flare

The Legal Cyber Threat Landscape: Infostealer Malware and Ransomware Extortion Against the Legal Industry

By Eric Clay, Security Researcher

Table of Contents

Introduction

The threat landscape is constantly shifting; from 2022 to 2023, we've seen more than a 100% increase in data exfiltration ransomware attacks affecting all industries. However, cyber risk is not spread evenly across industries and sectors. The legal sector is at considerable risk due to the privileged information that law firms hold and the disruption that a data breach or ransomware attack can cause.

In addition, law firms often have a large attack surface, with most employees heavily utilizing IT equipment and resources without necessarily having a strong background in IT security. We studied how at risk law firms were using two primary measures: ransomware data disclosures affecting law firms and stealer logs that contained corporate access.

Executive Summary: What Do Legal CISOs Need to Know?

Law firms and legal organizations handle sensitive and confidential client information on a daily basis, making them prime targets for cybercriminals seeking to exploit this data for financial gain or other malicious purposes. The nature of legal work often involves extensive collaboration and sharing of files and documents, increasing the potential for cyber threats to infiltrate the network through various entry points.

This study looks at two key metrics to understand how legal risk is changing over time. First, we will examine trends in infostealer malware targeting law firms and legal services companies, and secondly, we will look at how the rate of double and triple extortion ransomware attacks against law firms is changing over time.

Key Findings

- Out of a sample size of 50 law firms with more than 500 employees, 69% had stealer logs containing corporate access being given away on illicit Telegram channels or sold on Russian or Genesis Markets, representing a potential vector for compromise.
- Credentials present in stealer logs included those with access to subdomains that indicate access to corporate resources including:
    - remote.
    - Vpn.
    - Citrix.
    - palolto.
    - okta.
- The median number of stealer logs with corporate access for our sample size was two while the average was six due to a few law firms having dozens of corporate access credentials being given away or sold.
- Between 2022 and 2023, we tracked a 102% increase in unique company data being disclosed on ransomware blogs, with more disclosures in the first six months of 2023 than all of 2022. This trend was particularly acute for the legal industry, where we saw a 135% increase in double and triple extortion attacks.
- We have high confidence that the legal industry is targeted due to the large amounts of high-value sensitive client data law firms and legal services companies hold, leading to higher ransom payments and increased incentives for threat actors to target them.

Defining Our Terms

Before we begin, let's spend a moment defining what we mean by double and triple extortion ransomware attacks and infostealer malware logs.

What is Data Exfiltration Ransomware?

Data exfiltration ransomware refers to a type of cyberattack in which hackers exfiltrate data in lieu of or in addition to encryption, and threaten to leak or sell it if a ransom is not paid. Data exfiltration can be combined with encryption (double extortion) and with DDoS attacks, threats to specific employees, and other tactics (triple extortion). These tactics aim to increase the pressure on victims to meet the attackers' demands. During these attacks, data is often uploaded to dedicated public "ransomware blogs" in very large files.

What are Infostealer Malware Logs?

Infostealer malware logs are files that contain detailed records of the activities performed by infostealer malware on an infected system. These logs typically include information such as browsing history, login credentials, crypto wallets, and session cookies that the malware has captured from the victim's device. The purpose of these logs is to provide the attackers with valuable information that can be used for various malicious purposes, such as identity theft or selling the stolen data on underground markets. Infostealer logs containing credentials with access to corporate IT assets are particularly risky, as an attacker may gain access to multiple corporate resources present in one log.

Our Analysis

We wanted to understand how the threat landscape is changing for law firms. To do this we looked at two datasets. First, we looked at infostealer malware with corporate access (a significant vector for attacks), then we looked at attacks that involved data data dumps on ransomware blogs for each year that affected law firms to determine how double and triple extortion schemes targeting law firms changed between 2022 and 2023.

- How the number of double and triple extortion ransomware attacks targeting the legal industry has changed in the past 18 months compared to attacks against all industries.
- The average size of law firms targeted by ransomware groups.
- What percentage of the top 50 law firms in the United States have had corporate credentials disclosed in infostealer logs.

Infostealer Malware with Corporate Access

The first part of our analysis focused on examining the prevalence of infostealer malware with access to corporate resources. We selected 50 large firms with more than 500 employees and analyzed each firm using Flare's stealer log collection to determine whether the firm had credentials with corporate access either for sale on a dark web marketplace or being shared on specialized Telegram channels.

We analyzed stealer logs associated with each law firm's domain and identified the ones that featured subdomains indicating likely corporate access (versus potential customer access). For example, we excluded logs containing subdomains such as:

- portal.lawfirm.com
- customer.lawfirm.com

And included logs in our count that had subdomains such as:

- vpn.lawfirm.com
- remote.lawfirm.com
- securemail.lawfirm.com
- sftps.lawfirm.com

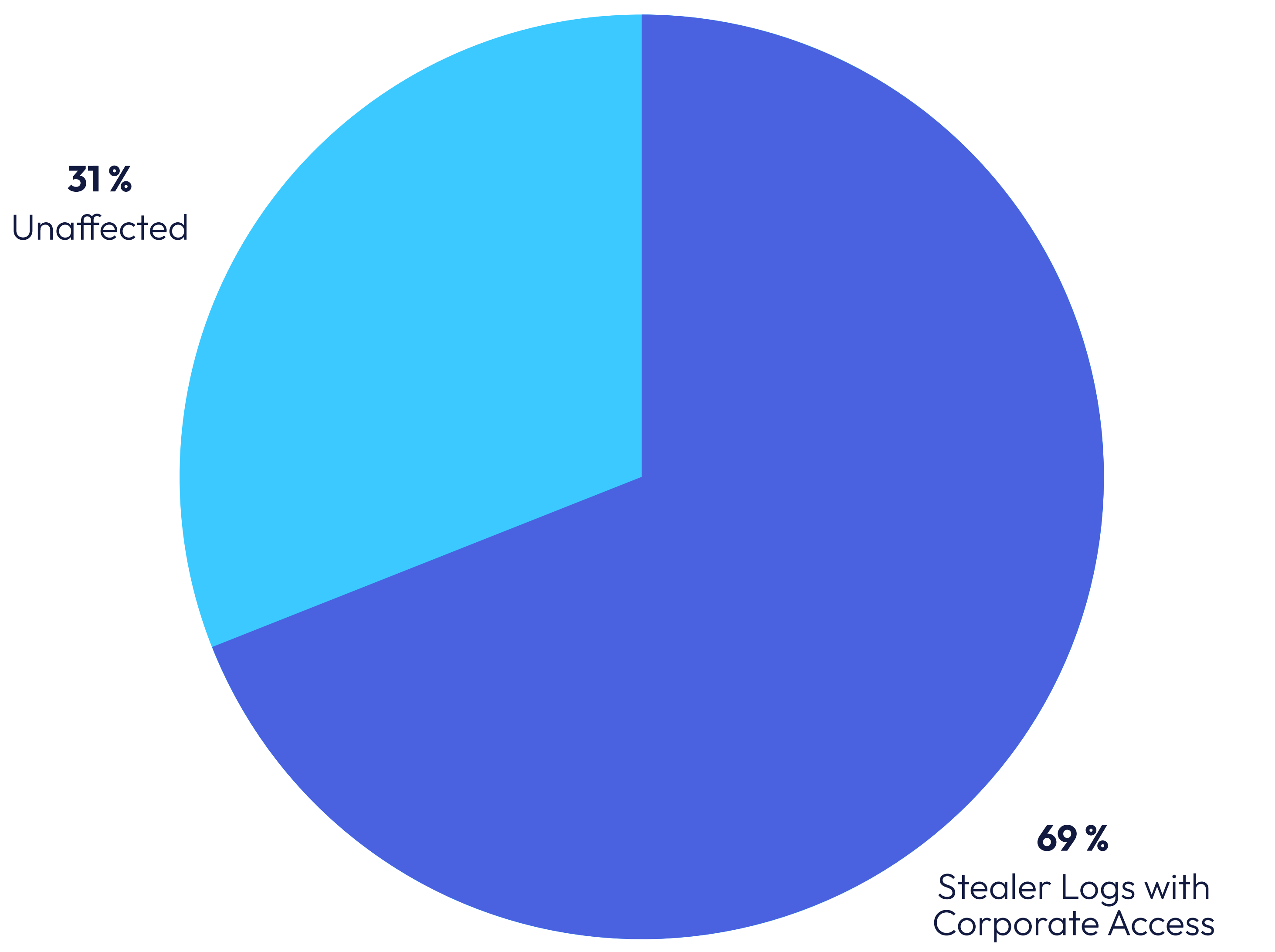
We identified many subdomains that indicated likely corporate access including:

- remote
- securemail
- securefileshare
- vpn
- Sftps
- Single-Sign On (SSO)
- Internal subdomains unique to the firm

The pie chart on the right shows the percentage of law firms affected by stealer logs with corporate access in the past 2 years, out of our sample size of 50.

On average each law firm had six logs with corporate access exposed, but this number was skewed based on a few outliers that had dozens of stealer logs with corporate credentials. To get a better understanding of how many logs each law firm had, we looked at the median number of logs with corporate access in our sample data. This number was considerably lower at two, with 11 law firms having no corporate credentials exposed.

Law Firms Affected by Stealer Logs with Access (Percentage)

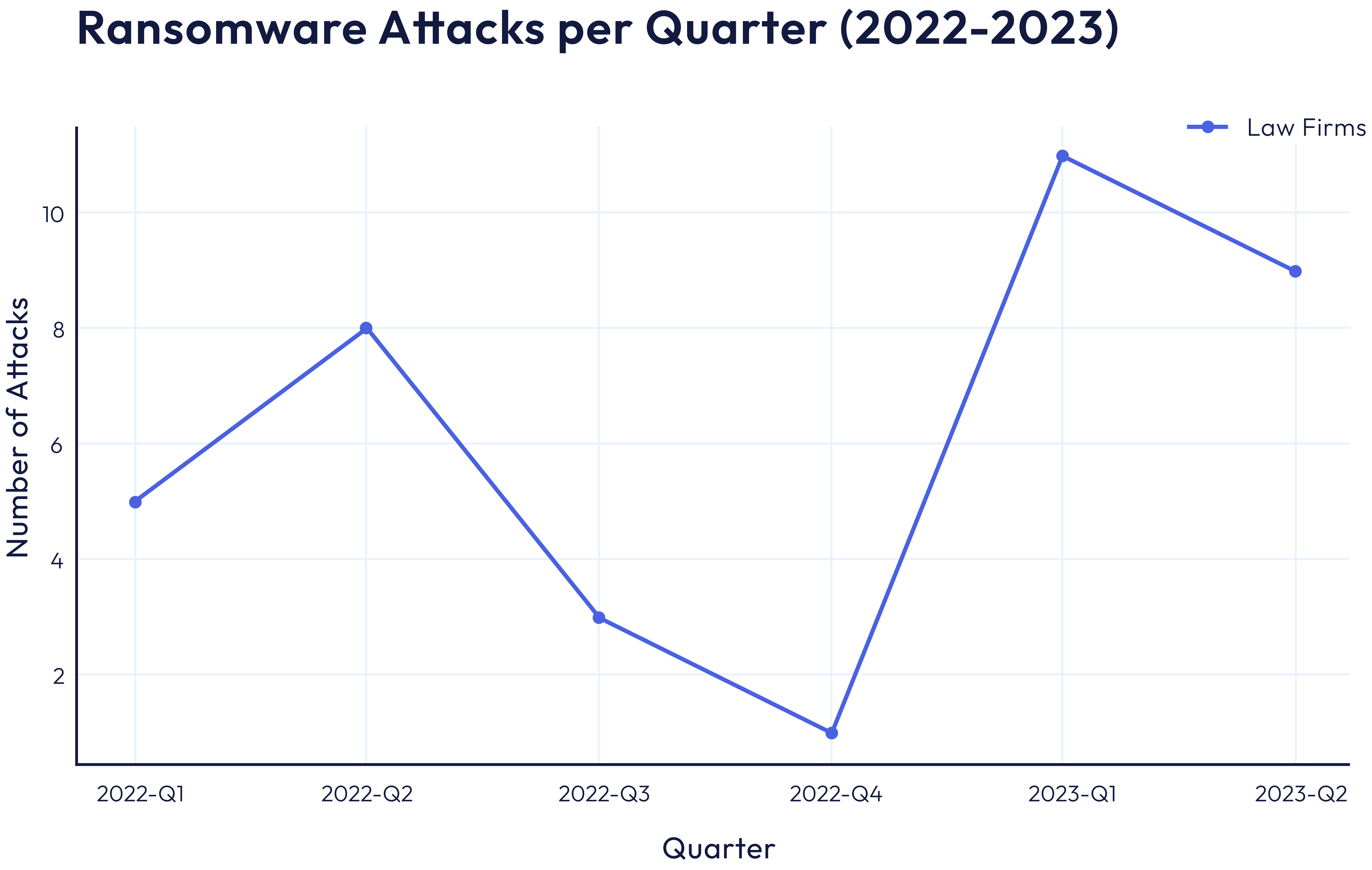


Why Does This Matter?

Based on our research, infostealer malware is an increasingly common vector for ransomware attacks and data breaches against organizations. Threat actors simply have to sift through logs in order to identify those that have access to corporate resources, leverage those credentials, and expand access. Stealer logs can also enable threat actors to bypass MFA through session replay attacks. We have direct evidence of initial access brokers on Exploit.In and XSS directly purchasing stealer logs in order to gain initial access to corporate IT environment which can then be resold after the threat actor establishes a backdoor in order to facilitate ransomware attacks, data breaches, financial theft, and other cybercrime.

Ransomware Attack Analysis

For our ransomware data set, we analyze double and triple extortion attacks against the legal industry based on data disclosures on ransomware blogs. If infostealer logs are a primary vector of attack, ransomware is a common consequence of successful exploitation of a vector. By analyzing this data, we are able to identify law firms that ransomware actors successfully breached and had their data disclosed, typically as a result of refusing to pay the ransom. It is worth noting that this only provides a small segment of likely law firms that were the victims of ransomware, but it does enable us to compare trends against other global industries.



In 2022, 17 law firms were breached and had their files published on ransomware blogs, compared to 20 in the first six months of 2023. If the 2023 trend line continues, we expect 40–60 data disclosures specific to law firms in 2023. This trend is partially due to the dramatic increase in ransomware attacks against all industries and sectors, however, that doesn't fully account for the increase in law firm targeting. Across our data set, we saw:

- A **102.5%** increase in double and triple ransomware disclosures in H1 2023
- A **135.2%** increase in double and triple ransomware disclosures targeting law firms in H1 2023
- The average victim law firm had 437 employees and $42,000,000 in revenue

We theorize that significant increases likely represent a confluence of factors, including:

- An increase in double and triple extortion tactics by threat actors. Since we are measuring the "number of companies with disclosed ransomware files," part of the increase is likely due to threat actors increasingly adopting these tactics, particularly as companies build more sophisticated backup and recovery systems.

- An increasing number of attackers; Flare's research and collection team has identified 39 new ransomware gangs and affiliate groups since the beginning of 2023.

- The relative value of ransomware disclosure against various targets. The advent of double and triple extortion schemes places increased emphasis on attacking companies with valuable data where disclosure will cost the company excessive amounts of money or reputation. Law firms are an excellent target due to the amount of sensitive information they hold, and the potential damage to their reputation if the data is disclosed.

Recommendations for Legal Cybersecurity

- **Implement policies preventing credentials from being saved in browsers:** Infostealer malware principally targets the web browser of the infected device for credential harvesting. Utilize password managers and enact policies that prevent passwords from being saved in web browsers.

- **Restrict access to corporate SaaS and IT infrastructure for non-corporate devices:** Many infostealer infections that contain corporate credentials occur when employees use shared home computers and save passwords in their browser. Only corporate devices should be used to access IT infrastructure or corporate SaaS applications.

- **Proactively monitor infostealer logs to detect logs that contain corporate access:** Automatic monitoring for logs containing corporate credentials can proactively alert you to high-risk exposure before they are used in a breach. Ensure that your monitoring solution has extensive coverage across public & private Telegram channels, Russian Market, and Genesis Market.

- **Monitor initial access broker forums:** Initial access brokers are primarily active on dark web forums Exploit and XSS and are often the initial vector used by ransomware affiliates. Monitoring these forums for postings that advertise access to law firms may provide advanced notice that you have an active compromise in your organization.

- **Conduct technical third-party monitoring for organizations that have access to your IT environment:** Many breaches are caused by third parties that routinely access law firms IT infrastructure and SaaS environments. We recommend conducting extensive due diligence on any third-parties that have direct access to IT infrastructure, including conducting technical security audits to ensure they don't have any active compromises.

About Flare

Flare is the proactive external cyber threat detection solution for organizations. Our AI-driven technology constantly scans the online world, including the dark and clear web, to discover unknown events, automatically prioritize risks and deliver actionable intelligence you can use instantly to improve security.

Want to learn about how Flare can support your external risk monitoring?

Free Trial

Book a Demo

flare.io

hello@flare.io