

# EXECUTIVE SUMMARY

Presented by:



# 2025 THREAT HUNTING REPORT



# Adversaries Weaponize and Target AI at Scale

The modern threat landscape is defined by adversaries operating with speed, stealth, and innovation. Today's "enterprising adversary" executes attacks with calculated, business-like efficiency, operating with precision to maximize their impact and quickly achieve their goals.

These adversaries are adept at bypassing traditional cybersecurity defenses. They seek to stay undetected by moving to unmanaged networks and expanding their reach. Cross-domain threat hunting remains critical as adversaries operate across multiple domains — such as identity, endpoint, and cloud — 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.

As adversaries continue to evolve their operations, we must understand them in order to stop them. The CrowdStrike Counter Adversary Operations team brings together industry-leading threat intelligence and best-in-class managed threat hunting with the CrowdStrike Falcon® platform to detect, disrupt, and stop adversaries. Counter Adversary Operations comprises two closely integrated teams: CrowdStrike Intelligence analysts and CrowdStrike OverWatch threat hunters. Together, they protect thousands of customers from the most sophisticated adversaries by providing the intelligence and threat hunting skills and resources that most organizations lack.

The CrowdStrike 2025 Threat Hunting Report highlights the trends this team has observed from July 2024 to June 2025 and details how the team uses innovation and proactive, intelligence-informed threat hunting. Following is a summary of the report's key findings and observations.



# Key Findings

CrowdStrike OverWatch observed the following year-over-year trends between July 1, 2024 and June 30, 2025.



## Malware-free intrusions are on the rise:

**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 is dominating the attack landscape:

**73%** of the total interactive intrusions from July 2024 to June 2025 were **associated with eCrime activity**, highlighting the persistent and pervasive threat of adversaries seeking financial gain.



## Cloud environments are under siege:

**Cloud intrusions increased 136%** in the first half of 2025 compared to all of 2024.



## China is targeting the cloud:

CrowdStrike OverWatch observed a **40% year-over-year increase** in intrusions by suspected cloud-conscious China-nexus actors.



## Voice phishing (vishing) attacks are surging:

















In the first half of 2025, vishing attacks already **surpassed the total number seen in 2024.**



## Targeted intrusions against the government sector are on the rise:

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.**

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

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.

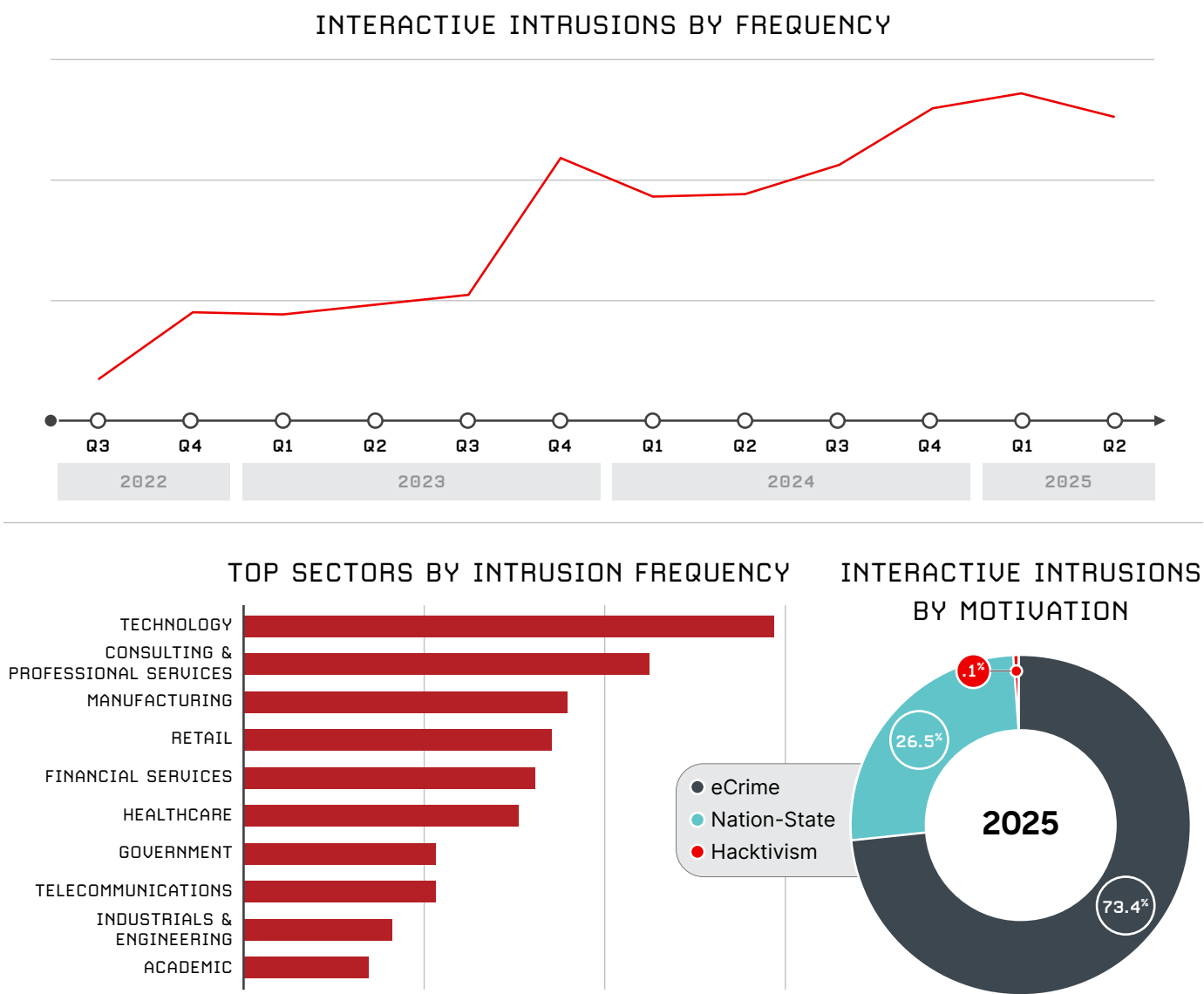
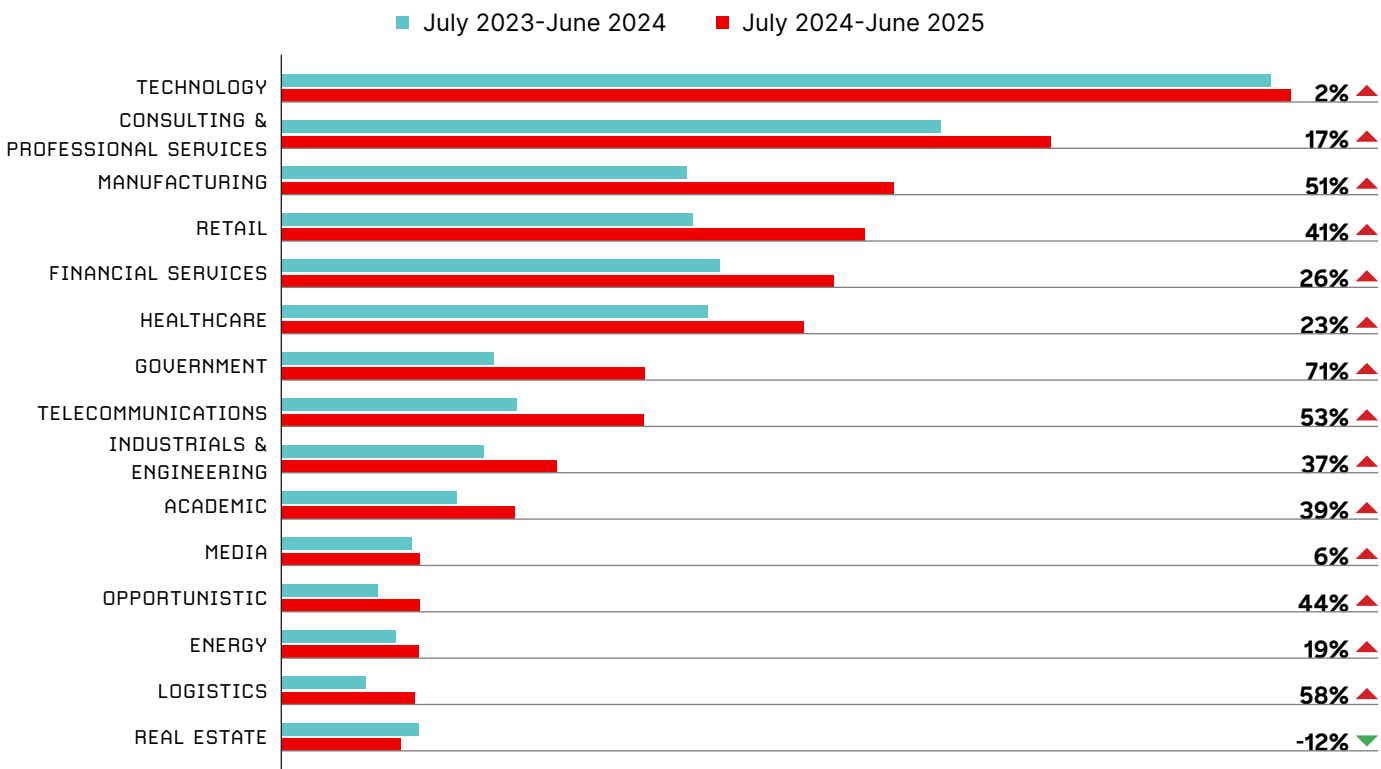


Figure 1. Interactive intrusion breakdown

## 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.

### TOP TARGETED SECTORS BY INTRUSION FREQUENCY



### NATION-STATE US. eCRIME

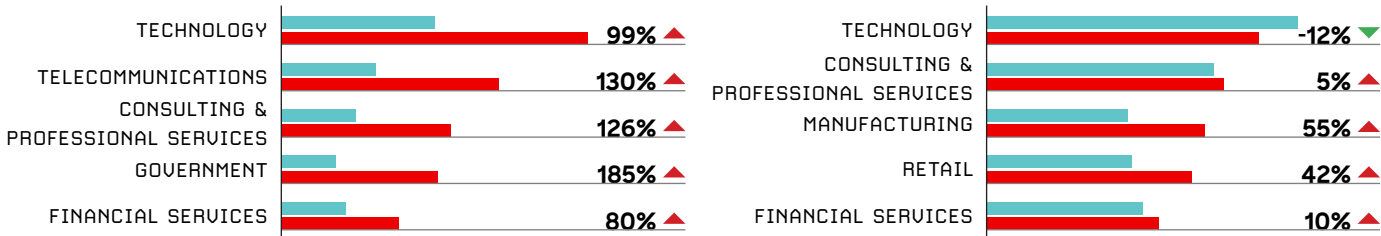


Figure 2. Targeted sectors by intrusion frequency

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.



## MOST INTRUSIVE ADVERSARIES

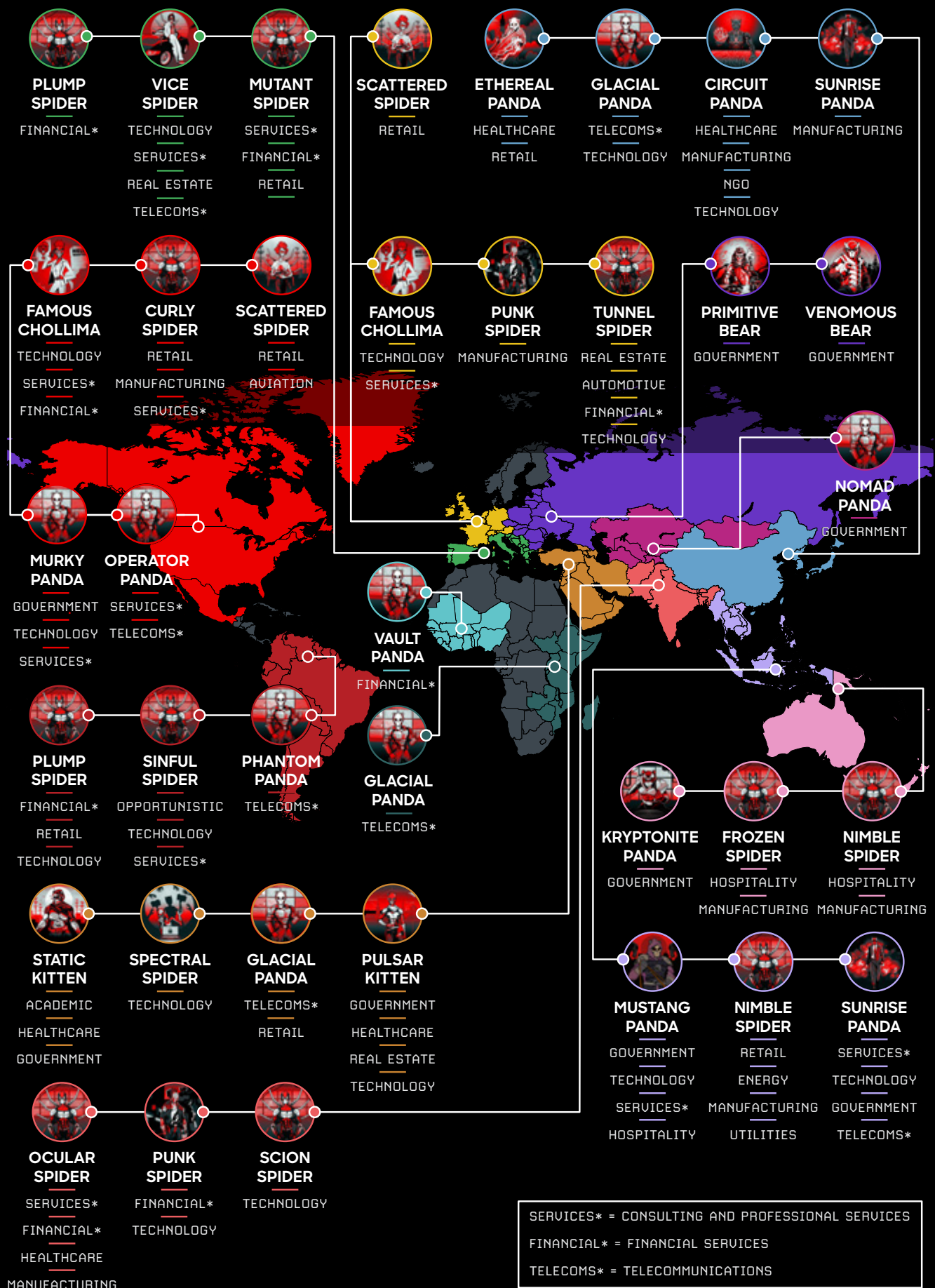


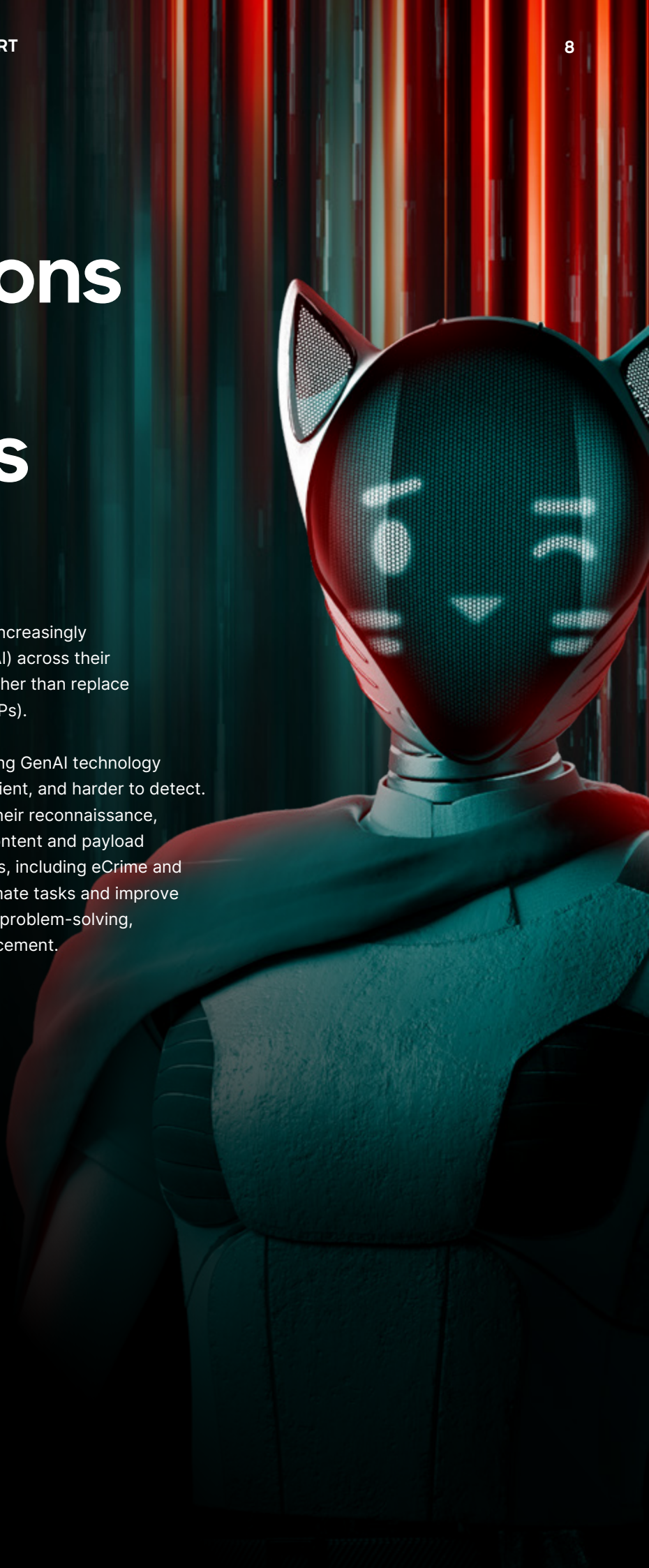
Figure 3. Interactive adversary disruptions across the world, July 2024-June 2025

# Observations from the Front Lines

## Adversaries Use GenAI to Augment Operations

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

Nation-state adversaries 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:

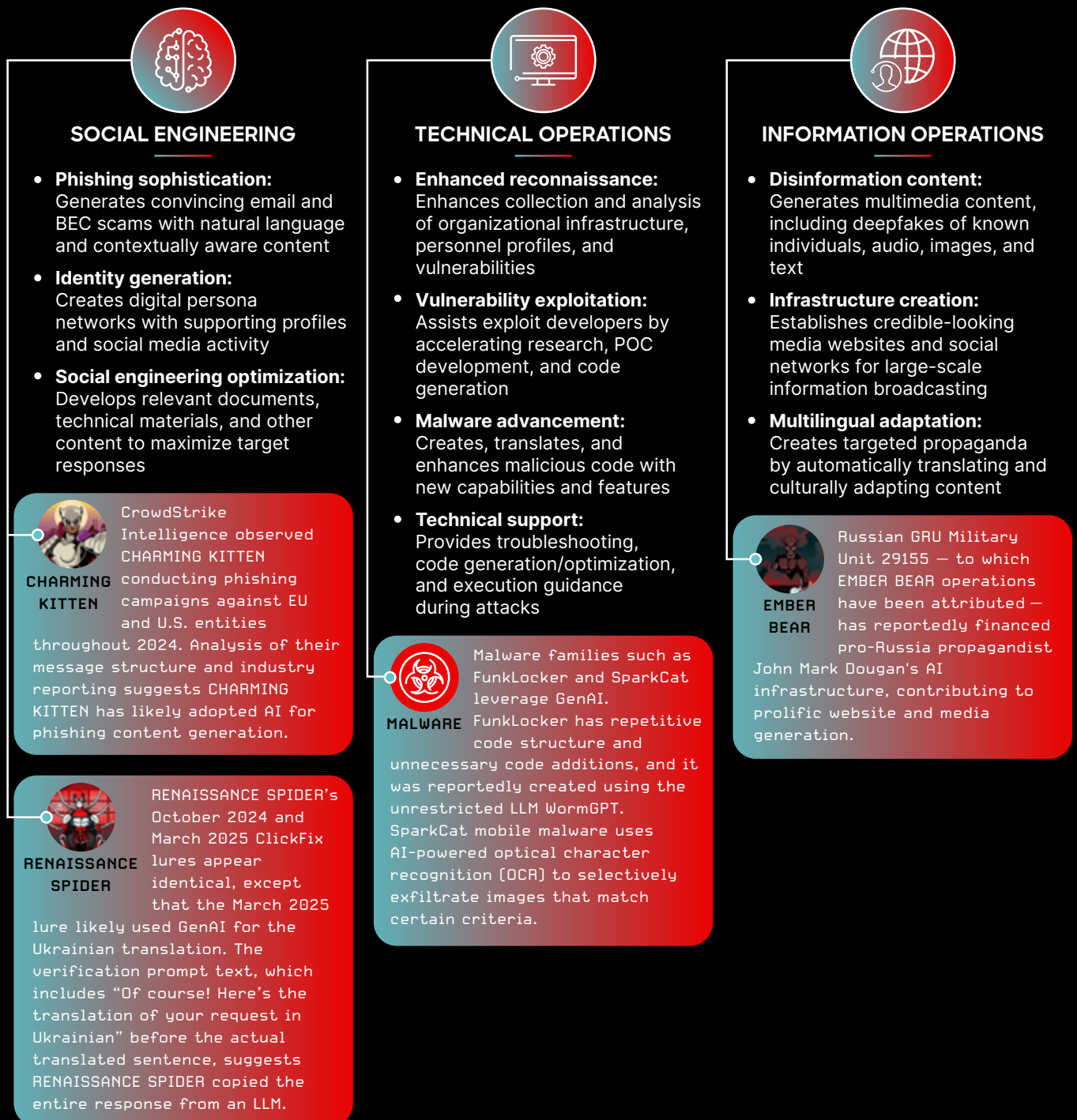
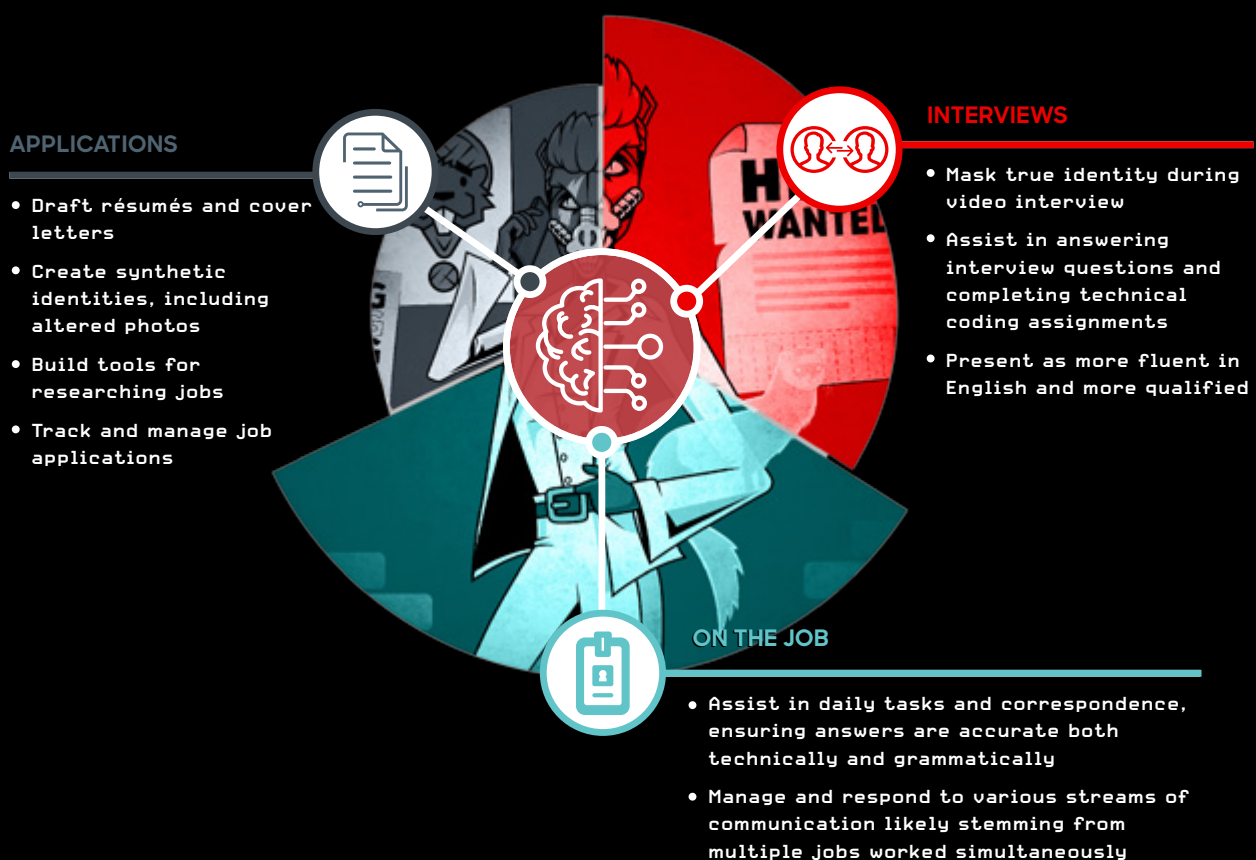


Figure 4. Adversary use of GenAI as a primary attack vector

## FAMOUS CHOLLIMA Leads in GenAI-Supported Operations

Democratic People's Republic of Korea (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 throughout their IT worker operations.



**Figure 5.** FAMOUS CHOLLIMA's use of GenAI in insider threat operations

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.

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. Though defenders can use AI for security capabilities, organizations' continued AI tooling integration creates an expanded attack surface that threat actors will likely seek to exploit by directly targeting AI applications.

# 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.

# 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.

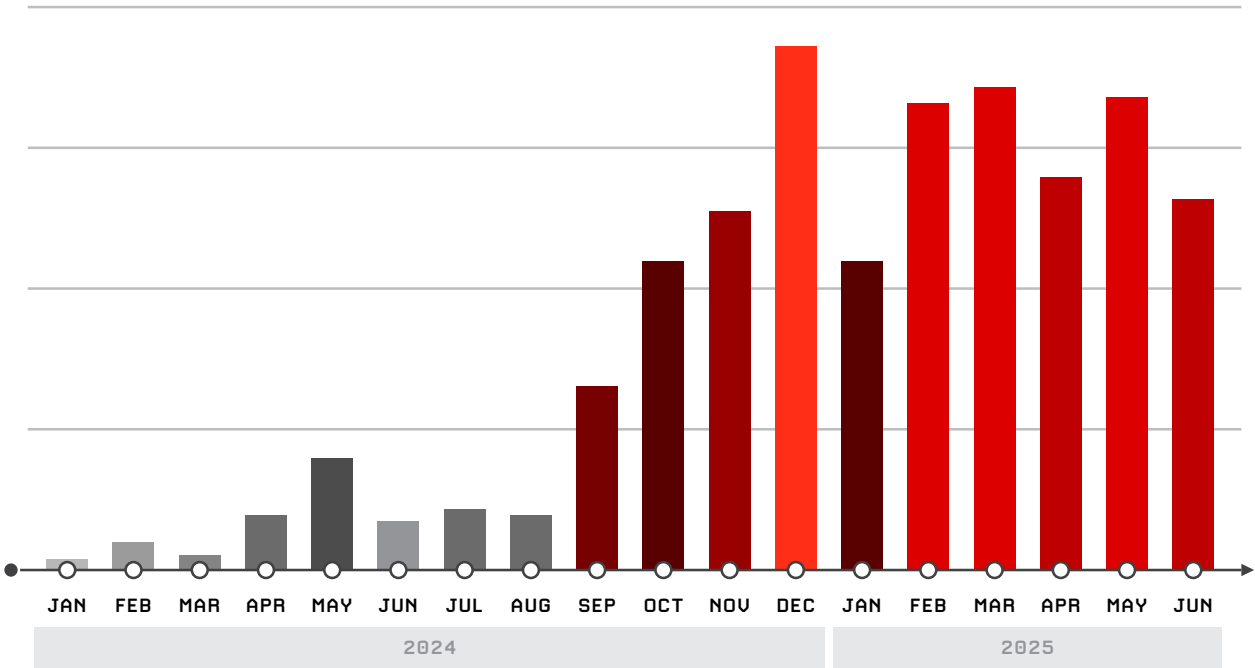


Figure 6. Vishing attacks observed by month, January 2024-June 2025



## CLOUD HUNTING

The CrowdStrike 2025 Global Threat Report identified that China's cyber espionage capabilities reached a critical inflection point in 2024, marked by increasingly bold targeting, stealthier tactics, and expanded operational capacity.

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.

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 7 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

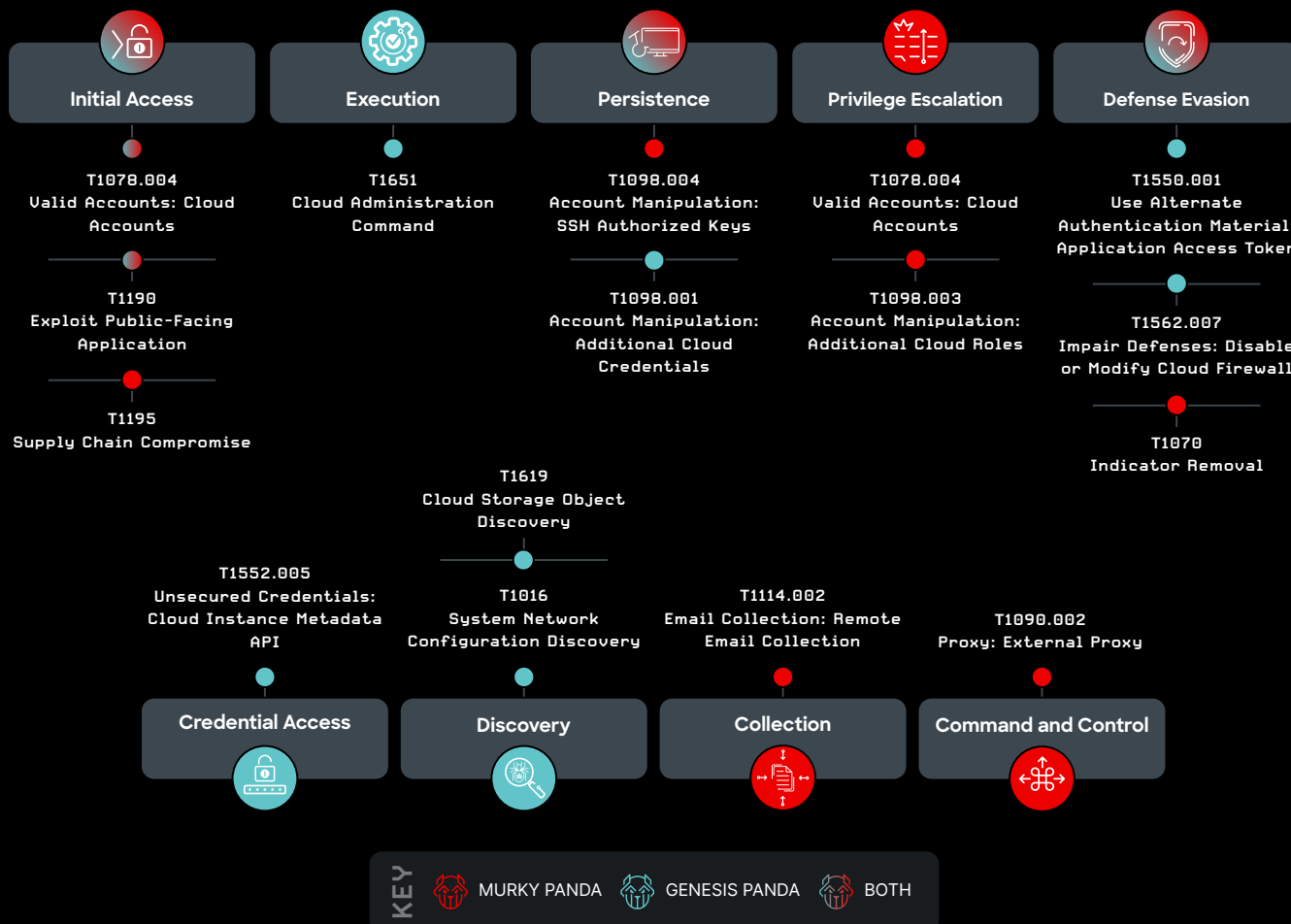


Figure 7. Prevalent MITRE ATT&CK® TTPs used by MURKY PANDA and GENESIS PANDA

## 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 threat 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.

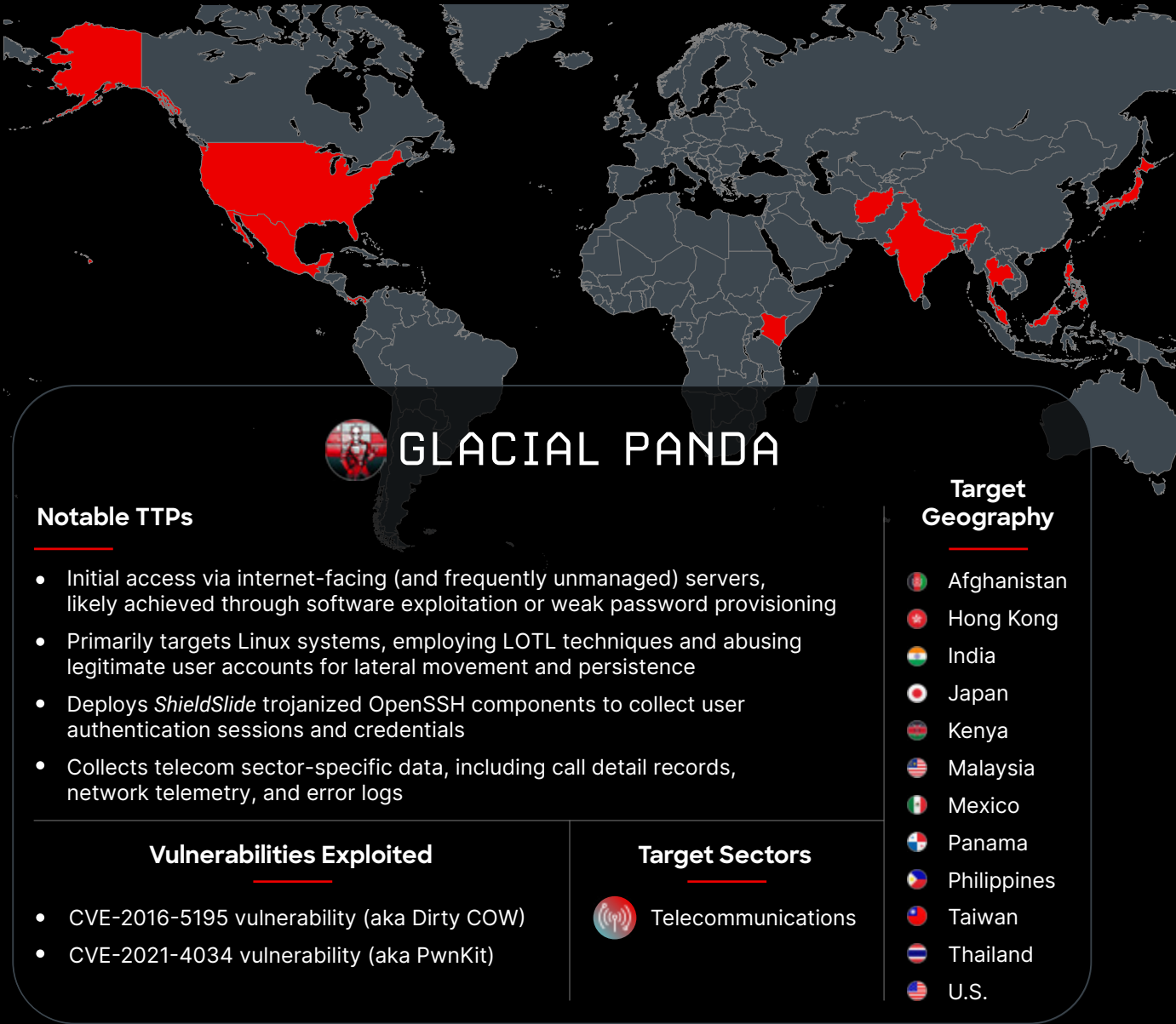


Figure 8. GLACIAL PANDA: TTPs and targets

## 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.



# Conclusion

The past 12 months 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.

The CrowdStrike 2025 Threat Hunting 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, multifactor authentication (MFA) bypass, and social engineering while moving laterally between on-premises, cloud, and software as a service (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 extended detection and response (XDR) platforms ensures comprehensive visibility and a unified defense against adversaries.

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

## 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 security information and event management (SIEM) solutions provide unified visibility across endpoints, networks, cloud environments, and identity systems, enabling analysts to correlate suspicious behaviors and see the full attack path. 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.

# 4

## 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 promptly addressed.

# 5

## 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.

# 6

## 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.

# Download the Full Report

The CrowdStrike 2025 Threat Hunting Report presents a comprehensive analysis of the most significant trends and events in cyber threat activity in 2025. Download a free copy of the report at [www.crowdstrike.com/en-us/resources/reports/threat-hunting-report/](https://www.crowdstrike.com/en-us/resources/reports/threat-hunting-report/).



## About CrowdStrike

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

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

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

**CrowdStrike: We stop breaches.**

Learn more: [www.crowdstrike.com](https://www.crowdstrike.com)

Follow us: [Blog](#) | [X](#) | [LinkedIn](#) | [Facebook](#) | [Instagram](#) | [YouTube](#)

Start a free trial today: [www.crowdstrike.com/free-trial-guide](https://www.crowdstrike.com/free-trial-guide)

© 2025 CrowdStrike, Inc. All rights reserved.

Presented by:

