Doctor Web: A dangerous Android backdoor distributed via Google Play

Published: 2019-07-12 · Archived: 2026-04-05 22:41:04 UTC

12.07.2019

Real-time threat news | Hot news | Threats to mobile devices | All the news | Virus alerts

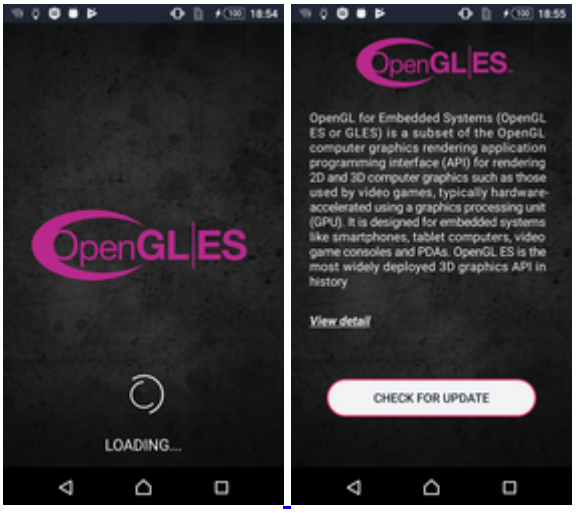
July 12, 2019

Doctor Web has identified a new backdoor trojan on Google Play that executes cybercriminal commands, allowing the criminals to remotely control the infected Android devices and spy on users.

The malware was dubbed **Android.Backdoor.736.origin**. It is distributed under the guise of the OpenGL Plugin application that is supposed to check the existing version of the OpenGL ES interface and download its updates.

When launched, **Android.Backdoor.736.origin** requests several important system permissions that allow it to collect confidential information and work with the file system. It also tries to get permission to overlay its windows over the interfaces of other programs.

Its window contains a button to “check” for updates to the OpenGL ES interface. When a user taps the window, the trojan simulates a search for new versions of OpenGL ES, but does not actually perform any checks.



When the victim closes the application window, **Android.Backdoor.736.origin** removes its icon from the list on the main screen and creates a shortcut instead. This makes it harder for the user to remove the trojan, since deleting the shortcut will not effect the malware itself.

Android.Backdoor.736.origin is continuously active in the background and can be launched not only via its icon or a shortcut, but also automatically at startup and at the cybercriminals' command via Firebase Cloud Messaging. The trojan's basic malicious functionality is contained in an encrypted auxiliary file, stored in the directory containing the program resources. It is decrypted and loaded into memory upon each launch of **Android.Backdoor.736.origin**.

The backdoor communicates with several command and control servers to receive commands from the attackers and send the collected data. The cybercriminals can also control the trojan via the Firebase Cloud Messaging service. **Android.Backdoor.736.origin** is capable of:

- sending information on contacts from the contact list to the server;
- sending information on text messages to the server (the investigated version of the trojan did not have the permissions for this);
- sending the phone call history to the server;
- sending the device location to the server;
- downloading and launching an APK or a DEX file using the DexClassLoader class;
- sending the information on the installed software to the server;
- downloading and launching a specified executable file;
- downloading a file from the server;
- uploading a specified file to the server;
- transmitting information on files in the specified directory or a memory card to the server;
- executing a shell command;
- launching the activity specified in a command;
- downloading and installing an Android application;
- displaying a notification specified in a command;
- requesting permission specified in a command;
- sending the list of permissions granted to the trojan to the server;

- not letting the device go into sleep mode for a specified time period.

The trojan AES encrypts all data transmitted to the server. Each request is protected with a unique generated key based on the current time. The same key encrypts the server response.

Android.Backdoor.736.origin can install applications using several methods:

- automatically, if the system has root access (using a shell command);
- using a system package manager (system software only);
- displaying a standard system installation dialog where the user needs to confirm the installation.

As you can see, this backdoor is a serious threat. Not only does it act as spyware, but it can also be used for phishing because it can display windows and notifications with any content. It can also download and install any other malicious application, as well as execute arbitrary code. For example, at the command of attackers, **Android.Backdoor.736.origin** can download and launch an exploit to obtain root privileges. It will then no longer need the user's permission to install other programs.

Doctor Web has notified Google about the trojan; it was already removed from Google Play at the time of publication.

Android.Backdoor.736.origin and its components are successfully detected and removed by Dr.Web for Android, so they do not pose any threat to our users.

Read more about **Android.Backdoor.736.origin**

#Android, #backdoor, #Google_Play, #spyware

13349 en 5

0

Doctor Web’s Q1 2026 review of virus activity on mobile devices

01.04.2026

Virus reviews

Read

Doctor Web’s Q1 2026 virus activity review

01.04.2026

Virus reviews

Read

Dr.Web for personal computers receives SKD AWARDS product excellence distinction

24.03.2026

Corporate news | Dr.Web products

Read
