SUREFIRE CYBER

From Response to Resilience

CASE STUDY I MEDICAL

Critical Care Clinic Turns Ransomware Attack into an Opportunity to Bolster Defenses

Challenges

- Critical patient care disrupted following a ransomware attack.
- Legacy servers, no endpoint detection, no multifactor authentication for email, and no incident response plan.
- Onsite backups also encrypted — and cloud backups only stored limited patient data.

Solutions

- Fast response: negotiated, secured and tested decryptor keys within 48 hours.
- Non-stop recovery: fully restored infrastructure to support critical care within 24 hours of receiving decryptor keys and all other systems, including Active Directory and electronic medical records, within days.
- Forensic investigation: pinpointed root cause while also uncovering other vulnerabilities and security gaps and provided appropriate mitigation steps to increase resiliency.

Benefits

- Restored normal operations — and patient care — within days.
- Hardened the environment by implementing endpoint protection and multifactor authentication.
- Increased security awareness and delivered best practice recommendations to further improve security posture.

When a critical care clinic was hit by a ransomware attack, patient care came to a standstill. The ransomware group had encrypted every system, including Active Directory (AD) and the electronic medical records (EMR) server, rendering the medical staff powerless to do their jobs.

Sadly, this scenario is not unusual. Bad actors aren't known for their scruples and while some consider medical facilities off-limits, many simply seek the path of least resistance and biggest payout. Medical facilities have become attractive targets because they are known to pay ransoms — and quickly — to regain access to "do or die" patient data.

With continuity of service at severe risk, the clinic was quick to call its cyber insurance carrier, who in turn, immediately engaged Surefire Cyber to assist with mitigation and system restoration.

Experience and efficiency lead to swift recovery

As the ransomware compromised both the primary and on-site backups, and there were limited cloud documents at hand, reinstating from archived data was not feasible; therefore, the Surefire Cyber team promptly began ransom negotiations. Step one was requesting proof of life. In other words, asking the threat actor to decrypt several files to confirm the decryptor's viability.

After the threat actor demonstrated the tool's effectiveness by unlocking sample artifacts, Surefire Cyber's experts proceeded with ransom negotiations and helped the clinic settle on a reduced ransom amount. The team at Surefire Cyber facilitated the payment process with a third-party vendor to confirm that the threat actor was not on the Office of Foreign Assets Control (OFAC) Specially Designated Nationals and Blocked Persons list and posted payment on behalf of the client.

With the decryptor in hand, the team conducted further testing to ensure the decryptor would work for all impacted files. This additional evaluation is a vital step as a malfunctioning decryptor can cause further damage to encrypted files.

The entire process — from initial threat actor communications and decryptor testing to negotiating down the ransom and facilitating payment — was completed in less than 48 hours.

In parallel, the Surefire Cyber team worked to determine if the threat actor had also exfiltrated any data — a process that combines what a threat actor states or provides (e.g., a file tree listing) with the team's internal forensics findings. While the team found no evidence of data exfiltration in this case, it's always important for victim organizations to understand if a threat actor has touched or siphoned any data so they can take appropriate actions to mitigate impact — for example, notifying regulatory authorities and affected individuals.

Surefire Cyber treats each client case as a top priority. However, knowing that this clinic's inability to access EMRs could jeopardize critical patient care, the team would not rest until the job was done. They worked around the clock over the weekend to restore and, as necessary, rebuild systems. By Monday morning (five days post attack), the clinic was back up, running, and seeing patients.

"The medical clinic has a huge impact on so many lives. I could not go to sleep until I knew they were in a good place. I wanted to ensure they were back up and running and had the information they needed to treat their patients when they opened their doors Monday."

Out with the old, in with the new to reinforce security

During the response process, the Surefire Cyber team also dug into forensics. They isolated the impacted systems and leveraged an automated platform that was developed in-house to collect and process forensic artifacts. This allowed the team's forensic experts to rapidly analyze the entirety of the evidence. Not only did they identify the root cause of the incident — Remote Desktop Protocol (RDP) exploitation — but they also established a narrative around the nature and timeline of threat actor activity within the environment, including checks for persistence mechanisms, and possible modifications to AD. As part of their due diligence process, this analysis is designed to verify that the threat actor is no longer in the environment or able to access any systems.

Turning an emergency into a best practice, teachable moment

To further help the clinic improve its security posture, the team addressed several other issues, including the outdated and highly vulnerable servers and the environment's lack of endpoint protection and multifactor authentication. Moreover, the clinic received a full incident report based on engagement findings.

In the documentation, Surefire Cyber included a set of best practice recommendations — for example, outlining a high-level approach on how to avoid RDP exploitation and suggesting the clinic create and rehearse an incident response plan, establish a patch management program, and limit and/or restrict applications and services open to the internet. In short, a game plan to help the clinic ward off, or at minimum, better prepare for future attacks and improve their cyber resiliency.

Surefire Cyber is redefining the incident response model by delivering a swifter, stronger response to cyber incidents. Our client-centric approach reduces stress and provides clients the confidence they need to help prepare, respond, and recover from cyber incidents – and to fortify their cyber resilience after an event.