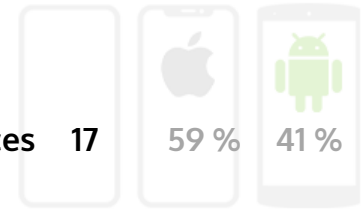
Mobile Threat Risk Report

Tenant: mi-go4mobile
VPC: mtddemo
Prepared: 16-12-2021

Enterprise Risk Report

Time Frame: 02-01-2020 – 16-12-2021

WHAT WAS ANALYZED



Total Devices 17

59 %

41 %

1199 Networks

29 Phishing Visibility

15014 Apps

Phishing

29 URLS where identified on 4 Devices

FACTORS CONTRIBUTING TO YOUR RISK

Which of your devices are at risk

- 0 compromised devices
- 6 % devices with active critical risks
- 65 % devices on vulnerable OS's
- 24 % devices vulnerable to hardware exploits
- 76 % devices that can be updated

How many devices are running risky apps or profiles

- 3 malicious apps found
- 3447 apps with high privacy and security scores
- 29 side-loaded apps detected
- 4 unmanaged profiles installed

How many devices have exposed to rogue networks

- 2 devices connected to rogue Wi-Fi networks

WHY IT MATTERS

Phishing – Phishing is often the start of a wider attack and greatly increases the risk associated with the device and any user identities being used there.

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

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.