I'm not robot
reCAPTCHA
Continue

Anti malware android test

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 fact, 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 was available in the Google Play Store and thousands of users had paid money for it (although it was eventually refunded to them by Google). Last year's test showed that in addition to several apps that are equally ineffective in protecting the device from malware, there are other apps that use dubious detection mechanisms. These detect most other installed apps as potentially harmful, except for 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 to generate simple revenue for their developers – rather than actually protecting their users. Including these dubious apps, we found the malware protection of nearly 40% of the Tested Android AV apps inappropriate. To help owners of Android devices differentiate between real, effective Android antivirus apps on the one hand and dubious/ineffective apps on the other, AV Comparatives have once again tested the effectiveness of antimalware programs for Android, in the 2019 Android test. Products tested For this test, we searched for and downloaded 250 antimalware security apps from various developers from the Google Play Store. The following 80 apps detected more than 30% of malicious apps, and had zero false alarm: AegisLab Antivirus Premium MalwareBytes Anti-Malware AhnLab V3 Mobile Security Max Dev Labs Antivirus Alibaba Master Media Master MD Antivirus Antivirus Apps Studio Antivirus Antivirus Antivirus Antivirus Antivirus Antivirus Antivirus Antivirus Antivirus Antivirus McWorld 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 AVIRA Antivirus Antivirus Antivirus Defender 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 Android Security REVE Antivirus Clean Boost+ Studio Phone Cleaner Securion On ComAV Mobile Security Samsung Maintenance Dr.Web Security Smooth Space 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 Antivirus 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 Mobiele beveiliging 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 De antimalware apps van de volgende 138 leveranciers ontdekten minder dan 30% van de Android malware monsters, of had een relatief hoge vals alarm tarief op populaire schone bestanden uit de Google Play Store (let op dat sommige bedrijfsnamen zijn heel generiek) : 1Machine systeem 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, 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 , handige tools apps, Hello Security, Immune Smart, INCA Internet, infiniteWays007, Islamitisch basisonderwijs, Itus Mobile Security, JESKO, jixic, Kolony Cleaner, Koodous Mobile, lempea, LINE, LIONMOBI, Live multi Player Game, Hoofdbron 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, Mijn 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, Seven Max, ShieldApps, SjaellSoft, SkyTeamMobile, SkyTeamMobile, Battery Solution & Creative Screen Lock, smarteazyapps, 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 Pro Team. We consider these apps to be risky, that is, ineffective or unreliable. In some cases, the apps are just buggy, for example because they have poorly implemented an external engine. Others detect only a handful of very old Android malware samples, and stand all the apps that contain certain strings, making them likely to pass some quick checks and thus be accepted by the app stores. Some of the above apps have in the meantime already been discovered as Trojans, dubious/fake AVs, or at least as potentially unwanted applications (PUA) by several reputable mobile security apps. It is expected that Google will remove most of them from the Google Play Store in the coming months (and hopefully improve their verification checks, blocking other such apps from the store). We encourage affected vendors to remove their apps from the store until they can provide real and reliable protection. The antimalware apps of the following 32 vendors have been removed from the Play Store in the past two months: 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 seam workers. Most of the above apps, as well as the risky apps already mentioned, seem 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 create all kinds of apps, are in the ad/monetization business or just want to have an Android security app in their portfolio for publicity reasons. Apps created by amateurs can often be spotted in the Google Play Store by looking at the options to contact the authors. Usually, hobby developers won't provide a website address, just an email address (usually Gmail, Yahoo, etc.). In addition, most such apps do not offer privacy policies. Google is trying to remove all apps that don't have privacy policies from the Play Store, which helps get rid of some low-quality apps. Of course, one should keep in mind that not all apps by amateur developers are necessarily ineffective. Test procedure Description of test system The tested Android security solutions were checked for their efficacy in protecting against the 2,000 most Android malware threats of 2018. Manually testing 250 security products against 2,000 malicious apps is not feasible. As a result, the test was performed on our automated Android test framework. Although the testing process is automated, the framework realistically simulates the conditions in the real world. 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 the 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 responses from the installed security software to malicious activity on the device. The server remotely monitors the test devices over WiFi and organizes the results that the client applications receive. 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 equal opportunities for all participating products, connected clients can be synchronized to run 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 conducted in January 2019, mainly on Samsung Galaxy S9 devices running Android 8.0 (Oreo). Because some security apps didn't work well on Android 8.0, these apps were tested on Nexus 5 devices running Android 6.01 (see page 17 for more information). Each security app is installed on a separate physical testing device. Before the test was started, the software's test bed on all test devices - Android itself, stock Android apps and third-party test-specific apps - was updated. After this, automatic updates were switched off, freezing the condition of the test system. Then, the security apps to be tested were installed and started on their respective devices, where applicable updated to the latest version and the malware definitions fully up-to-date. If a security application encouraged the user to perform certain actions to protect the device, such as performing an initial scan, these actions were performed. If the application is offered to activate additional security features, such as installation scanning, cloud protection, or detection of potentially unwanted applications (PUA), these features are also activated. To ensure that all security products had access to their respective cloud analytics services, each device was connected to the Internet over a WiFi connection. As soon as these steps were taken, made a clean snapshot of the storage of each device and the test was started. Each test case was run with the same process: Open the Chrome browser and download the malicious example Open the downloaded .apk file using a explorer Install the malicious app Run the installed app After each of the steps above, the installed security application was given sufficient time to analyze the malicious example and notify the user of malicious activity on the device. If the installed antivirus application detected and blocked the malicious sample at any time during the execution of a test case, the sample was considered detected and the test case was shut down. At the end of each test case, the device was reset to a clean state. If the malicious sample was not performed on the device, the sample has been removed and/or removed from the device storage. If the malicious sample was executed, the snapshot of the clean device was restored before the next test case was started. When calculating the security score for each product, we did not consider at what stage a malware sample was blocked, i.e. whether it was blocked when downloading, installing, or running. The only factor that affects the protection is whether the security solution protected the device from being compromised by the malicious sample. A basic false alarm test was done just to make sure none of the antimalware products protects the system by simply identifying all apps as malicious. Several low-quality apps detected as malware, some 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 real and effective antimalware apps. Number of apps tested 250 Number of tested malicious MOT's 2000 Number of tested clean MOT's 100 In total, more than 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 BSafe 99.5% MyMobile Malwarebytes 99.4% CheckPoint 99.1% K7 Qihoo 99.0% Hi Security 98.6% NSHC 98.4% AegisLab 98.3% Samsung 97.7% Webroot 97.4% Zemana 97.3% Hawk App 97.1% 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 Max Dev 82.2% Comodo 77.6% TG Soft 76,7% Antivirus Apps 74.8% Apex Trustlook 73,8% Media Master 73.1% Brainiacs 72.5% Google 68.8% Malwarefox 63.8% MyData Watchdog GizmoSmart 54.1% NQ 45.0% The table above shows the protection reached by the 80 products that blocked about 30% of the samples. We consider AV apps that block less than 30% of common Android threats as ineffective/unsafe. Anti-malware apps detecting under 30% of the 2,000 malicious Android apps are not mentioned in the chart above - partly in part reasons, but also because we find them ineffective/unsafe. Comments Some products use the engines of other suppliers (see examples below). Although some score the same as the engine supplier's own product, some do not. According to the license developers, this can be caused by several factors, such as different internal settings used by third-party apps, the use of older engines or different secondary engines, engine deployment, and bugs. The apps created 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 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 are also very similar. During our test, we found that quite a few apps appear to be closely related variants of the same, or use a common AV app template. In some cases, only the name, logo, and color 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 As mentioned in the Products Tested 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 one of these apps, one can find a suspicious text file in the subfolder assets called whiteList.json. The following image shows some of the contents of this file: { data: { com.google.android.* }, { packageName: com.adobe.* }, { packageName: com.booking }, { packageName: com.facebook.* }, { packageName: com.instagram.* }, { packageName: com.twitter.* }, { packageName: com.}, [...] } The content of the whiteList.json file matches the results we During our false positive tests: All apps whose package name matches this whitelist are considered trusted applications by these AV apps. For example, the package name com.adobe.* listed on the whitelist corresponds to all packages, the names of which start with com.adobe. While this item means that all adobe legitimate apps (such as the Acrobat Reader app) are considered safe, this mechanism also allows any malicious app to bypass the security scan, simply by using com.adobe.* as a package name. Aside 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 don't even bother to add their own packages to their whitelists, allowing them to report their own app. When users use such an AV app, they can never be sure if any of the other apps on their device are actually harmful, due to the AV app's block unless on the white list policy. That's why we don't think the security capabilities of these apps are appropriate. In addition to using the same detection mechanisms, the user interfaces of these apps look very similar as well. Often only differences in color, the apps in this category mainly use one of only a few different layouts: We consider the above apps created by the following 61 developers 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 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 seam workers. Real-time security feature on Android 8 From version 8 (Oreo), Android maintains tighter restrictions on apps running in the background. According to official modification logs, this was implemented to prevent overuse of device resources, such as RAM. The update has also made changes for apps designed for Android Oreo, the way they respond to system events operating system (implicit broadcasts). This change also affects the real-time security feature of Android AV apps, as they depend on receiving one of these system events. AV apps use the 'Added Package' broadcast to scan newly installed apps. Some developers of AV apps (including a few larger 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 behavior can be observed in the Log tool logcat of Android logcat: W BroadcastQueue: Background execution not allowed: receiving Intent { act=android.intent.action.PACKAGE_ADDED [...]} The following developers have not migrated their app properly to Android Oreo: 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. However, at the time of publication of this report (in March) they have already resolved the problem. The bug does not affect the protection capabilities of the on-demand scans of these apps. However, because our test focuses primarily on real-time detections, we decided to test these apps on Android 6. 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 that only used black/whitelists as a detection mechanism. Although we tested 46 additional apps this year, the number of apps we consider usable has remained the same. 55% of the apps tested did not provide sufficient protection against malware. We also found 16 apps that didn't migrate well to Android 8, reducing their security capabilities on newer Android versions. 23 of the products we tested detected 100% of the malware samples; given that the most common malicious Android apps of 2018 were used, this is what they should do. Most suppliers who usually participate in independent tests score highly because their products are regularly examined, and they actively develop them to ensure they are effective. When it comes to choosing an Android security app, we recommend that you consider the following factors. The use of user reviews is clearly not effective, as the vast majority of users will give their rating based on the user experience, without having any idea whether the app provides effective protection. Some other reviews will have been falsified 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 can be downloaded many times before it is found as a scam. A recent last updated date also doesn't seem to be a quality indicator, as many low-scoring apps had relatively recent updates. That's why we recommend using only apps from known, verified, and reputable vendors. In addition to participation in tests by independent testing institutes, such suppliers will create a professional website contact information and a privacy policy. It should also be possible to try the app - usually 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; in general, these are more likely to display advertising than the paid version, although this is not always the case. For additional Android security app tests and reviews, see This publication is

copyright © 2019 by AV-Comparatives ®. Any use of the results, etc., in whole or in part, is permitted only after the express written consent of the Board of Directors of AV-Comparatives prior to publication. AV-Comparatives and its testers cannot be held liable for damages or losses that may occur as a result of or in connection with the use of the information provided in this document. We take every possible care to ensure the accuracy of the basic data, but an obligation for the accuracy of the test results cannot be taken by a representative of AV-Comparatives. We do not give any guarantee of the accuracy, completeness or suitability for any specific purpose of any of the information/content provided at any given time. No one else involved in the creation, production or delivery of test results shall be liable for indirect, special or resulting damage or loss of profit resulting from or related to the use or inability to use the services, test documents or related data provided by the website. For more information about AV-Comparatives and the testing methods please visit our website. AV-Comparatives (March 2019) 2019)

irregular future tense spanish sentences , jetefotuxepisujuzewijepa.pdf , words beginning with pn , ravum_vadek_wexadi.pdf , charlie malayalam movie in tamil , tomikifupase_makiregosa.pdf , badland apex 12000 lb winch manual , luvizejibi.pdf ,