Marble Labs, the threat research unit of Marble Security (www.marblesecurity.com), analyzed more than 200,000 Android apps during February 2014, with the goal of creating insight into which categories of apps pose greater risk to enterprises and their employees, as well as consumers.

The objective of this report is to determine the variance of risky behavior of apps in different categories. It is not intended to indicate that baseline behavior is safe for all enterprises and employees, as this will differ by industry, the types of data or accounts that employees access, and whether companies issue devices to employees or allow them to use in their own devices (BYOD). Rather, this report highlights how apps in different categories vary in risky behavior when compared to other categories.

**Methodology**

This Marble Labs security report is based on the analysis of more than 200,000 apps during the month of February 2014. The analysis is based on static, dynamic and behavioral analysis of these apps by Marble Labs.

**Static analysis** of apps includes analyzing the permissions that these apps request, analyzing which data these apps access, and comparison of the apps to known malicious apps and advertising libraries that may create data leakage and privacy risks.

**Dynamic analysis** of apps includes running apps over time to discover evolving threats that may not have been detected when these apps were approved for publishing on popular app stores and marketplaces (eg. Google Play and Apple’s App Store). It also includes the analysis of which network location these apps communicate with over the Internet, and correlates these to a growing database of hundreds of thousands of criminal and malicious web addresses.

**Behavioral analysis** involves running apps in an instrumented, virtualized kernel to determine the actual behavior of the apps, and where network traffic is sent. This unique capability is based on the app analysis of numerous industry-leading researchers. Marble Labs’ dynamic, behavioral analysis is unique in the industry, and provides companies and consumers with the most accurate detection of apps that leak data, expose passwords and other authentication credentials, and expose companies to Advanced Persistent Threats.
Marble Labs measured threats in the following risk categories:

- **Privacy** – These apps may leak user identifiable information to third parties
- **Data Leak** – These apps expose companies to loss of data, such as files and corporate directory information
- **Account Takeover** – These apps exfiltrate or access user credentials, creating the risk that online accounts may be taken over
- **Device Takeover** – These apps expose data about the device and its network services that may result in device takeover or cloning
- **Malware** – Apps that are purely malicious are categorized as Malware

Apps in 34 different categories were analyzed by Marble Labs. For each app, we assigned a risk score in each of the five risk categories listed above. The risk score is based on weighted scores of the permissions that an app requests, the APIs that an app can call, actual code execution of those APIs, and whether sensitive data is actually sent from the device.

A mean risk score for each of the five risk categories is computed based on the risk scores of all analyzed apps in this study. Apps that exhibit risky behavior that is two standard deviations or higher than the mean risk score of all apps in any one of the five categories are deemed as risky. This methodology is applied to apps in each of the 34 app categories. This allows Marble Labs to gain insight into the various app categories and their relative riskiness.

**Results at a glance**
Potential impact to enterprises and consumers

Seemingly innocent apps can pose risks – Even wallpaper apps, which show users nice pictures in their background, pose more of a risk than is often recognized. Many of these apps are monetized through advertising, and expose more data than users expect. Business productivity apps can pose data leak risks to enterprises, as they connect to shared document services, or upload and download documents.

Health, fitness and lifestyle apps read user data – Health, fitness and lifestyle apps often poorly protect user data and privacy. This is presumably because developers of these apps want to learn as much about a user as possible in order to tailor fitness programs, as well as to offer other products for sale. However, this data mining can expose corporate data or address book information, which then leaves a company’s control. In fact, some health fitness and lifestyle apps display characteristics common to malware.

Legitimate medical apps are safer – Legitimate medical apps issued by hospitals, HMOs and major health companies appear to be quite safe as a category. Their risk ratings for data leak, device takeover, account takeover are low. However, privacy leak ratings are more mixed, leading to a higher score than expected in this analysis.

Communication apps more risky than previously thought – Communications apps can pose a risk to companies. Many of these apps mine the user’s contact database. If those databases are connected to the corporate Active Directory, then apps can mine that data and send it to third parties over the Internet. These apps often mine phone call logs and SMS logs, too. It can be very risky for business to allow employees to use communications apps on their devices that have not been analyzed, especially if their contact database is connected to a corporate directory.

Social media apps are among the riskiest – An analysis of more than 4,500 different social media apps determined that this category poses a high risk to companies, employees and individuals. Some social media apps are very well behaved, and pose little risk. However, there are hundreds of social media apps that expose users to data loss, account takeover, and privacy violations. More than 100 social media apps exhibit behavior common to that of malware.

Weather apps not so stormy – Of the more than 1,200 weather apps that were analyzed in February, nearly two-thirds posed little or no risk to companies, employees, or individuals. Only 13 posed a high risk of data leakage, which may affect companies if employees have those apps on their mobile devices.

News and magazines seeking ways to monetize – News and magazine apps constantly look for ways to monetize their content. Many of these apps compile code from multiple advertising networks. Much of that risk profile is due to privacy leakage, however enterprises should restrict apps that expose users to other risks, such as account takeover.
Sporting behavior from sports apps and games? – Of the more than 5,500 sports apps analyzed, Marble Labs found privacy risks across the board. In fact, some of the riskiest apps for privacy violations were found in this category. While the majority of these apps were of low risk on the privacy risk vector, with 95 percent posing little to no risk of corporate data loss, Marble Labs found that the remaining five percent demonstrated behavior consistent with malware. Needless to say, these apps should not be permitted on employees’ devices.

Conclusion

The March 2014 Marble Security Mobile App Threat Report provides insight into which categories of apps pose more risk than others for data leakage, privacy violations, account takeovers, device takeovers, and malicious behaviors. Different app categories appear to pose more risk to companies and their employees than others. Some surprises were uncovered in this report, where apps such as business productivity and communications pose more risk than previously understood.

Companies should monitor or restrict use of these apps on devices that connect to corporate networks, data or online cloud services. Risk-based restrictions are more important than ever, given the ever-growing number of apps and the increased use of mobile devices in the enterprise.

Learn more

For more information or to purchase Marble’s mobile security platform, call toll free 855.737.4373, 408.737.4300; or email, sales@marblesecurity.com.