The New York Times https://www.nytimes.com/2021/09/29/technology/personaltech/stalkerware-apps-protection.html

TECH FIX

Stalkerware’ Apps Are Proliferating. Protect Yourself.

These spyware apps record your conversations, location and everything you type, all while camouflaged as a calculator or calendar.

By Brian X. Chen

Published Sept. 29, 2021 Updated Sept. 30, 2021

It looked like a calculator app. But it was actually spyware recording my every keystroke — the type of data that would give a stalker unfettered access to my private life.

That’s what I concluded after downloading the free app Flash Keylogger onto an Android smartphone this week. The app described itself as a tool to monitor the online activities of family members by logging what they type. Once it was installed from Google’s official app store, its icon could be changed to that of a calculator or calendar app. In my tests, the app documented all of my typing, including web searches, text messages and emails.

Flash Keylogger is part of a rapidly expanding group of apps known as “stalkerware.” While these apps numbered in the hundreds a few years ago, they have since grown into the thousands. They are widely available on Google’s Play Store and to a lesser degree on Apple’s App Store, often with innocuous names like MobileTool, Agent and Cerberus. And they have become such a tool for digital domestic abuse that Apple and Google have started in the last year acknowledging that the apps are an issue.

From last September to May, the number of devices infected with stalkerware jumped 63 percent, according to a study by the security firm NortonLifeLock. This month, the Federal Trade Commission said it had barred one app maker, Support King, from offering SpyFone, a piece of stalkerware that gains access to a victim’s location, photos and messages. It was the first ban of its kind.

“It’s extremely invasive, it’s a very big deal and it’s linked to some of the worst abuse I’ve seen in intimate partner abuse,” Eva Galperin, a cybersecurity director at the Electronic Frontier Foundation, the digital rights organization, said of the apps.

Stalkerware is a thorny issue because it lives in a gray area. There are legitimate uses for surveillance apps, like parental control software that monitors children online to protect them from predators. But this technology becomes stalkerware when it’s stealthily installed on a partner’s phone to spy on him or her without consent.

Such apps are more pervasive on phones running Android, researchers said, because the more open nature of Google’s software system gives the programs deeper access to device data and lets people install whatever apps they want on their phones. Yet new stalking software targeting iPhones has also emerged.

Let Us Help You Protect Your Digital Life

- With Apple’s latest mobile software update, we can decide whether apps monitor and share our activities with others. Here’s what to know.
- A little maintenance on your devices and accounts can go a long way in maintaining your security against outside parties’ unwanted attempts to access your data. Here’s a guide to the few simple changes you can make to protect yourself and your information online.
- Ever considered a password manager? You should.
- There are also many ways to brush away the tracks you leave on the internet.

Google said it banned apps that violated its policies, including the Flash Keylogger app after I contacted Google about it.

An Apple spokesman referred me to a safety guide that it published last year in response to the threat of these apps. He added that the new stalkerware was not a vulnerability in the iPhone that could be fixed with technology if an abuser had access to a person’s device and passcode.

Fighting stalkerware is tough. You may not suspect it’s there. Even if you did, it can be difficult to detect since antivirus software only recently began flagging these apps as malicious.

Here’s a guide to how stalkerware works, what to look out for and what to do about it.

The Different Types of Stalkerware

Surveillance software has proliferated on computers for decades, but more recently spyware makers have shifted their focus to mobile devices. Because mobile devices have access to more intimate data, including photos, real-time location, phone conversations and messages, the apps became known as stalkerware.

Various stalkerware apps collect different types of information. Some record phone calls, some log keystrokes, and others track location or upload a person's photos to a remote server. But they all generally work the same way: An abuser with access to a victim's device installs the app on the phone and disguises the software as an ordinary piece of software, like a calendar app.

From there, the app lurks in the background, and later, the abuser retrieves the data. Sometimes, the information gets sent to the abuser's email address or it can be downloaded from a website. In other scenarios, abusers who know their partner's passcode can simply unlock the device to open the stalkerware and review the recorded data.

Self-Defense Steps

So what to do? The Coalition Against Stalkerware, which was founded by Ms. Galperin and other groups, and many security firms offered these tips:

- **Look for unusual behavior on your device**, like a rapidly draining battery. That could be a giveaway that a stalker app has been constantly running in the background.

- **Scan your device**. Some apps, like MalwareBytes, Certo, NortonLifeLock and Lookout, can detect stalkerware. But to be thorough, take a close look at your apps to see if anything is unfamiliar or suspicious. If you find a piece of stalkerware, pause before you delete it: It may be useful evidence if you decide to report the abuse to law enforcement.

- **Seek help.** In addition to reporting stalking behavior to law enforcement, you can seek advice from resources like the National Domestic Violence Hotline or the Safety Net Project hosted by the National Network to End Domestic Violence.

- **Audit your online accounts** to see which apps and devices are hooked into them. On Twitter, for example, you can click on the "security and account access" button inside the settings menu to see which devices and apps have access to your account. Log out of anything that looks shady.

- **Change your passwords and passcode.** It's always safer to change passwords for important online accounts and avoid reusing passwords across sites. Try creating long, complex passwords for each account. Similarly, make sure your passcode is difficult for someone to guess.

- **Enable two-factor authentication.** For any online account that offers it, use two-factor authentication, which basically requires two forms of verification of your identity before letting you log into an account. Say you enter your user name and password for your Facebook account. That's Step 1. Facebook then asks you to punch in a temporary code generated by an authentication app. That's Step 2. With this protection, even if an abuser figures out your password using a piece of stalkerware, he or she still can't log in without that code.

- **On iPhones, check your settings.** A new stalker app, WebWatcher, uses a computer to wirelessly download a backup copy of a victim's iPhone data, according to Certo, a mobile security firm. To defend yourself, open the Settings app and look at the General menu to see if "iTunes Wi-Fi Sync" is visible. If it shows up, disabling this will prevent WebWatcher from copying your data.

  Apple said this was not considered an iPhone vulnerability because it required an attacker to be on the same Wi-Fi network and have physical access to a victim's unlocked iPhone.

- **Start fresh.** Buying a new phone or erasing all the data from your phone to begin anew is the most effective way to rid a device of stalkerware.

- **Update your software.** Apple and Google regularly issue software updates that include security fixes, which can remove stalkerware. Make sure you're running the latest software.

In the end, there's no true way to defeat stalkerware. Kevin Roundy, NortonLifeLock's lead researcher, said he had reported more than 800 pieces of stalkerware inside the Android app store. Google removed the apps and updated its policy in October to forbid developers to offer stalkerware.

But more have emerged to take their place.

"There are definitely a lot of very dangerous, alarming possibilities," Mr. Roundy said. "It's going to continue to be a concern."