Skycure®
Mobile Threat Defense

Government Devices are Top Targets for MobileThreats

Today, mobile devices are a key component of anyone's day-to-day activities and tied directly to their personal and work productivity. This means potentially sensitive data resides on and passes through these devices, and many government roles require some level of clearance.

Attackers know this, which is why they've begun specifically targeting government agencies, employers and contractors as their primary target. We're seeing twice as many security incidents on government mobile devices than non-government mobile devices:

How many of your devices are exposed to attack?

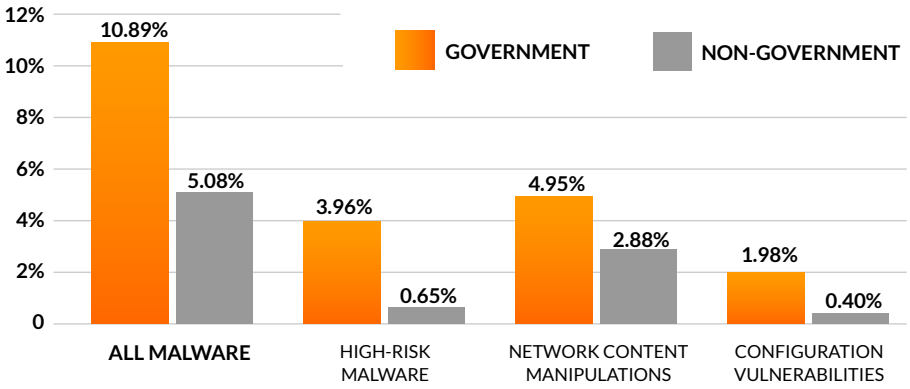

Figure 1: Difference in incidents on govt v. non-govt mobile devices, compiled via Skycure Global Mobile Threat Intelligence.

As government devices continue to become a more attractive target for attackers, government agencies must be prepared to defend against and properly mitigate these threats across the complicated (and always evolving) mobile threat landscape.

"Basic policy enforcement will not suffice indefinitely. As mobile attack techniques become more practical and realistic, enterprises will be required to more quickly 'step up their games' in terms of security."

— Gartner
"Guide to Mobile Threat Defense"

Government devices encountering **network threats:**

18%

Government devices with **malware:**

11%

Mobile devices must be kept safe and secure while maintaining end user privacy, device performance.

Mobile Security has eclipsed what EMM and MDM alone can provide. As Gartner outlines in their When and How to Go Beyond EMM and Ensure Secure Enterprise Mobility report, "EMM solutions have limitations in that they are unable to detect platform and app vulnerabilities. They are also limited in their capacity to detect malware threats on their own. Mobile threat defense (MTD) tools help to fill this void by protecting enterprises from threats on mobile platforms."

Within the mobile landscape, there are four major threat vectors that government agencies must now defend against:

Malware Defense

Network Defense

Vulnerability Defense

Physical Defense

EXAMPLE RISKS

- Repackaged Apps
- Spyware
- Ransomware
- Keyloggers

- SSL Decryption
- SSL Stripping
- Content Manipulation
- ARP Spoofing

- Malicious profiles
- Stagefright
- Rooting
- Jailbreaking
- Clickjacking

- Stolen device
- Unauthorized access
- USB Debugging
- Plugjacking

CORE MOBILE THREAT DEFENSE CAPABILITIES

Organizations like Gartner and the SANS Institute have outlined key capabilities that governments should look for in a comprehensive mobile threat defense solution, including:

- Multi-layered detection across multiple parameters
- Built-in Mobile App Reputation Service (MARS)
- Proactive blocking of malicious app installs

- Active Honeypot technology
- Protect sensitive resources with or without Internet
- Automatic secured communication during attacks

- Continuous monitoring of platform integrity
- Machine-learning anomaly detection and behavioral profiling to detect unauthorized activities on device
- Alert when OS updates are available (before manufacturer does)

- Integration with leading EMM vendors
- Bi-directional communications regarding device compliance, policy enforcement
- Basic MDM functionality when no EMM is in place

About Skycure

Skycure's layered approach to mobile threat defense relies on the device itself to provide the first line of defense, cloud-based servers to perform secondary, deep analysis and integrate with critical enterprise infrastructure, and crowd-sourced threat intelligence collected from every Skycure mobile app across the globe to enable predictive determination of both good and bad developers, apps and networks. Additionally, Skycure Research Labs continues their innovative approach to staying ahead of malicious hackers by diligently developing new methods of predicting and detecting unknown threats and identifying some of the most-discussed mobile device vulnerabilities of the past few years, including at least one for every major iOS release.

hello@skycure.com | 1-800-650-4821 | @SkycureSecurity

Skycure®