

Independent Tests of Anti-Virus Software



Android Test 2019

TEST PERIOD: JANUARY 2019
LANGUAGE: ENGLISH
LAST REVISION: 12TH MARCH 2019

WWW.AV-COMPARATIVES.ORG

Contents

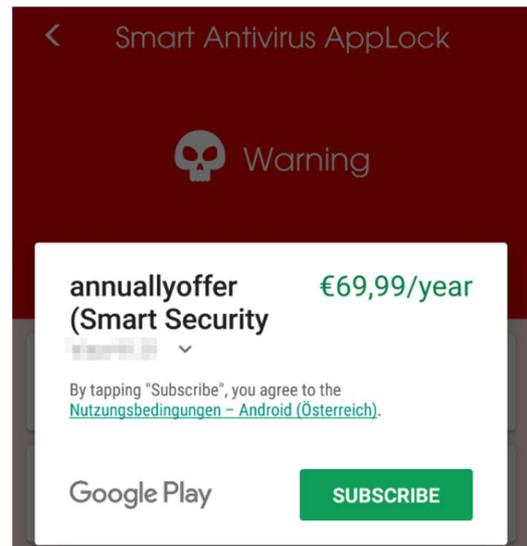
INTRODUCTION	3
TESTED PRODUCTS	4
TEST PROCEDURE	7
TEST CASES	8
TEST RESULTS	9
NOTES	11
CONCLUSION	18
COPYRIGHT AND DISCLAIMER	19

Introduction

AV-Comparatives' 2017 test of Android antivirus products was inspired by the discovery of an Android app called *Virus Shield*, which claimed to scan mobile devices for malware, but in fact did nothing of the sort. In reality, running the app simply showed a progress bar, supposed to represent scan progress, followed by an announcement at the end of the "scan" that the device was free of malicious apps. Worryingly, the app had been available on the Google Play Store, and thousands of users had paid money for it (although this was ultimately refunded to them by Google).

Last year's test showed that in addition to several apps that are equally ineffective at protecting the device against malware, there are other apps that employ dubious detection mechanisms. These detect most other installed apps as potentially harmful, excluding only those with white-listed package names. With user interfaces seemingly generated from a few templates, the main purpose of these apps seems to be generating easy revenue for their developers – rather than actually protecting their users¹.

Including these dubious apps, we found the malware protection of almost 40% of the tested Android AV apps to be inappropriate.



To help owners of Android devices to distinguish between genuine, effective Android antivirus apps on the one hand, and dubious/ineffective ones on the other, AV-Comparatives have again tested the effectiveness of antimalware programs for Android, in the 2019 Android Test.

¹ <https://www.welivesecurity.com/2018/04/05/google-play-ad-slingers/>

Tested Products

For this test, we searched for and downloaded **250** antimalware security apps by various different developers from the Google Play Store.

The following **80** apps detected over 30% of malicious apps, and had zero false alarms:

AegisLab Antivirus Premium	MalwareBytes Anti-Malware
AhnLab V3 Mobile Security	Max Dev Labs Antivirus
Alibaba Alibaba Master	Media Master MD Antivirus
Antivirus Apps Studio Antivirus	MicroWorld eScan Mobile Security
Antiy AVL	MY-DATA Mobile Security
Apex Apps Mobile Security	MYMobile Security Warrior
APUS Group APUS Security	NQ Mobile Security
Avast Mobile Security	NSHC Droid-X 4U
AVG AntiVirus	ONE App Virus Cleaner
AVIRA Antivirus	Panda Free Antivirus and VPN
Bitdefender Mobile Security & Antivirus	Phone Clean Apps Virus Cleaner
Brainiacs Apps Antivirus System	Power Tools Apps Antivirus
BSafe Labs Antivirus	Privacy Lab Antivirus & Mobile Security
BullGuard Mobile Security and Antivirus	PSafe dfndr security
CAP Lab Phone Cleaner	Qihoo 360 Mobile Security
Check Point ZoneAlarm Mobile Security	Quick Heal Antivirus & Mobile Security
Chili Security Android Security	REVE Antivirus Mobile Security
Clean Boost+ Studio Phone Cleaner	Securion OnAV
Comodo Mobile Security	Samsung Device Maintenance
Dr.Web Security Space	Smooth Apps Studio Super Antivirus
DU APPS STUDIO Speed Booster & Cleaner	Sophos Mobile Security
Emsisoft Mobile Security	Super Cleaner Studio Super Antivirus
ESET Mobile Security & Antivirus	Supermobilesafe Super Security
ESTsoft Dr.Capsule Antivirus	STOPzilla Mobile Security
Fotoable Antivirus & cleaner	Super Security Studio Antivirus
F-Secure Internet Security & Mobile Antivirus	Symantec Norton Security
G DATA Internet Security	TAPI Security Labs Antivirus & Virus Cleaner
GizmoSmart Antivirus	Tencent WeSecure
Google Play Protect	TG Soft VirIT Mobile Security

Hawk App Super Cleaner	ThreatTrack VIPRE Mobile Security
Hi Security Virus Cleaner	Total Defense Mobile Security
Hyper Speed Antivirus	Trend Micro Mobile Security & Antivirus
IKARUS Mobile Security	TrustGo Antivirus & Mobile Security
IntelliAV Anti-Virus	Trustlook Antivirus & Mobile Security
IObit AMC Security	Trustwave Mobile Security
Kaspersky Lab Mobile Antivirus	WatchdogDevelopment Mobile Security
K7Computing Mobile Security	We Make It Appen Antivirus
Lookout Security & Antivirus	Webroot Mobile Security & Antivirus
McAfee Mobile Security	Zemana Antivirus & Security
MalwareFox Anti-Malware	ZONER AntiVirus

The antimalware apps from the following 138 vendors detected less than 30% of the Android malware samples, or had a relatively high false alarm rate on popular clean files from the Google Play Store: *1Machine System Sdn Bhd, actionappsgamesstudio, Amantechnoapps, AMIGOS KEY, Amnpardaz Soft, AndroHelm Security, ANTI VIRUS Security, Antivirus Mobile Lab, antivirus security, appflozen, appsshow, Appzila, Arcane Apps, AS team security phone Lab, asuizksidev, Ayogames, AZ Super Tools, azemoji studio, Baboon Antivirus, bESapp, Best Battery Apps, Best HD Wallpapers APPS, Best Tools Pro, BestOne, Bit Inception, BKAV, Bom Bom, Booster studio Laboratory Inc., brouno, Bulletproof AV, Caltonfuny Antivirus Phone, Cheetah Mobile, CHOMAR, Chromia, Cloud 7 Services, Core Antivirus Lab, CPCORP TEAM: Photo blur & photo blender, CreativeStudioApps, CY Security, Defenx, DefineSoft, DreamBig Studios, DU Master, electro dev, Erus IT Private Limited, Falcon Security Lab, Fast n Clean, fluer-apps.com, Formation App, Free Apps Drive, FrouZa, Galaxy TEAM, GameXpZeroo, GlobalsApps, gndnSoftware, GOMO Apps, GoNext App Developers, Gridinsoft, LLC, handy tools apps, Hello Security, Immune Smart, INCA Internet, infiniteWays007, Islamic Basic Education, Itus Mobile Security, JESKO, jixic, Kolony Cleaner, Koodous Mobile, lempea, LINE, LIONMOBI, Live multi Player Game, Main Source 365 Tech, Mama Studio, MAN Studio, Marsolis Tech, Max Antivirus Lab, Max Mobi Secure, MaxVV, Mob Utilities, Mobile Tools Plus, Mobtari, Mond Corey, M-Secure, MSolutions, MSYSOFT APPS, My Android Antivirus, NCN-NetConsulting, Nepelion Camp, Nisi Jsc, Niulaty, NP Mobile Security, NPC Studios, Omha, Oxic Studio, Pix2Pic Studio, playyourapp, Pro Tool Apps, prote apps, Protector & Security for Mobile, Puce, Radial Apps 2018, RedBeard, Secure Cloud, SecureBrain2, Security and Antivirus for Android solutions, Security Apps Team, Security Defend, SECURITY LAB, Security Systems Lab, SecurityApplock, Sept Max, ShieldApps, SjaellSoft, SkyMobileTeam, Smart Battery Solution & Creative Screen Lock, smarteasyapps, Software Center, Soft War, stmdefender, Systweak Software, TAIGA SYSTEM, Tokyo Tokyo, Tools dev, tools for android, Utilitarian Tools, Vainfotech, VHSTUDIO, Vikrant Waghmode, Virinchi Software, Virtues Media & Application, VSAR, Wingle Apps, Xtechnoz Apps, XZ Game, Z Team Pro.*

We consider those apps to be risky, that is to say, ineffective or unreliable. In some cases the apps are simply buggy, e.g. because they have poorly implemented a third-party engine. Others detect only a handful of very old Android malware samples, and allow any apps that contain certain strings, making them likely to pass some quick checks and thus be accepted by the app stores.

A number of the above apps have in the meantime already been detected either as Trojans, dubious/fake AVs, or at least as “potentially unwanted applications” (PUA) by several reputable mobile security apps. It is to be expected that Google will remove most of them from the Google Play Store in the coming months (and hopefully enhance their verification checks, thus blocking other such apps from the store). We would recommend the vendors concerned to remove their apps from the store until they can provide genuine and reliable protection.

The antimalware apps of the following 32 vendors have in the last two months been removed from the Play Store: **antisecurity.inc, AppLocker Cleaner Booster, AppsNewLook, AVC Security, Bastiv, Big Fun Free Apps, Birina Industries, Cooler Technologies, Document Viewer 2019, Erus IT, GearMedia, Himlamo, koala security studio, LA Antivirus Lab, Mobile Antivirus Lab, Mobile Tools, NCK Corp, Ocean Developers, PICOO Design, Protection & Security for Mobile Lab, Rivalab, Secure Performance Dev, Smart bapp, Taobao, Top Maxi Group, TrustPort, Vasa Pvt, Vasonomics, Vitekco, wallpaperdus, Weather Radar Forecast, and zeeworkers.**

Most of the above apps, as well as the risky apps already mentioned, appear to have been developed either by amateur programmers or by software manufacturers that are not focused on the security business. Examples of the latter category are developers who make all kinds of apps, are in the advertisement/monetization business, or just want to have an Android protection app in their portfolio for publicity reasons. 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 tries² to purge from the Play Store all apps which lack a privacy policy, which helps 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.

² <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 2,000 most common Android malware threats of 2018. Manually testing 250 security products against 2,000 malicious apps is not practicable. Because of this, 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 in January 2019, mostly on Samsung Galaxy S9 devices running Android 8.0 ("Oreo"). As some security apps did not work properly on Android 8.0, those apps were tested on Nexus 5 devices running Android 6.0.1 instead (see page 17 for details). 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 offered to activate additional 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 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 antivirus application detected and blocked the malicious sample, the sample was considered “detected” and the test case was concluded.

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

When calculating the protection score for each product, we did not consider at which stage a malware sample was blocked, i.e. whether it was blocked on download, on installation or on execution. The only factor 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 apps as malicious. Several low-quality apps detected as malware a number of the 100 clean and popular apps from the Google Play Store.

Test Cases

For this test, the 2,000 most common Android malware threats of 2018 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	250
Number of tested malicious APKs	2000
Number of tested clean APKs	100

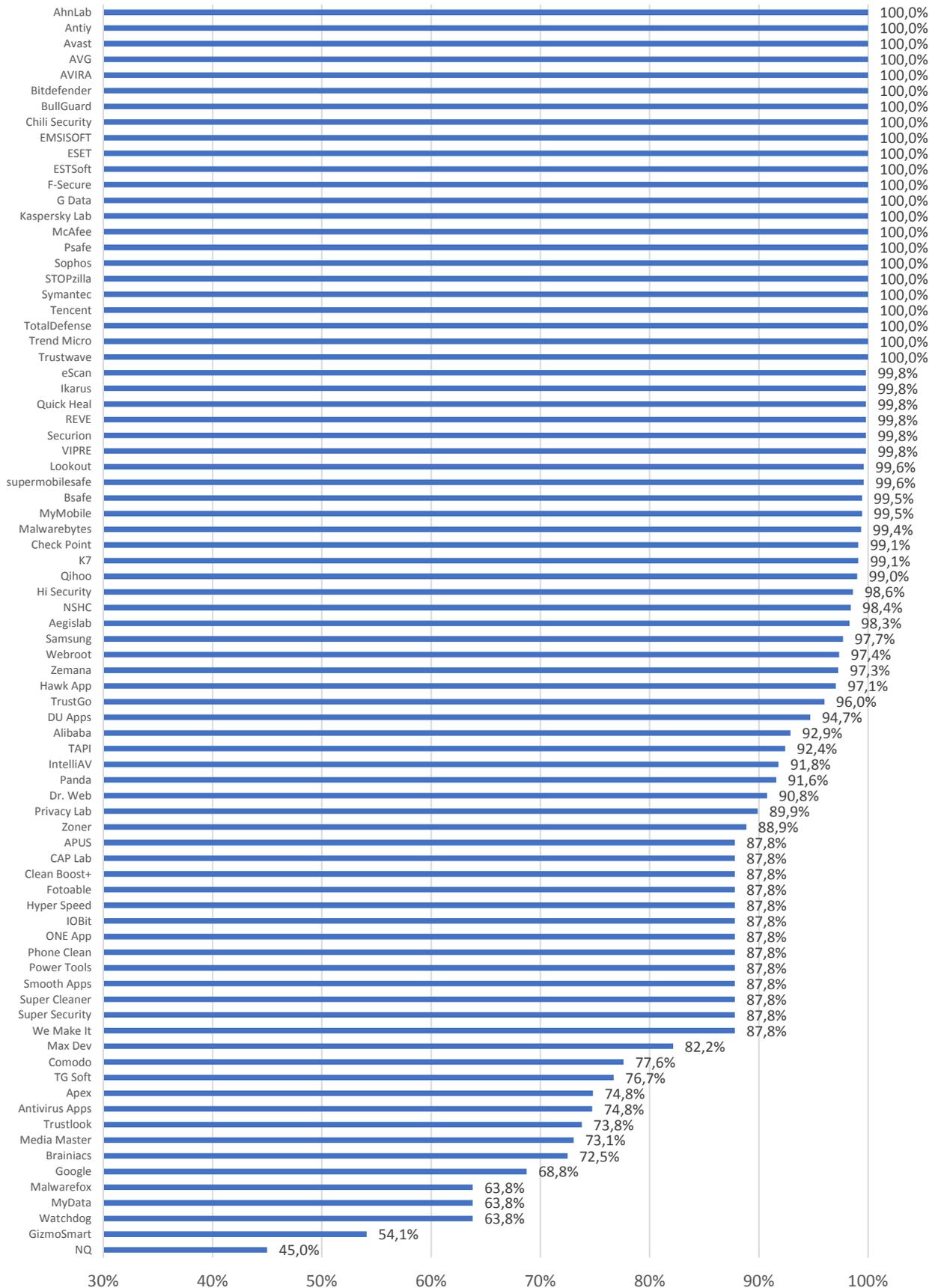
In total, over 500,000 test runs were performed for this report.

Test Results

Vendor	%
AhnLab	100%
Antiy	
Avast	
AVG	
AVIRA	
Bitdefender	
BullGuard	
Chili Security	
Emsisoft	
ESET	
ESTSoft	
F-Secure	
G Data	
Kaspersky Lab	
McAfee	
PSafe	
Sophos	
STOPzilla	
Symantec	
Tencent	
Total Defense	
Trend Micro	
Trustwave	
eScan	99.8%
Ikarus	
Quick Heal	
REVE	
Securion	
VIPRE	
Lookout	99.6%
Supermobilesafe	99.5%
BSafe	
MyMobile	99.4%
Malwarebytes	99.1%
CheckPoint	
K7	99.0%
Qihoo 360	98.6%
Hi Security	98.4%
NSHC	98.3%
AegisLab	97.7%
Samsung	97.4%
Webroot	97.3%
Zemana	97.1%
Hawk App	

Vendor	%
TrustGo	96.0%
DU Apps	94.7%
Alibaba	92.9%
Tapi	92.4%
IntelliAV	91.8%
Panda	91.6%
Dr. Web	90.8%
Privacy Lab	89.9%
Zoner	88.9%
APUS	87.8%
CAP Lab	
Clean Boost+	
Fotoable	
Hyper Speed	
IOBit	
ONE App	
Phone Clean	
Power Tools	
Smooth Apps	
Super Cleaner	
Super Security	
We Make It Appen	82.2%
Max Dev	77.6%
Comodo	76,7%
TG Soft	74.8%
Antivirus Apps	
Apex	73,8%
Trustlook	73.1%
Media Master	72.5%
Brainiacs	68.8%
Google	63.8%
Malwarefox	
MyData	54.1%
Watchdog	45.0%
GizmoSmart	
NQ	

The table above shows the protection rates reached by the 80 products that blocked over 30% of samples. We consider AV apps that block less than 30% of common Android threats (listed on page 5) to be ineffective/unsafe.

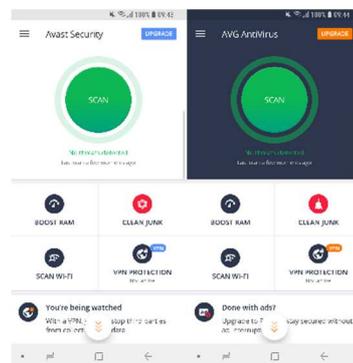


Anti-malware apps detecting under 30% of the 2,000 malicious Android apps are not listed in the chart above – partly for display reasons, but also because we consider them ineffective/unsafe.

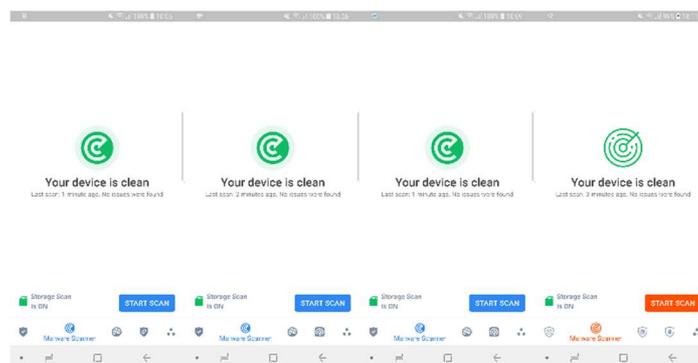
Notes

Some products make use of other vendors’ engines (see examples below). While some score the same as the engine vendor’s own product, some do not. According to the licensing developers, this may be caused by several factors, such as different internal settings used by the third-party apps, the use of older engines or different secondary engines, engine implementation and bugs.

- The apps made by **APUS Group, Asuizksidev, Bit Inception, CAP Lab, Clean Boost+ Studio, Fotoable, Hyper Speed, IOBit, LBE, ONE App, Phone Clean Apps, Power Tools Apps, Smooth Apps Studio Super Cleaner Studio, Super Security Studio, We Make It Appen** use the **Antiy** OpenAVL scan engine.
- **Max Dev Labs** uses the **Tencent** scan engine.
- **Hi Security** uses the **McAfee** scan engine.
- **Brainiacs, BSafe Labs** and **MyMobile Security** use the **Ikarus** scan engine.
- **AVG** and **PSafe** use the **Avast** engine. Since AVG and Avast are owned by the same company, the look-and-feel of their mobile apps are also very similar:



- **Chili Security, Emsisoft, eScan, REVE, STOPzilla, Total Defense** and **VIPRE** use an engine made by **Bitdefender**. The Chili Security, Emsisoft and Total Defense apps are basically identical to the Bitdefender mobile product – see screenshots below:

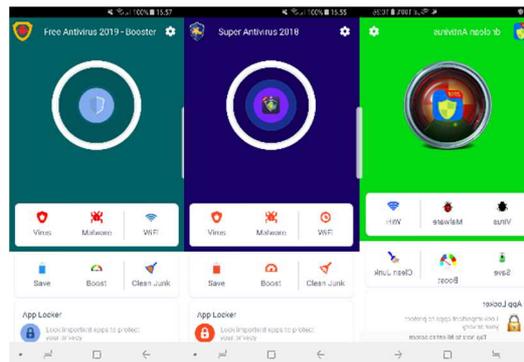


- **MalwareFox, MyData, Watchdog Development** use the scan engine of **Zemana**. Their Apps also look very similar.



During our test, we found that quite a few apps seem to be closely related variants of the same thing, or use a common “AV app template”. In some cases, only the name, logo and colour scheme are different. Examples are shown below:

- **Best HD Wallpapers APPS, Booster studio, and Media Master MD**



- **Asuizksidev, Bit Inception, Brainiacs, My Android Antivirus, Pro Tool Apps, Sept Max, and We Make It Appen**



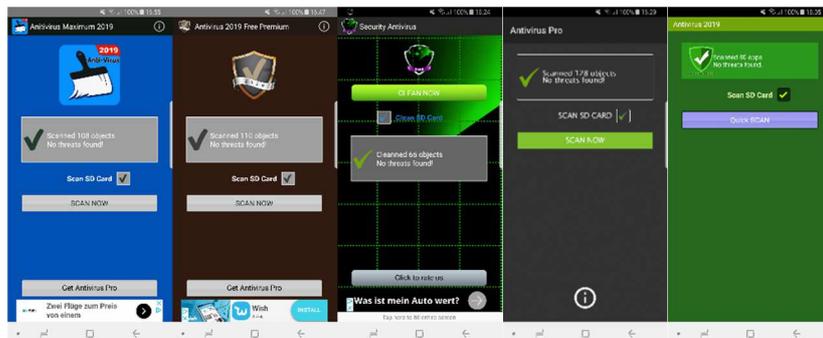
- Amigos Key, Bulletproof AV, Cloud 7 Services, Main Source 365, Mobile Tools Plus, and ShieldApps



- Big Fun Free Apps, and Xtechnoz Apps



- Amantechnoapps, fluer-apps, Kolony Cleaner, NCN-NetConsulting, and Vainfotech



- AZ Super Tools, and DreamBig Studios



Risky Security Apps

As mentioned in the Tested Products section, some apps were not included in the results table, because we consider them risky. About half of those apps were excluded because of their low malware detection capabilities. The other half blocked many of the malicious samples used in the test, but should in our opinion still be considered risky; in the section below, we explain why we came to this conclusion.

When opening the package files of any of those apps, one can find a suspicious text file in the “assets” subfolder named “whiteList.json”. The following figure shows some of the content of this file:

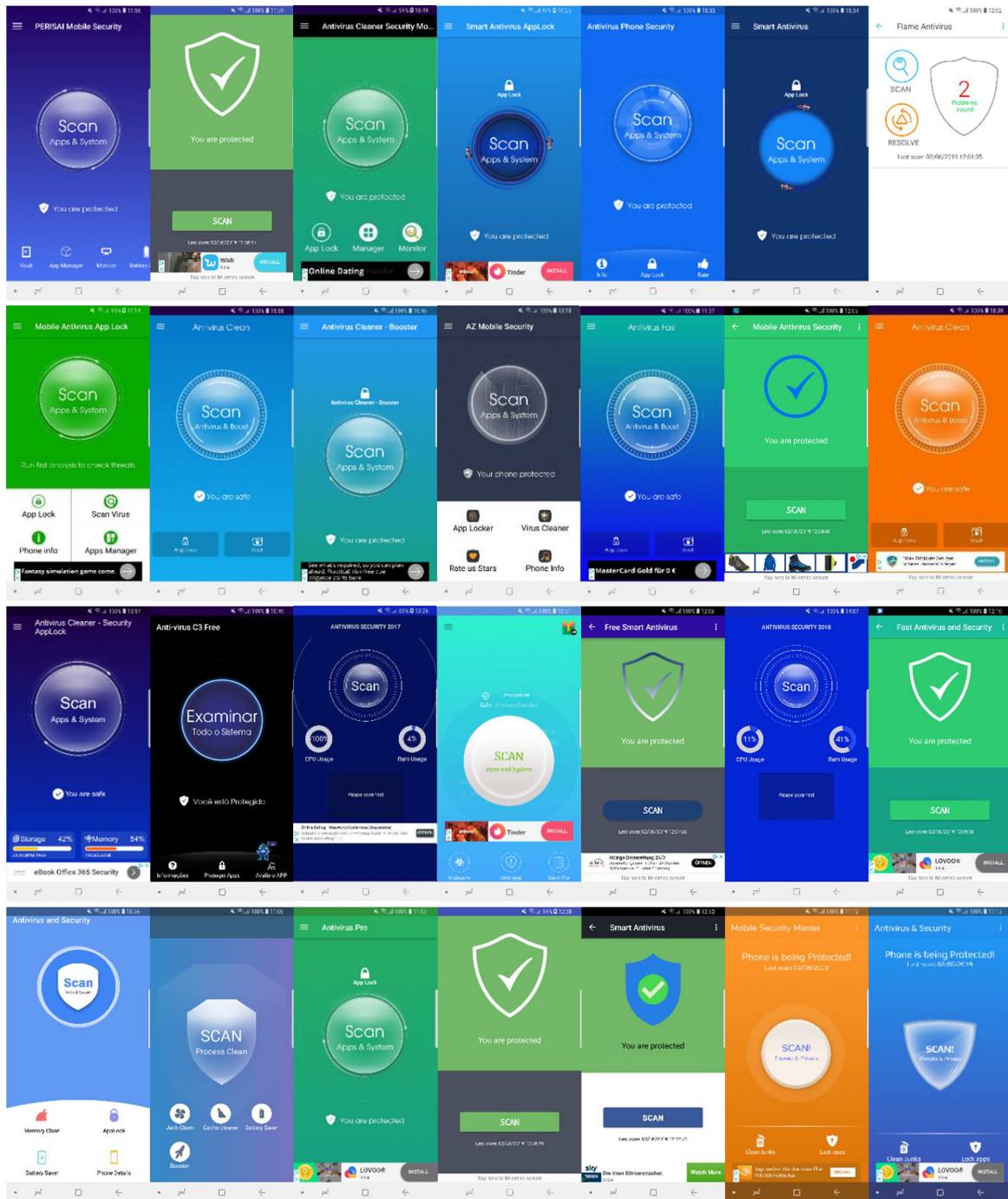
```
{
  "data":
  [
    {
      "packageName": "com.google.android.*"
    },
    {
      "packageName": "com.adobe.*"
    },
    {
      "packageName": "com.facebook.*"
    },
    {
      "packageName": "com.instagram.*"
    },
    {
      "packageName": "com.twitter.*"
    },
    {
      "packageName": "com.whatsapp"
    },
    [...]
  ]
}
```

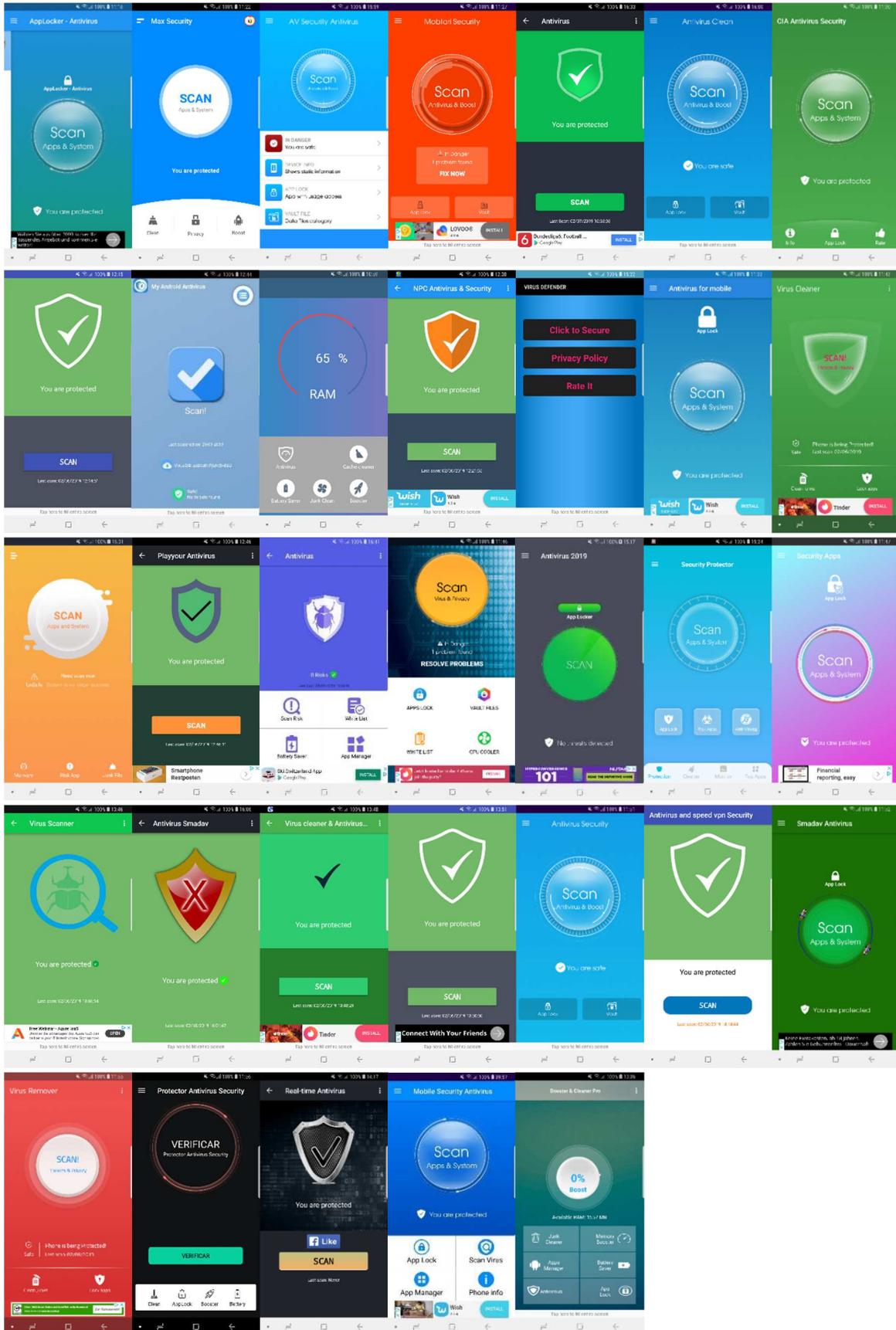
“whiteList.json”

The content of the “whiteList.json” file is consistent with the results we found during our false-positive tests: all apps whose package name match this white-list are considered “trusted applications” by these “AV apps”. For example, the whitelisted package name “com.adobe.*”, matches all packages, whose names start with “com.adobe.”. While this entry means that all genuine apps made by Adobe (such as the Acrobat Reader app) will be regarded as safe, this mechanism also allows any malicious app to bypass the security scan, simply by using “com.adobe.*” as its package name.

Apart from the apps on their respective whitelists, the risky “AV apps” block almost all other apps, regardless of whether they were installed from the official Google Play Store or not. Some of them do not even bother to add their own packages to their whitelists, causing them to report their own app. If using such an AV app, users can never be sure if any of the other apps on their device are actually malicious, because of the AV app’s “block unless whitelisted” policy. Therefore, we do not consider the protection capabilities of these apps to be appropriate.

In addition to using the same “detection” mechanisms, the user interfaces of these apps look very similar as well. Often only differing in colour, the apps in this category mainly use one of just a few different layouts:





We consider the above apps made by the following 61 developers to be risky: **1Machine System Sdn Bhd, actionappsgamesstudio, Antivirus Mobile Lab, appflozen, AppLocker Cleaner Booster, AppsNewLook, appsshow, AS team security phone Lab, AVC Security Joint Stock Company, Ayogames, azemoji studio, bESapp, Best Battery Apps, brouno, Caltonfuny Antivirus Phone, Chromia, Core Antivirus Lab, CPCORP TEAM, CreativeStudioApps, electro dev, Fast n Clean, FrouZa, GameXpZeroo, GlobalsApps, handy tools apps, jixic, lempea, MAN Studio, Marsolis Tech, MaxVV, Mobile Antivirus Lab, Mobtari, Mond Corey, Mondev44, MSolutions, MSYSOFT APPS, My Android Antivirus, Niulaty, NPC Studios, Ocean Developers, Omha, Oxic Studio, Pix2Pic Studio, playyourapp, prote apps, Protector & Security for Mobile, Radial Apps 2018, Security and Antivirus for Android solutions, Security Apps Team, SecurityApplock, Smart bapp, Smart Battery Solution & Creative Screen Lock, stmdefender, Tokyo Tokyo, Tools dev, tools for android, Utilitarian Tools, Virtues Media & Applications, Wingle Apps, XZ Game, and zeeworkers.**

Real-Time Protection Feature on Android 8

Starting with version 8 (“Oreo”), Android enforces stricter limits on apps that run in the background. According to the official change logs, this was implemented to prevent excessive usage of device resources, such as RAM.

The update also made changes that require apps designed for Android Oreo to change the way they react to system events sent by the operating system (“implicit Broadcasts”)³. This change also affects the real-time protection feature of Android AV apps, since they rely on receiving one of these system events. AV apps use the “Package Added” Broadcast to check and scan newly installed apps.

Some developers of AV apps (including a few “bigger” developers) seem to have missed this change. This causes the real-time protection feature of their apps to miss newly installed apps, rendering the feature useless. The faulty behaviour can be observed in the Android log tool logcat:

```
W BroadcastQueue: Background execution not allowed: receiving Intent {
act=android.intent.action.PACKAGE_ADDED [...]}
```

The following developers did not migrate their app to Android Oreo properly: AZ Tools, CHOMAR, Defenx, GOMO Apps, IObit, eScan, PSafe, REVE Antivirus, supermobilesafe, Systweak, TG Soft, Trustlook, Trustwave, Vainfotech, VHSTUDIO, Z Team Pro.

Initially (in January and February), the **Qihoo 360** app also contained this bug. At the time of publishing this report (in March) however, they have already fixed the problem.

The bug does not affect the protection capabilities of the on-demand scans of these apps. Since our test mostly focuses on real-time detections, however, we decided to test these apps on Android 6 instead.

³ <https://developer.android.com/about/versions/oreo/background>

Conclusion

Some of the Android security products in our test blocked so few of the malware samples– in some cases literally none – that they cannot reasonably be described as anti-malware apps. Compared to last year, we found even more apps using only black/whitelists as a detection mechanism. In fact, even though we tested 46 additional apps this year, the number of apps which we consider “usable” has stayed the same. 55% of the tested apps offered insufficient malware protection. Furthermore, we also found 16 apps that have not been migrated to Android 8 properly, decreasing their protection capabilities on newer Android versions.

23 of the products we tested detected 100% of the malware samples; considering that the most common malicious Android apps of 2018 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. Most of the 250 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 scam. A recent “last updated” date also does not seem to be a good quality indicator, as many low-scoring apps had relatively recent updates.

Because of this, we recommend using only apps of well-known, verified and reputable vendors. 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 a 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/testmethod/mobile-security-reviews/>

Copyright and Disclaimer

This publication is Copyright © 2019 by AV-Comparatives®. Any use of the results, etc. in whole or in part, is ONLY permitted after the explicit written agreement of the management board of AV-Comparatives prior to any publication. AV-Comparatives and its testers cannot be held liable for any damage or loss, which might occur as result of, or in connection with, the use of the information provided in this paper. We take every possible care to ensure the correctness of the basic data, but a liability for the correctness of the test results cannot be taken by any representative of AV-Comparatives. We do not give any guarantee of the correctness, completeness, or suitability for a specific purpose of any of the information/content provided at any given time. No one else involved in creating, producing or delivering test results shall be liable for any indirect, special or consequential damage, or loss of profits, arising out of, or related to, the use or inability to use, the services provided by the website, test documents or any related data.

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

AV-Comparatives
(March 2019)