Stalkerware Grows 239% Worldwide Over the Past Three Years

2023-03-14

Stalkerware is often installed secretly on mobile phones by abusive spouses, ex partners and other close contacts to spy on their targets

TEMPE, Ariz. and PRAGUE, March 14, 2023 /PRNewswire/ -- The risk of encountering stalkerware on a mobile device increased 239% globally over a three-year period according to the latest threat telemetry from Avast, a leading digital security and privacy brand of Gen™ (NASDAQ: GEN). Stalkerware, a category of malware and form of tech abuse, steals the physical and online freedom of the targeted person by covertly tracking their location and monitoring smartphone activity, including websites visited, text messages and phone calls.

"The growth we're seeing in stalkerware is a huge concern," said Jakub Vavra, Threat Operations Analyst at Avast. "Stalkerware is often installed secretly on mobile phones by abusive spouses, ex-partners, so-called friends or concerned parents, and has the capacity to inflict serious physical and psychological harm on those affected. This is not only about stealing personal data, there are also tangible implications concerning the safety of the individual targeted."

Over the past three years, Threat Researchers at Avast, which is part of the Coalition Against Stalkerware, have discovered a diverse range of mobile applications intended for non-consensual stalking and have worked with app stores such as Google Play to facilitate their removal. Recently, their analysis has found that child surveillance apps that can remotely control affected devices and stay hidden have become some of the most prevalent forms of stalkerware, and are often misused for monitoring calls, SMS, internet activity and social media, recording audio and video, taking photos or screenshots of a person's phone, and tracking live locations. Another common type of stalkerware are apps that market themselves as lost or stolen device trackers. Once installed on a device they either hide themselves completely or present themselves as Notes applications to evade detection from the unsuspecting phone owner. The stalker can control these apps remotely and carry out similar malicious activity.

"Avast detects and blocks stalkerware with a combination of automation and human intervention to ensure an optimal level of protection from new and evolving threats," continued Vavra. "We'll continue to do all we can to protect people's liberties and their online freedoms from this growing problem."

"Stalkerware is an invasive monitoring tool abusers use to perpetrate stalking, harassment, and other forms of violence and abuse. National Network to End Domestic Violence (NNEDV) is deeply concerned about the significant increase in the use of stalkerware and the dangerous implications for survivors domestic and dating violence and sexual assault," said Erica Olsen, Senior Director of Safety Net Project at NNEDV. "Our Safety Net Project conducted an assessment of service providers documenting that the most common types of technology abuse – harassment, limiting access to tech, and surveillance – all increased during the pandemic. We are grateful for Gen's partnership and dedication to addressing stalkerware and survivor safety."

Below is some guidance from Avast Threat Researchers to help people identify the signs of potential stalkerware applications and how to protect themselves from them:

- Your device's performance is suddenly and unexpectedly worse. You may notice slow-downs or more frequent crashes or freezes.
- Your settings have changed without your consent. If you suddenly have a new browser homepage, new icons on your desktop, a different default search engine, or other changes that you did not make, it might be due to stalkerware.
- You get odd messages, such as a sudden flood of pop-ups or error messages from programs that always worked fine before.
- You have unexplained calls on your bill.
- The abuser has had physical access to your device.
- The abuser knows things about what you are doing, where you are going and who you have been communicating with.

How to prevent stalkerware if you think you are at risk:

- Secure your phone against all unauthorized physical access. Ensure your phone or device uses two-factor authentication such as a pin code and a second form of identity confirmation, for example an email backup or thumbprint.
- Install a reliable antivirus product on your mobile phone. A good mobile antivirus will treat stalkerware as a potentially unwanted program (PUP) and give you the option to remove it.

How to manually remove stalkerware from your phone:

- First, in a situation of coercive control, removing stalkerware from your phone could inform the abuser that you have found and deleted it, which could put your physical safety at risk. Therefore, make sure you are free from harm before removing the stalkerware application from your phone.
- Reboot your phone into safe mode. Hold down your phone's power button to see your Power off and Restart options. Long-press the Power off option and the Reboot to safe-mode option will appear. Tap OK.
- Remove any suspicious apps. Once rebooted in safe mode, open your Settings, and tap Apps or Apps & notifications. Sort through your apps and look for anything you do not recognize.
- Remove any malicious apps. Tap Uninstall to remove it from your device. If you're not sure if an app is malicious, search for the name of the app on the internet to see if other people have shared any issues with it.

About Avast:
Avast is a leader in digital security and privacy, and a brand of Gen™ (NASDAQ: GEN), a global company dedicated to powering Digital Freedom through a family of trusted consumer brands. Avast protects hundreds of millions of users from online threats with a threat detection network that is among the most advanced in the world, using machine learning and artificial intelligence technologies to detect and stop threats in real time. Avast digital security products for Mobile, PC or Mac are top-ranked and certified by VB100, AV-Comparatives, AV-Test, SE Labs, and others. Avast is a member of the Coalition Against Stalkerware, No More Ransom and Internet Watch Foundation. Visit: www.avast.com.

Keep in touch with Avast:

- For security and privacy insights, visit the Avast blog:https://blog.avast.com/
- For in-depth technical analysis of threats, visit the Avast Decoded blog: https://decoded.avast.io/
- For handy guides, advice, and tips, visit Avast Academy:https://www.avast.com/c-academy
- For more information about Avast visit: https://www.avast.com/en-gb/about and

https://www.avast.com/company-faqs
- Follow us on Twitter: @Avast
- Join our LinkedIn community: https://www.linkedin.com/company/avast
- Visit our Facebook group:www.facebook.com/avast

Methodology

The data included in this report was collected from Avast's threat detection network and represents stalkerware detected and blocked on mobile devices between January 2020 and December 2022.

"Risk" refers to the risk ratio which is defined as the ratio of people targeted by stalkerware and actively protected by Avast in the given country and month relative to the total number of active users in the given country and month.

Avast Threat Researchers found the number of people targeted by stalkerware worldwide grew from an average rate of 18 per 100,000 people in 2020 to 61 per 100,000 in 2022.

Media contact:

pr@avast.com

View original content to download multimedia:https://www.prnewswire.com/news-releases/stalkerware-grows-239-worldwide-over-the-past-three-years-301771135.html

SOURCE Gen Digital Inc.