Stopping Ransomware Attack Before Damage Occurs

Issue

Wanna Cry ransomware kill switch communications on customer network. This malware infects hosts and encrypts files while installing a backdoor Trojan.

How We Detected

ThreatWatch behavioral analytics platform detected malicious activity. We observed indicators in their network that have been attributed to ransomware infections, specifically Wanna Cry. Ten unique internal hosts attempted to connect to known Wanna Cry sinkhole IPs in a short period of time.

How We Responded

A notification was sent describing potential malicious activity using our proprietary SORAD alert notification. We provided a list of all the unique IPs associated with Wanna Cry plus recommended actions to contain, remediate and mitigate any existing or future infections.

Customer Response & Follow-Up

Early notification enabled them 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 how the compromise started. In the immediate timeframe after the detection, the company remained on high alert and we continued to keep monitoring their traffic to ensure indicators were no longer in their network.

Customer:

Not-for-profit healthcare system

Time to Detection