semperis

CASE STUDY HEALTHCARE PROVIDER

A SWIFT RESPONSE TO A HEALTHCARE CLIENT'S RANSOMWARE ATTACK

Sirius Healthcare and Semperis thwart devastating impacts and put in place a strong security stance

THE CLIENT

A private orthopedic specialty medical practice with 30 locations and over 2,000 employees in the state it serves.

ATTACK PROFILE

- The client's complex and distributed AD environment included more than 130 servers and 25 domain controllers, making them vulnerable to a ransomware attack.
- Bad actors' persistence resulted in a successful attack that compromised most systems.
- Initial access was gained by phishing.
- Lateral movement and privilege escalation succeeded in compromising multiple AD domain controllers and the enterprise forest and domain.
- The discovery of several unaffected domain controllers enabled the response team to help the client recover quickly.
- Semperis Directory Services Protector (DSP) ensured that attackers were no longer in the environment and attack paths were shut down.

> *We had what I would consider a relatively thoughtful network implementation. We applied a reasonable effort to bolster security, but there are always things you could do better—and that came back to bite us. We fell victim to a ransomware attack. It was pretty brutal, impacting most of our systems.*
>
> **The Client's Chief Technology Officer**

RAPID RESPONSE, DETECTION AND REMEDIATION

When a large orthopedic, physical therapy and sports medicine practice sustained a ransomware attack in February 2021, the healthcare organization took swift action to minimize the impact.

Unbeknownst to the client, they had a complex and distributed Microsoft® Active Directory® (AD) that made them vulnerable.

"We had what we thought to be a thoughtful network implementation," said the client's chief technology officer (CTO). "We applied a reasonable effort to bolster security, but there are always things you could do better—and that came back to bite us. We fell victim to a ransomware attack. It was pretty brutal, impacting most of our systems."

Initiated through a phishing email, the attackers gained initial access, made lateral movements, and successfully compromised privileged accounts. The bad actors established persistence for administrative access to many of this client's critical systems. They started with the exploitation of weaknesses, misconfigurations and blind spots in the company's AD environment. Very fortunately, the client did not suffer any data exfiltration, and their business operations had minimal negative consequences.

The client tapped Sirius Healthcare for help with incident response, remediation and to strengthen defenses. Sirius brought in Semperis, a security company with expertise in defending hybrid and multi-cloud environments, as well as purpose-built tools for AD environments. Among the key aspects of the recovery effort was immediately shutting down risky access while a thorough analysis and cleansing of the client's AD took place. The team found a domain controller (DC) that was unimpacted by the attack to aid in the recovery effort. A thorough analysis of the environment and subsequent cleansing of the Active Directory was an important step in the remediation. For example, Semperis directed the client to reset their KRBTGT (Kerberos ticket-granting ticket, a three-way trust guarding the gates to a network); to reset their account password twice, and to disable print spooler services running on all domain controllers. "We took a lot of immediate measures to fight the attack, including quarantining affected DCs, shutting down risky access, and finding clean DCs to aid our recovery," the CTO said.

MOVING BEYOND THE ATTACK WITH IMPROVED VISIBILITY AND SECURITY

"Once we were back on our feet, we needed to know that the bad guys were out of our environment," the CTO explained. "At this point, we did not know if we were still compromised. We had to operate under the assumption that they were everywhere, and we had to find them and root them out."

Sirius and Semperis helped this client monitor the environment to discern any lingering attacker reconnaissance was still taking place. Semperis' AD-focused security tools were employed to help the client gain an accurate and complete picture of the incident and the clients' AD security stance. Among those tools was Semperis' threat detection and response platform, Directory Services Protector (DSP). "The DSP tool delivered as promised, but I think the real value of bringing in Semperis was their people and their deep understanding of and insight into AD and AD-based attacks," the CTO said.

Now DSP constantly scans and monitors the orthopedic practice's IT environment looking for AD misconfigurations that attackers exploit to gain access. In addition, DSP tracks changes made to AD with the ability to automatically roll back malicious activities executed by bad actors, or even innocent mistakes made by internal IT team members. Perhaps the greatest value of DSP is its ability to look at AD in a deeper way than traditional security tools. DSP tracks the AD replication stream, which detects sophisticated and previously invisible attacks such as a DC Shadow attack, a late stage kill chain attack that allows attackers with privileged credentials to register rogue domain controllers.

Now controls have been put in place so that the orthopedic practice's hybrid AD environment is constantly monitored. Indicators of exposure to an attack and suspicious changes are flagged so they can be can dealt with immediately to thwart devastating impacts. "We've really started to take things to the next level," said the CTO. "Now we use DSP to alert us on group policy changes. [Group policies, in part, control what users can and cannot do on a computer system.] It has allowed us to implement stronger [internal] change control and improvement processes to prevent rogue IT activities that might be convenient to us but are not secure."

SIRIUS | HEALTHCARE

semperis

ABOUT SIRIUS HEALTHCARE

At every step of the healthcare continuum, and throughout the entire technology life cycle, Sirius Healthcare provides best-of-breed multivendor technology solutions that help healthcare organizations improve quality of care, control costs, enhance security, comply with regulations and extend reach to communities. Learn more about Sirius Healthcare and call Sirius today at 800-460-1237 to schedule a discussion of your needs.

ABOUT SEMPERIS

For security teams charged with defending hybrid and multi-cloud environments, Semperis ensures integrity and availability of critical enterprise directory services at every step in the cyber kill chain and cuts recovery time by 90%. Purpose-built for securing hybrid Active Directory environments, Semperis' patented technology protects over 50 million identities from cyberattacks, data breaches, and operational errors. The world's leading organizations trust Semperis to spot directory vulnerabilities, intercept cyberattacks in progress, and quickly recover from ransomware and other data integrity emergencies. Semperis is headquartered in New Jersey and operates internationally, with its research and development team distributed between San Francisco and Tel Aviv.

Semperis hosts the award-winning Hybrid Identity Protection conference. The company has received the highest level of industry accolades, most recently ranked #157 in the Inc. 5000 and the fourth fastest-growing company in the tri-state area and 35th overall in Deloitte's 2020 Technology Fast 500™. Semperis is accredited by Microsoft and recognized by Gartner.