

TECHNICAL CASE STUDY

Defend Against Insider Threats

How CrowdStrike Falcon Adversary OverWatch Protects Organizations from the Inside Out

What Are Insider Threats?

An insider threat originates from someone within your organization — whether they are a current or former employee, contractor or partner — who exploits legitimate access to harm the business. These threats are difficult to detect because they come from trusted individuals who already have legitimate access to an organization's systems, networks and data. Adversaries are exploiting the rise in remote work by submitting falsified documents and successfully navigating the hiring process to infiltrate organizations. Once inside, they conduct espionage, steal data or sabotage operations while remaining undetected.

The Impact of Insider Threats

Insider threats can lead to data theft, regulatory penalties and damaged trust. Adversary groups like Democratic People's Republic of Korea (DPRK)-nexus **FAMOUS CHOLLIMA** use insiders to steal information for harmful operations. The CrowdStrike OverWatch team recently uncovered FAMOUS CHOLLIMA insiders applying to or working at more than 150 organizations¹ and confirmed that data theft occurred in 50% of service engagements,² illustrating how insiders pose serious risks to reputation and finances.

CrowdStrike OverWatch detected an insider threat before the employee ever logged in, stopping the adversary within an hour of their laptop being connected.

ADVERSARY

FAMOUS CHOLLIMA

TOP INDUSTRIES

Technology, Fintech, Financial, Manufacturing

TOP REGIONS

United States, U.K., Australia

CHALLENGES

- **150+** companies targeted by FAMOUS CHOLLIMA insider threats¹
- **50%** of cases reviewed included data theft²
- **Up to an estimated \$44M** in potential losses avoided by CrowdStrike customers as a result of exposed insider threats,² in addition to prevention of IP theft and data breaches

SOLUTIONS

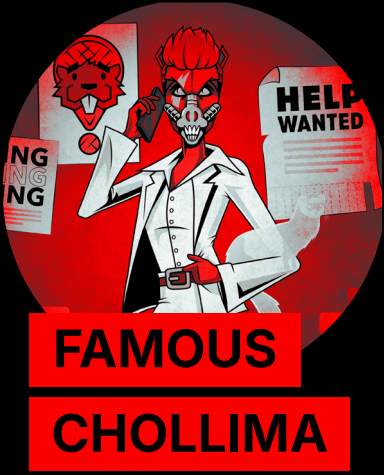
Falcon Adversary OverWatch delivers cutting-edge, real-time threat detection, combining comprehensive telemetry and expert human analysis to uncover insider threats. Through unparalleled visibility across organizations and close collaboration with law enforcement, CrowdStrike OverWatch threat hunters quickly detect malicious insiders and alert customers before serious damage occurs.

PRODUCTS & SERVICES

- CrowdStrike endpoint security
- CrowdStrike Falcon® Cloud Security
- CrowdStrike Falcon® Identity Protection
- CrowdStrike Falcon® Adversary OverWatch

¹ CrowdStrike 2024 Threat Hunting Report

² These statistics are based on internal assessments and customer feedback provided to CrowdStrike. Individual results may vary depending on specific customer environments and use cases.



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

© 2024 CrowdStrike, Inc. All rights reserved.


Identifying insider threats is challenging, especially with the rise of remote work. Traditional security defenses like firewalls and access controls focus on external attacks, but insiders with authorized access blend in easily. Malicious actors pass hiring checks using stolen identities, AI-generated resumes and good interviewing skills. Once hired, they use strategies — like the use of laptop farms — to mask their geolocation, appearing as local employees. These threats are often highly coordinated, with multiple insiders exploiting remote setups. Without global visibility, organizations struggle to connect the dots and detect these insider activities.

How Falcon Adversary OverWatch Hunts Down Insider Threats

Falcon Adversary OverWatch's intelligence-led threat hunting is critical in detecting deeply embedded insider threats. Here's how it mitigates these risks:

- 1. Global Telemetry and Detection:** CrowdStrike OverWatch correlates telemetry from multiple customer environments to identify patterns missed by individual organizations, such as malicious actors applying across different companies.
- 2. Advanced Monitoring:** Using the CrowdStrike Falcon® platform, CrowdStrike OverWatch conducts real-time monitoring and behavioral analysis to catch insider threats early, even during onboarding or at the first connection of their device.
- 3. Speed and Collaboration:** CrowdStrike OverWatch uses AI-powered detections to identify adversaries in minutes and partners with law enforcement to dismantle insider networks, ensuring rapid response against threats.

CrowdStrike OverWatch harnesses the power of the crowd to stop insider threats. Because insider threats lack clear, fingerprintable indicators, they are difficult to detect using traditional security measures. With global telemetry across CrowdStrike's customers, CrowdStrike OverWatch threat hunters can identify patterns that individual organizations may miss. Internal teams may attempt to track investigative leads, but this becomes impractical at scale. CrowdStrike OverWatch excels in correlating data across environments and promptly detecting insider threats.

CASE 1: Insider Threats Stopped Before the First Day on the Job



A customer unknowingly hired a DPRK IT worker, who was scheduled to start working in six days. The employee was hired through a contractor with insufficient security and background checks. By the fourth day, the shipped laptop arrived at a remote laptop farm and was connected to the network.

As soon as the laptop connected to the laptop farm, CrowdStrike OverWatch identified that the source IP matched another active insider threat case. CrowdStrike threat hunters observed that screen-sharing software and a browser-based sharing site were immediately configured. Upon examining the laptop telemetry, CrowdStrike OverWatch recognized the user as a compromised persona from previous cases.

CrowdStrike OverWatch triggered a detection and immediately alerted the customer by phone. The customer provided additional corroborating details, including the employee's CV and contact information, which further solidified the attribution. The customer promptly locked the DPRK insider from account access and terminated their employment the following morning.

Since CrowdStrike OverWatch detected the insider pre-employment, the organization avoided wage losses and prevented the DPRK malicious actor from gaining access to its internal systems and sensitive data, which would have been accessible to this specific IT worker.

CASE 2: Identity Telemetry Leveraged to Detect Insider Threats

In a related case, Falcon Adversary OverWatch detected another insider threat using a slightly different approach — this time, without an endpoint involved. Instead, CrowdStrike OverWatch hunted on Active Directory traffic and metadata collected by CrowdStrike Falcon® Identity Protection to detect single sign-on (SSO) login attempts from a DPRK-linked laptop farm.

By correlating the Active Directory user names with previously identified compromised identities, CrowdStrike threat hunters were able to detect and attribute the threat as soon as they were issued an Active Directory account and began using SSO. This identity-based detection allowed CrowdStrike OverWatch to stop the insider before they could gain significant access to the customer's resources.

Up to an estimated

\$44M

in potential losses were avoided by CrowdStrike customers as a result of exposed insider threats,² and IP theft and data breaches were prevented

How You Can Mitigate Advanced Threats

Combating advanced threats like malicious insiders requires a robust, multi-layered security strategy. CrowdStrike delivers comprehensive cross-domain detection and response by combining real-time detection with proactive threat hunting across identities, endpoints and cloud environments.

- **Core Detection and Response:** Protect against sophisticated attacks using **CrowdStrike endpoint security**, **Falcon Cloud Security** and **Falcon Identity Protection**. These solutions provide continuous monitoring and automated threat detection across all key entry points. With real-time visibility into endpoints, cloud workloads and user identities, CrowdStrike enables you to detect and stop breaches.
- **Falcon Adversary OverWatch Cross-Domain Threat Hunting:** Stop breaches everywhere with 24/7 proactive threat hunting powered by AI and industry-leading adversary intelligence. By leveraging unified visibility across clouds, identities and endpoints, CrowdStrike experts hunt threats across domains, monitoring for compromised users in cloud attacks and tracking lateral movement between cloud and endpoint. CrowdStrike OverWatch breaks down silos, significantly reducing complexity and accelerating response time for customers.

Protect your organization from every angle. Experience the power of CrowdStrike Falcon Adversary OverWatch and stop advanced threats before they cause reputational and financial damages.

Additionally, **CrowdStrike Insider Risk Services** provide organizations with a robust framework to anticipate, detect and respond to insiders. These services combat intentional and unintentional risks, from negligence and disgruntled employees to nation-state-aligned adversaries like FAMOUS CHOLLIMA. With specialized offerings, including incident response, technical assessments, program reviews, tabletop exercises and red team simulations, CrowdStrike empowers organizations to identify vulnerabilities, enhance access controls and fortify defenses against insider risks.

Attend a hands-on
workshop →

Request a demo →

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: <https://www.crowdstrike.com/>

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

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