Detects 146 security holes in pre-installed Android applications

It is time to apply strict control procedures to the applications developed by the OEMs themselves.

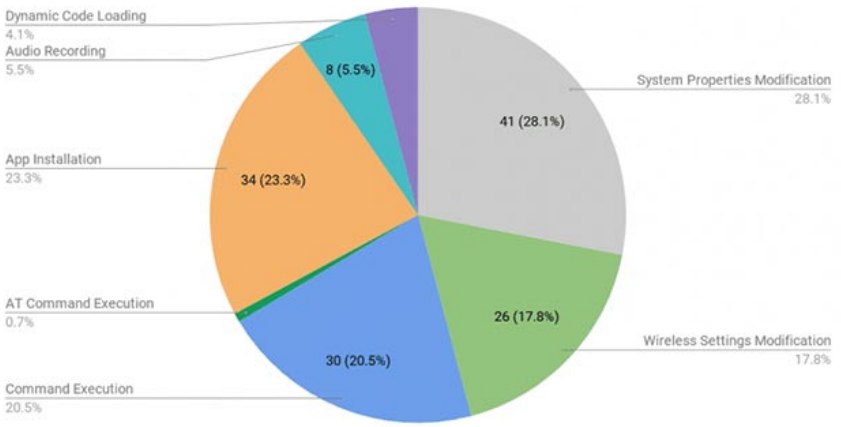
Unless you use Google Pixel or a handful of Android-powered smartphones, you'll never get the most 'original' experience of this operating system because nearly all smartphone manufacturers choose to. Develop a customized Android version to create unique features for your product.

The development of customized Android platforms is nothing bad, even praiseworthy because it can be considered as a factor that helps create diversity - a characteristic factor when it comes to the Android ecosystem. However, the problem is that most custom versions not only contain bloatware (software that is pre-installed on the device by the manufacturer), but also full of security flaws.

Researchers from security firm Kryptowire recently discovered a total of 146 security holes in pre-installed applications on customized Android versions of 29 OEMs (also known as device manufacturers).), ranging from simple vulnerabilities such as unauthorized application installation, to serious issues such as the ability to modify system settings, and even sneakily take screenshots, record calls to Send data to a third party.

Notably, this list also contains applications from some famous OEMs, with a large number of users such as Asus, Samsung and Xiaomi.

Since last year, Google has used a system called Build Test Suite (BTS) to scan harmful pre-installed applications on custom Android builds for devices that come with its services. But despite the emergence of such security checks, the malicious application continues to slip through the 'narrow gap' and is evidenced by research by Kryptowire experts.



One thing worth noting is that many of the applications that contain vulnerabilities are those of the OEMs themselves. When third-party applications downloaded by users are found to contain malware, there is at least one solution: uninstall. But with the application installed by the manufacturer is different, users will not be able to delete these applications and have to accept 'living with floods'.

In addition, there is no guarantee that OEMs will release a security patch for these applications, and things will be bad for users of older devices, which have stopped supporting.

For its part, Google has also made great efforts to eliminate harmful applications on its platform. The Mountain View giant has recently teamed up with three reputable security companies: ESET, Lookout and Zimperium to push further tighter measures against malicious third-party applications before they can. harm to users.

Perhaps it is time to apply the same rigorous control procedures to the applications developed by OEMs themselves.