If using an Android phone, be careful: You may be being tracked without knowing

Android - Google's mobile operating system has behaviors that silently monitor users that make them unaware. More seriously, it can also access a user's personal data store through a large number of pre-installed applications that are virtually difficult to uninstall.

Recently, a study prepared and conducted by the IMDEA Networks Institute with Carlos III Madrid University, and legally supported by the Spanish Data Protection Agency, discovered that the licensing model The Android operating system as well as the platform's applications can allow a large number of malicious agents to track and steal users' personal information around the world.

More specifically, this is a survey conducted by Spanish scientists with 'the highest seriousness', revealing that Android - Google's popular mobile operating system has taken actions silently monitoring users that makes them unaware. More seriously, it can also access a user's personal data store through a large number of pre-installed applications that are virtually difficult to uninstall.

1. Detects code execution vulnerabilities in WinRAR, noting more than 100 infringement cases

Besides, these malicious acts will not depend on the brand or the manufacturer. Whether you are using Huawei, Samsung, Xiaomi or LG phones, it can still happen. Research by Spanish security experts found that the main cause of the problem lies in the operating system and in this case, most people are affected because Android is

universal mobile software. The most variable on the market today. According to the latest data from Kantar Worldpanel Comtech alone, in the case of bullfighting, by the end of 2018, there were 89.9% of the terminals in this country running on the Android platform, while this figure of Apple , with iOS operating system, still maintained at 9.9%.

However, things didn't stop there. According to Kantar, up to 3 out of 4 smart phones have been sold in major markets in Europe (England, Spain, France, Italy and Germany) using the Android operating system. Therefore, it is not surprising that this operating system has conquered 75.8% of European users (only 23.5% of phones sold in Europe by the end of 2018 are iPhone). Only in the US market, Android cannot create overwhelming victory before iOS when Apple's market share, as of the end of 2018, stood at 43.7%, while Android's market share reached 56%.

So it can be seen that, although most manufacturers build their own customized versions, basically, most of the smartphones currently in use around the world work with Android. This means that most users who just turn on their smartphone are at risk of being monitored without knowing it.

1. Counter-Strike 1.6 features new Zero-Day, allowing malicious servers to hack gamers' computers

The conclusions of the study carried out by the IMDEA Networks Institute based at Leganés and University of Carlos III Madrid are highlighted in an article titled 'An Analysis of Pre-installed Android Software' (roughly translated). : Analysis of pre-installed Android software). And this article was published by the Spanish Data Protection Agency (AEPD) on Monday 19 March due to its huge impact on privacy issues and data protection laws. personal citizenship.

In fact, AEPD plans to elaborate on this study as well as its conclusions for the operational subgroups of the European Data Protection Commission (CEPD), a direct management agency. The European Union, from there joined with other European data protection agencies as well as European supervisors to find a solution to the problem.

Access personal information

Research by Spanish security experts has looked at more than 82,000 pre-installed applications on more than 1,700 Android devices produced by 214 different brands. In this way, the researchers were able to identify and point out the toxic agents present in the pre-installed software on Android, and use privilege access to system resources to retrieve fish data. benevolent user. However, things don't stop there. The investigation also shows

trade agreements between Android device manufacturers and third parties, including organizations that monitor, track users and provide advertising on the Internet.

1. DDoS is ranked as the top threat for businesses in 2018

One of the main conclusions of the study refers to how the licensing model works on the Android operating system and its applications. In fact, this model has absolutely nothing to do with the standards that Google requires developers to follow before posting their application to Play Store. Therefore, this can also be considered as one of the main reasons that allow a large number of malicious agents to track and retrieve personal information from users at the operating system level.

Besides, the problem is that users are completely unaware of the existence of these agents, while personal information is still collected regularly. AEPD has specifically emphasized the harmful effects of this behavior on user privacy. In addition, the presence of such software, accompanied by system privileges, means that users will not be able to easily remove them.

Dark business deals

Researchers have identified more than 4,845 proprietary or custom licenses in the production of terminals. This type of permission allows Google Play 'apps' to bypass the licensing model on Android to access user data without their consent when installing a new 'application'. Normally, when users want to download an application on their terminal, they will access the Play Store app store and when the download process is complete, the operating system will consult users in installing or canceling the application. However, this does not happen to Android-based applications that analysts have considered in the study. Therefore, it can be said that in this case, the user does not have control over his or her terminal.

1. Android apps contain malicious code that uses motion sensors to avoid detection

But it has not stopped here, when analyzing many applications preinstalled on Android devices, researchers have identified the identity of more than 1,200 companies, organizations, as well as the current of more than 11,000 libraries (SDKs) of third parties, most of which involve online advertising and monitoring services for commercial purposes. These preinstalled applications are executed with separate privileges, and in many cases are capable of making users unable to uninstall them.

A thorough analysis of the behavior of 50% of these applications shows that a significant portion of them contain dangerous or unwanted behaviors, such as malware patterns, Trojans in general. or pre-installed software to facilitate other fraudulent acts to work more easily on the system.

Regarding the information provided when users use a new terminal, the researchers have also noticed the lack of transparency of the application and the Android OS itself shown through the display. Show users the complex integration between different rights, thereby limiting their ability to make decisions and at the same time the ability to manage their personal information.

Usually, the reason manufacturers (smartphones) choose Android for their device is because this is an open platform (open source). Therefore, they can completely edit and design customized Android version according to their products and business purposes. For example, to improve the performance of products and add specific functions to help the product make a difference and class in the market.

1. Malware and user security bugs are found in top free VPN applications

As explained by researchers, usually when manufacturers distribute their own customized version of Android, they will also include more software (applications) by themselves or a third party (Mobile operators, social networks or advertising services) developed. 'These are usually popular pre-installed applications that ordinary users do not have a lot of expertise to uninstall, remove from the device and cannot verify technically whether whether or not the application complies with regulatory data protection guidelines, 'the researchers warn.

That is why we can clearly state that there is a lack of transparency in the pre-installed application process as well as operating on a specific Android device, since users are completely unaware of it. This situation is happening and how it happens, as well as the privacy infringement conducted silently.

The absence of academic and systematic analytical tools on risks created by pre-installed software on Android devices prompted Spanish computer scientists to conduct research. this. At the same time, the study also paved the way for the implementation of appropriate sanctions requiring manufacturers and service providers related to Android operating systems to act to improve the quality of products and Its services, as well as regain users' trust.