Anti-Virus Comparatives

Android Test

Language: English
January 2017

Last Revision: 28th February 2017

www.av-comparatives.org

Introduction

In April 2014, the website Android Police (www.androidpolice.com) published the results of their investigation into an Android app called *Virus Shield*.[1] At the time, the app had been downloaded over 10,000 times, and was the most successful new paid-for app and third most successful paid-for app overall. It had also received an impressive 4.7 out of 5 rating from users. As its name suggests, Virus Shield was supposed to be an antimalware app for Android devices. However, when Android Police investigated the app, they found that it had no antivirus functions at all, and that tapping on the icon supposed to activate the protection does literally nothing except change the icon from a cross to a tick (checkmark). The only true claims made by the developer were that it had minimal effect on battery life and did not display advertisements.

On discovering that the app was a scam, Google removed[2] *Virus Shield* from the Play Store, suspended the developer's account, and refunded users who had purchased the app.[3] This means that on this occasion, little or no harm was done, but it shows clearly how easy it is to produce a poorly performing app and make it successful by means of good marketing. Android Police should be congratulated for discovering this scam; they point out that it would be difficult for Google to stop all such scams, and that more rigorous testing of apps available on the Play Store would make the store less open than it is now. It should be noted that it is easier to spot a malicious app – due to suspicious code – than a useless app like Virus Shield, which is not in itself harmful. There is also the possibility that thorough scrutiny of apps before they can be released might be prohibitively expensive and/or time-consuming. Google's advice to check the ratings of an app before purchasing it is in principle good, but clearly it would not have helped in this case – regardless of whether the overwhelmingly positive reviews were fakes posted by the developer, or genuine reviews posted by duped users. Of the apps tested for this report, practically all had a rating of 4 or higher, even though a number of them turned out to be ineffective.

In the case of antimalware apps, there is a straightforward solution: testing the apps against real malware samples by independent research labs. The aim of this test is to find out which of the antimalware apps for Android in the Google Play Store are genuine and effective, and to expose any that are ineffective or just fake.

[1] http://www.androidpolice.com/2014/04/06/the-1-new-paid-app-in-the-play-store-costs-4-has-over-10000-downloads-a-4-7-star-rating-and-its-a-total-scam/
[2] http://www.theregister.co.uk/2014/04/08/google_kills_virus_app_after_decompilation_proves_its_a_fake/
[3] http://www.theregister.co.uk/2014/04/22/google_to_refund_buyers_of_fake_antivirus_app/

Tested Products

For this test, we searched for and downloaded over 100 antimalware security apps of different developers from the Google Play Store.

The following **110** security apps were analyzed:

ADV Antivirus Mobile Agency
AegisLab Antivirus Premium
AhnLab V3 Mobile Security
AiDevLab Security Antivirus Max Clean
AndroHelm AntiVirus
Antiy AVL
Ascal Antivirus & Mobile Security
Avast Mobile Security & Antivirus
AVC Security Antivirus Clean
AVG Antivirus PRO
AVIRA Antivirus Security
Baboon Antivirus
Baidu DU Antivirus Mobile Security & AppLock
Bastiv Security Antivirus
Bitdefender Mobile Security & Antivirus
BitInception Antivirus
BKAV Security Antivirus Free
Bluesteeleffect Studios Antivirus Security Cleaner Pro
Brainiacs Apps Antivirus System
BuildOut Tech Antivirus
BullGuard Mobile Security and Antivirus
CA Uber Apps Security Antivirus Android
Check Point ZoneAlarm Mobile Security
Cheetah Mobile CM Security CleanMaster
CHOMAR Antivirus Security
Comodo Mobile Security
Cora Mobile Antivirus
CTPlate Free Antivirus
CY Security Antivirus Cleaner
Kaspersky Antivirus & Security
LINE Antivirus
LionMobi Power Security Antivirus Clean
Live multi Player Game Antivirus Total Security
Lookout Antivirus & Security
MalwareBytes Anti-Malware
Max Security Antivirus PRO
McAfee Security & Antivirus
MediaCenterSocial Antivirus
Melodiu Ideas LuLa Antivirus Malware Protect
NCN-NetConsulting Free Antivirus Clean&Boost
Netlink Mobile Antivirus Pro
NguyenManh Antivirus Security
NOAH Security Antivirus
NQ Mobile Security & Antivirus
NSHC Ariasecure Bornaria security (Antivirus)
One App Super Clean Speed Security MAX
Panda Free Antivirus
Perfect Tools Antivirus
Play Studio Apps Mobile Security Antivirus
Playnos Yalp Security Antivirus
Pocao Antivirus
Poke And Touch Security Antivirus
Pro Tool Apps Antivirus Security
Psafe Antivirus
Qihoo 360 Mobile Security
Quick Heal Antivirus & Mobile Security
Quicken Security Studio Smart Antivirus
REVE Antivirus Mobile Security

Defenx Security Suite

DevByMe MDD Guard Antivirus & Antispyware

Dr.Web Antivirus Light

Duc Nguyen FJC Antivirus Spy Mobile Security Pro

Emsisoft Mobile Security

EnjoyPlus Security Antivirus

eScan Mobile Security

ESET Mobile Security & Antivirus

EveryZone Turbo Vaccine Mobile

Farga Security Antivirus

Fast Track Super Security Free AntiVirus

Fotoable Photo Editor Creative Cleaner&Security&Applock

F-Secure Mobile Security

G DATA Internet Security

GO Security Antivirus Applock

Gpaddy Antivirus Pro

Green Booster Antivirus

Guaraw Yadaw Antvirus Security Shield

H2 Free Antivirus

Hi Dev Team Security Antivirus & Privacy

Hornet Antivirus PRO

Ikarus mobile.security

IncodeSolutions Anti-Malware

Iobit AMC Security

Itus Antivirus

K7 Mobile Security

Security Defend Total Antivirus Defender PRO

Smartdev Studio Security Antivirus

Sophos Free Antivirus and Security

SPAMfighter VIRUSfighter Antivirus

Stock VIP Antivirus

Super Security Tech Ace Security Plus Antivirus

SuperSoftDev Antivirus

Symantec Norton Antivirus & Security

Taolee Antivirus

Tencent WeSecure Antivirus

TG Soft VirIT Mobile Security

TiTanTech CleaningVirus 360

Total Defense Mobile Security

Trend Micro Mobile Security & Antivirus

TrustGo Antivirus & Mobile Security

Trustlook Premium Mobile Antivirus

Vasa Virus Seeker Mobile Security

Viettel Antivirus Free Mobile Security

VSAR Total Virus Scanner & Remover

Webroot Security Premier

WeMakeItAppen Antivirus Fast

WhiteArmor Security Pro

Z Security Apps Studio Virus Cleaner Antivirus

Zemana Mobile Antivirus

Zillya! Internet Security & Antivirus

ZONER Mobile Security

The antimalware apps from the following 9 vendors were so buggy that they could not be installed/tested: ***CY Security***, ***DevByMe***, ***Gauraw Yadaw***, ***Live multi Player Game***, ***MediaCenterSocial***, ***NguyenManh***, ***REVE***, ***SPAMfighter***, and ***SuperSoftDev***.

The antimalware apps from the following 3 vendors pose risks, as they contain unsafe features, collect sensitive data: ***Cora***, ***Melodiu Ideas*** and ***Netlink***

The antimalware apps of the following 10 vendors have in the meantime already been removed by Google from the Play Store: ***BuildOut Tech***, ***Duc Nguyen***, ***EveryZone***, ***Perfect Tools***, ***Playnos Yalp***, ***Poke And Touch***, ***Quicken***, ***Stock***, ***Taolee*** and ***TiTanTech***.

Most of the apps removed by Google, as well as the heavily buggy or unsafe apps/apps with low protection scores, appear to have been developed either by amateur programmers, or by software manufacturers that are not focused on the security business (i.e. develop all kinds of apps, and/or are in the advertisement/monetization business). Apps made by amateurs can be often spotted in the Google Play Store by looking at the options for contacting the authors. Typically, hobby developers will not provide a website address, merely an email address (usually Gmail, Yahoo, etc.).

Additionally, most such apps do not provide any sort of privacy policy. Google is planning[4] to purge from the Play Store all apps which lack a privacy policy, which could help to get rid of some low-quality apps. Of course, one should bear in mind that not all apps made by amateur developers are necessarily ineffective.

[4] https://nakedsecurity.sophos.com/2017/02/10/google-set-to-purge-play-store-of-apps-lacking-a-privacy-policy/

Test Procedure

Description of test system

The Android security solutions tested were checked for their efficacy in protecting against the top 1,000 most common Android malware threats of 2016. Manually testing 100+ security products against 1,000 malicious apps is not practicable. Because of that, the test was run on our automated Android testing framework.

Even though the testing process is automated, the framework realistically simulates real-world conditions. This includes testing on physical Android devices (as opposed to emulators), as well as simulation of realistic device usage patterns.

The framework consists of two components: a client app on each of the test devices, and a server application. The client app monitors the status of the device and sends its findings to the server at the end of a test case to document the testing process. The client monitors file and process changes, newly installed apps and their permissions, as well as reactions of the installed security software to malicious activities on the device. The server remotely controls the test devices via WiFi and organizes the results received by the client applications.

The system scales well with the number of connected clients. This allows a large number of security products to be tested in parallel. To ensure even chances for all participating products, connected clients can be synchronized to start the execution of a test case at the same time. This is especially important for testing recent malware samples, which security vendors may not have encountered yet.

Methodology

The test was performed on the 12th of January 2017, on Nexus 5 devices running Android 6.0.1 ("Marshmallow"). Each security app was installed on a separate physical test device. Before the test was started, the software testbed on all test devices - Android itself, stock Android apps, plus testing-specific third-party apps - was updated. After this, automatic updates were switched off, thus freezing the state of the test system. Next, the security apps to be tested were installed and started on their respective devices, updated to the latest version where applicable, and the malware definitions brought fully up to date.

If any security application encouraged the user to perform certain actions to secure the device, such as running an initial scan, these actions were performed. If the application contained protection functions such as on-install scanning, cloud protection, or detection of Potentially Unwanted Applications (PUA), these features were activated as well. To ensure that all security products could access to their respective cloud analysis services, each device was connected to the internet via a WiFi connection.

Once these steps were taken, a clean snapshot of each device's storage was created, and the test was started.

Each test case was conducted using the same process:

1. Open the Chrome browser and download the malicious sample
2. Open the downloaded .apk file using a file explorer app
3. Install the malicious app
4. Execute the installed app

After each of the above steps, the installed security application was granted enough time to analyze the malicious sample and notify the user of malicious activity on the device.

If, at any point during the execution of a test case, the installed Anti-Virus application detected and blocked the malicious sample, the sample was considered "detected" and the test case was concluded (apps detected after installation were not executed, for instance).

At the end of each test case, the device was reset to a clean state. If the malicious sample was not executed on the device, the sample was uninstalled and/or deleted from the device storage. If the malicious sample was run, the clean device snapshot was restored before starting the next test case.

When calculating the protection score for each product, we did not distinguish between different detection times during a test case (e.g., after download vs. after install). The only aspect influencing the protection rate is whether the security solution protected the device from being compromised by the malicious sample.

A basic false-alarm test was done, just to check that none of the antimalware products "protects" the system by simply identifying all new apps as malicious. None of the apps tested detected any of 50 popular installed on a clean Android device as malware.

Test Cases

For this test, the Top 1,000 most common Android malware threats of 2016 were used. With such samples, detection rates of between 90% and 100% should be easily achieved by genuine and effective antimalware apps.

Number of tested apps	110
Number of tested malicious APKs	1000
Number of tested clean APKs	50

In total, around 100,000 test runs have been performed for this report.

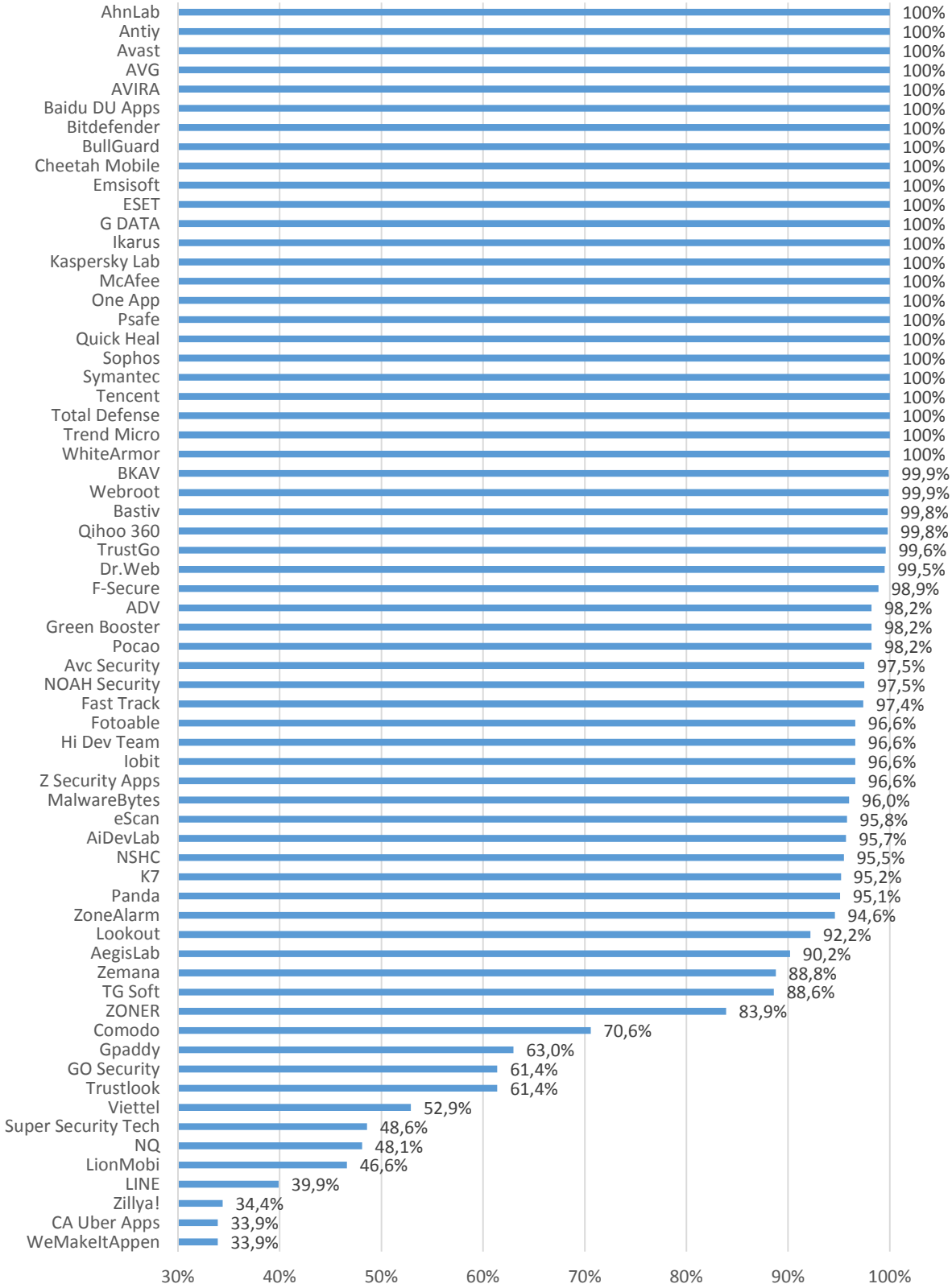
Test Results

Vendor	%
AhnLab	100,0%
Antiy	
Avast	
AVG	
AVIRA	
Baidu DU Apps	
Bitdefender	
BullGuard	
Cheetah Mobile	
Emsisoft	
ESET	
G DATA	
Ikarus	
Kaspersky Lab	
McAfee	
One App	
Psafe	
Quick Heal	
Sophos	
Symantec	
Tencent	
Total Defense	
Trend Micro	
WhiteArmor	
BKAV	99,9%
Webroot	
Bastiv	99,8%
Qihoo 360	
TrustGo	99,6%
Dr.Web	99,5%
F-Secure	98,9%
ADV	98,2%
Green Booster	
Pocao	
Avc Security	97,5%
NOAH Security	
Fast Track	97,4%
Fotoable	96,6%
Hi Dev Team	
Iobit	
Z Security Apps	
MalwareBytes	96,0%
eScan	95,8%
AiDevLab	95,7%
NSHC	95,5%
K7	95,2%
Panda	95,1%
ZoneAlarm	94,6%
Lookout	92,2%

Vendor	%
AegisLab	90,2%
Zemana	88,8%
TG Soft	88,6%
ZONER	83,9%
Comodo	70,6%
Gpaddy	63,0%
GO Security	61,4%
Trustlook	
Viettel	52,9%
Super Security Tech	48,6%
NQ	48,1%
LionMobi	46,6%
LINE	39,9%
Zillya!	34,4%
CA Uber Apps	33,9%
WeMakeItAppen	

AndroHelm	0 - 30%
Ascal	
Baboon	
BitInception	
Bluesteeleffect Studios	
Brainiacs Apps	
CHOMAR	
CTPlate	
Defenx	
EnjoyPlus	
Farga	
H2	
Hornet	
IncodeSolutions	
Itus	
Max Security	
NCN-NetConsulting	
Play Studio Apps	
Pro Tool Apps	
Security Defend	
SmartDev Studio	
Vasa	
VSAR	

The table above shows the protection rates reached by the products of the respective vendors. We consider apps scoring below 30% on common Android threats to be unsafe and completely unacceptable.

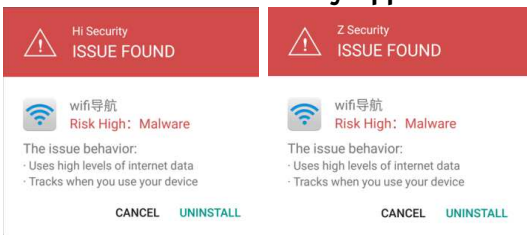


The anti-malware apps of **AndroHelm**, **Ascal**, **Baboon**, **BitInception**, **Bluesteeleffect Studios**, **Brainiacs Apps**, **CHOMAR**, **CTPlate**, **Defenx**, **EnjoyPlus**, **Farga**, **H2**, **Hornet**, **IncodeSolutions**, **Itus**, **Max Security**, **NCN-NetConsulting**, **Play Studio Apps**, **Pro Tool Apps**, **Security Defend**, **SmartDev Studio**, **Vasa** and **VSAR** detected between 0% and 30% of the 1,000 malicious Android apps, and are not listed in the chart above – partly for display reasons, but also because they are ineffective.

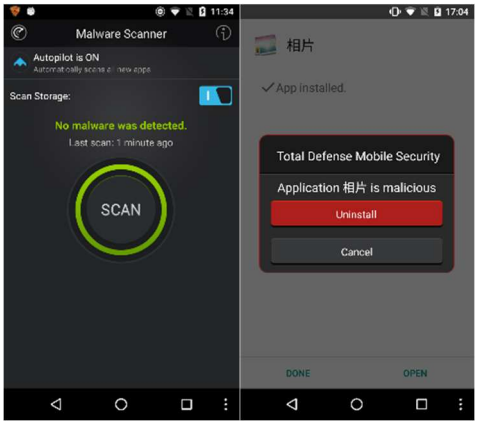
Notes

Some products make use of other engines (see examples below). While some score the same, some of them score differently despite making use of the same engine. According to the licensing developers, this is often the case due to several factors, such as other internal settings used by the third-party apps, the use of older engines or additional engines, engine implementation and bugs.

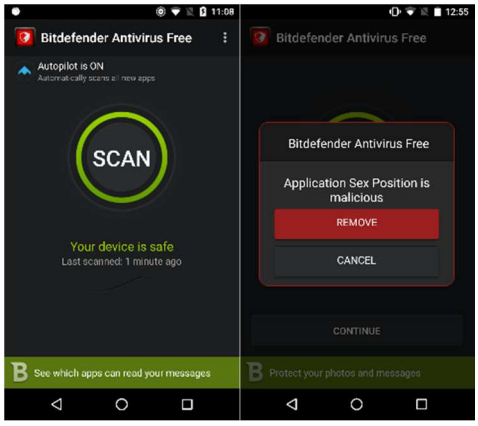
- **AiDevLab** makes use of the **Tencent** engine.
- **GO Security** makes use of the **Trustlook** engine**.**
- **PSafe** is using an engine from **Qihoo**.
- **Iobit**, **Fotoable**, **One App**, **WeMakeItAppen** and **CA Uber Apps** make use of the ***OpenAVL*** engine.
- **Hi Dev Team** and **Z Security Apps Studio** are both from ***TCL***.



- **TotalDefense** uses and appears to be a rebranded version of **Bitdefender**.

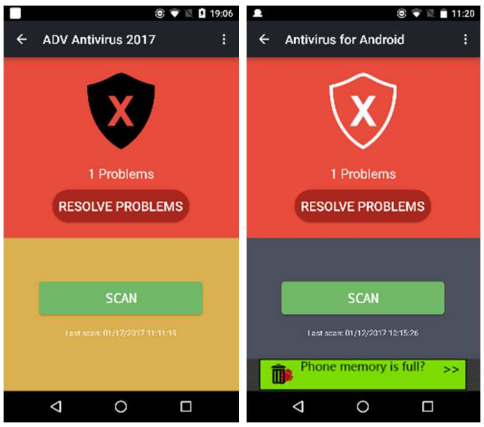


TotalDefense



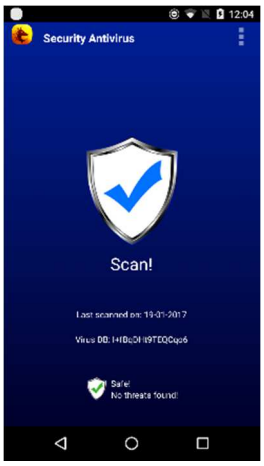
Bitdefender

- **ADV** and **Pocoa** are basically the same (but claim to be from different developers):

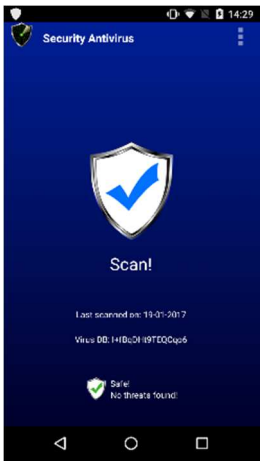


ADV *Pocoa*

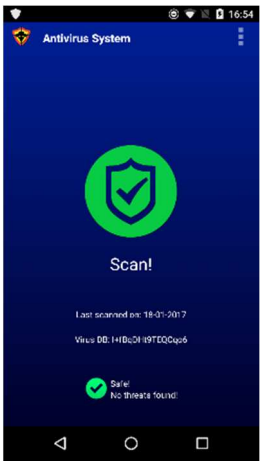
- **Bluesteeleffect Studios**, **EnjoyPlus**, **Brainiacs Apps**, **ProTool Apps** are basically all the same (claim to be from different developers). All of them detected **0%** of the used malware test-set.



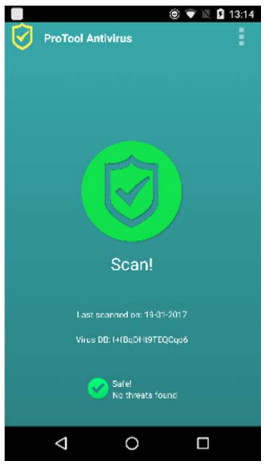
Bluesteeleffect Studios



EnjoyPlus



Brainiacs Apps



ProTool Apps

Conclusion

Amongst the security apps available from the Google Play Store there are a few which have so many bugs that they either cannot be installed, or crash so frequently as to be unusable.

Some of the Android security products detected far too few of the malware samples in our test – in some cases literally nothing - to be recommended as anti-malware apps. In a few cases, this might be due to apps having been abandoned by the developer and thus no longer being updated in the Play Store. Whilst such cases cannot be regarded as scams, we consider it irresponsible of the developers not to remove these apps from the Store.

A few products from relatively well-known vendors did not score very well. It is possible that the manufacturers have developed them purely for marketing reasons. That is to say, there is not much money in the Android security-app market, but having an Android app visible in the Google Play Store helps to keep the vendor visible, and may thus promote their other, more profitable products such as Windows security programs.

24 of the products we tested detected 100% of the malware samples; considering that the most common malicious Android apps of 2016 were used, this is what they should do. Most of the vendors that usually take part in independent tests score highly, as their products are regularly scrutinised, and they actively develop them to ensure they are effective.

When it comes to choosing an Android security app, we recommend considering the following factors. Using user ratings is clearly not effective, as the vast majority of users will give their rating based solely on the user experience, without having any idea as to whether the app offers effective protection. Some other reviews will have been faked by developers. Practically all the 110 apps we looked at had a review score of 4 or higher on the Google Play Store. Similarly, the number of downloads can only be a very rough guide; a successful scam app may be downloaded many times before it is found to be a fake. Using well-known and reputable, verified vendors is recommended. As well as participating in tests by independent test institutes, such vendors will have a professional website with contact information and a privacy policy. It should also be possible to try the app – typically some few weeks trial use is allowed – before purchasing. Users can then assess the usability and any additional features of the product. A number of vendors make very effective free versions of their apps; generally these are more likely to display advertising than the paid version, though this is not always the case.

For additional Android security app tests and reviews, please see:
https://www.av-comparatives.org/mobile-security/

Copyright and Disclaimer

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

AV-Comparatives (February 2017)