AV TEST

The Independent IT-Security Institute

Magdeburg Germany

Test Report: Anti-Malware solutions for Android

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

Update March, 15th 2012 (Version 1.1a)

Added a remark regarding the detection rate of Bitdefender, ESET, Trend Micro and Vipre on page 8.

Update March, 13th 2012 (Version 1.1)

It has been brought to our attention that certain parts in our initial report and the testing methodology are considered imprecise and/or flawed by third parties. Therefore AV-TEST performed additional tests to sort out any of those issues and provides the updated results in this report.

The retest was performed between March 9th to 13th, with the most current program versions and signature updates (including full Internet access to enable in-the-cloud queries) of all products that were not in the light green or dark green category.

We would especially like to thank MYMobileSecurity (MYAndroidProtection), NQmobile (Netqin) and Total Defense for their feedback on this topic.

Update March, 7th 2012 (Version 1.0a)

The product name of Avast has been corrected to "avast! Free Mobile Security" instead of "avast! Mobile Security".

Content

1. Introduction

The Smartphone market grew enormously over the last five years and the mobile malware evolved rapidly, too. Right now there are over 450.000 apps in the Android market, where as there were less than 100.000 in July 2010[1]. This makes it the fastest growing software market overall. With the rise of new apps, the number of malware increases as well. Figure 1 shows the growth of the AV-TEST Android malware collection. The increasing curve is similar to what we've seen for PC malware in the last years. The threats for Android include Phishing- and Banking-Trojans, Spyware, Bots, Root Exploits, SMS Fraud, Premium Dialers and Fake Installers. There have also been reports about Download-Trojans – apps that download their malicious code after installation – which means that these apps can't be easily detected by Google's Bouncer technology[2] during publication in the Google Android Market. Our collection used for this test contains more than 20 different Android malware families, which cover each of the previously named threats.
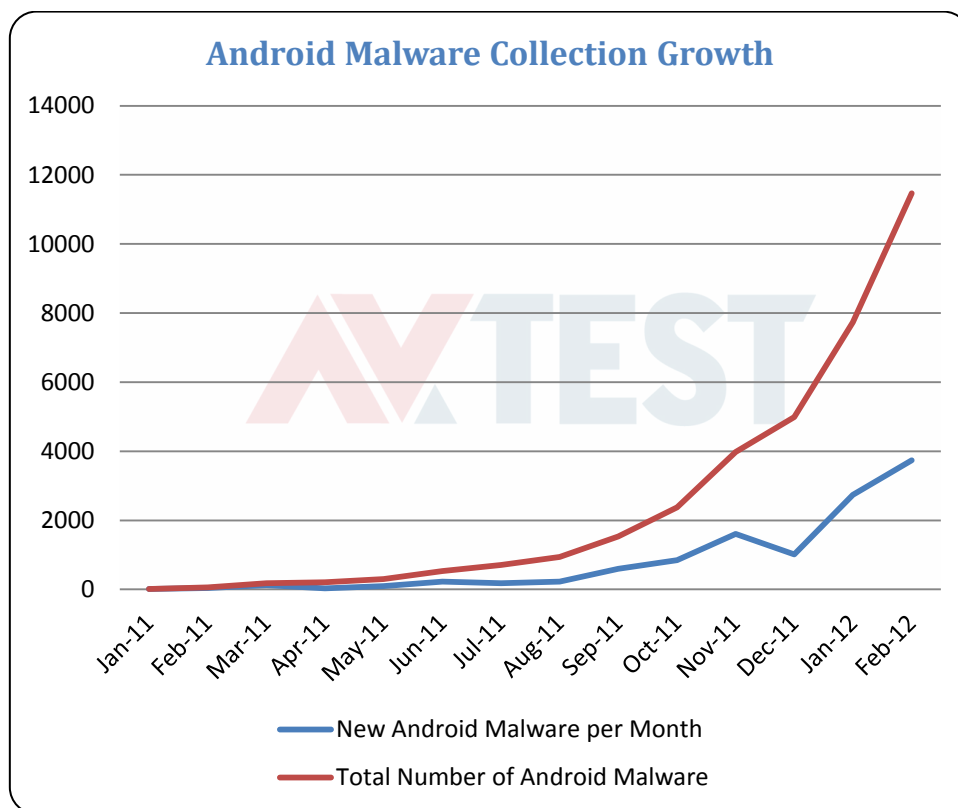

Figure 1: Android malware collection growth since January 2011

In November 2011 we've revealed that many Antivirus apps, which are available for free in Google's Android Market, don't provide a sufficient malware protection for your Android mobile. This time we are trying to cover the good and the bad and started reviewing as many Android Anti-Malware apps as we could find, regardless whether an app requires a specific Android version or device. These apps include free and non-free programs, intended for personal use. This report aims to give an impression of the malware detection rates. As an independent test institute, we aren't in the position to recommend a specific product, but you can certainly use our report to find your personal favorite. However please bear in mind, that malware may not the only or the most important threat to your

---

[1] <http://en.wikipedia.org/wiki/Android_operating_system>
[2] Google's Bouncer technology checks apps for malware during publication in Google's Android Market
<http://googlemobile.blogspot.com/2012/02/android-and-security.html>

device. Even if a product scores poorly in malware detection it may have other convenient features, such as remote lock and wipe, backup and phone locating, that make it useful for your purposes. It is also possible to run two or more security apps on your device at the same time, using only the best features of the single apps.

2. Test report

The large number of tested apps required a scalable test environment, so we decided to use the Android emulator supplied by the Android SDK as basis for the review. The emulator has some advantages in contrast to a real device. There is root-access without exploiting the device and you can easily switch between API versions and screen sizes. It has also some disadvantages. You don't have a real phone number, which might be required to activate an app through SMS, and the emulated 3G connection may have a too high latency for querying the cloud of some vendors. While the advantages of the emulator make testing more comfortable, the disadvantages limit the number of apps, which could be properly tested. To get around this limitation, the apps, which didn't work in the emulator, were tested on a real device and all emulator results were cross checked and verified on a real device. The emulator was set up with API level 10 (Gingerbread, Version 2.3) and for non-emulated testing we used a Samsung GalaxyTab (GT-P1010) with Froyo (Version 2.2) and a Samsung Galaxy Nexus (GT-I9250) with Ice Cream Sandwich (Version 4). The products were updated to their latest available versions/signature updates and were allowed to connect to their cloud during the test. The real devices were flashed to factory default settings after every test to provide each product the same clean environment.

Among the tested apps we saw two different approaches for the on-demand scan. While many apps simply scan the complete device storage, some other apps scan installed apps and important files only. The latter were not able to scan the malware set with 618 malicious APK-files as it was stored on the SD card. Therefore, we tested the real-time protection feature of those apps instead. That means that all malware apps in our sample set were installed on a device or emulator one by one. After an app has been installed, the tester waited for feedback of the real-time protection, which should pop up if it finds a malicious app. In case of an undetected sample, it was uninstalled manually. This is a time consuming approach and may not work in the future with larger sample sets (see Fig. 1).

Regarding the detection rates, it makes no difference whether a malicious app is detected by an on-demand scan or by the real-time scan, when the app is installed. From the testers' point of view, an on-demand scan with many samples is much easier to realize than an on-access scan. However from the user's point of view the only criterion is protection, no matter at which point and how this takes place.

After an on-demand scan has been completed and all detections were removed the testers saved the remaining files, because the reporting abilities weren't consistent among all apps. The files that were left over and have not been modified were flagged as "not detected". In case of the on-access testing, the testers wrote their own report since the samples were tested one by one. With the knowledge of which specific files have been detected by a scanner, we were able to analyze the scan results based on malware families. The family based analysis can help vendors to improve the protection for malware families with low detection rates. If the results would only provide a total, absolute detection rate, it would be impossible to notice if an app that scored well missed an entire malware family or not. So this way of displaying the results gives both the reader and the vendor much more insight. Furthermore this helps to decide whether a product that doesn't score 100% is still a good choice, e.g. because it misses on a malware family that is no threat to a specific user group or environment.

In this report no exact detection rates are given, instead the products are grouped into five different categories, referring to different ranges of detections (Fig. 2 and Fig. 3). The first category contains products that detected over 90%, the second category 90% to 65%, the third 65% to 40%, the fourth everything less than 40% but above 0% and finally the last group contains the products that didn't detect anything.

> 90%	> 65%	> 40%	> 0%	0%

Figure 2: Detection rate legend

There are several reasons for doing that:

1. The number of malware samples is still fairly small
2. Determining the prevalence of malware apps is difficult
3. Malware apps are quickly removed from the market (and even remotely from the device)

This all comes down to one issue: It can happen very easily that a sample set is distorted by samples that are not really relevant anymore or were never at all. It is impossible for us to measure the prevalence of malware apps. It is also not possible to determine when and how long they have been a threat to the user. Therefore we identified the most widely known malware families and primarily used those for the test. Only malicious apps that we have discovered between August and December 2011 have been included in the test set. A few further malicious apps which don't belong to the listed families have been put in a category called "Other" and represent other families. Even with those precautions it is possible that malware samples that are not suitable for this test are included. Already 30 wrongly chosen samples could change the result by 5%. In order to avoid too heavy effects from these issues, the results are categorized. However, by looking at the individual family detections it is still possible to get a fairly accurate picture of the absolute detection rate.

The products were distributed over all detection ranges as shown in Figure 3.
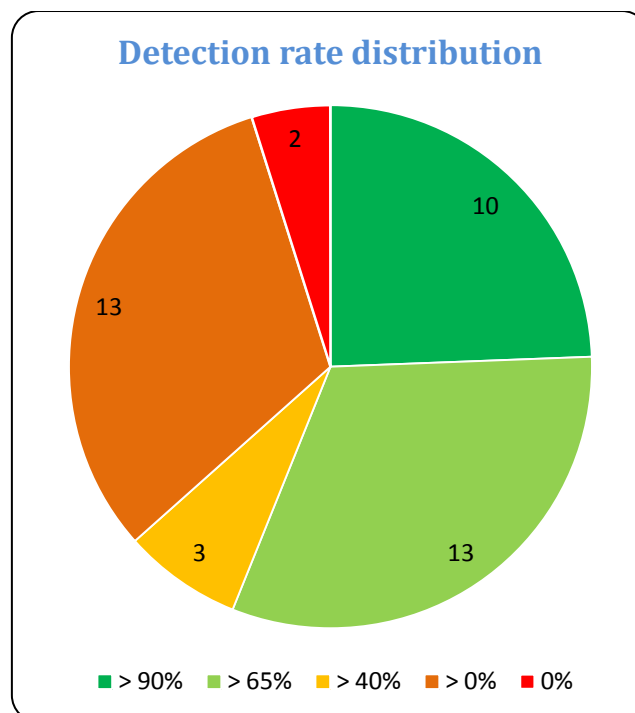

Figure 3: Detection rate distribution

3. Test results

During February and March 2012 we reviewed 41 different Android Anti-Malware solutions. The test results are shown in Figure 4[3].

The best products in our tests (with detection rates of 90% and above) come from the following top 10 companies, listed in alphabetic order: Avast, Dr. Web, F-Secure, Ikarus, Kaspersky, Lookout, McAfee, MYAndroid Protection, NQ Mobile and Zoner. Users of products made by these companies can be assured that they are protected against malware.

Products with a detection rate of between 65% and 90% can also be considered to be very good and have the potential to join the group of best products above if small changes are made to the set of malware tested. Some of these products only fail to detect just one or two malware families that may not even be prevalent in certain environments. The following 13 products, listed in alphabetic order, fall into this category: AegisLab, AVG Mobilation, Bitdefender, BullGuard, Comodo, ESET, Norton, QuickHeal, Super Security, Total Defense, Trend Micro, Vipre and Webroot.

It should be noted that Bitdefender, ESET, Trend Micro and Vipre missed the top category by just a few samples. The average family detection rate for these four products was in the area of 88.1% to 89.9%.

	Product	Average Family Detection	
A	avast! Free Mobile Security		>90%
A	Dr.Web anti-virus Light		
A	F-Secure Mobile Security		
A	IKARUS mobile.security LITE		
A	Kaspersky Mobile Security		
A	Lookout Security & Antivirus		
B	McAfee Mobile Security		
B	MYAndroid Protection		
B	NQ Mobile Security		
A	Zoner AntiVirus Free		
A	AegisLab Antivirus Free		>65%
A	AVG Mobilation Anti-Virus Free		
A	Bitdefender Mobile Security		
B	BullGuard Mobile Security		
B	Comodo Mobile Security		
A	ESET Mobile Security		
A	Norton Mobile Security Lite		
A	Quick Heal Mobile Security		
A	Super Security		
B	Total Defense Mobile Security		
A	Trend Micro Mobile Security		
A	Vipre Mobile Security (BETA)		
A	Webroot SecureAnywhere		
B	BluePoint Security Free		>40%
B	G Data Mobilesecurity		
B	Kinetoo Malware Scan		
B	ALYac Android		>0%
B	Android Antivirus		
B	Android Defender Virus Shield		
B	Antivirus Free		
B	BlackBelt AntiVirus		
B	CMC Mobile Security		
B	Fastscan Anti-Virus Free		
B	GuardX Antivirus		
B	MobiShield Mobile Security		
B	MT Antivirus		
B	Privateer LITE		
B	Snap Secure		
B	TrustGo Mobile Security		
B	LabMSF Antivirus beta		0
B	MobileBot Antivirus		

**Figure 4: Average detection rate per malware family[3]
(products in alphabetic order per category)**

BluePoint, G Data and Kinetoo fall into the third category, namely that of products with a detection rate of between 40% and 65%. It is possible that the manufacturers of these products do not yet have a sufficient infrastructure that enables them to collect a wide range of malware or that they focus on a local market. These products provide reliable malware protection against a few families,

---

[3] Products marked with "A" were tested during February 2012. Products marked with "B" were retested during March 2012. See the report update page at the beginning of the document.

but have trouble dealing with and detecting others. It can be expected that these products will improve when their manufacturers focus on a wider variety of malware samples.

The fourth category, which is used for products with a detection rate of less than 40%, does not contain any products from well-known anti-virus protection manufacturers. Some of the products in this category also performed below average in our last test. We have now reviewed two other products that are listed in this final category and we could not clearly determine whether or not they correctly scanned the set of malware test or whether they were actually able to detect anything at all. We were therefore unable to record a detection rate when using our set of well-known samples or the EICAR test file[4].

Even in the on-access tests these products had no detections. So it is safe to assume that these products really don't detect anything, but we still wanted to point out the possibility of a flaw in our testing methodology.

The malware family based analysis in Figure 5 shows that some products miss the top group only due to their low detection of one or two malware families. You can expect better signatures for these families to be added in the near future. The detection of specific families can also depend on each vendor's definition of malware. Some families might only be annoying advertisement apps, while others include real malicious code, which can lead to monetary damage or data loss. Therefore some vendors may decide to not detect certain potentially unwanted, but not clearly malicious, apps.

---

[4] The EICAR test file can be used to determine whether an anti-malware software is operational or not and can be obtained here <http://www.eicar.org/86-0-Intended-use.html>

	Average Family Detection	Adrd	BaseBrid	Boxer	DorDrae	Exploit.Lotoor	FakeInst	Geinimi	Glodream	Gonca	Jifake	Kmin	KungFu	Nickspy	Opfake	Rooter	SerBG	Xsider	Yzhc	Other
avast! Free Mobile Security																				
Dr.Web anti-virus Light																				
F-Secure Mobile Security																				
IKARUS mobile.security LITE																				
Kaspersky Mobile Security (Lite)																				
Lookout Security & Antivirus																				
McAfee Mobile Security																				
MYAndroid Protection Antivirus																				
NQ Mobile Security																				
Zoner AntiVirus Free																				
AegisLab Antivirus Free																				
AVG Mobilation Anti-Virus Free																				
Bitdefender Mobile Security																				
BullGuard Mobile Security																				
Comodo Mobile Security																				
ESET Mobile Security																				
Norton Mobile Security Lite																				
Quick Heal Mobile Security																				
Super Security																				
Total Defense Mobile Security																				
Trend Micro Mobile Security																				
Vipre Mobile Security (BETA)																				
Webroot SecureAnywhere Mobile																				
BluePoint Security Free																				
G Data Mobilesecurity																				
Kinetoo Malware Scan																				
ALYac Android																				
Android Antivirus																				
Android Defender Virus Shield																				
Antivirus Free																				
BlackBelt AntiVirus																				
CMC Mobile Security																				
Fastscan Anti-Virus Free																				
GuardX Antivirus																				
MobiShield Mobile Security																				
MT Antivirus																				
Privateer LITE																				
Snap Secure																				
TrustGo Mobile Security																				
LabMSF Antivirus beta																				
MobileBot Antivirus																				

Figure 5: Detection by malware family (products in alphabetic order per category)

AV TEST

4. Testing issues

Despite the fact that some apps weren't able to scan our sample set on the SD card and therefore have to be tested in a time consuming on-access test, we were also faced with apps which couldn't delete all detections automatically. They didn't even provide a "Do it! And never ask me again!" option in the case of more than one malware detection. This fact led to testers clicking a "remove"-button several hundred times. While such options are very common in desktop applications, they aren't in the Android world yet. Also scan reports couldn't be saved within most of the tested apps. Some apps use SQLite databases to save their scan results and we were able to collect the corresponding db-files from the emulators only. As accessing those files requires root privileges, they weren't collected from the real devices. The average user shouldn't miss such features, as its device should never be infected with hundreds of malicious apps, but those simple functions would make a testers life much easier.

As pointed out before, there are also apps which use their cloud to detect malware. While this worked flawlessly with most products, both in emulated environments as well as on a real device there were a few exceptions. We have seen products that were not able to query their cloud in the emulator at all, even if full internet access was provided. There were also products that did have some trouble on a real device. This might be due to latency issues and could only be resolved by repeated tests until no further problems occurred.

5. Conclusion

Even if Google now checks all apps on its Android Market, you should consider installing a security app, because nowadays the malware authors are able to load their malicious code after a seemingly clean app has been installed. Regarding the detection rates, you can trustfully choose from at least 17 products to protect your Android device. What you should also have in mind when choosing your mobile security app are additional functions such as backup and anti-theft protection (e.g. find your lost device or wipe all data remotely).

To keep your device free of malware even without a security app, you should install apps only from trusted sources, like the Google Android Market or the Amazon Appstore for Android. Read the comments carefully and check whether the required permissions are reasonable (e.g. a game usually shouldn't need the permission to read or write SMS unless its description lists the specific features using these permissions). As it may take between two to four weeks until Google removes malicious apps from its Android Market, you should also be careful with new apps on the market. Wait until apps are well-established, e.g. they were downloaded several thousand times and have many good ratings, or visit the developer's website, which should at least provide contact information.

In most cases when there is a free (often called Lite) and a paid version, the malware detection capabilities are the same. So if you are just looking at the detection rates, you can take the Lite result and apply this to the paid version and vice versa. Another finding of the test is, that the well known Desktop IT vendors perform above the average. Even the worst products from those vendors are still better than most of the specialized mobile security software vendors.

6. Product details

Product	Vendor	Android Package[5]	Version
AegisLab Antivirus Free	AegisLab	com.aegislab.sd3prj.antivirus.free	1.0.4
ALYac Android	ESTsoft	com.estsoft.alyac	1.2.5.0
Android Antivirus	Android Antivirus	and.anti	1.6
Android Defender	AndroidAppTools	com.virusshield.android	1.1
Antivirus Free	Creative Apps	com.zrgiu.antivirus	1.3.1
avast! Free Mobile Security	AVAST	com.avast.android.mobilesecurity	1.0.1282
AVG Mobilation Anti-Virus Free	AVG Mobilation	com.antivirus	2.10
Bitdefender Mobile Security	BitDefender	com.bitdefender.security	1.1.483
BlackBelt AntiVirus	BlackBelt SmartPhone Defence	com.blackbelt.antivirus	2.2.0002
BluePoint Security Free	BluePoint Security	bluepointfree.ad	4.0.17
BullGuard Mobile Security	BullGuard	com.smobile.securityshield.android.bullgard	10.0.22.14023
CMC Mobile Security	CMC InfoSec	com.cmcinfosec.mobilesec	2.1
Comodo Mobile Security	Comodo Security Solutions	com.comodo.pimsecure	1.1.16984.2
Dr.Web anti-virus Light	Doctor Web	com.drweb	6.01.5
ESET Mobile Security	ESET	com.eset.emsw	1.0.288.223
Fastscan Anti-Virus Free	K-TEC	jp.ktinc.fastscan	1.1.5
F-Secure Mobile Security	F-Secure	com.fsecure.browser	7.6.08787
G Data MobileSecurity	G Data	de.gdata.mobilesecurity	23.4.19038
GuardX Antivirus	QStar	org.qstar.guardx	2.3
IKARUS mobile.security LITE	IKARUS Security Software	com.ikarus.mobile.security	0.9.8.9008
Kaspersky Mobile Security (Lite)	Kaspersky Lab	com.kms	9.10.106
Kinetoo Malware Scan	CPU Media SARL	com.cpumedia.android.kinetoo	1.7.1
LabMSF Antivirus beta	LabMSF	com.ReSync.RNGN	1.0
Lookout Security & Antivirus	Lookout Mobile Security	com.lookout	7.1
McAfee Mobile Security	McAfee	com.wsandroid.suite	2.0.1.366
MobileBot Antivirus	Desktop Shark	avm.defender	1.05
MobiShield Mobile Security	trustmobi	com.trustmobi.MobiShield	3.1.5
MT Antivirus	KissDroid	com.hot.free.defence.main	1.0.8
MYAndroid Protection Antivirus	MYMobileSecurity	com.mymobileprotection20	4.6.12.68
Norton Mobile Security Lite	NortonMobile	com.symantec.mobilesecurity	2.5.0.392
NQ Mobile Security	NetQin Mobile	com.nqmobile.antivirus20	6.0.06.16
Privateer LITE	Privateer Labs	com.privateer.lite	2.1.4
Quick Heal Mobile Security	Quick Heal Technologies	com.quickheal.platform	1.01.017
Snap Secure	Exclaim Mobility	com.exclaim.snapsecure.app	7.18
Super Security	Superdroid.net	com.superdroid.security2	1.04
Total Defense Mobile Security	Total Defense	com.tdi.security	3.0.3.16256
Trend Micro Mobile Security	Trend Micro	com.trendmicro.tmmspersonal	2.1
TrustGo Mobile Security	TrustGo Mobile	com.trustgo.security	1.0.1
Vipre Mobile Security (BETA)	GFI Software	com.ssd.vipre	1.0.231
Webroot SecureAnywhere Mobile	Webroot	com.webroot.security	2.2.1.1046
Zoner AntiVirus Free	ZONER	com.zoner.android.antivirus	1.2.10

Figure 6: Product details of all products listed in the test results

---

[5] The Android package name is unique among all apps in the Google Android Market. You can use it as search term if you want to install a specific program from the Android Market.
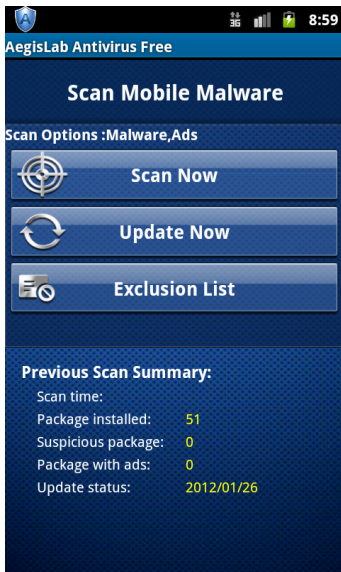
AegisLab Antivirus Free belongs to the second range with its detection rate between 65% and 90%. It has additional Anti-Theft functions in the Elite Version.
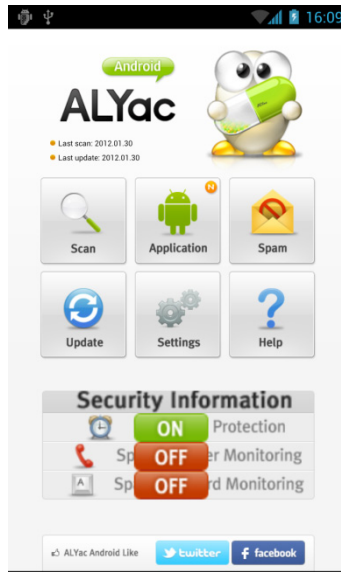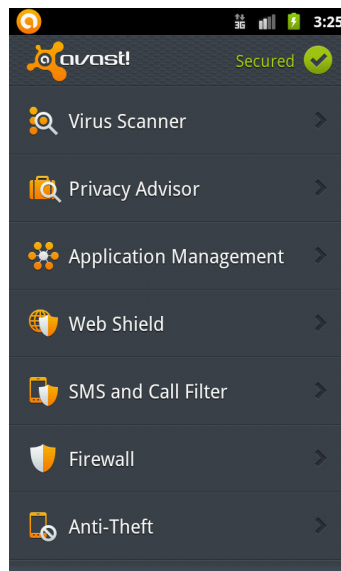

ALYac Android is a free Mobile Security. It has a clear user interface but the detection rates need to improve.
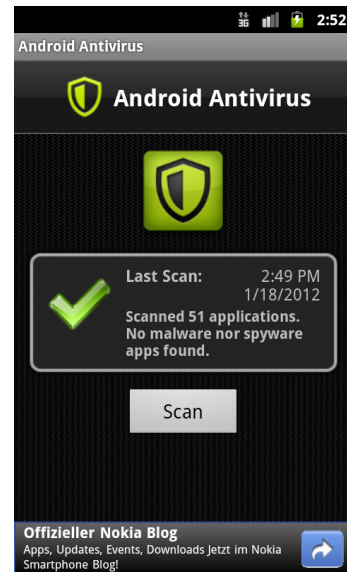

Android Antivirus showed only very few detections in our tests and crashed several times. The advertisements worked properly.
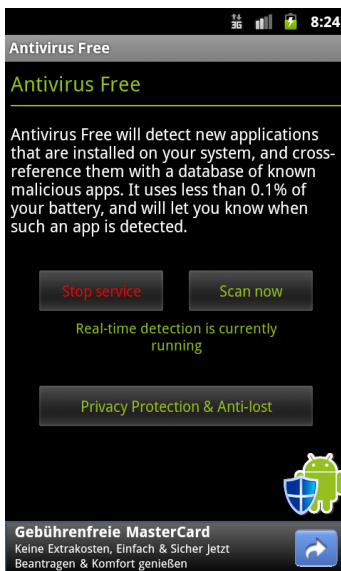

Antivirus Free just detects a handful of samples in the test set. It shows advertisements at the bottom of the screen.

avast! Free Mobile Security is available for free, easy to use and has many features to protect your device. With its very good detection rate it is one of the best security products for your Android device.
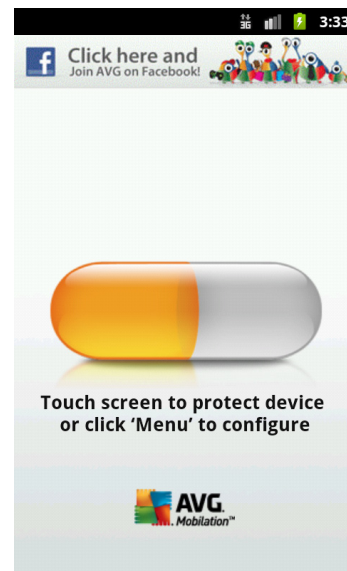
AVG Mobilation Anti-Virus Free is a good choice to secure your phone, being in the second group of detection rates. It also provides Anti-Theft functions.
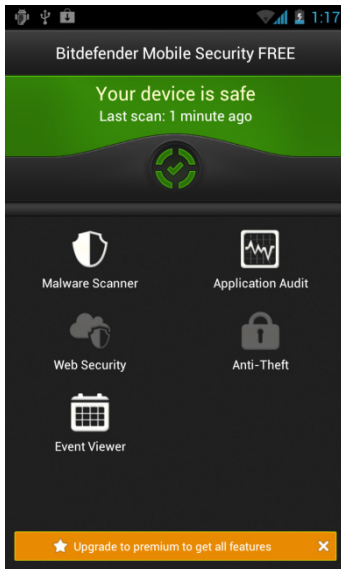
The premium version of **Bitdefender Mobile Security** includes a variety of other useful functions in addition to the good malware and privacy scanner.
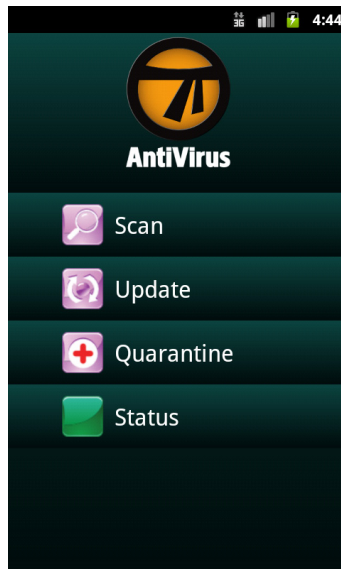
BlackBelt AntiVirus is simple to use. However the poor detection rate doesn't excuse to pay for the product after the trial period has expired.
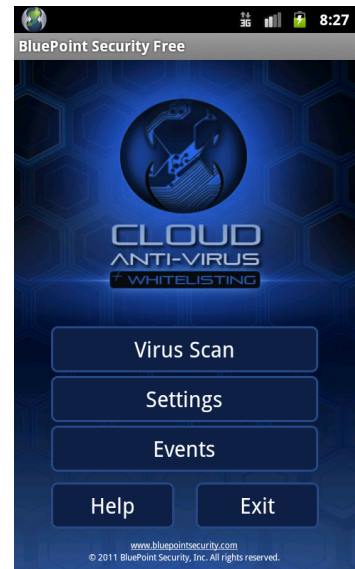
BluePoint Security Free uses a clear user interface and has an average detection rate with its cloud scan engine.
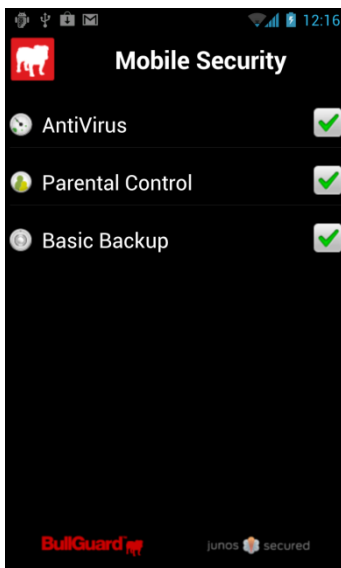
BullGuard Mobile Security contains Parental Control and Backup beside its good virus scanner.
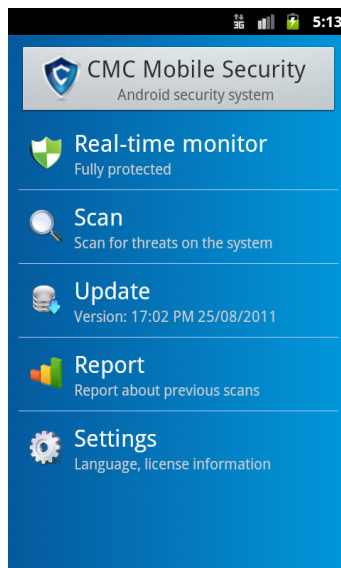
The free **CMC Mobile Security** seems to be out of date. The latest signatures are several months old.
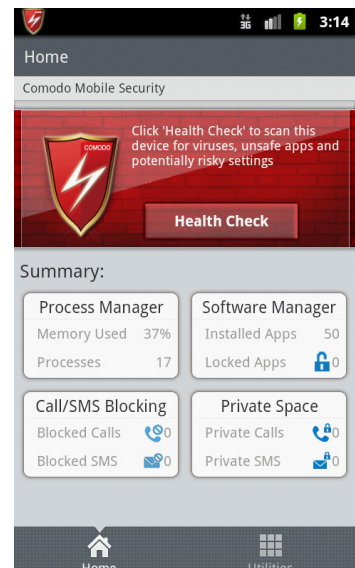
Comodo Mobile Security provides statistics at its home screen and provides good malware detection.
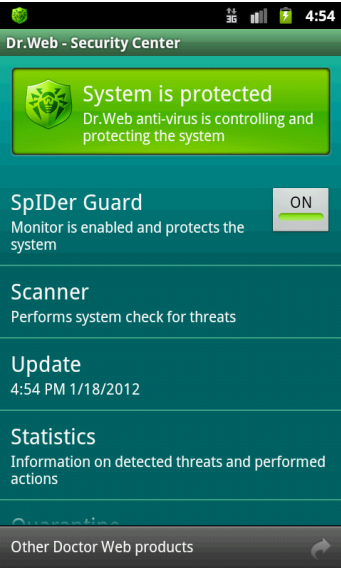
Dr.Web anti-virus Light has very good detection rates. You need the premium version to use Anti-Theft and Anti-Spam features.
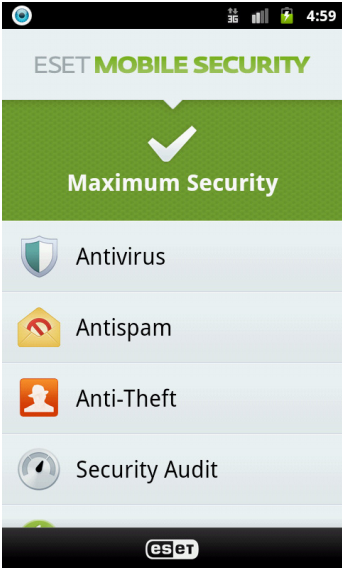
ESET Mobile Security provides a good to very good malware detection and extended Anti-Theft functions.
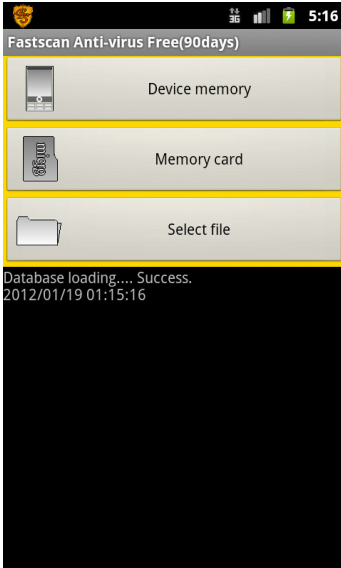
Fastscan Anti-Virus Free covers all malware families but the signatures still need to enhance.

F-Secure Mobile Security has one of the best test results. F-Secure offers a comprehensive package with Anti-Theft and Safe Browsing.
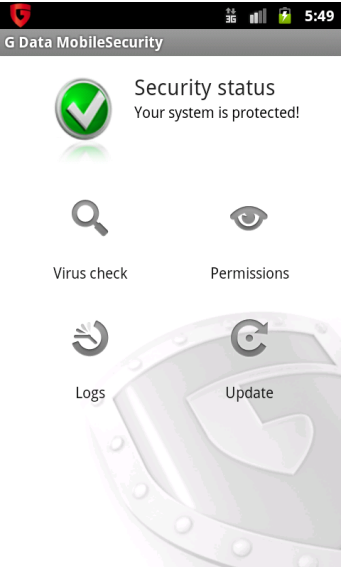
G Data MobileSecurity scans on-demand and periodically with a satisfactory detection rate. You can also check apps for specific permissions.
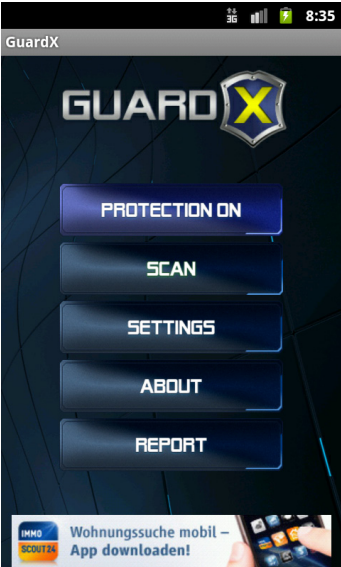
GuardX Antivirus displays advertisements. It has no real advantage over using no virus scanner with its very low detection rate.
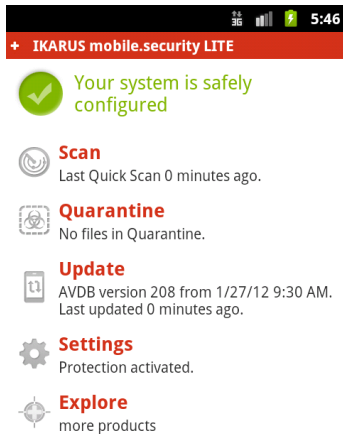
IKARUS mobile.security LITE is a plain virus scanner and got top marks in the malware detection test.
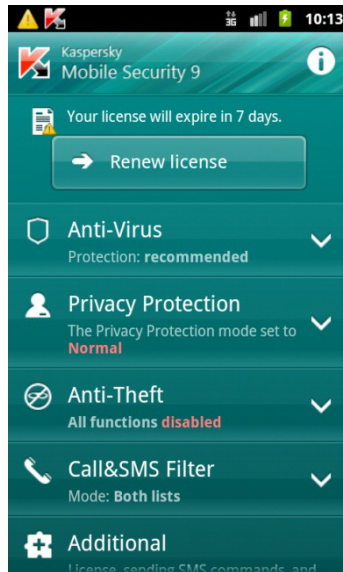
Kaspersky Mobile Security (Lite) is one of the best malware protection solutions and contains Anti-Theft, Privacy Protection, Parental Control and Data Encryption.
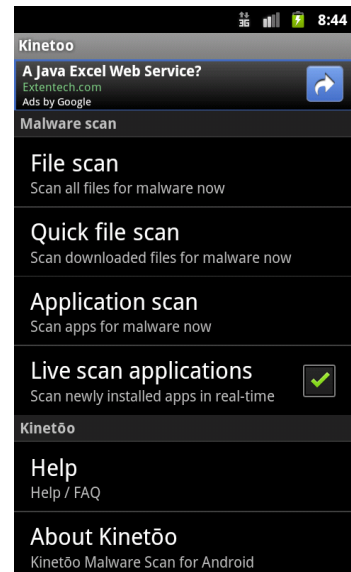
Kinetoo Malware Scan offers an average detection rate. The free version contains a regularly updated database of mobile malware and spyware.


With **LabMSF Antivirus** we found neither any malware nor the EICAR test file.
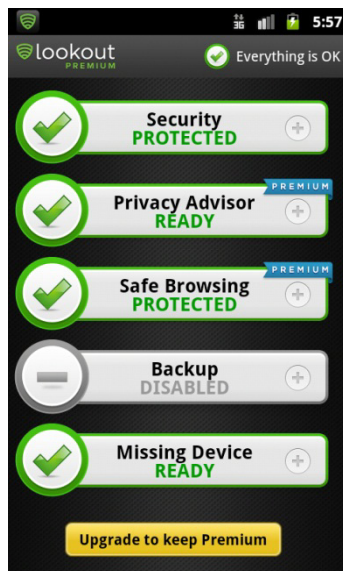
Lookout Security & Antivirus achieved very good results for malware detection. Privacy Advisor, Safe Browsing, Remote Lock and Wipe and other functions are available in the premium version.
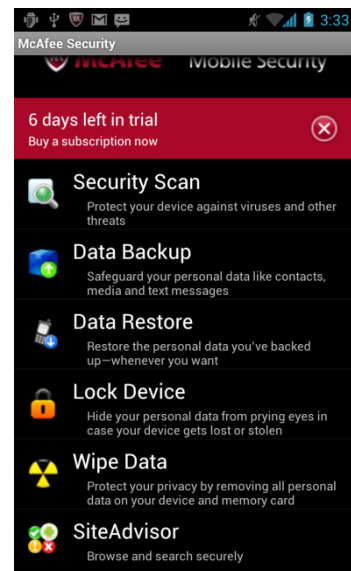
McAfee Mobile Security offers comprehensive security functions with a 1-year subscription and very good detection rates.
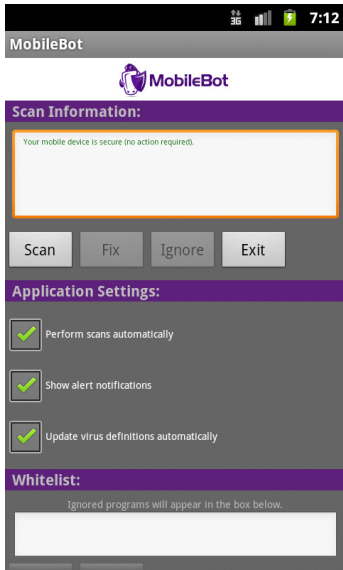
**MobileBot Antivirus** couldn't find any malware sample, but it's free of ads.
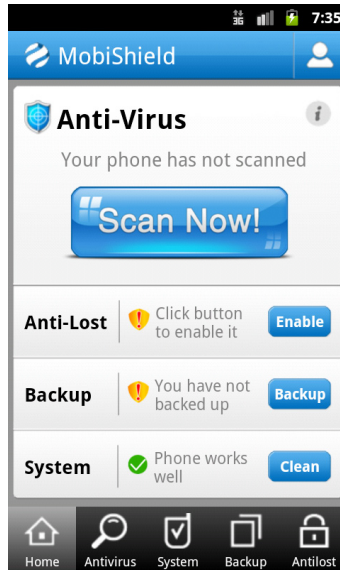
MobiShield Mobile Security contains free Antivirus, Backup, System Optimization, Anti-Theft, Traffic-Monitor and more. The malware detection test ends with moderate results.
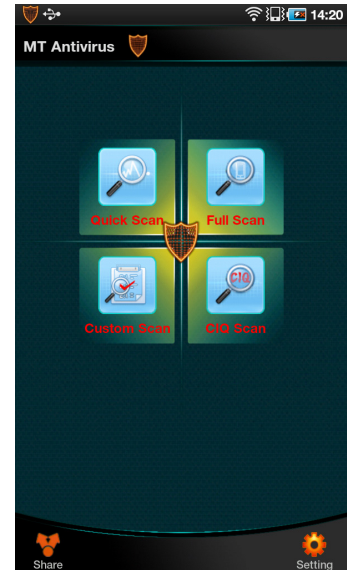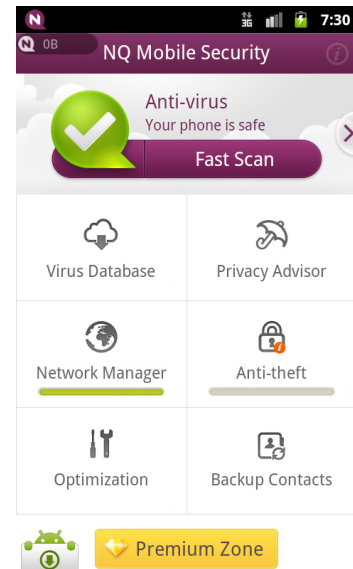

The only well working feature of **MT Antivirus** seems to be the advertisements at the bottom. Detection rates are very poor.
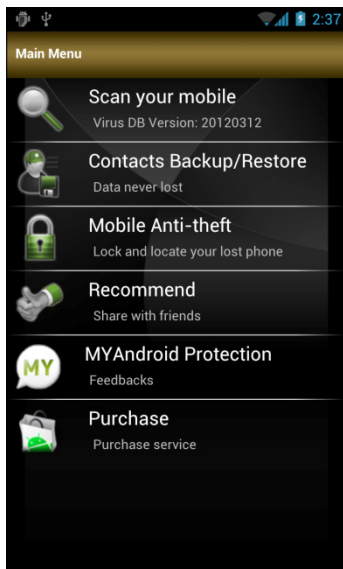

MYAndroid Protection Antivirus looks good, is easy to use and has a very good detection rate, making it one of the top products.
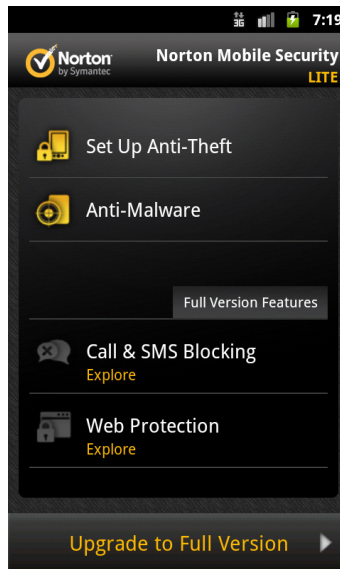
Norton Mobile Security Lite achieves good test results. The free version includes Anti-Malware and Anti-Theft.

NQ Mobile Security provides Antivirus, Network Manager, Privacy Advisor, Optimization and Backup in its free version, combined with very good detection results.
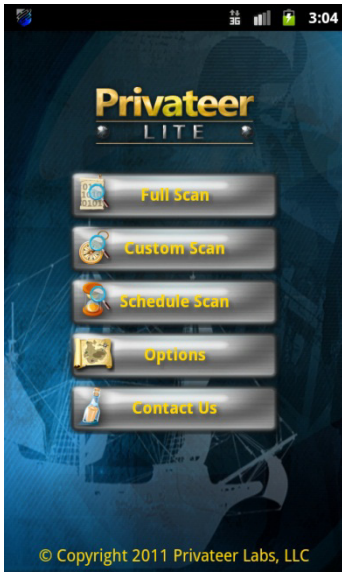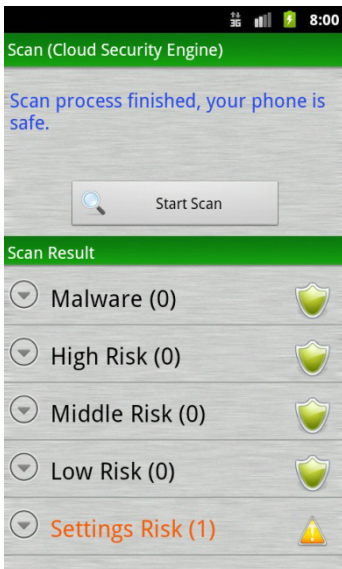
Privateer LITE has no additional functions to its scan feature, which didn't detect too many samples.
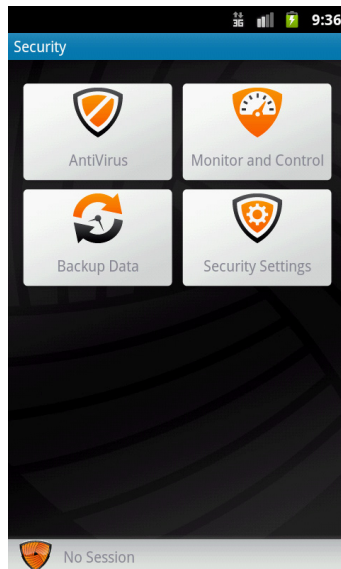

Quick Heal Mobile Security includes good Anti-Malware detection, Call Blocker, Anti-Theft and Message Filtering.
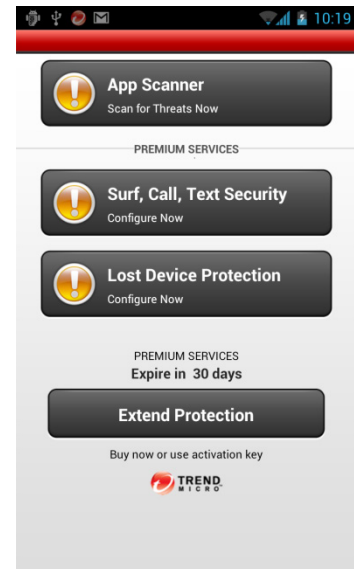

Snap Secure has a clear menu but it detected less than 40 percent of our malware test set.


Super Security is a free solution with a good detection rate. It has several other functions.


**Total Defense Mobile Security** provides a good AntiVirus module, Monitoring and Backup.

Trend Micro Mobile Security Personal Edition scored well in the malware detection test. Safe Browsing, Parental Control Call and Message Filter as well as Anti-Theft functions are integrated.
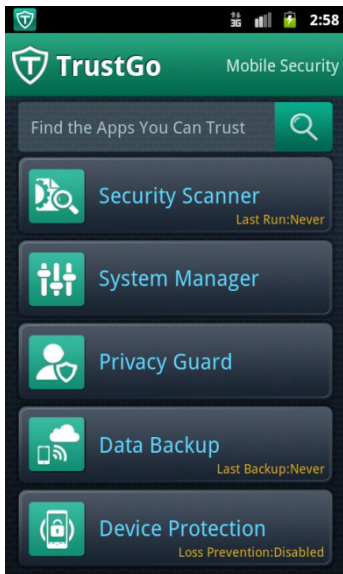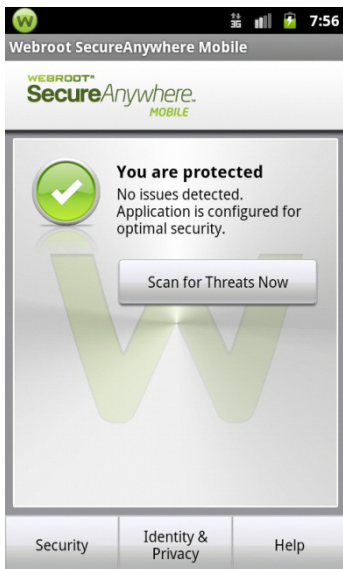
TrustGo Mobile Security has to improve its detection rates. It offers many functions for free.
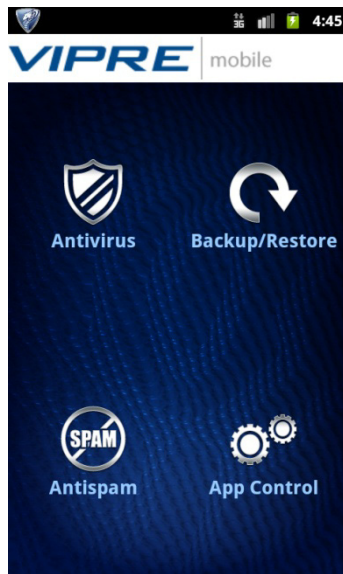
Vipre Mobile Security is available for free. It's a beta release but already shows good detection rates.
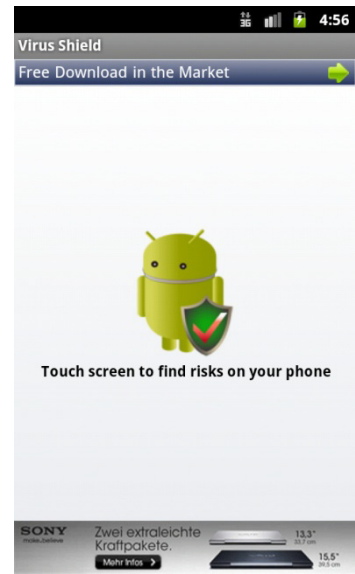
Virus Shield didn't detect much in our test. Every scan ended with full screen advertisements.

Webroot SecureAnywhere Mobile shows good detection results in the malware test. The premium version offers Secure Browsing, Lost Device Protection, Call and SMS Filter and an App Inspector.

Zoner AntiVirus Free surprises with very good test results and many free functions such as Anti-Theft, Task Manager, Call Filter, Parental Control and others.