CROWDSTRIKE

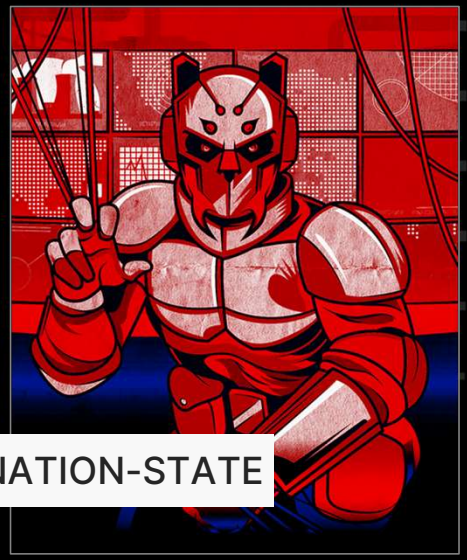
CrowdStrike 2024 Threat Hunting Report

Alex Kriechbaum

Sales Engineer

CROWDSTRIKE

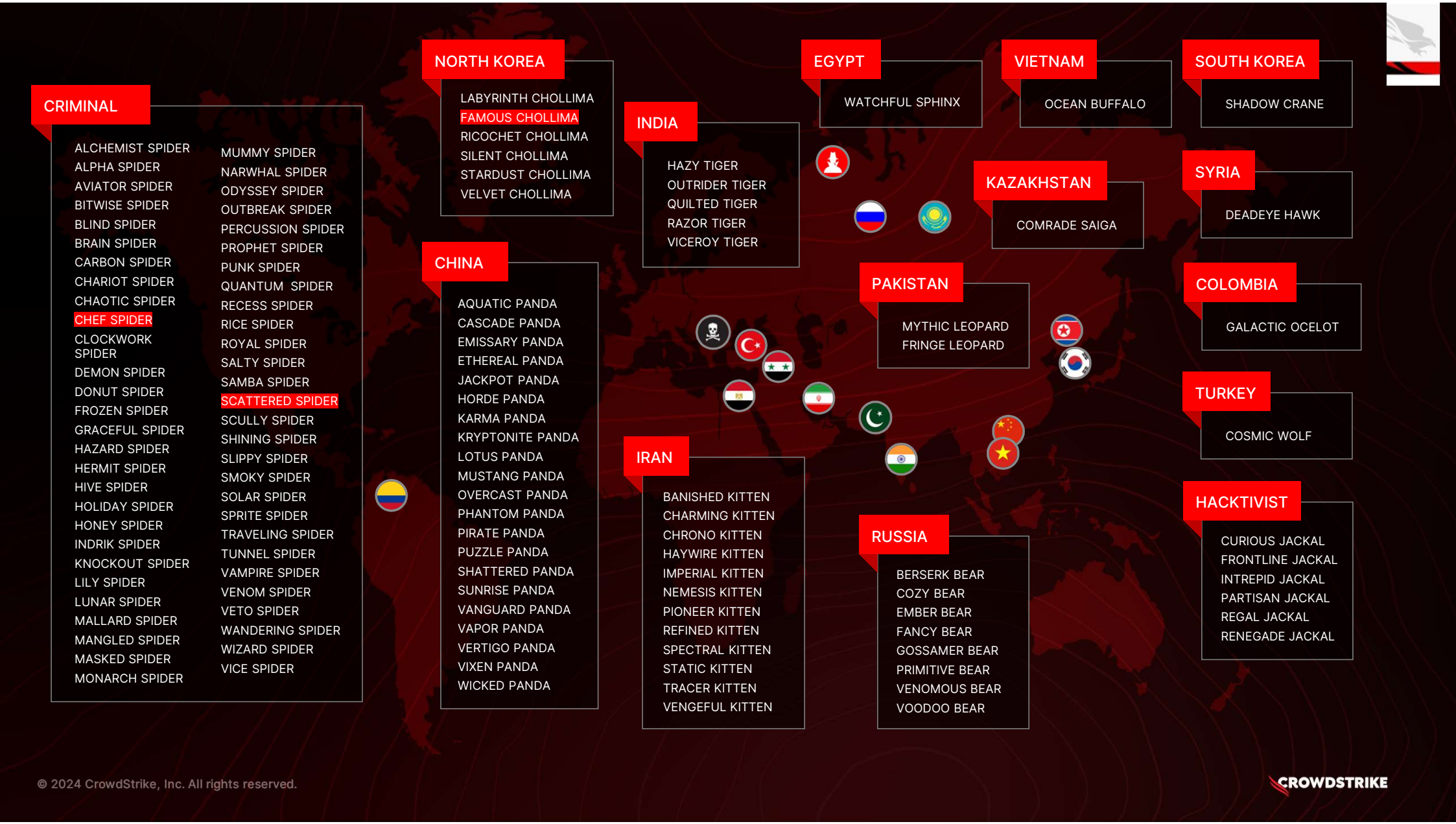
Threat Actor Motivation



NATION-STATE

eCRIME

HACKTIVISM



CROWDSTRIKE

Key Stats

245+ total adversaries tracked by CrowdStrike

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

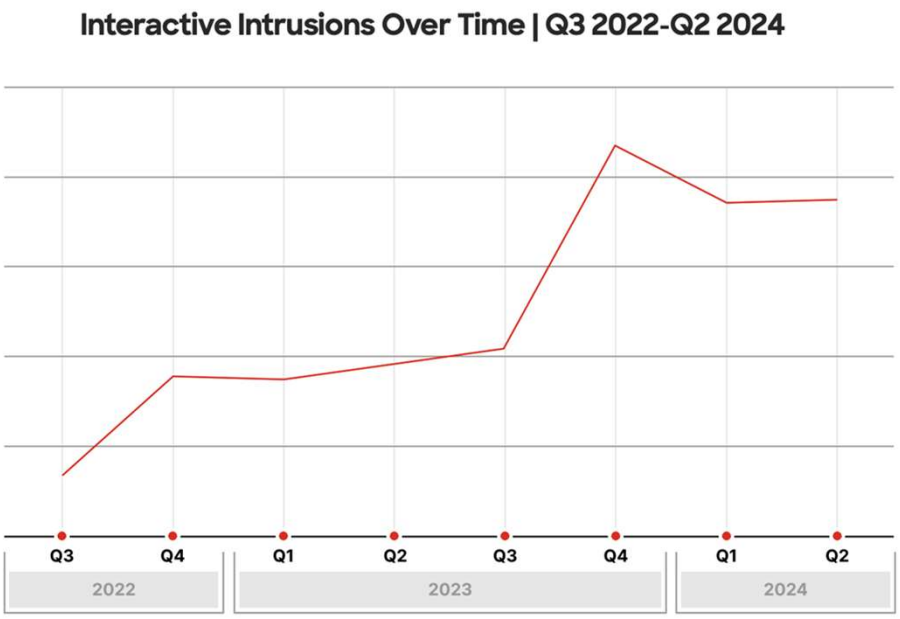
70% increase in the use of legitimate RMM tools

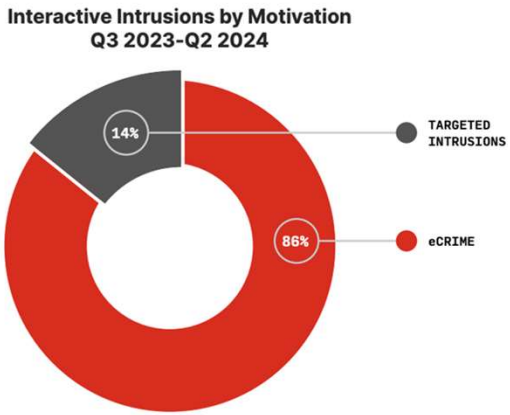
5 of the top 10 MITRE tactics observed were identity-based

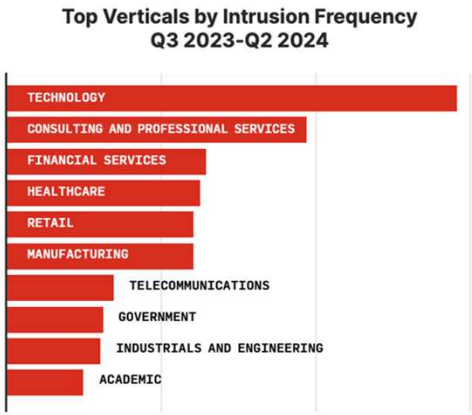
142% increase in access broker advertisements targeting healthcare

75% increase in cloud intrusions

CROWDSTRIKE





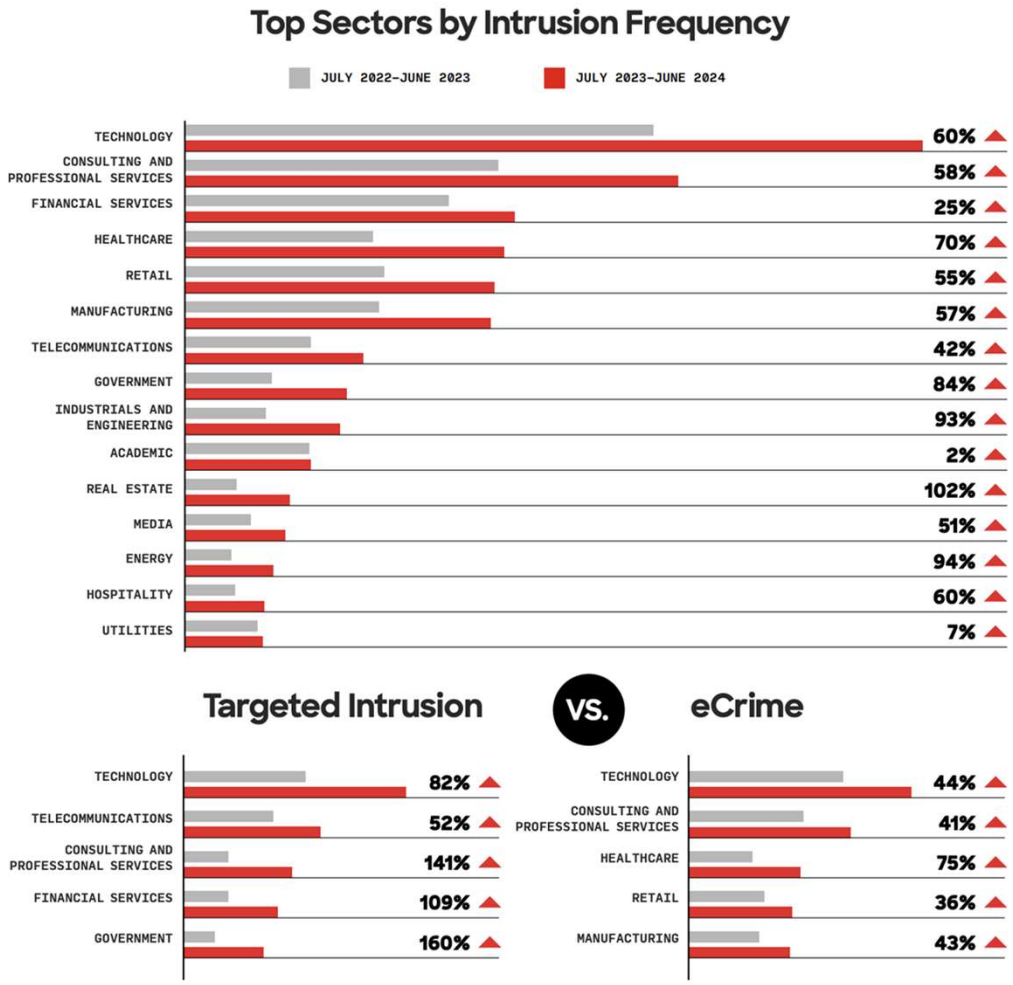


Interactive Intrusions

>>

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.

CROWDSTRIKE



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%)**

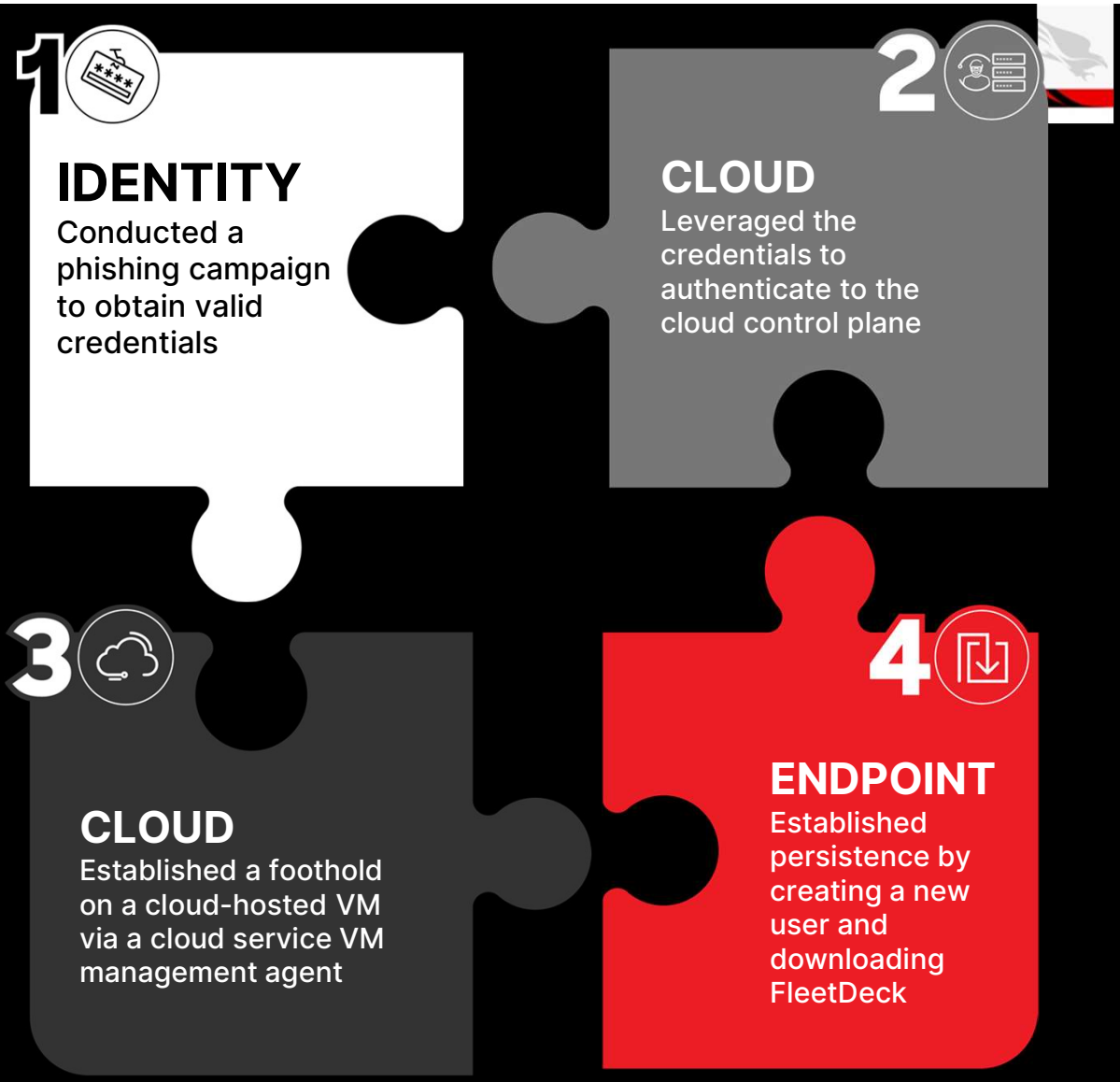
CROWDSTRIKE

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

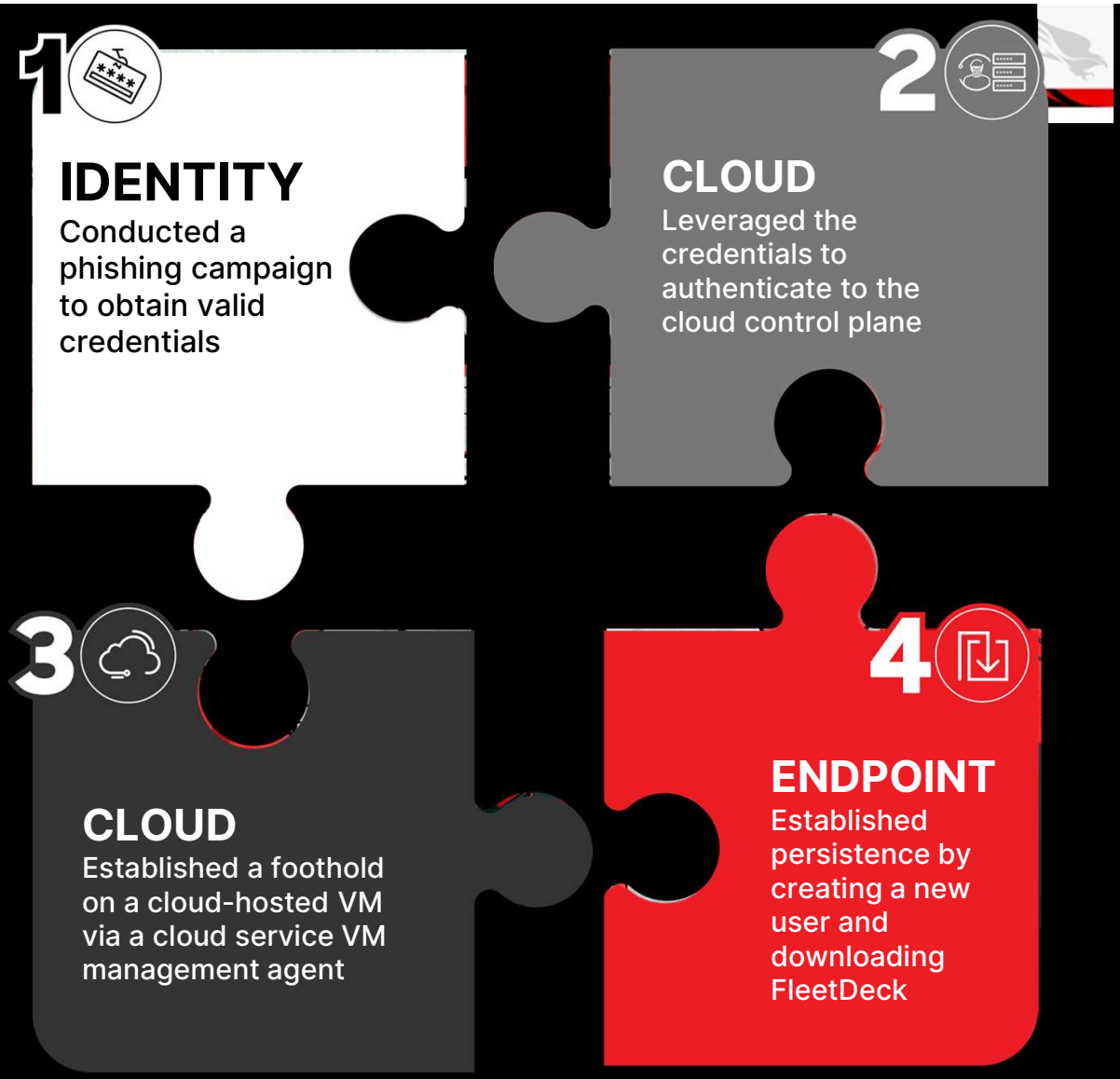
Having full insight into telemetry spanning endpoint, identity and cloud environments is a force multiplier to hunt cross-domain attacks



CROWDSTRIKE

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

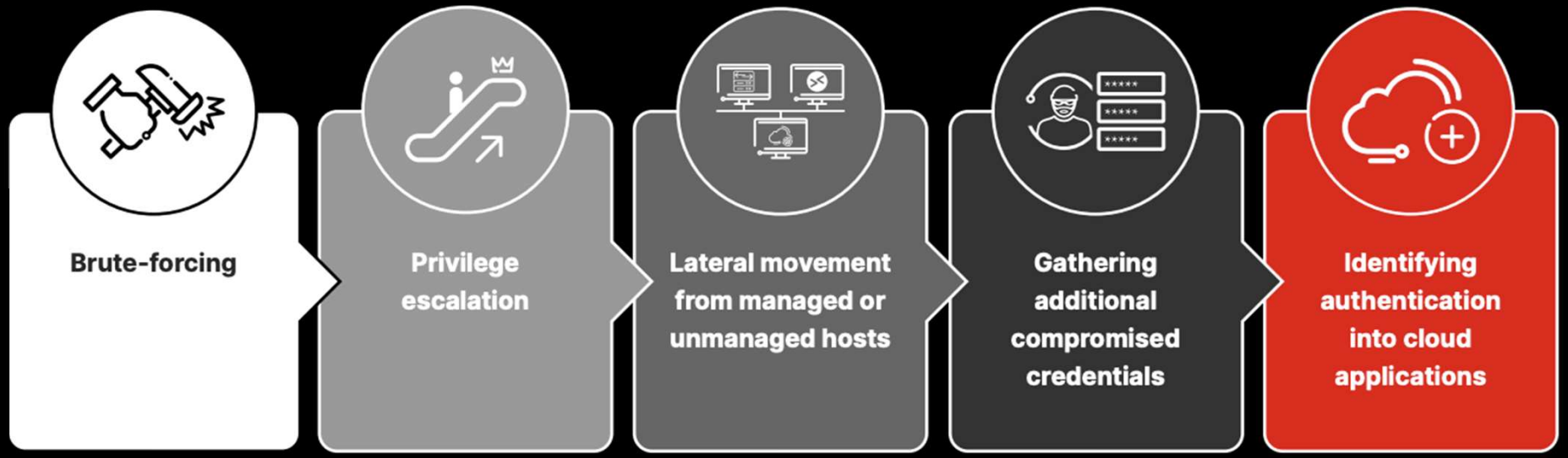


CROWDSTRIKE

Stealthy Adversaries Exploit Legitimate Credentials to Gain Access

Surge in access broker advertisements

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



CROWDSTRIKE

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.

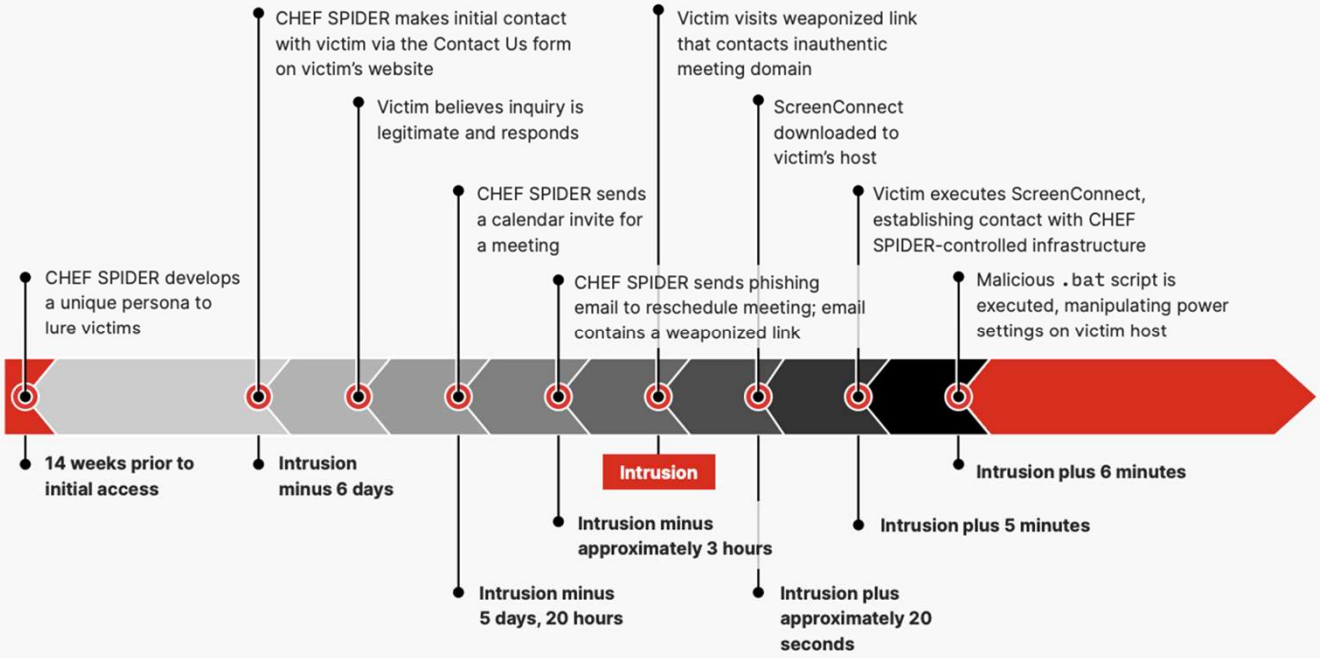
CROWDSTRIKE

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

CROWDSTRIKE

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

CROWDSTRIKE

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

CROWDSTRIKE

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.

CROWDSTRIKE

FAMOUS CHOLLIMA

TACTICS, TECHNIQUES & PROCEDURES

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

MALWARE

- BeaverTail
- InvisibleFerret
- Open-source RMM tools

MALWARE

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

TARGET GEOGRAPHY

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

CROWDSTRIKE

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

FAMOUS CHOLLIMA

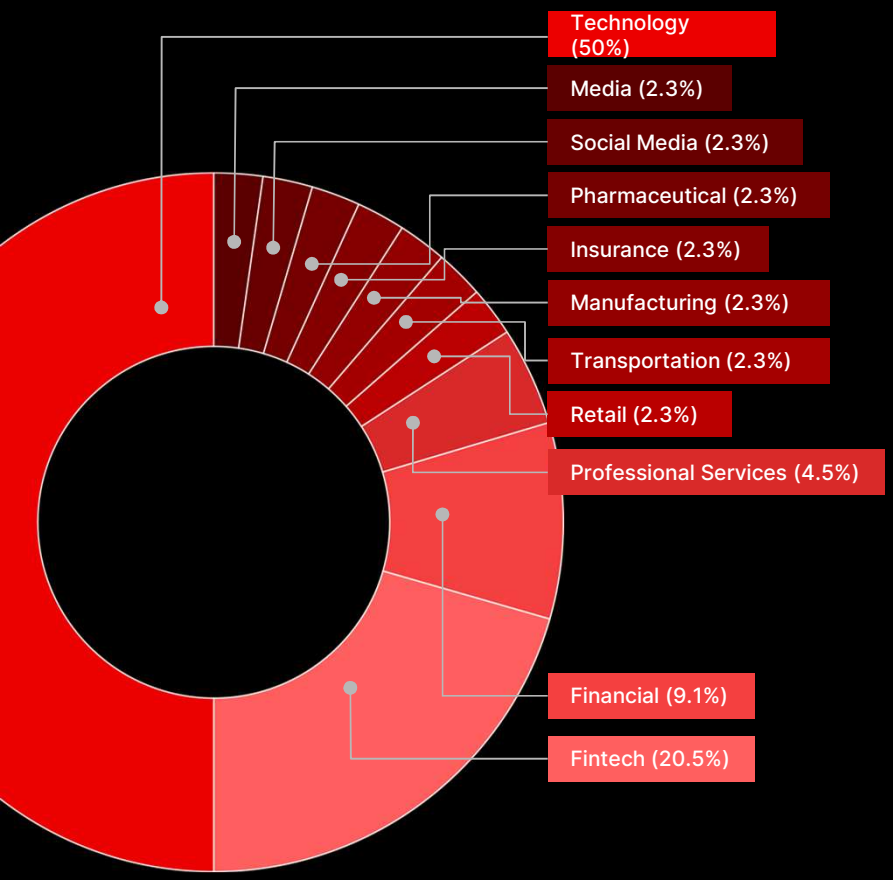
Malware Ops (BeaverTail & InvisibleFerret)

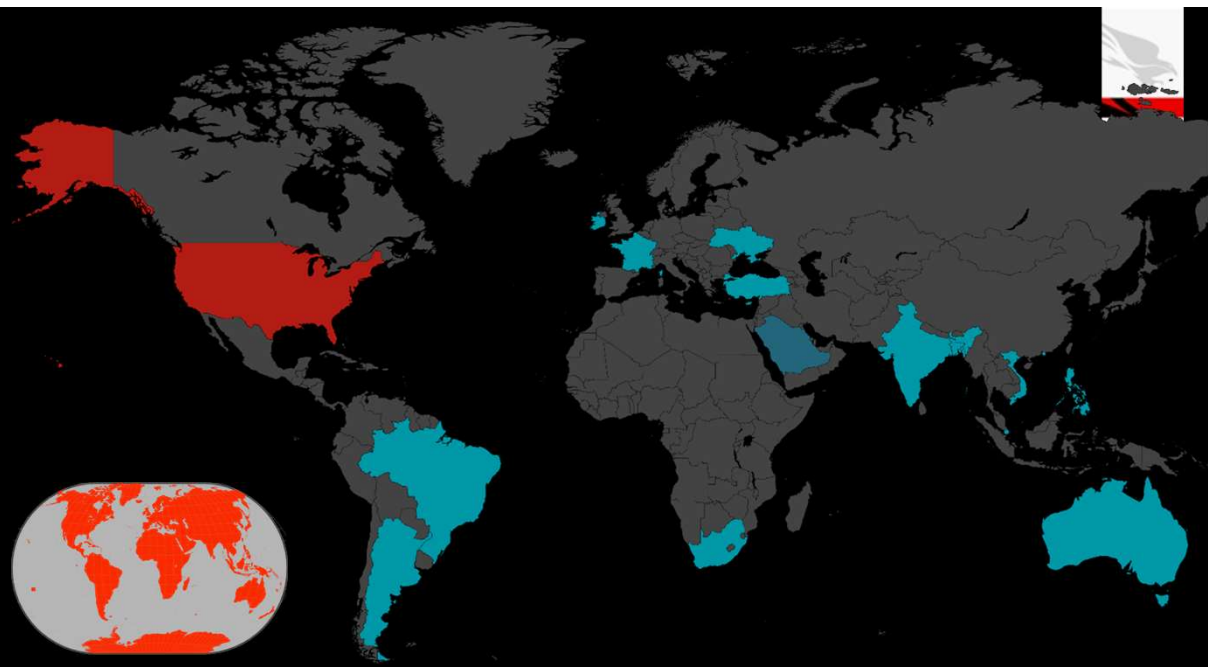
- Cryptocurrency Credential Theft
- Credit Card Information Theft
- Possible Data Exfil

IT Workers

- 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

CROWDSTRIKE

Kim Jong-un
(Supreme Leader)

- **KWP Cadre Department**
- **Foreign Ministry** (issues passports)

- **DPRK Cabinet**
  - Ministry of Public Health
  - Ministry of Physical Culture & Sports
  - Ministry of Posts & Telecommunications
  - Ministry of External Economic Relations
- **Office 39** (KWP)
  - External Construction General Bureau
  - Dae-Sung General Bureau
  - Un-Ha General Bureau
  - (8 more Bureaus)
- **Munitions Industry Department** (KWP)
  - Korea Computer Center
  - 75 Bureau
- **Finance Accounting Department** (KWP)
  - Hotel Management Department
- **Propaganda & Agitation Department** (KWP)
  - Mansudae Art Studio
- **Ministry of People's Armed Forces**
  - Reconnaissance General Bureau
  - General Political Bureau
    - Korean People's Army Fine Art Company

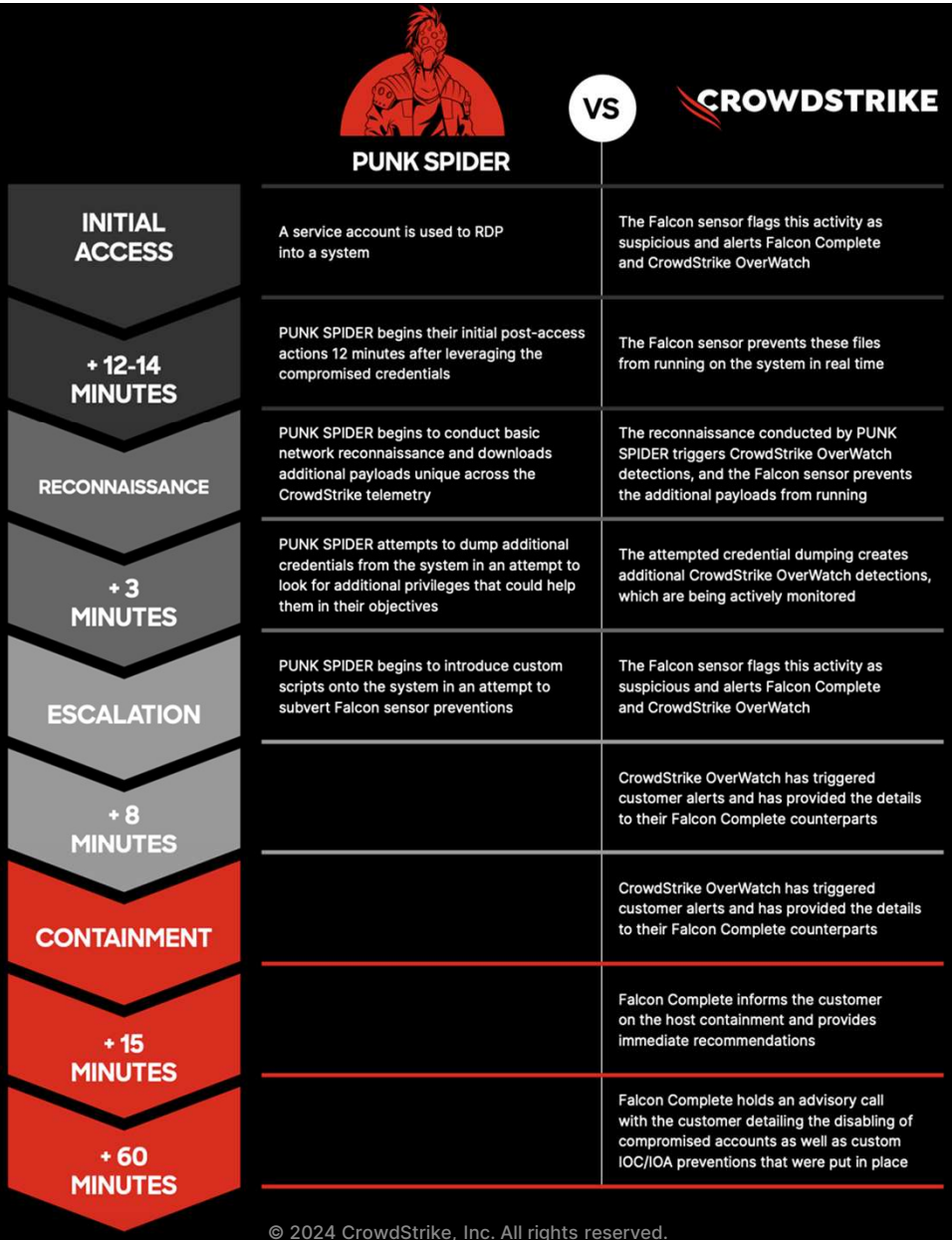
★Entities under the Cabinet must obtain permission from the Financial Planning Department separately

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

CROWDSTRIKE

Outlook

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



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.

CROWDSTRIKE

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

CROWDSTRIKE

Thank You

CROWDSTRIKE