Redpoint
Cybersecurity LLC

REDPOINT INCIDENT RESPONSE USE CASE

THE PROBLEM

A mid-size law firm suffered a major breach:

- **The client's Managed Services Provider's (MSP) infrastructure was compromised and was used as a launch-off point to attack the MSP's customers, allowing sophisticated malware to run and infect the majority of the firm's infrastructure.**
- **The firm had a backup strategy; however, some of the backups were infected as well.**
- **The firm was completely shut down, and all systems were unusable.**

TOOLS & TECHNIQUES

- **Emergency Response:** Redpoint was engaged after the initial indicators of compromise were identified.

  Our team provided remote assistance within 3 hours of being notified and was on-site within 24 hours

- **Analysis:** Our cybersecurity engineers utilized proprietary software to exfiltrate data from the endpoints to a centralized location for analysis.

  An Endpoint Detection and Response (EDR) tool was installed on all infected endpoints used to gain visibility into the client's compromised infrastructure.

- **Remediation:** Redpoint was able to identify the infected machines and quarantined them immediately upon arrival.

  In parallel to this, endpoints containing the utilized EDR tool were prepared to be redeployed.

OUTCOMES

- **Immediate** initial engagement response, and on-site personnel within 24 hours.
- Triaged and performed investigation as well as **recovered & remediated** all areas of compromise within the first 12 hours of investigation.
- Provided client with the capability to get systems back up and running safely to **resume normal business** operations.

CONTACT US TODAY

TAB BRADSHAW

tab@redpointcyber.com

Principal

Redpoint Cybersecurity

RUSSELL SAFIRSTEIN

russell@redpointcyber.com

President

Redpoint Cybersecurity