



INDUSTRY THREAT BRIEF | LEGAL SECTOR

Law Firms Under Pressure

Legal-Sector Threat Report, October 2026

Data window: September 2025 to August 2026

RESEARCH BY



Law Firms Under Pressure

Legal-Sector Threat Report, October 2026. Data window: **September 2025 to August 2026**

Law firms are unusually valuable extortion targets. A successful intrusion can expose years of client material at once: tax returns, bank statements, medical records, custody disputes, signed agreements, and privileged communications. Paying a ransom does not make that data private again. It can still be sold, published, or used for further extortion.

Darkweb IQ is inside the market where many of those attacks begin. Our analysts use misattributable personas to maintain direct relationships with the brokers who sell access to corporate networks. The access-offer findings in this report come from those interactions, not public breach disclosures or leak-site aggregation.

About this report. This report is a joint publication of SecurIT360 and Darkweb IQ. The research and findings come from Darkweb IQ analysts. Where the findings say “we” or “our,” they refer to Darkweb IQ. SecurIT360 contributed the guidance on where its services fit.

KEY FINDINGS

157

Legal-sector organizations whose access brokers offered for sale

66%

Of those had fewer than 50 employees

98

Associated with brute-force or password-guessing activity

28

Firms where Darkweb IQ intercepted the access

What one firm lost

One legal-sector dataset currently being monetized shows what a single compromise can expose. We are withholding the firm's identity.

The dataset contains roughly **319,000 files**, including more than **310,000 PDFs**, organized across more than 40 client matters with the firm's original folder structure intact. Among them:

- 10,600 folders of discovery material
- 4,900 containing bank statements
- 4,400 containing tax returns
- 3,900 covering credit cards and liabilities
- 3,800 containing settlement files
- 3,700 containing income records and pay stubs
- 2,200 involving custody and parenting matters
- 700 containing financial affidavits

The same matters include retainers, depositions, subpoenas, divorce and modification petitions, decrees, and medical records.

A password can be reset. A tax return, medical history, custody dispute, or privileged legal record cannot. That permanence is what gives stolen legal data its leverage.

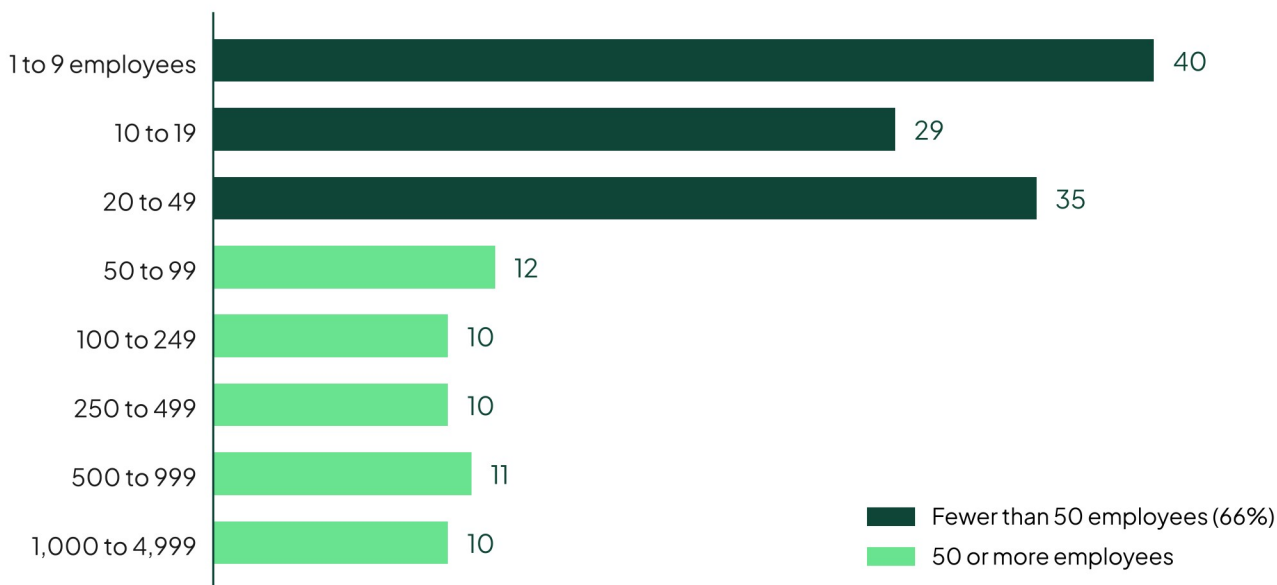
Access to law firms is already being sold

Ransomware often begins before the ransomware operator becomes involved. Initial-access brokers compromise an organization, confirm that the access works, and sell that foothold to another criminal. Between September 2025 and August 2026, brokers offered Darkweb IQ operatives access to **157 law firms and other legal-sector organizations**.

Of those, **66% had fewer than 50 employees**. But the market was not limited to small practices. It also included **21 organizations with more than 500 employees** and **10 with more than 1,000**.

Darkweb IQ intercepted access to **28 firms**, removing it from circulation before another buyer could use it.

FIRMS WITH ACCESS OFFERED, BY HEADCOUNT



157 legal-sector organizations, September 2025 to August 2026. 128 are in the United States and 13 in Canada. The rest are in Australia, the United Kingdom, Ireland, and elsewhere.

The distribution matters. Attackers are not limiting themselves to firms of a particular size. Small practices account for most of the volume, but large firms appear in the same market. What matters is whether someone has found a working way in.

Activity also accelerated late in the period. July and August 2026 added 34 firms, the two busiest months since October 2025.

Most access starts with a password

The routes into these firms were overwhelmingly ordinary. Where brokers identified the technique used, two methods dominated.

Password guessing. Attackers automate login attempts against VPNs, remote desktop services, and other externally accessible systems until a credential works.

Infostealer malware. Malware running on an employee's computer captures saved passwords, browser sessions, and other authentication material, which is then sold to other criminals.

Of the 157 firms:

- **98** were associated with brute-force or password-guessing activity
- **30** with credentials obtained from infostealer logs
- **5** with software exploitation

The categories overlap where more than one technique was used. Brokers recorded a technique for 110 of the 157 firms.

The important point is the imbalance. Exploiting software accounted for a small fraction of the access we observed. Most of it came down to credentials.

The way in

When Darkweb IQ intercepted access, we notified the affected organization. Among the 23 firms that reported back on the point of entry:

- Microsoft Remote Desktop: **11**
- Fortinet VPN: **6**
- SonicWall VPN: **4**
- AnyDesk: **1**
- Single sign-on portal: **1**

These are not obscure systems. They are the same tools employees use to connect to work every day.

Darkweb IQ recorded the privilege level for 18 of the 30 accesses it intercepted at the 28 firms. Four came with administrator rights. Two gave domain-administrator access: one at a firm of roughly 1,500 employees through a dedicated Fortinet VPN account, and one at a roughly 100-person firm through remote desktop and AnyDesk. Two smaller firms had local-administrator credentials exposed through Fortinet and SonicWall VPN access.

The other 14 were standard user accounts. Both matter. A user account can provide the foothold needed to start an intrusion. A domain administrator account can remove much of the work that normally follows.

By the time credentials like these reach an access broker, the question is no longer whether the firm has an exploitable vulnerability. Someone already has a working way in.

Vendor exposure becomes firm exposure

A law firm's attack surface does not end at its own network. We reviewed **76 technology vendors widely used by law firms** across three Darkweb IQ datasets: broker access offers, ransomware leak-site activity, and stolen corporate credentials. Across those vendors, we found:

3,052

Corporate credentials in infostealer data

18

Vendors appearing in broker access offers, across 42 offers all-time

3

Vendors appearing in ransomware leak-site posts

None of those findings alone proves that a vendor was breached. A stolen credential may come from an infected employee device, while a broker offer may involve exposed remote access rather than the vendor's production environment.

But a law firm does not need its vendor's entire network to be compromised for that exposure to matter. If an attacker obtains working access to a provider that stores client data, manages identity, handles backups, or connects to the firm, the vendor's access can become the firm's problem. Three areas stand out.

Document and practice management. One document-management vendor appeared in **seven separate broker access offers since September 2025**, more than any other vendor during that period. One June 2026 offer came from stolen credentials.

Security, backup, and identity. Eleven vendors in these categories appeared in credential or broker data. Darkweb IQ also intercepted live access involving a zero-trust vendor and a backup provider.

Collaboration and communications. One collaboration and identity provider accounted for **1,933 of the 3,052 corporate credentials** found across the vendor set.

We found no corporate credentials, broker access offers, or ransomware posts associated with the legal-AI vendors reviewed during the period.

Credential counts cover the 90 days to September 2, 2026. Access offers and ransomware posts cover our full dataset through August 2026.

Access is only the first step

The access market shows how criminals get a foothold. Legal-sector extortion campaigns show what can happen next.

The campaign tracked as **Luna Moth**, **Silent Ransom Group**, and **UNC3753** has repeatedly targeted legal and professional-services firms without needing stolen credentials at all.¹ The attacker calls an employee while posing as internal IT or a vendor. A supposed migration, billing problem, or technical issue becomes the pretext for a screen share or the installation of legitimate remote-management software. Once connected, the attacker collects sensitive files and follows with an extortion demand. In some cases, the victim is manipulated into helping move the data themselves.

Public reporting has tied the campaign to Jones Day, which disclosed in April 2026 that an outside party accessed files belonging to ten clients. The group published its negotiation and a file listing.² Weil Gotshal reportedly faced an **\$18 million to \$20 million** payment within three days of a demand.³

The technique is different from the access offers we track, but the underlying advantage is the same: trusted access beats a sophisticated exploit.

Why legal data creates leverage

Extortion does not require encryption. Data like the client files described at the start of this report carries leverage on its own.

Darkweb IQ has tracked the data-monetization site Leak Bazaar since October 2025. The site posts stolen corporate data in sorted, structured form and offers it for sale. Its operator told our undercover personnel that outright sales have been few. His largest payout this year came another way. A listing on the site was used to pressure a victim during ransom negotiations. His share of that ransom was roughly **\$50,000**. These figures are his own and are unverified.

Legal files are well suited to this kind of pressure. A firm's systems can keep running after a theft like this. Its clients' tax returns, custody files, and privileged communications are still exposed. The victim may be the most valuable buyer.

SOURCES

1. FBI, "Silent Ransom Group Targeting Law Firms," cybersecurity advisory, May 23, 2025. <https://ic3.gov/CSA/2025/250523.pdf>
2. Cyber Daily, "Ransomware group claims hack of legal giant Jones Day," April 8, 2026. <https://www.cyberdaily.au/security/13435-ransomware-group-claims-hack-of-legal-giant-jones-day>
3. Legal Cheek, "Weil reportedly pays up to \$20 million after hackers steal client data," June 3, 2026, citing The Insurer. <https://www.legalcheek.com/2026/06/weil-reportedly-pays-up-to-20-million-after-hackers-steal-client-data/>

What actually changes the outcome

The activity in this report points to a fairly short list of controls. Use it as a checklist with your IT team, managed service provider, and security partners.

- 01 Put MFA on every path into the firm.** VPN, remote desktop, email, SSO, and administrative access should all require a second factor. That removes most of the value from guessed or stolen passwords.
- 02 Eliminate routine administrator access.** Employees should not work from administrator accounts. Privileged credentials should be separate, tightly controlled, and used only when required.
- 03 Do not expose remote desktop directly to the internet.** RDP and other remote-management services should sit behind controlled access with MFA and appropriate network restrictions.
- 04 Train for phone-based intrusion, not only phishing email.** An unsolicited caller claiming to be IT should not get a screen share, software installation, or authentication code without independent verification.
- 05 Stop storing corporate passwords in unmanaged browsers.** Use a firm-controlled password manager and MFA, particularly where employees access company systems from personal devices.
- 06 Review vendors based on what they can access.** Certifications matter, but they do not tell you what an attacker could reach with a compromised vendor credential. Firms should know which providers hold sensitive data, connect to their environment, manage identity, or control backups.
- 07 Know when your access is being sold.** An access offer is not merely evidence of a past compromise. It can be an early warning that an intrusion has not happened yet. The period between a broker putting access up for sale and another criminal using it is one of the few points in the attack chain where defenders may still be able to act first.

Where SecurIT360 fits

SecurIT360 helps law firms close the gaps this report describes: exposed remote access, guessed and stolen credentials, over-privileged accounts, and vendor connections that brokers turn into products.

- **Find the way in before a broker does.** Penetration testing, including continuous testing through PenGarde, probes the kinds of internet-facing VPN, remote desktop, and login paths that appear in these access offers.
- **Watch every path into the firm.** Managed detection and response from the SecurIT360 Security Operations Center watches for the suspicious logins, remote sessions, and administrator activity that can follow a sold credential.
- **Pressure-test controls and vendors.** Security assessments, cyber risk management, and vCISO support help firms confirm that MFA, privileged access, and remote access controls work as intended, and map which providers hold client data or connect to the environment.
- **Respond fast when access is used.** SecurIT360 incident response helps firms contain an intrusion when an alert or extortion demand arrives.

Where Darkweb IQ fits

Darkweb IQ builds one-on-one relationships with the actors who sell access to corporate networks. Our analysts vet what they are offering and identify affected organizations. When we find credentials or network access associated with a customer, we alert them so the access can be disabled before it becomes the starting point for an attack.

Find out what an attacker could reach at your firm.

Learn whether access to your firm is being offered for sale, and close the paths that make it possible.

SECURIT360

Testing, monitoring, and response

securit360.com

DARKWEB IQ

Vetted alerts on access offered for sale

darkwebiq.com

About SecurIT360

SecurIT360 is a cybersecurity firm with offices in Birmingham and Kansas City. Its practitioners deliver managed detection and response, penetration testing, incident response, AI security, and advisory services to organizations where security can't slow operations down, including law firms. Learn more at securit360.com.

About Darkweb IQ

Darkweb IQ stops ransomware before it starts. Its undercover operatives build one-on-one relationships with the initial access brokers who sell entry into corporate networks, using misattributable personas. Darkweb IQ also tracks employee credentials stolen by infostealer malware. Analysts vet every alert before it reaches a customer, so access can be shut down before it is used. Learn more at darkwebiq.com.