Mobile Threat Risk Report

Sample Customer

Prepared April 2020

Enterprise Risk Report | My Score: 8.5

Time Frame: Jan 1, 2020 – April 1, 2020

WHAT WAS ANALYZED

Total Devices **1,000** 77% 24%

8,432 Networks

0 Phishing Visibility

116,768 Apps

FACTORS CONTRIBUTING TO YOUR RISK

Which of your devices are at risk

6 compromised devices

68% iOS devices vulnerable to public exploit

- **49%** HW exploit; **47%** OS exploit

7% devices with active critical risks

87% devices on vulnerable OS's

64% devices that can be updated

How many devices are running risky apps or profiles

10 malicious apps found

4,036 apps with high privacy and security scores

63 side-loaded apps detected

138 unmanaged profiles installed

How many devices have exposed to rogue networks

48 devices connected to rogue Wi-Fi networks

162 critical network attacks

WHY IT MATTERS

Risky Devices – Devices that are compromised or have vulnerabilities/settings that can increase the likelihood of being compromised.

Risky/Non-Compliant Apps – Sideloaded or legitimate apps with security & privacy risks that can lead to data loss or device compromise.

Malware – Malicious apps that can steal data directly or deliver exploits to completely compromise/weaponize the device.

Profiles – Unmanaged profiles can expose devices to risky configurations, data leakages, or other potential data loss.

Risky Networks – Risky networks can lead to data/credential loss or the delivery of device compromising exploits.

RECOMMENDATIONS

Compromised Devices - Quarantine the device to remove access to corporate assets. (Wi-Fi, App-Connect & Email)

High Risky Devices - Enforce device OS updates and remove risky configurations.

Risky/Non-Compliant Apps - Review app policies to identify specific app risks for your organization. Whitelist MobileIron developer certificates to identify unsanctioned sideloaded apps.

Phishing - Enable Phishing detections ASAP.

Malware - Flag device, alert user, and remove malware.

Unsafe or Rogue Networks - Do not allow users to access sensitive corporate resources while on risky network.