
***Issued 3/5/18***

## Android Phones Caught Selling with Pre-Installed Factory Malware

More than 40 Android phone models, most of them manufactured by companies in China, ship with pre-installed malware that was injected into the firmware straight from the factory. Security company Dr. Web says that it came across a new Trojan called Android.Triada.231 in the firmware of several Android devices back in mid-2017, and after an in-depth research, it discovered that over 40 models are likely to be affected. Most of the compromised phones are in the low-end category, and they include devices from Leagoo, Doogee, Umi, and Cubot. Newer models include the Leagoo M9 launched in December. Dr. Web explains that it contacted the affected companies to report the problem, and it discovered that at least in one case, the culprit was a partnership with a software developing company in Shanghai which required Android OEMs to pre-install one of its apps into the image of the mobile operating system. “These Trojans infect the process of an important Android system component, Zygote. This process is used to launch all applications. Once the Trojans inject into this module, they penetrate other running applications,” Dr. Web explains in its analysis. Removing the malware from a phone isn’t possible without installing a clean version of the operating system, in which case the manufacturer is the only one that can help. If the device is rooted, security applications can help clean the infection.