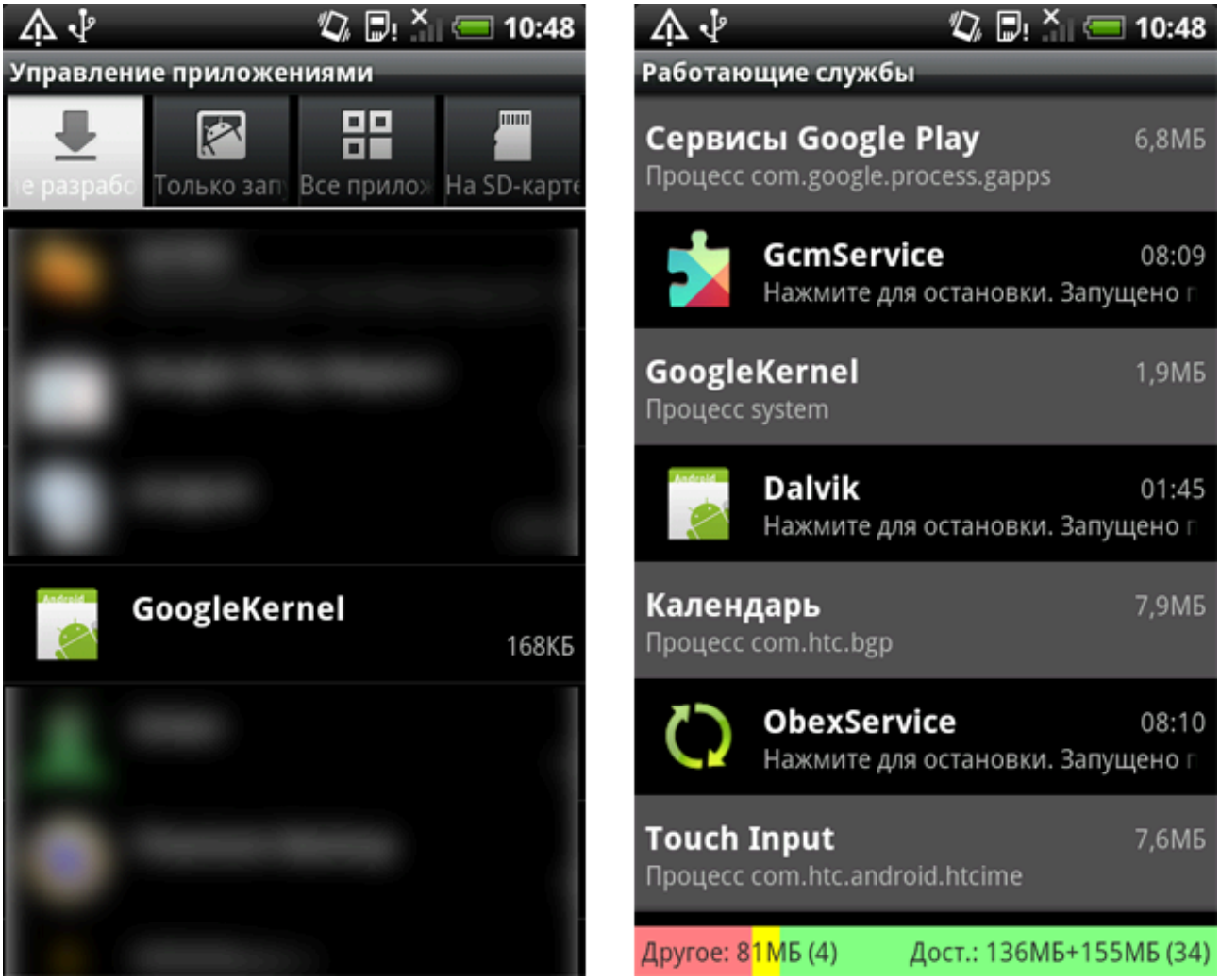
First widely distributed Android bootkit Malware infects more than 350,000 Devices

By The Hacker News

Published: 2014-01-29 · Archived: 2026-04-05 22:31:39 UTC



In the last quarter of 2013, sale of a Smartphone with ANDROID operating system has increased and every second person you see is a DROID user.

A Russian security firm '*Doctor Web*' identified the first mass distributed Android bootkit malware called '*Android.Oldboot*', a piece of malware that's designed to re-infect devices after reboot, even if you delete all working components of it.

The bootkit *Android.Oldboot* has infected more than 350,000 android users in China, Spain, Italy, Germany, Russia, Brazil, the USA and some Southeast Asian countries. China seems to a mass victim of this kind of malware having a 92 % share.

A Bootkit is a rootkit malware variant which infects the device at start-up and may encrypt disk or steal data, remove the application, open connection for Command and controller.

A very unique technique is being used to inject this Trojan into an Android system where an attacker places a component of it into the boot partition of the file system and modify the 'init' script (*initialize the operating system*) to re-load the malware as you switch on your android.

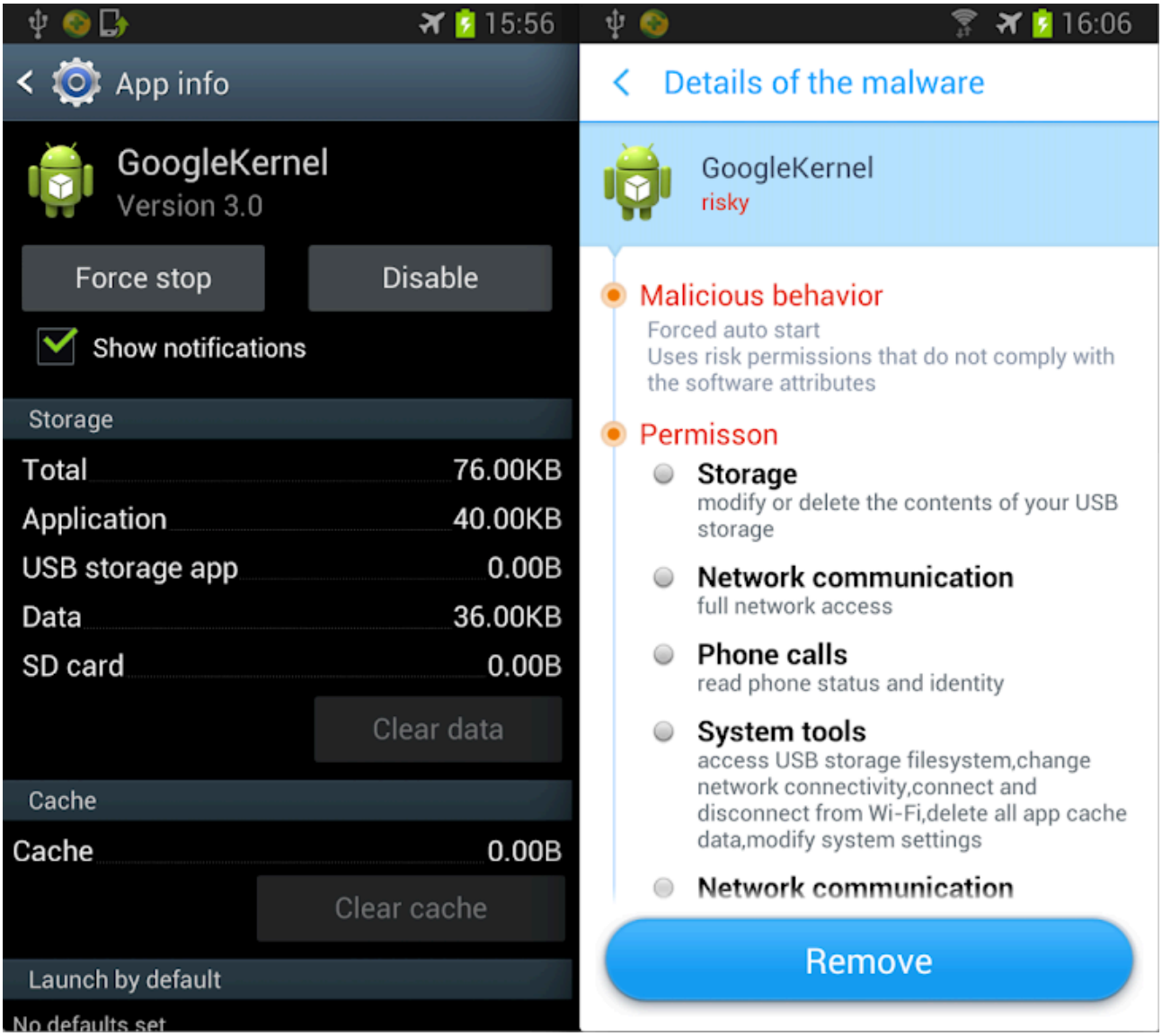
When you start your device, this script loads the Trojan '*imei_chk*' (detects it as Android.Oldboot.1) which extract two files *libgooglekernel.so (Android.Oldboot.2)* and *GoogleKernel.apk* (Android.Oldboot.1.origin), copy them respectively in */system/lib* and */system/app*.

Android.Oldboot acts as a system service and connects to the command-and-controller server using *libgooglekernel.so* library and receives commands to download, remove installed apps, and install malicious apps.

Since it becomes a part of the boot partition, formatting the device will not solve the problem. The researchers believe that the devices somehow had the malware pre-loaded at the time of shipping from the manufacturer, or was likely distributed inside modified Android firmware. So, users should beware of certain modified Android firmware.

Two weeks ago, Some Chinese Security Researchers have also detected a bootkit called '**Oldboot**', possibly the same malware or another variant of it.

> "*Due to the special RAM disk feature of Android devices' boot partition, all current mobile antivirus products in the world can't completely remove this Trojan or effectively repair the system.*"
>
> "*According to our statistics, as of today, there're more than 500, 000 Android devices infected by this bootkit in China in last six months.*



The Android malware Android.Oldboot is almost impossible to remove, not even with formatting your device. But if your device is not from a Chinese manufacturer, then chances that you are a victim of it, are very less.

This bootkit is not the first of this kind. Two years back, in the month of March we reported, NQ Mobile Security Research Center uncovered the world's first Android bootkit malware called '**DKFBootKit**', that replaces certain boot processes and can begin running even before the system is completely booted up.

But *Android.Oldboot* malware is a bit more dangerous because even if you remove all working components of it from your android successfully, the component imei_chk will persist in a protected boot memory area and hence will reinstall itself on next boot and continuously infect the Smartphone.

Users are recommended to install apps from authorized stores such as *Google Play*, disable installation of apps from '*Unknown Sources*' and for a better security install a reputed security application.

You can also try to re-flash your device with its original ROM. After flashing, the bootkit will be removed.

Found this article interesting? Follow us on Google News, Twitter and LinkedIn to read more exclusive content we post.

Source: http://thehackernews.com/2014/01/first-widely-distributed-android.html