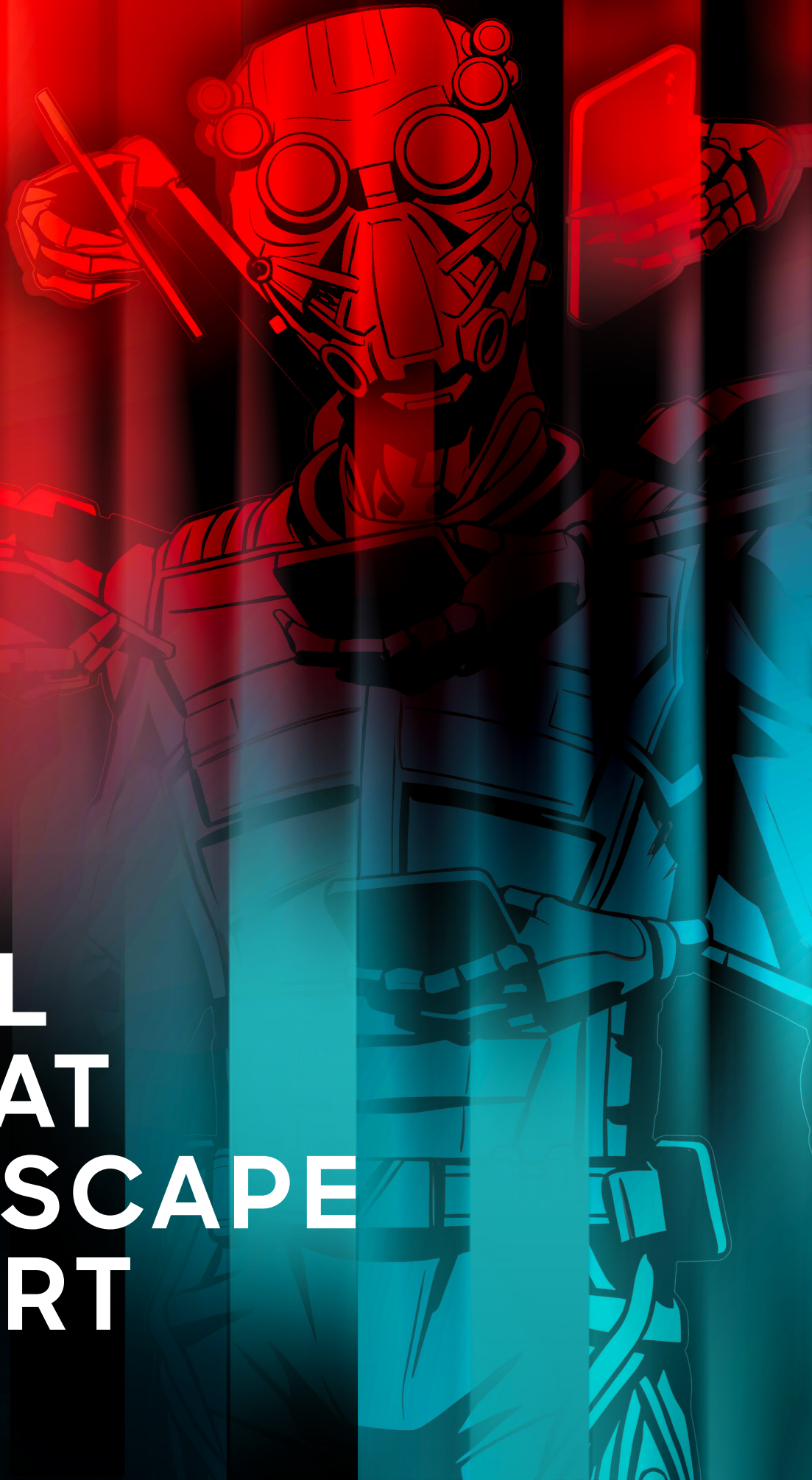




2026 LEGAL THREAT LANDSCAPE REPORT

Table of Contents

- Introduction3
- Adversary Naming Conventions5
- Sector Profile6
 - Data Snapshot7
- Top Adversary Threats9
- eCrime10
 - Big Game Hunting10
 - eCrime Highlights12
 - Enabling and Commodity Threats14
- Nation-State15
 - China15
 - DPRK18
 - Russia19
 - Iran20
- Non-State21
- Outlook22
- Recommendations24

Introduction

The legal sector faces persistent and multifaceted cyber threats. Intrusions conducted by both eCrime and nation-state threat actors targeting legal entities in 2026 have nearly doubled compared to the 2023 baseline. This reflects the sector's strategic value: Law firms hold privileged communications, merger and acquisition details, intellectual property, government matters, and financial records, making them attractive to adversaries seeking financial gain and long-term strategic intelligence alike. The consequences of a breach can extend well beyond the incident itself, carrying regulatory, reputational, and client retention risks that can persist for years.

The CrowdStrike 2026 Legal Threat Landscape Report presents analysis covering activity observed from September 1, 2025, through August 31, 2026. The report details the key themes, trends, and events shaping the legal sector threat landscape and provides anticipatory assessments to help organizations prepare for the continued evolution of eCrime and nation-state threats. In addition to threat analysis, the report provides actionable recommendations to help legal sector security and leadership teams prioritize investments and strengthen resilience.

eCrime activity, driven primarily by [CHATTY SPIDER](#), represents the dominant threat to legal sector entities. Their laser focus on the sector represents a persistent throughline, with malicious activity growing 129% in the first eight months of 2026 compared to all of 2024, when the adversary was first observed targeting legal entities. CHATTY SPIDER has demonstrated a consistent pattern of surges and dormancy periods while continuously evolving their tactics, techniques, and procedures (TTPs), escalating from callback phishing in 2024 to voice phishing (vishing), Quick Assist abuse, and, most recently, physical intrusion at law firm locations.

In the reporting period, eCrime accounted for 82% of all malicious activity targeting legal entities. Big game hunting (BGH) adversaries named 455 legal entities on dedicated leak sites (DLSs), a 39% increase from the prior 12-month reporting period. In addition to CHATTY SPIDER, BGH adversaries [SNARKY SPIDER](#) and [CORDIAL SPIDER](#), as well as initial access broker (IAB) [HERALD SPIDER](#), all heavily targeted the sector during the reporting period.

Nation-state threat actors accounted for approximately 18% of all incidents observed targeting the legal sector during the reporting period, nearly one in five attributed intrusions. China-nexus adversaries represent the bulk of this activity, with [WARP PANDA](#), [TITAN PANDA](#), [OVERCAST PANDA](#), and [MURKY PANDA](#) all conducting targeted operations against legal entities. These adversaries demonstrated increasing operational sophistication, progressing from large-scale credential validation to zero-day exploitation of enterprise virtualization infrastructure, targeted abuse of legal-specific software, and precision intelligence collection against executive-level personnel. Though the volume of China-nexus activity targeting the sector has remained relatively consistent over the years, the number of threat actors targeting the sector has nearly doubled from 2023 to 2026, potentially highlighting its increasing importance.

Additional nation-state threats include Democratic People's Republic of Korea (DPRK)-nexus adversary [FAMOUS CHOLLIMA](#). The adversary employs a dual-track approach of IT worker insider threat schemes and malware operations specifically targeting named Am Law firms, suggesting both deliberate intelligence collection and financial motivations. Though the adversary is broadly opportunistic and generally sector-agnostic in targeting, their activities nonetheless represent a credible threat to legal sector entities. Russia-nexus, Iran-nexus, and non-state threat actors all targeted the sector only in limited circumstances during the reporting period.

Together, these trends highlight the breadth and sophistication of threats facing the legal sector. As AI capabilities advance, adversaries will likely accelerate the scale and sophistication of their operations, compressing the time available for detection and response. This environment demands continuous, intelligence-driven defense rather than a reactive posture.

[CrowdStrike Counter Adversary Operations](#) combines threat intelligence, managed threat hunting, and trillions of telemetry events from the AI-powered [CrowdStrike Falcon® platform](#) to detect, disrupt, and stop evasive adversaries. Counter Adversary Operations comprises two closely integrated teams. The CrowdStrike Intelligence team, which provided the analysis for this report, identifies new adversaries, tracks malicious activity, and captures emerging cyber threat developments in real time. The CrowdStrike OverWatch team applies this intelligence through proactive threat hunting across customer telemetry to detect and disrupt malicious activity. Together, these teams deliver intelligence and hunting capabilities that help legal sector organizations stay ahead of sophisticated adversaries.

Explore the
[CrowdStrike
Adversary Hub](#)
for the latest
insights on
adversaries,
tradecraft,
and activity.

ADVERSARY NAMING CONVENTIONS

**BEAR**

RUSSIA

**BISON**

BELARUS

**BUFFALO**

VIETNAM

**CHOLLIMA**

DPRK [NORTH KOREA]

**CRANE**

ROK [REPUBLIC OF KOREA]

**HAWK**

SYRIA

**JACKAL**

HACKTIVIST

**KITTEN**

IRAN

**LEOPARD**

PAKISTAN

**LYNX**

GEORGIA

**OCELOT**

COLOMBIA

**PANDA**

PEOPLE'S REPUBLIC OF CHINA

**SAIGA**

KAZAKHSTAN

**SPHINX**

EGYPT

**SPIDER**

eCRIME

**TIGER**

INDIA

**WOLF**

TÜRKIYE

Sector Profile

The legal sector provides services for the study, development, and application of law. The sector comprises law firms, legal service providers, and in-house legal departments that handle confidential client matters, regulatory compliance, litigation, contracts, and intellectual property protection.

Threat actors across all motivations target legal entities because of the extraordinarily sensitive client data they possess. This includes privileged communications, intellectual property, merger and acquisition details, litigation strategies, and financial information that can be sold on criminal markets or exploited for espionage, extortion, or competitive advantage.

Legal firms also serve as high-value pivot points to access their clients' networks and data. This makes them attractive targets for nation-state threat actors seeking intelligence on government or corporate matters and for eCrime threat actors conducting ransomware attacks or data theft. Additionally, the confidential nature of legal work creates significant pressure to pay ransoms quickly to prevent reputational damage and regulatory consequences from data breaches.

LIKELY LEGAL SECTOR TARGETING MOTIVATIONS

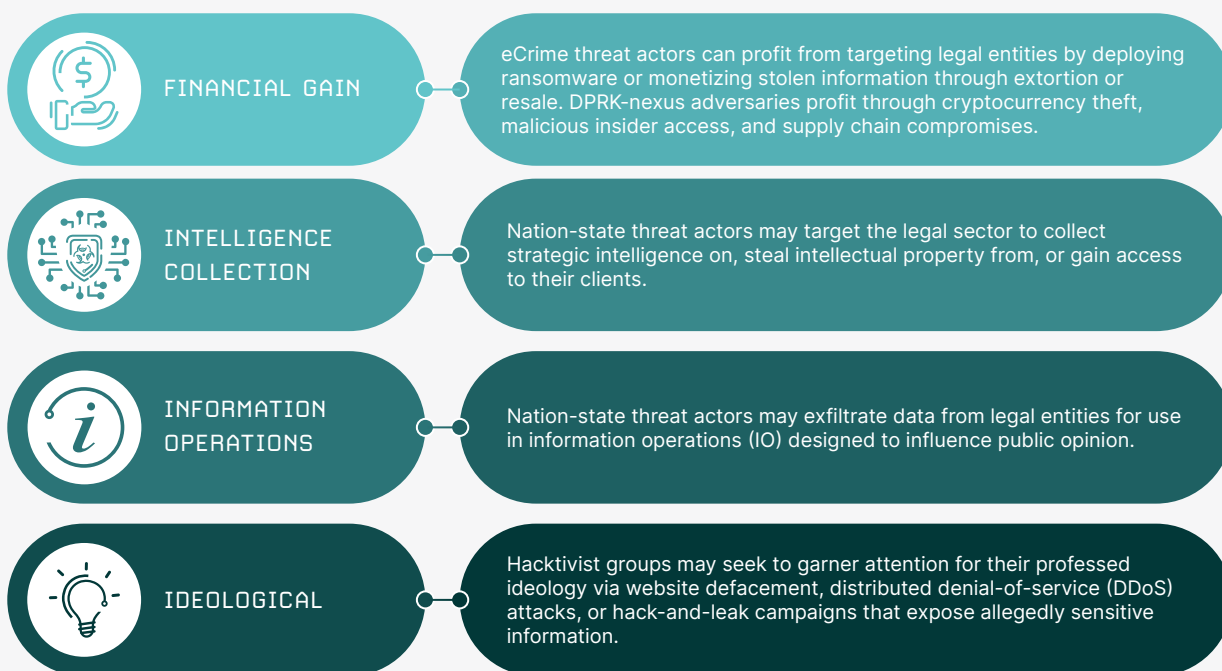


Figure 1. Likely motivations for targeting legal entities

Data Snapshot

Figure 2 depicts malicious activity against the legal sector that CrowdStrike OverWatch, CrowdStrike Falcon® Complete, and CrowdStrike Services observed from September 1, 2025, to August 31, 2026.

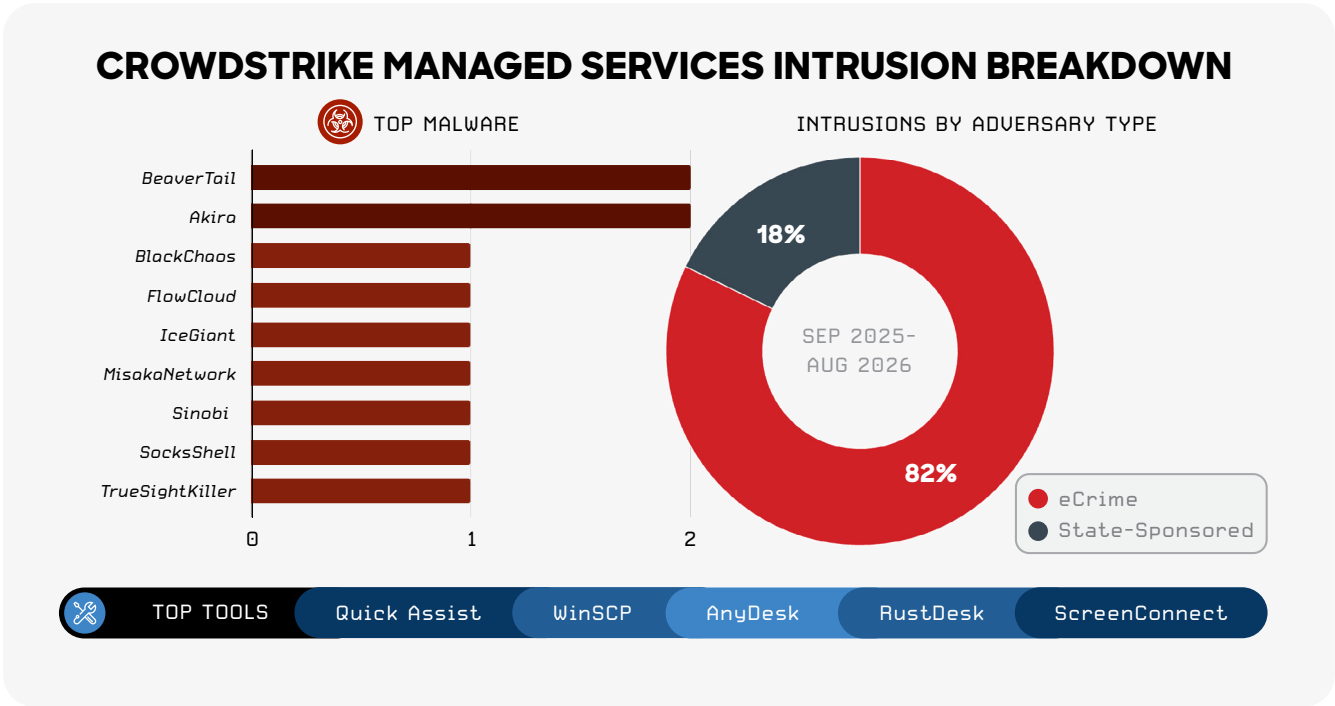


Figure 2. CrowdStrike Managed Services legal sector intrusion breakdown, September 1, 2025, to August 31, 2026

Figure 3 provides a geographic overview of adversaries that targeted the legal sector during the reporting period, as reported in CrowdStrike Intelligence finished intelligence reports.



Figure 3. CrowdStrike Intelligence legal sector threat landscape overview, September 1, 2025, to August 31, 2026



Top Adversary Threats

During the reporting period, the following adversaries posed a persistent threat to the legal sector. Based on analyzed targeting trends, these adversaries represent the top threats to the legal sector for 2026 and into 2027. The following sections offer detailed discussions of these adversaries as well as others that targeted legal entities.

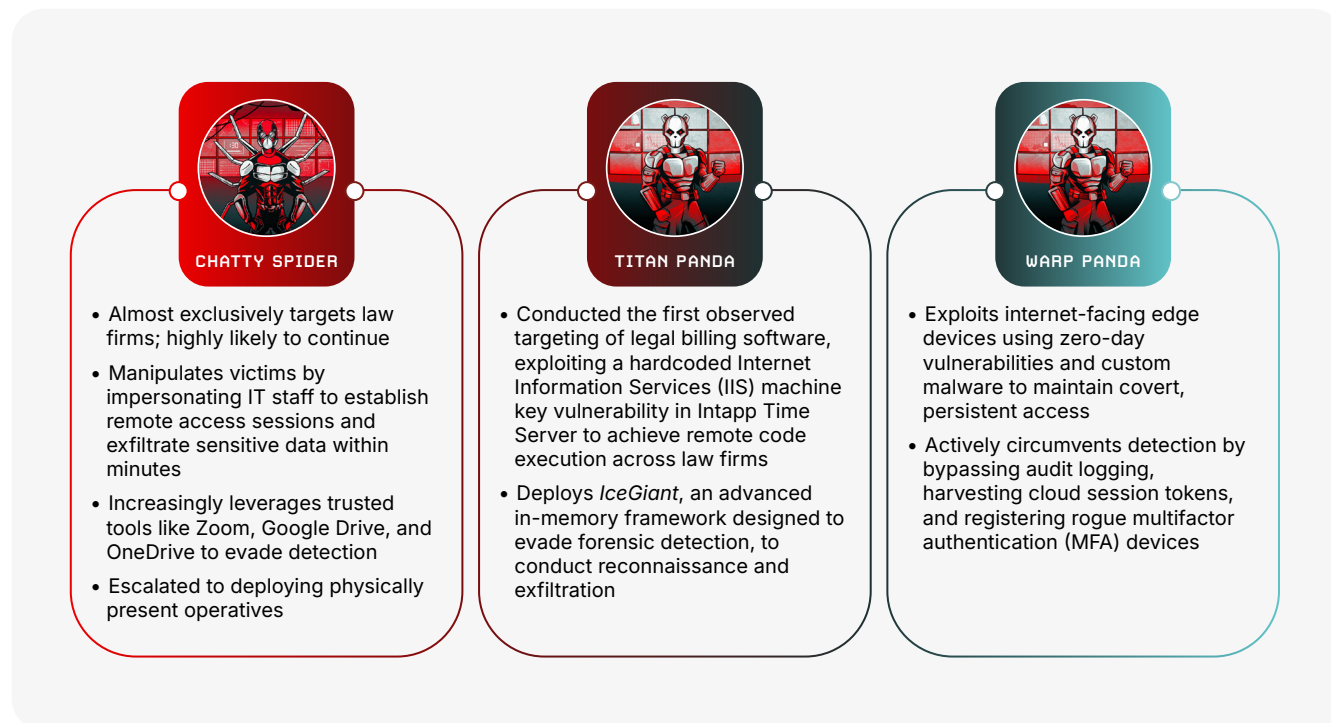


Figure 4. Top adversary threats to the legal sector, September 1, 2025, to August 31, 2026

eCrime

eCrime operations continue to target legal entities, as these entities possess a substantial amount of monetizable sensitive information, including personally identifiable information (PII) such as Social Security numbers, bank details, and medical records. Additionally, legal entities store high-value corporate data such as trade secrets and intellectual property. CrowdStrike Intelligence has observed threat actors target the legal sector in BGH operations and via enabling and commodity services.

Big Game Hunting

BGH adversaries gain initial access to victims via various techniques, including leveraging exploits, brute-forcing account credentials, and procuring network access from IABs. After gaining access, these adversaries often deploy ransomware, steal data, and threaten to publicly expose the stolen data on DLSSs, leveraging the victims' need to avoid the financial and reputational consequences associated with data leaks.

From September 2025 to August 2026, BGH adversaries named 455 legal entities on various DLSSs, a 39% increase from the 327 legal entities named in the prior 12-month reporting period.

Though BGH adversaries are opportunistic in nature, this increase, paired with a 36% increase in BGH activity across all sectors in the current reporting period, indicates legal entities remain a popular sector to opportunistically target.

During the reporting period, most legal entities impacted by BGH activity were North America-based. Figure 5 details the number of BGH incidents impacting legal entities each month, the top adversaries targeting the sector, and the top regions targeted by BGH adversaries from September 2025 to August 2026.

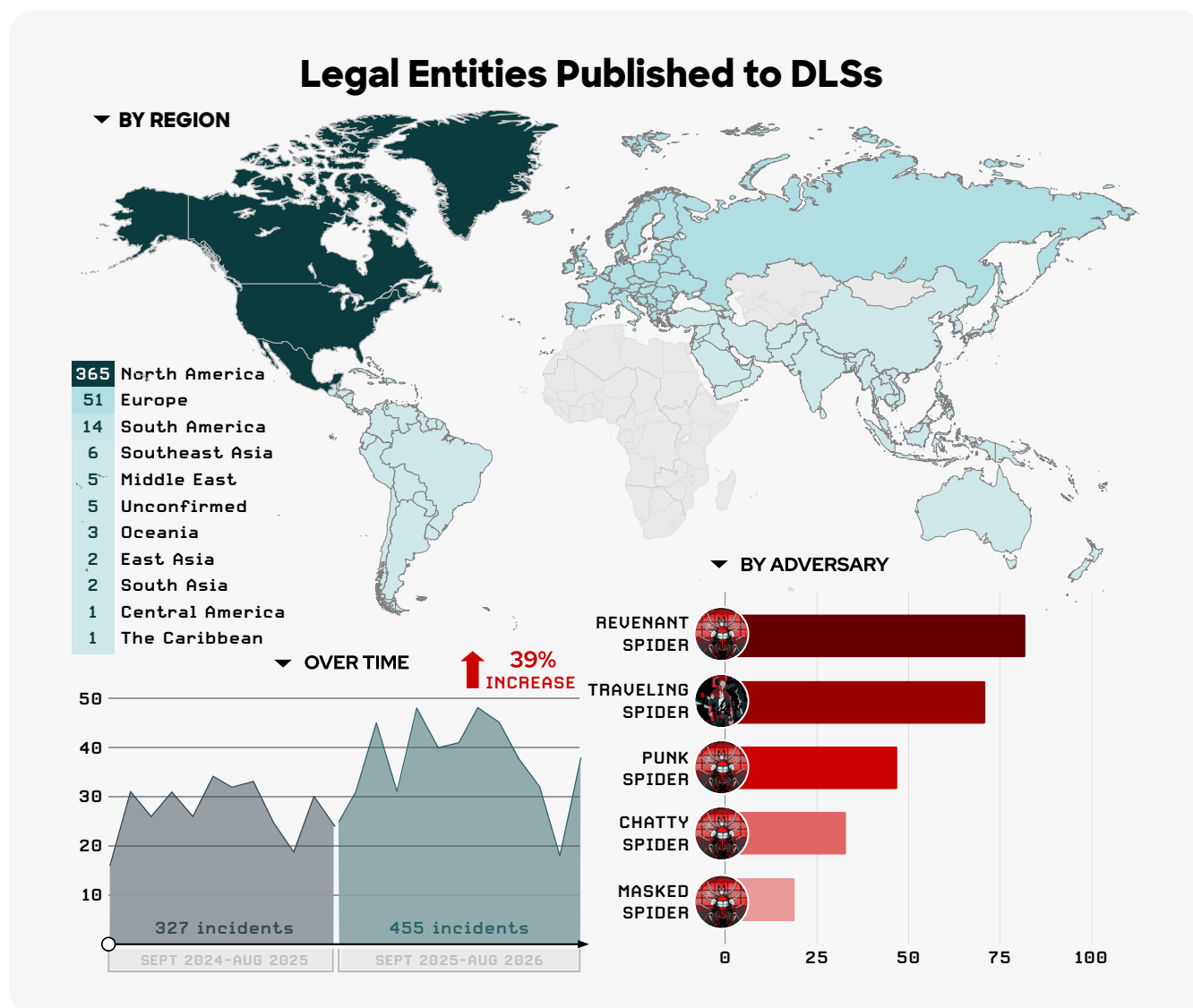


Figure 5. Top adversaries, top regions, and incident numbers for the legal sector, September 1, 2025, to August 31, 2026

The legal sector had the eighth-highest number of entities posted on BGH adversaries' DLSs in both the current and previous reporting periods. [REVENANT SPIDER](#) affiliates, [TRAVELING SPIDER](#) affiliates, [PUNK SPIDER](#), CHATTY SPIDER, and [MASKED SPIDER](#) represent major threats to the legal sector. During the reporting period, these adversaries posted the most legal entities to their respective DLSs. REVENANT SPIDER operates the *Qilin* ransomware as a service (RaaS), and TRAVELING SPIDER operates the *INC*, *Lynx*, and *Sinobi* RaaS programs. PUNK SPIDER, CHATTY SPIDER, and MASKED SPIDER are not known to operate RaaS programs.

CrowdStrike Intelligence assesses that BGH operations will remain a significant threat to legal entities throughout the next 12 months. This assessment is made with high confidence based on the following factors:

- Incidents impacting legal entities increased by 39% in the current reporting period compared to the previous reporting period
- The legal sector was among the top 10 sectors most frequently targeted by eCrime operations in both the current and previous reporting periods
- BGH adversaries will likely continue to opportunistically target legal entities

eCrime Highlights

CHATTY SPIDER's Persistent Targeting of U.S.-Based Law Firms

CHATTY SPIDER's malicious activity increased 129% in the first eight months of 2026 compared to all of 2024 across CrowdStrike's managed services' telemetry and findings, reflecting a significant escalation in the adversary's operational tempo. In the reporting period, CHATTY SPIDER almost exclusively targeted U.S.-based law firms. The adversary typically resumes data theft and extortion campaigns following a mid-year hiatus; however, CHATTY SPIDER returned from this break slightly earlier than usual in 2026.

Their operations demonstrated speed and efficiency by establishing remote access, identifying files of interest, and exfiltrating data in compressed time frames. **In one 2025 intrusion, the adversary attempted to exfiltrate data just four minutes after gaining initial access.** Like many extortion actors, CHATTY SPIDER threatens to leak stolen data on their clearweb DLS if negotiations are unsuccessful.

Throughout this period, CHATTY SPIDER impersonated legitimate IT staff to persuade targeted attorneys or their assistants to establish remote support sessions via legitimate remote monitoring and management (RMM) tools such as Zoho Assist, Quick Assist, AnyDesk, RustDesk, LogMeln Rescue, and, more recently, the remote meeting software Zoom and Cisco Webex. These remote sessions allow the adversary to browse workstations for sensitive data of interest. CHATTY SPIDER has historically exfiltrated stolen data via WinSCP; however, most observed intrusions in 2026 have involved exfiltration via cloud-based file-sharing sites such as Google Drive and OneDrive.

CHATTY SPIDER tends to gradually change their tradecraft; sudden escalations in TTPs are rare. However, in November 2025, the adversary hired a Russian national to physically access a U.S.-based law firm. The individual posed as an internal IT employee and was granted access to an onsite workstation, where he enabled the adversary to deploy RMM tools and attempted to exfiltrate data via cloud storage services. Law enforcement detained the individual during a second attempted visit the following day. Public reporting indicates the adversary used U.S.-based individuals to perform several physical intrusions during 2026.¹

CHATTY SPIDER consistently targets attorneys and administrative employees whose contact details are publicly available on firm websites. The adversary's focus on manipulating employee trust and use of legitimate tooling to gain access underscore their reliance on user execution. CHATTY SPIDER will likely continue to target the U.S.-based legal sector, an assessment made with high confidence based on the fact that **law firms constituted nearly 90% of victims in their intrusions during the reporting period.**

¹ <https://edition.cnn.com/2026/06/27/politics/cybercriminals-hire-burglars-russian-us-law-firms>

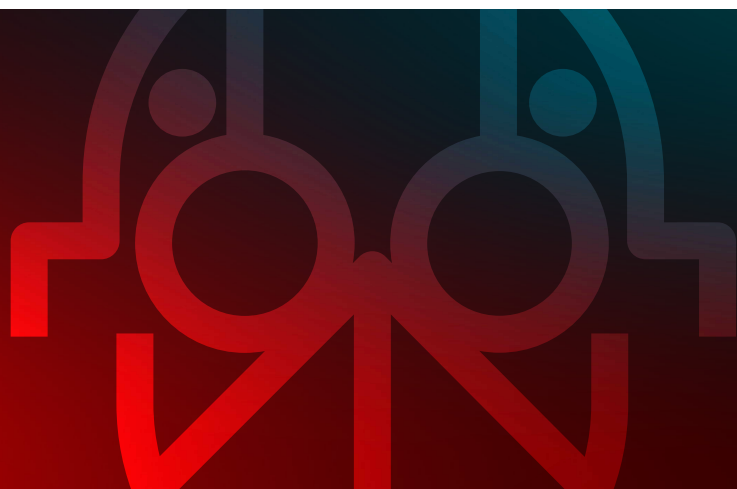
Emerging Threats to the Legal Sector: SNARKY SPIDER and CORDIAL SPIDER Target Law Firms in Data Theft and Extortion Campaigns

SNARKY SPIDER and CORDIAL SPIDER have targeted legal entities in their high-tempo data theft and extortion campaigns. In one case, both adversaries targeted the same law firm one month apart.

SNARKY SPIDER, which first emerged in October 2025 and significantly increased their operational tempo throughout January 2026, is a native English-speaking eCrime adversary linked to The Com, a primarily English-speaking online ecosystem comprising multiple interconnected subgroups. The adversary uses vishing calls to impersonate IT staff and direct employees to single sign-on (SSO)-themed phishing pages. After obtaining initial access, SNARKY SPIDER exfiltrates data exclusively from SSO-integrated SaaS applications and threatens to publish data unless the victim pays a ransom.

CORDIAL SPIDER, which began operations in November 2025 and significantly increased activity in January 2026, employs nearly identical TTPs as those of SNARKY SPIDER. These include vishing calls that impersonate IT personnel, citing the need to update SSO passkeys.

CORDIAL SPIDER's target profile spans the aviation, cryptocurrency, energy, financial services, hospitality, legal, real estate, technology, and transportation sectors, confirming their opportunistic nature. However, CrowdStrike Intelligence assesses the adversary will continue to target the legal sector. This assessment is made with high confidence based on their particular focus on law firms in recent activity.



Enabling and Commodity Threats

Initial Access Brokers

IABs provide other eCrime threat actors with services intended to expedite victim identification and access, ultimately resulting in increased profits and higher-tempo operations. Figure 6 provides insights into the IAB activity observed during the reporting period. Most advertised legal entities were based in the United States.

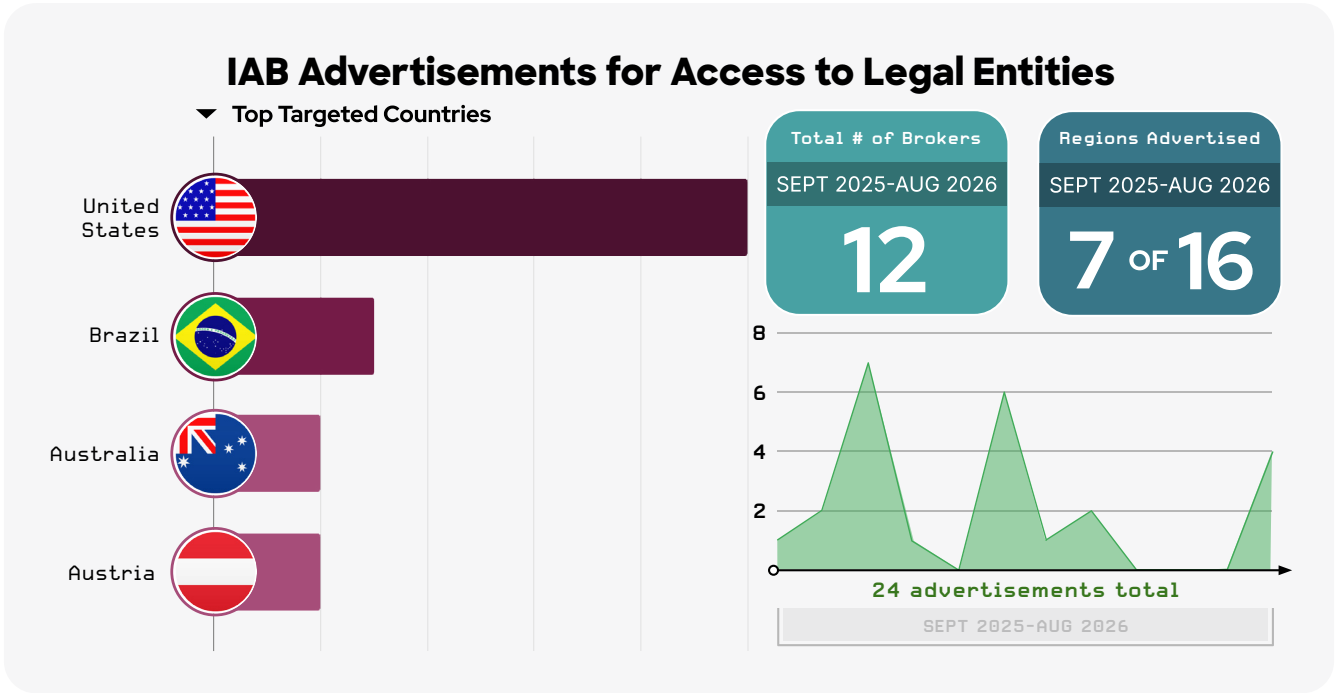


Figure 6. Summary of IABs targeting legal entities, September 1, 2025, to August 31, 2026

Throughout the reporting period, advertisements’ asking prices for legal entities ranged from 30 USD to 6,000 USD. The average advertisement price was 1,573.89 USD, and the median was 1,000 USD.

CrowdStrike Intelligence assesses that IABs will likely continue to opportunistically target legal entities throughout 2026 and 2027. Despite the decline in the number of legal entities advertised during the reporting period, this assessment is made with high confidence, as eCrime threat actors continue to use IAB services to access victim networks.

Nation-State

China



Figure 7. China-nexus legal sector threat landscape, September 1, 2025, to August 31, 2026

Multiple China-nexus adversaries conducted sustained cyber espionage campaigns against the legal sector throughout the reporting period. They demonstrated operational evolution across three key areas: zero-day exploitation of enterprise infrastructure, sophisticated cloud environment compromise, and targeted exploitation of legal-specific software.

Law firms, particularly those in regions of interest such as the U.S. and U.K., provide access to privileged client communications covering government matters, mergers and acquisitions, intellectual property disputes, and trade secrets critical for competitive and geopolitical advantage. They also serve as pivot points to access client networks aligned with Chinese Communist Party (CCP) priorities.

Major Operations During the Reporting Period

WARP PANDA Exploits Zero-Day, Enabling Malware Campaigns: Throughout 2025, CrowdStrike Intelligence discovered multiple WARP PANDA intrusions at U.S.-based entities, including several legal sector entities, in which the adversary deployed *BRICKSTORM*, *TetanusStorm*, *SharpStorm*, *DualGauge*, and *GuestConduit* in the victims' VMware vCenter environments. During several of these intrusions, and as late as early 2026, WARP PANDA exploited ESXi command logging bypass vulnerability CVE-2026-41709 as a zero-day, significantly reducing audit trail visibility.

TITAN PANDA Abuses Legal Billing Software: In April 2026, TITAN PANDA conducted the first observed targeting of legal sector-specific software. The adversary exploited a hardcoded IIS machine key vulnerability in Intapp Time Server, software almost exclusively used by law firms for timekeeping and billing. The adversary highly likely compromised a U.S. legal entity on April 20, 2026, and a U.S. technology entity on April 28, 2026, leveraging ViewState deserialization to achieve remote code execution (RCE) and deploy *IceGiant* reconnaissance modules. Default machine key reuse among IIS-based applications is a significant risk, as it can enable ViewState deserialization attacks against multiple organizations through common sector-specific server software. TITAN PANDA and other adversaries with prior access to these keys can therefore compromise legal sector organizations running publicly accessible Intapp Time Server installations with default configurations.

OVERCAST PANDA Targets Legal Executives: In September and October 2025, OVERCAST PANDA targeted executive-level employees at a U.K.-based legal firm, deploying *FlowCloud* malware on hosts assigned to director- and executive-level employees. This is consistent with Chinese intelligence collection priorities targeting key personnel with access to sensitive information and decision-making authority.

MURKY PANDA Leverages Operational Relay Box (ORB)² Network to Access Microsoft 365 Email Accounts, Conduct Password Spraying: While slightly outside the reporting period, MURKY PANDA's ORB28 password spraying campaign represented the largest-scale operation by target count. In July 2025, MURKY PANDA leveraged hundreds of compromised Zyxel-brand small office/home office (SOHO) routers to conduct credential validation attacks against Microsoft Azure environments. The campaign impacted more than 340 primarily U.S.-based entities across numerous sectors, with the legal sector among the most affected. The operation employed a highly distributed approach likely intended to evade detection.

One U.S. law firm experienced nearly 500 distinct failed login attempts to as many accounts from approximately 300 distinct IP addresses over a 30-day period.

These operations collectively demonstrate the Chinese intelligence community's increasing focus on the legal sector, progressing from opportunistic credential validation to sophisticated, sustained operations featuring zero-day exploitation, sector-specific targeting, and precision intelligence collection against executive-level personnel.

Adversary Highlight: WARP PANDA

WARP PANDA represents a sustained and strategically focused China-nexus cyber espionage threat to U.S. entities across multiple sectors, including the legal sector. The adversary typically exploits internet-facing edge devices to gain initial access, then pivots to VMware vCenter environments to deploy custom malware such as *BRICKSTORM* and *SharpStorm*, maintaining persistent covert access for extended periods of time. The legal sector's concentration of client communications, merger and acquisition materials, active litigation strategy, and cross-client access makes it a high-value collection target for a state-directed adversary seeking intelligence with downstream operational utility.

In some intrusions identified during the reporting period, WARP PANDA conducted targeted cloud operations, obtaining user session tokens to access Microsoft 365 environments without triggering credential-based alerts. In at least one case, the adversary registered a new MFA device on a compromised account, establishing a persistent foothold that would survive a password reset. This deliberate measure indicates the adversary anticipated and planned around partial remediation efforts.

² An ORB network is a traffic relay system (generally composed of a mix of compromised devices and leased servers) used to obfuscate the origin and destination of malicious traffic.

CrowdStrike Intelligence assesses with moderate confidence that WARP PANDA will continue to prioritize virtualization infrastructure and edge device vulnerabilities against legal and adjacent professional services entities through at least mid-2027. The adversary's demonstrated zero-day use and rapid adaptation following patching indicate ongoing investment in offensive capability development that is unlikely to diminish in the near term. Virtualization infrastructure and edge device attack surfaces will almost certainly remain primary initial access vectors given the adversary's established tooling investment in hypervisor-resident implants.

Adversary Highlight: TITAN PANDA

During the reporting period, TITAN PANDA exploited legal-specific software and demonstrated advanced understanding of IIS-based application vulnerabilities. Active since at least 2021, the adversary has compromised several North America-based legal firms since 2024. All affected firms shared customers in common sectors, including technology, energy, and manufacturing. This suggests TITAN PANDA targets these entities to enable follow-on intrusions aligned with broader intelligence collection objectives.

TITAN PANDA's operations centered on exploiting a hardcoded IIS machine key vulnerability in Intapp Time Server, a web-based application almost exclusively used by legal organizations running on IIS servers. On April 28, 2026, the adversary exploited default Intapp Time Server configurations at a U.S.-based technology entity, leveraging ViewState deserialization to achieve RCE and loading two *IceGiant* modules for comprehensive system reconnaissance. TITAN PANDA highly likely exploited the same vulnerability against a U.S.-based legal entity on April 20, 2026, to load a malicious .NET module. How TITAN PANDA obtained the default machine keys is unknown, though IIS compromise of a legal entity running Intapp Time Server may have exposed the hardcoded keys in the application's configuration file, enabling ViewState deserialization attacks against any organization running default installations.

TITAN PANDA employs *IceGiant*, an advanced, malicious in-memory .NET assembly framework running on IIS servers, for post-exploitation activities, including reconnaissance, persistence, lateral movement, and data exfiltration. *IceGiant* reflects extensive operations security (OPSEC) considerations: Components load directly into process memory, comprise encrypted data fragments stored across multiple IIS HTTP cache entries, and expire after a short period to remove evidence of activity. TITAN PANDA almost certainly conducts independent vulnerability research to enable initial access and deploy *IceGiant*, as they used two different zero-day SharePoint exploitation chains during 2026 operations and adapted the initial exploit chain after vendor patch releases.

CrowdStrike Intelligence assesses with high confidence that TITAN PANDA will continue to prioritize IIS-based application vulnerabilities against North American law firms through at least mid-2027. Legal entities using IIS-hosted applications with hardcoded or default machine key configurations will almost certainly remain high-priority targets given TITAN PANDA's demonstrated capability to leverage these credentials for persistent access and lateral movement to client networks.

DPRK

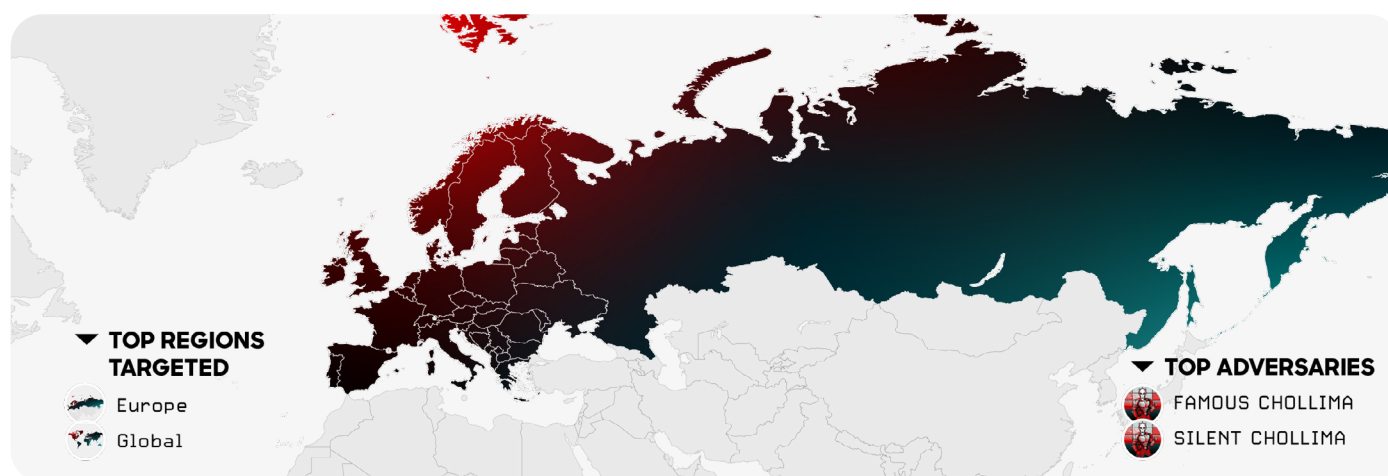


Figure 8. DPRK-nexus legal sector threat landscape, September 1, 2025, to August 31, 2026

DPRK-nexus adversaries conducted limited activity against the legal sector during the reporting period. In late January 2026, [SILENT CHOLLIMA](#) deployed their *TigerRAT* malware to a Europe-based public legal entity and reportedly attempted to access documents relating to anti-money laundering legislation. This targeting aligns with North Korea's ongoing cryptocurrency theft campaigns and interest in understanding anti-money laundering controls. Pivoting from this intrusion, industry sources identified a supply chain compromise (likely conducted by SILENT CHOLLIMA) leveraging unnamed Republic of Korea-developed enterprise resource planning (ERP) software previously targeted by the adversary.

FAMOUS CHOLLIMA opportunistically targeted the legal sector as part of broader campaigns focused on financial gain and sanctions evasion. These operations, which combined malware operations and insider threat operations, were ancillary to their primary objectives of cryptocurrency theft and IT worker infiltration schemes.

Russia

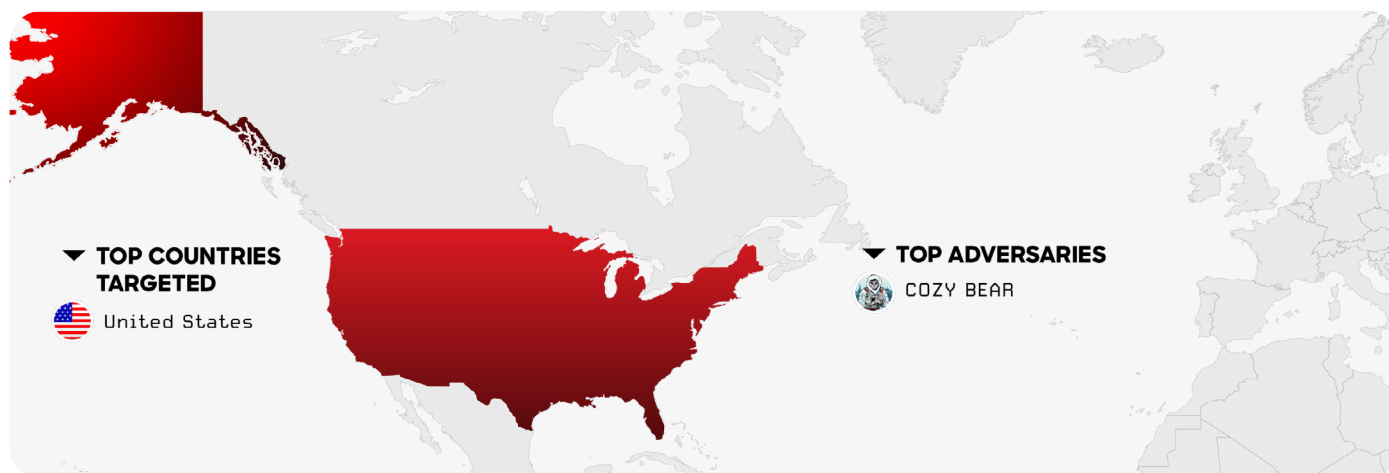


Figure 9. Russia-nexus legal sector threat landscape, September 1, 2025, to August 31, 2026

CrowdStrike Intelligence observed limited Russia-nexus targeted intrusion activity impacting legal entities during the reporting period. In August 2025 and September 2025, CrowdStrike OverWatch and CrowdStrike Falcon Complete responded to multiple [COZY BEAR](#) phishing attempts at a U.S.-based legal entity in which the adversary used Entra ID OAuth 2.0 phishing links to gain initial access to victim accounts. COZY BEAR will likely continue occasional targeting of North American and European legal entities relevant to their strategic intelligence collection scope, including political affairs.

CrowdStrike Intelligence assesses that Russia-nexus adversaries do not pose a significant threat to legal organizations located outside of Ukraine, unless such entities directly connect to Russia's immediate sphere of interest or are targeted as part of broader campaigns against sensitive organizations. This assessment is made with moderate confidence based on limited observed Russia-nexus activity targeting the legal and financial services sectors as well as Russian intelligence services' historical and current likely collection priorities.

Iran

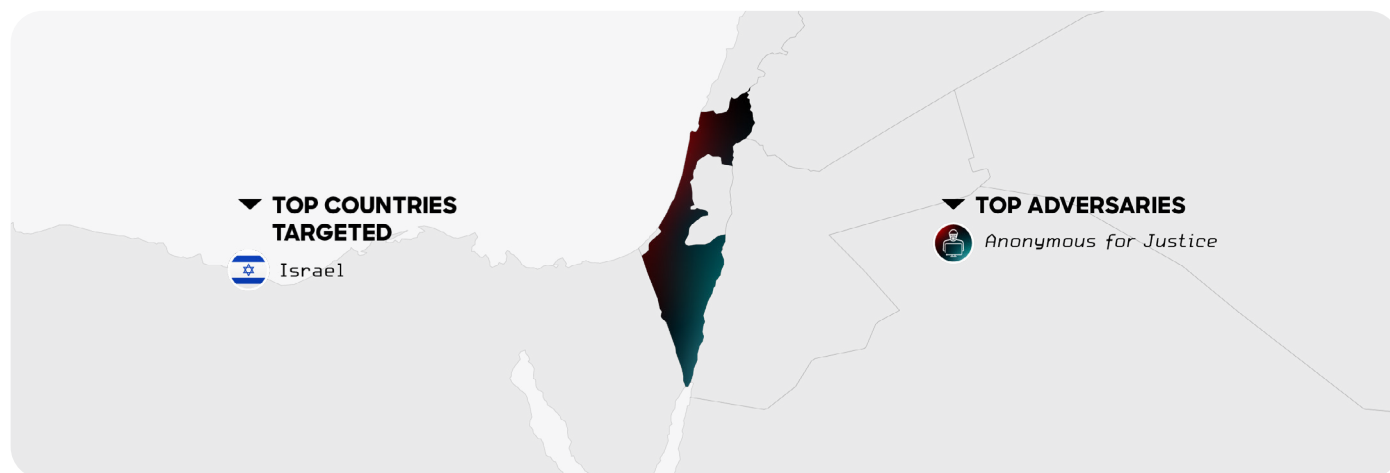


Figure 10. Iran-nexus legal sector threat landscape, September 1, 2025, to August 31, 2026

CrowdStrike Intelligence observed limited Iran-nexus targeted intrusion activity impacting legal entities during the reporting period. However, Iran-nexus adversaries likely broadened their cyber operation scope in response to the U.S.-Iran conflict to include Western organizations across various industries.

From March 8 to 18, 2026, *Anonymous for Justice* (aka *Anon_Israel*) claimed responsibility for at least 20 data deletion operations against Israeli entities across several sectors, including legal entities. Despite their claims of affiliation with the *Anonymous* collective, *Anonymous for Justice* is a pro-Palestinian hacktivist group likely operating as an Iran-nexus persona. Additionally, while *Anonymous for Justice* provided videos purportedly showing the data deletions, CrowdStrike Intelligence cannot independently verify the group's claims and has previously assessed their past claims to be heavily exaggerated for psychological intimidation purposes. However, the group has stated that their motivation is the reported U.S. strikes.

Non-State



Figure 11. Non-state legal sector threat landscape, September 1, 2025, to August 31, 2026

Non-state threat actors conducted limited cyber operations targeting the legal sector during the reporting period.

Between July 7, 2026, and July 29, 2026, pro-Russia hackers led by Z-Pentest and [BOUNTY JACKAL](#) conducted a campaign against government, critical infrastructure, and private sector entities in Spain, including several legal entities. This campaign was conducted under the #OpSpain campaign tag and likely motivated in part by Spain's July 2026 50 million EUR contribution to Ukraine through the NATO Prioritised Ukraine Requirements List (PURL) program.

Hacktivist groups' cyber campaigns against legal entities may stem from the following factors:

- Legal firms frequently engage with controversial clients
- Legal firms are visible in politically charged regions
- Legal firms possess sensitive client data that provides ideological justification for targeting and financial incentive for data theft

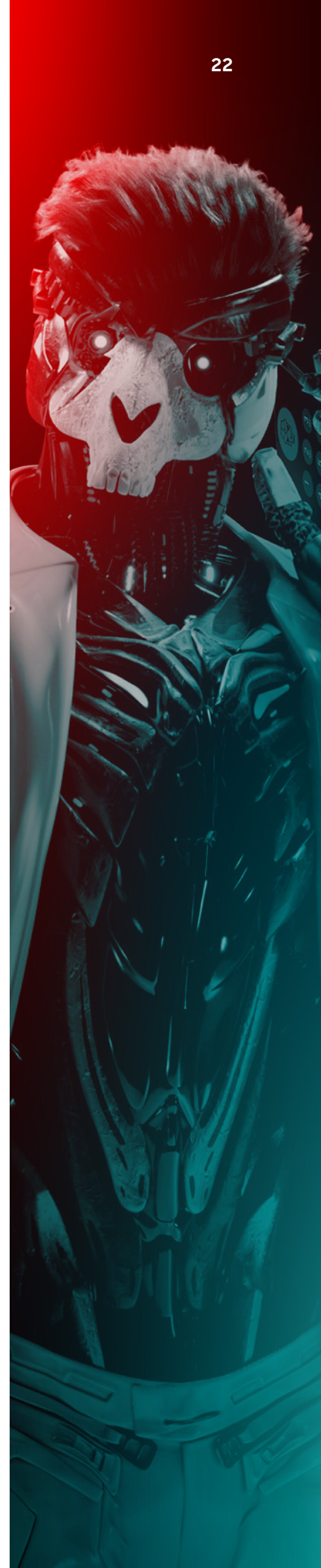
Outlook

The legal sector faced a sustained and multidimensional threat environment during the reporting period, driven by profit-motivated eCrime threat actors, nation-state adversaries pursuing strategic intelligence objectives, and hacktivists seeking to advance ideological causes. The sector's access to sensitive client data, litigation materials, and regulatory intelligence makes it an attractive target across all threat categories.

eCrime activity will remain the most consistent and operationally disruptive threat. CrowdStrike Intelligence assesses with high confidence that BGH adversaries will continue targeting the legal sector to obtain and monetize sensitive data, supported by its sustained position as the sector with the eighth-highest number of entities posted on BGH adversaries' DLSSs and the 39% increase in legal entities posted to DLSSs compared to the previous reporting period. CHATTY SPIDER will remain one of the most significant individual threats to the sector. Emerging threats from SNARKY SPIDER and CORDIAL SPIDER indicate diversification in adversary tradecraft targeting the legal sector. IABs will also highly likely continue opportunistically enabling these operations, sustaining ransomware and data extortion risk with direct implications for business continuity and client confidentiality.

Among nation-state threat actors, China-nexus adversaries will highly likely remain the greatest intelligence collection threat to the legal sector, maintaining sustained operations against U.S. and European law firms. Geopolitical drivers, including U.S.-China technology decoupling, sanctions enforcement, and economic espionage priorities, will sustain operational tempo against firms with strategic client portfolios. WARP PANDA's exploitation of CVE-2026-41709 and TITAN PANDA's first-observed targeting of legal-specific software (Intapp Time Server) demonstrate sophisticated technical evolution and sector-specific operational focus. Legal entities using IIS-based applications and virtualization infrastructure will almost certainly remain high-priority targets through at least mid-2027 given demonstrated adversary capability investments and operational patterns.

DPRK-nexus adversaries will continue posing a limited but meaningful threat, driven by Pyongyang's sanctions circumvention efforts and revenue generation requirements. SILENT CHOLLIMA's late January 2026 deployment of *TigerRAT* against a Europe-based public legal entity, specifically targeting anti-money laundering documentation, demonstrates focused intelligence collection aligned with cryptocurrency theft and sanctions evasion objectives. FAMOUS CHOLLIMA will likely continue exploiting the legal sector opportunistically through IT worker infiltration schemes. Law firms with expertise in financial crimes, sanctions compliance, and cryptocurrency regulation present particularly attractive targets.



Russia- and Iran-nexus adversaries do not currently represent a primary threat to the broader legal sector, though both warrant monitoring. Russia-nexus adversaries may conduct ad hoc operations against legal entities relevant to their strategic intelligence collection scope, particularly those engaged with politically sensitive matters, as evidenced by COZY BEAR's August-September 2025 OAuth 2.0 phishing attempts against a U.S.-based legal entity. Iran-nexus adversaries may expand targeting opportunistically amid the 2026 U.S.-Iran conflict.

Hacktivist activity will likely persist throughout 2026 and into 2027, characterized by DDoS attacks, website defacements, and hack-and-leak operations. Israeli legal entities face the highest risk from pro-Palestinian hacktivist personas, while firms in countries perceived as supporting geopolitical positions or experiencing domestic political unrest will face sporadic targeting. As hacktivist groups frequently prioritize geographical and ideological targeting over sector-specific activity, legal entities may be impacted as secondary targets within broader campaigns rather than as primary objectives.

The legal sector's role as custodian of sensitive client data and privileged communications ensures it will remain a high-value target across all threat categories. The overall trajectory, characterized by increasing eCrime sophistication, sustained China-nexus technical evolution, and persistent opportunistic targeting by other adversaries, demands continuous, intelligence-driven defense rather than a reactive posture.



Recommendations

1

Strengthen defenses against social engineering and identity abuse

Social engineering and identity-based attacks remain effective paths to initial access in the legal sector. Adversaries use phishing, vishing, impersonation, remote support tools, and authentication abuse to compromise trusted users and gain access to sensitive systems and data. Organizations should strengthen MFA, tightly control remote access tools, enforce least-privilege access, and monitor for anomalous authentication, token, and SaaS activity that may indicate compromised accounts or unauthorized access.

2

Harden internet-facing applications and critical systems

Legal organizations depend on internet-facing applications, virtualization platforms, and specialized business systems that can provide adversaries with high-value access when vulnerabilities or insecure configurations are exploited. Organizations should maintain comprehensive asset visibility, prioritize remediation of vulnerabilities in externally exposed and business-critical systems, review default and hardcoded configurations, and strengthen protections around systems that provide access to sensitive data or broader enterprise environments.

3

Reduce visibility gaps across identity, cloud, email, remote access, and virtual infrastructure

Adversaries use identity, cloud, email, remote access, and virtual infrastructure to establish persistence, access sensitive information, and evade detection. Legal organizations should expand telemetry and detection coverage across these environments and correlate activity to identify related behavior. Particular attention should be given to suspicious authentication activity, session and token abuse, new MFA registrations, and unusual remote access patterns.

Recommendations

4

Prepare for data theft, extortion, and disruptive operations

Legal organizations hold privileged communications, litigation materials, intellectual property, financial information, and other sensitive client data that can be monetized or used for extortion and reputational pressure. Organizations should strengthen data access governance, segment sensitive systems, monitor for unusual data access and exfiltration, and regularly test incident response and recovery plans. Preparedness should address both operational disruption and data theft so that teams can contain incidents quickly while limiting broader legal, regulatory, client, and reputational impact.

5

Prioritize intelligence-led defense and proactive hunting

The legal sector faces sustained targeting from financially motivated, nation-state, and ideologically driven adversaries pursuing theft, extortion, espionage, and disruptive objectives. An intelligence-led approach helps security teams focus defenses on the adversaries, techniques, and attack paths most relevant to their organization. Applying threat intelligence through proactive hunting can help uncover persistent access earlier, identify emerging activity, and accelerate response before intrusions escalate.

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-sensor 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>