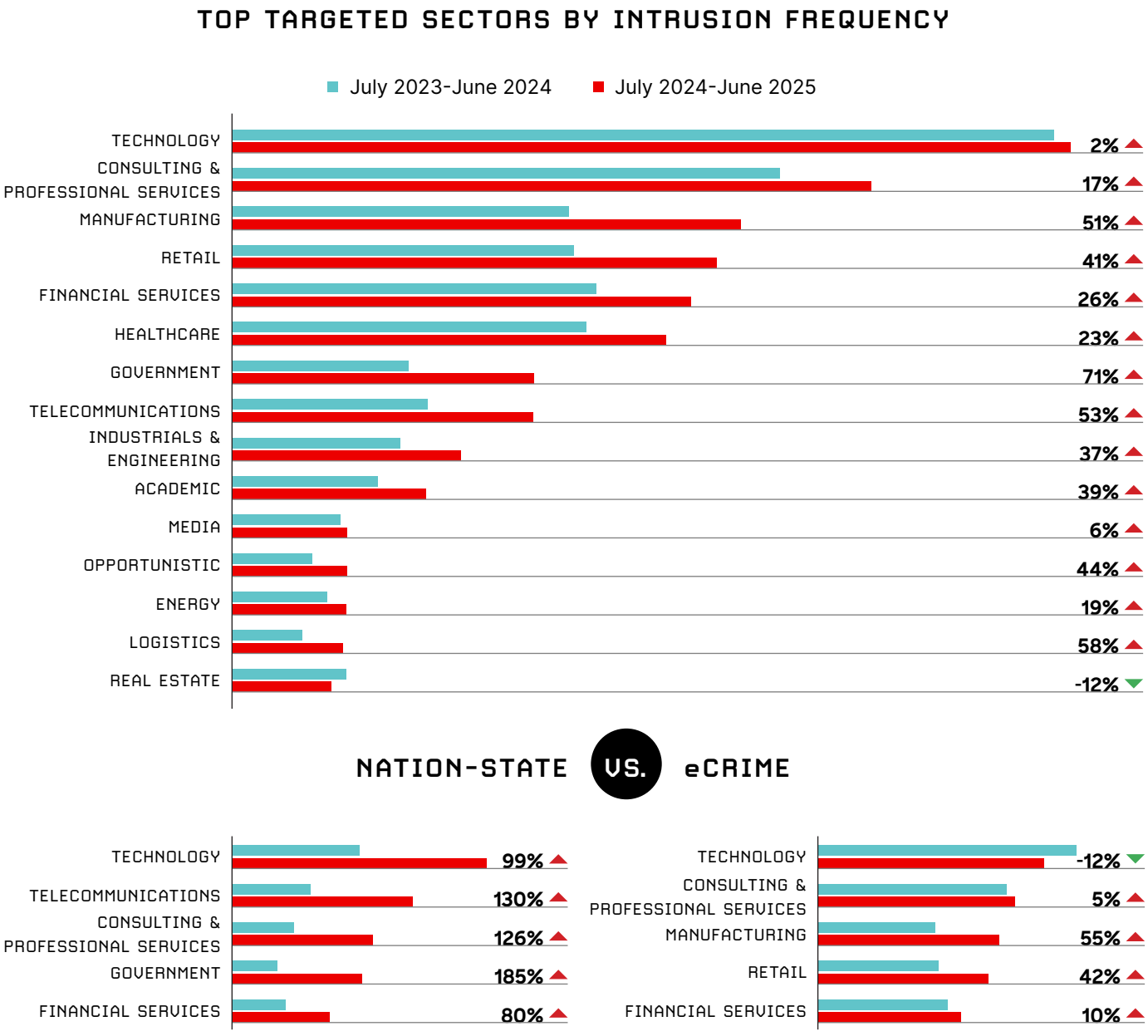


Figure 3. Targeted sectors by intrusion frequency

The government and telecommunications sectors saw a significant increase in interactive intrusions during the reporting period, namely by nation-state adversaries. Russia-nexus activity accounted for most of the government targeting, while China-nexus activity accounted for most of the telecommunications targeting.

SECTOR SPOTLIGHTS

Government

CrowdStrike observed a 71% increase in overall interactive intrusions and a 185% increase in nation-state activity within the government sector over the past 12 months. Though the government sector is consistently a high-value target for a variety of nation-state adversaries, this significant increase is attributed to activity conducted by Russia-nexus adversaries such as PRIMITIVE BEAR and VENOMOUS BEAR, who conduct suspected espionage operations against Ukraine government entities in direct support of the conflict in Ukraine.

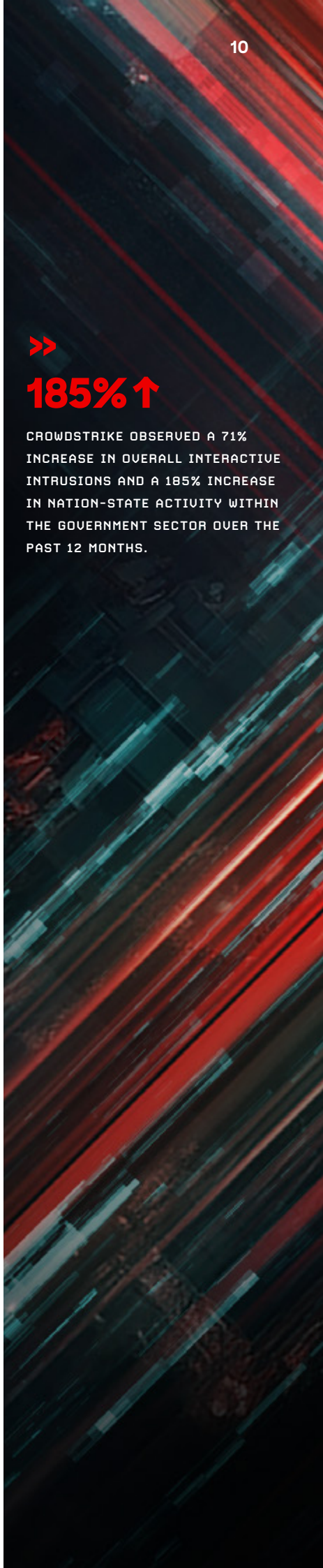
Telecommunications

CrowdStrike observed a 53% increase in overall interactive intrusions and a 130% increase in nation-state activity within the telecommunications sector over the past 12 months. This activity has primarily focused on entities in countries across Asia and North America. It is directly related to a surge in China-nexus adversaries' operations against the telecommunications industry, which have become the most significant and consistent targeted intrusion threat to this sector over the past year. The telecommunications sector is a high-value target for nation-state adversaries, providing access to subscriber and organizational data that supports their intelligence collection and counterintelligence efforts. Telecommunication network access can also enable intrusion vectors and traffic collection against downstream customer organizations that obtain connectivity from the provider.

Manufacturing and Retail

CrowdStrike observed notable increases in eCrime interactive intrusions targeting the manufacturing (55%) and retail (41%) sectors over the past 12 months. CURLY SPIDER emerged as a prominent threat actor conducting intrusions against North America-based retail and manufacturing entities at an increased rate. CURLY SPIDER is an eCrime group that has conducted ransomware intrusions (which predominantly involve vishing) targeting North America- and Western Europe-based entities across various sectors.

Manufacturing and retail entities remain high-value targets for eCrime intrusions because these entities' operating nature incentivizes them to pay ransoms quickly. Manufacturers cannot afford production delays, and retailers risk losing customer data and sales, especially during busy shopping seasons. These industries typically have larger budgets and complex computer systems that can be outdated, which also makes them attractive targets.



MITRE ATT&CK OBSERVATIONS

CrowdStrike OverWatch tracks interactive intrusion activity against the MITRE ATT&CK® Enterprise Matrix, a framework that categorizes and tracks adversary behavior.[1]

Figure 4 illustrates the top MITRE ATT&CK tactics and techniques CrowdStrike OverWatch detected in interactive intrusion activity over the past 12 months. CrowdStrike OverWatch is constantly hunting for post-exploitation behaviors regardless of the initial access vector. As a result, CrowdStrike OverWatch most often observes techniques within the Defense Evasion tactic, when adversaries are attempting to disguise their malicious activities as innocuous, expected activity.

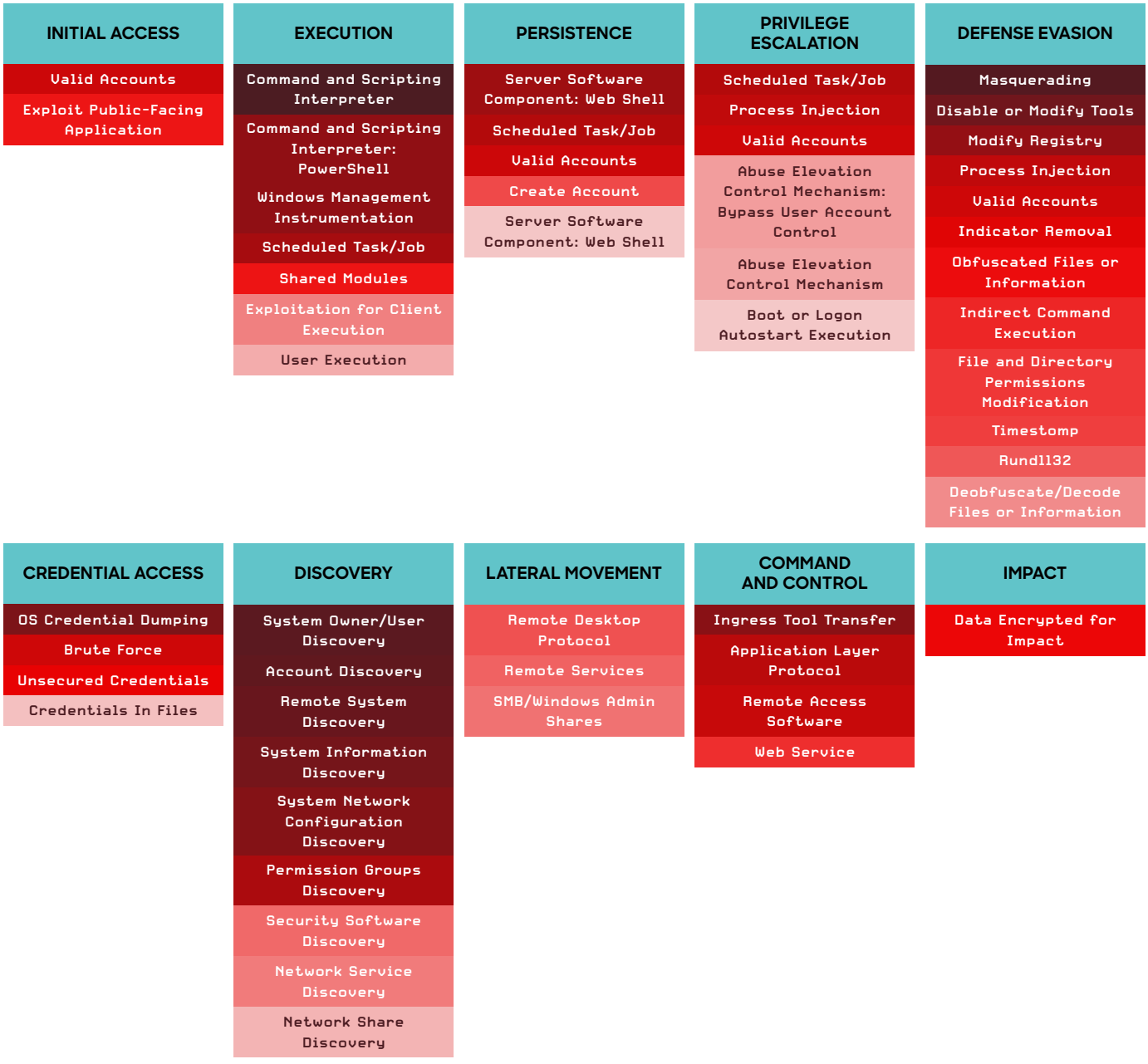


Figure 4. MITRE ATT&CK heat map highlighting the top techniques CrowdStrike OverWatch observed adversaries employ in each tactic area, July 2024-June 2025

1 To learn more about the MITRE ATT&CK Enterprise Matrix, visit https://attack.mitre.org/matrices/enterprise/

Though CrowdStrike OverWatch observed the most total activity within the Defense Evasion tactic, five of the top 10 most commonly used MITRE ATT&CK techniques in the past 12 months were Discovery techniques. This highlights that adversaries are both spending their time orienting themselves within a network and ensuring their activities are not detected by security measures whenever possible. eCrime access brokers rely on these techniques — including Account Discovery, System Network Configuration Discovery, and Remote System Discovery — to evaluate targets as part of the threat actors' efforts to monetize operations.

Defense Evasion techniques such as Masquerading and Disable or Modify Tools — as well as Ingress Tool Transfer, a Command and Control technique — were also in the top 10 most leveraged techniques. These techniques allow adversaries to blend their activity into expected network activity while enabling follow-on activities in various other tactic areas, such as Privilege Escalation and Credential Access.

INTRUSION TRENDS BY ADVERSARY

CrowdStrike's insight into adversaries is unmatched. With detailed information about more than 265 attributed eCrime, nation-state, and hacktivist adversaries — and more than 150 active clusters of malicious activity that have not yet met CrowdStrike's standards for adversary graduation — CrowdStrike OverWatch threat hunters are well positioned to quickly and accurately disrupt the adversary. Figure 5 highlights the most prevalent adversary operations identified over the past 12 months.

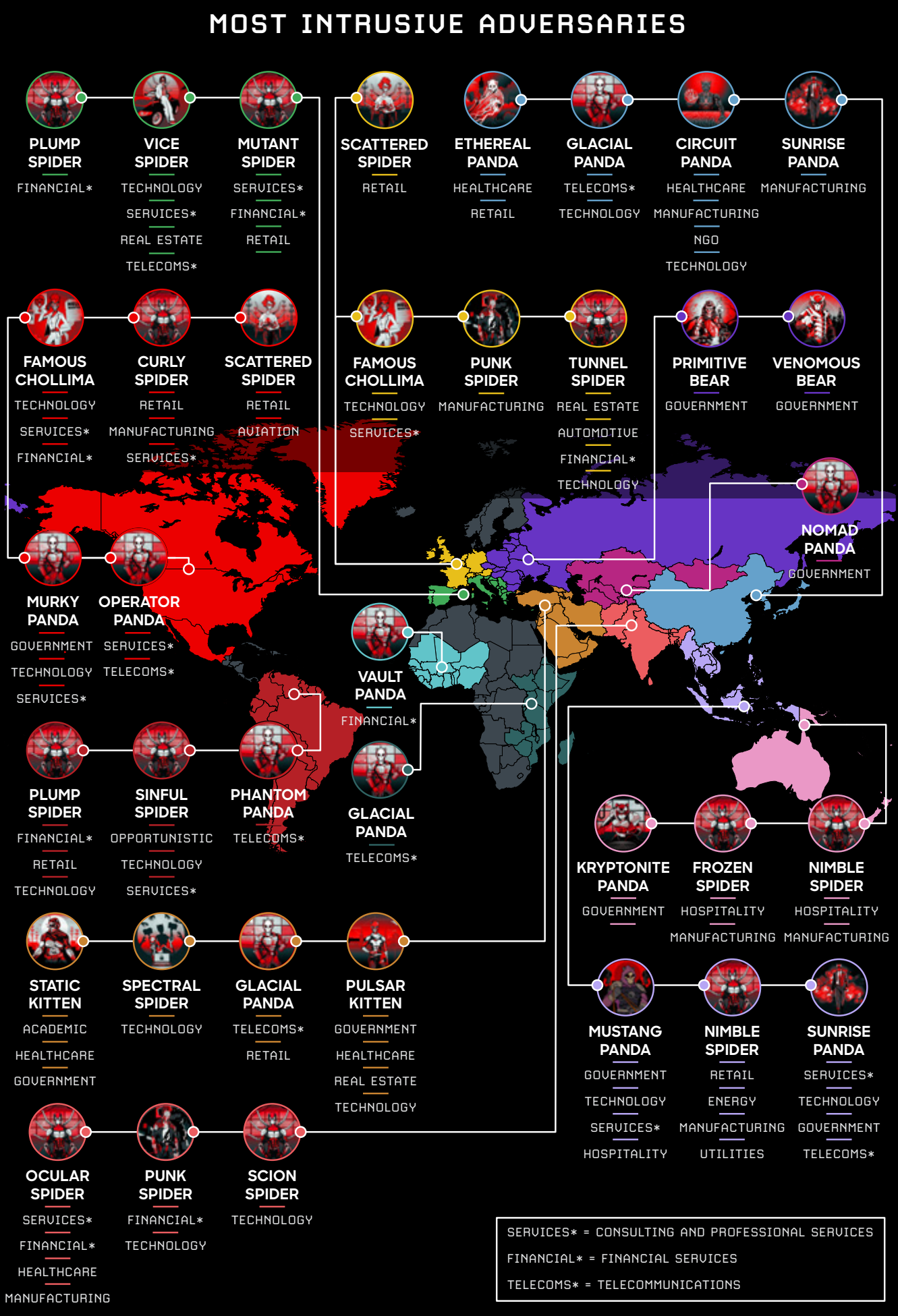


Figure 5. Interactive adversary disruptions across the world, July 2024-June 2025

Observations from the Front Lines

COUNTERING THE ADVERSARY: GENERATIVE ARTIFICIAL INTELLIGENCE

Enterprising threat actors have capitalized on the surge of recently developed GenAI models to conduct social engineering, technical operations, and information operations (IO). GenAI tools have likely contributed to increased speed, access to expertise, and scalability in threat actor operations. At the same time, organizations' integration of AI into business operations has created a new attack surface for threat actors to target. Despite these observable advantages for attackers, AI-enhanced cyber operations face similar constraints to traditional cyber operations, including resource availability and authorities.

Defining GenAI

GenAI is a subset of AI designed to create new data based on existing data. It is powered primarily by advanced machine learning models such as large language models (LLMs), which use natural language processing to generate text, and diffusion models, which create images, audio, and video content.[2]

2 Generative AI in Cybersecurity || What Is the Difference Between a Diffusion Model and LLM in Simple Terms || Explained: Generative AI

How Threat Actors Leverage GenAI to Augment Operations

Throughout 2024 and 2025, threat actors have increasingly integrated GenAI across their operations, using it to enhance their methods rather than replace existing tactics, techniques, and procedures (TTPs).

Nation-state adversaries — such as those attributed to Iran and North Korea — are increasingly adopting GenAI technology to make their cyber operations faster, more efficient, and harder to detect. They are using publicly available models to aid their reconnaissance, vulnerability research, and phishing campaign content and payload development. Threat actors with fewer resources, including eCrime and hacktivist actors, have employed GenAI to automate tasks and improve their tools, including script generation, technical problem-solving, malware development, and infrastructure enhancement.

Adversary use of GenAI spans three primary vectors, each with distinct adoption patterns and impact:

Figure 6. Adversary use of GenAI as a primary attack vector

FAMOUS CHOLLIMA Leads in GenAI-Supported Operations

DPRK-nexus adversary FAMOUS CHOLLIMA conducts insider threat operations at an exceptionally high operational tempo. In the past 12 months, CrowdStrike OverWatch investigated over 320 incidents where FAMOUS CHOLLIMA operatives obtained fraudulent employment as remote software developers. FAMOUS CHOLLIMA has been able to sustain this pace by interweaving GenAI-powered tools that automate and optimize workflows at every stage of the hiring and employment process.

Though some specific technical implementation details remain speculative, the breadth of evidence from multiple sources presents a clear picture of an adversary deeply invested in leveraging GenAI to enhance their operational capabilities and scale their deceptive employment schemes. FAMOUS CHOLLIMA is highly likely to continue to rely on GenAI tools to facilitate success at every stage of their IT worker operations.

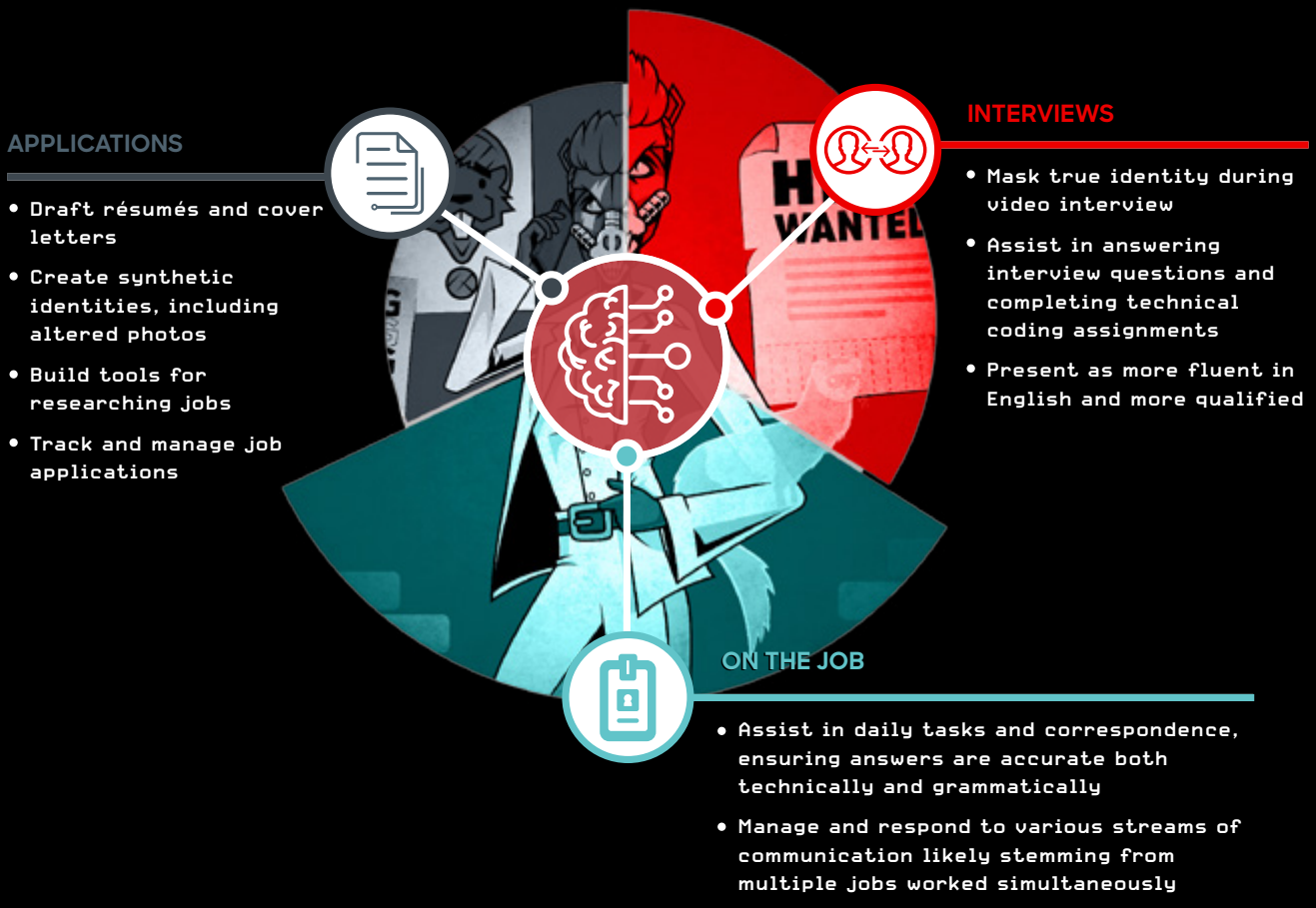


Figure 7. FAMOUS CHOLLIMA's use of GenAI in insider threat operations

APPLICATIONS

FAMOUS CHOLLIMA uses GenAI tools to generate synthetic identities used in insider threat activity. Email addresses associated with FAMOUS CHOLLIMA aliases were present in a user database leak of the AI photo editing tool `cutout[.]pro`, which plausibly could have been used to alter images for social media profiles or identification documents.[3] Google Gemini and OpenAI have also reported that DPRK IT workers have abused their GenAI tools to draft cover letters and résumés, research job openings, and build tools for managing and tracking job applications.[4]

INTERVIEWS

FAMOUS CHOLLIMA operatives very likely use real-time deepfake technology to mask their true identities in video interviews. Using a real-time deepfake plausibly allows a single operator to interview for the same position multiple times using different synthetic personas, enhancing the odds that the operator will get hired. CrowdStrike has also observed FAMOUS CHOLLIMA operatives searching terms associated with real-time face swapping and AI webcam troubleshooting, retrieving the AI face swapping app Hacksider from GitHub, and paying for the premium subscription via PayPal during services engagements.

Reports released by OpenAI in June 2025 further indicate that FAMOUS CHOLLIMA used the company's LLMs to assist in answering employment-related questions, to help complete technical coding assignments, and to prepare for real-time interview questions.[5] Use of GenAI tools in this way likely makes FAMOUS CHOLLIMA operatives appear more fluent in English or more qualified than they are, further helping impostors obtain job offers.

ON THE JOB

Once hired, FAMOUS CHOLLIMA IT workers use GenAI code assistants (such as Microsoft Copilot or VSCodium) and GenAI translation tools to assist with daily tasks and correspondence related to their legitimate job functions. Though an average employee may use GenAI in a similar manner, these tools — especially those enabling English-language communication — are especially crucial to FAMOUS CHOLLIMA. These operatives are not fluent in English, likely work three or four jobs simultaneously, and require GenAI to complete their work and manage and respond to multiple streams of communication.

CrowdStrike has investigated incidents where operators use GenAI tools to assist in drafting and translating work-related emails and use chatbots to respond to instant messages and emails. Industry sources have also seen operatives using GenAI to manage the workflows of multiple jobs via AI-enhanced unified chat applications.[6]

---

3 Hacker Leaks Records of 20 Million Users of AI Visual Creation Platform Online
4 Adversarial Misuse of Generative AI
5 Disrupting Malicious Uses of AI: June 2025
6 How AI Services Power the DPRK's IT Contracting Scams

COUNTERING FAMOUS CHOLLIMA

These recommendations can be implemented to help protect against FAMOUS CHOLLIMA's insider threat activity:

- **Implement** enhanced identity verification processes during the hiring phase that include rigorous background investigations and corroboration of online professional profiles.
- **Implement** real-time deepfake challenges during interview or employment assessment sessions.
- **Augment** security controls pertaining to remote access to corporate systems, with a particular focus on geolocation masking and endpoint security circumvention attempts.
- **Validate** connected USB and other peripheral devices to identify and prevent the use of physical and software-based remote tools.
- **Monitor** employee communication channels for manifestations of aberrant translation activities or concurrent administration of multiple accounts.
- **Create** training programs designed to teach hiring managers and IT personnel to recognize and report potential indicators of insider threats employing AI tools.

Threat Actors Targeting AI Tools

The increasing adoption of AI tools and technology within organizational networks and workflows is likely to lead to a rise in adversaries targeting these tools. Threat actors are using organizations' AI tools as initial access vectors to execute diverse post-exploitation operations.

In April 2025, CrowdStrike observed multiple threat actors exploit CVE-2025-3248, an unauthenticated code injection vulnerability in Langflow AI. Langflow is a widely used tool for building AI agents and workflows. Attackers can exploit CVE-2025-3248 using specially crafted HTTP requests to achieve unauthenticated remote code execution.

Threat actors leveraged CVE-2025-3248 against this AI tool to pursue three main objectives: persistence, credential access, and malware deployment. They established persistence through reverse shell connections, modified SSH configurations, and cron-based scheduled tasks. Credential access involved threat actors dumping password and shadow files and targeting cloud environment credentials. Threat actors also deployed various malware, including the cryptomining malware *XMRig*, multi-stage VShell remote access tools (RATs), and *Cerber* ransomware.

This activity demonstrates that threat actors are viewing AI tools as integrated infrastructure rather than peripheral applications, targeting them as primary attack vectors. As organizations continue adopting AI tools, the attack surface will continue expanding, and trusted AI tools will emerge as the next insider threat.

Outlook

GenAI enhances threat actors' operations rather than replacing existing attack methodologies. The effectiveness of these tools, however, depends on system availability, defensive-offensive capability balance, and operational integration. GenAI is not likely to definitively benefit offensive or defensive operations. Rather, more sophisticated users will likely maintain their advantage in exploiting GenAI's potential, especially in technical operations. This is partly because AI-generated code still requires significant human expertise to be effective.

» GENAI IS NOT LIKELY TO DEFINITIVELY BENEFIT OFFENSIVE OR DEFENSIVE OPERATIONS. RATHER, MORE SOPHISTICATED USERS WILL LIKELY MAINTAIN THEIR ADVANTAGE IN EXPLOITING GENAI'S POTENTIAL, ESPECIALLY IN TECHNICAL OPERATIONS. THIS IS PARTLY BECAUSE AI-GENERATED CODE STILL REQUIRES SIGNIFICANT HUMAN EXPERTISE TO BE EFFECTIVE.

Threat actors of all motivations and skill levels will almost certainly increase their use of GenAI tools for social engineering in the near- to mid-term, particularly as these tools become more available, user-friendly, and sophisticated. For these same reasons, threat actors conducting IO campaigns will also almost certainly continue to use AI-generated videos, audio, images, and text content to influence political movements or events. They will also likely continue to leverage GenAI to build seemingly credible media websites and social networks for large-scale information dissemination.

Though defenders can leverage AI for security capabilities — including red teaming and detecting and responding to threats — organizations' continued AI tooling integration creates an expanded attack surface that threat actors will likely seek to exploit by directly targeting AI applications.

How CrowdStrike OverWatch Applies AI to Threat Hunting

CrowdStrike OverWatch focuses on building a symbiotic relationship with AI that scales human insight without sacrificing precision. This enables the team to operate with speed, depth, and efficiency across global environments — without compromising the human judgment that makes threat hunting effective. CrowdStrike OverWatch leverages AI to:

Scale Operations: CrowdStrike OverWatch's tooling is built on machine learning, allowing the team to reduce noise, surface high-confidence signals, and enable elite threat hunters to move faster with greater precision. While much of the industry positions AI as a tool for finding threats, we view it as a force multiplier — one that separates the irrelevant from the important at scale.

Identify Complex Behaviors: Deep learning plays a critical role in this process. It's a domain of machine learning that is used to train AI models to learn to recognize complex patterns by processing large amounts of unstructured data. While much of the industry is just now embracing it under the banner of GenAI, CrowdStrike OverWatch began integrating deep learning into threat hunting as early as 2016. That early investment gave us the maturity and infrastructure to detect complex, stealthy behaviors that would otherwise go unnoticed.

Build Resilience Against AI-Enabled Adversaries and Model Poisoning: Responsible AI is one of the core principles that has shaped CrowdStrike OverWatch from the beginning, ensuring both trust and long-term resilience. As AI increasingly becomes a high-value target for adversaries, that discipline matters more than ever. Adversaries are now using techniques like model poisoning and prompt engineering to misguide what AI learns by labeling malicious code as safe. CrowdStrike OverWatch prevents this by design. Our models are trained only on curated, validated data from confirmed threat activity — they never scrape data from open sources and are not built on untrusted inputs. All training takes place within tightly controlled pipelines, and models are retrained frequently with input from front-line threat hunters and intelligence analysts. This closed-loop validation helps ensure that learning stays accurate and resilient to manipulation.

HUNTING CROSS-DOMAIN ADVERSARIES

Cross-domain threat hunting enables detection of adversary activities that span multiple security areas, including identity systems, endpoints, and cloud environments. These attacks are challenging to detect because activities are distributed, resulting in a reduced footprint within each individual security domain. When viewed separately, these dispersed actions may appear benign or unrelated, making it harder to identify them as parts of a coordinated malicious campaign.

Adversaries are also becoming more adept at finding and pivoting to unmanaged hosts on target networks, seeking to bypass traditional security measures such as endpoint detection and response (EDR). By implementing innovative hunting solutions, organizations can effectively broaden their threat hunting field by adding more data sources. This enhanced visibility enables fast and comprehensive hunting and investigations, ensuring better protection against evolving threats. When faced with some of the most elusive cross-domain adversaries — namely BLOCKADE SPIDER and China-nexus OPERATOR PANDA — cross-domain visibility from innovative solutions, such as CrowdStrike Falcon® Next-Gen SIEM, can play a pivotal role in an organization's threat hunting strategy.

Hunting in a Shifting Ransomware Landscape

The ransomware landscape continuously shifts, with emerging adversaries filling the void created by the disruption of criminal operations and established adversaries. In 2024, prolific big game hunting (BGH) adversaries ALPHA SPIDER and BITWISE SPIDER were both disrupted by law enforcement, leading to the rise of OCULAR SPIDER's *RansomHub* ransomware as a service (RaaS) program. In turn, the *RansomHub* RaaS infrastructure went offline in March 2025, seemingly following a conflict with the *DragonForce* RaaS administrator and several *RansomHub* affiliates.

Though law enforcement operations and conflicts among criminals disrupt illicit activities, they also motivate RaaS affiliates to create or join private ransomware operations or other RaaS programs. These new organizations, operations, and services create a shifting and fluid eCrime threat landscape, though threat actors continue to leverage well-established TTPs to encrypt and/or steal data.

In 2025, these ransomware TTPs commonly involve dumping credentials from Veeam Backup & Replication configuration databases, targeting unmanaged systems,[7] and using ransomware to remotely encrypt files. Adversaries often use these techniques together in a complementary manner, where the use of one technique facilitates the use of another.

7 An unmanaged system is a device or endpoint that is not monitored, controlled, or protected by the organization's security tools

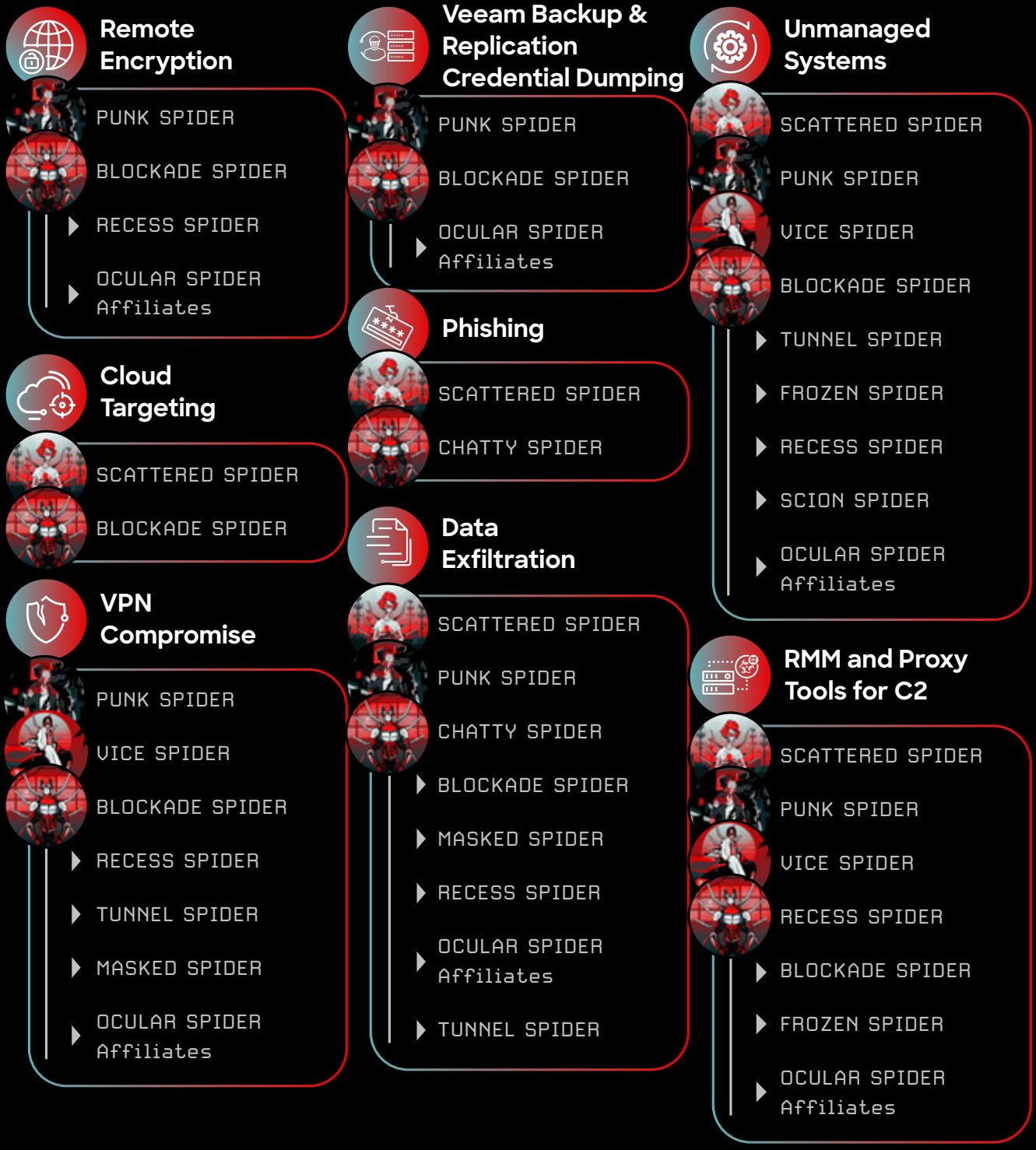


Figure 8. Most commonly used TTPs leveraged by ransomware operators in 2025

STOPPING REMOTE FILE ENCRYPTION WITH FALCON PREVENT

CrowdStrike Intelligence tracks multiple adversaries — including PUNK SPIDER and BLOCKADE SPIDER — whose ransomware variants support remotely encrypting files via Server Message Block (SMB) network shares. This technique allows adversaries to operate on unmanaged systems, from which they then execute ransomware to encrypt files on remote systems without transferring the ransomware binary to the targeted systems.

CrowdStrike® Falcon Prevent® customers can enable the File System Containment feature to gain enhanced protection against remote encryption attacks occurring over SMB. When this feature is enabled in prevention policy settings, the Falcon sensor detects the activity and contains the compromised user on the targeted host, preventing the attack.

BLOCKADE SPIDER is a sophisticated, financially motivated eCrime adversary that commonly uses these ransomware techniques to facilitate the deployment of *EMBARGO* ransomware and data theft to monetize their operations.

In addition to dumping credentials from Veeam Backup & Replication configuration databases and moving laterally to virtualized infrastructure such as VMware ESXi[8] and other unmanaged systems to remotely encrypt files with *EMBARGO* ransomware, BLOCKADE SPIDER also displayed the capability to target cloud environments, making this adversary one of the most adept at quickly operating across domains.

CASE STUDY:

Disrupting BLOCKADE SPIDER

CrowdStrike OverWatch identified that BLOCKADE SPIDER had accessed a victim's network via an unmanaged VPN appliance in early 2025. The adversary moved laterally to several managed systems, where they performed actions typically observed in BGH activity, including attempting to dump credentials from a Veeam Backup & Replication configuration database and delete backup files.

BLOCKADE SPIDER made several attempts to interfere with the Falcon sensor. Though these attempts failed, the adversary was not deterred and rapidly adapted their strategy. Tracking and disrupting this adversary quickly required additional data sources, which is where cross-domain data from identity sources and Falcon Next-Gen SIEM proved crucial.

8 More on how to use Falcon Next-Gen SIEM to protect against VMware vCenter attacks: How Falcon Next-Gen SIEM Protects Enterprises from VMware vCenter Attacks

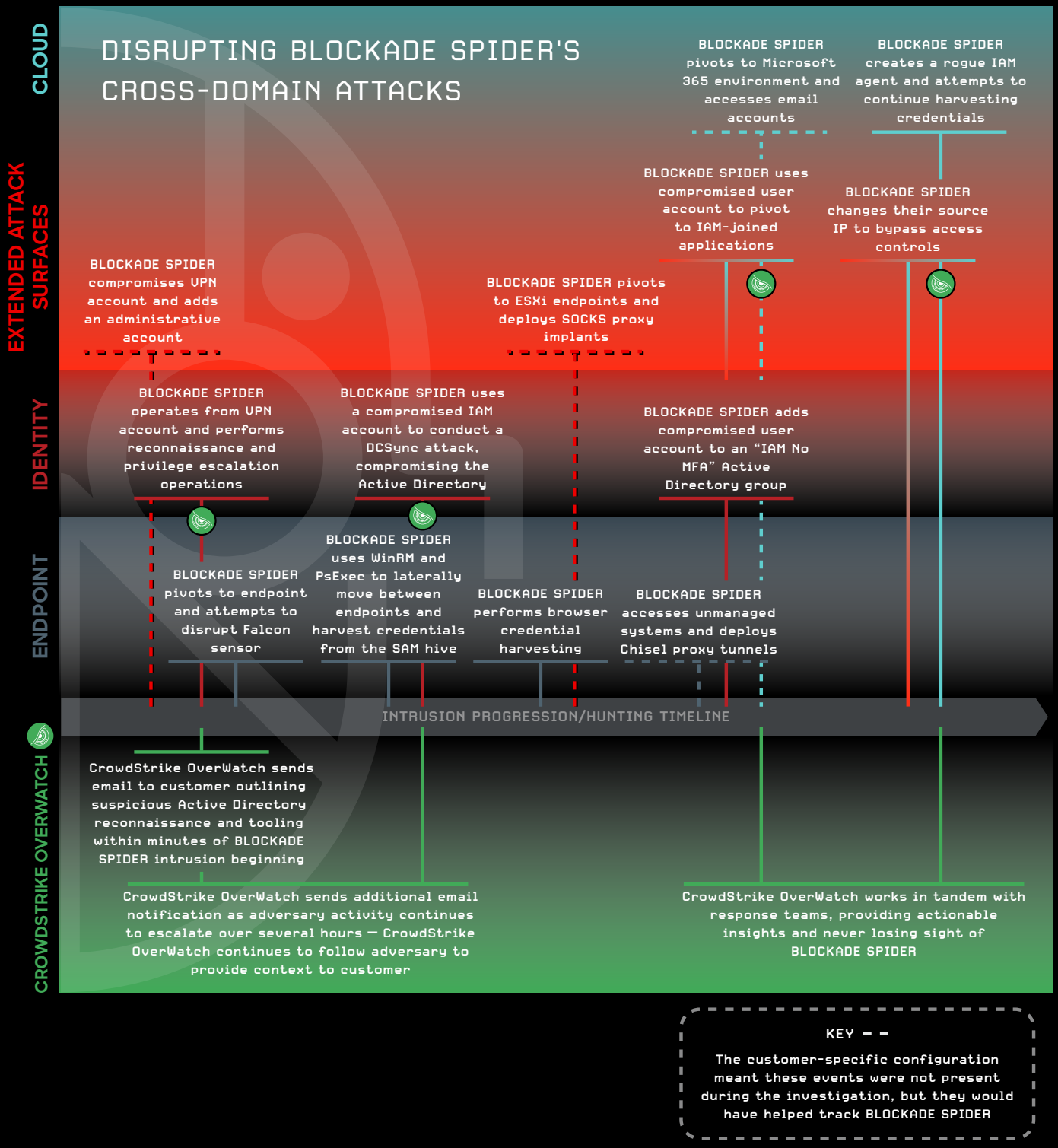
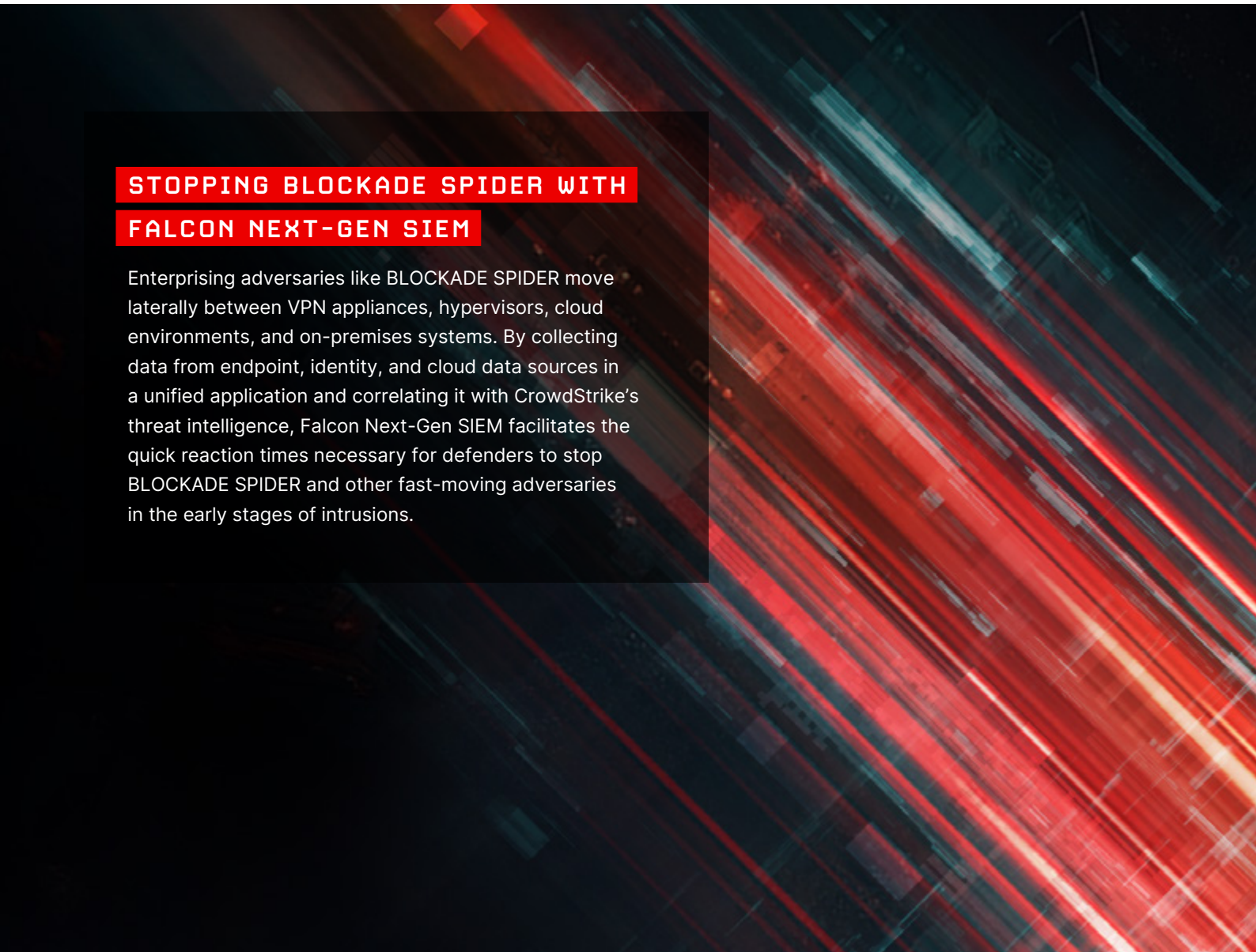


Figure 9. BLOCKADE SPIDER cross-domain attack path

CrowdStrike Falcon® Identity Protection data enabled CrowdStrike OverWatch to trace a VPN service account as the initial source of activity. Using this bastion account, BLOCKADE SPIDER conducted the credential dumping technique DCSync to retrieve further account credentials and began adding compromised accounts to new Active Directory groups. CrowdStrike OverWatch was able to follow this activity through identity data and monitor for further malicious activity using these newly compromised accounts.

By leveraging log data from an identity and access management (IAM) solution ingested into Falcon Next-Gen SIEM, further actionable insights on BLOCKADE SPIDER's interest in Active Directory manipulation quickly became available. CrowdStrike OverWatch threat hunters were also able to continuously follow and alert on the adversary's activities as they pivoted between unmanaged on-premises systems and cloud environments. Finally, threat hunters observed BLOCKADE SPIDER successfully bypass multifactor authentication (MFA) requirements to access the victim's IAM environment and deploy a rogue Active Directory agent.

Despite the adversary embedding themselves deeply in the victim's on-premises and cloud infrastructure, Falcon Next-Gen SIEM data provided threat hunters with the capability to track BLOCKADE SPIDER's activities through various data sources, and the customer was ultimately able to shut down BLOCKADE SPIDER's access to their network.



STOPPING BLOCKADE SPIDER WITH FALCON NEXT-GEN SIEM

Enterprising adversaries like BLOCKADE SPIDER move laterally between VPN appliances, hypervisors, cloud environments, and on-premises systems. By collecting data from endpoint, identity, and cloud data sources in a unified application and correlating it with CrowdStrike's threat intelligence, Falcon Next-Gen SIEM facilitates the quick reaction times necessary for defenders to stop BLOCKADE SPIDER and other fast-moving adversaries in the early stages of intrusions.

CASE STUDY:

Hunting OPERATOR PANDA

To hunt for enterprising adversaries such as China-nexus OPERATOR PANDA, also known as Salt Typhoon, defenders can benefit from correlating data across multiple sources, especially from devices beyond the scope of traditional EDR coverage, such as routers, switches, VPN appliances, and firewalls. OPERATOR PANDA often gains initial access through internet-facing applications, like Cisco switches, which are known blind spots not covered by EDR.

In mid-November 2024, OPERATOR PANDA targeted a U.S.-based telecommunications entity and a U.S.-based consulting and professional services entity. During both intrusions, the adversary gained initial access by exploiting Cisco switches running Cisco IOS and Cisco IOS XE, widely used software for Cisco network appliances. To further hinder detection of their activity, OPERATOR PANDA sanitized logs from the Cisco switches they had compromised.

OPERATOR PANDA is also known to chain vulnerabilities to achieve their objectives. For example, they leveraged CVE-2023-20198 to create a local user account, which they then exploited to abuse another vulnerability, CVE-2023-20273, in a different component of the Cisco web UI feature. This allowed the adversary to inject commands with root privileges, enabling them to run arbitrary commands on the device.

The introduction of Falcon Next-Gen SIEM logs and telemetry to the toolkit of CrowdStrike OverWatch hunters allows them to develop new hunting equities to look for anomalous activity on these devices. The added context provided by next-gen SIEM data paints a more detailed, comprehensive picture of adversary activity for threat hunters and has the potential to shift detection forward in the attack timeline.

Outlook

Armed with data from multiple sources ingested into next-gen SIEM tools, threat hunters can identify, track, and disrupt elusive adversaries such as BLOCKADE SPIDER and OPERATOR PANDA, despite their sophisticated hands-on-keyboard tradecraft and minimal endpoint footprint.

Any blind spots constitute critical weaknesses in defensive postures and allow evasive adversaries to avoid detection and stealthily impact victims. Falcon Next-Gen SIEM equips threat hunters with the capability to hunt across these blind spots. Leveraging next-gen SIEM data will be key to defeating sophisticated adversaries in the future.

IDENTITY HUNTING

Vishing and help desk social engineering have continued to play a dominant role in eCrime operations in 2025. Adversaries are bypassing traditional security measures by exploiting human weaknesses, leveraging compromised credentials and social engineering to gain initial access and move laterally within organizations. It is difficult for a single security tool to distinguish between a legitimate employee and an adversary using stolen credentials, leaving organizations vulnerable to identity-driven attacks. The rise of this social engineering trend was identified in the CrowdStrike 2025 Global Threat Report, and in the first half of 2025, vishing attacks have already surpassed the total number seen in 2024. This means that vishing is on track to double last year's volume by the end of 2025.

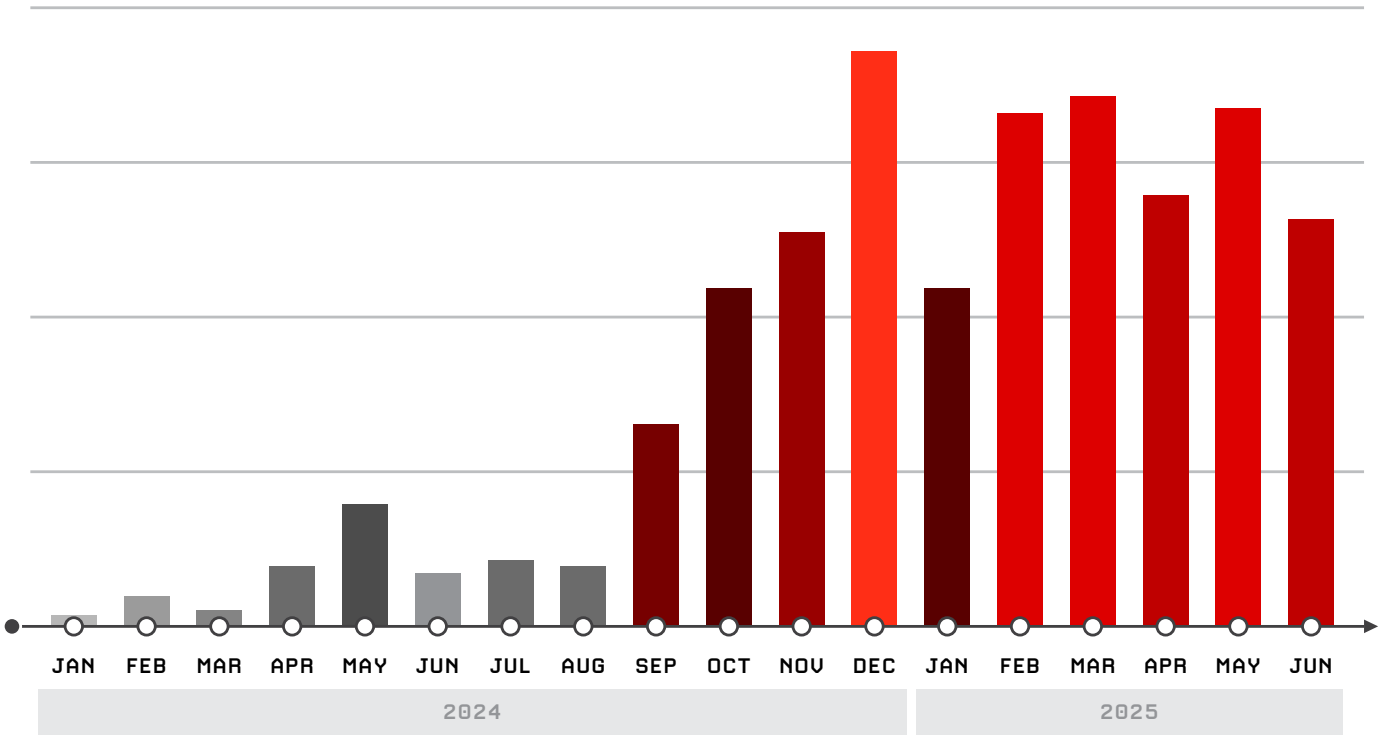


Figure 10. Vishing attacks observed by month, January 2024-June 2025

Identity protection is a force multiplier in countering vishing attacks. By correlating activity across multiple domains — including third-party data for phishing detection with next-gen SIEM capabilities — organizations can uncover suspicious behaviors indicative of compromise. Proactive, intel-driven threat hunting across domains aids rapid detection and disruption of adversary activity before it escalates.

ADVERSARY SPOTLIGHT:

SCATTERED SPIDER

Following a period of relative inactivity between December 2024 and March 2025, SCATTERED SPIDER returned in April 2025 with aggressive ransomware campaigns targeting the U.K. and U.S. aviation, insurance, and retail sectors. In most 2025 incidents to date, the adversary has leveraged help desk social engineering to gain initial access, a technique they first used in 2023 and have since matured, leading to its widespread adoption by multiple distinct eCrime actors.

In help desk social engineering, a threat actor impersonates a legitimate employee in a call to a targeted organization's help desk and requests a password and/or MFA method reset. Once the SCATTERED SPIDER caller has passed identity verification questions, the help desk agent provides a temporary password over the phone and/or revokes the existing MFA device or method, enabling the adversary to authenticate and configure their own device for MFA. SCATTERED SPIDER typically uses help desk social engineering to compromise Microsoft Entra ID, single sign-on (SSO), and virtual desktop infrastructure accounts.

During these calls, SCATTERED SPIDER has impersonated targeted organizations' legitimate employees and accurately provided the impersonated individuals' employee IDs in response to the help desks' identity verification questions. SCATTERED SPIDER and other eCrime actors have also routinely demonstrated the ability to acquire personally identifiable information to pass help desk verification questions. In one call where the adversary could not provide the impersonated employee's ID, the threat actor offered to provide the employee's date of birth and Social Security number as alternative verification credentials.

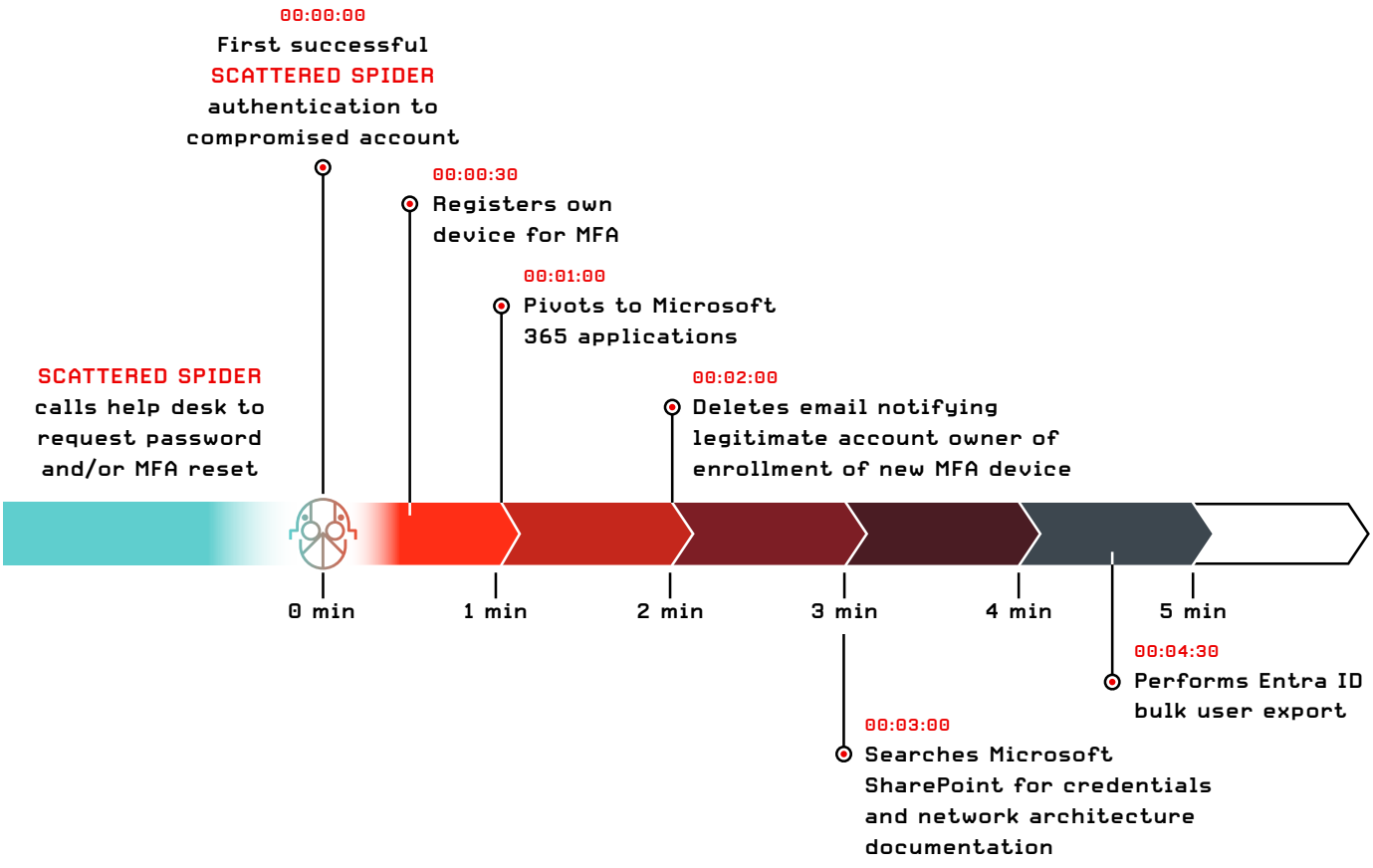


Figure 11. Timeline of SCATTERED SPIDER social engineering attack

Within minutes of performing the account takeover, SCATTERED SPIDER operators can often be observed leveraging these accounts to pivot to integrated software as a service (SaaS) applications, including data warehousing, document management and storage, and IAM platforms. These serve as a foothold for persistence, lateral movement, and data exfiltration techniques.

SCATTERED SPIDER often compromises accounts belonging to targeted organizations' IT and security staff, as these employees typically have access to documentation on network architecture, security tooling, and incident response procedures. The adversary has also targeted C-suite executives' accounts, likely due to their access to sensitive data, communications, and other resources that may support data theft and extortion.

When SCATTERED SPIDER logs in to compromised accounts, they often configure residential proxies (such as NSOCKS) to appear as though they are logging in from the same geographical area and with the same user agent as the legitimate account owner. The adversary also often compromises accounts outside of typical local business hours, likely to enable the longest possible access to the account before the legitimate user reports being locked out.

Account Takeover to Ransomware in 24 Hours

SCATTERED SPIDER continues to pursue ransomware deployment and data theft and extortion as monetization methods in 2025. In one 2025 incident in which SCATTERED SPIDER deployed ransomware, the adversary progressed from initial access to encryption in approximately 24 hours. This progression is significantly quicker than the adversary's average time between their first interaction with victims and either ransomware execution or adversary eviction in 2024 and 2023 — approximately 35.5 hours and 85 hours, respectively.

The adversary excels at using identity compromise to pivot between multiple surfaces in a network, evading targeted organizations' heavily monitored endpoints. This includes performing bulk exports of Entra ID data, obtaining credentials from privileged access management (PAM) applications, and even performing help desk social engineering calls during the intrusion to gain access to accounts with higher privileges. In one technique seen in most SCATTERED SPIDER intrusions, the adversary attaches domain controller virtual machine (VM) hard disks to unmanaged adversary-controlled VMs to dump `ntds.dit` without being detected by host-based security tooling.

Countering SCATTERED SPIDER

Countering SCATTERED SPIDER requires a multi-domain approach to threat hunting, as the adversary minimizes time spent on endpoints. Though compromising identities is SCATTERED SPIDER's preferred method of initial access, examining identity data is only part of the overall puzzle that threat hunters must consider.

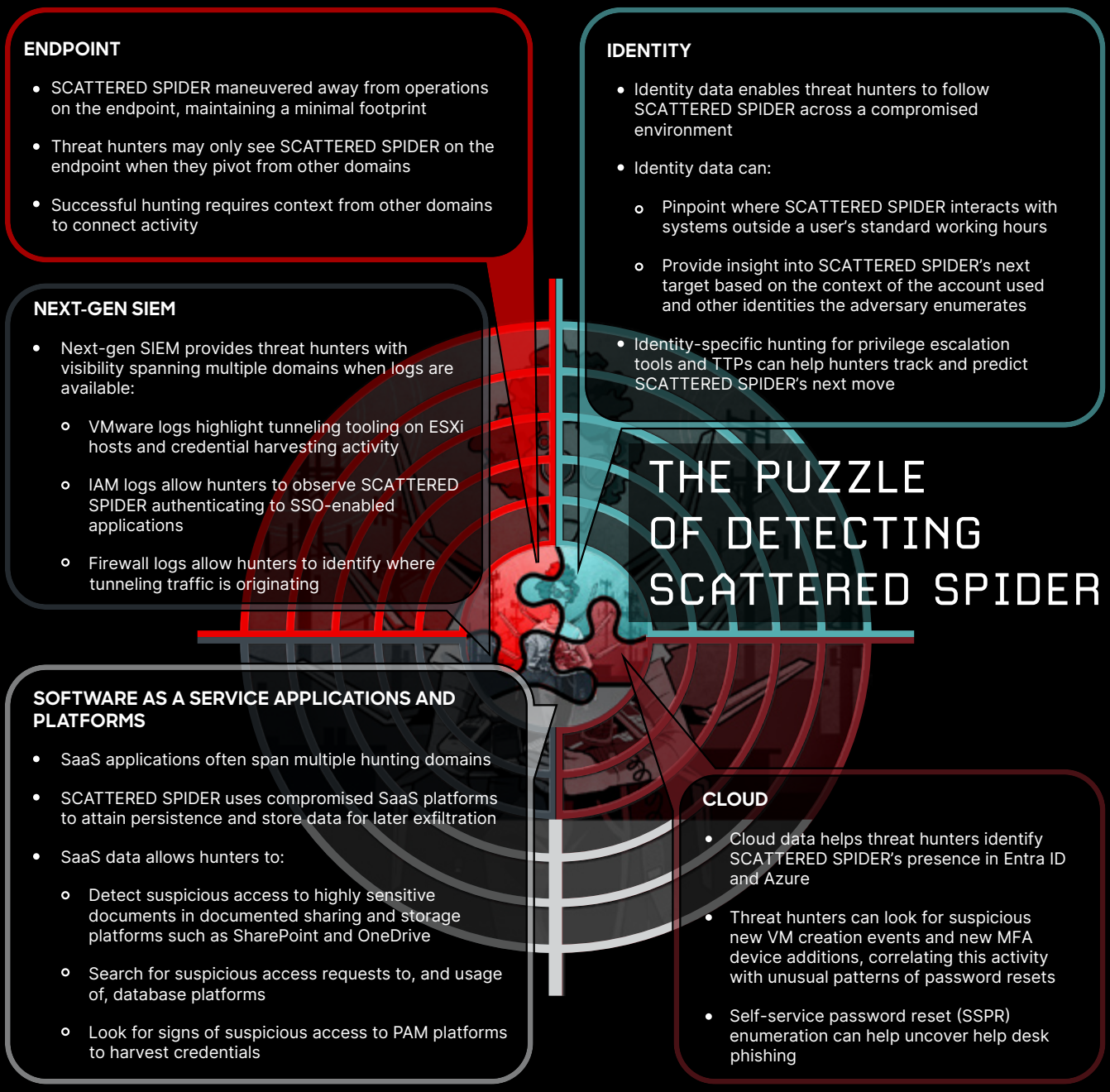


Figure 12. Hunting SCATTERED SPIDER across domains

To defend against adversaries like SCATTERED SPIDER, organizations should adopt the following proactive measures:

- **Identity Protection:** Use phishing-resistant MFA (avoiding SMS-based methods), isolate privileged accounts from regular workflows, strengthen password reset procedures, and restrict help desk involvement in MFA enrollment.
- **Detection and Monitoring:** Continuously monitor for authentication anomalies, administrative changes, and unusual network traffic to critical systems; enable comprehensive logging and behavioral analytics; and watch for suspicious application usage, search terms, and data access patterns that could indicate malicious activity.
- **Infrastructure Security:** Secure VMware environments, segment networks to contain potential intrusions, block the use of unauthorized tools, apply least-privilege access across cloud environments, and disable outdated or legacy authentication methods.
- **Incident Readiness:** Maintain isolated and regularly tested backups, develop and rehearse incident response playbooks, perform regular readiness assessments, and train IT and help desk teams to recognize and respond to social engineering tactics.

Outlook

When it comes to identities compromised by vishing, providing threat hunters with as much information regarding the characteristics of an account up front is a necessity. Rapidly ascertaining key details — such as when an account password was last reset, what privileges and groups an account has access to, and an account's MFA status — provides vital context to threat hunters assessing whether activity is likely malicious.

As enterprising adversaries like SCATTERED SPIDER expand their attacks beyond the endpoint, technologies like identity protection and next-gen SIEM become essential. Modern threat hunting requires analysts who are able to pivot between data sources as quickly as the adversary is able to pivot during an intrusion.

CLOUD HUNTING

The CrowdStrike 2025 Global Threat Report identified that China's cyber espionage capabilities reached a critical inflection point over the past year, marked by increasingly bold targeting, stealthier tactics, and expanded operational capacity. In 2024, China-nexus threat actors employed the ORB07 operational relay box (ORB) network[9] to conduct password spraying attacks against Microsoft Azure accounts. The network, which consists of thousands of nodes, is likely used by multiple China-nexus adversaries for the sole purpose of targeting Azure accounts, highlighting a newfound emphasis on cloud exploitation operations.

Over the past 12 months, CrowdStrike OverWatch observed a 40% increase in cloud intrusions associated with China-nexus adversaries. This increase suggests cloud exploitation continues to be a key focus for these adversaries. The cloud's vast data, scalability, and exploitable misconfigurations enable adversaries to achieve persistence, move laterally, and exfiltrate data.

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

Two China-nexus adversaries — GENESIS PANDA and MURKY PANDA — have proven to be particularly adept at navigating cloud environments over the past year, each showcasing different techniques that require different hunting strategies. GENESIS PANDA conducts high-volume operations with less emphasis on operational security and a suspected role as an access broker. MURKY PANDA is a more sophisticated and elusive adversary prioritizing evasion techniques in the cloud and using trusted relationships for initial access. Figure 13 compares these adversaries' most prevalent TTPs.

CROWDSTRIKE OVERWATCH: 2025 CLOUD HUNTING BY THE NUMBERS

- Leveraging CrowdStrike Falcon® Cloud Security telemetry, CrowdStrike OverWatch identified a 136% increase in cloud intrusions in the first half of 2025 compared to all of 2024
- Over the past 12 months, CrowdStrike OverWatch observed a 40% increase in cloud-conscious intrusions by suspected China-nexus actors

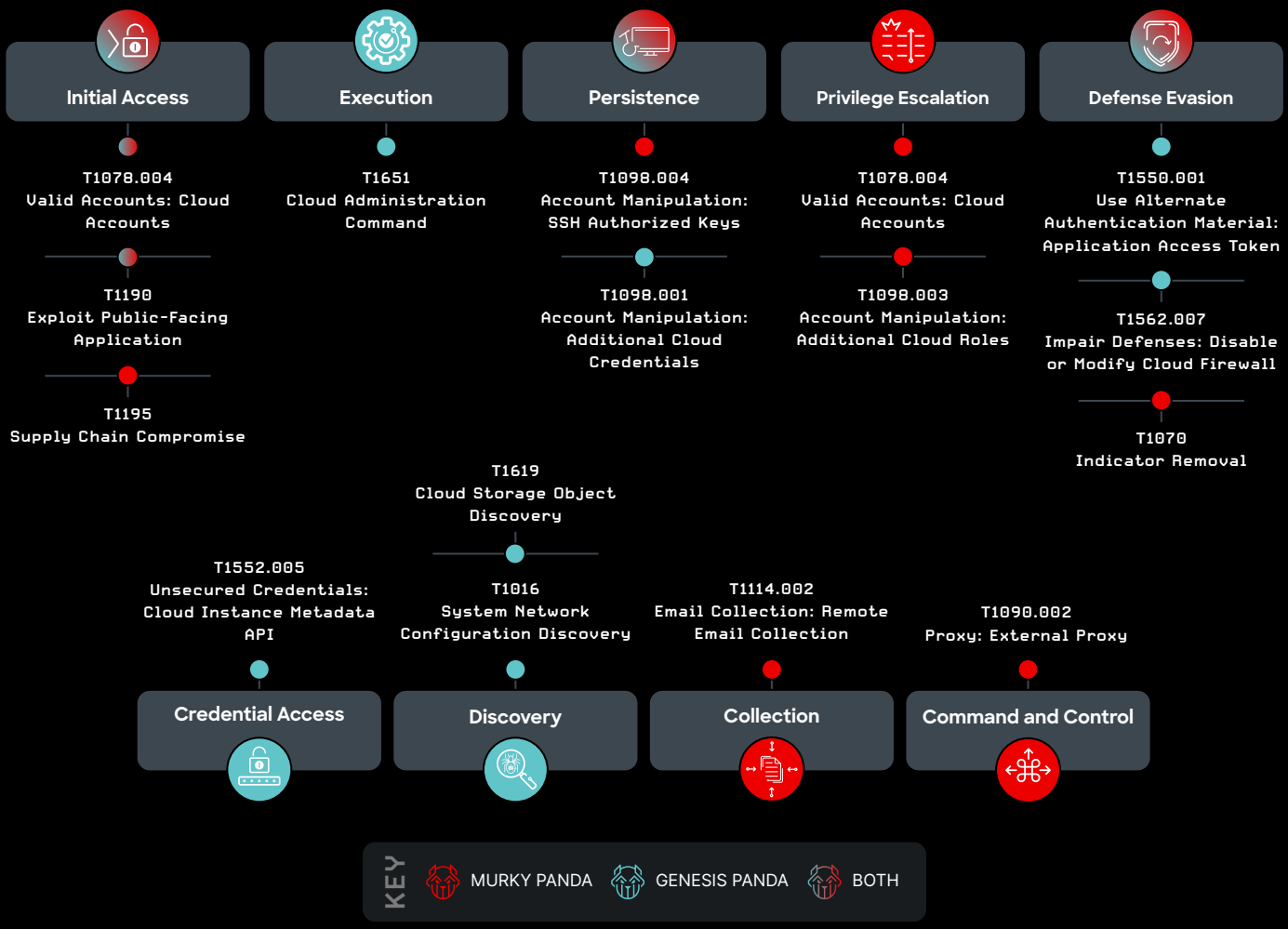


Figure 13. Prevalent MITRE ATT&CK TTPs used by MURKY PANDA and GENESIS PANDA

CASE STUDY:

Hunting GENESIS PANDA Across the Cloud Control Plane

Adversary Profile

GENESIS PANDA targets a wide variety of sectors — including financial services, media, telecommunications, and technology — in at least 11 countries. The adversary likely serves as an initial access broker to facilitate future intelligence collection. This assessment is made with moderate confidence based on the volume of activity the adversary conducted, their exploitation of a wide range of web-facing vulnerabilities, limited observation of data exfiltration, and TTP overlaps with penetration testing-type activity.

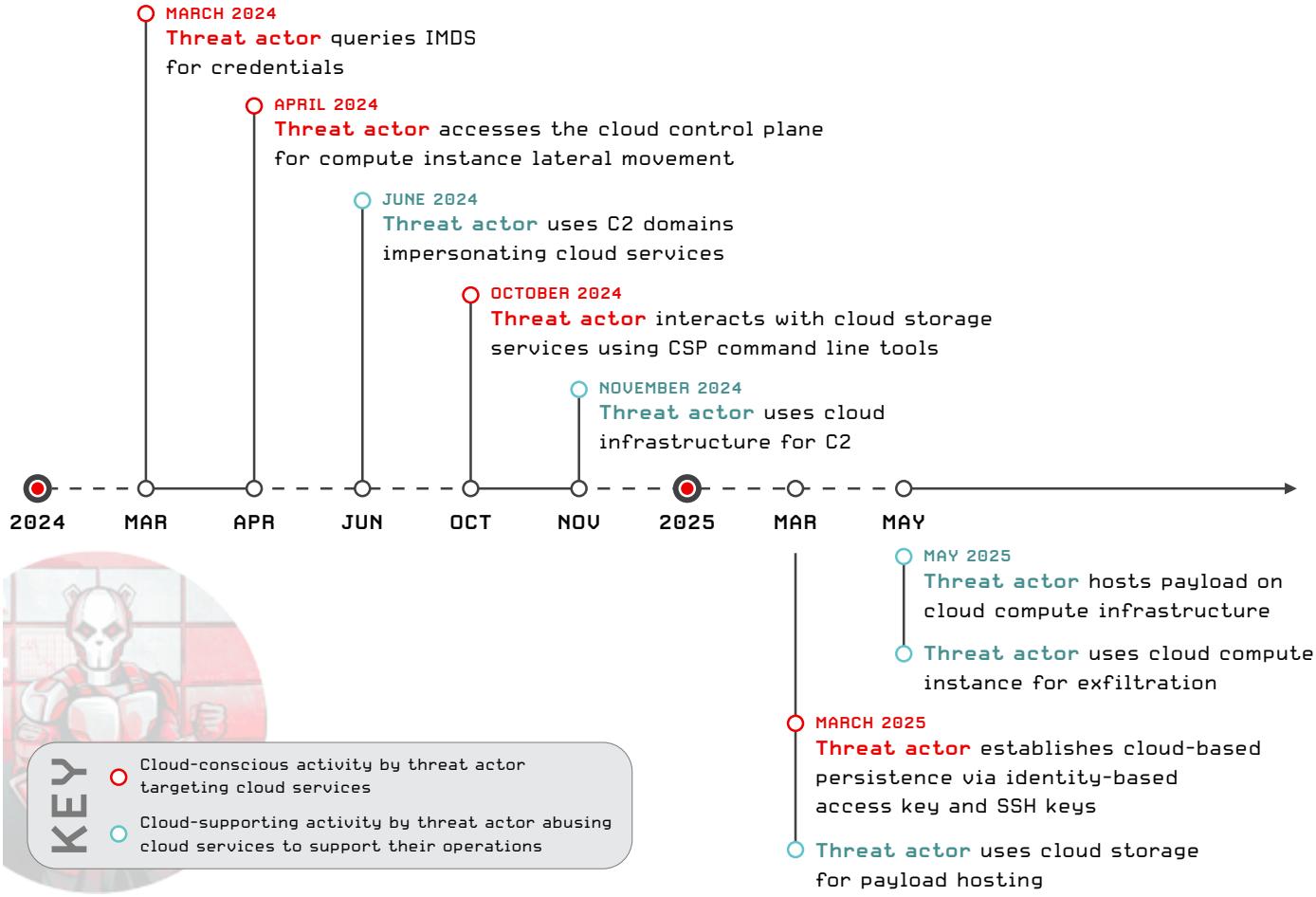


Figure 14. GENESIS PANDA: Weaponizing the cloud control plane

Since at least March 2024, GENESIS PANDA has proven increasingly capable of using cloud services to support tool deployment, command and control (C2) communications, and exfiltration. The adversary has also proven capable of targeting cloud service provider (CSP) accounts to expand access and establish alternate forms of persistence. In addition to hosting data on cloud services, GENESIS PANDA uses cloud infrastructure to exfiltrate the output of basic discovery commands.

GENESIS PANDA's use of CSPs to support operations underscores the adversary's knowledge of cloud administration and ability to move laterally in target environments. Despite their knowledge of cloud environments, the adversary has not been observed exfiltrating contents from S3 buckets, further reinforcing the likelihood that they serve as an initial access broker.

Although GENESIS PANDA targets a variety of systems, they show consistent interest in compromising cloud-hosted systems to leverage the cloud control plane for lateral movement, persistence, and enumeration.

Cloud Service Enumeration

When compromising a cloud-hosted server, GENESIS PANDA consistently queries the associated Instance Metadata Service (IMDS) primarily to obtain credentials for the cloud control plane but also to enumerate network and general instance configurations. GENESIS PANDA occasionally uses CSP command line tools, likely in conjunction with cached credentials on compromised VMs.

In October 2024, CrowdStrike OverWatch identified hands-on-keyboard activity from a GENESIS PANDA implant running on a cloud compute instance. The threat actor may have used this information in preparation for lateral movement, as soon after, they began to ping and SSH to other internal hosts. On multiple occasions, the adversary demonstrated an interest in cloud storage service enumeration.

Pivoting to the Cloud Control Plane

GENESIS PANDA often uses credentials — likely obtained from compromised VMs — to pivot to the target organization's cloud account. Pivoting to the cloud control plane grants the adversary access to run commands on other cloud-hosted VMs. During multiple intrusions, GENESIS PANDA gained access to the target organization's cloud service account, added local users to various VMs, performed host-based enumeration, and deployed malware.

GENESIS PANDA also uses the access provided by the cloud control plane to establish various forms of persistence. In early March 2025, CrowdStrike OverWatch identified an intrusion in which GENESIS PANDA obtained credentials to the target organization's cloud provider account by querying the IMDS after exploiting a public-facing Jenkins server. The adversary then added SSH keys and created a backdoor access key on the cloud service account. GENESIS PANDA later returned using the backdoor access key in conjunction with a likely custom .NET-based tool to regain access to the cloud service console. This intrusion illustrates the adversary's desire to establish persistence at multiple layers of the target organization and their ability to use custom tooling for cloud-based targeting.

CASE STUDY:

MURKY PANDA's Abuse of Trusted Relationships

Adversary Profile

MURKY PANDA targets various entities in North America, displaying a particular interest in targeting cloud environments through trusted relationships between partner organizations and their cloud tenants. The adversary almost certainly has advanced capabilities, including access to low-prevalence malware such as *CloudedHope*, and the expertise to quickly weaponize n-day and zero-day vulnerabilities. MURKY PANDA demonstrates a high level of operations security by deleting indicators of their presence on victim environments, targeting edge devices for initial access, exploiting n-day or zero-day vulnerabilities, and leveraging trusted relationship compromises. Similar to other China-nexus adversaries, MURKY PANDA relies heavily on exploiting internet-facing appliances for initial access.

Trusted Relationship Abuse

In late 2024, CrowdStrike Services responded to an incident in which MURKY PANDA very likely compromised a supplier of a North American entity and used the supplier's administrative access to the victim entity's Entra ID tenant to add a temporary backdoor Entra ID account. Using this account, the threat actor then backdoored several preexisting Entra ID service principles related to Active Directory management and emails. The adversary's goals appear targeted in nature based on their focus on accessing emails.

In early 2025, CrowdStrike Services responded to another MURKY PANDA intrusion in the environment of a customer of a third-party application for Entra ID. During this intrusion, MURKY PANDA almost certainly compromised this application to access victim emails as part of a trusted relationship compromise. CrowdStrike OverWatch data indicates that service principal sign-ins for the application typically originate from Microsoft Azure-associated IP addresses. However, during the intrusion, service principal sign-ins also originated from a likely compromised network-attached storage (NAS) device and a virtual private server (VPS).

On March 7, 2025, the application vendor disclosed that they had been notified on February 20, 2025, that a threat actor had exploited the vulnerability as a zero-day and conducted unauthorized activity within the vendor's Azure environment, corroborating CrowdStrike Services' findings.

Outlook

China-nexus adversaries are becoming increasingly skillful at exploiting and navigating cloud environments. They use specialized techniques and tools to support their operations. As these adversaries are likely to continue to focus on cloud exploitation operations, with attacks growing in scale and sophistication, understanding the differing techniques used by adversaries like GENESIS PANDA and MURKY PANDA is crucial. This understanding will enable the necessary adjustments to defense and hunting strategies.

ENDPOINT HUNTING

Though fast-moving adversaries often dominate the threat landscape, equally dangerous threats operate on extended timelines. These patient predators prioritize stealth and persistence, executing meticulous "long game" strategies that include sustained access, covert data harvesting, and environmental preparation for future operations. Their minimal digital footprint allows them to blend seamlessly into legitimate network traffic, making detection exceptionally challenging.

China-nexus adversaries have increasingly mastered this approach. This is particularly evident in their increased targeting of the telecommunications sector. CrowdStrike OverWatch observed a 130% increase in nation-state activity against the telecommunications sector over the past 12 months. This high-value sector offers significant intelligence value, making telecommunications entities prime targets for stealthy actors. The sector is similarly valuable to threat hunters, as focused hunting efforts at telecommunications entities can often uncover new adversaries and TTPs.

CrowdStrike OverWatch threat hunters routinely identify multiple threat actors conducting concurrent operations on the same target network, particularly at telecommunications entities. Threat actors who conduct long-term intelligence collection operations in specialized telecommunications environments often share several high-level TTPs. Deep knowledge of threat actors' characteristic behaviors can enable threat hunters to separate and track these threat actors' activities, leading to new insights.

GLACIAL PANDA — a China-nexus adversary dominating the telecommunications industry — represents such an insight. After extensive proactive hunting efforts by CrowdStrike OverWatch, CrowdStrike Intelligence introduced GLACIAL PANDA as the latest China-nexus adversary to specialize in this "long game" approach to intelligence collection operations targeting telecommunications entities. In uncovering yet another China-nexus threat actor targeting the space, the CrowdStrike OverWatch team further demonstrated its skill in quickly and efficiently hunting these enterprising adversaries.

CASE STUDY:

Hunting GLACIAL PANDA Living off the Land

GLACIAL PANDA highly likely conducts targeted intrusions for intelligence collection purposes, accessing and exfiltrating call detail records and related communications telemetry from multiple telecommunications organizations. This activity could have significant privacy implications for the organizations' customers. The adversary primarily targets Linux systems typical in the telecommunications industry, including legacy operating system distributions that support older telecommunications technologies.

GLACIAL PANDA

Notable TTPs

- Initial access via internet-facing (and frequently unmanaged) servers, likely achieved through software exploitation or weak password provisioning
- Primarily targets Linux systems, employing LOTL techniques and abusing legitimate user accounts for lateral movement and persistence
- Deploys *ShieldSlide* trojanized OpenSSH components to collect user authentication sessions and credentials
- Collects telecom sector-specific data, including call detail records, network telemetry, and error logs

Vulnerabilities Exploited

- CVE-2016-5195 vulnerability (aka Dirty COW)
- CVE-2021-4034 vulnerability (aka PwnKit)

Target Sectors

- Telecommunications

Target Geography

- Afghanistan
- Hong Kong
- India
- Japan
- Kenya
- Malaysia
- Mexico
- Panama
- Philippines
- Taiwan
- Thailand
- U.S.

Figure 15. GLACIAL PANDA: TTPs and targets

GLACIAL PANDA activity is characterized by interactive intrusion tradecraft that prioritizes persistence and stealth. This adversary is known to use:

- Living off the land (LOTL) techniques that leverage common Linux system tools
- Legitimate user account abuse for initial host access and lateral movement
- Trojanized OpenSSH suite tools to capture user credentials and provide backdoor access
- Trojanized cron daemons to hide adversary-configured jobs
- External C2 via reverse shell connections using netcat or a publicly available Perl script
- Access propagation between interconnected organizations, such as company subsidiaries or business relationships

Interactive intrusions involve human operators controlling systems in real time and adapting procedures according to their objectives and the current network environment. In the telecommunications industry, legacy systems that support older technologies can provide a beachhead, where adversaries can establish persistence while planning subsequent stages of their intrusion. Adversaries may spend only a short time interacting with core systems. This type of activity requires advanced threat hunting capabilities to identify and mitigate.

CrowdStrike OverWatch uses multiple hunting strategies to identify GLACIAL PANDA's illegitimate actions among normal user and administrative activities, necessitated by the adversary's minimal malware footprint and legitimate account abuse. Low-prevalence binary hunting patterns uncover trojanized software and malicious code. These binary hunting patterns can focus on the hex representation of compiled code residing in memory in trojanized applications. Additionally, threat hunters' deep understanding of the adversary's characteristic command line preferences and process invocations can locate malicious hands-on-keyboard activity among normal user sessions. Behavioral patterns identifying repeated access to sensitive data sources on Linux hosts have also proven highly successful in identifying GLACIAL PANDA's aggressive and repetitive host reconnaissance and data collection procedures.

CrowdStrike OverWatch can also take advantage of the Falcon platform's broad visibility to identify attempted connections between separate customer networks and provide early warning of adversary activity.

ShieldSlide: Credential Harvesting and Backdoor Access via Trojanized OpenSSH Binaries

GLACIAL PANDA deploys trojanized OpenSSH tools on compromised Linux hosts to log user authentication events and support lateral movement by tracking remote connections to other hosts. Though several other adversaries also modify OpenSSH components, code overlaps across variants are sufficient to attribute GLACIAL PANDA's tooling. This capability is collectively dubbed *ShieldSlide*.

ShieldSlide binaries are almost identical to legitimate OpenSSH components, except for a small modification to the source code that logs victim credentials. The *ShieldSlide*-trojanized SSH server binary also provides backdoor access, authenticating any account (including root) when a hardcoded password is entered.

Despite *ShieldSlide* being functionally equivalent to its legitimate counterparts, CrowdStrike OverWatch routinely identifies maliciously modified system services using low-prevalence binary hunting techniques, alerting customers that user accounts on their network are at risk of being compromised.

To hunt for and protect against threats like GLACIAL PANDA, CrowdStrike recommends the following measures:

- **Update software** on supported operating systems regularly by employing rigorous patch management policies, and migrate end-of-life (EOL) systems to versions with vendor update support wherever possible.
- **Monitor legacy or EOL assets** that no longer receive security or software updates, particularly for unusual network activity to and from these hosts.
- **Monitor legitimate system binaries** for malicious modifications, including `/usr/bin/ssh`, `/usr/sbin/sshd`, `/usr/sbin/cron`, and OpenSSH pluggable authentication modules.
- **Monitor SSH connections** between hosts for anomalous activity, limiting which user accounts are allowed to log in via SSH.
- **Enforce network access control policies** for servers according to role and requirement.
- **Enforce complex account password strategies** — avoiding default or generic options — for SSH authentication, and employ more secure methods such as SSH key authentication, particularly on remotely accessible servers. Limit situations in which server credentials (e.g., for databases) are stored unencrypted on hosts.
- **Deploy** CrowdStrike Falcon® Insight XDR on compatible hosts, ensuring maximum network environment coverage.

VULNERABILITY HUNTING

The CrowdStrike 2025 Global Threat Report revealed that 52% of vulnerabilities observed by CrowdStrike in 2024 were related to initial access, with exploitation of internet-exposed applications remaining a prevalent initial access method. Effective exposure and vulnerability management is crucial in addressing the worst-case scenario: zero-day vulnerability exploitation.

In critical vulnerability situations, a defense-in-depth strategy is essential. Integrating CrowdStrike OverWatch's threat hunting capabilities with exposure management tools and solutions can provide a vital backstop, mitigating damage during the crucial period before a patch is released. When adversaries such as GRACEFUL SPIDER develop and deploy zero-day exploits to bypass existing patches, CrowdStrike OverWatch's ability to identify and hunt for post-exploitation malicious behaviors acts as a critical fail-safe, ensuring rapid and effective coverage against subsequent widespread exploitation by opportunistic adversaries.

CASE STUDY:

Hunting GRACEFUL SPIDER's Zero-Day

A series of incidents impacting Cleo data transfer products in late 2024 highlights the intersection of detection deployment and development, exposure management, extended detection and response (XDR), threat hunting, and threat intelligence. On Saturday, December 7, 2024, CrowdStrike OverWatch detected suspected exploitation of multiple Cleo products on Windows and Linux servers. The team observed compromises across Cleo instances in multiple sectors and geographies. Based on the targets, speed, scope, and tactics demonstrated by the threat actor during the initial wave, CrowdStrike Intelligence determined the activity was likely a zero-day file upload exploit leading to remote code execution related to an earlier vulnerability.

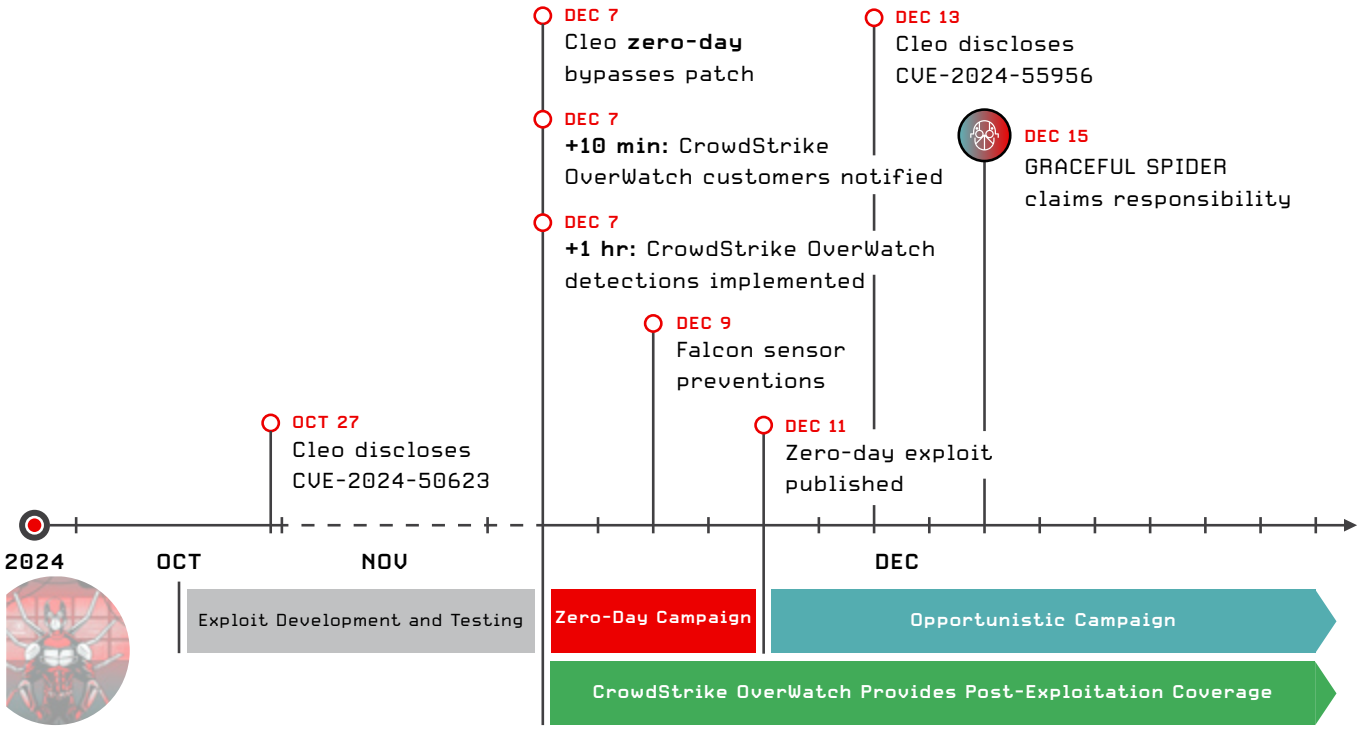


Figure 16. Uncovering a zero-day: A day-by-day breakdown of adversary activity

Criminal enterprises often capitalize on weekends to maximize impact — but so does CrowdStrike OverWatch. Rapidly after the initial detection of Cleo exploitation, CrowdStrike OverWatch alerted affected customers and deployed hunting patterns to identify malicious files being written to significant directories, providing a baseline for early-stage detection coverage for all CrowdStrike OverWatch customers.

CrowdStrike OverWatch telemetry confirmed malicious activity began with the creation of a malicious ZIP archive file in a `temp` directory corresponding to the specific Cleo product (e.g., `C:\VLTrader\temp\`) in Microsoft Windows environments. The attacker then wrote a file to the `autorun` directory that imported the ZIP file, executing the attacker command. When the ZIP file was imported, a malicious host definition XML file was extracted and evaluated. This XML file defined a host structure with specific properties and included a mailbox configured to execute a system command.

The CrowdStrike Falcon sensor prevented further malicious post-exploitation behaviors on compromised Cleo servers, which included process injection and PowerShell execution. CrowdStrike Intelligence confirmed the commands attempted to execute multiple obfuscated shellcode stages, culminating in the download and execution of a high-prevalence, pirated version of Cobalt Strike. These tactics, as well as the targeting of Cleo managed file transfer (MFT) applications, were consistent with eCrime activity in general and BGH specifically. GRACEFUL SPIDER later claimed responsibility for the initial wave of December activities targeting Cleo on their dedicated leak site (Figure 16).

Exploit proliferation then enabled subsequent waves of exploitation. On December 11, 2024, offensive security researchers posted a functional CVE-2024-55956 exploit and a detailed technical description of the vulnerability. Opportunistic actors rapidly adopted the exploit, and CrowdStrike Intelligence subsequently observed numerous attempts to exploit the vulnerability, with slight formatting variations, on the same day.

However, by this time, CrowdStrike OverWatch and the Falcon sensor could fully backstop Cleo products against further compromise by other threat actors. By December 9, 2025, CrowdStrike OverWatch — together with the CrowdStrike sensor team — had successfully implemented measures to detect and prevent Cleo post-exploitation activity within the CrowdStrike Falcon sensor.

Patch Circumvention Enables Zero-Day Enterprise

The December 2024 CVE-2024-55956 Cleo zero-day campaigns bypassed patch fixes for the previously disclosed file upload vulnerability CVE-2024-50623. Though CVE-2024-50623 and CVE-2024-55956 are distinct vulnerabilities, they share the same fundamental root causes and exploit improper validation of input to the `/Synchronization` endpoint. This endpoint is meant to be inaccessible but could be reached by forging a fake license number. Exploitation of this vulnerability allows arbitrary file reads and writes on the targeted instance server, with the opportunity to pivot into remote code/command execution.

The initial CVE-2024-50623 patch addressed, in part, the file path validation issue but did not mitigate the improper validation bug allowing actors to forge a fake license number. Resourceful threat actors such as GRACEFUL SPIDER realized the initial path validation fixes could be bypassed and once again abused the unmitigated license forgery issue to achieve remote code execution via CVE-2024-55956.

To hunt for and protect against threats from emerging exploit campaigns, CrowdStrike recommends the following measures:

- **Deploy** EDR/XDR capabilities on compatible hosts to ensure maximum visibility and coverage across the network environment.
- **Inventory** and review enterprise assets to ensure visibility across the organization.
- **Identify** vulnerable assets through continuous exposure assessment and vulnerability scanning.
- **Monitor** externally exposed assets for signs of risk or potential compromise.
- **Update software** by using intelligence-driven patch management policies that prioritize exposed assets with known exploited vulnerabilities.
- **Enforce script execution policies** on supported platforms to block PowerShell and other script-based activity on hosts where it is not required.

Hunting for GRACEFUL SPIDER's Zero-Day Campaign Artifacts

Efforts by CrowdStrike OverWatch ensured that malicious activity and detections led to customer notifications within hours and Falcon sensor prevention measures could be rolled out within days. When threat actors compromise internet-exposed services to achieve remote code execution, CrowdStrike telemetry is capable of capturing the resulting anomalous file, network, and process activities. During this Cleo exploitation campaign, CrowdStrike OverWatch leveraged Falcon Next-Gen SIEM extensively to hunt for both campaign-specific indicators and generic intrusion artifacts across sensor telemetry.

Hunting for exploited software requires an understanding of the environment to formulate baselines in the monitored network. Though the following example is designed for CrowdStrike customers, as it leverages the CrowdStrike Query Language (CQL), it demonstrates concepts that are broadly applicable to all threat hunters. It demonstrates how to monitor potentially vulnerable processes against identified baselines to detect suspicious artifacts that may be indicative of ongoing exploitation activity.

```
[ // detect uncommon process rollups
#event_simpleName=ProcessRollup2

// replace the <process_filename> placeholder with the file name of the investigated
process, e.g., java.exe
ParentBaseFileName=<process_filename>

// regex to defeat known goods
// replace <expected_command_x> in accordance with baselines in your environment
CommandLine!=/<expected_command_1>|<expected_command_2>|<...>|<expected_command_n>/
]

OR [ // detect uncommon file write operations
#event_simpleName=/^(ELFFileWritten|PeFileWritten|NewScriptWritten)$/

// replace the <process_filename> placeholder with the file name of the investigated
process, e.g., java.exe
ContextBaseFileName=<process_filename>

// regex to defeat known goods
// replace <expected_filename_x> in accordance with baselines in your environment
TargetFileName!=/<expected_filename_1>|<expected_filename_2>|<...>|<expected_filename_n>/
]

// this formats the results in a user-friendly way
| case{
CommandLine=* | artifact:=CommandLine;
TargetFileName=* | artifact:=TargetFileName;
}
| table([@timestamp, #event_simpleName, aid, ComputerName, artifact])
```

Figure 17. Example CQL query: Monitoring potentially vulnerable processes

Conclusion

The past year marked a defining chapter in the evolution of threat hunting. From the rapid rise of cross-domain intrusions and identity-based attacks to the growing weaponization of GenAI and targeting of cloud infrastructure, adversaries have demonstrated their ability to innovate, adapt, and scale operations with speed. Whether motivated by financial gain, espionage, or long-term access, enterprising adversaries are exploiting complexity, leveraging trusted relationships, and moving beyond traditional attack surfaces to evade detection.

CrowdStrike OverWatch threat hunters have revealed how adversaries no longer operate in silos. They navigate across the identity, endpoint, and cloud domains, using hands-on-keyboard tradecraft that challenges traditional security tools. Defenders are rising to meet the challenge with faster detection, deeper context, and coordinated defense rooted in intelligence.

This report underscores that proactive, intelligence-driven hunting is essential. Security teams must integrate telemetry across the enterprise, operationalize threat intelligence, and use automation to extend human capability. It is not enough to respond; defenders must anticipate, pivot, and relentlessly pursue the adversary.

As adversaries sharpen their capabilities, the CrowdStrike Counter Adversary Operations team remains resolute in detecting and disrupting the world's most sophisticated threat actors. This commitment ensures that wherever the adversary goes, the team is already there.

Recommendations

1 Adopt AI-powered solutions to scale security operations

As threat actors adopt AI to strike faster, scale operations, and evade detection, defenders face mounting pressure to keep pace. Security teams are already stretched thin, grappling with growing alerts, contending with skills shortages, and racing to respond at speed. To close these widening gaps, security teams should operationalize agentic AI, systems capable of reasoning, adapting, and acting autonomously within defined guardrails and organizational policies. These capabilities can scale intelligence-driven operations by using emerging threat intelligence and expertise to triage alerts, conduct investigations, and execute response actions. By offloading time-intensive, repetitive tasks, agentic AI empowers human analysts to focus on proactive threat hunting and hypothesis-driven investigation, elevating both strategic impact and operational efficiency.

2 Secure the entire identity ecosystem

Adversaries increasingly target identities using credential theft, MFA bypass, and social engineering while moving laterally between on-premises, cloud, and SaaS environments via trusted relationships. This allows them to impersonate legitimate users, escalate privileges, 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, and 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.

3 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 legacy 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-gen 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. Agentic AI-powered triage and investigations can extend these capabilities, autonomously analyzing signals across domains to surface high-fidelity insights and prioritize real threats.

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

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.

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 proof-of-concept (POC) exploits and technical blogs, enabling adversaries to craft effective and hard-to-detect payloads.

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

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

Know the 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 GenAI 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 their 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

Prevents advanced threats like ransomware and fileless attacks with AI-powered next-gen antivirus; combines machine learning, behavioral analysis, memory scanning, and exploit mitigation to stop modern threats

FALCON INSIGHT XDR | DETECTION AND RESPONSE FOR ENDPOINT AND BEYOND

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

FALCON FIREWALL MANAGEMENT | HOST-BASED FIREWALL

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

FALCON DEVICE CONTROL | USB SECURITY

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

FALCON FOR MOBILE | MOBILE THREAT DETECTION

Protects against threats to iOS and Android devices, extending 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

FALCON FOR XIoT | XIoT ASSET PROTECTION

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

FALCON INSIGHT FOR ChromeOS | ChromeOS PROTECTION

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

FALCON FOR LEGACY SYSTEMS | PROTECTION FOR LEGACY OPERATING SYSTEMS

Provides lightweight, cloud-native protection for older Windows systems — no upgrades or added complexity

Counter Adversary Operations

FALCON ADVERSARY OVERWATCH | INTELLIGENCE-LED THREAT HUNTING

Provides 24/7 protection across endpoints, identities, cloud workloads, and next-gen SIEM 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 IOCs, 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 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 operating system, 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; help with compliance efforts; and maintain continuous continuous security for all configurations, human and non-human users, shadow apps, data, devices connecting to SaaS, 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 PRIVILEGED ACCESS

Powered by Falcon Identity Protection, minimizes identity risk with just-in-time (JIT) access, granting elevated permissions only when needed and under secure conditions

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 | SECURITY INFORMATION AND EVENT MANAGEMENT

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

Data Protection

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

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

FALCON DATA PROTECTION FOR CLOUD | RUNTIME CLOUD DATA PROTECTION

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

Security and IT Operations

FALCON EXPOSURE MANAGEMENT | EXPOSURE MANAGEMENT

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

FALCON EXPOSURE MANAGEMENT: CAASM

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

FALCON FILEVANTAGE | FILE INTEGRITY MONITORING

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

FALCON FOR IT | INTELLIGENT ENDPOINT AUTOMATION

Extends the Falcon platform to accelerate observability and response workflows for security operations teams

FALCON ADVERSARY OVERWATCH: NEXT-GEN SIEM | THREAT HUNTING

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

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

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

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

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

AI SECURITY SERVICES

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

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

AI for SecOps Readiness | Allows you to safely integrate AI into detection and response workflows with tailored use cases, architectural guidance, and a roadmap to increase speed, precision, and impact

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

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

Cloud Breach Emulation and Response Exercise | Helps your team quickly uncover gaps and sharpen its response to cloud threats

TECHNICAL ASSESSMENT SERVICES

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

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

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

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

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

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

TRAINING AND SECURITY UPSKILLING

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

CROWDSTRIKE PULSE SERVICES

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

About CrowdStrike

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

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

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

CrowdStrike: We stop breaches.

Learn more: www.crowdstrike.com

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

Start a free trial today: www.crowdstrike.com/free-trial-guide