COLORTOKENS

THREAT RESEARCH

REvil & Maze Groups Targeting Law Firms

What Happened?

Data breaches are becoming more common, and law firms, given the sensitivity of the valuable data they handle, are falling victim to cyberattacks at an alarming rate. Law firms are repeatedly targeted because of the vast amount of sensitive information and client data that they retain.

According to media reports, at least seven law firms have been infiltrated by ransomware in the last six months. Hacker groups Maze and REvil have taken responsibility for the attacks and are identified as significant threat groups targeting law firms in 2020.

Hard Facts on Cyber Attacks Targeting Law Firms

- According to the Department of Justice, at least 25% of all law firms have been subjected to some form of data breach[1].
- According to the American Bar Association, breaches reported by law firms are expected to increase drastically in 2020 and about 42% of law firms with up to 100 employees have already experienced a data breach.
- According to a recent study done by BlueVoyant, 70% of the law firms studied had credentials stolen, 15% revealed high security vulnerabilities and 100% showed evidence of targeted threat activity[2].

Recent Ransomware Attacks on Law Firms

- In May 2020, Hacker Group REvil threatened to release almost 1TB of private legal secrets of renowned Hollywood celebrities, following a ransomware attack on a high-profile New York entertainment law firm Grubman Shire Meiselas & Sacks. REvil demanded $21 million to not expose the business dealings of U2, Bruce Springsteen, Madonna, Nicki Minaj and many others.
- In April 2020, a data breach at a legal software provider exposed potentially sensitive information belonging to over 193 Global Law Firms, including Baker McKenzie, Clifford Chance LLP and Hogan Lovells. According to a report by cybersecurity company TurgenSec, the stolen data was posted publicly on a website and remained up for "an extended period" of time.
- In April 2020, Travelex chose to pay $2.3 million — in the form of 285 Bitcoins — to the Hacker Group REvil after its ransomware attack crippled Travelex's currency exchange services.
- In February 2020, Hacker Group Maze reportedly held and published client data of over five law firms. It also re-listed the Texas law firm Baker Wotring on its site under the heading "full dump" and further released the firm's private legal data of personal injury cases, fee agreements, HIPPA consent forms, and more.

[1] https://www.theblanchlawfirm.com/how-to-protect-your-law-firm-from-ransomware-in-2020/
[2] https://www.bluevoyant.com/sector-17-infographic

Other Threats to Law Firms In 2020

- Phishing
- Data theft
- Attacks targeting legacy systems
- Increased supply chain attacks
- Hardware and firmware attacks
- More sophisticated ransomware attacks

Tips to Prevent Data Breaches at Law Firms

- Implement micro-segmentation to prevent access between network segments
- Prevent usage of untrusted software
- Develop and implement a cyberattack protocol
- Conduct in-house cyber audits, Ethical Hacks and Penetration Testing
- Utilize off-site data storage with encrypted security
- Conduct regular backups and maintenance
- Implement multi-factor authentication (MFA) for all company accounts
- Build an effective and tested business continuity plan

ColorTokens Security Solutions for Law Firms

The 2020 Data Breach Investigation Report (DBIR), points out that in law firms, more often than in other industries, security breaches occur in the form of ransomware and privilege misuse. ColorTokens solutions provide full protection from most targeted attacks on Law Firms:

Xshield helps you gain real-time visibility into your security posture across all workloads in data center and cloud environments

ColorTokens' Zero Trust approach to security protects you from external as well as insider threats

Incident response times are improved by leveraging security intelligence and attack path analysis

Xprotect enables different levels of security to be applied on endpoints, based on the type and purpose of endpoints

Securely lockdown legacy desktops and servers that run unpatched software

Leverage whitelisting, blacklisting, and configurable security rules to achieve proactive security

Xassure, ColorTokens' security service, delivers fast detection and response from ransomware attacks, data exfiltration and other targeted attacks

Xassure delivers proactive threat hunting and managed services for round-the-clock protection

ColorTokens' multi-layered security can lock down endpoints in the case of a breach, containing the breach and preventing further damage.

ColorTokens' ransomware prevention approach is detailed here.

ColorTokens Inc., a leader in proactive security, provides a modern and new generation of security that empowers global enterprises to singlehandedly secure cloud workloads, dynamic applications, endpoints, and users. Through its award-winning cloud-delivered solution, ColorTokens enables security and compliance professionals to leverage real-time visibility, workload protection, endpoint protection, application security, and Zero Trust network access—all while seamlessly integrating with existing security tools. For more information, please visit www.colortokens.com