Independent Tests of
Anti-Virus Software

Stalkerware Test 2020

LANGUAGE: ENGLISH
LAST REVISION: 10TH JUNE 2020

WWW.AV-COMPARATIVES.ORG

Introduction

What is this report about?

Supposing somebody told you that there could be software on your smartphone[1], tablet or laptop that let someone else monitor your physical location, emails, browsing history, phone calls, and even take pictures with your device's camera. You would probably think that this was illegal malware, right? Or something used by governments to spy on suspected terrorists? Actually, it would be neither of these. Welcome to the twilight world of stalkerware[2].

Stalkerware has been described[3] thus: ***"...these apps have functionality that allows them to invade the privacy of an individual without their consent or knowledge: the application icon can be hidden from the applications menu, while the app continues to run in the background..."***.

On the face of it, stalkerware has a lot in common with totally legal, legitimate, and commendable parental control software. Parental controls allow parents to ensure the safety and wellbeing of their children by monitoring their Internet usage and phone calls, and checking where they are. To a very significant extent, stalkerware does exactly the same.

Parental control software is completely honest and open about its existence. If a child tries to open a web page that their parents do not want them to see, the child will see a block page made by the software vendor, telling them that this site is out of bounds. The setup routines of parental control programs often advise parents to talk to their children about the software and why it is being installed. The child then knows that the parents can monitor the websites they try to access, the phone numbers they call, and so on.

The really big difference between parental control software and stalkerware is that the latter goes out of its way to hide its presence on a device.

On a Windows PC, any user, even without admin rights on the device, can see typical indicators that a parental control program has been installed: program shortcuts, entries in Settings/Control Panel, a System Tray icon, and a clearly named folder in Program Files. Additionally, any process(es) will be visible in Task Manager, and any Windows Service belonging to the product will be appropriately named and described. The same applies to normal Android apps, which add icons to the home screen, and can be configured by opening the app and finding its settings in a menu. With stalkerware, none of this applies, as it is made to be almost invisible.

One very typical stalkerware usage scenario is a jealous partner[4] who suspects their other half may be having an affair. By installing stalkerware[5] on their partner's smartphone, the user can track that person's movement, record phone calls, and monitor emails as well as text messages. Stalkerware that is specifically aimed at such scenarios is also known as *Spouseware*.

[1] https://www.makeuseof.com/tag/what-is-stalkerware/
[2] https://citizenlab.ca/2019/06/the-predator-in-your-pocket-a-multidisciplinary-assessment-of-the-stalkerware-application-industry/
[3] https://securelist.com/beware-of-stalkerware/90264/
[4] https://www.vice.com/en_us/article/bjepkm/how-to-tell-if-partner-is-spying-on-your-phone-stalkerware
[5] https://www.schneier.com/academic/paperfiles/Privacy_Threats_in_Intimate_Relationships.pdf

What is the legal situation regarding stalkerware?

In short, the software itself is legal but using it "incorrectly" might be punishable. Laws against covert surveillance will of course vary from country to country, although surely there are many jurisdictions where it is illegal.

The websites and setup wizards of stalkerware programs typically warn that you must not use the software in contradiction of the law of the country or territory that you live in. They also state that you must not install the software on a device owned or used by anybody else without telling the actual owner 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 invisible on the device.

For this report, we have defined stalkerware as monitoring software that has clearly been designed to be invisible to the device user. We have then made a factual statement as to which antivirus programs detected this software in our test. Readers should note that different AV vendors may have different definitions of what their respective programs should and should not detect. Thus, we run the same test at two different points in time: The first test was performed in November 2019 and a retest followed in May 2020. There may also be legal problems relating to detection of software that can be sold legally in some jurisdictions. For stalkerware that was not detected in November but was detected in May, this was most probably not the case; rather, the vendor simply did not detect it at the time of the first test. If a vendor did not detect the same stalkerware program 6 months after the initial test, it might be due to their detection policies/definitions.

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. 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 or PC, it might initially 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. You will also lose the evidence that could help prove that you have been stalked. Antivirus programs can help to remove stalkerware, 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 this page.

We give simple instructions for detecting/removing stalkerware here. If you do not feel confident enough to do this 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 vendors 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. As this test demonstrates, different AV vendors have different criteria for identifying stalkerware. On Android, the process of uninstalling one AV app and installing/configuring another one is straightforward. On Windows, it is more complicated, and running two antivirus programs at the same time is not recommended. Ask an expert for help if you need it.

If there is already a security solution on your device, but you still observe suspicious activities that are not detected by it, open the AV's configuration options and check what programs have been whitelisted. The person who installed the stalkerware could have marked (whitelisted) the spy program 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.

General 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.
- Use an antivirus program on all your devices, ideally one that lets you password-protect the settings. Check its whitelist, to see if an unknown program has been designated as harmless.
- 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.
- 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 is always a good idea, but might also 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.

Test Procedure

We tested and evaluated the ability of 10 antivirus (AV) products to detect stalkerware on Android and Windows systems. The first iteration of tests was performed in November 2019. A second round of tests followed in May 2020, in which we verified that all the AV vendors detected most of the stalkerware testcases at that time. If a product fails to detect a testcase in the first test and fails to detect it even six months later in the second test, this could be due to the vendor's detection policy or definition of threats.

Lab Setup

The test of Android products was performed on a non-rooted Samsung Galaxy S9, running Android 8.0. For Windows, the test was performed under Windows 10 Pro 64-bit. Both systems had an active Internet connection.

Methodology

For each stalkerware program, a scan was performed with the respective antivirus product. We checked to see if the AV product detected the stalkerware by showing a warning or detection message on the device's screen or blocked the stalkerware. If it did so, we counted it as detected.

Tested Products

We examined 10 well-known AV apps for Android, and 10 common AV programs for Windows. The products were chosen together with the Electronic Frontier Foundation (EFF)[6], based on popularity in the USA. The products, along with their current versions at the respective times of testing (November 2019 and May 2020), are listed below.

	Android Products			Windows Products		
Vendor	Product	Version November 2019	Version May 2020	Product	Version November 2019	Version May 2020
Avast	Mobile Security	6.23	6.27	Free Antivirus	19.8	20.3
Avira	Antivirus Security	6.1	6.5	Internet Security Suite	15.0	15.0
Bitdefender	Mobile Security	3.3	3.3	Internet Security	24.0	24.0
ESET	Mobile Security	5.2	5.4	Internet Security	13.0	13.1
Kaspersky	Internet Security	11.32	11.46	Internet Security	20.0	20.0
Lookout	Mobile Security	10.28	10.32			
McAfee	Mobile Security	5.3	5.6	Total Security	22.5	23.1
Microsoft				Windows Defender	4.18	4.18
NortonLifeLock	Mobile Security	4.7	4.8	Norton 360 Deluxe	22.19	22.20
Panda	Dome	3.5	3.5	Free Antivirus	19.00	20.00
Trend Micro	Mobile Security	11.0	11.3	Internet Security	16.0	16.0

Testcases

For this report, we selected 20 stalkerware apps for Android and 10 stalkerware programs for Windows. The latest versions available in November 2019 were downloaded from the vendor's website, installed, and set up on the test systems for both test periods.

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, or blocked/removed the stalkerware.

We considered whether to write the names of the stalkerware used in the test. We decided to not do so, in order not to promote the stalkerware programs, or give hints about which AV products might not detect which stalkerware.

Symbols: ✔ Stalkerware detected ✖ Stalkerware not detected

Each pair of symbols represents whether the stalkerware was detected in November 2019 (left) and May 2020 (right). The respective detection rates for the two test dates are shown at the bottom of the table.

[6] https://www.eff.org/

The table below shows the results for November 2019 and May 2020 of the respective AV products on 20 selected stalkerware apps for Android.

Protection against Stalkerware Apps on Android										
Testcase	**Avast**	**Avira**	**Bitdefender**	**ESET**	**Kaspersky**	**Lookout**	**McAfee**	**Norton**	**Panda**	**Trend Micro**
	2019 | 2020	2019 | 2020	2019 | 2020	2019 | 2020	2019 | 2020	2019 | 2020	2019 | 2020	2019 | 2020	2019 | 2020	2019 | 2020
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 November 2019	70%	70%	45%	70%	95%	65%	55%	75%	30%	90%
Detection Rate May 2020	75%	85%	75%	90%	95%	70%	80%	80%	35%	95%

The table below shows the results for November 2019 and May 2020 of the respective AV products on 10 selected stalkerware programs for Windows.

	Protection against Stalkerware Programs on Windows									
Testcase	**Avast**	**Avira**	**Bitdefender**	**ESET**	**Kaspersky**	**McAfee**	**Microsoft**	**Norton**	**Panda**	**Trend Micro**
	2019 | 2020	2019 | 2020	2019 | 2020	2019 | 2020	2019 | 2020	2019 | 2020	2019 | 2020	2019 | 2020	2019 | 2020	2019 | 2020
Stalkerware A	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓
Stalkerware B	✓ ✓	✓ ✓	✓ ✓	✗ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓
Stalkerware C	✓ ✓	✓ ✓	✓ ✓	✗ ✓	✗ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓
Stalkerware D	✓ ✓	✗ ✗	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✗ ✓	✓ ✓	✓ ✓	✓ ✓
Stalkerware E	✓ ✓	✗ ✓	✓ ✓	✗ ✓	✗ ✓	✓ ✓	✓ ✓	✗ ✓	✓ ✓	✓ ✓
Stalkerware F	✗ ✓	✗ ✓	✗ ✓	✓ ✓	✓ ✓	✗ ✓	✗ ✓	✗ ✓	✗ ✓	✗ ✓
Stalkerware G	✗ ✓	✗ ✓	✗ ✓	✗ ✓	✗ ✓	✗ ✓	✗ ✓	✓ ✓	✗ ✓	✗ ✓
Stalkerware H	✗ ✓	✗ ✓	✗ ✓	✗ ✓	✗ ✓	✗ ✓	✗ ✗	✓ ✓	✗ ✓	✓ ✓
Stalkerware I	✗ ✗	✗ ✗	✗ ✓	✗ ✓	✗ ✓	✗ ✗	✗ ✗	✓ ✓	✗ ✗	✓ ✓
Stalkerware J	✗ ✗	✗ ✗	✗ ✓	✗ ✓	✗ ✓	✗ ✓	✗ ✗	✗ ✓	✗ ✗	✗ ✗
Detection Rate November 2019	50%	30%	50%	30%	40%	50%	40%	70%	50%	70%
Detection Rate May 2020	80%	70%	100%	100%	100%	90%	70%	100%	80%	90%

Discussion

Results

The detection rates for the Android products in November ranged from 30% to 95%, with two products detecting less than 50% of the testcases. On Windows, the overall detection rates in November were poor relative to Android; the highest detection rate was only 70%, and only two products reached this level. Six months later in May, most products – for both Android and Windows – had improved their detection rates. On Android, 9 out of 10 products detected between 75% and 95% of the testcases. On Windows, all products had improved their detection rates to at least 70%, with four programs reaching 100%.

From the results, we clearly see that AV products are reactive with stalkerware, meaning that they detected most testcases at a later time. 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.

Operating System Differences

In comparison to its Android counterparts, stalkerware on Windows is more sophisticated in terms of visibility, access rights, and file distribution on the hard drive. Many of the tested Windows stalkerware programs managed to hide their presence very effectively. There are no desktop shortcuts or Start Menu entries, and processes/services are disguised with innocent-looking names such as "Sync service". Furthermore, the installed stalkerware can place its files in many different locations on the hard drive.

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 (*/data/app/<app-package-name>/*), 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 and remove 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 vendors suggest disabling any security solution built into the operating system (i.e. Microsoft Defender on Windows, 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. Some Android stalkerware detected if an AV was installed on the target device and alerted the user via the respective web interface. With a similar aim, some Windows stalkerware recommended the user to whitelist it in the AV program's settings.

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.

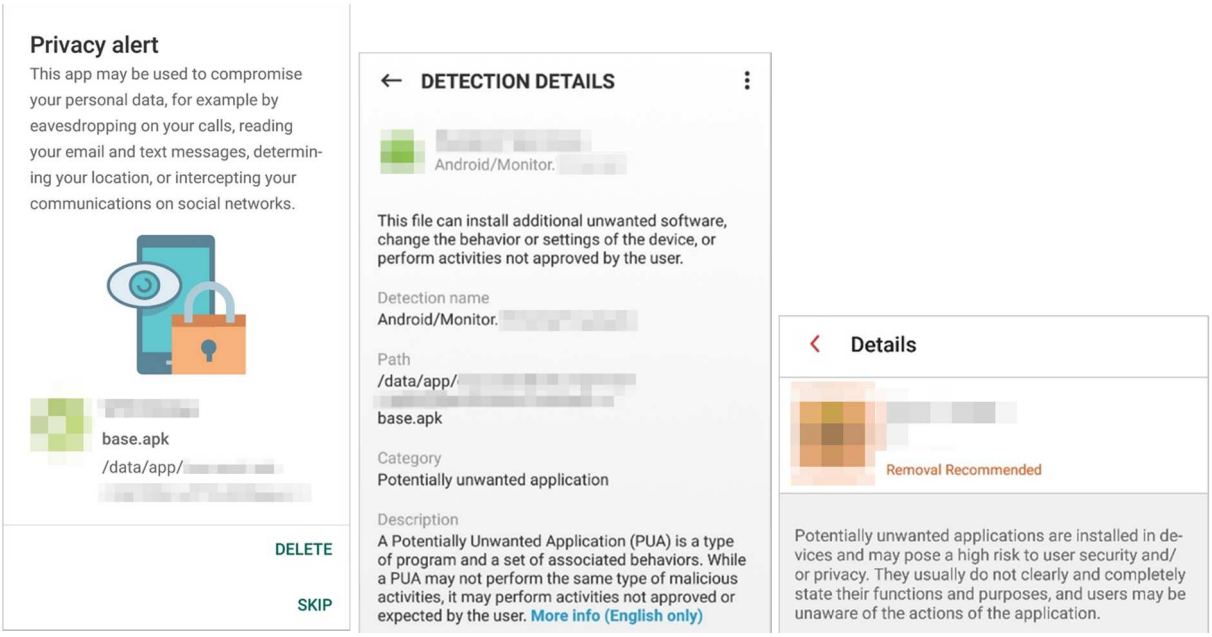
In general, it might also be the case that the stalkerware actively interferes with the functionality of the target system or antivirus, e.g. causing very high CPU utilisation or preventing the user from launching the AV program, browsers, and other installed programs.

Antivirus

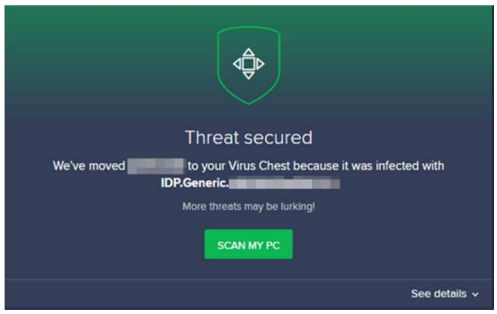
Some Android stalkerware apps acquire device administration rights in order to obtain more control and to prevent themselves from being uninstalled easily. Some products had difficulties with such apps and were not able to remove them, despite successfully detecting them.

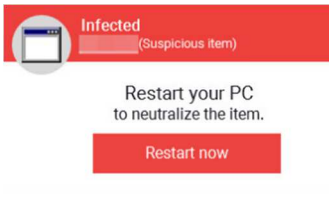
Many AV products allow you to change the default scanning options to run more-comprehensive file scans that include e.g. archives and system apps, and detect potentially unwanted applications (PUA) and riskware. Choosing the highest detection settings may help detecting stalkerware software, as several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

Some of the Android AV products we tested gave exemplary, descriptive warnings, 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. Some other products also had good detection messages, which explained that the detected apps posed a security/privacy risk and might take actions or install other software without the user's knowledge. In these cases, it was necessary to click the "Details" button to get this information.

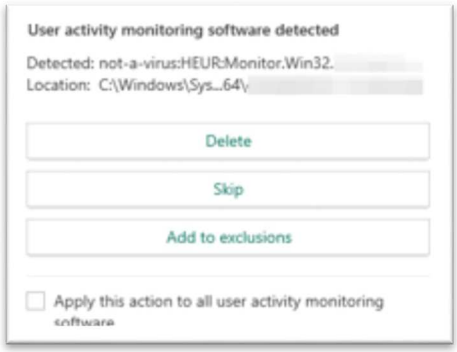


By contrast, many Windows AV products showed only generic detection messages that did not provide meaningful details or further clarifications.





Some Windows antivirus programs did provide more helpful warnings, such as *User activity monitoring software detected* or *legitimate software that can be used by criminals*. However, in some of these cases, the detection included the term *not-a-virus* in its name, and even provided the option *Add to exclusions*, making it easy to whitelist the program. This might give the victim the false impression that the detected program does not pose a serious risk. It would also make it easy for the stalker to whitelist the stalkerware after installing it.



In our opinion, many of the tested AV products, especially those for Windows, do not provide enough information about the stalkerware programs they detect. We would welcome clear and informative messages when stalkerware is detected, which clarify the nature of the specific threat. As mentioned earlier, removing detected stalkerware will almost certainly alert the stalker to the fact that they have been found out, which may bring its own problems. We therefore suggest that automatic deletion of stalkerware on detection is not appropriate.

Continuing the fight against stalkerware

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.

[7] https://www.eff.org
[8] http://stopstalkerware.org

Copyright and Disclaimer

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

AV-Comparatives
(June 2020)