Detecting Threats on Infected Personal Mobile Devices

Issue

Command & Control traffic indicating a "botnet" type of malware that was connecting to a China-based control server.

How We Detected

Malware Command & Control (or "C&C") traffic patterns were detected along with positive identification of malicious activity from our reputation analysis of the destination system.

How We Responded

The Security Operations Center (SOC) provided phone and e-mail notification describing potential impact of compromised device and recommendation on how to check the device for malware and reimage/clean the device.

Customer Response & Follow-Up

Investigation determined that the device was a malware-infected personal Android device connected to the production wireless network. Device was blocked from future access to the network.

Customer:

Retailer with E-Commerce Presence

Reduced Cost