



CrowdStrike 2024 Threat Hunting Report

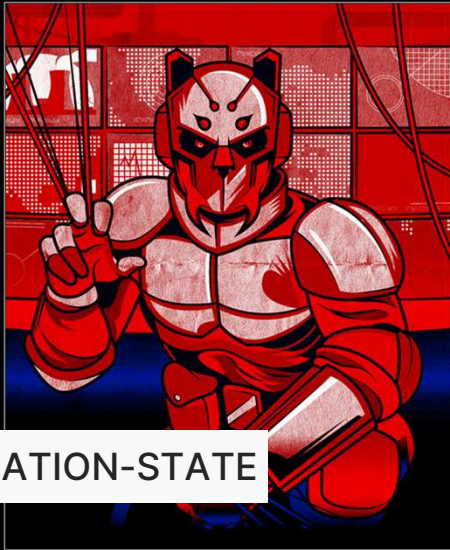
Alex Kriechbaum

Sales Engineer

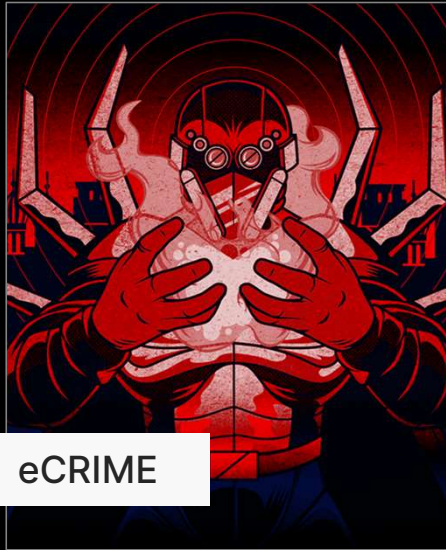




Threat Actor Motivation



NATION-STATE



eCRIME



HACKTIVISM

CRIMINAL

ALCHEMIST SPIDER
ALPHA SPIDER
AVIATOR SPIDER
BITWISE SPIDER
BLIND SPIDER
BRAIN SPIDER
CARBON SPIDER
CHARIOT SPIDER
CHAOTIC SPIDER
CHEF SPIDER
CLOCKWORK SPIDER
DEMON SPIDER
DONUT SPIDER
FROZEN SPIDER
GRACEFUL SPIDER
HAZARD SPIDER
HERMIT SPIDER
HIVE SPIDER
HOLIDAY SPIDER
HONEY SPIDER
INDRIK SPIDER
KNOCKOUT SPIDER
LILY SPIDER
LUNAR SPIDER
MALLARD SPIDER
MANGLED SPIDER
MASKED SPIDER
MONARCH SPIDER

MUMMY SPIDER
NARWHAL SPIDER
ODYSSEY SPIDER
OUTBREAK SPIDER
PERCUSSION SPIDER
PROPHET SPIDER
PUNK SPIDER
QUANTUM SPIDER
RECESS SPIDER
RICE SPIDER
ROYAL SPIDER
SALTY SPIDER
SAMBA SPIDER
SCATTERED SPIDER
SCULLY SPIDER
SHINING SPIDER
SLIPPY SPIDER
SMOKY SPIDER
SOLAR SPIDER
SPRITE SPIDER
TRAVELING SPIDER
TUNNEL SPIDER
VAMPIRE SPIDER
VENOM SPIDER
VETO SPIDER
WANDERING SPIDER
WIZARD SPIDER
VICE SPIDER

NORTH KOREA

LABYRINTH CHOLLIMA
FAMOUS CHOLLIMA
RICOCHET CHOLLIMA
SILENT CHOLLIMA
STARDUST CHOLLIMA
VELVET CHOLLIMA

INDIA

HAZY TIGER
OUTRIDER TIGER
QUILTED TIGER
RAZOR TIGER
VICEROY TIGER

EGYPT

WATCHFUL SPHINX

VIETNAM

OCEAN BUFFALO

SOUTH KOREA

SHADOW CRANE

SYRIA

DEADEYE HAWK

KAZAKHSTAN

COMRADE SAIGA

COLOMBIA

GALACTIC OCELOT

TURKEY

COSMIC WOLF

PAKISTAN

MYTHIC LEOPARD
FRINGE LEOPARD

IRAN

BANISHED KITTEN
CHARMING KITTEN
CHRONO KITTEN
HAYWIRE KITTEN
IMPERIAL KITTEN
NEMESIS KITTEN
PIONEER KITTEN
REFINED KITTEN
SPECTRAL KITTEN
STATIC KITTEN
TRACER KITTEN
VENGEFUL KITTEN

RUSSIA

BERSERK BEAR
COZY BEAR
EMBER BEAR
FANCY BEAR
GOSSAMER BEAR
PRIMITIVE BEAR
VENOMOUS BEAR
VOODOO BEAR

HACKTIVIST

CURIOUS JACKAL
FRONTLINE JACKAL
INTREPID JACKAL
PARTISAN JACKAL
REGAL JACKAL
RENEGADE JACKAL

CHINA

AQUATIC PANDA
CASCADE PANDA
EMISSARY PANDA
ETHEREAL PANDA
JACKPOT PANDA
HORDE PANDA
KARMA PANDA
KRYPTONITE PANDA
LOTUS PANDA
MUSTANG PANDA
OVERCAST PANDA
PHANTOM PANDA
PIRATE PANDA
PUZZLE PANDA
SHATTERED PANDA
SUNRISE PANDA
VANGUARD PANDA
VAPOR PANDA
VERTIGO PANDA
VIXEN PANDA
WICKED PANDA



Key Stats

245+ total adversaries tracked by CrowdStrike

86% of hands-on-keyboard attacks were executed by eCrime adversaries

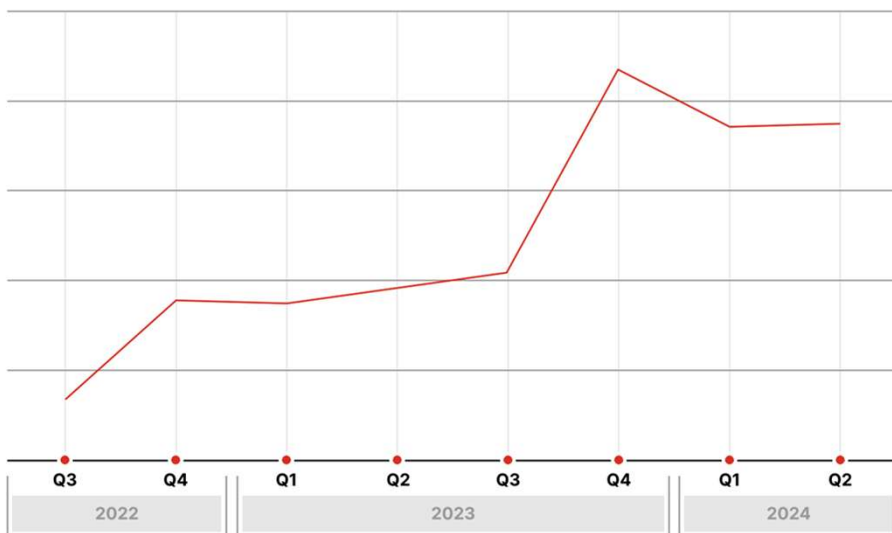
70% increase in the use of legitimate RMM tools

5 of the top 10 MITRE tactics observed were identity-based

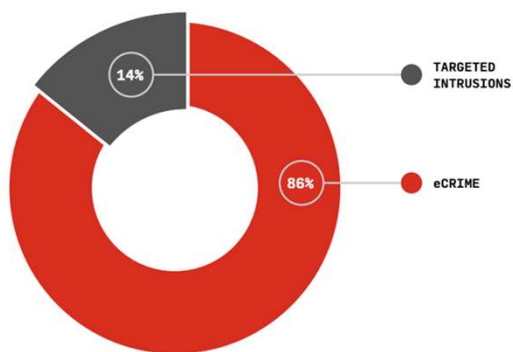
142% increase in access broker advertisements targeting healthcare

75% increase in cloud intrusions

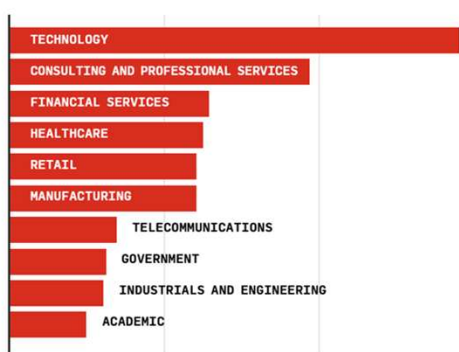
Interactive Intrusions Over Time | Q3 2022-Q2 2024



Interactive Intrusions by Motivation
Q3 2023-Q2 2024



Top Verticals by Intrusion Frequency
Q3 2023-Q2 2024



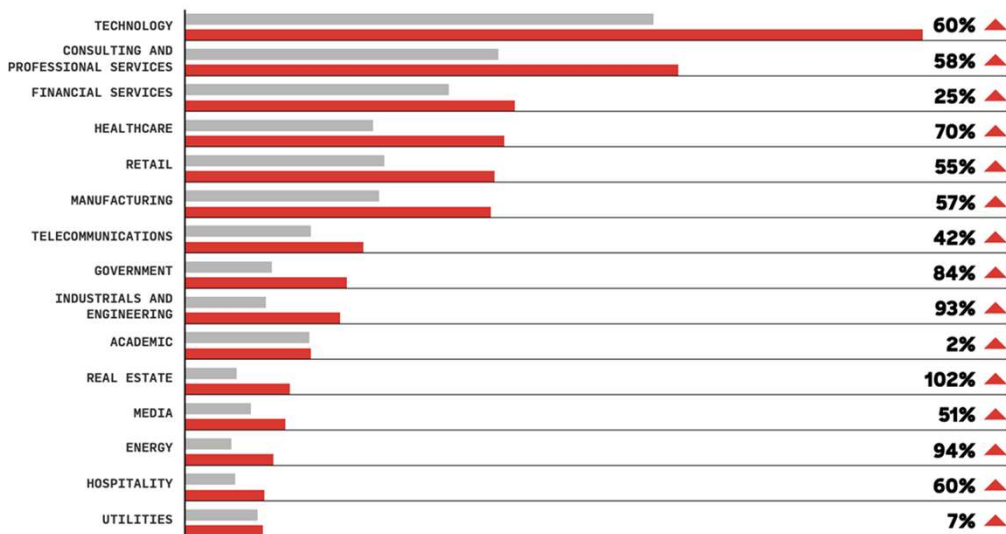
Interactive Intrusions



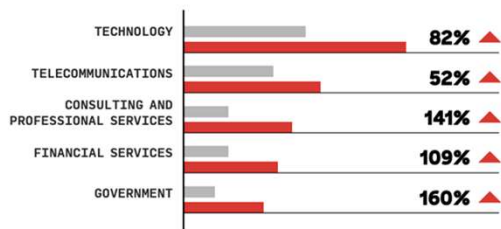
Interactive intrusions, or hands-on-keyboard attacks, are typically more **sophisticated and difficult to detect** compared to automated attacks, requiring advanced threat hunting and incident response capabilities to identify and mitigate.

Top Sectors by Intrusion Frequency

■ JULY 2022-JUNE 2023 ■ JULY 2023-JUNE 2024

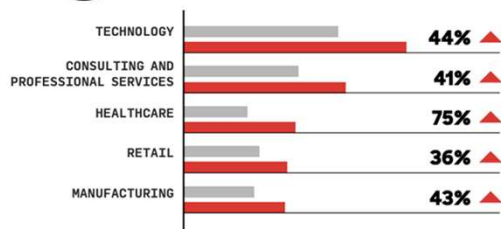


Targeted Intrusion



vs.

eCrime



Sector Highlights

- Across all sectors, interactive intrusions increased by **55%**
- Technology has been targeted the most for the last **7 years**
- Targeted intrusion: The largest increase was in the consulting and professional services sector **(+141%)**
- eCrime intrusion: The largest increase was in the healthcare sector **(+75%)**



Key Findings

- **Cross-domain** attacks are on the rise
- Stealthy adversaries exploit **legitimate credentials** to gain access
- Adversaries target the **cloud control plane** for full access to cloud infrastructure
- Exploiting **RMM tools** is a tried-and-true technique in endpoint intrusion
- Businesses unknowingly employ adversaries, enabling **insider threats**

SCATTERED SPIDER Cross-Domain Attack

Having full insight into telemetry spanning endpoint, identity and cloud environments is a force multiplier to hunt cross-domain attacks



1

IDENTITY

Conducted a phishing campaign to obtain valid credentials



2

CLOUD

Leveraged the credentials to authenticate to the cloud control plane



3

CLOUD

Established a foothold on a cloud-hosted VM via a cloud service VM management agent



4

ENDPOINT

Established persistence by creating a new user and downloading FleetDeck

SCATTERED SPIDER Cross-Domain Attack

Having full insight into telemetry spanning endpoint, identity and cloud environments is a force multiplier to hunt cross-domain attacks



1

IDENTITY

Conducted a phishing campaign to obtain valid credentials

2



CLOUD

Leveraged the credentials to authenticate to the cloud control plane



3

CLOUD

Established a foothold on a cloud-hosted VM via a cloud service VM management agent

4



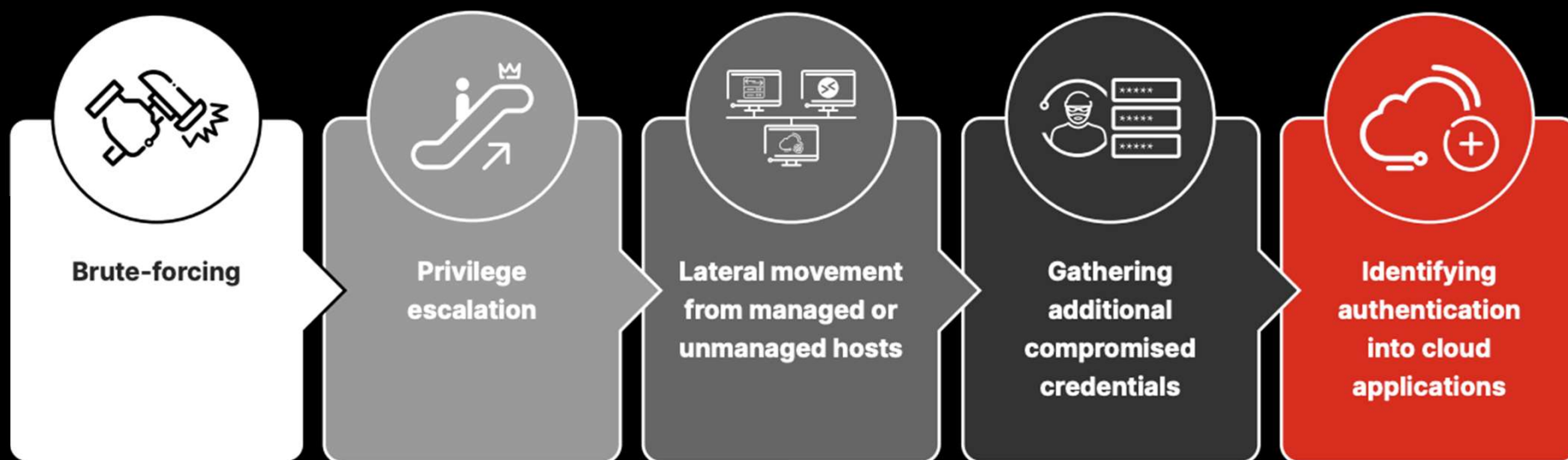
ENDPOINT

Established persistence by creating a new user and downloading FleetDeck

Stealthy Adversaries Exploit Legitimate Credentials to Gain Access

Surge in access broker advertisements

142% in healthcare and 152% in consulting and professional services





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 Control Plane Is a Prime Target

The cloud control plane is the **backbone of cloud operations**, serving as a command center to manage, secure and optimize cloud environments.

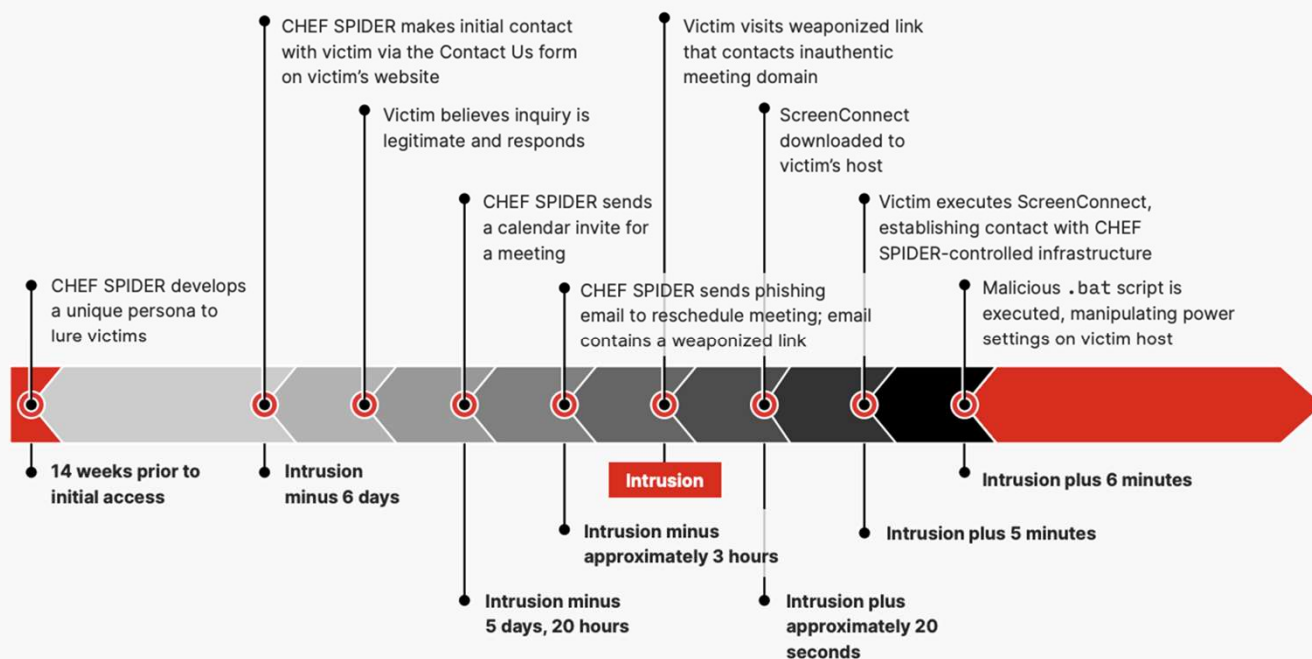
A compromised control plane gives adversaries **broad access and control** over the entire cloud environment, making it a prime target.



5 Steps to Mitigate Cloud-Conscious Adversaries

- **Gain** a comprehensive understanding of your cloud platform
- **Standardize and validate** cloud resource configurations pre-deployment; monitor for deviations
- **Apply** consistent security policies to all servers; deny outbound connections from non-allowlisted endpoints
- **Monitor** cloud assets and vulnerabilities; mitigate risks promptly
- **Apply** least privilege principle; evaluate credentials and configurations to ensure minimal necessary access

Remote Monitoring and Management Tool Exploit



CHEF SPIDER uses RMM tool for initial access

70% increase in adversaries exploiting legitimate RMM tools

156% increase in ConnectWise usage, becoming the most exploited RMM tool

Top 5 RMM tools:

1. ConnectWise ScreenConnect
2. AnyDesk
3. TeamViewer
4. Atera Agent
5. Splashtop



Protect Against RMM Threats

- **Establish** a baseline of approved RMM software and users
- **Define** expected legitimate RMM tool behavior, including normal directory paths, remote domains, IP addresses and files
- **Monitor** for known RMM-related filenames, paths or processes, and block access to service provider domains hosting RMM tools
- **Monitor** for anomalous DNS requests, network connections and process trees with unexpected parameters and flags
- **Search** for disk artifacts (e.g., logs) written by RMM tools



Hunting for RMM

- RustDesk
- AnyDesk
- TinyPilot
- VS Code Dev Tunnels
- Google Chrome Remote Desktop



Looking for Network Connections

- Unexpected source IP addresses when accessing cloud services
- Impossible travel logins
- Use of unauthorized VPNs



Validating with CrowdStrike Falcon® Identity Protection

Comparing and validating expected behaviors for a known role with non-expected behaviors



Disrupting the Adversary

Validating suspicious activity, especially in cases where:

- Unauthorized remote management or administration tools are deployed
- Employees are installing suspected malware
- Employees are repeatedly unwilling to enable video during calls



Strengthening Detections

Creating new detections and preventions for the CrowdStrike Falcon® platform



FAMOUS CHOLLIMA Insider Threats

FAMOUS CHOLLIMA malicious insiders were identified applying to or actively working at more than **100 companies** — most were U.S.-based technology entities.

Insider threats exploit **trusted employee-level access** to cause harm, making detection and prevention particularly challenging.



FAMOUS

CHOLLIMA

TACTICS, TECHNIQUES & PROCEDURES

- Phishing using job recruitment themes
- Abuse of Node.js packages
- Collection of cryptocurrency wallet information stored in browser
- Use of port 1244 for C2

MALWARE

- BeaverTail
- InvisibleFerret
- Open-source RMM tools

MALWARE

- | | |
|----------------------|-------------------------|
| • Defense | • Pharmaceutical |
| • Financial services | • Professional Services |
| • FinTech | • Retail |
| • Insurance | • Technology |
| • Manufacturing | • Transportation |
| • Media | |

TARGET GEOGRAPHY

- | | |
|---|---------------|
|  | Argentina |
|  | Australia |
|  | Brazil |
|  | Cyprus |
|  | France |
|  | Hong Kong |
|  | India |
|  | Ireland |
|  | Philippines |
|  | Saudi Arabia |
|  | Singapore |
|  | Turkey |
|  | Ukraine |
|  | United States |
|  | Vietnam |

IT Workers

- 130 companies targeted
- Deploy RMM tools on corporate laptop
- Data exfil in ~50% of cases
- Deployments of *BeaverTail* & *InvisibleFerret* in some cases
- DOJ: \$6.8M over 2 years

REWARD OF UP TO \$5 MILLION FOR INFORMATION ON NORTH KOREAN IT WORKERS AND RELATED MONEY LAUNDERING



North Korean information technology (IT) workers, using aliases Han Jiho, Jin Chunji, Xu Haoran, and Zhonghua, engaged in a scheme to obtain remote work for U.S. companies and launder the proceeds, generating \$6.8 million in illicit revenue for North Korea, in violation of U.S. and UN sanctions.

If you have information on Han, Jin, Xu, Zhonghua, their associates, or their activities, send it to us via our Tor-based tip line below. You may be eligible for a reward and relocation.

Tor Link: he5dybnt7sr6cm32xt77pazmtm65flqy6irivtflruqfc5ep7eiodiad.onion

U.S. Department of State
Diplomatic Security Service
Rewards for Justice

+1-202-702-7843
@RFJ USA





FAMOUS CHOLLIMA



Malware Ops
(BeaverTail & InvisibleFerret)



IT Workers

Cryptocurrency
Credential Theft



Credit Card
Information Theft



Possible Data Exfil



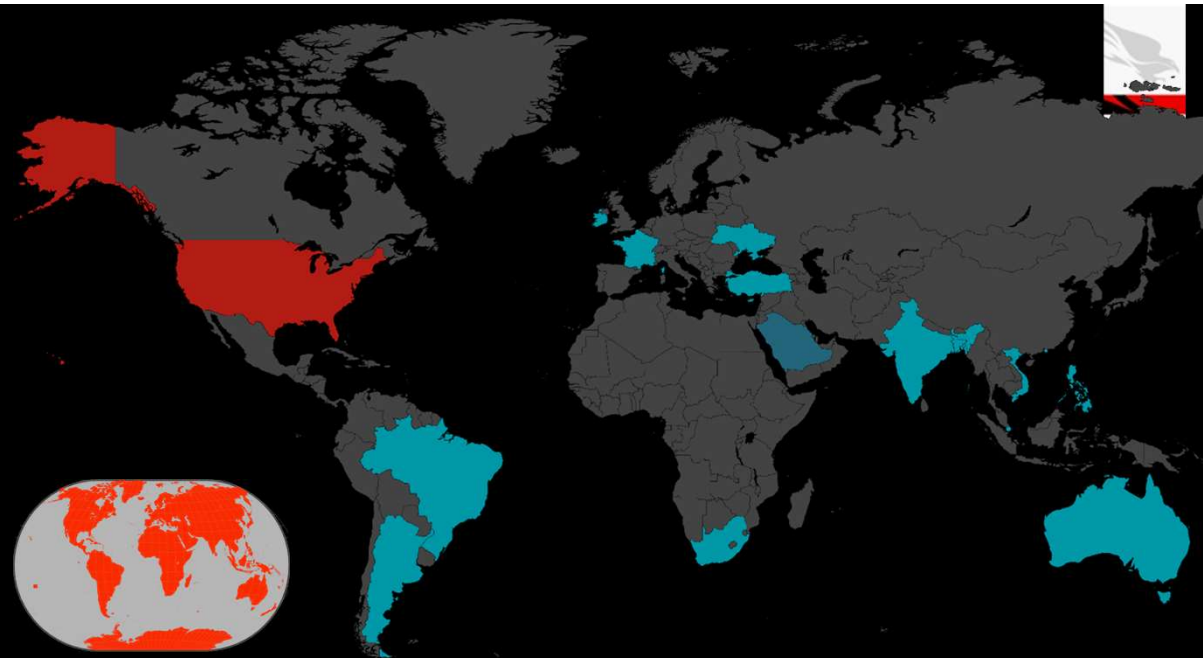
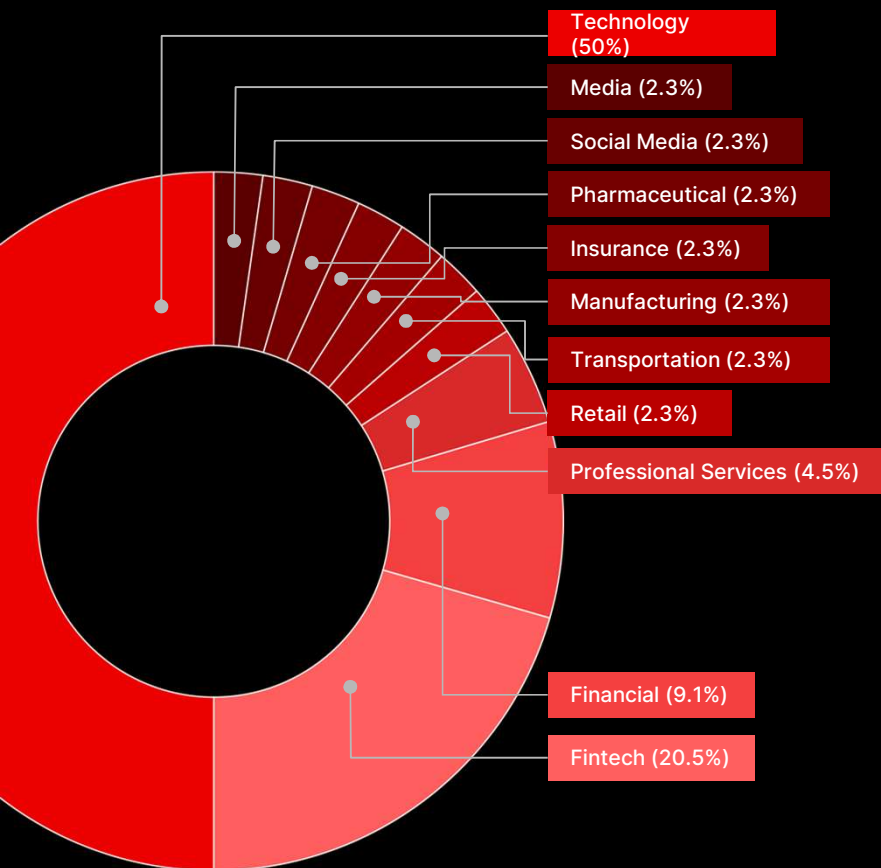
Legitimate work



Possible Data Exfil



Targeting



United States



Global



Saudi Arabia



France



Philippines



Ukraine



Brazil



Argentina



Ireland



India



Singapore



Australia



Vietnam



Hong Kong



Cyprus



South Africa



Turkey



Bangladesh



Kim Jong-un
(Supreme Leader)

KWP Cadre
Department

Foreign Ministry
(issues passports)

DPRK Cabinet

Office 39
(KWP)

Munitions Industry
Department
(KWP)

Finance Accounting
Department
(KWP)

Propaganda &
Agitation
Department
(KWP)

Ministry of People's
Armed Forces

Ministry of
Public Health

External Construction
General Bureau

Korea
Computer
Center

Hotel Management
Department

Mansudae Art Studio

Reconnaissance
General Bureau

General Political
Bureau

Ministry of
Physical Culture &
Sports

Dae-Sung General
Bureau

75 Bureau

Ministry of Posts &
Telecommunications

Un-Ha General
Bureau

Korean People's Army
Fine Art Company

Ministry of External
Economic Relations

(8 more Bureaus)

★Entities under the Cabinet must obtain permission from the
Financial Planning Department separately

★The Ministry of State Security sends its security agents to the
companies overseas for monitoring and control over overseas
workers.



Outlook

- Financially motivated
- Slow to change
- Experimenting with new infection vectors
- Low payout, high tempo operations



PUNK SPIDER



INITIAL ACCESS	A service account is used to RDP into a system	The Falcon sensor flags this activity as suspicious and alerts Falcon Complete and CrowdStrike OverWatch
+ 12-14 MINUTES	PUNK SPIDER begins their initial post-access actions 12 minutes after leveraging the compromised credentials	The Falcon sensor prevents these files from running on the system in real time
RECONNAISSANCE	PUNK SPIDER begins to conduct basic network reconnaissance and downloads additional payloads unique across the CrowdStrike telemetry	The reconnaissance conducted by PUNK SPIDER triggers CrowdStrike OverWatch detections, and the Falcon sensor prevents the additional payloads from running
+ 3 MINUTES	PUNK SPIDER attempts to dump additional credentials from the system in an attempt to look for additional privileges that could help them in their objectives	The attempted credential dumping creates additional CrowdStrike OverWatch detections, which are being actively monitored
ESCALATION	PUNK SPIDER begins to introduce custom scripts onto the system in an attempt to subvert Falcon sensor preventions	The Falcon sensor flags this activity as suspicious and alerts Falcon Complete and CrowdStrike OverWatch
+ 8 MINUTES		CrowdStrike OverWatch has triggered customer alerts and has provided the details to their Falcon Complete counterparts
CONTAINMENT		CrowdStrike OverWatch has triggered customer alerts and has provided the details to their Falcon Complete counterparts
+ 15 MINUTES		Falcon Complete informs the customer on the host containment and provides immediate recommendations
+ 60 MINUTES		Falcon Complete holds an advisory call with the customer detailing the disabling of compromised accounts as well as custom IOC/IOA preventions that were put in place

© 2024 CrowdStrike, Inc. All rights reserved.

Hunting PUNK SPIDER

Adversaries continue to operate with speed and stealth.

CrowdStrike's powerful combination of the AI-powered Falcon platform and **intelligence-led threat hunting** helps organizations detect elusive threats and outpace the adversary.



5 Steps to Be Prepared

1

Identity Protection

2

Effective Cloud Security

3

Cross-Domain Visibility

4

Practice Like You Want to Play

5

Know the Adversary

