Android: Researchers tell troubling findings of pre-installed software

March 27 2019, by Nancy Cohen

Credit: CC0 Public Domain

A study "An Analysis of Pre-installed Android Software" says pre-installed Android apps amount to a boatload of privacy issues. Just ask IMDEA Networks Institute, Stony Brooks University, Universidad Carlos II de Madrid and ICSI. They authored the study.

They talked about tracking and advertising services embedded in many pre-installed apps, and the partnerships that allow information to be shared, and control to be given to various other companies through permissions, backdoors and side-channels.

ICSI stands for International Computer Science Institute. IMDEA is a research organization in Madrid. Its focus is on computer and communication networks.

The problem traces back to some hardware vendors; they are pre-loading Android devices with apps that may absorb user data. Oh, and don't blame stupid, careless users (at least for allowing the harvesting apps). They are not aware because they are not asked to sign on to anything.

The study authors found that a number of smartphones enabling third-party access to user data, without consent, were involving non-Google pre-installed apps.

EL PAIS: Past research on the risks to privacy from cellphones may have looked at Google Play but this team instead analyzed pre-installed apps on standard phones "and it turns out that, due to a complex ecosystem of manufacturers, mobile operators, app developers and service providers, the guarantees offered by Android are looking less than foolproof."

Helpful to point out here, as Reuters reported, that device makers, with Android's open source nature, could be able to customize and package other apps with the operating system.

The study turned the spotlight on some 1,700 devices from 200 hardware makers. The probe involved 82,000 pre-installed apps.

ZDNet said that "According to researchers, the most used permission among apps that also embed a third-party SDK is the permission to read

system logs, followed by the ability to mount/unmount storage space, and the ability to install other apps."

Harry Domanski for *TechRadar* pointed to those vendors that provide their own version of the open-source operating system. In turn, they abuse the platform to release products with "integrated data-collecting services."

The ball may at times fall in your corner—sometimes. Downloading "a data-harvesting app and agreeing for it to use all your details for marketing purposes" is ok, said Roland Moore-Colyer for the *INQUIRER*.

The issue here is that the study is looking at apps coming at you pre-installed and not making it clear to you about data-harvesting activities. As Moore-Clyer pointed out, this data harvesting could be deliberate or just the result of "some dumb implementation."

Catalin Cimpanu looked at the study and made note of some additional rubs. He told *ZDNet* readers that "many pre-installed apps (also referred to as bloatware) can't be removed, and also use third-party libraries that secretly collect user data from within benign-looking and innocently-named applications."

Given all that, as much attention should be focused on solutions as well as causes. In looking for solutions, the landscape is complicated. The difficulty lies in the nature of the supply chain. Moore-Clyer said that "the supply chain of both software and hardware can be quite convoluted with all manner of deals being made to secure certain apps and services on devices, without anyone to oversee such activity."

Domanski referred to a "myriad of actors" ranging from software developers to advertisers, "potentially involved in secret partnerships."

EL PAIS: "An Android cellphone is not produced by just one manufacturer. The chip comes from one company and the updates of the operating system will possibly be outsourced to another, while separate software will be added by the mobile operators and distributors. There are a lot more players involved in the final product ...the result is an ecosystem so complex that all the players can sidestep the responsibility of where our personal data ends up...And what belongs to everyone belongs to no one."

The authors presented their "recommendations to improve transparency, attribution, and accountability in the Android ecosystem."

The *INQUIRER* said one suggestion has been for a third party to oversee what pre-installed apps get up to and ensure they adhere to privacy guidelines. "The boffins reckon Google could take on this role given its power in licensing Android."

Another suggestion was for governments and regulatory bodies to enact regulations.

Domanski said that a globally trusted regulatory body, as the authors' suggestion goes, would sign software certificates rather than the vendors.

Meanwhile, tech giants are under the spotlight far and wide because of the general concern over the tracking and harvesting of user data ("Pre-installed apps recently have drawn increased scrutiny," Reuters remarked).

TechCrunch reported on Google's reaction to the study. Natasha Lomas wrote, "Google has responded to the paper with the following statement—attributed to a spokesperson."

"We appreciate the work of the researchers and have been in contact

with them regarding concerns we have about their methodology. Modern smartphones include system software designed by their manufacturers to ensure their devices run properly and meet user expectations. The researchers' methodology is unable to differentiate pre-installed system software—such as diallers, app stores and diagnostic tools–from malicious software that has accessed the device at a later time, making it difficult to draw clear conclusions."

Google went on to state that they worked with "OEM partners" to help ensure the security of apps they decide to pre-install on devices. They also provide "tools and infrastructure" to help partners scan their software. Last but not least, they stated they gave partners policies regarding the safety of pre-installed apps, "and regularly give them information about potentially dangerous pre-loads" they identified.

Well, that is interesting.

The authors of the paper had said that the supply chain around Android's open source model lacked transparency and has facilitated potentially harmful behaviors and backdoored access to sensitive data and services without user awareness.

The authors, in their final remarks, said, "Despite a full year of efforts, we were only able to scratch the surface of a much larger problem. This work is therefore exploratory, and we hope it will bring more attention to the pre-installed Android software ecosystem and its impact on users' privacy and security."

More information: An Analysis of Pre-installed Android Software, haystack.mobi/papers/preinstal … droidSW_preprint.pdf

© 2019 Science X Network

Citation: Android: Researchers tell troubling findings of pre-installed software (2019, March 27) retrieved 24 April 2024 from
https://techxplore.com/news/2019-03-android-pre-installed-software.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.