AV-Comparatives

Mobile Security Test

Language: English

February 2015
Last revision: 30th March 2015

www.av-comparatives.org

Introduction

This test covers security products for smartphones and tablets running Google's Android operating system. The report covers details of the products made by leading manufacturers who have agreed to participate. The test was conducted in February 2015 on identical LG Nexus 5 smartphones running Android 4.4.4.

Please note that we will be conducting our main test and full review of mobile security products this summer, as usual. This report, which covers malware protection only, allows vendors to test new products before deciding whether to join the main public test and review later in the year. Participating vendors were allowed to decide whether to have their results published, but had to do this before the test was carried out. Thus the vendors shown in the results list were all confident of their respective products' abilities; several other vendors took part, but with the condition that the results would be kept internal.

Note

This test only covers malware protection. Users looking for a comprehensive review of mobile security products, including features, functionality and user interface, can consult our September 2014 review (http://www.av-comparatives.org/mobile-security), or wait until our next report is published (September of this year).

The perfect mobile-security product does not yet exist. As with Windows products, we recommend drawing up a short list after reading about the advantages and disadvantages of each product in our review. A free trial version of each candidate product can then be installed and tested for a few days; this should make the decision easier. For Android security products in particular, new versions with improvements and additional functionality are constantly being released.

The antimalware component of a mobile security product scans the mobile device for malicious software, which it deletes or quarantines. For this function to work effectively it has to be kept up-to-date; some products also make use of the cloud when scanning. When travelling abroad, users need to be careful that automatic updates and cloud scans do not incur high roaming costs from the mobile service provider. The results of our Android malware protection test can be seen on page 6.

Products tested

The products that participated in this year's test are listed below. The manufacturers either provided us with the latest version of their product available on their website or several third party stores, or confirmed that it was available from the Google Play Store at the time of the test (February 2015).
Most of the tested products can either be found on Google play or in case of Anguanjia on their website[1] and on several big Chinese third-party stores[2]. The tested Qihoo 360 version is only available on the Qihoo 360 website[3].

- AhnLab V3 Mobile 2.1.2.17
- Anguanjia 安全管家 5.0.0
- Antiy AVL for Android 2.3.10
- Avast Mobile Security 4.0.7875
- Avira Antivirus Security 3.9
- Bitdefender Mobile Security 2.36.716
- ESET Mobile Security 3.0.1249.0-0
- G Data Internet Security 25.7.1.3a605e88
- Kaspersky Internet Security 11.7.4.822
- Qihoo 360 AntiVirus 1.3.3.1025
- Quick Heal Total Security 2.01.020
- Trend Micro Mobile Security 6.0

[1] http://www.anguanjia.com/?c=Downsoft&id=6
[2] http://shouji.baidu.com/soft/item?docid=7514506
[3] http://edl.cloud.360safe.com/360Antivirus_1.3.3.1025_EN.apk

How great is the risk of infection with an Android smartphone?

This question is difficult to answer, as it depends on many different factors. In western countries, if using only official stores such as Google Play, the risk is lower than in many Asian countries, especially China. Many rooted phones and unofficial app stores can be found there, increasing the chance of installing a dangerous app. In many parts of Asia, the smartphone is used as a replacement for the PC, and is frequently used for online banking. Banking apps are also becoming more popular in Europe and the USA. There is a high risk involved in receiving the TAN code on the same phone that is used to carry out the subsequent money transfer. In western countries, assuming you stick to official app stores and don't root your phone, the risk is currently relatively low, in our opinion. However, we must point out that "low risk" is not the same as "no risk". In addition, the threat situation can change quickly and dramatically. It is better to be ready for this, and to install security software on your smartphone. Currently, we would say that protection against data loss in the event of the phone being lost or stolen is more important than malware protection.

Some security-software vendors may claim that several dozens of millions of Android malware samples exist; in reality, most of these programs are merely "potentially unwanted" rather than genuinely malicious apps. Furthermore, most of the true malware samples contain malicious code that has been used before, but has simply been repackaged in new/different apps; such apps may even only have been online in popular app stores - and thus present a high threat to users - for a short time.

What else can I do to protect my mobile device?

Methods of attacking mobile devices are getting more and more sophisticated. Fraudulent applications attempt to steal users' data or money. To reduce the risk of this happening, follow the advice given here. Only download apps from Google Play or reputable app makers' own stores. Avoid third-party stores and sideloading[4]. Another indication of untrustworthy apps is irrelevant access rights. For example, an app that measures the speed at which you are travelling has no need to access your phone book or call log. Of course, even if an app does this, it is not a clear-cut indication that it is malicious, but it makes sense to consider whether it is genuine and should be used. A look at the reviews in the app store is also a guide; avoid apps with bad or dubious reviews. If you Root your smartphone, you will have more functionality on the phone, but equally the opportunity for malicious apps to take control will also increase. Another point to consider is the warranty. It is not legally clear-cut whether the warranty is still valid if the phone is rooted. In many cases, the warranty will be considered null and void.

AVC UnDroid Analyser

At this point, we would like to introduce AVC UnDroid, our new malware analysis tool, which is available free to users. It is a static analysis system for detecting suspected Android malware and adware and providing statistics about it. Users can upload .apk files and see the results in various analysis mechanisms.

We invite readers to try it out: http://www.av-comparatives.org/avc-analyzer/

[4] http://en.wikipedia.org/wiki/Sideloading

Baseline protection provided by Google Android

Google Android contains basic protection against malware out-of-the-box. If the user installs new software on his phone, the phone asks the Google Safebrowsing API to check whether the app is malicious or not. Our intention was to identify the detection rate of this service for all malicious samples in the test. After some tests, we found out that the results vary, even if we always perform the test with the same malicious sample. After some research, we found that the number of requests to the API of Google Safebrowsing is limited[5]. Google does not provide absolute values for the number of requests. The API documentation states "*In order to ensure high availability of the API, Google limits the frequency of client requests. This is handled differently depending on the type of request*".

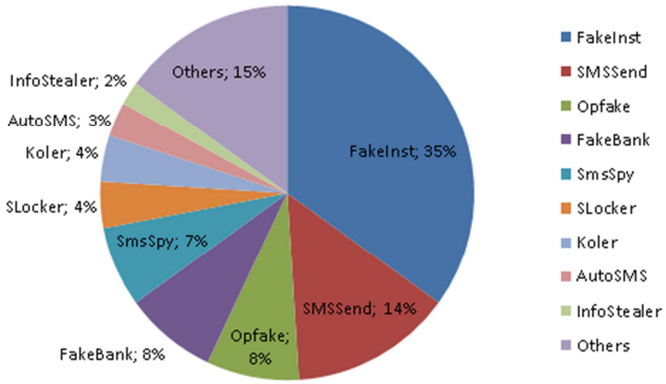
To double-check our findings we set up a man-in-the-middle attack and analysed the network traffic while installing new applications. We could confirm the findings from previous tests with this method, as the responses from the Google Safebrowsing API were different, even if we always installed the same application. In the case of a detection, the API showed a description of the string on the display, such as "It has been modified to include potentially harmful code" and additional data. In the case of a miss the response was just a two byte long response ("`08 00`" in Hex).

As the size of the sample set was big, we could not get any coherent detection rates for the Google Safebrowsing service. Requests to the security team of Google to whitelist our devices for those kind of limitations were not answered in time.

[5] https://developers.google.com/safe-browsing/developers_guide_v3#RequestFrequency

Test Set

We collected the malware samples used in the test during the period of few months leading up to the test. **4,523** malicious applications were used to create a representative test set. So-called "potentially unwanted apps" were removed from the test-set. The test-set consisted of 125 main malware families



The security products were updated and tested on the 23rd February 2015. The test was conducted with an active Internet connection on genuine Android smartphones (no emulators were used). The test set consisted exclusively of .APK files. An on-demand scan was conducted first. After this, every undetected app was installed manually. We did this to allow the products to detect the malware using real-time protection.

Protection rate results

Rank	Vendor	Protection rate[6]	Product
1.	Antiy	100.0%	Antiy AVL for Android 2.3
	Qihoo 360		Qihoo 360 AntiVirus 1.3
2.	AVIRA	99.9%	Avira Antivirus Security 3.9
	ESET		ESET Mobile Security 3.0
3.	Avast	99.8%	Avast Mobile Security 4.0
4.	AhnLab	99.7%	AhnLab V3 Mobile 2.1
5.	Bitdefender	99.6%	Bitdefender Mobile Security 2.36
	Kaspersky Lab		Kaspersky Internet Security 11.7
6.	Trend Micro	99.3%	Trend Micro Mobile Security 6.0
7.	Quick Heal	98.6%	Quick Heal Total Security 2.0
8.	G Data	96.1%	G Data Internet Security 25.7
9.	Anguanjia	94.7%	Anguanjia 安全管家 5.0

We additionally conducted a false-positive test using the top 200 ad-free programs from various popular app stores. Only **Avast** produced a single false alarm when installing those apps, all other programs in this test had none. We did however notice that all products are prone to false alarms and misidentification especially of Chinese apps and/or apps obtained outside of well-known stores. In Asia, perceptions of what constitutes unwanted apps may vary from those in Europe or North America. We removed disputed questionable or controversial samples from the test-sets.

[6] Some vendors provide several different product versions. The results reached in this test are therefore only applicable to the tested versions; they are not applicable to any other product versions, product names or languages.

Copyright and Disclaimer

For more information about AV-Comparatives and the testing methodologies please visit our website.

AV-Comparatives (March 2015)