Android developers have another challenge on their hands. Privateer Labs has reported that a certain component in Android OS can be exploited by malware to subvert the anti-virus software rendering anti-virus scans on your Android device ineffective. The malware can even corrupt the anti-virus software and use it as a malicious app. Reiley Hassell, the founder of the security firm Privateer Labs, declined to identify the Android OS component that is vulnerable, since he is taking it up with Google.

While Android mobile applications have had a stupendous growth in range and depth, it has also attracted its fair share of threats. Android overtook Symbian as the most malware-targeted mobile OS in the 2nd quarter, McAfee has reported. Riley indicated the recent security vulnerability is "definitely an Android problem". The software from the Android development market is not checked beforehand by the marketplace and the users end up with malicious apps masquerading as genuine ones.

"App phishing" is another strategy of cyber criminals where the users are tricked into downloading and installing a genuine-looking app but that actually contains a Trojan, which alerts the developer when the user activates the app. In case of a banking app, the developer can hijack the session by posing a fake authentication screen stealing the login details, resulting in loss of personal and financial data. The Trojanized malware Zitmo also known as ZeuS acts as a legitimate banking activation application, accepts incoming SMS messages, and forwards them to a remote Web server. The onetime pass codes banks send to users via SMSes for two-factor authentication purposes can be stolen by Zitmo-like apps.

Riley opined that this is a "tough problem to solve" and further elaborated that this needs to be solved by the Android development community as a whole. Determining who is to police the sanctity of Android apps is a challenge per se. Chris Wysopal of Veracode, an application security provider, has called for scanning of Android mobile applications for malware before they appear on the market. A signature-based scanning for malware can be enforced. Google this year has already revoked malicious apps twice from the market, once in March when it removed over 50 malicious apps and then again in June it removed a 2 dozen. This high attrition can slow down the growth of Android mobile applications.

Unlike the closed development ecosystem of Apple OS, Google has followed an open architecture model, where anyone can develop an Android application and put it in the market. Local as well as offshore Android development has taken off in a big way resulting in multitude of apps that are half-baked and incomplete. Some Android users download apps from

unauthorized online stores presenting a threat to the open source Android development architecture.

An Android mobile applications user can mitigate the risk of being targeted by malware by:

- Downloading apps only from trusted sources and from developers that are known by name and are rated
- Checking permissions that the app requests and matching it against its stated purpose

Being alert for any unusual phone behavior like installation of unknown applications, sending of SMSes to unknown recipients, or automatic placement of phone calls.

telefon dinleme