Behavioral Detection of Malicious Network Traffic

Issue

Suspicious outbound FTP connection allowed through the firewall to a “not normal” destination.

How We Detected

ThreatWatch 2.0® Network behavioral analytics platform detected anomaly.

How We Responded

A notification was sent describing potential malicious activity (possible data exfiltration) using our proprietary SORAD™ alert notification.

Customer Response & Follow-Up

Customer conducted investigation that determined the FTP connection was malicious, which resulted in a change to the firewall rules blocking the traffic. We added attacker’s profile to our consolidated threat reputation monitoring to improve future alert confidence and be on the lookout for similar threats.

Customer:

Large State Judiciary System

Vulnerability