Cybraics protects leading healthcare provider from Ransomware.

A HEALTHCARE CASE STUDY

Summary

Challenges

- Increasing medical device footprint and rapidly increasing attack surfaces
- Recent, targeted attacks were successful in penetration

Results

- Detection & remediation of Ransomware not found by other solutions
- Incremental funding provided by CEO to enable analytics services, based on detection of previously unknown threats

Customer Quote

"Aside from being the only ones that could identify the threat, the end-to-end service—raw data to actionable results—is what separates nLighten from other vendors."

Business Background

This Healthcare Network, located in the Midwest, is a network of both hospitals and healthcare facilities that provide services to millions of people annually. Throughout their facilities, they operate a broad range of services, from primary to emergency care, along with imaging services and complex surgeries. To continue providing leading-edge care, they have invested significantly in modernizing their operations and capabilities. The majority of their medical and bedside devices are interconnected to their information technology (IT) network as well as their medical supplier networks. New patient records, administration, and finance systems operate almost entirely in electronic form.

Scenario

The healthcare network's IT team, responsible for hospitals, clinics, surgery centers, and specialty centers has created several physical and logical networks to create diversity and scalability, while also isolating certain devices and connections (e.g. medical devices separate from other databases and applications) from the enterprise IT environment. The security team deployed an advanced threat detection service to identify threats across the entire IT network to augment the standard security tools, processes, and procedures in place. The advanced threat detection services conducted log analysis offsite using a Security Event and Incident Management (SIEM) system and a Managed Security Service Provider (MSSP), based on traditional signature-based products and endpoint protection.

What we Found

The Healthcare Network's IT team deployed the nLighten platform to ensure the network, medical devices, and databases were protected and to provide an additional level of inspection should the MSSP's approach be ineffective. nLighten analyzed firewall, DNS, and Active Directory logs and as a result the platform's multiple analytics immediately identified behavioral anomalies which did not match the expected activity of internal users. The customer identified the host as a network management server responsible for the monitoring and managing bedside devices. While the behavior was uncharacteristic for the network, it was not entirely unexpected for this management device. The Cybraics Managed SOC provided details of the traffic pattern and illustrated that this anomaly would occur less than once in 10 million evaluations, prompting the collective teams to conduct an additional investigation. The teams jointly isolated a single beaconing signal categorized as low-and-slow behavior, which is indicative of malware actively searching for a command and control server. The signal originated from the management server, but upon further investigation, it was found that the server was acting as a proxy for downstream devices. The actual origin of the signal was a host on a network not included in the analyzed data. Tracing the offending host, the Cybraics SOC discovered behavior consistent with Ransomware, and continued attempts to connect to a command and control server for additional instructions.

Significance

Ransomware is a very real and increasing threat that is targeting healthcare organizations. Initially deployed through malware, the malicious code attempts to contact its command and control. Once established, it allows the adversary to access and encrypt systems to a level that locks all users and system administrators out of the system. Typically, it targets Hospital Management Systems that contain patient and financial information. The adversary then demands payment to decrypt the system and return access. The victim usually has no other option other than paying the ransom. After access is returned, there is no assurance that the adversary has not taken sensitive information or left a backdoor in place for re-entry.

Results

nLighten detected, identified, and isolated a very weak beaconing signal that had avoided identification by several cyber tools, including perimeter firewalls, IDS devices, end-point protection, an advanced threat protection service, and an MSSP service. Cybraics collaborated with the customer in identifying the infected host and remediated the malicious threat, while ultimately protecting the customer from a potentially disruptive and costly breach.

"*Aside from being the only ones that could identify the threat, the end-to-end service—raw data to actionable results—is what separates nLighten from other vendors.*" said their CIO.

About Cybraics

Cybraics is an advanced analytics and artificial intelligence company, focused on solving the hardest problems in cybersecurity. We are a collection of like-minded citizens passionate about ensuring that our nations companies and citizens can live free of cybercrime. We have created the most comprehensive security analytics platform available – nLighten, which uniquely combines multiple modes of machine learning with an advanced artificial intelligence engine, Janus, to find unknown, advanced & insider threats as well as targeted attacks. nLighten analyzes virtually any dataset, identifies and prioritizes threats, and provides next steps for investigation & remediation. It is unlike any other security analytics solution in the market.