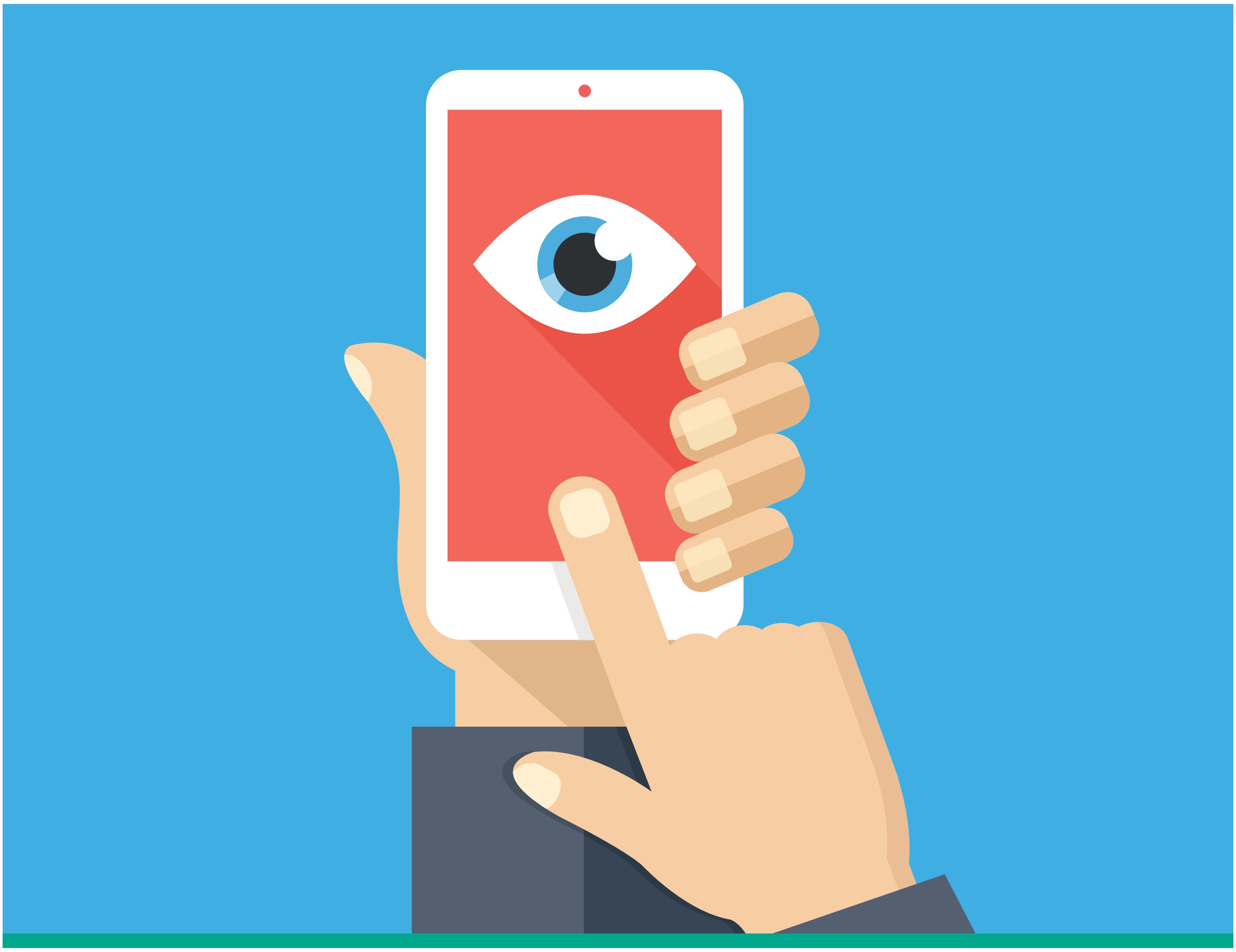


The State of **Stalkerware** in 2020

COALITION AGAINST STALKERWARE

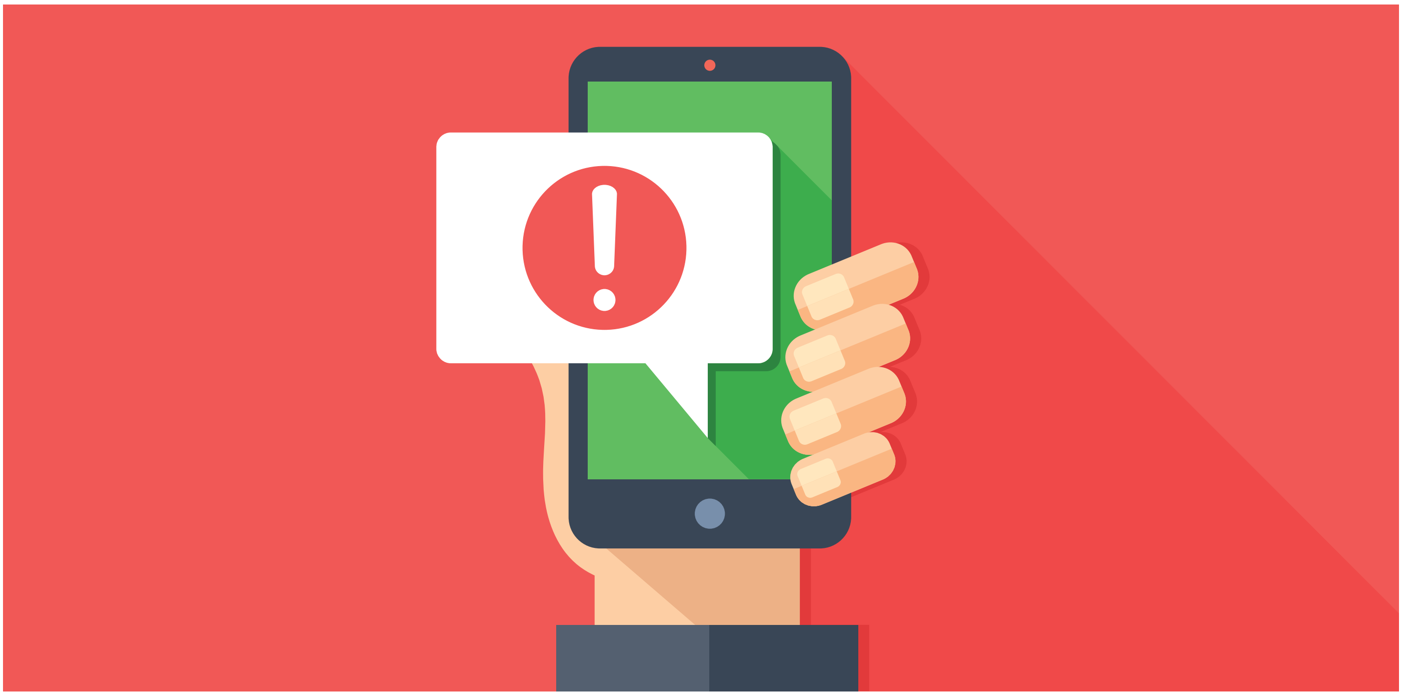
kaspersky

Contents

Main findings 2020

Kaspersky's data shows that the scale of the stalkerware issue has not improved much in 2020 compared to the last year:

- The number of people affected is still high. In total, 53,870 of our mobile users were affected globally by stalkerware in 2020. Keeping in mind the big picture, these numbers only include Kaspersky users, and the total global numbers will be higher. Some affected users may use another cybersecurity solution on their devices, while some do not use any solution at all.
- With more than 8,100 users affected globally, Nidb is the most used stalkerware sample, according to our 2020 stats. This sample is used to sell a number of different stalkerware products such as iSpyoo, TheTruthSpy and Copy9 among others.
- In terms of geographic spread, we see a largely consistent trend emerging: Russia, Brazil, and the United States of America (USA) remain the most affected countries globally, and they are the three leading countries in 2020.
- In Europe, Germany, Italy and the United Kingdom (UK) are the top three most-affected countries respectively.



Introduction and methodology

Technology has enabled people to connect more than ever before. We can choose to digitally share our lives with our partner, family, and friends regardless of how far we are physically. Yet, we are also seeing a rise in software that enables users to remotely spy on another person's life via their digital device, without the affected user giving their consent or being notified.

The risks of stalkerware can go beyond the online sphere and enter the physical world. The Coalition Against Stalkerware warns that stalkerware «may facilitate intimate partner surveillance, harassment, abuse, stalking, and/or violence.»

The software, known as stalkerware, is commercially available to everyone with access to the internet. The risks of stalkerware can go beyond the online sphere and enter the physical world. The Coalition Against Stalkerware warns that stalkerware «may facilitate intimate partner surveillance, harassment, abuse, stalking, and/or violence.» Stalkerware can also operate in stealth mode, meaning that there is no icon displayed on the device to indicate its presence and it is not visible to the affected user. The majority of affected users do not even know this type of software exists. This means they cannot protect themselves, online or offline, especially as the perpetrator using stalkerware usually knows their victim personally.

In recent years, Kaspersky has been actively working with partners to end the use of stalkerware. In 2019, we created a special alert that notifies users if stalkerware is installed on their phones. Following that we became one of ten founding members of the Coalition Against Stalkerware. We also published our first full report on the state of stalkerware in the same year to understand the scale of the problem.

This report continues to examine the issue of stalkerware and presents new statistics from 2020, in comparison to our previous data. The data in this report has been taken from aggregated threat statistics obtained from the Kaspersky Security Network. The Kaspersky Security Network is dedicated to processing cybersecurity-related data streams from millions of voluntary participants around the world. All received data is anonymized. To calculate our statistics, we review the consumer line of Kaspersky's mobile security solutions.

The issue of, and the story behind, stalkerware

Stalkerware is software that is commercially available to everyone with access to the internet. It is used to spy remotely on another person via their device, without the affected user giving their consent or being notified. Stalkerware operates in stealth mode, meaning that there is no icon displayed on the device indicating its presence, and it is not visible to the affected user. Therefore, the Coalition Against Stalkerware defines stalkerware as software which «may facilitate intimate partner surveillance, harassment, abuse, stalking, and/or violence".

The dimension of cyberviolence

Seven in ten women in Europe who have experienced cyberstalking have also experienced at least one form of physical and/or sexual violence from an intimate partner

According to a report by the European Institute for Gender Equality, «seven in ten women in Europe who have experienced cyberstalking have also experienced at least one form of physical and/or sexual violence from an intimate partner». Echoing these findings, experts from non-profit organizations (NPOs) that help domestic abuse survivors and victims emphasize that cyberstalking is also a form of violence. Just as with physical, psychological, and economic violence, an abuser can use surveillance to obtain complete control of their victim/survivor[1] and stay in charge of the situation.

Using stalkerware, the extent of control held by the abuser can be immense. Depending on the type installed, stalkerware may have a variety of functions to intrude into the victim's privacy. With the software's help, an abuser can:

- Read anything the surveilled person types – logging each keystroke on the device, including credentials to any kind of services such as banking applications, online shops and social networks, etc.
- Know where they are – by tracking a person's movements with GPS, in real time
- Hear what they say – eavesdrop on calls, or even record them
- Read messages on any messenger, regardless of whether encryption is used
- Monitor social network activity
- See photos and videos
- Switch on the camera

[1] Experts refer in their terminology more and more to the empowering term survivor instead of victim. Hence, in this report, we will use both terms.

All of this private information can be collected, usually from a mobile device, such as a tablet or a smartphone.

Non-profit organizations from the Coalition Against Stalkerware are experiencing a growing number of survivors seeking help with the problem

Non-profit organizations from the Coalition Against Stalkerware are experiencing a growing number of survivors seeking help with the problem:

- Findings from the Second National Survey on technology abuse and domestic violence in **Australia**, launched by WESNET with the assistance of Dr. Delanie Woodlock and researchers from Curtin University, state that 99.3% of domestic violence practitioners have clients experiencing technology-facilitated abuse and that the use of video cameras increased by 183.2% between 2015 and 2020.
- According to a study on cyberviolence in intimate relationships, conducted by the Centre Hubertine Auclert in **France**, 21% of victims have experienced stalkerware at the hands of their abusive partner, and 69% of victims have the feeling that the personal information on their smartphone has been accessed by their partner in a hidden way.
- In **Germany**, for several years, Women's Counselling Centers and Rape Crisis Centers (bff) have noticed an increasing use of stalkerware in conjunction with partner relationships.
- In the **USA**, stalking impacts an estimated 6-7.5 million people over a one-year period, and one-in-four victims report being stalked through some form of technology, according to the Stalking Prevention Awareness & Resource Center (SPARC).

Physical access is the key

Unfortunately, it is not too difficult to secretly install stalkerware on a victim's phone. The main barrier that exists is that stalkerware has to be configured on an affected device. Due to the distribution vector of such applications which are very different from common malware distribution schemes, it is impossible to get infected with a stalkerware through a spam message including a link to stalkerware or a trap via normal web surfing.

This means that the abuser will need to have physical access to the target device in order to install stalkerware. This is possible if the device either has no pin, pattern, or password to protect it or alternatively, the abuser knows the victim/survivor personally. Installation on the target device can be completed within a few minutes.

Prior to accessing the survivor's device, the abuser has to collect a link to the installation package from the stalkerware developer's webpage. In most cases, the software is not downloaded from an official application store. For Android devices, Google banned applications that are clearly stalkerware from its Google Play application store in 2020. This means the abuser will not be able to install such an application from the general app store. Instead, the abuser must follow several steps before being able to install stalkerware. As a result, the abuser may leave traces in the device settings that a user can check if they are concerned they may be being spied on.

Stalkerware tools are less frequent on iPhones than on Android devices

Stalkerware tools are less frequent on iPhones than on Android devices because iOS is traditionally a closed system. However, perpetrators can work around this limitation on jailbroken iPhones. They still need physical access to the phone to jailbreak it, so iPhone users who fear surveillance should always keep an eye on their device. Alternatively, an abuser can offer their victim an iPhone – or any other device – with pre-installed stalkerware as a gift. There are many companies who make their services available online to install such tools on a new phone and deliver it to an unwitting addressee in factory packaging to celebrate a special occasion.

[redacted] EXPRESS. Get A Phone Pre-Installed With [redacted] —
Delivered Straight To Your Door

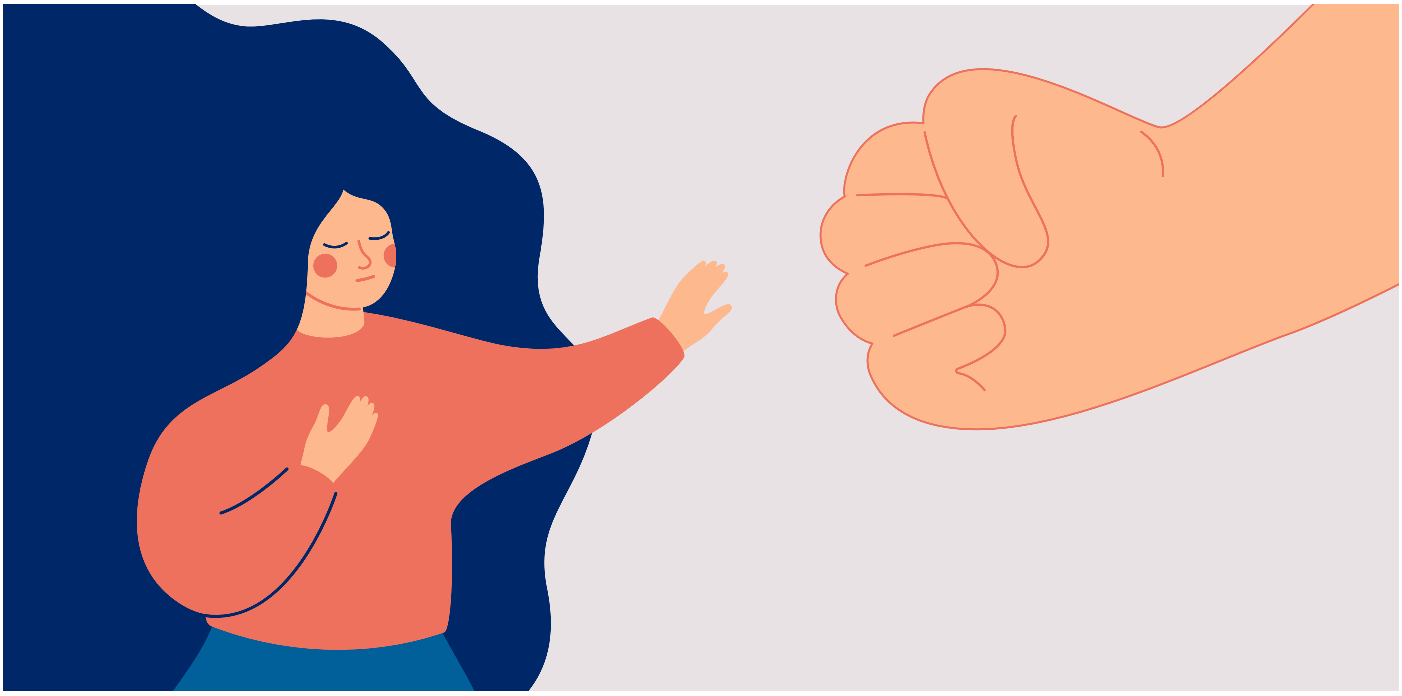
The risk of privacy leaks

The information monitored via stalkerware will be available to at least one person – the abuser who installed stalkerware on the survivor's phone. However, sometimes it is possible that all the private data may become publically available. Year on year, stalkerware servers are either hacked or left openly unprotected so that information can be accessed and leaked online. For example, in 2020, such a data breach occurred due to a product provided by ClevGuard. In previous years, we have seen similar incidents with Mobiispy in 2019 and with MSpy in 2018 and 2015.

These are just a few examples of a long list in which databases from companies developing stalkerware have been exposed, affecting millions of user accounts. With the possibility to track a person's location, it means that not only their cyberprivacy is lost but also their security in the physical world may be at risk.

The legal status

Stalkerware applications are sold and provided by companies under various facades, such as child monitoring or employee tracking solutions. While laws vary from one country and state to another, they are catching up. Generally speaking, it is only illegal to use such tools and apps that record user activity without their consent or that of legal authority. Slowly we are seeing some shifts in legislation. For instance, in 2020, France reinforced sanctions on secret surveillance: geolocating someone without their



consent is now punishable with one year imprisonment and a fine of 45,000 euros. If this is done within a couple, the sanctions are potentially higher, including two years' imprisonment and a fine of 60,000 euros.

Stalkerware tools often violate laws and expose the stalker to legal liability for any recordings made without the victim's knowledge. Stalkers must realize that they are breaking the law. If the use of stalkerware is reported, the punishment applies to the private perpetrator who installed the software – not its vendor. In the USA, only two stalking app developers have been fined in recent history. One had to pay a record 500,000 US dollar fine, which put an end to the app development process, while the other got off with an order to change the app's functionality for future sales.

The scale of the issue

Global detection figures – affected users

In this section, we look at the global numbers of unique users whose mobile device was found to have stalkerware detected.

The 2020 data shows that the stalkerware situation has not improved much: the number of affected people is still high. A total of 53,870 unique users were affected globally by stalkerware in 2020. Whereas in 2019, 67,500 unique users were affected globally. However, the fact must be taken into account that 2020 was an unprecedented year in which lives have changed in a dramatic way across the globe.

A total of 53,870 unique users were affected globally by stalkerware in 2020. Whereas in 2019, 67,500 unique users were affected globally.

To fight the COVID-19 pandemic, all countries in the world have faced massive restrictions such as self-isolation measures or lockdowns in order to make people stay at home. Considering that stalkerware is used as another tool to control an intimate partner who the abuser lives with as they go about their day-to-day life, this can explain the somewhat lower numbers in comparison with the previous year.

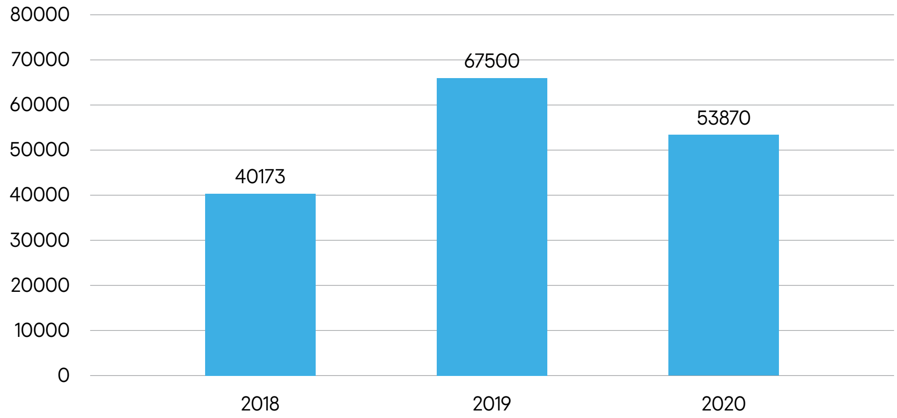


Table 1. Unique users affected by stalkerware globally from 2018 until 2020– total per year

That said, the 2020 numbers are still on a high, stable level. In comparison, in 2018, there were 40,173 detections of unique users being affected globally by stalkerware.

When looking at the figures of the total number of unique users affected by stalkerware in 2020 worldwide per month, this trend becomes even more noticeable. The first two months of the year were stable with many cases of affected devices arising, showing stalkerware was quite popular. The situation changed in March when many countries decided to announce quarantine measures. The curve shows a trend that the numbers began to stabilize as of June 2020 when many countries around the world eased restrictions.

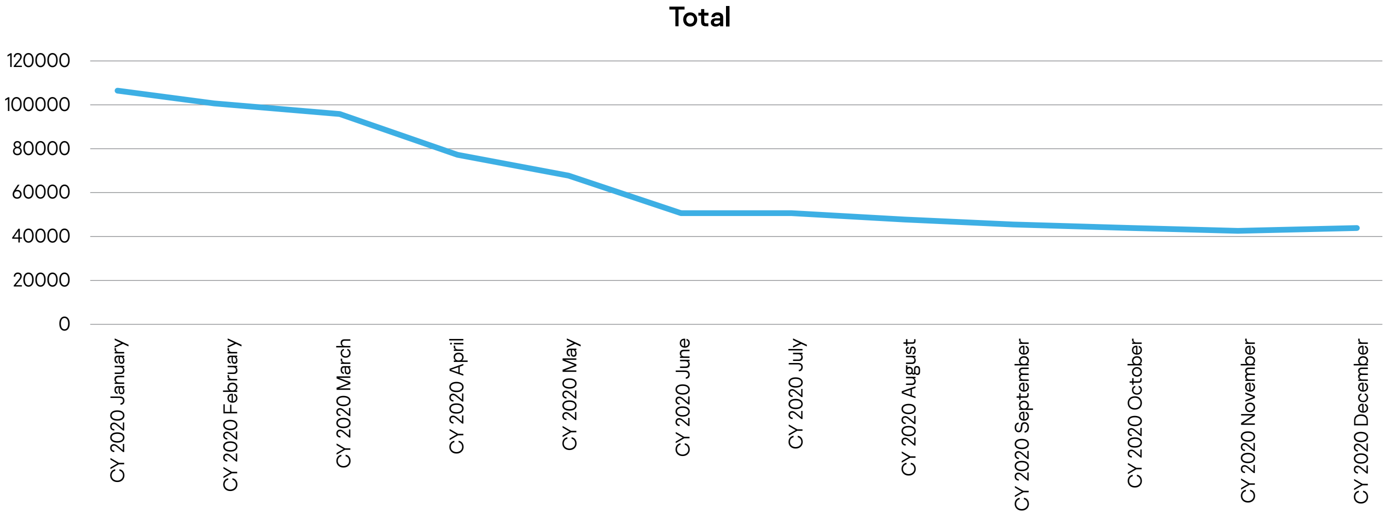


Table 2. Unique users affected by stalkerware in 2020 worldwide – total by month

That said, the 2020 numbers are still on a high, stable level. In comparison, in 2018, there were 40,173 detections of unique users being affected globally by stalkerware. This brings into perspective the total numbers from 2020, as we have seen a growing integration of technology into our lives. Sadly, this also means the software used for stalking is becoming more common as another form of intimate partner violence.

Global detection figures – stalkerware samples

In this section, we analyze which stalkerware samples are actually the most used to control mobile devices on a global level. In 2020 the most detected samples can be seen in the following results:

	Samples	Affected users
1	Monitor.AndroidOS.Nicb.a	8147
2	Monitor.AndroidOS.Cerberus.s	5429
3	Monitor.AndroidOS.Agent.af	2727
4	Monitor.AndroidOS.Anlost.a	2234
5	Monitor.AndroidOS.MobileTracker.c	2161
6	Monitor.AndroidOS.PhoneSpy.b	1774
7	Monitor.AndroidOS.Agent.hb	1463
8	Monitor.AndroidOS.Cerberus.a	1310
9	Monitor.AndroidOS.Reptilic.a	1302
10	Monitor.AndroidOS.SecretCam.a	1124

Table 3. 2020 Top 10 most detected stalkerware samples globally

1. With more than 8,100 users having been affected by it, **Nidb** was the most used stalkerware sample in 2020. The Nidb creator sells their product as Stalkerware as a Service. This means that anyone could rent their control server software and mobile application, rename it to any suitable marketing name and sell it separately—examples of this include iSpyoo, TheTruthSpy, Copy9, and others.
2. Both second and eighth place are occupied by Cerberus. These are two different samples under the same family. Variant **Cerberus.a** affected more than 5,400 users.
3. **Agent.af** comes in third place, with more than 2,700 users having been affected. This is marketed as Track My Phone and has typical features such as reading messages from any messenger, logging a person's call history, and tracking geolocation.
4. **Anlost.a** is a good example of stalkerware in disguise. It is advertised as an antitheft application, and its icon is present on the home screen (not usual behavior for stealthy stalkerware apps). Therefore, it is available on the Google Play Store. That said, it is possible to deliberately hide the icon from the home screen. One of the key functionalities of the application is to intercept SMS messages and read the call log. More than 2,200 users having been affected by this sample.
5. **MobileTracker.c** has several functionalities such as intercepting messages from popular social networks and taking remote control of the affected device. More than 2,100 users having been affected by this sample.
6. **PhoneSpy** is also known as Spy Phone app or Spapp Monitoring. This application consists of many spy features, covering all popular instant messengers and social networks.
7. **Agent.hb** is another version of MobileTracker. Like the original version, it offers many functionalities.
8. **Cerberus.b**, a different sample from the same family as Cerberus.a.
9. **Reptilic.a** is stalkerware that includes many features such as social media monitoring, call recordings, and browser history monitoring.
10. **SecretCam.a** is camera stalking software, meaning it is able to secretly record video from the front or back camera of the affected device.

Geography of affected users

Stalkerware is a global phenomenon that affects countries regardless of size, society, or culture. When looking at the top 10 affected countries worldwide in 2020, Kaspersky's findings show that largely the same countries remain the most affected, with Russia in the number one spot. Yet, we see an increase in stalkerware activity in Brazil and the USA in 2020 compared to 2019. However, we detected fewer incidents in India, which has fallen in the rankings. We have also detected a higher number of incidents in Mexico, which has risen in the ranking two places.

	Country	Affected users
1	Russian Federation	12389
2	Brazil	6523
3	United States of America	4745
4	India	4627
5	Mexico	1570
6	Germany	1547
7	Iran	1345
8	Italy	1144
9	United Kingdom	1009
10	Saud Arabia	968

Table 4. 2020 Top 10 most affected countries by stalkerware - globally

When considering Europe, Germany, Italy and the UK are the three most affected countries, in that order. They are followed by France in fourth place and Spain in fifth place.

	Country	Affected users
1	Germany	1547
2	Italy	1144
3	United Kingdom	1009
4	France	904
5	Spain	873
6	Poland	444
7	Netherlands	321
8	Romania	222
9	Belgium	180
10	Austria	153

Table 5. 2020 Top 10 most affected countries by stalkerware - Europe

How to check if a mobile device has stalkerware installed

It's hard for everyday users to know if stalkerware is installed on their devices. Generally, this type of software remains hidden which includes hiding the icon of the stalkerware app on the home screen and in the phone menu and even cleaning any traces that have been made. However, it may give itself away and there are some warning signs. Among the most important are:

- Keep an eye out for a fast draining battery, constant overheating and mobile data traffic growth.
- Do regular antivirus scanning on your Android device: If the cybersecurity solution detected stalkerware, **do not rush to remove it as the abuser may notice**. Have a safety plan in place and reach out to a local help organization.
- Check browser history: To download stalkerware, the abuser will have to visit some web pages, the affected user does not know about. Alternatively, there could be no history at all if abuse wiped it out.
- Check «unknown sources» settings: If «unknown sources» are enabled on your device, it might be a sign that unwanted software were installed from third-party source.
- Check permissions of installed apps: Stalkerware application may be disguised under a wrong name with suspicious access to messages, call logs, location, and other personal activity.

However, it's also important to understand that warning signs or symptoms are not necessarily proof that stalkerware is installed on a device.

In the context of domestic violence and abusive relationships it may be difficult or even impossible to deny the abusive partner access to the phone.

How to minimize the risk

There are a few pieces of advice that can help to increase your digital safety:

- Never lend your phone to anyone without seeing what happens with the phone and not leave it unlocked.*
- Use a complex lock screen password and change passwords on a regular basis.
- Do not disclose your password to anyone – not even your intimate partner or family members or close friends.*
- Do regular checks of your phone— delete apps you don't use and review the permissions granted to each app.
- Disable the option of third-party application installation on Android devices.
- Protect your Android devices with a cyber-security solution, such as Kaspersky Internet Security for Android (for free), which detects stalkerware and issues warnings.

*In the context of domestic violence and abusive relationships it may be difficult or even impossible to deny the abusive partner access to the phone.

Kaspersky's activities and contribution to end cyberviolence

Kaspersky is actively working to end the use of cyberviolence and stalkerware, as a company, and together with many other partners. In 2019, we created a special alert that notifies users when stalkerware is installed on their phones. In the same year, with nine other founding members we created the Coalition Against Stalkerware. In 2020, we created TinyCheck, a free tool to detect stalkerware on mobile devices – specifically for service organizations working with victims of domestic violence. TinyCheck can be found on https://github.com/KasperskyLab/TinyCheck. Since 2021, we are one of five partners in an EU-wide project aimed at tackling gender-based cyberviolence and stalkerware called DeStalk, which the European Commission chose to support with its Rights, Equality and Citizenship Program.

About the Coalition Against Stalkerware

The Coalition Against Stalkerware («CAS» or «Coalition») is a group dedicated to addressing abuse, stalking, and harassment via the creation and use of stalkerware. Launched in November 2019, the Coalition Against Stalkerware gained 26 partners in its first year. These include founding partners – Avira, Electronic Frontier Foundation, the European Network for the Work with Perpetrators of Domestic Violence, G DATA Cyber Defense, Kaspersky, Malwarebytes, The National Network to End Domestic Violence, NortonLifeLock, Operation Safe Escape, and WEISSER RING. The Coalition looks to bring together a diverse array of organizations to actively address the criminal behavior perpetrated through stalkerware and increase public awareness about this important issue. Due to the high societal relevance for users all over the globe and new variants of stalkerware emerging periodically, the Coalition Against Stalkerware is open to new partners and calls for cooperation. To find out more about the Coalition Against Stalkerware please visit the official website www.stopstalkerware.org.

Comments from the Partners of the Coalition Against Stalkerware

COALITION AGAINST STALKERWARE

Deborah J. Vagins

NNEDV President and CEO

«The National Network to End Domestic Violence (NNEDV) is proud to be a founding partner of the Coalition Against Stalkerware and to continue to support its important work. Through the efforts our Safety Net Project, we know that many victims of domestic violence experience harassment, monitoring, stalking, and fraud from partners who use stalkerware as a tool of abuse, which can have lasting impacts on survivors' safety and security. We reaffirm our commitment to understanding and addressing this tactic of abuse and ensuring that everyone, including survivors, can use technology without fear of violence.»

Iman Karzabi

Project Manager for the Regional Observatory of Violence Against Women at Centre Hubertine Auclert

«We are extremely proud to be part of the Coalition Against Stalkerware, and to see the results after one year of existence. The topic of stalkerware is now emerging, and fruitful discussions among private and public partners in the Coalition are allowing to better protect victims of domestic violence.»

Alessandra Pauncz

WWP EN Executive Director

«The effects of cyber violence on women and girls are devastating, all-consuming and never ending, because they are part of a continuum of violence (offline and online) that deprives them of their freedom.»

Eva Galperin

Director of Cybersecurity, Electronic Frontier Foundation

«The member organizations in the Coalition Against Stalkerware have made tremendous strides in the last year, including awareness-raising, detection of stalkerware, and research into the daily lives of survivors of domestic abuse. The Coalition has enabled us to take a holistic approach to a complex problem. There is no simple solution and we must keep pushing forward on many fronts.»

Karen Bentley

CEO and cofounder Safety Net Australia Project, Women's Services Network (WESNET)

"Our recent Australian research shows 99.3% of Domestic Violence practitioners in Australia have clients experiencing technology-facilitated abuse. We work with agencies and women every day who are stalked, monitored and surveilled by their abusers, and we see first-hand the impact on their lives. Stalkerware and other monitoring and surveillance is particularly traumatic. Survivors speak of feeling caged and tethered by technology with no hope of escaping their abuser because the technology follows. There is an epidemic of domestic violence and other forms of abuse in Australia as well as the rest of the world. Elimination of this violence can only occur with the cooperation of the entire community. Joining forces with the Coalition Against Stalkerware is crucial to raise awareness about how to make technology safer so it can be accessed by all safely."

James Donaldson

CEO of Copperhead

«The increasing prevalence of stalkerware in the environment should be a concern to everyone. These technologies can have frightening power over our lives that no person should ever wield.»

David Ruiz

Online Privacy Advocate at Malwarebytes

«Over the last year, we have made significant strides in educating the public about the growing dangers of stalkerware thanks to the incredible efforts of our partners. Sharing information and working together is critical to ensuring that we help reduce the dangers of apps that can be used to track people without their knowledge or consent. We hope more organizations join us as we continue to fight to ensure users can choose how and when to share their data with others.»

Kristina Shingareva

Head of External Relations at Kaspersky

«This is the first anniversary of the Coalition Against Stalkerware, and it has been quite a year in which we have learnt a lot. We now understand that stalkerware is not purely a technical problem. It's not the IT part of the issue that is challenging, but the fact that we need to deal with the commercial availability of stalkerware, the lack of regulation around how it is being used and, perhaps the most difficult problem, the fact that violence against women and different forms of online abuse have been normalized. We can provide technical training on different forms of tech-enabled abuse for the NPOs, but it's not enough – it should be complemented with a chapter focusing on and reflecting on survivors' psychological experiences.»

Matt Body

CTO of Traced

«As a security vendor we're acting on problems that severely affect people's lives. Being able to support the Coalition, we really feel like we're able to make a difference.»

For additional member insights please visit the Coalition Against Stalkerware website.