

CrowdStrike 2026 Legal Threat Landscape Report: Cybercriminals Blur Digital and Physical Lines in Attacks on U.S. Law Firms

October 28, 2026

CHATTY SPIDER activity surges 129% as adversaries recruit individuals to infiltrate law firms, targeting privileged client information for data theft and extortion

AUSTIN, Texas--(BUSINESS WIRE)--Oct. 28, 2026-- [CrowdStrike](#) (NASDAQ: CRWD) today released the [CrowdStrike 2026 Legal Threat Landscape Report](#), revealing that financially motivated adversaries accounted for 82% of observed malicious activity against the legal sector, with [CHATTY SPIDER](#) emerging as a dominant threat to U.S. law firms. Cybercriminals are finding new ways to monetize the sector, escalating from social engineering to physical intrusions to steal and turn sensitive client information into profit.

Adversaries are compressing the time from initial access to data theft, and as AI capabilities advance that window will only shrink, leaving defenders with less time to stop attacks. With privileged access to client communications, intellectual property, and corporate transactions, law firms serve as gateways to sensitive intelligence that cybercriminals can exploit, putting the businesses and government organizations they represent at risk.

CrowdStrike Legal Threat Landscape Report Highlights:

Based on frontline intelligence from CrowdStrike [Counter Adversary Operations](#) tracking more than 290 named adversaries, the report reveals:

- **Cybercrime Group Targets Firms with Increasing Aggression:** CHATTY SPIDER represented the dominant threat to legal entities with malicious activity growing 129%. In one intrusion, the group recruited an individual to impersonate IT staff and physically infiltrate law firms to establish remote access. In another, the adversary attempted to exfiltrate sensitive data just four minutes after gaining initial access, highlighting the speed of its operations.
- **Legal Entity Extortion Surges:** Big Game Hunting adversaries named 455 legal entities on data leak sites, a 39% year-over-year increase. Financially motivated adversaries accounted for the majority of observed activity against the legal sector, exploiting the highly confidential nature of client information to maximize extortion pressure.
- **SPIDERS Expand Identity-Based Attacks:** [SNARKY SPIDER](#) and [CORDIAL SPIDER](#) targeted law firms through identity-based attacks, exploiting trusted access to SaaS applications for data theft and extortion. Both adversaries targeted the same law firm just one month apart, highlighting the convergence of criminal groups on high-value legal targets.
- **China-Nexus Adversaries Intensify Espionage Operations:** As China-nexus adversary diversity doubled in the legal sector, [TITAN PANDA](#) conducted the first observed exploitation of legal-sector-specific billing software. [WARP PANDA](#) leveraged an ESXi zero-day for covert access. [MURKY PANDA](#) conducted large-scale password spraying, targeting nearly 500 accounts at a single U.S. law firm from 300 IP addresses over 30 days, demonstrating the scale and persistence of China-nexus operations.

"Law firms are the new ATM for cybercriminals. Adversaries are exploiting the value of privileged client information, and they're willing to go beyond the keyboard to get it," said Adam Meyers, head of counter adversary operations, CrowdStrike. "We're seeing criminals recruit individuals to physically infiltrate law firms, blurring the line between digital and physical attacks. Defenders need visibility across identities, endpoints, and cloud environments to detect and disrupt these operations before access turns into extortion."

Additional Resources:

- Download the [CrowdStrike 2026 Legal Threat Landscape Report](#).
- Listen to the [Adversary Universe podcast](#) for insights into threat actors and recommendations to amplify security.
- To learn more, read our [blog](#) or visit us [online](#).

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](#) | [Instagram](#)

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

© 2026 CrowdStrike, Inc. All rights reserved. CrowdStrike and CrowdStrike Falcon are marks owned by CrowdStrike, Inc. and are registered in the United States and other countries. CrowdStrike owns other trademarks and service marks and may use the brands of third parties to identify their products and services.

View source version on businesswire.com: <https://www.businesswire.com/news/home/20261028008406/en/>

Media Contact

Jake Schuster

CrowdStrike Corporate Communications

press@crowdstrike.com

Source: CrowdStrike