

REMINDER: Emailed to a group account. Do NOT reply using email group account.
For comments or inquiries email infosec@pjlhuillier.com.



Feb 15, 2013 Release # 203

-- Begin Transmission --

Why IOS is Safer Than Android? – Part 1

Google's Android platform has become a larger target for mobile malware writers than Apple iOS. This could be a result of Android's popularity—with more than 1 million activations per day, Android smart phones command a 59% market share worldwide. However, the relative vulnerability of Android vs. iOS comes down to the level of control the vendors have over products and the marketplace for development and distribution of apps.



Mobile malware writers know the best way to infect as many devices as possible to attack central application markets. The cybercriminals plant applications that include hidden (obfuscated) malicious functionality in an attempt to avoid detection included in the vendor's application vetting process (e.g., Google Bouncer).

Apple and iOS

Apple's walled garden App Store—where applications are fully vetted before being made available to customers—has prevented widespread malware infection of iOS users. As a centralized point of distribution, the App Store provides users with confidence that the apps they download have been tested and validated by Apple. Evidence of malicious malware showing up in the App Store is anecdotal at best, as Apple does not typically volunteer such information. However, it's safe to assume that since Apple does not make APIs (Application Programming Interface (APIs)) a protocol intended to be used as an interface by software components to communicate with each other available to developers, the iOS operating system has fewer vulnerabilities.



However, iOS isn't 100% invulnerable. Take the tale of Charlie Miller, a security researcher who deliberately created a suspicious application and submitted it to Apple. Apple initially approved the application, which uncovered a bug in iOS. As soon as Apple discovered that the application was suspicious, the company suspended Charlie's developer account for one year.

To be continued...

-- End of Transmission --

Information Security: It's a Shared Responsibility

REFERENCE(S): <http://www.sophos.com>

INTERNAL USE ONLY: For circulation within the PJ Lhuillier Group of Companies only.