CUSTOMER CASE STUDY

Retail eCommerce Customer Case Study

How Security On-Demand detected threats on mobile devices on an ecommerce retail system

The Breach

Security On-Demand's ThreatWatch behavioral analytics technology detected command and control traffic indicating a “botnet” type of malware that was connecting to a China-based control server.

SOD's Security Operations Center analyzed the critical alert and confirmed that malware with Command & Control (or “C&C”) traffic patterns were detected along with positive identification of malicious activity from our reputation analysis of the destination system.

The Result

The Security Operations Center (SOC) notified the client describing the potential impact of a compromised device and recommended how to check the device for malware and reimage/clean the device.

As the client investigated further, they determined that a personal Android deviceInvestigation 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.