Malware on medical device missed by advanced threat protection suite

Situation

Advanced malware running on medical imaging devices on healthcare network.

As a regional healthcare provider network providing services to millions of people annually, our customer understood how critical a secure network is to protect their patients. Even with separate networks to isolate devices from the enterprise network and an advanced threat detection service in place, they were concerned that sophisticated targeted threats could go undetected.

Solution

Deploy advanced behavioral analytics to identify pervasive undetected malware.

The healthcare institution deployed Cybraics' nLighten to identify previously undetected malware that had been running on its network. nLighten identified a very weak signal within the DNS logs indicating a potential active insider threat. Initially identified as DNS resolution requests made by a computer-generated schedule, the Cybraics SOC team flagged the suspicious domain names. While these domain names were not registered on any blacklist, Cybraics' unique analytics and proprietary algorithms were used to identify them as being associated with suspected bad actors. These two techniques combined to identify a medical imaging device on the customer network that was infected with malware.

Success

Safely remediate advanced malware off of medical device.

Working closely with Cybraics' SOC team, the healthcare institution implemented a phased plan to isolate and then remediate the compromised device without impacting services, safety, or quality of care to their patients. This compromised device could have been manipulated to harm patients, or act as an entry point to other areas of the network.

> *Medical devices are critical to operations and patient care, it's unsettling that our Advanced Threat Protection Suite from a major vendor didn't identify the adversary. Our patients were at risk; it's a good thing nLighten was able to detect this malware threat.*