The State of **Stalkerware** in 2019

COALITION AGAINST STALKERWARE

kaspersky

COALITION AGAINST STALKERWARE

About the Coalition Against Stalkerware

A new global working group combining expertise for victim support and cybersecurity to help affected users

Ten organizations – Avira, Electronic Frontier Foundation, European Network for the Work with Perpetrators of Domestic Violence, G DATA CyberDefense, Kaspersky, Malwarebytes, National Network to End Domestic Violence, NortonLifeLock, Operation Safe Escape and WEISSER RING – have launched in November 2019 the global initiative called Coalition Against Stalkerware to protect users against so-called stalkerware.

The Coalition was convened in order to facilitate communication between the security community and those organizations working to combat domestic violence. With its online portal www.stopstalkerware.org the Coalition aims at helping victims, facilitating knowledge transfer among members, developing best practices for ethical software development and educating the public about the dangers of stalkerware.

The project has been envisioned as a non-commercial initiative aimed at bringing stakeholders from non-profit organizations, industry and other areas such as law enforcement under the same umbrella. Due to the high societal relevance for users all over the globe, with new variants of stalkerware being developed on a regular basis, the Coalition Against Stalkerware is open to new partners and calls for cooperation.

For more information, please visit www.stopstalkerware.org

Founding Partners commenting on the relevance to **work together against stalkerware**:

COALITION AGAINST STALKERWARE

Alexander Vukcevic
Director Protection Labs
Avira

Monitoring software has evolved rapidly in past years, powerful surveillance functions have been added and the purpose of the tracking activity has fundamentally changed. The continuous surge in mobile device usage combined with a lack of legislative mitigation is giving people accessible tools to spy on spouses, family members or friends. Avira recognizes that this is a new threat category and invites IT security companies and organizations working against domestic violence to join forces, share information and work together to stop these privacy violations.

Eva Galperin
Director of Cybersecurity
Electronic Frontier Foundation

Stalkerware, used for spying on phones and computers in domestic abuse or harassment situations, is a very serious problem, and it often goes hand-in-hand with other forms of abuse, up to and including physical violence. The ubiquity of stalkerware is a complex problem and we need stakeholders from all parts of society in order to fight it effectively.

Anna McKenzie
Communications Manager
European Network for the Work with Perpetrators of Domestic Violence

Studies have shown that 70% of women victims of cyberstalking also experienced at least one form of physical or/and sexualised violence from an intimate partner. We need to stop perpetrators from using their partners' phones for stalking and hold them accountable for their violence. The Coalition Against Stalkerware enables us to bring our knowledge on gender-based violence and perpetrators to IT security companies – so we can work together towards ending violence against women and girls perpetrated via new technologies.

Hauke Gierow
Press spokesperson
G DATA CyberDefense

Placing spyware on a partner's phone constitutes a violation of fundamental human rights. We are determined to fight this behaviour and protect survivors of abusive behaviour, mostly women. G DATA Cyber Defense is committed to better educate users about potential risks as well as work with victims organisations to also tackle non-technical issues associated with stalkerware.

Vyacheslav Zakorzhevsky
Head of Anti-Malware Research
Kaspersky

In order to counter this issue, it is important for cybersecurity vendors and advocacy organizations to work together. IT security industry gives its input by improving detection of stalkerware and better notifying users of this threat to their privacy. While service and advocacy organizations directly work with victims of domestic violence, know their pain points and requests, and can guide our work. So acting together, shoulder to shoulder, we will be capable to assist survivors through technical expertise and capacity building.

David Ruiz
Online Privacy Writer
Malwarebytes Labs

For years, Malwarebytes has detected and warned users about the potentially dangerous capabilities of stalkerware, an invasive threat that can rob individuals of their expectation of, and right to privacy. Just like the abuse it can enable, stalkerware also proliferates away from public view, leaving its victims and survivors in isolation, unheard and unhelped. Forming and fighting together with the Coalition against Stalkerware is the next, necessary step in stopping this digital threat—a collaborative approach steered by the promise of enabling the safe use of technology for everyone, everywhere.

Erica Olsen
Director of the Safety Net Project
National Network to End Domestic Violence

When designed to operate in complete stealth mode, with no persistent notification to the device owner, stalkerware can give abusers, stalkers, and other perpetrators a robust tool to perpetrate harassment, monitoring, stalking, fraud, and abuse. This type of abuse can be terrifying, traumatizing, and raises significant safety and privacy concerns. The creation of this Coalition is an exciting step forward to address this problem.

Kevin Roundy
Research Director
NortonLifeLock

At NortonLifeLock, our research experts have been working hard to take stalkerware out of the hands of abusers for more than 12 years, giving victims and potential victims tools to help protect themselves and be free of harassment, violence and attacks. We are proud to be a founding member of the Coalition Against Stalkerware to share our expertise and join forces in the fight to help stop abuse.

Wilson "Chilly" Hightower
Head of Intake
Operation Safe Escape

The insidious existence of stalkerware only serves to violate, harm, and instill a constant sense of fear and anxiety in many of our clients. It is an active and existential threat to the security and privacy of all people. As our lives become more ingrained and dependent on technology, the threat stalkerware already poses grows by an order of magnitude. It is more important than ever to get ahead of this threat to take the power away from potential abusers, stalkers, and other malicious entities. Operation Safe Escape could not be more proud to be part of this group effort to restore privacy and a sense of safety to our clients and people everywhere.

Horst Hinger
Deputy Managing Director
WEISSER RING

As a non-profit organization we know that technology facilitates abusers access to their victims' private data. Rarely victims seek help because they feel ashamed. For WEISSER RING stalking is increasingly an important issue we encounter in our victim help. In 2018 we have assisted 1019 cases of stalking which was about three percent more than the year before. According to German police crime statistics, in 2018 there had been in total almost 19,000 cases of stalking, 500 more than the year before – a clear increase as well. Therefore we have developed the NO STALK app together with the WEISSER RING Foundation to provide victims with an effective tool in order to document stalking in an evidence-proof manner.

Contents

Introduction and methodology

Six months ago, we created a special alert that notifies users about commercial spyware (stalkerware) products installed on their phones. This report examines the use of stalkerware and the number of users affected by this software in the first eight months of 2019.

Consumer surveillance technology has evolved rapidly in recent years and the very purpose of surveillance activity has changed dramatically. The rise of the internet and subsequent explosion in mobile device usage has led to a thriving type of surveillance software – known as stalkerware. The software allows users to spy on other people - for example, to monitor their messages, call information and GPS locations - in complete stealth. It can often be used to abuse the privacy of current or former partners and even strangers. This can be done by simply manually installing an application on the targeted victim's smartphone or tablet. Once in place, the stalker receives access to a range of personal data, despite being remote from the victim. It differs greatly from parental control software. While parental control apps aim to restrict access to risky and inappropriate content and persistently notifies a user about its requests, stalkerware is about providing the abuser with surveillance to spy on a victim, without the consent of an individual.

Stalkerware is about providing the abuser with surveillance to spy on a victim, without the consent of an individual

The vast majority of stalkerware apps are not available on official app stores – like Google Play – and installation requires access to a dedicated website and access to the victim's device. Those with bad intentions may use it to monitor employee emails, track children's movements and even spy on what a partner is up to. Such uses may lead to harassment, surveillance without consent, stalking and even domestic violence. However, current laws to regulate the use of stalkerware are not yet strong enough to deter culprits from abusing and taking advantage of other people.

The data in this report has been taken from aggregated threat statistics obtained from the Kaspersky Security Network, to measure how often and how many users encountered stalkerware threats in the first eight months of 2019, compared to what was found last year. The Kaspersky Security Network is the infrastructure dedicated to processing cybersecurity-related data streams from millions of voluntary participants around the world. In this report, we have explored why stalkerware is being used and where it is implemented most prolifically.

Main findings

Worldwide, the number of users with stalkerware installed on their devices rose by 35% within just one year

- From January to August 2019, around the world, there were more than 518,223 cases when our protection technologies either registered presence of stalkerware on users' devices or detected an attempt to install it – a 373% increase in the same period in 2018
- In the first eight months of 2019, 37,532 users encountered stalkerware at least once. This is a 35% increase from the same period in 2018 when 27,798 users were targeted
- The number of users targeted by full-throttle spyware detected as Trojan-Spy reached 26,620 the first eight months of 2019, which makes it a minority compared to the number of users who encountered stalkerware
- Internationally, the Russian Federation Russian Federation remains the most prominent region for stalkerware globally, accounting for 25.6% of potentially affected users, in the first eight months of 2019. India is in second place with 10.6% of affected users, and Brazil is in third place (10.4%). The United States hold forth place with 7.1%
- When it comes to Europe - Germany, Italy and the UK hold the top three places respectively

Rise of the stalkerware problem

This year has seen a sharp rise in the number of detections of stalkerware on Android devices protected by Kaspersky products. One reason for this rise could be the improvement in detecting stalkerware software through cybersecurity solutions. In April, Kaspersky launched functionality in its Android security app – Privacy Alert – that specifically alerts users if a software that can be used for stalking is found on their device. Since then, the number of detections has steadily risen. For instance, 4,315 users encountered stalkerware in March 2019, compared to 7,075 in April – a 64% increase in just one month. This figure rose to 9,251 during August, 94% higher than the month before the functionality was launched.

These openly-sold consumer surveillance programs are often used for spying on colleagues, family members or partners, and are in great demand. For a relatively modest fee, sometimes as little as $7 per month, these apps stay hidden while keeping their operators informed about the device activity, such as its owner's location, browser history, text messages, social media chats, and more. Some of them can even make video and voice recordings.

To further examine the extent of the stalkerware problem, Kaspersky has analyzed the last eight months' worth of activity. Between January to August 2019, 37,533 users encountered stalkerware on their devices at least once. This is a 35% increase from the same period in 2018 when 27,798 users were targeted. Overall, there were 518,223 cases when Kaspersky products either registered the presence of stalkerware on users' devices or detected an installation attempt in the period from January to August 2019 - a staggering 373% increase compared to the period in 2018.

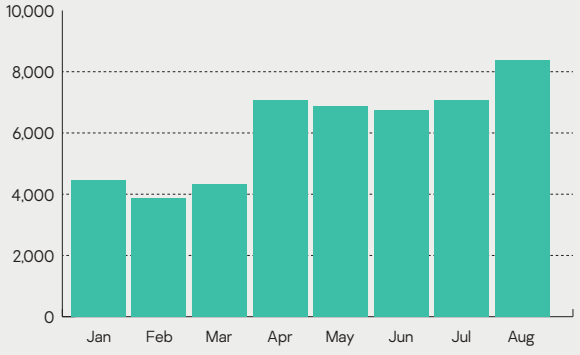


Fig.1 Number of users who encountered stalkerware in Jan-Aug 2019

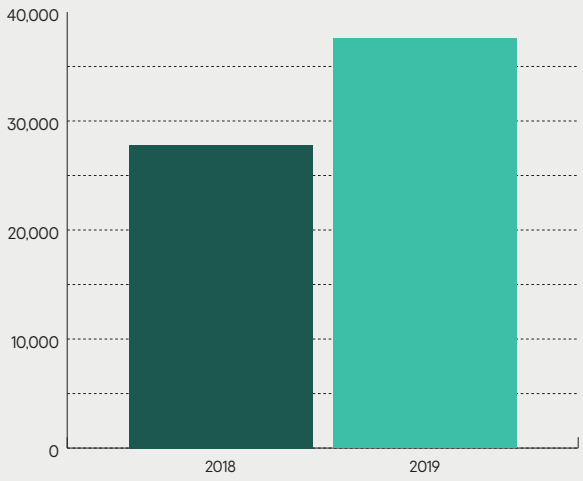


Fig.2 Users targeted by stalkerware 2018 vs 2019

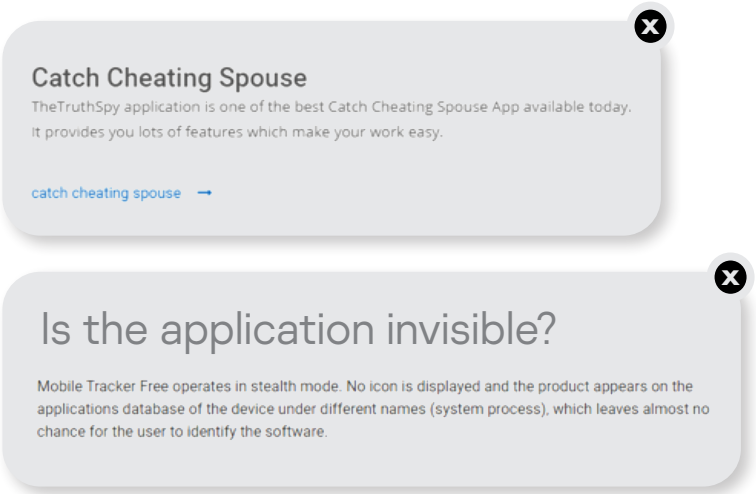


Fig.3 Screenshots from the Mobile Tracker Free official website

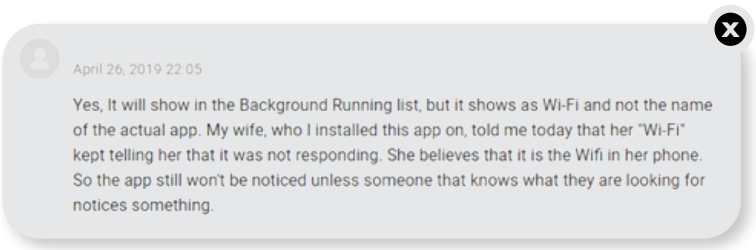


Fig.4 Screenshot from the TheTruthSpy official website

Examples of software used for stalking purposes

A third-party can also access victims' photos from the phone and the camera in real-time, along with their browser history, files on the device, calendar and contact list

The most prolific stalkerware family in 2019 was identified as Monitor.AndroidOS.MobileTracker.a, which affected 6,559 unique users. In second place, Monitor.AndroidOS.Cerberus.a was detected on the devices of 4,370 users, closely followed in third place by Monitor.AndroidOS.Nidb.a (4,047).

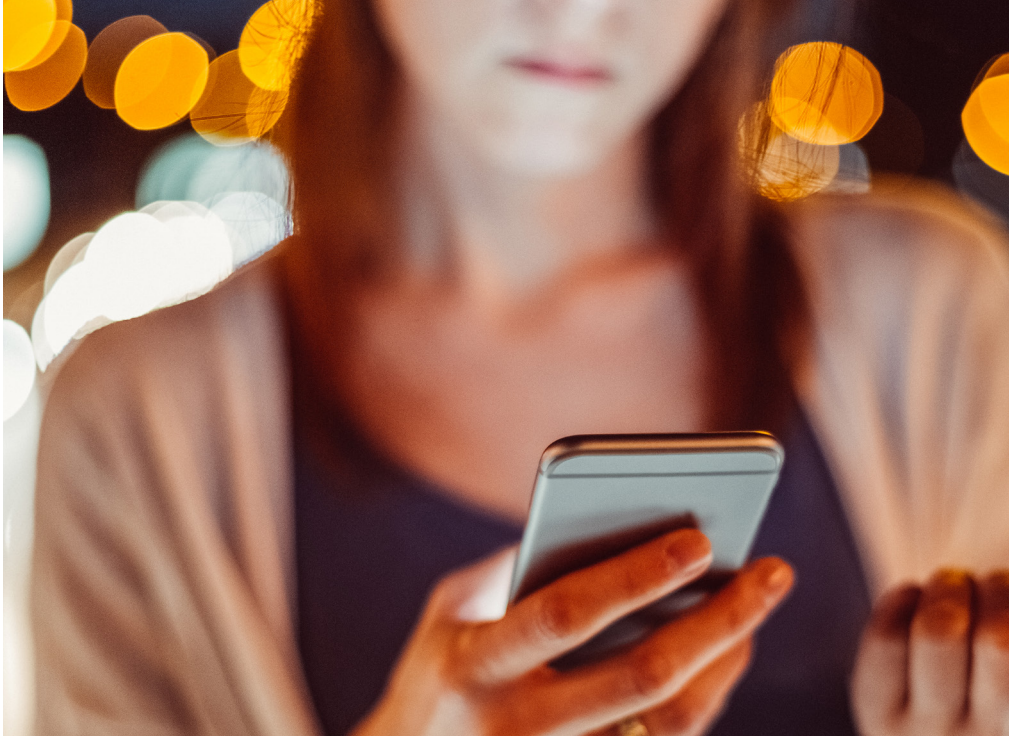
Comparing the results from 2018, the top two differ from last year. Monitor.AndroidOS.Nidb.a and Monitor.AndroidOS.PhoneSpy.b were found most on the devices of users in 2018, reaching 4,427 and 2,819 respectively. Monitor.AndroidOS.XoloSale.a was the third most common stalkerware reaching 1,946 users.

In our internal classification system, a Monitor.AndroidOS.MobileTracker.a record is used to identify a Mobile Tracker Free application, which is positioned as a tool to track the activity of children or employees. In fact, the application allows tracking of the user's location, their correspondence both in SMS messages and messenger applications (WhatsApp, Hangouts, Skype, Facebook Messenger, Viber, Telegram, etc.), as well as calls. A third-party can also access victims' photos from the phone and the camera in real-time, along with their browser history, files on the device, calendar and contact list. In addition, the application provides the ability to remotely control the device. As well as all of this, there is a possibility of working in a hidden mode under the disguise of system applications

The next application - Cerberus (Monitor.AndroidOS.Cerberus.a) - is positioned as an anti-theft app. However, it also allows a stalker to work in 'hidden' mode and to prevent its deletion. Among other things, it provides the ability to track the location of the device, take pictures from the camera and screenshots, as well as record audio from the microphone.

The third-placed Monitor.AndroidOS.Nidb.a is in fact a group of similar applications: iSpyoo/TheTruthSpy/Copy9. Unlike the previous two applications, some representatives of this group openly advertise themselves as a means of spying on a partner and even write articles about it.

The set of functions is quite standard for such programs yet still impressive - website tracing, interception of correspondence in SMS and in messenger applications, call tracing and browser history. Like many other similar applications, they require super-user rights (administration rights) to operate some functions. They can work in 'hidden' mode, and their names in the list of installed applications mimic the system processes.



Where is stalkerware found?

There is a global market for legal spyware and stalkerware software, as proven by the diverse range of regions where the most attacks are taking place. The top 10 countries with the largest share of users attacked with stalkerware do not have geopolitical similarities and are not in close proximity.

1. Russian Federation – **25.61%**
2. India – **10.56%**
3. Brazil – **10.39%**
4. United States – **7.11%**
5. Germany – **3.55%**
6. Italy – **2.65%**
7. Mexico – **2.10%**
8. United Kingdom – **1.95%**
9. France – **1.76%**
10. Iran – **1.68%**

Other – **32.65%**

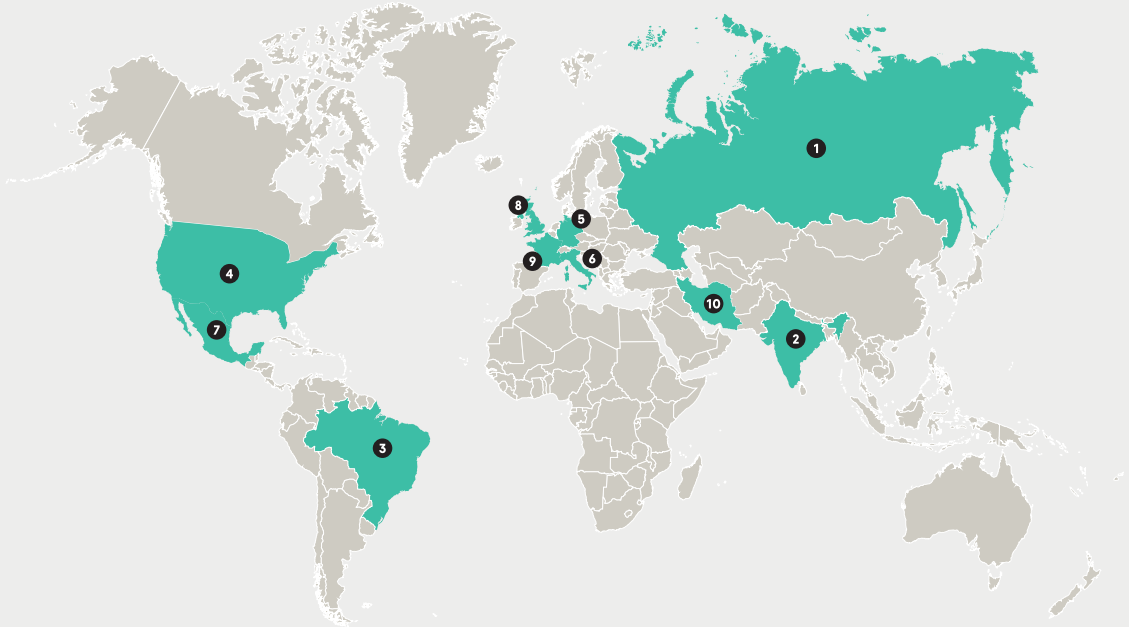


Fig. 5 Geography of users who encountered stalkerware in 2019

A survey showed that 85% of domestic violence workers say they have assisted victims whose abuser tracked them using GPS

Kaspersky's findings show that Russia is the region where stalkerware activity is peaking. Persistent activity in India has led to the country being the second most prominent region for stalkerware-related incidents from January to August, with 10.56% users affected.

Brazil accounted for 10.39% of attacked users in 2019, while the United States are now fourth (7.11%). There are advocacy groups in the country raising awareness about the dangers of stalkerware and conducting revealing user research. 72 domestic violence shelters were surveyed by National Public Radio, with 85% of domestic violence workers saying they have assisted victims whose abuser tracked them using GPS. Nearly three-quarters (71%) of domestic abusers monitor survivors' computer activities, while 54% tracked survivors' cell phones with stalkerware. The fifth most prevalent country in 2019 was Germany with (3.55%).

Stalkerware on the cyberthreat landscape

Over 37,000 users were attacked by stalkerware in 2019 compared to almost 27,000 the year before

When comparing stalkerware and spyware to the rest of the attacks mobile users face – such as adware, riskware and malware – it takes up a big share of less targeted not-a-virus programs. In the first eight months of 2019, Kaspersky detected 2,350,862 users attacked with potentially unwanted threats and just 1.60% of them were related to stalkerware. However, unlike the majority of mass potential threats (like adware), stalkerware requires a specific stalker to act and carry out its operation. Every target is being stalked and chosen on purpose. So, while the numbers are lower, stalkerware takes a more targeted effort to affect a victim and has a disturbing figure of abuse behind each of them.

To get the big picture when assessing the stalkerware development dynamics, we've compared stalkerware to the full scale, illegal surveillance malware for PC that we detect as Trojan Spy. The results have proved, that while illegal spyware is in decline, stalkerware is thriving.

Our analysis of the first eight months of 2019 shows that the number of users who encountered stalkerware had, in fact, surpassed the figure for Trojan-Spy attacks. While 2018 saw more than 43,000 Trojan Spy targets compared to around 28,000 stalkerware targets, in 2019 the picture changed. The number of users that encountered stalkerware grew by 35% to reach over 37,000, while spyware tools accounted for 26,620 of targets.

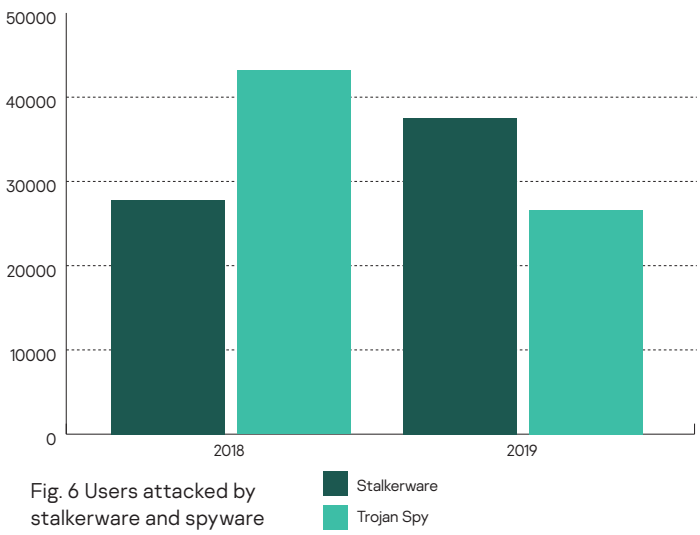


Fig. 6 Users attacked by stalkerware and spyware

There has been a notable rise in the number of stalkerware-related incidents registered by Kaspersky products when compared to all threats from the figures in 2018. Between January and August last year, such software made up just 1.01% of the overall number of users who faced any kind of potentially dangerous (adware and others from not-a-virus category) software (2,740,023). It appears that stalkerware is growing in popularity, while more traditional malware attacks are less prolific than they were 12 months ago.

Conclusion and recommendations

It is clear to see that stalkerware is on the rise and becoming much more prominent in the cybersecurity landscape. In accordance with the overall number of detected riskware, adware and spyware attack fluctuations year-on-year, the percentage of stalkerware-related incidents continues to rise. It may take time to discover the role of stalkers on the cyberthreat landscape, but more incidents are now accounted for. Thanks to improved cybersecurity software, there has been a sharp rise in detection rates since Kaspersky launched its own solution to notify users about stalkerware in April 2019.

There has also been a level of consistency around which countries are the most likely to experience stalkerware-related incidents, with Russia, India, the United States and Germany amongst the most prominent for the last two years.

The good news for users is that functionality and effective solutions are being put in place so they can protect themselves. Practical ways to solve the problem are coming to the fore. IT security companies and advocacy organizations working with domestic abuse victims should join forces to ensure that cybersecurity companies respond better to stalkerware. Such initiatives would help victims through technology and expertise.

We believe that every person has a right to be privacy-protected. That's why we deliver security expertise, work closely with international organizations and law enforcement agencies to fight cybercriminals, as well as develop technologies, solutions and services that help you stay safe from the cyberthreats.

About Kaspersky

With more than 20 years of experience in cybersecurity, Kaspersky's deep threat intelligence and security expertise is constantly transforming into innovative security solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. Over 400 million users are protected by Kaspersky technologies, and we help 270,000 corporate clients protect what matters most to them. Kaspersky's company culture is based on transparency, trust and a global mindset with over 3,900 specialists in 35 offices in 31 countries.

www.kaspersky.com

www.securelist.com

kaspersky