

Independent Tests of Anti-Virus Software



Android Stalkerware Test 2021

LAST REVISION: 4TH MAY 2021

WWW.AV-COMPARATIVES.ORG

Introduction

The term “stalkerware” refers to software that monitors the use of an electronic device such as a computer, tablet or smartphone, without the knowledge or consent of the device’s user. A stalkerware app typically allows the attacker to read the victim’s text/email/instant messenger communications, monitor and record their phone calls, log their keystrokes, and access their GPS location.

One very typical stalkerware usage scenario is a jealous partner¹ who suspects their other half may be having an affair. Stalkerware that is specifically aimed at such scenarios is also known as *Spouseware*². Despite multiple lockdown periods taking place around the globe due to the Covid-19 pandemic in 2020, cybersecurity experts report that the use of stalkerware has actually increased significantly³.

Even though stalkerware is often marketed as a parental control software, there is one major difference. Genuine parental control apps are designed to be visible and recognisable as such. They display alerts when e.g. blocking pages. Like other apps for the respective platform, they display program icons, can be found in lists of installed/running programs, and can be configured from a menu on the device itself. Stalkerware, on the other hand, does its best to remain well hidden on the victim’s device. Wherever possible, it avoids showing program icons, does not display notifications, and uses innocent-sounding names for any components or processes that it cannot hide. After the initial configuration, it may not even be possible to open the app on the target device to modify its settings.

Installing stalkerware usually requires physical access to the device, but is generally quick and easy to install. Stalkerware developers usually recommend switching off any third-party antivirus apps or built-in protection measures such as Google Play Protect. They may also provide instructions for whitelisting the stalkerware app to avoid future detection by security services.

The application on the device is monitored and controlled from a cloud-based dashboard. This gives the stalker access to the information gathered from the victim’s device, which is stored on the developer’s servers. A further threat to the victim is possible lack of security measures applied to these. There have been reports of such databases being hacked, resulting in a further violation of the victims’ privacy⁴.

It is hard to clearly define the legal status of stalkerware, as it depends on the respective jurisdictions applicable to the victim and the developer. In many countries, the software itself is legal but using it “inappropriately” might be punishable. Stalkerware developers usually state in their terms and conditions that you must not use the software in contradiction of the law of the country or territory that you live in, or install the software on a device owned or used by anybody else without telling them that you are doing so. We would ask what sense there is in telling users that they have to inform the device owner that the program is installed, whilst at the same time taking every conceivable measure to make it undetectable on the device.

¹ https://www.vice.com/en_us/article/bjepkm/how-to-tell-if-partner-is-spying-on-your-phone-stalkerware

² [https://www.schneier.com/academic/paperfiles/Privacy Threats in Intimate Relationships.pdf](https://www.schneier.com/academic/paperfiles/Privacy%20Threats%20in%20Intimate%20Relationships.pdf)

³ <https://www.prnewswire.co.uk/news-releases/use-of-stalkerware-and-spyware-apps-increase-by-93-since-lockdown-began-in-the-uk-817172964.html>

⁴ <https://krebsonsecurity.com/2018/09/for-2nd-time-in-3-years-mobile-spyware-maker-mspy-leaks-millions-of-sensitive-records/>

Following the surge in sales of stalkerware over the past years, countries around the world have started taking action against stalkerware developers. In 2014, for the first time ever a US court ordered a stalkerware app developer to stop production, and pay a fine of USD 500,000⁵.

In addition to the legal steps noted above, Google have taken their own technical measures against stalkerware. Firstly, they have banned⁶ stalkerware apps from the Google Play Store. Secondly, Google Play Protect attempts to recognise stalkerware apps and block them. Finally, in the latest versions of Android, Google have made it more difficult for the setup routines of stalkerware apps to hide the stalkerware automatically.

Whilst Google are to be commended for their efforts, users should be aware that these measures alone cannot prevent stalkerware from being used. The installation files can still be downloaded from the developers' own websites. A stalker could deactivate Google Play Protect before attempting to install them. Additionally, a stalker may well be able to manually hide the spy programs after installation. Even if you have the latest Android version, you shouldn't assume that you can't have stalkerware installed.

The idea for this stalkerware test came out of talks between AV-Comparatives and the Electronic Frontier Foundation (EFF)⁷ in autumn 2019. The subject of stalkerware was also discussed with antivirus vendors at AV-Comparatives' Awards Ceremony in 2020. EFF is a non-profit organisation that works to promote civil liberties, privacy and freedom of expression for Internet users. In November 2019, EFF combined with other organisations to form the *Coalition Against Stalkerware*⁸, which aims to raise awareness of stalkerware and how it can contribute to domestic violence. Its stated goals include enforcing existing privacy legislation, and bringing in new laws where necessary, to tackle the problem using a law-enforcement approach. It is also trying to improve technical measures to prevent the use of stalkerware. These include an agreed definition of stalkerware that will distinguish it from unconcealed, legitimate software such as parental control programs; and co-operation between antivirus vendors that would lead to the sharing of known stalkerware samples.

⁵ <https://www.justice.gov/opa/pr/man-pleads-guilty-selling-stealthgenie-spyware-app-and-ordered-pay-500000-fine>

⁶ <https://www.infosecurity-magazine.com/news/stalkerware-banned-from-google/>

⁷ <https://www.eff.org>

⁸ <https://stopstalkerware.org>

What should you do if you think your device might have stalkerware installed?

If you are worried that you have been a victim of electronic stalking, we suggest that you first of all contact a support group or helpline for victims of stalking in your home country. Borrow a trusted friend's phone or computer to do this. Also, bear in mind that the stalker could be tracking your location; consider switching the phone off or disabling GPS tracking. This report provides technical information about stalkerware programs, but this is only one aspect of a much bigger problem. If you find that stalkerware software has been installed on your phone, it might be best just to turn the device off without taking any other action. If you remove the stalkerware straight away, you will alert whoever is spying on you that they have been found out (a sample message to this effect from a stalkerware console is shown below). Not only will you lose the evidence that could help prove that you have been stalked, but this could lead to serious repercussions from whoever installed this application on your device, with your own security being at stake. In some cases, this could result in a life and death situation.



Antivirus programs help detect stalkerware and inform the user about what the application is able to do, but to decide *when* to remove it, you need a different kind of help. For further information relating specifically to stalkerware, including indicators that it might be installed on your device, please see <https://stopstalkerware.org/get-help/>.

In this report we give simple instructions for detecting stalkerware and informing the user about what this application is able to do. If you do not feel confident enough to try detecting or removing the application yourself, we suggest asking an expert. On the assumption that whoever installed it probably knows you, it might even be a good idea to find an expert outside of your normal circle of friends and family.

First of all, install an antivirus product (if you don't already have one), and start a full system scan with the highest possible detection settings. Repeat this, as the AV product will continuously update its malware signatures and databases. It might be the case that the AV product will not detect the stalkerware when you first scan it, but will later download new detection information that can identify it. Stalkerware developers also try their best to improve and change their products to stay under the radar of antivirus software. If an AV scan does not find anything, but you are still suspicious, it might be a good idea to scan your device using at least two different AV programs made by two unconnected vendors. You could use a free program or trial version for the second program. Different AV vendors may have different criteria for identifying stalkerware. On Android, the process of uninstalling one AV app and installing/configuring another one is straightforward. Ask an expert for help if you need it.

If there is already a security solution on your device, but this has not detected any stalkerware, open the AV's configuration options and check if any programs have been whitelisted. The person who installed the stalkerware could have whitelisted the spy program, i.e. marked it as "clean" in the AV program's settings. In that case, try to remove any programs you do not recognise from the list of exceptions (whitelist) and then start a new scan.

Additional tips

- Make sure your devices (phone, tablet, computer) are protected with a PIN or password that no-one else knows. Ensure they are locked when out of your sight.
- Do not lend your phone to anyone, even for a short time. It might take less than a minute to install a stalkerware program on it.
- Be aware that it is possible to buy mobile phones with stalkerware pre-installed. If you receive a shrink-wrapped smartphone as a gift, it just might contain more than you expected.
- Check whether the option “install from unknown sources” has been turned on for your browser in your Security Settings. Most stalkerware apps are not available on the Google Play Store and so have to be downloaded directly from the developer’s website, hence requiring this permission.
- Check whether Google Play Protect settings have been deactivated. This step is usually recommended during the installation of stalkerware, as Play Protect regularly scans the apps on the device for malicious behaviour.
- Uninstall any apps you do not recognise or do not need.
- Consider whether the performance of your device has changed. Has it slowed down, or does the battery drain more quickly than you would expect? Of course, there might be other explanations for these effects.
- Look out for messages from unknown senders via social media, text, or email. This might be an indication that your device has been compromised.
- If you have found stalkerware on your device and removed it, change the passwords for your email and social media platforms, Internet banking and so on. Use passwords that no-one else can guess. Do not let apps (other than a trusted password manager) save your passwords.
- Users of Apple iPhones should be aware that there is stalkerware for iOS too. If you have an iPhone and are worried about stalkerware, you should ask an independent expert if there are any hidden processes on your phone.

If you are thinking about using stalkerware to spy on someone

We strongly advise you not to do this. There is a very good chance of stalkerware being discovered. Whatever the legal status of the software may be, the act of stalking⁹ someone is a crime in many countries. You could go to prison for it. You might lose your friends, family, health or career over it¹⁰. In short, the person you might hurt most by installing stalkerware is yourself. If you are thinking about being involved in any aspect of someone’s private life without their explicit consent, we strongly discourage you from doing so and suggest you seek professional mental help¹¹.

⁹ <https://en.wikipedia.org/wiki/Stalking> ; <https://en.wikipedia.org/wiki/Cyberstalking>

¹⁰ <https://www.stop-stalking-berlin.de/en/for-people-who-stalk-2/consequences/>

¹¹ https://www.stop-stalking-berlin.de/en/home_en/

Tested Products

We examined ten well-known AV apps for Android. The products, along with their current versions at the respective times of testing (March 2021), are listed below.

Product	Version
Avast Mobile Security	6.37
Avira Antivirus Security	7.5
Bitdefender Mobile Security	3.3
ESET Mobile Security	6.2
F-Secure SAFE Mobile Antivirus	17.9
G Data Mobile Security	27.3
Kaspersky Mobile Security	11.65
Malwarebytes for Android	3.7
NortonLifeLock Norton 360 Mobile Security	5.4
Trend Micro Mobile Security	12.2

Test Procedure

For this report, we selected 20 stalkerware apps for Android. The latest versions available at time of testing (March 2021) were downloaded from the vendor's website, installed, and set up on the target device. We used non-rooted Samsung Galaxy S9 mobile phones, with an active Internet connection. We set up each stalkerware app on a mobile phone, following the step-by-step instructions provided. We always gave whatever permissions were requested by the app, and hid the app icon if given the opportunity. Our aim was to simulate a realistic scenario from a victim's perspective. For every stalkerware program, the full (paid) version of each antivirus app was installed from the Google Play Store and used to run a scan. We checked to see if the AV product detected the stalkerware by showing a warning or detection message on the device's screen. If it did so, we counted it as detected. After testing each stalkerware/AV-app combination, we reset the phone, and went on to the next one.

Test Results

We considered a stalkerware program to have been successfully detected by the AV program if the latter displayed a warning or detection message. We decided not to write the names of the stalkerware used in the test. This was partly so as not to publicise any of these programs, and also to avoid giving stalkers any information about which AV programs will not detect their preferred stalkerware program. Our aim is to encourage vendors to improve their detection of all stalkerware programs, not just the ones used in any particular test. To this end, we do not inform vendors which stalkerware programs we use in our tests, or when we will be running these stalkerware-detection tests. We might use (updated versions of) the same programs in future tests. This will allow us to see if vendors are maintaining/improving their detection rates. The majority of the stalkerware apps used this year were also used in last year's test¹². However, we have used the latest versions of these apps, to check whether vendors that detected them last time have updated their detection mechanisms. Some stalkerware developers have ceased their operations since our last test, so these apps have been replaced with others this year.

¹² https://www.av-comparatives.org/wp-content/uploads/2020/06/avc_stalkerware_2020.pdf

The table below shows the results for of the respective AV products on 20 selected stalkerware apps for Android.

Detection of Stalkerware Apps on Android										
Testcase	Avast	Avira	Bitdefender	ESET	F-Secure	G Data	Kaspersky	Malwarebytes	NortonLifeLock	Trend Micro
Stalkerware 1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Stalkerware 2	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Stalkerware 3	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Stalkerware 4	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Stalkerware 5	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Stalkerware 6	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Stalkerware 7	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Stalkerware 8	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Stalkerware 9	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓
Stalkerware 10	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓
Stalkerware 11	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓
Stalkerware 12	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓
Stalkerware 13	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓
Stalkerware 14	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓
Stalkerware 15	✓	✗	✓	✓	✗	✓	✓	✓	✗	✓
Stalkerware 16	✗	✗	✓	✓	✗	✓	✓	✓	✗	✓
Stalkerware 17	✗	✗	✓	✓	✗	✓	✓	✓	✗	✗
Stalkerware 18	✓	✗	✗	✗	✗	✓	✗	✗	✗	✗
Stalkerware 19	✓	✗	✗	✗	✗	✓	✗	✗	✗	✗
Stalkerware 20	✓	✗	✗	✗	✗	✓	✗	✗	✗	✗
Detection Rate	85%	70%	85%	85%	70%	100%	85%	80%	50%	80%

Key to symbols in table:



Stalkerware detected



Stalkerware not detected

Results

Although only one AV product detected all the stalkerware apps used in this test, it appears that AV vendors have been improving their stalkerware detection in recent times. As we can see, 7 out of 10 products detected between 80% and 100% of the testcases, while two apps scored 70%. The remaining product reached a 50% detection rate, which might be because it is a very well-known brand, and stalkerware developers thus try hard to evade it.

Compared to last year, there have been cases of the latest versions of some stalkerware not being detected by AVs this time. That is to say, the latest version of a few stalkerware apps that were widely detected in 2020 managed to evade detection quite successfully in this round of testing. As with “normal” malware, there is a cat-and-mouse game played between the authors of the stalkerware and the antivirus manufacturers. Each tries to stay one step ahead of the other. The specific nature of commercial stalkerware makes it harder for AV vendors to keep their signatures up to date. To maximise the chances of your AV program detecting stalkerware on your device, please see *What should you do if you think your device might have stalkerware installed?* above.

On Android, the stalkerware is always present in the list of apps in the device settings, but might use a different and not-so-obvious app name, so as not to be recognized immediately. All the stalkerware-related data is stored in a single location on Android devices, and the stalkerware’s capabilities are limited by the Android OS, unless it acquires system permissions to access further data and functionality. This makes it easier for Android AV apps to detect malicious applications, along with their related data, in one go. However, there are also some limitations to the protection capabilities of AV apps on Android.

Stalkerware

In order to avoid complications, some stalkerware developers suggest disabling any security solution built into the operating system (i.e. Google Play Protect on Android), and third-party antivirus programs, prior to the installation. For Android specifically, the option “Install unknown apps” has to be enabled in the Android security settings to properly install a stalkerware app from outside the Google Play store.

Every stalkerware app tested provided a cloud-based dashboard, where data collected from the target system is displayed. Fifteen products out of the twenty we tested let the buyer know which apps, including antivirus, had been installed on the target device. This information could be acquired by either looking at the activity logs or at the list of installed apps. Some stalkerware even notified the user via email that the application had been uninstalled, whereas other stalkerware alerted the user via the respective web interface.

On Android, a few of the more sophisticated stalkerware apps set up a password that would have to be entered in order to revoke the app’s device administration rights, and hence successfully uninstall it. This almost certainly means that the victim will not be able to deactivate the stalkerware even with the help of an AV app. Should you find yourself in this situation, we recommend seeking expert advice on what to do. Again, we suggest that you look at <https://stopstalkerware.org/get-help/>.

In general, it might also be the case that the stalkerware actively interferes with the functionality of the target system or antivirus, e.g. causing very high CPU utilisation or preventing the user from launching the AV program, browsers, and other installed programs.

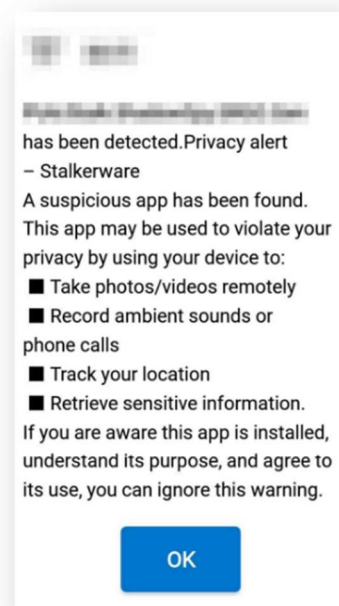
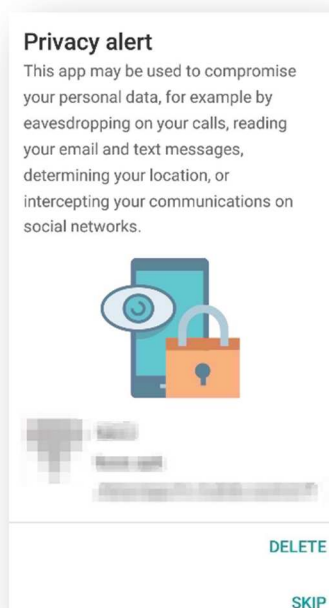
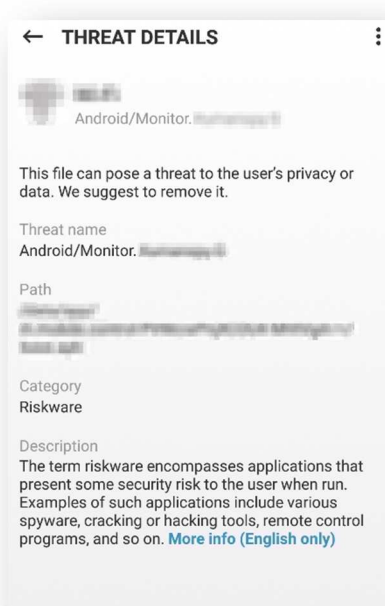
Antivirus

Some Android stalkerware apps acquire device administration rights to obtain more control, and to make the uninstallation process harder. Whilst some products are able to remove stalkerware apps with device admin privileges, others are not. In these cases, it is necessary to remove the device admin rights manually, after which the antivirus will be able to remove the stalkerware app.

Many AV products allow you to change the default scanning options to run more-comprehensive file scans that include e.g. archives and system apps, and detect potentially unwanted applications (PUA) and riskware. Choosing the highest detection settings may help detect stalkerware software, as several AV products detect stalkerware as PUA/riskware rather than malware.

When an antivirus app has detected a stalkerware program, we feel it should provide the victim with appropriate information, warnings and removal options. Ideally, the antivirus should make clear what the stalkerware can do, e.g. monitor phone calls, take pictures, record sounds, and track the phone's location. It should then warn the user that uninstalling the stalkerware could put them in danger, as the stalker will be aware that this has happened. For this reason, the stalkerware should not be uninstalled automatically. Only once the warning has been seen should the antivirus provide removal options.

In general, the detection messages shown by the AV products in this year's test have improved since last year. Some of the products we tested this time provided good descriptions of the threats, explaining that the detected stalkerware might eavesdrop on calls, read emails and text messages, determine the user's location, or intercept communications on social media networks. None of the security products uninstalled the stalkerware automatically. However, some products actively recommended removing it, and provided easy options for doing so, without warning the user of the possible consequences. Some examples of the better alerts from antivirus programs are shown below.



Appendix: TinyCheck tool

A completely different method of detecting stalkerware is TinyCheck¹³. This is a free, open-source network analysis tool, which runs on Linux-based devices such as Raspberry Pi mini-computers. It was only released quite recently, and is still being actively developed. It allows you to capture network traffic from any mobile device such as a mobile phone, and analyse this for stalkerware communications. Compared to antivirus apps, TinyCheck has the advantage that it leaves no traces; nothing needs to be installed on the device which is being investigated. The stalker will not see any additional installed software in the stalkerware dashboard, or in screenshots of the victim's device, making it a more secure way to detect stalkerware. However, the stalker might well be able to track the geolocation of the victim. If they go to a computer repair shop to get help with detecting stalkerware, this could be noticed by the stalker. The stalker might also notice if the phone has been connected to an unusual Wi-Fi network.

Non-experts will probably need some technical help to set up TinyCheck. Again, it might be best to ask someone outside of your circle of friends and acquaintances. Aside from any fees paid for the technical assistance, you may also need to pay for e.g. a Raspberry Pi mini-computer. Once the testing system has been set up and the TinyCheck app is running, you will need to perform some normal activities on your phone, such as calling someone, sending emails and text messages, taking pictures and surfing the web, for 10-20 minutes or so. Be careful not to do anything that would arouse the stalker's suspicion, of course. TinyCheck will indicate if stalkerware has been found. Additionally, the detailed data recorded by can be analysed by an expert adviser for further clues.

To see if TinyCheck can help to uncover stalkerware programs, we conducted a test in April 2021, using the same 20 stalkerware apps as for the antivirus test. We stress that the results of the TinyCheck test should not be compared with those of the antivirus apps. TinyCheck looks only at the stalkerware's communications, whereas antivirus software looks principally at the apps themselves. Only those communications sent during the test period are intercepted by TinyCheck, and these may be cleverly disguised and routed through innocent-looking web addresses to avoid detection. Nonetheless, we suggest that TinyCheck is a very valuable tool in the fight against stalkerware.

In the test, a stalkerware app was installed on the test smartphone, which was then connected to the Wi-Fi network of the Raspberry Pi device running TinyCheck. The same sequence of normal smartphone activities was carried out for each stalkerware app. We then looked at the respective results summary to see if app had been reported as stalkerware. Results are shown in the table below. Please note that these represent only definite detections of stalkerware. We did not perform any further analysis of the data.

Testcase	TinyCheck
Stalkerware 1	✓
Stalkerware 2	✓
Stalkerware 3	✓
Stalkerware 4	✓
Stalkerware 5	✓
Stalkerware 6	✓
Stalkerware 7	✓
Stalkerware 8	✓
Stalkerware 9	✓
Stalkerware 10	✓
Stalkerware 11	✓
Stalkerware 12	✓
Stalkerware 13	✓
Stalkerware 14	✓
Stalkerware 15	✗
Stalkerware 16	✗
Stalkerware 17	✗
Stalkerware 18	✓
Stalkerware 19	✗
Stalkerware 20	✗

Key to symbols in table:

✓ Stalkerware detected

✗ Stalkerware not detected

¹³ <https://github.com/KasperskyLab/TinyCheck>



Copyright and Disclaimer

This publication is Copyright © 2021 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
(May 2021)