ziften
CASESTUDY

How a Small Hospital Is Fighting Cybercrime Like the Big Guys

REGIONAL HOSPITAL GROUP

Challenge:

- Hospital network includes over 2,500 internal and external devices to be protected against breaches and data exfiltration.
- The two-man IT security team has fewer resources and toolsets than typically found at larger enterprise organizations.

Results:

- Discovered malicious malware communicating with command and control systems in foreign countries.
- Reinforced its HIPAA compliance through continuous monitoring of all user activity on external devices.
- Gained additional insights into activities on its network from a CyberDefenses breach investigation and security assessment.

Struggling to Protect a Large Target

The customer is a regional hospital network that provides comprehensive, community-based acute healthcare services. It operates three facilities in Texas with space for 500 patients, and also serves as a regional referral center for communities in parts of New Mexico.

While operating with only two security staff members, the customer is challenged by the same cybersecurity issues faced by much larger hospitals with bigger IT budgets. Regardless, the same rules and regulations apply to patient privacy and security. The customer needs to prevent data breaches in order to protect patients' sensitive information and remain HIPAA compliant.

What's more, the smaller size of the hospital can make it more attractive to attackers looking for high-value sensitive data to sell on the dark web. Attackers target small hospitals because they often lack security resources and the tight protocols and processes typically found in larger entities.

The customer's IT security team felt outmatched. Although they deployed a number of anti-malware and antivirus solutions, the team still lacked visibility into and oversight of all activity on its endpoint systems. With more than 2,100 internal devices and 450 external devices connected to the network, this is no trivial task.

Past Malware Detections

The customer has been using Ziften's Zenith security platform for endpoint protection for several years. During this time, the customer discovered malicious malware present on its systems making outbound connections to a variety of suspicious foreign locations, including Russia, China, and the Middle East. Fortunately, working with Ziften, the customer has determined no data exfiltration has taken place.

"Using Ziften and partnering with CyberDefenses, we can fine-tune our analyses and focus on the behaviors and activities that most impact our security outcomes."

- Customer's CISO

During these past threat investigations, the customer used its cyber insurance provider for incident response (IR). In the end, the customer was not confident the IR team truly cleaned up everything. The customer's CISO recalled, "The incident response team cleaned up the malware and then were gone. I remembered thinking we still had problems."

Another Detection Triggers a Robust Response

Recently, the customer discovered another security event: the breach of an Office 365 inbox. Wary of reaching out to their cyber insurance provider again, they contacted Ziften. "We weren't happy with the incident response we got two years ago," the CISO lamented. "We looked at our options and contacted Ziften for help."

Ziften brought in its partner, CyberDefenses, a military-grade cybersecurity services company, to conduct a more in-depth breach investigation and a full security assessment.

Getting Better Answers

Before using Ziften Zenith and CyberDefenses, the client didn't have enough staff, time, or knowledge to fully conduct a security assessment. Together with Ziften Zenith, the CyberDefenses security assessment has given the customer better insight into its IT environments to better defend itself against today's cybersecurity threat landscape.

For example, the CyberDefenses' security assessment showed a variety of issues on the customer's servers that needed immediate attention, including the presence of third-party malwares.

The simple endpoint protection and visibility capabilities from Ziften Zenith allowed CyberDefenses to find patterns and identify events and activities of special concern that have massively improved the customer's cybersecurity posture.

"Using Ziften and partnering with CyberDefenses has been tremendously valuable over the past several years," said the customer's CISO. "Using them in combination, we can fine-tune our analyses and focus on the behaviors and activities that most impact our security outcomes."

ziften
illuminate the unknown

CSE-10045-1A-EN, July 2018