What pre-installed adware means for mobile users

Following analysis of attacks on mobile devices, Kaspersky has uncovered that 14.8% of its users who were targeted by malware or adware in 2019 suffered a system partition infection, making the malicious files undeletable.

Source: www.pexels.com

Moreover, pre-installed default applications also play a role here: depending on the brand, the risk of undeletable applications varies from 1-5% in low-cost devices and goes up to 27% in extreme cases.

A system partition infection entails a high level of risk for the users of infected devices, as a security solution cannot access the system directories meaning it cannot remove the malicious files.

According to Kaspersky researchers, this type of infection is becoming a more common way to install adware – software created to display intrusive advertising. Infection can happen via two paths: the threat gains root access on a device and installs adware in the system partition, or the code for displaying ads gets into the firmware of the device before it even ends up in the hands of the consumer.

Among the threats uncovered in the system directories, Kaspersky found a variety of malicious programs - from Trojans that can install and run apps without the user's knowledge to less threatening, but nevertheless intrusive, advertising.

In some cases, adware modules were pre-installed before the user even received their device, which could lead to potentially undesired and unplanned consequences. For instance, many smartphones have functions providing remote

access to the device – if abused, such a feature could lead to a data compromise of a user's device.

A few vendors have openly admitted to embedding adware in their smartphones. While some allow it to be disabled, others do not, and they describe it as part of their business model to reduce the cost of the device for the end-user. Often, the user has little choice between buying the device at the full price, or a little cheaper with lifetime advertising.

"Our analysis demonstrates that mobile users are not only regularly attacked by adware and other threats, but their device may also be at risk even before they purchased it. Customers don't even suspect that they are spending their cash on a pocket-sized billboard. Some mobile device suppliers are focusing on maximising profits through in-device advertising tools, even if those tools cause inconvenience to the device owners. But this is not a good trend – both for security and usability. I advise users to look carefully into the model of smartphone they are looking to buy and take these risks into account – at the end of the day it is often a choice between a cheaper device or a more user-friendly one," comments Igor Golovin, Kaspersky security researcher.

View the full report.