Are free Android virus scanners any good?

Authors: Hendrik Pilz, Steffen Schindler

Published: 10. November 2011

Version: 1.1

Postal address: Klewitzstr. 7, 39112 Magdeburg, Germany

Phone +49 (0) 391 60754-60, Fax +49 (0) 391 60754-69

For further details, please visit: http://www.av-test.org

Content

1. Test report

The search query "Antivirus" in the Android market lists many programs, which pretend to protect a mobile device against threats in the Android world. AV-TEST wanted to know whether the apps are really protecting the user. The world wide acknowledged security institute had a deeper look on some of them and tested, whether their installation is worth the effort.

The test field consisted of free apps, which were compatible with the test device Samsung GalaxyTab (GT-P1010). The products of the well known security vendors Kaspersky and F-Secure were tested as well for comparison. The Android version was 2.2.1 (45.3% of all Android devices use version 2.2, as of 2011-10-03[1]). The products were installed through the official Android market. They had to prove their functionality in on-demand-scanning and the detection of 10 widely spread malicious apps which were to be installed on the test device.

During the scan of the test device the different implementations of the tools were noticeable. Some of them scanned installed apps only and consequently did not find the Android malware located on the SD memory card. This is not necessarily a problem: As long as the malware resides only on the removable media and is not installed on the system, it cannot do much harm. The scanned test set contained 83 Android installation packages (APK) and 89 Dalvik binaries (DEX). No files were older than 5 months. The best results claimed the products of Kaspersky and F-Secure, which detected at least 50% of all malware samples already in inactive state. The best free app was Zoner AntiVirus Free with 32% detected malicious apps. All other scanners detected at best 10% of the apps, some didn’t detect anything at all.

The results of the real-time guard functionality were quite shocking. The guard should warn the user upon installation of malicious apps. The 10 malware samples were chosen with the help of AV-TEST's own analysis system, which uses more than 30 virus scanners to analyze the APK files. The test set contains the 10 files, which were most often classified as malware by the virus scanners. Because of the high detection rates these files can be considered as well known and should therefore be detected by a reliable virus-scanner. Did the vendors of mobile security apps know them, too? The test results will show: Zoner AntiVirus Free was the only app with a respectable result. It detected 8 out of 10 samples during the installation attempts. BluePoint AntiVirus Free, Kinetoo Malware Scan and Privateer Lite still warned against one malicious app. Antivirus Free by Creative Apps, GuardX Antivirus and LabMSF Antivirus beta failed completely. In comparison to the free apps the commercial products of F-Secure and Kaspersky detected all threats without a problem.

The number of installations, which is given on the market website, shows that many users trust these free apps, although they do not offer a reliable protection. The by far most popular program is Antivirus Free by Creative Apps with 1,000,000 to 5,000,000 installations. The only useful free product Zoner AntiVirus Free has just 50,000 - 100,000 users. The best protection was achieved by the commercial tools of the well known security software vendors Kaspersky and F-Secure. The circulation of obviously near to useless security apps endangers those, who trust them and install apps from 3rd party app markets without further suspiciousness.

[1] http://developer.android.com/resources/dashboard/platform-versions.html

2. Test results

Name	Vendor	Version	Installation	Rating[2]	Size	Detection	
						Manual Scan	On installation
Antivirus Free	Creative Apps	1.3.1	1.000.000 - 5.000.000	4,5 / 41375	0,4 MB	0 / 172 (0%)	0 / 10 (0%)
http://zrgiu.com/							
BluePoint Antivirus Free	BluePoint Security	4.0.14	10.000 - 50.000	4,2 / 549	3,4 MB	2 / 172 (1%)	1 / 10 (10%)
http://www.bluepointsecurity.com/							
GuardX Antivirus	Qstar	2.3	100.000 - 500.000	4,6 / 2824	1,2 MB	0 / 172 (0%)	0 / 10 (0%)
http://guardx.qstar.org/							
Kinetoo Malware Scan	CPU Media SARL	1.6.9	10.000 - 50.000	4,2 / 184	0,2 MB	11 / 172 (6%)	1 / 10 (10%)
http://kinetoo.com/							
LabMSF Antivirus beta	LabMSF	1.0	1.000 - 5.000	4,3 / 16	1,0 MB	0 / 172 (0%)	0 / 10 (0%)
http://labmsf.com/							
Privateer Lite	Online Vault	2.1.4	1.000 - 5.000	4,5 / 28	1,1 MB	0 / 172 (0%)	1 / 10 (10%)
http://www.privateerlabs.net/privateer-mobile-released							
Zoner AntiVirus Free	ZONER	1.2.4	50.000 - 100.000	4,6 / 1614	0,9 MB	55 / 172 (32%)	8 / 10 (80%)
http://www.zonerantivirus.com							

Commercial products for comparison

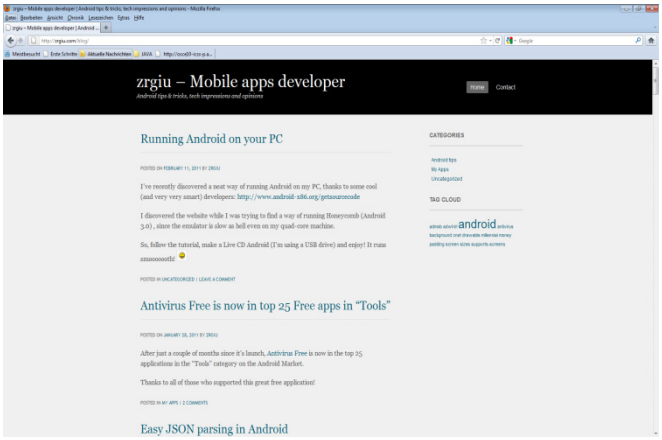
Name	Vendor	Version	Installation	Rating	Size
F-Secure Mobile Security[3]	F-Secure	7.1	-	-	4,5 MB
http://www.f-secure.com/de/web/home_de/protection/mobile-security/overview					
Kaspersky Mobile Security	Kaspersky Lab	9.10.77	10.000 - 50.000	4,2 / 992	3,8 MB
http://www.kaspersky.com/kaspersky_mobile_security					

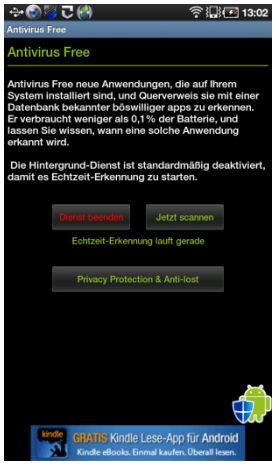
[2] Android Market Rating / Number of ratings
[3] F-Secure Mobile Security is not (yet) available via the Android Market

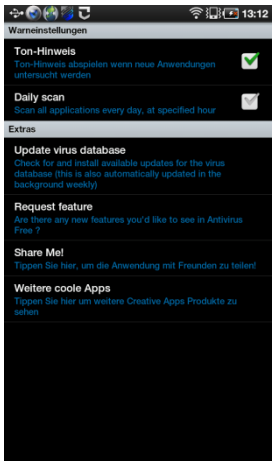
3. Product details

Antivirus Free

(Creative Apps) -- http://zrgiu.com/







Functions

- real-time scan
- manual scan
- automatic updates

Overview

Installations	1.000.000 – 5.000.000
Manual scan	0 / 0%
Real-time scan	0 / 0%

Permissions

Your location

coarse (network-based) location

Network communication

(full Internet access)

(view network state)

Phone calls

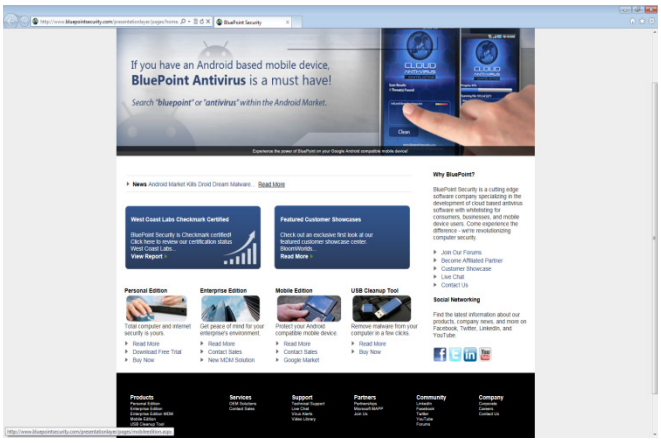
(Read phone state and identity)

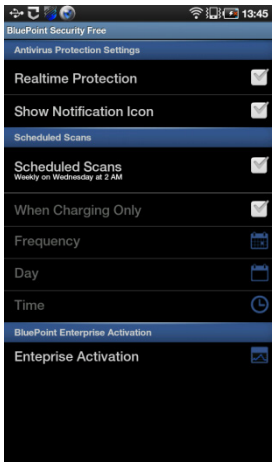
Storage

(Modify/delete USB storage contents modify/delete SD card contents)

BluePoint Antivirus Free

(BluePoint Security, Inc.) -- http://www.bluepointsecurity.com/





Functions

- real-time scan
- scans mail, sms and downloads
- manual scan (apps, user data, removable media)

Overview

Installations	10.000 - 50.000
Manual scan	2 / 1%
Real-time scan	1 / 10%

Permissions

Hardware controls
(Take pictures and videos)

(Control vibrator)

Your location
(Fine (GPS) location)

(Coarse (network-based) location)

Your personal information
(Read sensitive log data)

Network communication
(Full Internet access)

(Create Bluetooth connections)

(View network state)

(View Wi-Fi state)

(Receive data from Internet)

Storage
(Modify/delete USB storage contents modify/delete SD card contents)

System-tools
(Format external storage)

(Mount and unmount filesystems)

(Modify global system settings)

(Display system-level alerts)

(Retrieve running applications)

(Measure application storage space)

(Kill background processes)

(Write Access Point Name settings)

(Change Wi-Fi state)

(Prevent device from sleeping)

(Bluetooth administration)

Default
(Delete applications)

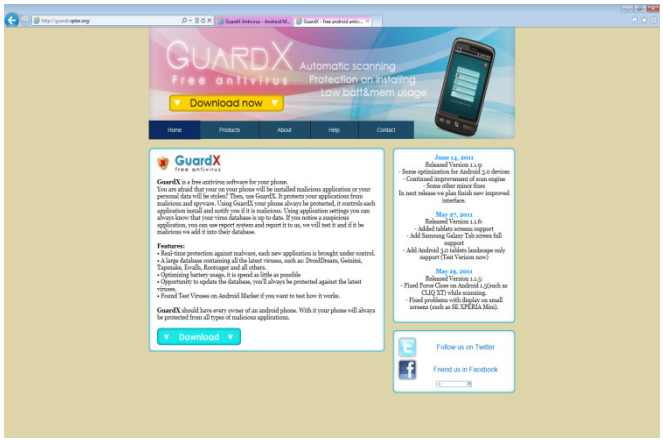
(Directly install applications)

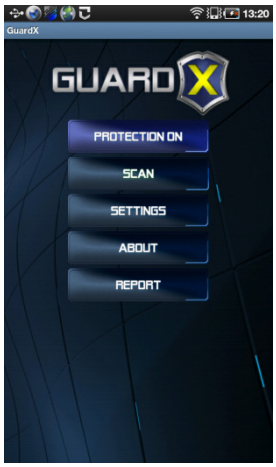
(Modify secure system settings)

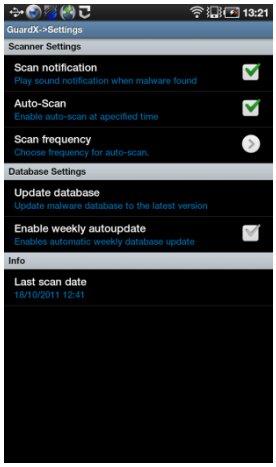
(Modify battery statistics)

GuardX Antivirus

(Qstar) -- http://guardx.qstar.org/







Functions

- Real-time scan
- manual scan
- manual and automatic updates

Overview

Installations	100.000 - 500.000
Manual scan	0 / 0%
Real-time scan	0 / 0%

Permissions

Network communication

(Full Internet access)

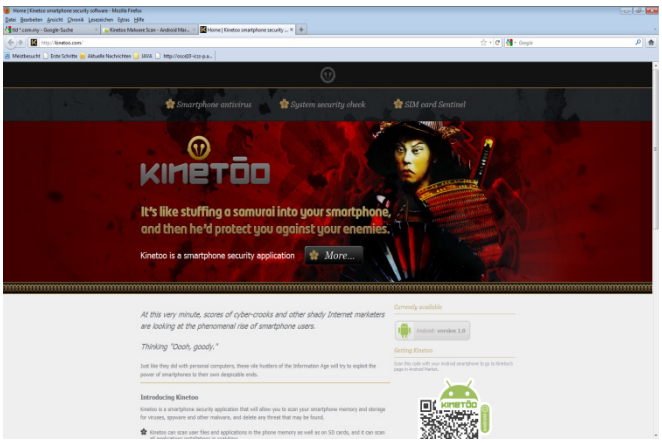
(View network state)

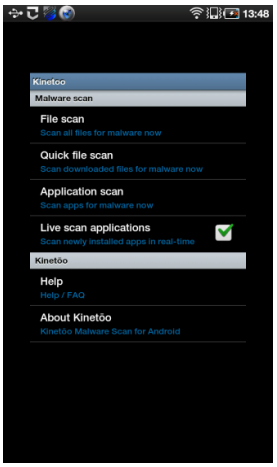
Phone calls

(Read phone state and identity)

Kinetoo Malware Scan

(CPU Media SARL) -- http://kinetoo.com/





Functions

- scan system and apps
- Real-time scan

Overview

Installations	10.000 - 50.000
Manual scan	11 / 6%
Real-time scan	1 / 10%

Permissions

Network communication

(Full Internet access)

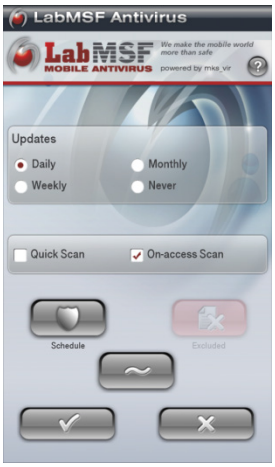
(View network state)

System-tools

(Automatically start at boot)

LabMSF Antivirus beta

(LabMSF) -- http://labmsf.com/



Functions

- Real-time scan
- manual scan
- manual and automatic updates

Overview

Installations	1.000 - 5.000
Manual scan	0 / 0%
Real-time scan	0 / 0%

Permissions

Network communication

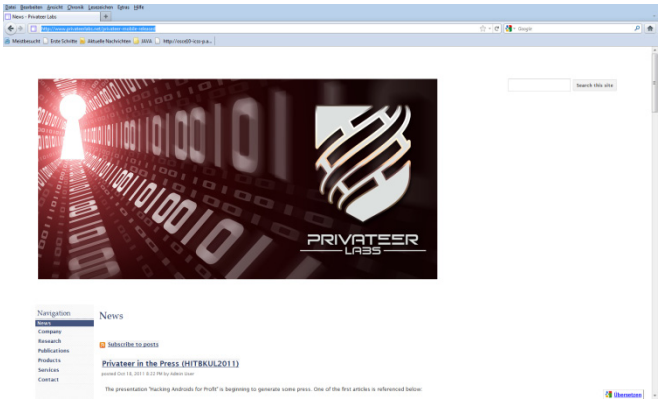
(Full Internet access)

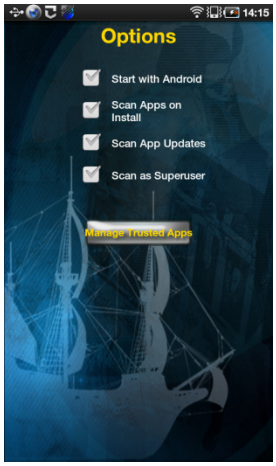
Storage

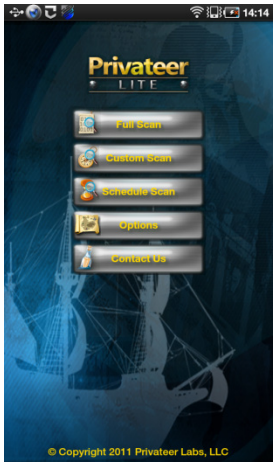
(Modify/delete USB storage contents modify/delete SD card contents)

Privateer Lite

(Online Vault) -- http://www.privateerlabs.net/privateer-mobile-released







Functions

- Real-time scan
- manual scan

Overview

Installations	1.000 - 5.000
Manual scan	0 / 0%
Real-time scan	1 / 10%

Permissions

Network communication

(Full Internet access)

(View network state)

System-tools

(Automatically start at boot)

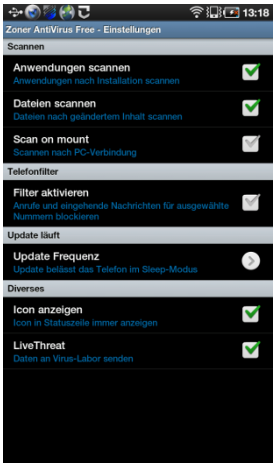
(Retrieve running applications)

Storage

(Modify/delete USB storage contents modify/delete SD card contents)

Zoner AntiVirus Free

(ZONER, Inc.) -- http://www.zonerantivirus.com



Functions

- Theft Protection (find and control your missing device)
- Installed app protection
- On-access and on-demand scan
- Phone filtering (block calls and messages)
- Parental lock for calls
- Kontroll Functions
- Task Manager
- Automatic and manual database updates
- Home screen widget

Overview

Installations	50.000 - 100.000
Manual scan	55 / 32%
Real-time scan	8 / 80%

Permissions

Services that cost you money
(Directly call phone numbers)

(Send SMS messages)

Your location
(Fine (GPS) location)

Your messages
(Receive SMS)

(Receive MMS)

Network communication
(Full Internet access)

(View network state)

Your personal information
(Read contact data)

Phone calls
(Intercept outgoing calls)

(Read phone state and identity)

Storage
(Modify/delete USB storage contents modify/delete SD card contents)

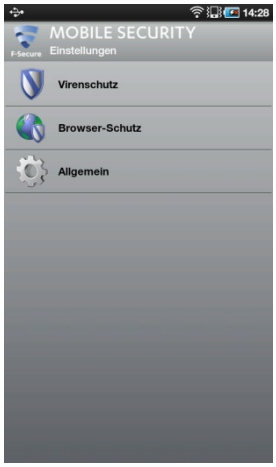
Hardware controls
(Control vibrator)

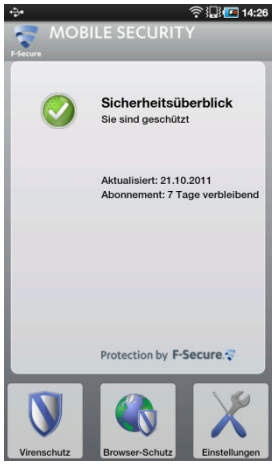
System-tools
(Automatically start at boot)

(Kill background processes)

F-Secure Mobile Security

(F-Secure) -- http://www.f-secure.com/en/web/home_global/protection/mobile-security/overview





Functions

- malware protection
- safe browsing
- Locate a lost or stolen smartphone
- Parental control
- your children can be located via their mobile phone

Permissions

Your personal information
(Add or modify calendar events and send email to guests)

(Read calendar events)

(Write contact data)

(Read Browser's history and bookmarks)

(Write Browser's history and bookmarks)

Services that cost you money
(Send SMS messages)

Your location
(Fine (GPS) location)

(Coarse (network-based) location)

Your messages
(Receive SMS)

(Read SMS or MMS)

(Edit SMS or MMS)

Network communication
(Full Internet access)

Storage
(Modify/delete USB storage contents modify/delete SD card contents)

Phone calls
(Read phone state and identity)

System-tools
(Format external storage)

(Mount and unmount filesystems)

(Write Access Point Name settings)

(Change Wi-Fi state)

(Prevent device from sleeping)

(Retrieve running applications)

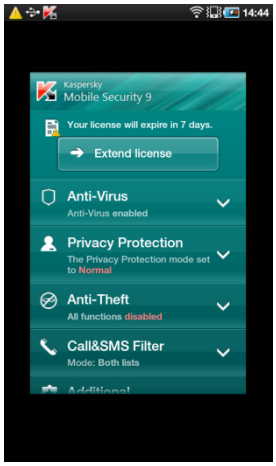
(Modify global system settings)

(Write sync settings)

(Read sensitive log data)

Kaspersky Mobile Security

(Kaspersky Lab) -- http://www.kaspersky.com/kaspersky_mobile_security



Functions

- Privacy Protection - for your eyes only
- Locate a lost or stolen smartphone
- Secure contacts, photos and files from unauthorized access
- Block unwanted calls or SMSs
- Parental control
- Protect your smartphone from malware and network attacks

Permissions

Your accounts
(Manage the accounts list)

(Discover known accounts)

Services that cost you money
(Directly call phone numbers)

(Send SMS messages)

Your location
(Coarse (network-based) location)

(Fine (GPS) location)

(Mock location sources for testing)

(Access extra location provider commands)

Your messages
(Read SMS or MMS)

(Edit SMS or MMS)

(Receive SMS)

Network communication
(Full Internet access)

(View network state)

Your personal information
(Read contact data)

(Write contact data)

(Read calendar events)

(Add or modify calendar events and send email to guests)

Phone calls
(Read phone state and identity)

(Modify phone state)

Storage
(Modify/delete USB storage contents modify/delete SD card contents)

System-tools
(Prevent device from sleeping)

(Write sync settings)

(Modify global system settings)

(Write Access Point Name settings)

(Change network connectivity)

(Automatically start at boot)

(Read subscribed feeds)

(Read sync settings)

(Set preferred applications)

(Kill background processe

4. Appendix

	Permission	Description
Your location	*coarse (network-based) location*	Access coarse location sources such as the cellular network database to determine an approximate device location, where available. Malicious applications can use this to determine approximately where you are.
	fine (GPS) location	Access fine location sources such as the Global Positioning System on the device, where available. Malicious applications can use this to determine where you are, and may consume additional battery power.
Network communication	*full Internet access*	Allows an application to create network sockets.
	View network state	Allows an application to view the state of all networks.
	Create Bluetooth connections	Allows an application to view configuration of the local Bluetooth device, and to make and accept connections with paired devices.
	View Wi-Fi state	Allows an application to view the state of all networks.
	Receive data from Internet	Allows the applications to accept cloud to device messages sent by the application's service. Using this service will incur data usage. Malicious applications may cause excess data usage.
Phone calls	*Read phone state and identity*	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and the like.
Storage	*Modify/delete USB storage contents modify/delete SD card contents*	Allows an application to write to the USB storage. Allows an application to write to the SD card.
Hardware controls	*Take pictures and videos*	Allows application to take pictures and videos with the camera. This allows the application at any time to collect images the camera is seeing.
	Control vibrator	Allows the application to control the vibrator.
System-tools	*Format external storage*	Allows the application to format removable storage.
	Mount and unmount filesystems	Allows the application to mount and unmount filesystems for removable storage.
	Modify global system settings	Allows an application to modify the system's settings data. Malicious applications can corrupt your system's configuration.
	Display system-level alerts	Allows an application to show system alert windows. Malicious applications can take over the entire screen.
	Retrieve running applications	lows application to retrieve information about currently and recently running tasks. May allow malicious applications to discover private information about other applications.
	Measure application storage space	Allows an application to retrieve its code, data, and cache sizes
	Kill background processes	Allows an application to kill background processes of other applications, even if memory isn't low.
	Write Access Point Name settings	Allows an application to modify the APN settings, such as Proxy and Port of any APN.
	Change Wi-Fi state	Allows an application to connect to and disconnect from Wi-Fi access points, and to make changes to configured Wi-Fi networks.
	Prevent device from sleeping	Allows an application to prevent the device from going to sleep.
	Bluetooth administration	Allows an application to have itself started as soon as the system has finished booting. This can make it take longer to start the device and allow the application to slow down the overall device by always running.
	Automatically start at boot	Allows an application to have itself started as soon as the system has finished booting. This can make it take longer to start the device and allow the application to slow down the overall device by always running.
	Change network connectivity	Allows an application to change the state of network connectivity.

	Permission	Description
System-tools	*Retrieve running applications*	Allows application to retrieve information about currently and recently running tasks. May allow malicious applications to discover private information about other applications.
	Write sync settings	Allows an application to modify the sync settings, such as whether sync is enabled for Contacts.
Default	*Delete applications*	Allows an application to delete Android packages. Malicious applications can use this to delete important applications.
	Directly install applications	Allows an application to install new or updated Android packages. Malicious applications can use this to add new applications with arbitrarily powerful permissions.
	Modify secure system settings	Allows an application to modify the system's secure settings data. Not for use by normal applications.
	Modify battery statistics	Allows the modification of collected battery statistics. Not for use by normal applications.
Phone calls	*Read phone state and identity*	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and the like.
	Intercept outgoing calls	Allows application to process outgoing calls and change the number to be dialed. Malicious applications may monitor, redirect, or prevent outgoing calls.
	Modify phone state	Allows the application to control the phone features of the device. An application with this permission can switch networks, turn the phone radio on and off and the like without ever notifying you.
Your personal information	*read sensitive log data*	Allows an application to read from the system's various log files. This allows it to discover general information about what you are doing with the device, potentially including personal or private information.
	Read contact data	Allows an application to read all of the contact (address) data stored on your device. Malicious applications can use this to send your data to other people.
	add or modify calendar events and send email to guests	Allows an application to add or change the events on your calendar, which may send email to guests. Malicious applications can use this to erase or modify your calendar events or to send email to guests.
	Read calendar events	Allows an application to read all of the calendar events stored on your device. Malicious applications can use this to send your calendar events to other people.
	Write contact data	Allows an application to modify the contact (address) data stored on your device. Malicious applications can use this to erase or modify your contact data.
	Read Browser's history and bookmarks	Allows the application to read all the URLs that the Browser has visited, and all of the Browser's bookmarks.
	Write Browser's history and bookmarks	Allows an application to modify the Browser's history or bookmarks stored on your device. Malicious applications can use this to erase or modify your Browser's data.

	Permission	Description
Services that cost you money	*Directly call phone numbers*	Allows the application to call phone numbers without your intervention. Malicious applications may cause unexpected calls on your phone bill. Note that this does not allow the application to call emergency numbers.
	Send SMS messages	Allows application to send SMS messages. Malicious applications may cost you money by sending messages without your confirmation.
Your messages	*Receive SMS*	Allows application to receive and process SMS messages. Malicious applications may monitor your messages or delete them without showing them to you.
	Receive MMS	Allows application to receive and process MMS messages. Malicious applications may monitor your messages or delete them without showing them to you.
	Read SMS or MMS	Allows application to read SMS messages stored on your device or SIM card. Malicious applications may read your confidential messages.
	Edit SMS or MMS	Allows application to write to SMS messages stored on your device or SIM card. Malicious applications may delete your messages.