CUSTOMER CASE STUDY

Healthcare Customer Case Study

How Security On-Demand detected malicious cyber activity on a large healthcare system

The Breach

Security On-Demand's ThreatWatch behavioral analytics platform detected malicious activity, which escalated to the Threat Reconnaissance Unit to be further evaluated by a SOC analyst. The Threat Reconnaissance Unit observed indicators in the customer's network that have been attributed to ransomware infections, specifically Wanna Cry ransomware.

The analysts observed that 10 unique internal hosts attempted to connect to known Wanna Cry sinkhole IPs in a short period of time. Typically, Wanna Cry ransomware kill switch communications on customer network and infects its hosts, encrypts files, all while installing a backdoor Trojan. Based on the detected malicious activity from ThreatWatch, SOD's team immediately notified the healthcare company.

The Result

Early notification enabled the healthcare organization to proactively address the issue and prevent any encryption. Although the connections were denied, the customer disconnected Internet access for several days to investigate further and identify ground zero of where and how the compromise started.

During the following days and weeks after the detection, the company remained on high alert, and we continued to monitoring their traffic to ensure indicators were no longer in their network.