Why Enterprises Need App Threat Intelligence and Defense

Apps are one of the greatest mobile threat vectors to the enterprise. Criminals and governments recognize this fact and are currently exploiting weaknesses in companies with BYOD and COPE programs.

App stores cannot detect targeted attacks or enterprise threats. Similarly, network threat detection alone isn't adequate for mobile employees.

By the numbers: Riskware is rife in the enterprise

Riskware are seemingly innocuous consumer apps that expose enterprise users to data leakage, credential theft, and the exfiltration of private information that can be used to target specific employees in advanced attacks. According to Gartner, 75% of all mobile security breaches will be through apps.[1]

- **20,000:** The average number of apps an enterprise with 2,000 BYOD users is exposed to[2]
- **30:** The number of countries those apps will communicate with
- **25:** The percentage of iOS apps that access users' contact databases, exposing companies to targeted APTs, spear phishing, and employee policy violations
- **53:** The percentage of all app publishers without privacy policies, who may sell private data to spammers and criminal networks with impunity
- **6:** The percentage of Android apps that read browser histories, exposing users and companies to targeted attacks

Even companies using iOS devices need app threat protection

Companies that use iOS devices in their mobile environments, especially those rolling out BYOD programs, need to understand and control malicious, promiscuous, and data mining apps. A wide range of app behaviors expose companies to targeted attacks, data loss, and not complying with security polices.

Dangerous behaviors exhibited by iOS apps may include:

- **Mining contact databases and calendars:** Because this data is linked to corporate Active Directories and entire organization's contact information may be leaked, opening it up to phishing and advanced persistent threats
- **Accessing Box, Dropbox, Evernote and other cloud services:** Apps may mine and copy the data stored within these services
- **Profiling corporate Wi-Fi and VPN networks:** Apps may send that data to potential attackers, who are usually offshore

[1] Gartner, 2014, http://www.gartner.com/newsroom/id/2846017
[2] Marble Security customer data

MARBLE SECURITY

- **Masquerading as enterprise sanctioned and signed apps:** These apps may install targeted Trojans, bypassing Apple App Store controls
- **Morphing into a malicious apps:** Some apps may change behaviors to target companies and individuals after App Store approval
- **Legitimate apps** with security vulnerabilities that expose corporate data

Only an app threat intelligence and defense solution can detect and combat these behaviors and prevent attacks on the enterprise.

Containerization alone is an insufficient defense

Leading enterprise mobile management (EMM) vendors, such as MobileIron and AirWatch, recommend that a complete mobile security solution include three layers of defense: device management, containerization, and app threat prevention. Less than 10 percent of all government agencies and corporations employ all of these safeguards.

Organizations mistakenly believe that a containerized environment alone can protect against threats from dangerous or malicious apps.

In fact, containerization without app threat prevention can only protect against risky apps when:

- BYOD devices are not allowed to connect to corporate Wi-Fi or VPN, which in itself is highly unpractical. If BYOD devices connect to a corporate network, malicious, promiscuous, or data mining apps will mine network settings and transmit that information
- All apps are verified to have secure communications, no man-in-the-middle vulnerabilities, no heart bleed or other SSL vulnerabilities and not communicating with other non-containerized apps
- All access to corporate data is containerized, such as email, address books, calendars, and all corporate apps.

About Marble Security

Marble Security is the leading provider of mobile threat intelligence and defense. The company's research and response team of developers and cybercrime specialists has analyzed millions of Android and iOS apps, detecting apps with malicious and privacy-leaking behaviors that frequently lead to advanced persistent threats (APTs), spear phishing attacks on employees and other information security risks.

AppHawk by Marble Security delivers comprehensive, correlated threat intelligence for Android and iOS devices. Marble integrates directly with mobile device management (MDM) or enterprise mobility management (EMM) solutions, providing granular risk control for bring-your-own-device (BYOD) programs.

Marble Security, Inc.
68 Willow Road
Menlo Park, CA 94025

T: 855.737.4370
sales@marblesecurity.com

www.marblesecurity.com