**Backdoor Discovered in Low-Cost Android Devices and Tablets**

Security researchers at Russian antivirus firm Dr. Webhave have discovered malicious firmware in cheap android smartphones and tablets that collects information from, displays ads and embeds APK files on the device. The two types of downloader Trojans i.e. ***“Android.DownLoader.473.origin”*** and ***“Android.Sprovider.7”,*** exist in firmware of many of the Android devices that work on MediaTek platform, mainly sold in Russia.

A big threat to Android app security, the Trojans can not only gather information of infected devices but also contact their command-and-control server, upgrade them automatically, secretly download and install programs upon orders received from the server, and run every time the device turns on or restarts.

The following is the set of Android devices which can potentially be infected with the Trojans.

* 7 MID
* Bravis NB105
* Bravis NB85
* Digma Plane 9.7 3G
* Explay Imperium 8
* General Satellite GS700
* Irbis TX97
* Irbis TZ43
* Irbis tz56
* Irbis tz70
* Irbis TZ85
* Itell K3300
* Jeka JK103
* Lenovo A319
* Lenovo A6000
* Marshal ME-711
* MegaFon Login 4 LTE
* Nomi C07000
* Optima 10.1 3G TT1040MG
* Oysters T72HM 3G
* Perfeo 9032\_3G
* Pixus Touch 7.85 3G
* Prestigio MultiPad PMT5001 3G
* Prestigio MultiPad Wize 3021 3G
* Ritmix RMD-1121
* SUPRA M729G
* SUPRA M72KG
* SUPRA V2N10

The Android.Sprovider.7 trojan was discovered in Lenovo A6000 and Lenovo A319 smartphones. Bypassing android app security, the Trojan is able to download, install and run APK files, make phone calls, run a specific system mobile app when a particular number is dialed, show ads on top of apps and status bar, upgrade a malicious leading module, etc.

A picture of a little carton is shown alongside all the running programs by the H5GameCenter program, and it cannot be disabled. Even if the program is deleted by any chance, the Trojan reinstalls it. In November 2016, security researchers had at Kryptowire had discovered hidden backdoor in various low-cost Android smartphones marketed in America. The backdoor secretly sends information to a Chinese server. This calls for strong android app security of all mobile apps and a comprehensive testing of low-cost devices before they and ready to be sold into the mobile markets.