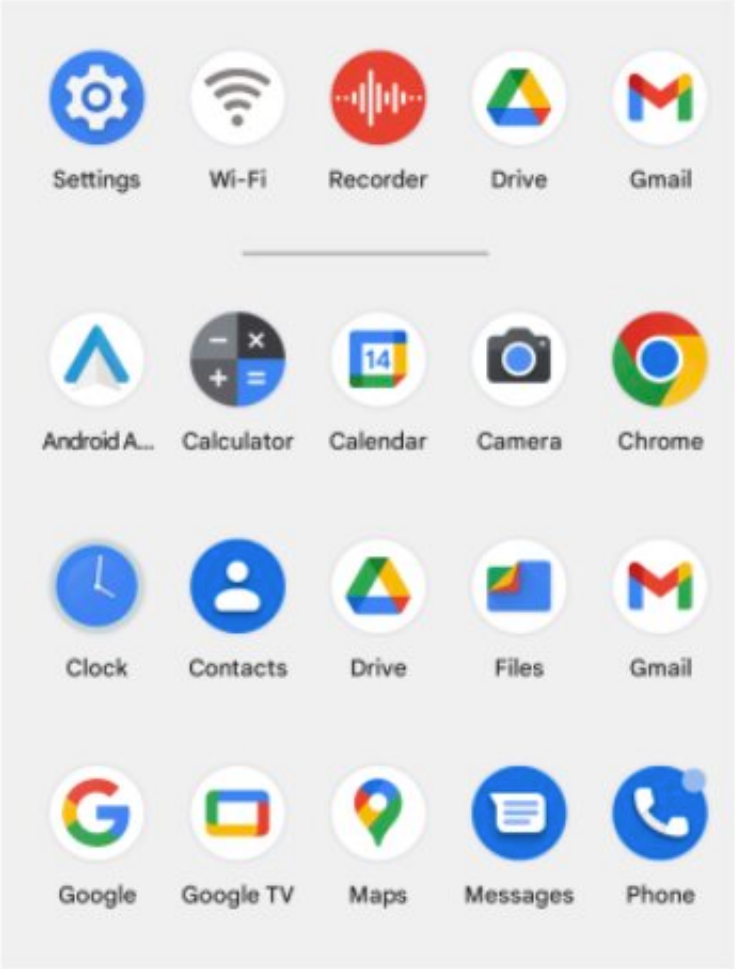
This is what happens when your phone is spying on you

March 14 2023



This app launcher on an Androip phone displays app icons: the Spyhuman app installed itself as the innocuous-seeming WiFi icon. What are spyware apps? Spyware apps surreptitiously run on a device, most often without the device owner's awareness. They collect a range of sensitive information such as location, texts and calls, as well as audio and video. Some apps can even stream

live audio and video. All this information is delivered to an abuser via an online spyware portal. Credit: Jacobs School of Engineering/University of California San Diego

Smartphone spyware apps that allow people to spy on each other are not only hard to notice and detect, they also will easily leak the sensitive personal information they collect, says a team of computer scientists from New York and San Diego.

While publicly marketed as tools to monitor underage children and employees using their employer's equipment, spyware apps are also frequently used by abusers to covertly spy on a spouse or a partner.

These apps require little to no technical expertise from the abusers; offer detailed installation instructions; and only need temporary access to a victim's device. After installation, they covertly record the victim's device activities—including any text messages, emails, photos, or voice calls—and allow abusers to remotely review this information through a web portal.

Spyware has become an increasingly serious problem. In one recent study from Norton Labs, the number of devices with spyware apps in the United States increased by 63% between September 2020 and May 2021. A similar report from Avast in the United Kingdom recorded a stunning 93% increase in the use of spyware apps over a similar period.

If you want to know if your device has been infected by one of these apps, you should check your privacy dashboard and the listing of all apps in settings, the research team says.

"This is a real-life problem and we want to raise awareness for everyone,

from victims to the research community," said Enze Alex Liu, the first author of the paper No Privacy Among Spies: Assessing the Functionality and Insecurity of Consumer Android Spyware Apps and a computer science Ph.D. student at the University of California San Diego.

Liu and the research team will present their work at the Privacy Enhancing Technologies Symposium in summer 2023 in Switzerland.

Researchers performed an in-depth technical analysis of 14 leading spyware apps for Android phones. While Google does not permit the sale of such apps on its Google Play app store, Android phones commonly allow such invasive apps to be downloaded separately via the Web. The iPhone, in comparison, does not allow such "side loading" and thus consumer spyware apps on this platform tend to be far more limited and less invasive in capabilities.

What are spyware apps?

Spyware apps surreptitiously run on a device, most often without the device owner's awareness. They collect a range of sensitive information such as location, texts and calls, as well as audio and video. Some apps can even stream live audio and video. All this information is delivered to an abuser via an online spyware portal.

Spyware apps are marketed directly to the general public and are relatively cheap–typically between $30 and $100 per month. They are easy to install on a smartphone and require no specialized knowledge to deploy or operate. But users need to have temporary physical access to their target's device and the ability to install apps that are not in the pre-approved app stores.

How do spyware apps gather data?

Researchers found that spyware apps use a wide range of techniques to surreptitiously record data. For example, one app uses an invisible browser that can stream live video from the device's camera to a spyware server. Apps also are able to record phone calls via the device's microphone, sometimes activating the speaker function in hopes of capturing what interlocutors are saying as well.

Several apps also exploit accessibility features on smartphones, designed to read what appears on the screen for vision-impaired users. On Android, these features effectively allow spyware to record keystrokes, for example.

Researchers also found several methods the apps use to hide on the target's device.

For example, apps can specify that they do not appear in the launch bar when they initially open. App icons also masquerade as "Wi-Fi" or "Internet Service."

Four of the spyware apps accept commands via SMS messages. Two of the apps the researchers analyzed didn't check whether the text message came from their client and executed the commands anyway. One app could even execute a command that could remotely wipe the victim's phone.

Gaps in data security

Researchers also investigated how seriously spyware apps protected the sensitive user data they collected. The short answer is: not very seriously. Several spyware apps use unencrypted communication channels to

transmit the data they collect, such as photos, texts and location. Only four out of the 14 the researchers studied did this. That data also includes login credentials of the person who bought the app. All this information could be easily harvested by someone else over WiFi.

In a majority of the applications the researchers analyzed, the same data is stored in public URLs accessible to anyone with the link. In addition, in some cases, user data is stored in predictable URLs that make it possible to access data across several accounts by simply switching out a few characters in the URLs. In one instance, the researchers identified an authentication weakness in one leading spyware service that would allow all the data for every account to be accessed by any party.

Moreover, many of these apps retain sensitive data without a customer contract or after a customer has stopped using them. Four out of the 14 apps studied don't delete data from the spyware servers even if the user deleted their account or the app's license expired. One app captures data from the victim during a free trial period, but only makes it available to the abuser after they paid for a subscription. And if the abuser doesn't get a subscription, the app keeps the data anyway.

How to counter spyware

"Our recommendation is that Android should enforce stricter requirements on what apps can hide icons," researchers write. "Most apps that run on Android phones should be required to have an icon that would appear in the launch bar."

Researchers also found that many spyware apps resisted attempts to uninstall them. Some also automatically restarted themselves after being stopped by the Android system or after device reboots. "We recommend adding a dashboard for monitoring apps that will automatically start themselves," the researchers write.

To counter spyware, Android devices use various methods, including a visible indicator to the user that can't be dismissed while an app is using the microphone or camera. But these methods can fail for various reasons. For example, legitimate uses of the device can also trigger the indicator for the microphone or camera.

"Instead, we recommend that all actions to access sensitive data be added to the privacy dashboard and that users should be periodically notified of the existence of apps with an excessive number of permissions," the researchers write.

Disclosures, safeguards and next steps

Researchers disclosed all their findings to all the affected app vendors. No one replied to the disclosures by the paper's publication date.

In order to avoid abuse of the code they developed, the researchers will only make their work available upon request to users that can demonstrate they have a legitimate use for it.

Future work will continue at New York University, in the group of associate professor Damon McCoy, who is a UC San Diego Ph.D. alumnus. Many spyware apps seem to be developed in China and Brazil, so further study of the supply chain that allows them to be installed outside of these countries is needed.

"All of these challenges highlight the need for a more creative, diverse and comprehensive set of interventions from industry, government and the research community," the researchers write. "While technical defenses can be part of the solution, the problem scope is much bigger. A broader range of measures should be considered, including payment interventions from companies such as Visa and Paypal, regular crackdowns from the government, and further law enforcement action

may also be necessary to prevent surveillance from becoming a consumer commodity."

More information: Report: www.sysnet.ucsd.edu/~voelker/p … s/spyware-pets23.pdf

Provided by University of California - San Diego