Igexin advertising API brings spyware to steal user information

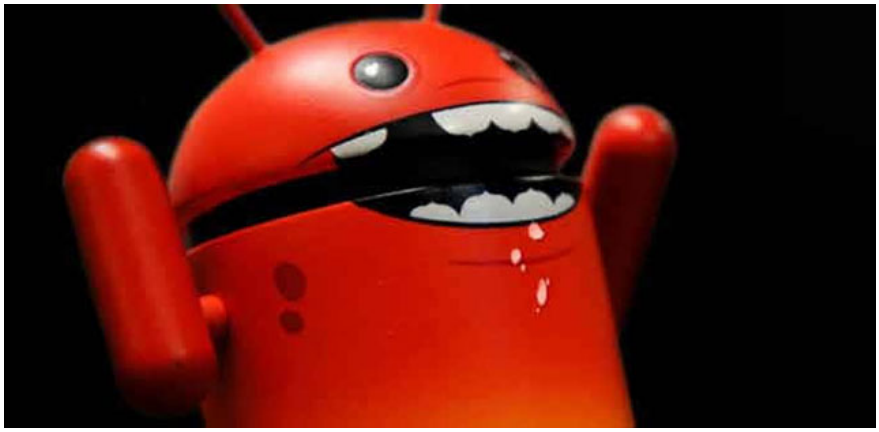
Mobile developers, if you find an easy-to-use advertising API, make sure it's not snoopware.

Mobile developers, if you find an easy-to-use advertising API, make sure it's not snoopware.

It is an important lesson that Lookout Security has found when analyzing the Igexin advertising software development kit (SDK) and showing hundreds of applications that cannot be found ('not found') on Google. Play.

This SDK has tracked a lot of mobile phones, saved call time, phone numbers, call status and sent back to igexin.com page. It is available on more than 500 applications that Lookout checks, after company researchers recognize the application communicates with the IP address associated with malware and begins to wonder.

'We found the application to download large files that were encrypted after making multiple requests to REST API at *http:/// sdk [.] Open [.] Phone [.] Igexin.com/api.php* one The endpoint is used by the Ads SDK of Igexin ', the company explained. 'Downloading encrypted files and the presence of calls on com.igexin has namespaces to *dalvik.system.DexClassLoade* of Andoird (used to separate classes (classes) from .jar files and. apk) is enough to show that there is a need for further analysis of malware capabilities. '



SDK to bring spyware to your computer and steal user information

Since then, researchers have found a number of SDK versions with framework that allows clients to download random code, get instructions from endpoint http:/// sdk [.] Open [.] Phone [.] Igexin [.] com / api.php.

The application will then download the executable JAR file on the 'Phone Home' of the SDK. Neither the user nor the application developer can control the occurrence: 'Users and application developers cannot control what is executed on the device after executing the remote API request'.

The amount of information that the app obtains is still limited to permissions on Android, but Lookout says that besides the call history, there is still an application that takes user history information.

You finished reading the article "**Igexin advertising API brings spyware to steal user information**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.

© 2019 TipsMake.com